Contents

TWO USEFUL SUBSTITUTIONS

We know that in most inequalities with a constraint such as $abc = 1$ the substitution $a = \frac{x}{y}$, $b = \frac{y}{z}$, $c = \frac{z}{x}$ simplifies the solution (don't kid yourself, not all problems of this type become easier!). But have you ever thought about other similar substitutions? For example, what if we had the conditions $x, y, z > 0$ and $xyz = x + y + z + 2$? Or $x, y, z > 0$ and $xy + yz + zx + 2xyz = 1$? There are numerous problems that reduce to these conditions and to their corresponding substitutions. You will be probably surprised when finding out that the first set of conditions implies the existence of positive real numbers a, b, c such that

$$x = \frac{b+c}{a}, \quad y = \frac{c+a}{b}, \quad z = \frac{a+b}{c}.$$

Let us explain why. The condition $xyz = x+y+z+2$ can be written in the following equivalent way:

$$\frac{1}{1+x} + \frac{1}{1+y} + \frac{1}{1+z} = 1.$$

Proving this is just a matter of simple computations. Take now

$$a = \frac{1}{1+x}, \quad b = \frac{1}{1+y}, \quad c = \frac{1}{1+z}.$$

Then $a + b + c = 1$ and $x = \frac{1-a}{a} = \frac{b+c}{a}$. Of course, in the same way we find $y = \frac{c+a}{b}$, $z = \frac{a+b}{c}$. The converse (that is, $\frac{b+c}{a}$, $\frac{c+a}{b}$, $\frac{a+b}{c}$ satisfy $xyz = x+y+z = 2$) is much easier and is settled again by basic computations. Now, what about the second set of conditions? If you look carefully, you will see that it is closely related to the first one. Indeed, $x, y, z > 0$ satisfy $xy + yz + zx + 2xyz = 1$ if and only if $\frac{1}{x}$, $\frac{1}{y}$, $\frac{1}{z}$ verify $\frac{1}{xyz} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + 2$, so the substitution here is

$$x = \frac{a}{b+c}, \quad y = \frac{b}{c+a}, \quad z = \frac{c}{a+b}.$$

So, let us summarize: we have seen two nice substitutions, with even nicer proofs, but we still have not seen any applications. We will see them in a moment ... and there are quite a few inequalities that can be solved by using these "tricks".

First, an easy and classical problem, due to Nesbitt. It has so many extensions and generalizations, that we must discuss it first.

Example 1. Prove that

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}\geq\frac{3}{2}$$

for all $a,b,c>0$.

Solution. With the "magical" substitution, it suffices to prove that if $x,y,z>0$ satisfy $xy+yz+zx+2xyz=1$, then $x+y+z=\frac{3}{2}$. Let us suppose that this is not the case, i.e. $x+y+z<\frac{3}{2}$. Because $xy+yz+zx\leq\frac{(x+y+z)^2}{3}$, we must have $xy+yz+zx<\frac{3}{4}$ and since $xyz\leq\left(\frac{x+y+z}{3}\right)^3$, we also have $2xyz<\frac{1}{4}$. It follows that $1=xy+yz+zx+2xyz<\frac{3}{4}+\frac{1}{4}=1$, a contradiction, so we are done.

Let us now increase the level of difficulty and make an experiment: imagine that you did not know about these substitutions and try to solve the following problem. Then look at the solution provided and you will see that sometimes a good substitution can solve a problem almost alone.

Example 2. Let $x,y,z>0$ such that $xy+yz+zx+2xyz=1$. Prove that

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\geq 4(x+y+z).$$

Mircea Lascu, Marian Tetiva

Solution. With our substitution the inequality becomes

$$\frac{b+c}{a}+\frac{c+a}{b}+\frac{a+b}{c}\geq 4\left(\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}\right).$$

But this follows from

$$\frac{4s}{b+c} \leq \frac{a}{b} + \frac{a}{c}, \quad \frac{4b}{c+a} \leq \frac{b}{c} + \frac{b}{a}, \quad \frac{4c}{a+b} \leq \frac{c}{a} + \frac{c}{b}.$$

Simple and efficient, these are the words that characterize this substitution.

Here is a geometric application of the previous problem.

Example 3. Prove that in any acute-angled triangle ABC the following inequality holds

$$\cos^2 A \cos^2 B + \cos^2 B \cos^2 C + \cos^2 C \cos^2 A \leq \frac{1}{4}(\cos^2 A + \cos^2 B + \cos^2 C).$$

Titu Andreescu

Solution. We observe that the desired inequality is equivalent to

$$\frac{\cos A \cos B}{\cos C} + \frac{\cos B \cos C}{\cos A} + \frac{\cos A \cos C}{\cos B} \leq$$

$$\leq \frac{1}{4}\left(\frac{\cos A}{\cos B \cos C} + \frac{\cos B}{\cos C \cos A} + \frac{\cos C}{\cos A \cos B}\right)$$

Setting

$$x = \frac{\cos B \cos C}{\cos A}, \quad y = \frac{\cos A \cos C}{\cos B}, \quad z = \frac{\cos A \cos B}{\cos C},$$

the inequality reduces to

$$4(x + y + z) \leq \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

But this is precisely the inequality in the previous example. All that remains is to show that $xy + yz + zx + 2xyz = 1$. This is equivalent to

$$\cos^2 A + \cos^2 B + \cos^2 C + 2\cos A \cos B \cos C = 1,$$

a well-known identity, proved in the chapter "Equations and beyond".

The level of difficulty continues to increase. When we say this, we refer again to the proposed experiment. The reader who will try first to solve the problems discussed without using the above substitutions will certainly understand why we consider these problems hard.

Example 4. Prove that if $x, y, z > 0$ and $xyz = x + y + z + 2$, then

$$2(\sqrt{xy} + \sqrt{yz} + \sqrt{zx}) \leq x + y + z + 6.$$

Mathlinks site

Solution. This is tricky, even with the substitution. There are two main ideas: using some identities that transform the inequality into an easier one and then using the substitution. Let us see. What does $2(\sqrt{xy} + \sqrt{yz} + \sqrt{zx})$ suggest? Clearly, it is related to

$$(\sqrt{x} + \sqrt{y} + \sqrt{z})^2 - (x + y + z).$$

Consequently, our inequality can be written as

$$\sqrt{x} + \sqrt{y} + \sqrt{z} \leq \sqrt{2(x + y + z + 3)}.$$

The first idea that comes to mind (that is using the Cauchy-Schwarz inequality in the form $\sqrt{x} + \sqrt{y} + \sqrt{z} \leq \sqrt{3(x + y + z)} \leq \sqrt{2(x + y + z + 3)}$) does not lead to a solution. Indeed, the last inequality is not true: setting $x+y+z = s$, we have $3s \leq 2(s+3)$. This is because from the AM-GM inequality it follows that $xyz \leq \dfrac{s^3}{27}$, so $\dfrac{s^3}{27} \geq s + 2$, which is equivalent to $(s - 6)(s + 3)^2 \geq 0$, implying $s \geq 6$.

Let us see how the substitution helps. The inequality becomes

$$\sqrt{\frac{b+c}{a}} + \sqrt{\frac{c+a}{b}} + \sqrt{\frac{a+b}{c}} \leq \sqrt{2\left(\frac{b+c}{a} + \frac{c+a}{b} + \frac{a+b}{c} + 3\right)}$$

The last step is probably the most important. We have to change the expression $\dfrac{b+c}{a} + \dfrac{c+a}{b} + \dfrac{a+b}{c} + 3$ a little bit.

We see that if we add 1 to each fraction, then $a + b + c$ will appear as common factor, so in fact

$$\frac{b+c}{a} + \frac{c+a}{b} + \frac{a+b}{c} + 3 = (a + b + c)\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right).$$

And now we have finally solved the problem, amusingly, by employing again the Cauchy-Schwarz inequality:

$$\sqrt{\frac{b+c}{a}}+\sqrt{\frac{c+a}{b}}+\sqrt{\frac{a+b}{c}}\leq\sqrt{(b+c+c+a+a+b)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)}.$$

We continue with a 2003 USAMO problem. There are many proofs for this inequality, none of them easy. The following solution is again not easy, but it is natural for someone familiar with this kind of substitution.

Example 5. Prove that for any positive real numbers a,b,c the following inequality holds

$$\frac{(2a+b+c)^2}{2a^2+(b+c)^2}+\frac{(2b+c+a)^2}{2b^2+(c+a)^2}+\frac{(2c+a+b)^2}{2c^2+(a+b)^2}\leq 8.$$

Titu Andreescu, Zuming Feng, USAMO 2003

Solution. The desired inequality is equivalent to

$$\frac{\left(1+\frac{b+c}{a}\right)^2}{2+\left(\frac{b+c}{a}\right)^2}+\frac{\left(2+\frac{c+a}{b}\right)^2}{2+\left(\frac{c+a}{b}\right)^2}+\frac{\left(1+\frac{a+b}{c}\right)^2}{2+\left(\frac{a+b}{c}\right)^2}\leq 8.$$

Taking our substitution into account, it suffices to prove that if $xyz=x+y+z+2$, then

$$\frac{(2+x)^2}{2+x^2}+\frac{(2+y)^2}{2+y^2}+\frac{(2+z)^2}{2+z^2}\leq 8.$$

This is in fact the same as

$$\frac{2x+1}{x^2+2}+\frac{2y+1}{y^2+2}+\frac{2z+1}{z^2+2}\leq\frac{5}{2}.$$

Now, we transform this inequality into

$$\frac{(x-1)^2}{x^2+2}+\frac{(y-1)^2}{y^2+2}+\frac{(z-1)^2}{z^2+2}\geq\frac{1}{2}.$$

This last form suggests using the Cauchy-Schwarz inequality to prove that

$$\frac{(x-1)^2}{x^2+2}+\frac{(y-1)^2}{y^2+2}+\frac{(z-1)^2}{z^2+2}\geq\frac{(x+y+z-3)^2}{x^2+y^2+z^2+6}.$$

So, we are left with proving that $2(x+y+z-3)^2 \geq x^2+y^2+z^2+6$. But this is not difficult. Indeed, this inequality is equivalent to

$$2(x+y+z-3)^2 \geq (x+y+z)^2 - 2(xy+yz+zx) + 6.$$

Now, from $xyz \geq 8$ (recall who x, y, z are and use the AM-GM inequality three times), we find that $xy+yz+zx \geq 12$ and $x+y+z \geq 6$ (by the same AM-GM inequality). This shows that it suffices to prove that $2(s-3)^2 \geq s^2-18$ for all $s \geq 6$, which is equivalent to $(s-3)(s-6) \geq 0$, clearly true. And this difficult problem is solved!

The following problem is also hard. We have seen a difficult solution in the chapter "Equations and beyond". Yet, there is an easy solution using the substitutions described in this unit.

Example 6. Prove that if $x, y, z \geq 0$ satisfy $xy+yz+zx+xyz = 4$ then $x+y+z \geq xy+yz+zx$.

India, 1998

Solution. Let us write the given condition as

$$\frac{x}{2}\cdot\frac{y}{2} + \frac{y}{2}\cdot\frac{z}{2} + \frac{z}{2}\cdot\frac{x}{2} + 2\frac{x}{2}\cdot\frac{y}{2}\cdot\frac{z}{2} = 1.$$

Hence there are positive real numbers a, b, c such that

$$x = \frac{2a}{b+c}, \quad y = \frac{2b}{c+a}, \quad z = \frac{2c}{a+b}.$$

But now the solution is almost over, since the inequality

$$x+y+z \geq xy+yz+zx$$

is equivalent to

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{2ab}{(c+a)(c+b)} + \frac{2bc}{(a+b)(a+c)} + \frac{2ca}{(b+a)(b+c)}.$$

After clearing denominators, the inequality becomes

$$a(a+b)(a+c) + b(b+a)(b+c) + c(c+a)(c+b) \geq$$

$$\geq 2ab(a+b)+2bc(b+c)+2ca(c+a).$$

After basic computations, it reduces to

$$a(a-b)(a-c)+b(b-a)(b-c)+c(c-a)(c-b)\geq 0.$$

But this is Schur's inequality!

We end the discussion with a difficult problem, in which the substitution described plays a key role. But this time using the substitution only will not suffice.

Example 7. Prove that if $x,y,z>0$ satisfy $xyz=x+y+z+2$, then $xyz(x-1)(y-1)(z-1)\leq 8$.

Gabriel Dospinescu

Solution. Using the substitution

$$x=\frac{b+c}{a},\quad y=\frac{c+a}{b},\quad z=\frac{a+b}{c},$$

the inequality becomes

$$(a+b)(b+c)(c+a)(a+b-c)(b+c-a)(c+a-b)\leq 8a^2b^2c^2 \qquad (1)$$

for any positive real numbers a,b,c. It is readily seen that this form is stronger than Schur's inequality $(a+b-c)(b+c-a)(c+a-b)\leq abc$. First, we may assume that a,b,c are the sides of a triangle ABC, since otherwise the left-hand side in (1) is negative. This is true because no more than one of the numbers $a+b-c$, $b+c-a$, $c+a-b$ can be negative. Let R be the circumradius of the triangle ABC. It is not difficult to find the formula

$$(a+b-c)(b+c-a)(c+a-b)=\frac{a^2b^2c^2}{(a+b+c)R^2}.$$

Consequently, the desired inequality can be written as

$$(a+b+c)R^2\geq\frac{(a+b)(b+c)(c+a)}{8}.$$

But we know that in any triangle ABC, $9R^2 \geq a^2 + b^2 + c^2$. Hence it suffices to prove that

$$8(a+b+c)(a^2+b^2+c^2) \geq 9(a+b)(b+c)(c+a).$$

This inequality follows from the following ones:

$$8(a+b+c)(a^2+b^2+c^2) \geq \frac{8}{3}(a+b+c)^3$$

and

$$9(a+b)(b+c)(c+a) \leq \frac{1}{3}(a+b+c)^3.$$

The first inequality reduces to

$$a^2+b^2+c^2 \geq \frac{1}{3}(a+b+c)^2,$$

while the second is a consequence of the AM-GM inequality. By combining these two results, the desired inequality follows.

Problems for training

1. Prove that if $x, y, z > 0$ satisfy $xy + yz + zx + 2xyz = 1$, then

$$xyz \leq \frac{1}{8} \text{ and } xy + yz + zx \geq \frac{3}{4}.$$

2. Prove that for any positive real numbers a, b, c the following inequality holds

$$\frac{b+c}{a} + \frac{c+a}{b} + \frac{a+b}{c} \geq \frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} + \frac{9}{2}.$$

J. Nesbitt

3. Prove that if $x, y, z > 0$ and $xyz = x + y + z + 2$, then

$$xy + yz + zx \geq 2(x+y+z) \text{ and } \sqrt{x} + \sqrt{y} + \sqrt{z} \leq \frac{3}{2}\sqrt{xyz}.$$

4. Let $x, y, z > 0$ such that $xy + yz + zx = 2(x+y+z)$. Prove that $xyz \leq x + y + z + 2$.

Gabriel Dospinescu, Mircea Lascu

5. Prove that in any triangle ABC the following inequality holds

$$\cos A + \cos B + \cos C \geq \frac{1}{4}(3 + \cos(A-B) + \cos(B-C) + \cos(C-A)).$$

Titu Andreescu

6. Prove that in every acute-angled triangle ABC,

$$(\cos A + \cos B)^2 + (\cos B + \cos C)^2 + (\cos C + \cos A)^2 \leq 3.$$

7. Prove that if $a, b, c > 0$ and $x = a + \frac{1}{b}$, $y = b + \frac{1}{c}$, $z = c + \frac{1}{a}$, then

$$xy + yz + zx \geq 2(x + y + z).$$

Vasile Cartoaje

8. Prove that for any $a, b, c > 0$,

$$\frac{(b+c-a)^2}{(b+c)^2 + a^2} + \frac{(c+a-b)^2}{(c+a)^2 + b^2} + \frac{(a+b-c)^2}{(a+b)^2 + c^2} \geq \frac{3}{5}.$$

Japan, 1997

ALWAYS CAUCHY-SCHWARZ

In recent years the Cauchy-Schwarz inequality has become one of the most used results in elementary mathematics, an indispensable tool of any serious problem solver. There are countless problems that reduce readily to this inequality and even more problems in which the Cauchy-Schwarz inequality is the key idea of the solution. In this unit we will not focus on the theoretical results, since they are too well-known. Yet, seeing the Cauchy-Schwarz inequality at work is not so well spread out. This is the reason why we will see this inequality in action in several simple examples first, employing then gradually the Cauchy-Schwarz inequality in some of the most difficult problems.

Let us begin with a very simple problem, a direct application of the inequality. Yet, it underlines something less emphasized: the analysis of the equality case.

Example 1. Prove that the finite sequence $a_0, a_1, \ldots, a_n$ of positive real numbers is a geometrical progression if and only if

$$(a_0^2+a_1^2+\cdots+a_{n-1}^2)(a_1^2+a_2^2+\cdots+a_n^2) = (a_0a_1+a_1a_2+\cdots+a_{n-1}a_n)^2.$$

Solution. We see that the relation given in the problem is in fact the equality case in the Cauchy-Schwarz inequality. This is equivalent to the proportionality of the n-tuples $(a_0, a_1, \ldots, a_{n-1})$ and $(a_1, a_2, \ldots, a_n)$, that is

$$\frac{a_0}{a_1} + \frac{a_1}{a_2} = \cdots = \frac{a_{n-1}}{a_n}.$$

But this is just actually the definition of a geometrical progression. Hence the problem is solved. Note that Lagrange's identity allowed us to work with equivalences.

Another easy application of the Cauchy-Schwarz inequality is the following problem. This time the inequality is hidden in a closed form,

which suggests using calculus. There exists a solution by using derivatives, but it is not as elegant as the featured one:

Example 2. Let p be a polynomial with positive real coefficients. Prove that $p(x^2)p(y^2) \geq p^2(xy)$ for any positive real numbers x, y.

Russian Mathematical Olympiad

Solution. If we work only with the closed expression $p(x^2)p(y^2) \geq p^2(xy)$, the chances of seeing a way to proceed are small. So, let us write $p(x) = a_0 + a_1x + \cdots + a_nx^n$. The desired inequality becomes

$$(a_0 + a_1x^2 + \cdots + a_nx^{2n})(a_0 + a_1y^2 + \cdots + a_ny^{2n})$$

$$\geq (a_0 + a_1xy + \cdots + a_nx^ny^n)^2.$$

And now the Cauchy-Schwarz inequality comes into the picture:

$$(a_0 + a_1xy + \cdots + a_nx^ny^n)^2$$

$$= (\sqrt{a_0} \cdot \sqrt{a_0} + \sqrt{a_1x^2} \cdot \sqrt{a_2y^2} + \cdots + \sqrt{a_nx^n} \cdot \sqrt{a_ny^n})^2$$

$$\leq (a_0 + a_1x^2 + \cdots + a_nx^{2n})(a_0 + a_1y^2 + \cdots + a_ny^{2n}).$$

And the problem is solved. Moreover, we see that the conditions $x, y > 0$ are useless, since we have of course $p^2(xy) \leq p^2(|xy|)$. Additionally, note an interesting consequence of the problem: the function $f : (0, \infty) \to (0, \infty)$, $f(x) = \ln p(e^x)$ is convex, that is why we said in the introduction to this problem that it has a solution based on calculus. The idea of that solution is to prove that the second derivative of is nonnegative. We will not prove this here, but we note a simple consequence: the more general inequality

$$p(x_1^k)p(x_2^k)\ldots p(x_k^k) \geq p^k(x_1x_2\ldots x_k),$$

which follows the Jensen's inequality for the convex function $f(x) = \ln p(e^x)$.

Here is another application of the Cauchy-Schwarz inequality, though this time you might be surprised why the "trick" fails at a first approach:

Example 3. Prove that if $x, y, z > 0$ satisfy $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$, then

$$\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1} \leq \sqrt{x+y+z}.$$

Iran, 1998

Solution. The obvious and most natural approach is to apply the Cauchy-Schwarz inequality in the form

$$\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1} \leq \sqrt{3(x+y+z-3)}$$

and then to try to prove the inequality $\sqrt{3(x+y+z-3)} \leq \sqrt{x+y+z}$, which is equivalent to $x+y+z \leq \frac{9}{2}$. Unfortunately, this inequality is not true. In fact, the reversed inequality holds, that is $x+y+z \geq \frac{9}{2}$, since $2 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \geq \frac{9}{x+y+z}$. Hence this approach fails. Then, we try another approach, using again the Cauchy-Schwarz inequality, but this time in the form

$$\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1} = \sqrt{a} \cdot \sqrt{\frac{x-1}{a}} + \sqrt{b} \cdot \sqrt{\frac{y-1}{b}} + \sqrt{c} \cdot \sqrt{\frac{z-1}{c}}$$

$$\leq \sqrt{(a+b+c)\left(\frac{x-1}{a} + \frac{y-1}{b} + \frac{z-1}{c}\right)}.$$

We would like to have the last expression equal to $\sqrt{x+y+z}$. This encourages us to take $a = x$, $b = y$, $c = z$, since in this case

$$\frac{x-1}{a} + \frac{y-1}{b} + \frac{z-1}{c} = 1 \text{ and } a+b+c = x+y+z.$$

So, this idea works and the problem is solved.

We continue with a classical result, the not so well-known inequality of Aczel. We will also see during our trip through the exciting world of the Cauchy-Schwarz inequality a nice application of Aczel's inequality.

Example 4. Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be real numbers and let $A, B > 0$ such that

$$A^2 \geq a_1^2 + a_2^2 + \cdots + a_n^2 \text{ or } B^2 \geq b_1^2 + b_2^2 + \cdots + b_n^2.$$

Then

$$(A^2 - a_1^2 - a_2^2 - \cdots - a_n^2)(B^2 - b_1^2 - b_2^2 - \cdots - b_n^2)$$
$$\leq (AB - a_1b_1 - a_2b_2 - \cdots - a_nb_n)^2.$$

Solution. We observe first that we may assume that

$$A^2 > a_1^2 + a_2^2 + \cdots + a_n^2 \text{ and } B^2 > b_1^2 + b_2^2 + \cdots + b_n^2.$$

Otherwise the left-hand side of the desired inequality is smaller than or equal to 0 and the inequality becomes trivial. From our assumption and the Cauchy-Schwarz inequality, we infer that

$$a_1b_1+a_2b_2+\cdots+a_nb_n \leq \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}\cdot\sqrt{b_1^2 + b_2^2 + \cdots + b_n^2} < AB$$

Hence we can rewrite the inequality in the more appropriate form

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n + \sqrt{(A^2 - a)(B^2 - b)} \leq AB,$$

where $a = a_1^2 + a_2^2 + \cdots + a_n^2$ and $b = b_1^2 + b_2^2 + \cdots + b_n^2$. Now, we can apply the Cauchy-Schwarz inequality, first in the form

$$a_1b_1+a_2b_2+\cdots+a_nb_n+\sqrt{(A^2 - a)(B^2 - b)} \leq \sqrt{ab}+\sqrt{(A^2 - a)(B^2 - b)}$$

and then in the form

$$\sqrt{ab} + \sqrt{(A^2 - a)(B^2 - b)} \leq \sqrt{(a + A^2 - a)(b + B^2 - b)} = AB.$$

And by combining the last two inequalities the desired inequality follows.

As a consequence of this inequality we discuss the following problem, in which the condition seems to be useless. In fact, it is the key that suggests using Aczel's inequality.

Example 5. Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be real numbers such that

$$(a_1^2+a_2^2+\cdots+a_n^2-1)(b_1^2+b_2^2+\cdots+b_n^2-1) > (a_1b_1+a_2b_2+\cdots+a_nb_n-1)^2.$$

Prove that $a_1^2 + a_2^2 + \cdots + a_n^2 > 1$ and $b_1^2 + b_2^2 + \cdots + b_n^2 > 1$.

Titu Andreescu, Dorin Andrica, TST 2004, USA

Solution. At first glance, the problem does not seem to be related to Aczel's inequality. Let us take a more careful look. First of all, it is not difficult to observe that an indirect approach is more efficient. Moreover, we may even assume that both numbers $a_1^2+a_2^2+\cdots+a_n^2-1$ and $b_1^2 + b_2^2 + \cdots + b_n^2 - 1$ are negative, since they have the same sign (this follows immediately from the hypothesis of the problem). Now, we want to prove that

$$(a_1^2 + a_2^2 + \cdots + a_n^2 - 1)(b_1^2 + b_2^2 + \cdots + b_n^2 - 1)$$

$$\leq (a_1b_1 + a_2b_2 + \cdots + a_nb_n - 1)^2 \tag{1}$$

in order to obtain the desired contradiction. And all of a sudden we arrived at the result in the previous problem. Indeed, we have now the conditions $1 > a_1^2 + a_2^2 + \cdots + a_n^2$ and $1 > b_1^2 + b_2^2 + \cdots + b_n^2$, while the conclusion is (1). But this is exactly Aczel's inequality, with $A = 1$ and $B = 1$. The conclusion follows.

Of a different kind, the following example shows that an apparently very difficult inequality can become quite easy if we do not complicate things more than necessary. It is also a refinement of the Cauchy-Schwarz inequality, as we can see from the solution.

Example 6. For given $n > k > 1$ find in closed form the best constant $T(n, k)$ such that for any real numbers $x_1, x_2, \ldots, x_n$ the following

inequality holds:

$$\sum_{1\le i<j\le n}(x_i-x_j)^2 \ge T(n,k)\sum_{1\le i<j\le k}(x_i-x_j)^2.$$

Gabriel Dospinescu

Solution. In this form, we cannot make any reasonable conjecture about $T(n,k)$, so we need an efficient transformation. We observe that $\sum_{1\le i<j\le n}(x_i-x_j)^2$ is nothing else than $n\sum_{i=1}^{n}x_i^2-\left(\sum_{i=1}^{n}x_i\right)^2$ and also

$$\sum_{1\le i<j\le k}(x_i-x_j)^2 = k\sum_{i=1}^{k}x_i^2-\left(\sum_{i=1}^{k}x_i\right)^2,$$

according to Lagrange's identity. Consequently, the inequality can be written in the equivalent form

$$n\sum_{i=1}^{n}x_i^2-\left(\sum_{i=1}^{n}x_i\right)^2 \ge T(n,k)\left[k\sum_{i=1}^{k}x_i^2-\left(\sum_{i=1}^{k}x_i\right)^2\right].$$

And now we see that it is indeed a refinement of the Cauchy-Schwarz inequality, only if in the end it turns out that $T(n,k)>0$. We also observe that in the left-hand side there are $n-k$ variables that do not appear in the right-hand side and that the left-hand side is minimal when these variables are equal. So, let us take them all to be zero. The result is

$$n\sum_{i=1}^{k}x_i^2-\left(\sum_{i=1}^{k}x_i\right)^2 \ge T(n,k)\left[k\sum_{i=1}^{k}x_i^2-\left(\sum_{i=1}^{k}x_i\right)^2\right],$$

which is equivalent to

$$(T(n,k)-1)\left(\sum_{i=1}^{k}x_i\right)^2 \ge (kT(n,k)-n)\sum_{i=1}^{k}x_i^2 \qquad (1)$$

Now, if $kT(n,k)-n>0$, we can take a k-tuple $(x_1,x_2,\ldots,x_k)$ such that $\sum_{i=1}^{k} x_i = 0$ and $\sum_{i=1}^{k} x_i^2 \neq 0$ and we contradict the inequality (1). Hence we must have $kT(n,k)-n\leq 0$ that is $T(n,k)\leq \frac{n}{k}$. Now, let us proceed with the converse, that is showing that

$$n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2 \geq \frac{n}{k}\left[k\sum_{i=1}^{k} x_i^2 - \left(\sum_{i=1}^{k} x_i\right)^2\right] \tag{2}$$

for any real numbers $x_1,x_2,\ldots,x_n$. If we manage to prove this inequality, then it will follow that $T(n,k)=\frac{n}{k}$. But (2) is of course equivalent to

$$n\sum_{i=k+1}^{n} x_i^2 \geq \left(\sum_{i=1}^{n} x_i\right)^2 - \frac{n}{k}\left(\sum_{i=1}^{k} x_i\right)^2.$$

Now, we have to apply the Cauchy-Schwarz inequality, because we need $\sum_{i=k+1}^{n} x_i$. We find that

$$n\sum_{i=k+1}^{n} x_i^2 \geq \frac{n}{n-k}\left(\sum_{i=k+1}^{n} x_i\right)^2$$

and so it suffices to prove that

$$\frac{n}{n-k}A^2 \geq (A+B)^2 - \frac{n}{k}B^2, \tag{3}$$

where we have taken $A=\sum_{i=k+1}^{n} x_i$ and $B=\sum_{i=1}^{k} x_i$. But (3) is straightforward, since it is equivalent to

$$(kA-(n-k)B)^2 + k(n-k)B^2 \geq 0,$$

which is clear. Finally, the conclusion is settled: $T(n,k)=\frac{n}{k}$ is the best constant.

We continue the series of difficult inequalities with a very nice problem of Murray Klamkin. This time, one part of the problem is obvious

from the Cauchy-Schwarz inequality, but the second one is not immediate. Let us see.

Example 7. Let a, b, c be positive real numbers. Find the extreme values of the expression

$$\sqrt{a^2x^2+b^2y^2+c^2z^2}+\sqrt{b^2x^2+c^2y^2+a^2z^2}+\sqrt{c^2x^2+a^2y^2+b^2z^2}$$

where x, y, z are real numbers such that $x^2+y^2+z^2=1$.

Murray Klamkin, Crux Mathematicorum

Solution. Finding the upper bound does not seem to be too difficult, since from the Cauchy-Schwarz inequality it follows that

$$\sqrt{a^2x^2+b^2y^2+c^2z^2}+\sqrt{b^2x^2+c^2y^2+a^2z^2}+\sqrt{c^2x^2+a^2y^2+b^2z^2}\leq$$

$$\leq\sqrt{3(a^2x^2+b^2y^2+c^2z^2+c^2y^2+a^2z^2+c^2x^2+a^2y^2+b^2z^2)}$$

$$=\sqrt{3(a^2+b^2+c^2)}.$$

We have used here the hypothesis $x^2+y^2+z^2=1$. Thus, $\sqrt{3(a^2+b^2+c^2)}$ is the upper bound and this value if attained for $x=y=z=\dfrac{\sqrt{3}}{3}$.

But for the lower bound things are not so easy. Investigating what happens when $xyz=0$, we conclude that the minimal value should be $a+b+c$, attained when two variables are zero and the third one is 1 or -1. Hence, we should try to prove the inequality

$$\sqrt{a^2x^2+b^2y^2+c^2z^2}+\sqrt{b^2x^2+c^2y^2+a^2z^2}$$

$$+\sqrt{c^2x^2+a^2y^2+b^2z^2}\geq a+b+c.$$

Why not squaring it? After all, we observe that

$$a^2x^2+b^2y^2+c^2z^2+b^2x^2+c^2y^2+a^2z^2+c^2x^2+a^2y^2+b^2z^2=a^2+b^2+c^2,$$

so the new inequality cannot have a very complicated form. It becomes

$$\sqrt{a^2x^2+b^2y^2+c^2z^2}\cdot\sqrt{b^2x^2+c^2y^2+a^2z^2}$$

$$+\sqrt{b^2x^2+c^2y^2+a^2z^2}\cdot\sqrt{c^2x^2+a^2y^2+b^2z^2}$$

$$+\sqrt{c^2x^2+a^2y^2+b^2z^2}\cdot\sqrt{a^2x^2+b^2y^2+c^2z^2}\geq ab+bc+ca$$

which has great chances to be true. And indeed, it is true and it follows from what else?, the Cauchy-Schwarz inequality:

$$\sqrt{a^2x^2+b^2y^2+c^2z^2}\cdot\sqrt{b^2x^2+c^2y^2+a^2z^2}\geq abx^2+bxy^2+caz^2$$

and the other two similar inequalities. This shows that the minimal value is indeed $a+b+c$, attained for example when $(x,y,z)=(1,0,0)$.

It is now time for the champion inequalities. We will discuss two hard inequalities and after that we will leave for the reader the pleasure of solving many other problems based on these techniques.

Example 8. Prove that for any nonnegative numbers $a_1,a_2,\ldots,a_n$ such that $\sum_{i=1}^{n}a_i=\frac{1}{2}$, the following inequality holds

$$\sum_{1\leq i<j\leq n}\frac{a_ia_j}{(1-a_i)(1-a_j)}\leq\frac{n(n-1)}{2(2n-1)^2}.$$

Vasile Cartoaje

Solution. This is a very hard problem, in which intuition is better than technique. We will concoct a solution using a combination between the Cauchy-Schwarz inequality and Jensen's inequality, but we warn the reader that such a solution cannot be invented easily. Fasten your seat belts! Let us write the inequality in the form

$$\left(\sum_{i=1}^{n}\frac{a_i}{1-a_i}\right)^2\leq\sum_{i=1}^{n}\frac{a_i^2}{(1-a_i)^2}+\frac{n(n-1)}{(2n-1)^2}.$$

We apply now the Cauchy-Schwarz inequality to find that

$$\left(\sum_{i=1}^{n}\frac{a_i}{1-a_i}\right)^2\leq\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{i=1}^{n}\frac{a_i}{(1-a_i)^2}\right)=\sum_{i=1}^{n}\frac{\frac{a_i}{2}}{(1-a_i)^2}.$$

Thus, it remains to prove the inequality

$$\sum_{i=1}^{n} \frac{\frac{a_i}{2}}{(1-a_i)^2} \leq \sum_{i=1}^{n} \frac{a_i^2}{(1-a_i)^2} + \frac{n(n-1)}{(2n-1)^2}.$$

The latter can be written of course in the following form:

$$\sum_{i=1}^{n} \frac{a_i(1-2a_i)}{(1-a_i)^2} \leq \frac{2n(n-1)}{(2n-1)^2}.$$

This encourages us to study the function

$$f : \left[0, \frac{1}{2}\right] \to \mathbb{R}, \quad f(x) = \frac{x(1-2x)}{(1-x)^2}$$

and to see if it is concave. This is not difficult, for a short computation shows that $f''(x) = \dfrac{-6x}{(1-x)^4} \leq 0$. Hence we can apply Jensen's inequality to complete the solution.

We end this discussion with a remarkable solution, found by the member of the Romanian Mathematical Olympiad Committee, Claudiu Raicu, to the difficult problem given in 2004 in one of the Romanian Team Selection Tests.

Example 9. Let $a_1, a_2, \ldots, a_n$ be real numbers and let S be a nonempty subset of $\{1, 2, \ldots, n\}$. Prove that

$$\left(\sum_{i \in S} a_i\right)^2 \leq \sum_{1 \leq i \leq j \leq n} (a_i + \cdots + a_j)^2.$$

Gabriel Dospinescu, TST 2004, Romania

Solution. Let us define $s_i = a_1 + a_2 + \cdots + a_i$ for $i \geq 1$ and $s_0 = 0$. Now, partition S into groups of consecutive numbers. Then $\sum_{i \in S} a_i$ is of the form $s_{j_1} - s_{i_1} + s_{j_2} - s_{i_2} + \cdots + s_{j_k} - s_{i_k}$, with $0 \leq i_1 < i_2 < \cdots < i_k \leq n$, $j_1 < j_2 < \cdots < j_k$ and also $i_1 < j_1, \ldots, i_k < j_k$. Now, let us observe that

the left-hand side is nothing else than

$$\sum_{i=1}^{n} s_i^2 + \sum_{1\le i<j\le n} (s_j - s_i)^2 = \sum_{1\le i<j\le n+1} (s_j - s_i)^2.$$

Hence we need to show that

$$(s_{j_1} - s_{i_1} + s_{j_2} - s_{i_2} + \cdots + s_{j_k} - s_{i_k})^2 \le \sum_{0\le i<j\le n+1} (s_j - s_i)^2.$$

Let us take $a_1 = s_{i_1}, a_2 = s_{j_1}, \ldots, a_{2k-1} = s_{i_k}, a_{2k} = s_{j_k}$ and observe the obvious (but important) inequality

$$\sum_{0\le i<j\le n+1} (s_j - s_i)^2 \ge \sum_{1\le i<j\le 2k} (a_i - a_j)^2.$$

And this is how we arrived at the inequality

$$(a_1 - a_2 + a_3 - \cdots + a_{2k-1} - a_{2k})^2 \le \sum_{1\le i<j\le 2k} (a_i - a_j)^2 \qquad (1)$$

The latter inequality can be proved by using the Cauchy-Schwarz inequality k-times:

$$\begin{cases} (a_1 - a_2 + a_3 - \cdots + a_{2k-1} - a_{2k})^2 \\ \qquad \le k((a_1 - a_2)^2 + (a_3 - a_4)^2 + \cdots + (a_{2k-1} - a_{2k})^2) \\ (a_1 - a_2 + a_3 - \cdots + a_{2k-1} - a_{2k})^2 \\ \qquad \le k((a_1 - a_4)^2 + (a_3 - a_6)^2 + \cdots + (a_{2k-1} - a_2)^2) \\ \cdots \\ (a_1 - a_2 + a_3 - \cdots + a_{2k-1} - a_{2k})^2 \\ \qquad \le k((a_1 - a_{2k})^2 + (a_3 - a_2)^2 + \cdots + (a_{2k-1} - a_{2k-2})^2) \end{cases}$$

and by summing up all these inequalities. In the right-hand side we obtain an even smaller quantity than $\sum_{1\le i<j\le 2k} (a_i - a_j)^2$, which proves that (1) is correct. The solution ends here.

Problems for training

1. Let a, b, c be nonnegative real numbers. Prove that

$$(ax^2 + bx + c)(cx^2 + bx + a) \geq (a + b + c)^2 x^2$$

for all nonnegative real numbers x.

Titu Andreescu, Gazeta Matematica

2. Let p be a polynomial with positive real coefficients. Prove that if $p\left(\frac{1}{x}\right) \geq \frac{1}{p(x)}$ is true for $x = 1$, then it is true for all $x > 0$.

Titu Andreescu, Revista Matematica Timisoara

3. Prove that for any real numbers $a, b, c \geq 1$ the following inequality holds:

$$\sqrt{a-1} + \sqrt{b-1} + \sqrt{c-1} \leq \sqrt{a(bc+1)}.$$

4. For any positive integer n find the number of ordered n-tuples of integers $(a_1, a_2, \ldots, a_n)$ such that

$$a_1 + a_2 + \cdots + a_n \geq n^2 \text{ and } a_1^2 + a_2^2 + \cdots + a_n^2 \leq n^3 + 1.$$

China, 2002

5. Prove that for any positive real numbers a, b, c,

$$\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a} + \frac{1}{2\sqrt[3]{abc}} \geq \frac{(a+b+c+\sqrt[3]{abc})^2}{(a+b)(b+c)(c+a)}.$$

Titu Andreescu, MOSP 1999

6. Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be real numbers such that

$$\sum_{1 \leq i < j \leq n} a_i a_j > 0.$$

Prove the inequality

$$\left(\sum_{1 \leq i \neq j \leq n} a_i b_j\right)^2 \geq \left(\sum_{1 \leq i \neq j \leq n} a_i a_j\right)\left(\sum_{1 \leq i \neq j \leq n} b_i b_j\right)$$

Alexandru Lupas, AMM

7. Let $n \geq 2$ be an even integer. We consider all polynomials of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1$, with real coefficients and having at least one real zero. Determine the least possible value of $a_1^2 + a_2^2 + \cdots + a_{n-1}^2$.

Czech-Polish-Slovak Competition, 2002

8. The triangle ABC satisfies the relation

$$\left(\cot\frac{A}{2}\right)^2 + \left(2\cot\frac{B}{2}\right)^2 + \left(3\cot\frac{C}{2}\right)^2 = \left(\frac{6s}{7r}\right)^2.$$

Show that ABC is similar to a triangle whose sides are integers and find the smallest set of such integers.

Titu Andreescu, USAMO 2002

9. Let $x_1, x_2, \ldots, x_n$ be positive real numbers such that

$$\frac{1}{1+x_1} + \frac{1}{1+x_2} + \cdots + \frac{1}{1+x_n} = 1.$$

Prove the inequality

$$\sqrt{x_1} + \sqrt{x_2} + \cdots + \sqrt{x_n} \geq (n-1)\left(\frac{1}{\sqrt{x_1}} + \frac{1}{\sqrt{x_2}} + \cdots + \frac{1}{\sqrt{x_n}}\right).$$

Vojtech Jarnik Competition, 2002

10. Given are real numbers $x_1, x_2, \ldots, x_{10} \in \left[0, \frac{\pi}{2}\right]$ such that

$$\sin^2 x_1 + \sin^2 x_2 + \cdots + \sin^2 x_{10} = 1.$$

Prove that

$$3(\sin x_1 + \sin x_2 + \cdots + \sin x_{10}) \leq \cos x_1 + \cos x_2 + \cdots + \cos x_{10}.$$

Saint Petersburg, 2001

11. Prove that for any real numbers a, b, c, x, y, z the following inequality holds

$$ax + by + cz + \sqrt{(a^2+b^2+c^2)(x^2+y^2+z^2)} \geq \frac{2}{3}(a+b+c)(x+y+z).$$

Vasile Cartoaje, Kvant

12. Prove that for any real numbers $x_1, x_2, \ldots, x_n$ the following inequality holds

$$\left(\sum_{i=1}^{n}\sum_{i=1}^{n}|x_i - x_j|\right)^2 \leq \frac{2(n^2-1)}{3}\left(\sum_{i=1}^{n}\sum_{j=1}^{n}|x_i - x_j|^2\right).$$

IMO 2003

13. Let $n > 2$ and $x_1, x_2, \ldots, x_n$ be positive real numbers such that

$$(x_1 + x_2 + \cdots + x_n)\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) = n^2 + 1.$$

Prove that

$$(x_1^2 + x_2^2 + \cdots + x_n^2)\left(\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2}\right) > n^2 + 4 + \frac{2}{n(n-1)}.$$

Gabriel Dospinescu

14. Prove that for any positive real numbers a, b, c, x, y, z such that

$$xy + yz + zx = 3,$$

$$\frac{a}{b+c}(y+z) + \frac{b}{c+a}(x+z) + \frac{c}{a+b}(x+y) \geq 3.$$

Titu Andreescu, Gabriel Dospinescu

15. Prove that for any positive real numbers $a_1, a_2, \ldots, a_n$, x_1, $x_2, \ldots, x_n$ such that

$$\sum_{i \leq i < j \leq n} x_i x_j = \binom{n}{2},$$

the following inequality holds

$$\frac{a_1}{a_2 + \cdots + a_n}(x_2 + \cdots + x_n) + \cdots + \frac{a_n}{a_1 + \cdots + a_{n-1}}(x_1 + \cdots + x_{n-1}) \geq n.$$

Vasile Cartoaje, Gabriel Dospinescu

EQUATIONS AND BEYOND

Real equations with multiple unknowns have in general infinitely many solutions if they are solvable. In this case, an important task characterizing the set of solutions by using parameters. We are going to discuss two real equations and two parameterizations, but we will go beyond, showing how a simple idea can generate lots of nice problems, some of them really difficult.

We begin this discussion with a problem. It may seem unusual, but this problem is in fact the introduction that leads to the other themes in this discussion.

Example 1. Consider three real numbers a, b, c such that $abc = 1$ and write

$$x = a + \frac{1}{a}, \quad y = b + \frac{1}{b}, \quad z = c + \frac{1}{c} \tag{1}$$

Find an algebraic relation between x, y, z, independent of a, b, c.

Of course, without any ideas, one would solve the equations from (1) with respect to a, b, c and then substitute the results in the relation $abc = 1$. But this is a mathematical crime! Here is a nice idea. To generate a relation involving x, y, z, we compute the product

$$\begin{aligned} xyz &= \left(a + \frac{1}{a}\right)\left(b + \frac{1}{b}\right)\left(c + \frac{1}{c}\right) \\ &= \left(a^2 + \frac{1}{a^2}\right) + \left(b^2 + \frac{1}{b^2}\right) + \left(c^2 + \frac{1}{c^2}\right) + 2 \\ &= (x^2 - 2) + (y^2 - 2) + (z^2 - 2) + 2. \end{aligned}$$

Thus,

$$x^2 + y^2 + z^2 - xyz = 4 \tag{2}$$

and this is the answer to the problem.

Now, another question appears: is the converse true? Obviously not (take for example the numbers $(x, y, z) = (1, 1, -1)$). But looking again

at (1), we see that we must have $\min\{|x|, |y|, |z|\} \geq 2$. We will prove the following result.

Example 2. Let x, y, z be real numbers with $\max\{|x|, |y|, |z|\} > 2$. Prove that there exist real numbers a, b, c with $abc = 1$ satisfying (1).

Whenever we have a condition of the form $\max\{|x|, |y|, |z|\} > 2$, it is better to make a choice. Here, let us take $|x| > 2$. This shows that there exists a nonzero real number u such that $x = u + \dfrac{1}{u}$, (we have used here the condition $|x| > 2$). Now, let us regard (2) as a second degree equation with respect to z. Since this equation has real roots, the discriminant must be nonnegative, which means that $(x^2 - 4)(y^2 - 4) \geq 0$. But since $|x| > 2$, we find that $y^2 \geq 4$ and so there exist a non-zero real number v for which $y = v + \dfrac{1}{v}$. How do we find the corresponding z? Simply by solving the second degree equation. We find two solutions:

$$z_1 = uv + \frac{1}{uv}, \quad z_2 = \frac{u}{v} + \frac{v}{u}$$

and now we are almost done. If $z = uv + \dfrac{1}{uv}$ we take $(a, b, c) = \left(u, v, \dfrac{1}{uv}\right)$ and if $z = \dfrac{u}{v} + \dfrac{v}{u}$, then we take $(a, b, c) = \left(\dfrac{1}{u}, v, \dfrac{u}{v}\right)$. All the conditions are satisfied and the problem is solved.

A direct consequence of the previous problem is the following:

If $x, y, z > 0$ are real numbers that verify (2), then there exist $\alpha, \beta, \chi \in \mathbb{R}$ such that

$$x = 2\mathrm{ch}(\alpha), \quad y = 2\mathrm{ch}(\beta), \quad z = 2\mathrm{ch}(\chi),$$

where $\mathrm{ch} : \mathbb{R} \to (0, \infty)$, $\mathrm{ch}(x) = \dfrac{e^x + e^{-x}}{2}$. Indeed, we write (1), in which this time it is clear that $a, b, c > 0$ and we take $\alpha = \ln a$, $\beta = \ln b$, $\chi = \ln c$.

Inspired by the previous equation, let us consider another one

$$x^2 + y^2 + z^2 + xyz = 4, \tag{3}$$

where $x, y, z > 0$. We will prove that the set of solutions of this equation is the set of triples $(2\cos A, 2\cos B, 2\cos C)$ where A, B, C are the angles of an acute triangle. First, let us prove that all these triples are solutions. This reduces to the identity

$$\cos^2 A + \cos^2 B + \cos^2 C + 2\cos A \cos B \cos C = 1.$$

This identity can be proved readily by using the sum-to-product formulas, but here is a nice proof employing geometry and linear algebra. We know that in any triangle we have the relations

$$\begin{cases} a = c\cos B + b\cos C \\ b = a\cos C + c\cos A \\ c = b\cos A + a\cos B \end{cases}$$

which are simple consequences of the Law of Cosines. Now, let us consider the system

$$\begin{cases} x - y\cos C - z\cos B = 0 \\ -x\cos C + y - z\cos A = 0 \\ -x\cos B + y\cos A - z = 0 \end{cases}$$

From the above observation, it follows that this system has a non-trivial solution, that is (a, b, c) and so we must have

$$\begin{vmatrix} 1 & -\cos C & -\cos B \\ -\cos C & 1 & -\cos A \\ -\cos B & -\cos A & 1 \end{vmatrix} = 0,$$

which expanded gives

$$\cos^2 A + \cos^2 B + \cos^2 C + 2\cos A \cos B \cos C = 1.$$

For the converse, we see first that $0 < x, y, z < 2$, hence there are numbers $A, B \in \left(0, \frac{\pi}{2}\right)$ such that $x = 2\cos A$, $y = 2\cos B$. Solving the equation with respect to z and taking into account that $z \in (0, 2)$ we

obtain $z = -2\cos(A+B)$. Thus we can take $C = \pi - A - B$ and we will have $(x, y, z) = (2\cos A, 2\cos B, 2\cos C)$. All in all we have solved the following problem.

Example 3. The positive real numbers x, y, z satisfy (3) if and only if there exists an acute-angled triangle ABC such that

$$x = 2\cos A, \quad y = 2\cos B, \quad z = 2\cos C.$$

With the introduction and the easy problems over it is now time to see some nice applications of the above results.

Example 4. Let $x, y, z > 2$ satisfying (2). We define the sequences $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$, $(c_n)_{n\geq 1}$ by

$$a_{n+1} = \frac{a_n^2 + x^2 - 4}{a_{n-1}}, \quad b_{n+1} = \frac{b_n^2 + y^2 - 4}{b_{n-1}}, \quad c_{n+1} = \frac{c_n^2 + z^2 - 4}{c_{n-1}},$$

with $a_1 = x$, $b_1 = y$, $c_1 = z$ and $a_2 = x^2 - 2$, $b_2 = y^2 - 2$, $c_2 = z^2 - 2$. Prove that for all $n \geq 1$ the triple (a_n, b_n, c_n) also satisfies (2).

Solution. Let us write $x = a + \frac{1}{a}$, $y = b + \frac{1}{b}$, $z = c + \frac{1}{c}$, with $abc = 1$. Then

$$a_2 = a^2 + \frac{1}{a^2}, \quad b_2 = b^2 + \frac{1}{b^2}, \quad c_2 = c^2 + \frac{1}{c^2}.$$

So, a reasonable conjecture is that

$$(a_n, b_n, c_n) = \left(a^n + \frac{1}{a^n}, b^n + \frac{1}{b^n}, c^n + \frac{1}{c^n}\right).$$

Indeed, this follows by induction from

$$\frac{\left(a^n + \frac{1}{a^n}\right)^2 + a^2 + \frac{1}{a^2} - 2}{a^{n-1} + \frac{1}{a^{n-1}}} = a^{n+1} + \frac{1}{a^{n+1}}$$

and two similar identities. We have established that

$$(a_n, b_n, c_n) = \left(a^n + \frac{1}{a^n}, b^n + \frac{1}{b^n}, c^n + \frac{1}{c^n}\right)$$

But if $abc = 1$, then certainly $a^n b^n c^n = 1$, which shows that indeed the triple (a_n, b_n, c_n) satisfies (2).

The following problem is a nice characterization of the equation (2) by polynomials and also teaches us some things about polynomials in two or three variables.

Example 5. Find all polynomials $f(x, y, z)$ with real coefficients such that

$$f\left(a + \frac{1}{a}, b + \frac{1}{b}, c + \frac{1}{c}\right) = 0$$

whenever $abc = 1$.

Gabriel Dospinescu

Solution. From the introduction, it is now clear that the polynomials divisible by $x^2 + y^2 + z^2 - xyz - 4$ are solutions to the problem. But it is not obvious why any desired polynomial should be of this form. To show this, we use the classical polynomial long division. There are polynomials $g(x, y, z)$, $h(y, z)$, $k(y, z)$ with real coefficients such that

$$f(x, y, z) = (x^2 + y^2 + z^2 - xyz - 4)g(x, y, z) + xh(y, z) + k(y, z)$$

Using the hypothesis, we deduce that

$$0 = \left(a + \frac{1}{a}\right) h\left(b + \frac{1}{b}, c + \frac{1}{c}\right) + k\left(b + \frac{1}{b}, c + \frac{1}{c}\right)$$

whenever $abc = 1$. Well, it seems that this is a dead end. Not exactly. Now we take two numbers x, y such that $\min\{|x|, |y|\} > 2$ and we write $x = b + \frac{1}{b}$, $y = c + \frac{1}{c}$ with $b = \frac{x + \sqrt{x^2 - 4}}{2}$, $c = \frac{y + \sqrt{y^2 - 4}}{2}$.

Then it is easy to compute $a + \frac{1}{a}$. It is exactly $xy + \sqrt{(x^2 - 4)(y^2 - 4)}$. So, we have found that

$$(xy + \sqrt{(x^2 - 4)(y^2 - 4)})h(x, y) + k(x, y) = 0$$

whenever $\min\{|x|, |y|\} > 2$. And now? The last relation suggests that we should prove that for each y with $|y| > 2$, the function $x \to \sqrt{x^2 - 4}$ is

not rational, that is, there aren't polynomials p, q such that $\sqrt{x^2-4} = \frac{p(x)}{q(x)}$. But this is easy because if such polynomials existed, than each zero of x^2-4 should have even multiplicity, which is not the case. Consequently, for each y with $|y| > 2$ we have $h(x,y) = k(x,y) = 0$ for all x. But this means that $h(x,y) = k(x,y) = 0$ for all x, y, that is our polynomial is divisible with $x^2+y^2+z^2-xyz-4$.

O a different kind, the following problem and the featured solution prove that sometimes an efficient substitution can help more than ten complicated ideas.

Example 6. Let $a, b, c > 0$. Find all triples (x, y, z) of positive real numbers such that

$$\begin{cases} x+y+z = a+b+c \\ a^2x+b^2y+c^2z+abc = 4xyz \end{cases}$$

Titu Andreescu, IMO Shortlist, 1995

Solution. We try to use the information given by the second equation. This equation can be written as

$$\frac{a^2}{yz}+\frac{b^2}{zx}+\frac{c^2}{xy}+\frac{abc}{xyz} = 4$$

and we already recognize the relation

$$u^2+v^2+w^2+uvw = 4$$

where $u = \frac{a}{\sqrt{yz}}$, $v = \frac{b}{\sqrt{zx}}$, $w = \frac{c}{\sqrt{xy}}$. According to example 3, we can find an acute-angled triangle ABC such that

$$u = 2\cos A, \quad v = 2\cos B, \quad w = 2\cos C.$$

We have made use of the second condition, so we use the first one to deduce that

$$x+y+z = 2\sqrt{xy}\cos C + 2\sqrt{yz}\cos A + 2\sqrt{zx}\cos B.$$

Trying to solve this as a second degree equation in $\sqrt{x}$, we find the discriminant

$$-4(\sqrt{y}\sin C - \sqrt{z}\sin B)^2.$$

Because this discriminant is nonnegative, we infer that

$$\sqrt{y}\sin C = \sqrt{z}\sin B \text{ and } \sqrt{x} = \sqrt{y}\cos C + \sqrt{z}\cos B.$$

Combining the last two relations, we find that

$$\frac{\sqrt{x}}{\sin A} = \frac{\sqrt{y}}{\sin B} = \frac{\sqrt{z}}{\sin C}$$

Now we square these relations and we use the fact that

$$\cos A = \frac{a}{2\sqrt{yz}}, \quad \cos B = \frac{b}{2\sqrt{zx}}, \quad \cos C = \frac{c}{2\sqrt{xy}}.$$

The conclusion is:

$$x = \frac{b+c}{2}, \quad y = \frac{c+a}{2}, \quad z = \frac{a+b}{2}$$

and it is immediate to see that this triple satisfies both conditions. Hence there is a unique triple that is solution to the given system. Notice that the condition

$$x + y + z = 2\sqrt{xy}\cos C + 2\sqrt{yz}\cos A + 2\sqrt{zx}\cos B$$

is the equality case in the lemma stated in the solution of the following problem. This could be another possible solution of the problem.

We have discussed the following very difficult problem in the chapter "An useful substitution". We will see that example 3 helps us find a nice geometric solution to this inequality.

Example 7. Prove that if the positive real numbers x, y, z satisfy $xy + yz + zx + xyz = 4$, then

$$x + y + z \geq xy + yz + zx.$$

India, 1998

Solution. It is not difficult to observe that at first glance, the condition $xy+yz+zx+xyz=4$ it's not the same as the equation (3). Let us write the condition $xy+yz+zx+xyz=4$ in the form

$$\sqrt{xy}^2+\sqrt{yz}^2+\sqrt{zx}^2+\sqrt{xy}\cdot\sqrt{yz}\cdot\sqrt{zx}=4.$$

Now, we can use the result from example 3 and we deduce the existence of an acute-angled triangle ABC such that

$$\begin{cases}\sqrt{yz}=2\cos A\\ \sqrt{zx}=2\cos B\\ \sqrt{xy}=2\cos C\end{cases}$$

We solve the system and we find the triplet

$$(x,y,z)=\left(\frac{2\cos B\cos C}{\cos A},\frac{2\cos A\cos C}{\cos B},\frac{2\cos A\cos B}{\cos C}\right)$$

Hence we need to prove that

$$\frac{2\cos B\cos C}{\cos A}+\frac{2\cos A\cos C}{\cos B}+\frac{2\cos A\cos B}{\cos C}\geq 2(\cos^2 A+\cos^2 B+\cos^2 C).$$

This one is a hard inequality and it follows from a more general result.

Lemma. *If ABC is a triangle and x,y,z are arbitrary real numbers, then*

$$x^2+y^2+z^2\geq 2yz\cos A+2zx\cos B+2xy\cos C.$$

Proof of the lemma. Let us consider points P,Q,R on the lines AB, BC, CA, respectively, such that $AP=BQ=CR=1$ and P,Q,R and do not lie on the sides of the triangle. Then we see that the inequality is equivalent to

$$(x\cdot\overrightarrow{AP}+y\cdot\overrightarrow{BQ}+z\cdot\overrightarrow{CR})^2\geq 0,$$

which is obviously true.

The lemma being proved, we just have to take

$$x = \sqrt{\frac{2\cos B \cos C}{\cos A}} \quad y = \sqrt{\frac{2\cos A \cos C}{\cos B}}, \quad z = \sqrt{\frac{2\cos A \cos B}{\cos C}}$$

in the above lemma and the problem will be solved.

But of course, this type of identities does not appear only in inequalities. We are going to discuss two problems in which the identity is very well masked.

Example 8. Find all continuous functions $f : (0, \infty) \to (0, \infty)$ satisfying

$$f(x)f(y) = f(xy) + f\left(\frac{x}{y}\right).$$

Sankt Petersburg

Solution. First of all, observe that by symmetry in x, y we must have $f\left(\frac{x}{y}\right) = f\left(\frac{y}{x}\right)$ and so $f(x) = f\left(\frac{1}{x}\right)$. Next, by taking $x = y = 1$ we obtain $f(1) = 2$ and then $f(x^2) = f^2(x) - 2$. These relations should now ring a bell! It seems that we are searching for something like $f(x) = x^k + \frac{1}{x^k}$. We are right, but still far from the solution. Let's make another small step: proving that $f(x) \geq 2$ for all x. Indeed, this is going to be easy, since $f(x^2) = f^2(x) - 2$ implies that $f(x) > \sqrt{2}$ for all x. Thus, $f^2(x) = f(x^2) + 2 > 2 + \sqrt{2}$. Repeating this argument, we find that for all x we have

$$f(x) > \sqrt{2 + \sqrt{2 + \sqrt{2 + \ldots}}} = 2$$

(the last equality being immediate for a beginner in analysis).

Yet, till now nothing related to our theme. Wrong! Let's observe that

$$f(x^2) + f(y^2) = f(xy)f\left(\frac{x}{y}\right)$$

for all x, y. Indeed, it suffices to write

$$x^2 = xy\frac{x}{y}, \quad y^2 = \frac{xy}{\frac{x}{y}}.$$

With this information, let us make one more step and write

$$f^2(x) + f^2(y) - 4 = f(x^2) + f(y^2) = f(xy)(f(x)f(y) - f(xy)).$$

We are now on the right track, since we find that

$$f^2(x) + f^2(y) + f^2(xy) = f(x)f(y)f(xy) + 4.$$

Using also the fact that $f(x) \geq 2$, we deduce the existence of a continuous function $g : (0, \infty) \to [1, \infty)$ such that $f(x) = g(x) + \dfrac{1}{g(x)}$. The above relation implies of course that $g(xy) = g(x)g(y)$. By considering $h(x) = \ln g(e^x)$, we obtain that h is a continuous solution of Cauchy's functional equation $f(x+y) = f(x) + f(y)$, thus $h(x) = kx$ for a certain k. This shows that $g(x) = x^k$ and that our thoughts were right; these are all solutions of the equation (the verification of the identity is immediate for this class of functions).

And finally, an apparently inextricable recursive relation.

Example 9. Let $(a_n)_{n\geq 0}$ be a non-decreasing sequence of positive integers such that

$$a_0 = a_1 = 47 \text{ and } a_{n-1}^2 + a_n^2 + a_{n+1}^2 - a_{n-1}a_n a_{n+1} = 4 \text{ for all } n \geq 1.$$

Prove that $2 + a_n$ and $2 + \sqrt{2 + a_n}$ are perfect squares for all $n \geq 0$.

Titu Andreescu

Solution. Using the idea from the chapter with real equations, we write $a_n = x_n + \dfrac{1}{x_n}$, with $x_n > 1$. The the given condition becomes $x_{n+1} = x_n x_{n-1}$ (we have used here explicitly that $x_n > 1$), which shows that $(\ln x_n)_{n\geq 0}$ is a Fibonacci-type sequence. Since $x_0 = x_1$, we deduce that $x_n = x_0^{F_n}$, where $F_0 = F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$. Now, we have to do more: who is x_0? And the answer $x_0 = \dfrac{47 + \sqrt{47^2 - 1}}{2}$ won't suffices. Let us remark that

$$\left(\sqrt{x_0} + \frac{1}{\sqrt{x_0}}\right)^2 = 49$$

from where we find that

$$\sqrt{x_0} + \frac{1}{\sqrt{x_0}} = 7.$$

Similarly, we obtain that

$$\sqrt[4]{x_0} + \frac{1}{\sqrt[4]{x_0}} = 3.$$

Solving the equation, we obtain

$$\sqrt[4]{x_0} = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \lambda^2$$

that is $x_0 = \lambda^8$. And so we have found the general formula $a_n = \lambda^{8F_n} + \lambda^{-8F_n}$. And now the problem becomes easy, since

$$a_n + 2 = (\lambda^{4F_n} + \lambda^{-4F_n})^2 \text{ and } 2 + \sqrt{2 + a_n} = (\lambda^{2F_n} + \lambda^{-2F_n})^2.$$

All we are left to prove is that $\lambda^{2k} + \frac{1}{\lambda^{2k}} \in \mathbb{R}$ for all $k \in \mathbb{R}$. But this isn't difficult, since

$$\lambda^2 + \frac{1}{\lambda^2} \in \mathbb{R}, \quad \lambda^4 + \frac{1}{\lambda^4} \in \mathbb{R}$$

and

$$\lambda^{2(k+1)} + \frac{1}{\lambda^{2(k+1)}} = \left(\lambda^2 + \frac{1}{\lambda^2}\right)\left(\lambda^{2k} + \frac{1}{\lambda^{2k}}\right) - \left(\lambda^{2(k-1)} + \frac{1}{\lambda^{2(k-1)}}\right).$$

Problems for training

1. Find all triples x, y, z of positive real numbers, solutions to the system:

$$\begin{cases} x^2 + y^2 + z^2 = xyz + 4 \\ xy + yz + zx = 2(x + y + z) \end{cases}$$

2. Let $x, y, z > 0$ such that $x^2 + y^2 + z^2 + xyz = 4$. Prove that

$$\sqrt{\frac{(2-a)(2-b)}{(2+a)(2+b)}} + \sqrt{\frac{(2-b)(2-c)}{(2+b)(2+c)}} + \sqrt{\frac{(2-c)(2-a)}{(2+c)(2+a)}} = 1.$$

Cristinel Mortici, Romanian Inter-county Contest

3. Prove that if $a, b, c \geq 0$ satisfy the condition $|a^2+b^2+c^2-4| = abc$, then

$$(a-2)(b-2) + (b-2)(c-2) + (c-2)(a-2) \geq 0.$$

Titu Andreescu, Gazeta Matematica

4. Find all triples (a, b, c) of positive real numbers, solutions to the system

$$\begin{cases} a^2 + b^2 + c^2 + abc = 4 \\ a + b + c = 3 \end{cases}$$

Cristinel Mortici, Romanian Inter-county Contest

5. Prove that in any triangle the following inequality holds

$$\left(\sin\frac{A}{2} + \sin\frac{B}{2} + \sin\frac{C}{2}\right)^2 \leq \cos^2\frac{A}{2} + \cos^2\frac{B}{2} + \cos^2\frac{C}{2}.$$

6. Let $x, y, z > 0$ such that $xy + yz + zx + xyz = 4$. Prove that

$$3\left(\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} + \frac{1}{\sqrt{z}}\right)^2 \geq (x+2)(y+2)(z+2).$$

Gabriel Dospinescu

7. Prove that in any acute-angled triangle the following inequality holds

$$\left(\frac{\cos A}{\cos B}\right)^2 + \left(\frac{\cos B}{\cos C}\right)^2 + \left(\frac{\cos C}{\cos A}\right)^2 + 8\cos A\cos B\cos C \geq 4.$$

Titu Andreescu, MOSP 2000

8. Solve in positive integers the equation

$$(x+2)(y+2)(z+2) = (x+y+z+2)^2.$$

Titu Andreescu

9. Let $n > 4$ be a given positive integer. Find all pairs of positive integers (x, y) such that

$$xy - \frac{(x+y)^2}{n} = n - 4.$$

Titu Andreescu

10. Let the sequence $(a_n)_{n\geq 0}$, where $a_0 = a_1 = 97$ and $a_{n+1} = a_{n-1}a_n + \sqrt{(a_n^2-1)(a_{n-1}^2-1)}$ for all $n \geq 1$. Prove that $2+\sqrt{2+2a_n}$ is a perfect square for all $n \geq 0$.

Titu Andreescu

11. Find all triplets of positive integers (k, l, m) with sum 2002 and for which the system

$$\begin{cases} \dfrac{x}{y} + \dfrac{y}{x} = k \\ \\ \dfrac{y}{z} + \dfrac{z}{y} = l \\ \\ \dfrac{z}{x} + \dfrac{x}{y} = m \end{cases}$$

has real solutions.

Titu Andreescu, proposed for IMO 2002

12. Find all functions $f : (0,\infty) \to (0,\infty)$ with the following properties:

a) $f(x)+f(y)+f(z)+f(xyz) = f(\sqrt{xy})f(\sqrt{yz})f(\sqrt{zx})$ for all x, y, z;

b) if $1 \leq x < y$ then $f(x) < f(y)$.

Hojoo Lee, IMO Shortlist 2004

13. Prove that if $a, b, c \geq 2$ satisfy the condition $a^2+b^2+c^2 = abc+4$, then

$$a+b+c+ac+bc \geq 2\sqrt{(a+b+c+3)(a^2+b^2+c^2-3)}.$$

Marian Tetiva

14. Prove that if $a, b, c \geq 0$ satisfy $a^2+b^2+c^2+abc = 4$ then

$$0 \leq ab+bc+ca-abc \leq 2.$$

Titu Andreescu, USAMO 2001

LOOK AT THE EXPONENT!

Most of the times, proving divisibility reduces to congruences and the famous theorems from this field, such as Fermat, Euler, or Wilson. But what do we do when we have to prove for example that $lcm(a,b,c)^2 | lcm(a,b) \cdot lcm(b,c) \cdot lcm(c,a)$ for any positive integers a, b, c? Then one thing is sure: the above methods fail. Yet, another smart idea appears: if we have to prove that $a|b$, then it is enough to prove that the exponent of any prime number in the decomposition of a is at least the exponent of that prime number in the decomposition of b. For simplicity, let us denote by $v_p(a)$ the exponent of the prime number p in the decomposition of a. Of course, if p doesn't divide a, then $v_p(a) = 0$. Also, it is easy to prove the following properties of $v_p(a)$:

1) $\min\{v_p(a), v_p(b)\} \leq v_p(a+b) \leq \max\{v_p(a), v_p(b)\}$

2) $v_p(ab) = v_p(a) + v_p(b)$

for any positive integer numbers a, b. Now, let us repeat the above idea in terms of $v_p(a)$: we have $a|b$ if and only if for any prime number p we have $v_p(a) \leq v_p(b)$ and we have $a = b$ if and only if for any prime number p, $v_p(a) = v_p(b)$.

Some other useful properties of $v_p(a)$ are:

3) $v_p(gcd(a_1, a_2, \ldots, a_n)) = \min\{v_p(a_1), v_p(a_2), \ldots, v_p(a_n)\}$,

4) $v_p(lcm(a_1, a_2, \ldots, a_n)) = \max\{v_p(a_1), v_p(a_2), \ldots, v_p(a_n)\}$ and

5) $v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \frac{n - s_p(n)}{p-1}$ whenever $p|n$. Here, $s_p(n)$ is the sum of digits of n when written in base b. Observe that 3) and 4) are simple consequences of the definitions. Less straightforward is 5). This follows from the fact that there are $\left[\frac{n}{p}\right]$ multiples of p, $\left[\frac{n}{p^2}\right]$ are multiples of p^2 and so on. The other equality is not difficult. Indeed, let us write $n = a_0 + a_1 p + \cdots + a_k p^k$, where $a_0, a_1, \ldots, a_k \in \{0, 1, \ldots, p-1\}$

and $a_k \neq 0$. Then

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots = a_1+a_2p+\cdots+a_kp^{k-1}+a_2+a_3p+\cdots+a_kp^{k-2}+\cdots+a_k$$

and now using the formula

$$1+p+\cdots+p^i = \frac{p^{i+1}-1}{p-1},$$

we find exactly 5). Enough with the introduction, let's see some concrete results. We have chosen with intention the first problem (the classical one) a very nasty one, so that the reader doesn't think that all the above formulas were for nothing and because it offers us the opportunity to prove a very nice inequality. There are hundreds of variants of it in all contests around the world and in all elementary magazines. Let us see.

Example 1. Prove that $\dfrac{(3a+3b)!(2a)!(3b)!(2b)!}{(2a+3b)!(a+2b)!(a+b)!a!(b!)^2} \in \mathbb{Z}$ for any positive integers a, b.

Richard Askey, AMM 6514

Solution. First, let us clearify something. When we write

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots,$$

we write in fact $\displaystyle\sum_{k\geq 1}\left[\frac{n}{p^k}\right]$ and this sum has clearly a finite number of non-zero terms. Now, let us take a prime p and let us apply formula 5), as well as the first observations. We find that

$$v_p((3a+3b)!(2a)!(3b)!(2b)!) = \sum_{k\geq 1}\left(\left[\frac{3a+3b}{p^k}\right]+\left[\frac{2a}{p^k}\right]+\left[\frac{3b}{p^k}\right]+\left[\frac{2b}{p^k}\right]\right)$$

and also

$$v_p = ((2a+3b)!(a+2b)!(a+b)!a!(b!)^2)$$

$$= \sum_{k\geq 1}\left(\left[\frac{2a+3b}{p^k}\right]+\left[\frac{a+2b}{p^k}\right]+\left[\frac{a+b}{p^k}\right]+\left[\frac{a}{p^k}\right]+2\left[\frac{b}{p^k}\right]\right)$$

Of course, it is enough to prove that for each $k \geq 1$ the term corresponding to k in the first sum is greater than or equal to the term corresponding to k in the second sum. With the substitution $x = \dfrac{a}{p^k}$, $y = \dfrac{b}{p^k}$, we have to prove that for any nonnegative real numbers x, y we have

$$[3x + 3y] + [2x] + [3y] + [2y] \geq [2x + 3y] + [x + 2y] + [x + y] + [x] + 2[y].$$

This isn't easy, but with another useful idea the inequality will become easy. The idea is that

$$[3x + 3y] = 3[x] + 3[y] + [3\{x\} + 3\{y\}]$$

and similar relations for the other terms of the inequality. After this operation, we see that it suffices to prove the inequality only for $0 \leq x, y < 1$. Why is the new inequality easy? Because we can easily compute all terms, after splitting in some cases, so that to see when $[2\{x\}]$, $[3\{y\}]$, $[2\{y\}]$ are 0, 1 or 2.

We won't continue studying these cases, since another beautiful problem is waiting.

Example 2. Let a, b be positive integers such that $a|b^2$, $b^3|a^4$, $a^5|b^6$, $b^7|a^8, \ldots$. Prove that $a = b$.

Solution. Let us take a prime p and try to prove that $v_p(a) = v_p(b)$. We see that the hypothesis $a|b^2$, $b^3|a^4$, $a^5|b^6$, $b^7|a^8, \ldots$ is the same as $a^{4n+1}|b^{4n+2}$ and $b^{4n+3}|a^{4n+4}$ for all natural number n. But the relation $a^{4n+1}|b^{4n+2}$ can be interpreted as $(4n + 1)v_p(a) \leq (4n + 2)v_p(b)$ for all n, that is

$$v_p(a) \leq \lim_{n\to\infty} \frac{4n + 2}{4n + 1} v_p(b) = v_p(b).$$

Similarly, the condition $b^{4n+3}|a^{4n+4}$ implies $v_p(a) \geq v_p(b)$ and so $v_p(a) = v_p(b)$. The conclusion follows: $a = b$.

We have mentioned in the beginning of the discussion a nice and easy problem, so probably it's time to solve it, although for sure the reader has already done this.

Example 3. Prove that $lcm(a,b,c)^2 | lcm(a,b) \cdot lcm(b,c) \cdot lcm(c,a)$ for any positive integers a, b, c.

Solution. Let p an arbitrary prime number. We have

$$v_p(lcm(a,b,c)^2) = 2\max\{x,y,z\}$$

and

$$v_p(lcm(a,b) \cdot lcm(b,c) \cdot lcm(c,a)) = \max\{x,y\} + \max\{y,z\} + \max\{z,x\},$$

where $x = v_p(a)$, $y = v_p(b)$, $z = v_p(c)$. So, we need to prove that

$$\max\{x,y\} + \max\{y,z\} + \max\{z,x\} \geq 2\max\{x,y,z\}$$

for any nonnegative integers x, y, z. But this is easy, since we may assume that $x \geq y \geq z$ (the symmetry allows us this supposition) and the inequality becomes $2x + y \geq 2x$, obviously true.

It is time for some difficult problems, which are all based on the observations from the beginning of the discussion.

Example 4. Prove that there exists a constant c such that for any positive integers a, b, n that verify $a! \cdot b! | n!$ we have $a + b < n + c \ln n$.

Paul Erdos

Solution. This time the other formula for $v_p(n!)$ is useful. Of course, there is no reasonable estimation of this constant, so we should better see what happens if $a! \cdot b! | n!$. Then $v_2(a!) + v_2(b!) \leq v_2(n!)$, which can be translated as $a - s_2(a) + b - s_2(b) \leq n - s_2(n) < n$. So, we have found almost exactly what we needed: $a + b < n + s_2(a) + s_2(b)$. Now, we need another observation: the sum of digits of a number A when written in binary is at most the number of digits of A in base 2, which is $1 + [\log_2 A]$ (this follows from the fact that $2^{k-1} \leq A < 2^k$, where

k is the number of digits of A in base 2). So, we have the estimations $a+b < n + s_2(a) + s_2(b) \leq n + 2 + \log_2 ab \leq n + 2 + 2\log_2 n$ (since we have of course $a, b \leq n$). And now the conclusion is immediate.

The following problem appeared in Kvant as a hard problem. It took quite a long time before an olympic found an extraordinary solution. We shall not present his solution; but another one, even easier.

Example 5. Is there an infinite set of positive integers such that no matter how we choose some elements of this set, their sum is not an integer power of exponent at least 2?

Kvant

Solution. Let us take $A = \{2^n \cdot 3^{n+1} | n \geq 1\}$ If we consider some different numbers from this set, their sum will be of the form $2^x \cdot 3^{x+1} \cdot y$, where $(y, 6) = 1$. This is surely not a power of exponent at least 2, since otherwise the exponent should divide both x and $x+1$. Thus this set is actually a good choice.

The following problem shows the beauty of elementary number-theory. It combines diverse ideas and techniques and the result is at least beautiful. This one is also a classic problem, that appeared in lots of mathematics competitions.

Example 6. Prove that for any natural number n, $n!$ is a divisor of

$$\prod_{k=0}^{n-1} (2^n - 2^k).$$

Solution. So, let us take a prime number p. Of course, for the argument to be non-trivial, we take $p \leq n$ (otherwise doesn't divide $n!$). First, let us see what happens with $p = 2$. We have

$$v_2(n!) = n - s_2(n) \leq n - 1$$

and also

$$v_2\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)=\sum_{k=0}^{n-1}v_2(2^n-2^k)\geq n-1$$

(since 2^n-2^k is even for $k\geq 1$), so we are done with this case. Now, let us assume that $p>2$. We have $p|2^{p-1}-1$ from Fermat's theorem, so we also have $p|2^{k(p-1)}-1$ for all $k\geq 1$. Now,

$$\prod_{k=0}^{n-1}(2^n-2^k)=2^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}(2^k-1)$$

and so, from the above remarks we infer that

$$v_2\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)=\sum_{k=1}^{n}v_2(2^k-1)$$

$$\geq\sum_{1\leq k(p-1)\leq n}v_2(2^{k(p-1)}-1)\geq card\{k|1\leq k(p-1)\leq n\}$$

Since

$$card\{k|1\leq k(p-1)\leq n\}=\left[\frac{n}{p-1}\right],$$

we have found that

$$v_2\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)\geq\left[\frac{n}{p-1}\right].$$

But we know that

$$v_2(n!)=\frac{n-s_p(n)}{p-1}\leq\frac{n-1}{p-1}<\frac{n}{p-1}$$

and since $v_2(n!)\in\mathbb{R}$, we must have

$$v_2(n!)\leq\left[\frac{n}{p-1}\right].$$

From these two inequalities, we conclude that

$$v_2\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)\geq v_2(n!)$$

and now the problem is solved.

Diophantine equations can also be solved using the methods employed in this topic. Here is a difficult one, given in a russian olympiad.

Example 7. Prove that the equation

$$\frac{1}{10^n} = \frac{1}{n_1!} + \frac{1}{n_2!} + \cdots + \frac{1}{n_k!}$$

does not have integer solutions such that $1 \leq n_1 < n_2 < \cdots < n_k$.

Tuymaada Olimpiad

Solution. Suppose we have found a solution of the equation and let us consider

$$P = n_1!n_2! \ldots n_k!.$$

We have

$$10^n((n_1+1)\ldots(n_k-1)n_k + \cdots + (n_{k-1}+1)\ldots(n_k-1)n_k + 1) = n_k!$$

which shows that n_k divides 10^n. Let us write $n_k = 2^x \cdot 5^y$. First of all, suppose that x, y are positive. Thus, $(n_1+1)\ldots(n_k-1)n_k + \cdots + (n_{k-1}+1)\ldots(n_k-1)n_k + 1$ is relatively prime with 10 and it follows that $v_2(n_k!) = v_5(n_k!)$. This implies of course that $\left[\frac{n_k}{2^j}\right] = \left[\frac{n_k}{5^j}\right]$ for all j (because we clearly have $\left[\frac{n_k}{2^j}\right] > \left[\frac{n_k}{5^j}\right]$) and so $n_k \leq 3$. A verification by hand shows that there is no solution in this case.

Next, suppose that $y = 0$. Then $(n_1+1)\ldots(n_k-1)n_k + \cdots + (n_{k-1}+1)\ldots(n_k-1)n_k + 1$ is odd and thus $v_2(n_k!) = n \leq v_5(n_k!)$. Again this implies $v_2(n_k!) = v_5(n_k!)$ and we have seen that this gives no solution. So, actually $x = 0$. A crucial observation is that if $n_k > n_{k-1} + 1$, then $(n_1+1)\ldots(n_k-1)n_k + \cdots + (n_{k-1}+1)\ldots(n_k-1)n_k + 1$ is again odd and thus we find again that $v_2(n_k!) = n \leq v_5(n_k!)$, impossible. So, $n_k = n_{k-1}+1$. But then, taking into account that n_k is a power of 5, we deduce that $(n_1+1)\ldots(n_k-1)n_k + \cdots + (n_{k-1}+1)\ldots(n_k-1)n_k + 1$ is congruent to 2 modulo 4 and thus $v_2(n_k!) = n+1 \leq v_5(n_k!)+1$. It follows that $\left[\frac{n_k}{2}\right] \leq 1 + \left[\frac{n_k}{5}\right]$ and thus $n_k \leq 6$. Since n_k is a power of 5, we

find that $n_k = 5$, $n_{k-1} =$ and a quick research of all possibilities shows that there are no solutions. Thus, the given equation has no solution in natural numbers.

A tricky APMO problem asked once upon a time to prove there is a number $2 < n < 2000$ such that $n|2^n + 2$. We will let to the reader the job to verify that $2 \cdot 11 \cdot 43$ is a solution (and especially the job to find how we arrived at this number) and also the exercise to prove that there are actually infinitely many such numbers. Yet... small verifications show that all such numbers are even. Proving this turns out to be a difficult problem and this was proved for the first time by Sierpinski.

Note. After the quadratic reciprocity law topic, it will be proved that 2 11 43 is a solution of the problem.

Example 8. Prove that for any $n > 1$ we cannot have $n|2^{n-1} + 1$.

Solution. Although very short, the proof is tricky. Let $n = \prod_{i=1}^{s} p_i^{k_i}$ where $p_1 < \cdots < p_s$ are prime numbers. The idea is to look at $v_2(p_i - 1)$. Choose that p_i which minimizes this quantity and write $p_i = 1 + 2^{r_i} m_i$ with m_i odd. Then of course we have $n \equiv 1 \pmod{2^{m_i}}$. Hence we can write $n - 1 = 2^m t$. We have $2^{2^m t} \equiv -1 \pmod{p_i}$ thus we surely have $-1 \equiv 2^{2^m t m_i} \equiv 2^{(p_i-1)t} \equiv 1 \pmod{p_i}$ (the last congruence being derived from Fermat's theorem). Thus $p_i = 2$, which is clearly impossible.

We continue with a very nice and hard problem, in which the idea of looking at the exponents really saves us. This problem seemed to appear for the first time in AMM , proposed by Armond E. Spencer. In the last years, it appeared in various contests.

Example 9. Prove that for any integers $a_1, a_2, \ldots, a_n$ the number $\prod_{1 \le i < j \le n} \frac{a_i - a_j}{i - j}$ is an integer.

Armond Spencer, AMM E 2637

Solution. This time, we consider a prime number p and we prove that for each $k \geq 1$, there are more numbers divisible by p^k in the sequence of differences $(a_i - a_j)_{1 \leq i < j \leq n}$ than in the sequence $(i-j)_{1 \leq i < j \leq n}$. Since

$$v_p\left(\prod_{1 \leq i < j \leq n} (a_i - a_j)\right) = \sum_{k \geq 1} N_{p^k}\left(\prod_{1 \leq i < j \leq n} (a_i - a_j)\right)$$

(here $N_x\left(\prod_{y \in A} y\right)$ is the number of terms from the sequence A that are multiples of x) and

$$v_p\left(\prod_{1 \leq i < j \leq n} (i - j)\right) = \sum_{k \geq 1} N_{p^k}\left(\prod_{1 \leq i < j \leq n} (i - j)\right),$$

the problem will be solved if we prove our claim. Now, let us fix $k \geq 1$ and let us suppose that there are exactly b_i indices $j \in \{1, 2, \ldots, n\}$ such that $a_j \equiv i \pmod{p^k}$, for each $i \in \{0, 1, \ldots, p^k - 1\}$. Then we have

$$N_{p^k}\left(\prod_{1 \leq i < j \leq n} (a_i - a_j)\right) = \sum_{i=0}^{p^k - 1} \binom{b_i}{2}.$$

We see that if $a_i = i$, then $b_i = \left[\frac{n+i}{p^k}\right]$ (there are $\left[\frac{n+i}{p^k}\right]$ numbers congruent with $i \pmod{p}$ between 1 and n; any of them is of the form $i + jp$, with $0 \leq j \leq \frac{n-i}{p}$, of course, if $i = 0$ we have $1 \leq j \leq \frac{n}{p}$). So,

$$N_{p^k}\left(\prod_{1 \leq i < j \leq n} (i - j)\right) = \sum_{i=0}^{p^k - 1} \binom{\left[\frac{n_i}{p^k}\right]}{2}$$

and it suffices to prove that

$$\sum_{i=0}^{p^k - 1} \binom{b_i}{2} \geq \sum_{i=0}^{p^k - 1} \binom{\left[\frac{n_i}{p^k}\right]}{2}.$$

Now, observe that we are practically asked to find the minimal value of $\sum_{i=0}^{p^k-1}\binom{x_i}{2}$, when $\sum_{i=0}^{p^k-1} x_i = n$ (it is clear that $\sum_{i=0}^{p^k-1} b_i = n = \sum_{i=0}^{p^k-1}\left[\frac{n_i}{p^k}\right]$ from the definition of b_i). For this, let us suppose that $x_1 \leq x_2 \leq \cdots \leq x_{p^k-1}$ is the n-tuple which attains the minimal value (such a n-tuple exists since the equation $\sum_{i=0}^{p^k-1} x_i = n$ has a finite number of solutions). If $x_{p^k-1} > x_0 + 1$, then we consider the n-tuple $(x_0+1, x_1, \ldots, x_{p^k-2}, x_{p^k-1}-1)$ which has the sum of the components n, but for which

$$\binom{x_0+1}{2} + \binom{x_1}{2} + \cdots + \binom{x_{p^k-2}}{2} + \binom{x_{p^k-1}-1}{2}$$

$$< \binom{x_0}{2} + \binom{x_1}{2} + \cdots + \binom{x_{p^k-2}}{2} + \binom{x_{p^k-1}}{2}.$$

The last inequality is true, since it is equivalent with $x_{p^k-1} > x_0+1$, so it is true. But this contradicts the minimality of $(x_0, x_1, \ldots, x_2, \ldots, x_{p^k-1})$. So, we must have $x_{p^k-1} \leq x_0 + 1$ and from here it follows that $x_i \in \{x_0, x_0+1\}$ for all $i \in \{0, 1, 2, \ldots, p^k-1\}$. Thus, there is $j \in \{0, 1, 2, \ldots, p^k-1\}$ such that $x_0 = x_1 = \cdots = x_j$ and $x_{j+1} = x_{j+2} = \cdots = x_{p^k-1} = x_0 + 1$. This easily implies that the minimal n-tuple is in fact $\left(\left[\frac{n+i}{p^k}\right]\right)_{i=0,p^k-1}$ and the problem is solved.

Finally, it is time for a challenge.

Example 10. Let a, b two different positive rational numbers such that for infinitely many numbers n, $a^n - b^n$ is integer. Then prove that a, b are also integers.

Gabriel Dospinescu, Mathlinks Contest

Solution. Let us start by writing $a = \frac{x}{z}$, $b = \frac{y}{z}$, where x, y, z are different natural numbers relatively prime. We know thus that $z^n | x^n - y^n$

for infinitely many numbers n. Let M be the set of those numbers n. Now, assume that $z > 1$ and take p a prime divisor of z. Assuming that p does not divide x, it obviously follows that it can't divide y. We have thus two cases:

i) If $p = 2$, then let n such that $2^n | x^n - y^n$ and write $n = 2^{u_n} v_n$, where v_n is odd. From the identity

$$x^{2^{u_n} v_n} - y^{2^{u_n} v_n} = (x^{v_n} - y^{v_n})(x^{v_n} + y^{v_n}) \dots (x^{2^{u_n - 1} v_n} - y^{2^{u_n - 1} v_n})$$

it follows that

$$v_2(x^n - y^n) = v_2(x^{v_n} - y^{v_n}) + \sum_{k=0}^{u_n - 1} v_2(x^{2^k v_n} + y^{2^k v_n}).$$

But $x^{v_n - 1} + x^{v_n - 2} + \dots + x y^{v_n - 2} + y^{v_n - 1}$ is obviously odd (since v_n, x, y are odd), hence

$$v_2(x^{v_n} - y^{v_n}) = v_2(x - y).$$

Similarly, we can prove that

$$v_2(x^{v_n} + y^{v_n}) = v_2(x + y).$$

Since for $k > 0$ we have

$$x^{2^k v_n} + y^{2^k v_n} \equiv 2 \pmod 4,$$

we finally deduce that

$$2^{u_n} v_n \leq v_2(x^n - y^n) \leq v_2(x + y) + v_2(x - y) + u_n - 1 \qquad (*)$$

Consequently, $(2^{u_n})_{n \in M}$ is bounded, a simple reason being the inequality $2^{u_n} \leq v_2(x+y) + v_2(x-y) + u_n - 1$. Hence $(u_n)_{n \in M}$ takes only a finite number of values and from $(*)$ it follows that $(v_n)_{n \in M}$ also takes a finite number of values, that is M is finite.

ii) If p is odd, then let d the smallest positive integer k such that $p | x^k - y^k$. Then for any n in M we will have $p | x^n - y^n$. Let $x = tu$, $y = tv$,

where $(u,v)=1$. Obviously, tuv is not a multiple of p. It follows then that $p|(u^d-v^d, u^n-v^n)=u^{(n,d)}-v^{(n,d)}|x^{(n,d)}-y^{(n,d)}$ and by the choice of d, we must have $d|n$. Take now n in M and write it in the form $n=md$, with m natural. Let $A=x^d$, $B=y^d$. Then $p^m|p^n|x^n-y^n=A^m-B^m$ and this happens for infinitely many numbers m. Moreover, $p|A-B$. Let R the infinite set of those numbers m. For any m in R we have $m\leq v_p(A^m-B^m)$. Now, let us write $m=p^ij$, where j is relatively prime with p. We clearly have

$$A^m-B^m=(A^j-B^j)\frac{A^{pj}-B^{pj}}{A^j-B^j}\cdots\frac{A^{jp^i}-B^{jp^i}}{A^{jp^{i-1}}-B^{jp^{i-1}}}$$

(we have assumed that $i>1$, since the final conclusion will be obvious in any other case). An essential observation is that we cannot have $p^2|\frac{A^{jp^k}-B^{jp^k}}{A^{jp^{k-1}}-B^{jp^{k-1}}}$ for a certain $k>1$. Indeed, otherwise we would have $p^2|A^{jp^k}-B^{jp^k}\Rightarrow p^2|A^{pj}-B^{pj}$ (Euler's theorem). Yet, we also have $p^2|A^{jp^{k-1}(p-1)}+A^{jp^{k-1}(p-2)}B^{jp^{k-1}}+\cdots+b^{jp^{k-1}(p-1)}$. From $p^2|A^j-B^j$ we have

$$A^{jp^{k-1}(p-1)}+A^{jp^{k-1}(p-2)}B^{jp^{k-1}}+\cdots+B^{jp^{k-1}(p-1)}$$

$$\equiv pA^{jp^{k-1}(p-1)}\pmod{p^2},$$

so we should have $p|A$, that is $p|x$, false.

Let us prove now that we cannot have $p^2|\frac{A^{pj}-B^{pj}}{A^j-B^j}$. Indeed, otherwise (since $p|A-B$), we can write $A^j=B^j+wp$ and then a simple computation using Newton's binomial formula shows that

$$\frac{A^{pj}-B^{pj}}{A^j-B^j}=A^{j(p-1)}+A^{j(p-2)}+\cdots+B^{j(p-1)}$$

$$\equiv pB^{j(p-1)}+\frac{p-1}{2}B^{j(p-2)}p^2\equiv pB^{j(p-1)}\pmod{p^2}$$

and thus it would follow that $p|B$, that is $p|y$, false.

After all, we have shown that in this case we must have

$$m \leq v_p(A^m - B^m) \leq v_p(A^j - B^j) + i.$$

Using again the fact that $A \equiv B \pmod{p}$, we infer that

$$A^{j-1} + A^{j-2}B + \cdots + B^{j-1} \equiv jA^{p-1} \equiv j \pmod{p},$$

which shows that

$$v_p(A^j - B^j) = v_p(A - B).$$

Thus, for infinitely many numbers m we have

$$m \leq v_p(A - B) + [\log_2 m],$$

which is clearly impossible.

Thus, we must have $p|x$ and $p|y$, contradiction with the fact that x, y, z are relatively prime. This shows that $z = 1$ and a, b are integers.

Problems for training

1. Prove the identity

$$\frac{lcm(a,b,c)^2}{lcm(a,b) \cdot lcm(b,c) \cdot lcm(c,a)} = \frac{gcd(a,b,c)^2}{gcd(a,b) \cdot gcd(b,c) \cdot gcd(c,a)}$$

for any positive integers a, b, c.

USAMO, 1972

2. Let a, b, c, d be positive integers such that $ab = cd$. Prove that

$$gcd(a,c) \cdot gcd(a,d) = a \cdot gcd(a,b,c,d).$$

Polish Mathematical Olympiad

3. Let $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ be positive integers such that $gcd(a_i, b_i) = 1$ for all $i \in \{1, 2, \ldots, k\}$. Let $m - lcm[b_1, b_2, \ldots, b_k]$. Prove that

$$gcd\left(\frac{a_1 m_1}{b_1}, \frac{a_2 m_2}{b_2}, \ldots, \frac{a_k m_k}{b_k}\right) = gcd(a_1, a_2, \ldots, a_k).$$

IMO Shortlist 1974

4. Let n such that $2^{n-2005}|n!$. Prove that this number has at most 2005 non-zero digits when written in base 2.

5. Prove that for any natural number n we have

$$\frac{(n^2)!}{\binom{n}{n}\binom{n+1}{n}\dots\binom{2n-1}{n}n!^n} \in \mathbb{R}.$$

R.M Grassl, T. Porter, AMM E 3123

6. Prove the identity

$$(n+1)lcm_{k=0,n}\binom{n}{k} = lcm(1,2,\dots,n+1)$$

for any positive integer n.

Peter L Montgomery, AMM E 2686

7. Let $0 < a_1 < \dots < a_n$ be integers. Find the maximal value of the number m for which we can find the integers $0 < b_1 < \dots < b_m$ such that

$$\sum_{k=1}^{n} 2^{a_k} = \sum_{k-1}^{m} b_k \text{ and } \prod_{k=1}^{n}(2^{a_k})! = \prod_{k=1}^{m} b_k!.$$

Gabriel Dospinescu

8. Prove that the least common multiple of the numbers $1, 2, \dots, n$ equals the least common multiple of the numbers $\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}$ if and only if $n+1$ is a prime.

Laurentiu Panaitopol, TST 1990 Romania

9. Prove that for any $n \in \mathbb{N}$ we have $n!(n+1)!(n+2)!|(3n)!$.

Komal

10. Prove that the product of the numbers between $2^{1917}+1$ and $2^{1991}-1$ is not a perfect square.

Tournament of the Towns, 1991

11. Show that if n is a positive integer and a and b are integers, then $n!$ divides $a(a+b)(a+2b)\dots(a+(n-1)b)bn-1$.

IMO Shortlist, 1985

12. Prove that $k!^{k^2+k+1}$ divides $(k^3)!$.

Poland Olympiad

13. Let x, y be relatively prime different natural numbers. Prove that for infinitely many primes p the exponent of p in $x^{p-1} - y^{p-1}$ is odd.

AMM

14. Let $a_1, \ldots, a_n > 0$ such that whenever k is a prime number of a power of a prime number, we have

$$\left\{\frac{a_1}{k}\right\} + \cdots + \left\{\frac{a_n}{k}\right\} < 1.$$

Prove that there is a unique index $i \in \{1, 2, \ldots, n\}$ such that $a_1 + \cdots + a_n < 1 + [a_i]$.

16. Find the exponent of 2 in the decomposition of the number

$$\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}.$$

AMM

17. Prove that $(x_n)_{n\geq 1}$ the exponent of 2 in the decomposition of the numerator of $\frac{2}{1} + \frac{2^2}{2} + \cdots + \frac{2^n}{n}$, goes to infinity as $n \to \infty$. Even more, prove that $x_{2^n} \geq 2^n - n + 1$ (hint: try to prove first the identity $\frac{2}{1} + \frac{2^2}{2} + \cdots + \frac{2^n}{n} = \frac{2^n}{n} \sum_{k=0}^{n-1} \frac{1}{\binom{n-1}{k}}$).

Adapted after a Kvant problem

18. Prove that the product of at most 25 consecutive integers is not a square.

Narumi's theorem

PRIMES AND SQUARES

The study of the properties of the prime numbers is so well developed (yet, many old conjectures and open questions wait their solution), that some properties have become classical and need to be known. In this unit, we will try to present a unitary view over the properties of some classes of primes and also some classical results related to representations as sum of two squares. These things are not new, but they must be included in the mathematical culture of a serious problem-solver. Yet, in the end of the unit, we will discuss as usual some non-classical and surprising problems. So, don't skip this unit!

Since we will use some facts several times in this paper, we prefer to make some notations before discussing the problems. So, we will consider A, B the sets of all prime numbers of the form $4k+1$ and $4k+3$, respectively. Also, let C be the set of all numbers which can be written as the sum of two perfect squares. Our purpose is to present some classical things related to A, B, C. The most spectacular property of the set A is surely the fact that any element is the sum of two squares of positive integers. This is not a trivial property and we will see a beautiful proof for this theorem of Fermat, which is far from easy.

Example 1. Prove that A is a subset of C.

Solution. Thus, we need to prove that any prime number of the form $4k+1$ is the sum of two squares. We will use a very nice theorem of Thue, which says that if n is a positive integer and a is relatively prime with n, then there exist integers $0 < x, y \leq \sqrt{n}$ such that $xa \equiv \pm y \pmod{n}$ for a suitable choice of the signs $+$ and $-$. The proof is simple, but the theorem itself is a diamond. Indeed, let us consider all the pairs $xa - y$, with $0 \leq x, y \leq [\sqrt{n}]$. So, we have a list of $([\sqrt{n}]+1)^2 > n$ numbers and it follows that two numbers among them give the same remainder when divided by n, let them be $ax_1 - y_1$ and $ax_2 - y_2$. It is not difficult to see

that we may assume that $x_1 > x_2$ (we certainly cannot have $x_1 = x_2$ or $y_1 = y_2$). If we take $x = x_1 - x_2$, $y = |y_1 - y_2|$, all the conditions are satisfied and the theorem is proved.

We will use now Wilson's theorem to find an integer n such that $p|n^2 + 1$. Indeed, let us write $p = 4k + 1$ and observe that we can take $n = (2k)!$. Why? Because from Wilson's theorem we have

$$-1 \equiv (p-1)! \pmod{p} \equiv 1 \cdot 2 \ldots \left(\frac{p-1}{2}\right)\left(p - \frac{p-1}{2}\right)\ldots(p-1)$$

$$\equiv (-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!^2 \equiv (2k)!^2 \pmod{p}$$

and the claim is proved. Now, since $p|n^2 + 1$, it is clear that p and n are relatively prime. Hence we can apply Thue's theorem and we find the existence of positive integers $0 < x, y < \sqrt{p}$ (since $\sqrt{p} \notin \mathbb{R}$) such that $p|n^2x^2 - y^2$. Because $p|n^2 + 1$, we find that $p|x^2 + y^2$ and because $0 < x, y < \sqrt{p}$, we conclude that we have in fact $p = x^2 + y^2$. The theorem is proved.

Now, it is time now to study some properties of the set B. Since they are easier, we will discuss them all in a single example.

Example 2. Let $p \in B$ and suppose that x, y are integers such that $p|x^2 + y^2$. Then $p|(x, y)$. Consequently, any number of the form $n^2 + 1$ has only prime factors that belong to A or are equal to 2. Conclude that A is infinite and then that B is infinite.

Solution. Let us focus on the first question. Suppose that $p|(x, y)$ is not true. Then, it is obvious that xy is not a multiple of p. Because $p|x^2 + y^2$, we can write $x^2 \equiv -y^2 \pmod{p}$. Combining this with the observation that $(x, p) = (y, p) = 1$ and with Fermat's theorem, we find that $1 \equiv x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, which is clearly impossible. This settles the first question. The second one follows clearly from the first one. Now, it remains to prove the third assertion.

Proving that B is infinite is almost identical with the proof that there exist infinitely many primes. Indeed, suppose that $p_1, p_2, \ldots, p_n$ are all the elements of B greater than 3 and consider the odd number $N = 4p_1p_2 \ldots p_n + 3$. Because $N \equiv 3 \pmod 4$, N must have a prime factor that belongs to B. But since p_i is not a divisor of N for any $i = \overline{1,n}$ the contradiction is reached and thus B is infinite. In the same manner we can prove that A is infinite, but this time we must use the second question. Indeed, we consider this time the number $M = (q_1q_2 \ldots q_m)^2 + 1$, where $q_1, q_2, \ldots, q_m$ are all the elements of A and then simply apply the result from the second question. The conclusion is plain.

It is not difficult to characterize the elements of the set C. A number is a sum of two squares if and only if any prime factor of it that also belongs to B appears at an even exponent in the decomposition of that number. The proof is just a consequence of the first examples and we will not insist. Having presented some basic results that we will use in this unit, it is time to see how many applications these two examples have. An easy consequence of the previous observations is the following.

As a simple application of the first example, we consider the following problem, which is surely easy for someone who knows Fermat's theorem regarding the elements of A and very difficult otherwise.

Example 3. Find the number of integers $x \in \{-1997, \ldots, 1997\}$ for which $1997 | x^2 + (x+1)^2$.

India, 1998

Solution. We know that any congruence of the second degree reduces to the congruence $x^2 \equiv a \pmod p$. So, let us proceed and reduce the given congruence to this special form. This is not difficult, since $x^2 + (x+1)^2 \equiv 0 \pmod{1997}$ is of course equivalent to $2x^2 + 2x + 1 \equiv 0 \pmod{1997}$, which in turn becomes $(2x+1)^2 + 1 \equiv 0 \pmod{1997}$. Since $1997 \in A$, the congruence $n^2 \equiv -1 \pmod{1997}$ surely has at

least a solution. More precisely, there are exactly two solutions that belong to $\{1, 2, \ldots, 1996\}$ because if n_0 is a solution, so is $1997 - n_0$ and it is clear that it has at most two non-congruent solutions mod 1997. Because $(2, 1997) = 1$, the function $x \to 2x + 1$ is a permutation of $\mathbb{R}_{1997}$ and so the initial congruence has exactly two solutions with $x \in \{1, 2, \ldots, 1996\}$. In a similar way, we find that there are exactly two solutions with $x \in \{-1997, -1996, \ldots, -1\}$. Therefore there are exactly four numbers $x \in \{-1997, \ldots, 1997\}$ such that $1997 | x^2 + (x + 1)^2$.

From a previous observation, we know that the condition that a number is a sum of two squares is quite restrictive. This suggests that the set X is quite RARA. This conclusion can be translated in the following nice problem.

Example 4. Prove that C doesn't have bounded gaps, that is there are arbitrarily long sequences of integers, no term of which can be written as the sum of two perfect squares.

AMM

Solution. The statement of the problem suggests using the Chinese Remainder Theorem, but here the main idea is to use the complete characterization of the set C, that we have just discussed: $C = \{n \in \mathbb{R} |$ if $p|n$ and $p \in B$, then $v_p(n) \in 2\mathbb{R}\}$. Hence we know what we have to do. We will take long sequences of consecutive integers, each of them having a prime factor that belongs to B and has exponent 1. More precisely, we take different elements of B, let them $p_1, p_2, \ldots, p_n$ (we can take as many as we need, since B is infinite) and then we look for a

solution of the system of congruences

$$\begin{cases} x \equiv p_1 - 1 \pmod{p_1^2} \\ x \equiv p_2 - 2 \pmod{p_2^2} \\ \dots \\ x \equiv p_n - n \pmod{p_n^2} \end{cases}$$

The existence of such a solution follows from the Chinese Remainder Theorem. Thus, the numbers $x+1, x+2, \dots, x+n$ cannot be written as the sum of two perfect squares, since $p_i | x_i$, but p_i^2 does not divide $x+i$. Since n is as large as we want, the conclusion follows.

The Diophantine equation $x(x+1)(x+2)\dots(x+n) = y^k$ has been extensively studied by many mathematicians and great results have been obtained. But these results are very difficult to prove and we prefer to present a related problem, with a nice flavor of elementary mathematics.

Example 5. Prove that a set of $p-1$ consecutive positive integers, where $p \in B$, cannot be partitioned into two subsets, each having the same product of the elements.

Solution. Let us suppose that the positive integers $x+1, x+2, \dots, x+p-1$ have been partitioned into two classes X, Y, each of them having the same product of the elements. If at least one of them is a multiple of p, then there must be another one divisible by p (since in this case both the products of elements from X and Y must be multiples of p), which is clearly impossible. Thus, none of these numbers is a multiple of p, which means that the set of remainders of these numbers when divided by p is exactly $1, 2, \dots, p-1$. Also, from the hypothesis it follows that there exists a positive integer n such that

$$(x+1)(x+2)\dots(x+p-1) = n^2.$$

Hence $n^2 \equiv 1 \cdot 2(p-1) \equiv -1 \pmod{p}$, the last congruence being true by Wilson's theorem. But from the second example we know that

the congruence $n^2 \equiv -1 \pmod{p}$ is impossible for $p \in B$ and this is the needed contradiction.

The results stated in the second example are an useful tool in solving non-standard Diophantine equations. The technique is better explained in the following two examples.

Example 6. Prove that the equation $x^4 = y^2 + z^2 + 4$ does not have integer solutions.

Reid Barton, Rookie Contest, 1999

Solution. Practically, we have to show that $x^4 - 4$ does not belong to C. Hence we need to find an element of B that has an odd exponent in the decomposition of $x^4 - 4$. The first case is when x is odd. Using the factorization $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ and the observation that $x^2 + 2 \equiv 3 \pmod{4}$, we deduce that there exists $p \in B$ such that $v_p(x^2 + 2)$ is odd. But since p cannot divide $x^2 - 2$ (otherwise $p | x^2 + 2 - (x^2 - 2)$, which is not the case), we conclude that $v_p(x^4 - 4)$ is odd and so $x^4 - 4$ does not belong to C. We have thus shown that in any solution of the equation x is even, let us say $x = 2k$. Then, we must also have $4k^4 - 1 \in C$, which is clearly impossible since $4k^4 - 1 \equiv 3 \pmod{4}$ and thus $4k^4 - 1$ has a prime factor that belongs to B and has odd exponent. Moreover, it worth noting that the equation $x^2 + y^2 = 4k + 3$ can be solved directly, by working modulo 4. We leave to the reader the details, which are trivial.

The following problem is much more difficult, but the basic idea is the same. Yet, the details are not so obvious and, most important, it is not clear how to begin. It has become a classical problem due to its beauty and difficulty.

Example 7. Let $p \in B$ and suppose that x, y, z, t are integers such that $x^{2p} + y^{2p} + z^{2p} = t^{2p}$. Prove that at least one of the numbers x, y, z, t is a multiple of p.

Solution. First of all, we observe that it is enough to assume that x, y, z, t are relatively prime. Next, we prove that t is odd. Supposing the contrary, we obtain that $x^{2p} + y^{2p} + z^{2p} \equiv 0 \pmod 4$. Since $a^2 \pmod 4 \in \{0, 1\}$, the latter implies that x, y, z are even, contradicting the assumption that $(x, y, z, t) = 1$. Hence t is odd. This implies that at least one of the numbers x, y, z is odd. Suppose that it is z. Now, another step is required. We write the equation in the form

$$x^{2p} + y^{2p} = \frac{t^{2p} - z^{2p}}{t^2 - z^2}(t^2 - z^2)$$

and we look for a prime number $q \in B$ with an odd exponent in the decomposition of a factor that appears in the right-hand side. The best candidate for this factor seems to be

$$\frac{t^{2p} - z^{2p}}{t^2 - z^2} = (t^2)^{p-1} + (t^2)^{p-2}z^2 + \cdots + (z^2)^{p-1},$$

which is congruent to $3 \pmod 4$. This follows from the hypothesis $p \in B$ and the fact that $a^2 \equiv 1 \pmod 4$ for any odd number a. Thus, there exists $q \in B$ such that $v_q\left(\frac{t^{2p} - z^{2p}}{t^2 - z^2}\right)$ is odd. Since $x^{2p} + y^{2p} \in C$, it follows that $v_q(x^{2p} + y^{2p})$ is even and so $v_q(t^2 - z^2)$ is odd. In particular $q|t^2 - z^2$ and, because $q|(t^2)^{p-1} + (t^2)^{p-2}z^2 + \cdots + (z^2)^{p-1}$, we deduce that $q|pt^{2(p-1)}$. If $q \neq p$, then $q|t$, hence $q|z$ and also $q|x^{2p} + y^{2p}$. Because $q \in B$, we infer that $q|(x, y, z, t) = 1$, which is clearly impossible. Therefore $q = p$ and so $p|x^{2p} + y^{2p}$. Because $p \in B$, we find that $p|x$ and $p|y$. The conclusion follows.

It's time for a hard problem.

Example 8. Find the smallest nonnegative integer n for which there exists a non-constant function $f : \mathbb{Z} \to [0, \infty)$ with the following properties:

a) $f(xy) = f(x)f(y)$;

b) $2f(x^2+y^2)-f(x)-f(y) \in \{0,1,\ldots,n\}$ for all integers x and y. For this n, find all the functions with the above properties.

Solution. We will use all results proved in the beginning of the note. First, we will prove that for $n=1$ there are functions which verify a) and b). We remind that A and B are the sets of all primes of the form $4k+1$ and $4k+3$, respectively. For any $p \in B$ we define:

$$f_p : \mathbb{Z} \to \mathbb{Z}, \quad f_p(x) = \begin{cases} 0, & \text{if } p|x \\ 1, & \text{otherwise} \end{cases}$$

Using properties of sets A and B, one can easily verify that f_p verifies the restrictions of the problem. Hence f_p is a solution of the problem for any $p \in B$.

We will prove now that if f is non-constant and verifies the conditions of the problem, then $n > 0$. Suppose not. Then $2f(x^2+y^2) = f(x)+f(y)$ and hence $2f^2(x) = 2f(x^2+0^2) = f(x)+f(0)$. It is clear that we have $f^2(0) = f(0)$. Since f is non-constant, we must have $f(0) = 0$. Consequently, we must have $2f^2(x) = f(x)$ for every integer x. But if there exists x such that $f(x) = \dfrac{1}{2}$, then $f^2(x^2) \neq 2f(x^2)$, contradiction. Thus, $f(x) = 0$ for any integer x and f is constant, contradiction. So, $n = 1$ is the smallest number for which there are non-constant functions which verify a) and b).

We will prove now that any non-constant function f which verifies a) and b) must be of the form f_p. We have already seen that $f(0) = 0$. Since $f^2(1) = f(1)$ and f is non-constant, we must have $f(1) = 1$. Also, $2f^2(x) - f(x) = 2f(x^2+0^2) - f(x) - f(0) \in \{0,1\}$ for every integer x. Thus, $f(x) \in \{0,1\}$.

Since

$f^2(-1) = f(1) = 1$ and $f(-1) \in [0,\infty)$, we must have $f(-1) = 1$ and $f(-x) = f(-1)f(x) = f(x)$ for any integer x. Then, since $f(xy) = f(x)f(y)$, it is enough to find $f(p)$ for any prime p. We prove that there is

exactly one prime number p for which $f(p) = 0$. Since f is non-constant, there exists a prime number p for which $f(p) = 0$. Suppose there is another prime q for which $f(q) = 0$. Then $2f(p^2 + q^2) \in \{0, 1\}$, which means $f(p^2 + q^2) = 0$. Then for any integers a and b we must have: $0 = 2f(a^2+b^2)f(p^2+q^2) = 2f((ap+bq)^2+(aq-bp)^2)$. Since $0 \leq f(x)+f(y) \leq 2f(x^2 + y^2)$ for any x and y, we must have $f(ap + bq) = f(aq - bp) = 0$. Since p and q are relatively prime, there are integers a and b such that $aq - bp = 1$. Then we have $1 = f(1) = f(aq - bp) = 0$, contradiction. So ,there is exactly one prime number p for which $f(p) = 0$. Let us suppose that $p = 2$. Then $f(x) = 0$ for any even x and $2f(x^2+y^2) = 0$ for any odd numbers x and y. This implies that $f(x) = f(y) = 0$ for any odd numbers x and y and thus f is constant, contradiction. Therefore $p \in A \cup B$. Suppose $p \in A$. According to proposition 2, there are positive integers a and b such that $p = a^2 + b^2$. Then we must have $f(a) = f(b) = 0$. But $\max\{a, b\} > 1$ and there is a prime number q such that $q | \max\{a, b\}$ and $f(q) = 0$ (otherwise, we would have $f(\max\{a, b\} = 1)$. But it is clear that $q < p$ and thus we have found two distinct primes p and q such that $f(p) = f(q) = 0$, which, as we have already seen, is impossible. Consequently, $p \in B$ and we have $f(x) = 0$ for any x divisible by p and $f(x) = 1$ for any x which is not divisible by p. Hence, f must be f_p and the conclusion follows.

Problems for training

1. Prove that if $p \in A$, then it can be represented in exactly one way as the sum of the squares of two integers, except for the order of the terms.

2. Prove that a positive integer can be written as the sum of two perfect squares if and only if it can be written as the sum of the squares of two rational numbers.

Euler

3. Find all positive integers n with the property that the equation $n = x^2 + y^2$, where $0 \leq x \leq y$ and $(x, y) = 1$ has exactly one solution.

4. Here is another proof of the theorem from example 1. Suppose that $p = 4k + 1 \in A$ and let $x, y \in \mathbb{Z}$ such that $\max\{|x|, |y|\} < \frac{p}{2}$ and $2x\varepsilon\binom{2k}{k} \pmod{p}$, $y \equiv (2k)!x \pmod{p}$. Prove that $p = x^2 + y^2$.

Gauss

5. Find all pairs of positive integers (m, n) such that

$$m^2 - 1 | 3^m + (n! - 1)^m.$$

Gabriel Dospinescu

6. The positive integers a, b have the property that the numbers $15a + 16b$ and $16a - 15b$ are both perfect squares. What is the least possible value that can be taken on by the smallest of the two squares?

IMO CE AN?

7. Prove that the number $4mn - m - n$ cannot be a perfect square if m, n are positive integers.

IMO 1984 Shortlist

8. Find all n-tuples of positive integers $(a_1, a_2, \ldots, a_n)$ such that

$$(a_1! - 1)(a_2! - 1) \ldots (a_n! - 1) - 16$$

is a perfect square.

Gabriel Dospinescu

9. Find all pairs of positive integers (x, y) such that the number $\frac{x^2 + y^2}{x - y}$ is a divisor of 1995.

Bulgaria, 1995

10. Prove that the equation $y^2 = x^5 - 4$ does not have integer solutions.

Balkan, 1998

11. Solve in integer numbers the equation $x^2 = y^7 + 7$.

ROMOP, 2001

12. Find all positive integers n such that the number $2^n - 1$ has a multiple of the form $m^2 + 9$.

IMO Shortlist, 1999

13. Prove that there exists infinitely many pairs of consecutive numbers, no two of them having any prime factor that belongs to B.

14. Prove that if $n^2 + a \in C$ for any positive integer n, then $a \in C$.

Gabriel Dospinescu

15. Let T the set of the positive integers n for which the equation $n^2 = a^2 + b^2$ has solutions in positive integers. Prove that T has density 1.

Moshe Laub, 6583

16. a) Prove that for any real number x and any natural number N one can find integer numbers p, q such that $|qx - p| \leq \frac{1}{N+1}$.

b) Suppose that $a \in \mathbb{Z}$ is a divisor of a number of the form $n^2 + 1$. Then prove that $a \in C$.

17. Find all functions $f : \mathbb{N} \to \mathbb{Z}$ with the properties:

1. if $a|b$ then $f(a) \geq f(b)$

2. for any natural numbers a, b we have

$$f(ab) + f(a^2 + b^2) = f(a) + f(b).$$

Gabriel Dospinescu, Mathlinks Contest

18. (for the die hards) Let $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ be the famous Lucas's sequence. Then the only $n > 1$ such that L_n is a perfect square is $n = 3$.

Cohn's theorem

T_2'S LEMMA

T_2's lemma is clearly a direct application of the Cauchy-Schwarz inequality. Some will say that it is actually the Cauchy-Schwarz inequality and they are not wrong. Anyway, this particular lemma has become very popular among the American students who attended the training of the USA IMO team. This happened after a lecture delivered by the first author at the Mathematical Olympiad Summer Program (MOSP) held at Georgetown University in June, 2001.

But what exactly does this lemma say? It says that for any real numbers $a_1, a_2, \ldots, a_n$ and any positive real numbers $x_1, x_2, \ldots, x_n$ the inequality

$$\frac{a_1^2}{x_1} + \frac{a_2^2}{x_2} + \cdots + \frac{a_n^2}{x_n} \geq \frac{(a_1 + a_2 + \cdots + a_n)^2}{x_1 + x_2 + \cdots + x_n} \tag{1}$$

holds. And now we see why calling it also the Cauchy-Schwarz inequality is natural, since it is practically an equivalent form of this inequality:

$$\left(\frac{a_1^2}{x_1} + \frac{a_2^2}{x_2} + \cdots + \frac{a_n^2}{x_n}\right)(x_1 + x_2 + \cdots + x_n)$$

$$\geq \left(\sqrt{\frac{a_1^2}{x_1}} \cdot \sqrt{x_1} + \sqrt{\frac{a_2^2}{x_2}} \cdot \sqrt{x_2} + \cdots + \sqrt{\frac{a_n^2}{x_n}} \cdot \sqrt{x_n}\right)^2.$$

But there is another nice proof of (1), by induction. The inductive step is reduced practically to the case $n = 2$, which is immediate. Indeed, it boils down to $(a_1x_2 - a_2x_1)^2 \geq 0$ and the equality occurs if and only if $\dfrac{a_1}{x_1} = \dfrac{a_2}{x_2}$. Applying this result twice it follows that

$$\frac{a_1^2}{x_1} + \frac{a_2^2}{x_2} + \frac{a_3^2}{x_3} \geq \frac{(a_1 + a_2)^2}{x_1 + x_2} + \frac{a_3^2}{x_3} \geq \frac{(a_1 + a_2 + a_3)^2}{x_1 + x_2 + x_3}$$

and we see that a simple inductive argument finishes the proof. With this brief introduction, let us discuss some problems. And there are plenty

of them given in mathematical contests or proposed in mathematical magazines!

First, an old problem, that became classical. We will see that with T_2's lemma it becomes straightforward and even more, we will obtain a refinement of the inequality.

Example 1. Prove that for any positive real numbers a, b, c

$$\frac{a^3}{a^2+ab+b^2}+\frac{b^3}{b^2+bc+c^2}+\frac{c^3}{c^2+ca+a^2}\geq\frac{a+b+c}{3}.$$

Tournament of the Towns, 1998

Solution. We will change the left-hand side of the inequality so that we could apply T_2's lemma. This is not difficult: we just have to write it in the form

$$\frac{a^4}{a(a^2+ab+b^2)}+\frac{b^4}{b(b^2+bc+c^2)}+\frac{c^4}{c(c^2+ca+a^2)}.$$

It follows that the left-hand side is greater than or equal to

$$\frac{(a^2+b^2+c^2)^2}{a^3+b^3+c^3+ab(a+b)+bc(b+c)+ca(c+a)}$$

But we can easily observe that

$$a^3+b^3+c^3+ab(a+b)+bc(b+c)+ca(c+a)=(a+b+c)(a^2+b^2+c^2),$$

so we have proved an even stronger inequality, that is

$$\frac{a^3}{a^2+ab+b^2}+\frac{b^3}{b^2+bc+c^2}+\frac{c^3}{c^2+ca+a^2}\geq\frac{a^2+b^2+c^2}{a+b+c}.$$

The second example also became representative for a whole class of problems. There are countless examples of this type in numerous contests and mathematical magazines, so we find it necessary to discuss it at this point.

Example 2. For arbitrary positive real numbers a, b, c, d prove the inequality

$$\frac{a}{b+2c+3d} + \frac{b}{c+2d+3a} + \frac{c}{d+2a+3b} + \frac{d}{a+2b+3c} \geq \frac{2}{3}.$$

Titu Andreescu, IMO 1993 Shortlist

Solution. If we write the left-hand side in the form

$$\frac{a^2}{a(b+2c+3d)} + \frac{b^2}{b(c+2d+3a)} + \frac{c^2}{c(d+2a+3b)} + \frac{d^2}{d(a+2b+3c)},$$

then the way to continue is clear, since from the lemma we obtain

$$\frac{a}{b+2c+3d} + \frac{b}{c+2d+3a} + \frac{c}{d+2a+3b} + \frac{d}{a+2b+3c}$$

$$\geq \frac{(a+b+c+d)^2}{4(ab+bc+cd+da+ac+bd)}.$$

Hence it suffices to prove the inequality

$$3(a+b+c+d)^2 \geq 8(ab+bc+cd+da+ac+bd).$$

But it is not difficult to see that

$$(a+b+c+d)^2 = a^2+b^2+c^2+d^2+2(ab+bc+cd+da+ac+bd),$$

implies

$$8(ab+bc+cd+da+ac+bd) = 4(a+b+c+d)^2 - 4(a^2+b^2+c^2+d^2).$$

Consequently, we are left with the inequality

$$4(a^2+b^2+c^2+d^2) \geq (a+b+c+d)^2,$$

which is just the Cauchy-Schwarz inequality for four variables.

The problem below, given at the IMO 1995, was discussed extensively in many publications. It could be also solved by using the above lemma.

Example 3. Let a, b, c be positive real numbers such that $abc = 1$. Prove that

$$\frac{1}{a^3(b+c)} + \frac{1}{b^3(c+a)} + \frac{1}{c^3(a+b)} \geq \frac{3}{2}.$$

Solution. We have:

$$\frac{1}{a^3(b+c)} + \frac{1}{b^3(c+a)} + \frac{1}{c^3(a+b)} = \frac{\frac{1}{a^2}}{a(b+c)} + \frac{\frac{1}{b^2}}{b(c+a)} + \frac{\frac{1}{c^2}}{c(c+a)}$$

$$\geq \frac{\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right)^2}{2(ab+bc+ca)} = \frac{(ab+bc+ca)^2}{2(ab+bc+ca)} = \frac{ab+bc+ca}{2} \geq \frac{3}{2},$$

the last inequality following from the AM-GM inequality.

The following problem is also not difficult, but it uses a nice combination between this lemma and the Power-Mean inequality. It is another example in which proving the intermediate inequality (that is, the inequality that remains to be proved after using the lemma) is not difficult.

Example 4. Let $n \geq 2$. Find the minimal value of the expression

$$\frac{x_1^5}{x_2 + x_3 + \cdots + x_n} + \frac{x_2^5}{x_1 + x_3 + \cdots + x_n} + \cdots + \frac{x_n^5}{x_1 + x_2 + \cdots + x_{n-1}},$$

where $x_1, x_2, \ldots, x_n$ are positive real numbers satisfying $x_1^2 + x_2^2 + \cdots + x_n^2 = 1$.

Turkey, 1997

Solution. Usually, in such problems the minimal value is attained when the variables are equal. So, we conjecture that the minimal value is $\frac{1}{n(n-1)}$ attained when $x_1 = x_2 = \cdots = x_n = \frac{1}{\sqrt{n}}$. Indeed, by using the lemma, it follows that the left-hand side is greater than or equal to

$$\frac{\left(\sum_{i=1}^{n} x_i^3\right)^2}{\sum_{i=1}^{n} x_i(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n)}.$$

But it is not difficult to observe that

$$\sum_{i=1}^{n} x_i(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n) = \left(\sum_{i=1}^{n} x_i\right)^2 - 1.$$

So, proving that

$$\frac{x_1^5}{x_2 + x_3 + \cdots + x_n} + \frac{x_2^5}{x_1 + x_3 + \cdots + x_n} + \cdots + \frac{x_n^5}{x_1 + x_2 + \cdots + x_{n-1}} \geq \frac{1}{n(n-1)}$$

reduces to proving the inequality

$$\left(\sum_{i=1}^{n} x_i^3\right)^2 \geq \frac{\left(\sum_{i=1}^{n} x_i\right)^2 - 1}{n(n-1)}.$$

But this is a simple consequence of the Power-Mean inequality. Indeed, we have

$$\left(\frac{\sum_{i=1}^{n} x_i^3}{n}\right)^{\frac{1}{3}} \geq \left(\frac{\sum_{i=1}^{n} x_i^2}{n}\right)^{\frac{1}{2}} \geq \frac{\sum_{i=1}^{n} x_i}{n},$$

implying

$$\sum_{i=1}^{n} x_i^3 \geq \frac{1}{\sqrt{n}} \text{ and } \sum_{i=1}^{n} \sqrt{x_i} \leq \sqrt{n}.$$

The conclusion follows.

In 1954, H.S.Shapiro asked whether the following inequality is true for any positive real numbers $a_1, a_2, \ldots, a_n$:

$$\frac{a_1}{a_2 + a_3} + \frac{a_2}{a_3 + a_4} + \cdots + \frac{a_n}{a_1 + a_2} \geq \frac{n}{2}.$$

The question turned out to be extremely difficult. The answer is really unexpected: one can prove that the inequality is true for all $n = 3, 4, 5, 6, 7$ (and for all small values of n the shortest proof is based on

this lemma), but it is false for all even numbers $n \geq 14$ as well as for sufficiently large odd numbers n. Let us examine the case $n = 5$, a problem proposed for MOSP 2001.

Example 5. Prove that for any positive real numbers a_1, a_2, a_3, a_4, a_5,

$$\frac{a_1}{a_2+a_3}+\frac{a_2}{a_3+a_4}+\frac{a_3}{a_4+a_5}+\frac{a_4}{a_5+a_1}+\frac{a_5}{a_1+a_2}\geq\frac{5}{2}.$$

Solution. Again, we apply the lemma and we conclude that it suffices to prove the inequality

$$(a_1+a_2+a_3+a_4+a_5)^2$$

$$\geq\frac{5}{2}[a_1(a_2+a_3)+a_2(a_3+a_4)+a_3(a_4+a_5)+a_4(a_5+a_1)+a_5(a_1+a_2)]$$

Let us denote $a_1+a_2+a_3+a_4+a_5=S$. Then we observe that

$$a_1(a_2+a_3)+a_2(a_3+a_4)+a_3(a_4+a_5)+a_4(a+5+a_1)+a_5(a_1+a_2)$$
$$=\frac{a_1(S-a_1)+a_2(S-a_2)+a_3(S-a_3)+a_4(S-a_4)+a_5(S-a_5)}{2}$$
$$=\frac{S^2-a_1^2-a_2^2-a_3^2-a_4^2-a_5^2}{2}.$$

With this identity, we infer that the intermediate inequality is in fact

$$(a_1+a_2+a_3+a_4+a_5)^2\geq\frac{5}{4}(S^2-a_1^2-a_2^2-a_3^2-a_4^2-a_5^2),$$

equivalent to $5(a_1^2+a_2^2+a_3^2+a_4^2+a_5^2)\geq S^2$, which is nothing else then the Cauchy-Schwarz inequality.

Another question arises: is there a positive real number such that for any positive real numbers $a_1, a_2, \ldots, a_n$ and any $n \geq 3$ the following inequality holds:

$$\frac{a_1}{a_2+a_3}+\frac{a_2}{a_3+a_4}+\cdots+\frac{a_n}{a_1+a_2}\geq cn.$$

This time, the answer is positive, but finding the best such constant is an extremely difficult task. It was first solved by Drinfield (who, by the way, is a Fields' medalist). The answer is quite complicated and we

will not discuss it here (for a detailed presentation of Drinfield's method the interested reader can consult the written examination given at ENS in 1997). The following problem, given at the Moldavian TST in 2005, shows that $c = \sqrt{2} - 1$ is such a constant (not optimal).

For any $a_1, a_2, \ldots, a_n$ and any $n \geq 3$ the following inequality holds:

$$\frac{a_1}{a_2 + a_3} + \frac{a_2}{a_3 + a_4} + \cdots + \frac{a_n}{a_1 + a_2} \geq (\sqrt{2} - 1)n.$$

The proof is completely elementary, yet very difficult to find. An ingenious argument using the arithmetic-geometric means inequality does the job: let us write the inequality in the form

$$\frac{a_1 + a_2 + a_3}{a_2 + a_3} + \frac{a_2 + a_3 + a_4}{a_3 + a_4} + \cdots + \frac{a_n + a_1 + a_2}{a_1 + a_2} \geq \sqrt{2} \cdot n.$$

Now, using the AM-GM inequality, we see that it suffices to prove the stronger inequality:

$$\frac{a_1 + a_2 + a_3}{a_2 + a_3} \cdot \frac{a_2 + a_3 + a_4}{a_3 + a_4} \cdots \frac{a_n + a_1 + a_2}{a_1 + a_2} \geq (\sqrt{2})^n.$$

Observe that

$$(a_i + a_{i+1} + a_{i+2})^2 = \left(a_i + \frac{a_{i+1}}{2} + \frac{a_{i+1}}{2} + a_{i+2}\right)^2$$

$$\geq 4\left(a_i + \frac{a_{i+1}}{2}\right)\left(\frac{a_{i+1}}{2} + a_{i+2}\right)$$

(the last inequality being again a consequence of the AM-GM inequality). Thus,

$$\prod_{i=1}^{n}(a_i + a_{i+1} + a_{i+2})^2 \geq \prod_{i=1}^{n}(2a_i + a_{i+1}) \prod_{i=1}^{n}(2a_{i+2} + a_{i+1}).$$

Now, the real trick is to rewrite appropriately the last products. Let us observe that

$$\prod_{i=1}^{n}(2a_{i+2} + a_{i+1}) = \prod_{i=1}^{n}(2a_{i+1} + a_i),$$

so

$$\prod_{i=1}^{n}(2a_i+a_{i+1})\prod_{i=1}^{n}(2a_{i+2}+a_{i+1})=\prod_{i=1}^{n}[(2a_i+a_{i+1})(a_i+2a_{i+1})]$$

$$\geq\prod_{i=1}^{n}(2(a_i+a_{i+1})^2)=2^n\left(\prod_{i=1}^{n}(a_i+a_{i+1})\right)^2.$$

The conclusion now follows.

This lemma came handy even at the IMO 2005 (problem 3). In order to prove that for any positive real numbers x,y,z such that $xyz\geq 1$ the following inequality holds

$$\sum\frac{x^2+y^2+z^2}{x^5+y^2+z^2}\leq 3,$$

a few students successfully used the above mentioned lemma. For example, a student from Ireland applied this result and called it "SQ Lemma". During the coordination, the Irish deputy leader explained what "SQ" stood for: "...escu". A typical solution using this lemma is as follows:

$$x^5+y^2+z^2=\frac{x^4}{\frac{1}{x}}+\frac{y^4}{y^2}+\frac{z^4}{z^2}\geq\frac{(x^2+y^2+z^2)^2}{\frac{1}{x}+y^2+z^2},$$

hence

$$\sum\frac{x^2+y^2+z^2}{x^5+y^2+z^2}\leq\sum\frac{\frac{1}{x}+y^2+z^2}{x^2+y^2+z^2}=2+\frac{xy+yz+zx}{xyz(x^2+y^2+z^2)}\leq 3.$$

It is now time for the champions. We begin with a difficult geometric inequality for which we have found a direct solution using T_2's lemma. Here it is.

Example 6. Prove that in any triangle ABC the following inequality holds

$$\frac{r_ar_b}{m_am_b}+\frac{r_br_c}{m_bm_c}+\frac{r_cr_a}{m_cm_a}\geq 3.$$

Ji Chen, Crux Mathematicorum

Solution. Of course, we start by translating the inequality into an algebraic one. Fortunately, this is not difficult, since using Heron's relation and the formulas

$$r_a = \frac{K}{s-a}, \quad m_a = \frac{\sqrt{2b^2+2c^2-a^2}}{2}$$

and the likes the desired inequality takes the equivalent form

$$\frac{(a+b+c)(b+c-a)}{\sqrt{2a^2+2b^2-c^2}\cdot\sqrt{2a^2+2c^2-b^2}} + \frac{(a+b+c)(c+a-b)}{\sqrt{2b^2+2a^2-c^2}\cdot\sqrt{2b^2+2c^2-a^2}}$$

$$+\frac{(a+b+c)(a+b-c)}{\sqrt{2c^2+2b^2-a^2}\cdot\sqrt{2c^2+2a^2-b^2}} \geq 3.$$

In this form, the inequality is more that monstrous, so we try to see if a weaker form holds, by applying the AM-GM inequality to each denominator. So, let us try to prove the stronger inequality

$$\frac{2(a+b+c)(c+b-a)}{4a^2+b^2+c^2} + \frac{2(a+b+c)(c+a-b)}{4b^2+c^2+a^2}$$

$$+\frac{2(a+b+c)(a+b-c)}{4c^2+a^2+b^2} \geq 3.$$

Written in the more appropriate form

$$\frac{c+b-a}{4a^2+b^2+c^2} + \frac{c+a-b}{4b^2+c^2+a^2} + \frac{a+b-c}{4c^2+a^2+b^2} \geq \frac{3}{2(a+b+c)}$$

we see that by T_2's lemma the left-hand side is at least

$$\frac{(a+b+c)^2}{(b+c-a)(4a^2+b^2+c^2)+(c+a-b)(4b^2+a^2+c^2)+(a+b-c)(4c^2+a^2+b^2)}.$$

Basic computations show that the denominator of the last expression is equal to

$$4a^2(b+c)+4b^2(c+a)+4c^2(a+b)-2(a^3+b^3+c^3)$$

and consequently the intermediate inequality reduces to the simpler form

$$3(a^3+b^3+c^3)+(a+b+c)^3 \geq 6[a^2(b+c)+b^2(c+a)+c^2(a+b)].$$

Again, we expand $(a+b+c)^3$ and obtain the equivalent inequality

$$4(a^3+b^3+c^3)+6abc \geq 3[a^2(b+c)+b^2(c+a)+c^2(a+b)],$$

which is not difficult at all. Indeed, it follows from the inequalities

$$4(a^3+b^3+c^3) \geq 4[a^2(b+c)+b^2(c+a)+c^2(a+b)]-12abc$$

and

$$a^2(b+c)+b^2(c+a)+c^2(a+b) \geq 6abc.$$

The first one is just an equivalent form of Schur's inequality, while the second follows immediately from the identity

$$a^2(b+c)+b^2(c+a)+c^2(a+b)-6abc = a(b-c)^2+b(c-a)^2+c(a-b)^2.$$

After all, we have managed to prove the intermediate inequality, hence the problem is solved.

The journey continues with a very difficult problem, given at the Japanese Mathematical Olympiad in 1997 and which became famous due to its difficulty. We will present two solutions for this inequality. The first one uses a nice combination between this lemma and the substitution discussed in the unit "Two useful substitutions".

Example 7. Prove that for any positive real numbers a, b, c the following inequality holds

$$\frac{(b+c-a)^2}{a^2+(b+c)^2}+\frac{(c+a-b)^2}{b^2+(c+a)^2}+\frac{(a+b-c)^2}{c^2+(a+b)^2} \geq \frac{3}{5}.$$

Japan, 1997

Solution. Of course, from the introduction to this problem, the reader has already noticed that it is useless to try a direct application of the lemma, since any such approach is doomed. But with the substitution

$$x=\frac{b+c}{a}, \quad y=\frac{c+a}{b}, \quad z=\frac{a+b}{c},$$

we have to prove that for any positive real numbers x, y, z satisfying $xyz = x + y + z + 2$, the inequality

$$\frac{(x-1)^2}{x^2+1} + \frac{(y-1)^2}{y^2+1} + \frac{(z-1)^2}{z^2+1} \geq \frac{3}{5}$$

holds. It is now time to use T_2's lemma in the form

$$\frac{(x-1)^2}{x^2+1} + \frac{(y-1)^2}{y^2+1} + \frac{(z-1)^2}{z^2+1} \geq \frac{(x+y+z-3)^2}{x^2+y^2+z^2+3}.$$

Hence it is enough to prove the inequality

$$\frac{(x+y+z-3)^2}{x^2+y^2+z^2+3} \geq \frac{3}{5}.$$

But this is equivalent to

$$(x+y+z)^2 - 15(x+y+z) + 3(xy+yz+zx) + 18 \geq 0.$$

This is not an easy inequality. We will use the proposed problem 3 from the unit "Two useful substitutions" to reduce the above inequality to the form

$$(x+y+z)^2 - 9(x+y+z) + 18 \geq 0,$$

which follows from the inequality $x + y + z \geq 6$. And the problem is solved.

But here is another original solution.

Alternative solution. Let us apply T_2's lemma in the following form:

$$\frac{(b+c-a)^2}{a^2+(b+c)^2} + \frac{(c+a-b)^2}{b^2+(c+a)^2} + \frac{(a+b-c)^2}{c^2+(a+b)^2}$$

$$= \frac{((b+c)^2 - a(b+c))^2}{a^2(b+c)^2+(b+c)^4} + \frac{((c+a)^2 - b(c+a))^2}{b^2(c+a)^2+(c+a)^4} + \frac{((a+b)^2 - c(a+b))^2}{c^2(a+b)^2+(a+b)^4}$$

$$\geq \frac{4(a^2+b^2+c^2)^2}{a^2(b+c)^2+b^2(c+a)^2+c^2(a+b)^2+(a+b)^4+(b+c)^4+(c+a)^4}.$$

Consequently, it suffices to prove that the last quantity is greater than or equal to $\frac{3}{5}$. This can be done by expanding everything, but here is an elegant proof using the observation that

$$a^2(b+c)^2 + b^2(c+a)^2 + c^2(a+b)^2 + (a+b)^4 + (b+c)^4 + (c+a)^4$$

$$= [(a+b)^2 + (b+c)^2 + (c+a)^2](a^2+b^2+c^2)$$

$$+2ab(a+b)^2 + 2bc(b+c)^2 + 2ca(c+a)^2.$$

Because

$$(a+b)^2 + (b+c)^2 + (c+a)^2 \leq 4(a^2+b^2+c^2),$$

we observe that the desired inequality reduces to

$$2ab(a+b)^2 + 2bc(b+c)^2 + 2ca(c+a)^2 \leq \frac{8}{3}(a^2+b^2+c^2)^2.$$

But this inequality is not so difficult. Indeed, first we observe that

$$2ab(a+b)^2 + 2bc(b+c)^2 + 2ca(c+a)^2$$

$$\leq 4ab(a^2+b^2) + 4bc(b^2+c^2) + 4ca(c^2+a^2).$$

Then, we also find that

$$4ab(a^2+b^2) \leq a^4 + b^4 + 6a^2b^2,$$

since $(a-b)^4 \geq 0$. Hence

$$4ab(a^2+b^2) + 4bc(b^2+c^2) + 4ca(c^2+a^2) \leq 2(a^2+b^2+c^2)^2$$

$$+2(a^2b^2+b^2c^2+c^2a^2) \leq \frac{8}{3}(a^2+b^2+c^2)^2$$

and so the problem is solved. With minor changes, we can readily see that this solution works without the assumption that a, b, c are positive.

We end this discussion (which remains probably permanently open) with a difficult problem, based on two hidden applications of T_2's lemma.

Example 8. Let $a_1, a_2, \ldots, a_n > 0$ such that $a_1 + a_2 + \cdots + a_n = 1$. Prove that:

$$(a_1a_2+a_2a_3+\cdots+a_na_1)\left(\frac{a_1}{a_2^2+a_2}+\frac{a_2}{a_3^2+a_3}+\cdots+\frac{a_n}{a_1^2+a_1}\right)\geq\frac{n}{n+1}.$$

Gabriel Dospinescu

Solution. How can we get to $a_1a_2 + a_2a_3 + \cdots + a_na_1$? Probably from $\frac{a_1^2}{a_1a_2} + \frac{a_2^2}{a_2a_3} + \cdots + \frac{a_n^2}{a_na_1}$ after we use the lemma. So, let us try this the following estimation:

$$\frac{a_1}{a_2}+\frac{a_2}{a_3}+\cdots+\frac{a_n}{a_1}=\frac{a_1^2}{a_1a_2}+\frac{a_2^2}{a_2a_3}+\cdots+\frac{a_n^2}{a_na_1}\geq\frac{1}{a_1a_2+a_2a_3+\cdots+a_na_1}.$$

The new problem, proving that

$$\frac{a_1}{a_2^2+a_2}+\frac{a_2}{a_3^2+a_3}+\cdots+\frac{a_n}{a_1^2+a_1}\geq\frac{n}{n+1}\left(\frac{a_1}{a_2}+\frac{a_2}{a_3}+\cdots+\frac{a_n}{a_1}\right)$$

seems even more difficult, but we will see that we have to make one more step in order to solve it. Again , we look at the right-hand side and we write $\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_n}{a_1}$ as

$$\frac{\left(\frac{a_1}{a_2}+\frac{a_2}{a_3}+\cdots+\frac{a_n}{a_1}\right)^2}{\frac{a_1}{a_2}+\frac{a_2}{a_3}+\cdots+\frac{a_n}{a_1}}.$$

After applying T_2's lemma, we find that

$$\frac{a_1}{a_2^2+a_2}+\frac{a_2}{a_3^2+a_3}+\cdots+\frac{a_n}{a_1^2+a_1}=\frac{\left(\frac{a_1}{a_2}\right)^2}{a_1+\frac{a_1}{a_2}}+\frac{\left(\frac{a_2}{a_3}\right)^2}{a_2+\frac{a_2}{a_3}}+\cdots+\frac{\left(\frac{a_n}{a_1}\right)^2}{a_n+\frac{a_n}{a_1}}$$

$$\geq\frac{\left(\frac{a_1}{a_2}+\frac{a_2}{a_3}+\cdots+\frac{a_n}{a_1}\right)^2}{1+\frac{a_1}{a_2}+\frac{a_2}{a_3}+\cdots+\frac{a_n}{a_1}}.$$

And we are left with an easy problem: if $t = \frac{a_1}{a_2} + \cdots + \frac{a_n}{a_1}$, then $\frac{t^2}{1+t} \geq \frac{nt}{n+1}$, or $t \geq n$. But this follows immediately from the AM-GM inequality.

Problems for training

1. Let a, b, c, d be positive real numbers such that $a+b+c+d = 1$. Prove that

$$\frac{a^2}{a+b} + \frac{b^2}{b+c} + \frac{c^2}{c+d} + \frac{d^2}{d+a} \geq \frac{1}{2}.$$

Ireland, 1999

2. Let $a, b, c,$ be positive real numbers satisfying $a^2+b^2+c^2 = 3abc$. Prove that

$$\frac{a}{b^2c^2} + \frac{b}{c^2a^2} + \frac{c}{a^2b^2} \geq \frac{9}{a+b+c}.$$

India

3. Let $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ be positive real numbers such that

$$x_1 + x_2 + \cdots + x_n \geq x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

Prove that

$$x_1 + x_2 + \cdots + x_n \leq \frac{x_1}{y_1} + \frac{x_2}{y_2} + \cdots + \frac{x_n}{y_n}.$$

Romeo Ilie, Romanian Olympiad, 1999

4. For arbitrary positive real numbers a, b, c prove the inequality

$$\frac{a}{b+2c} + \frac{b}{c+2a} + \frac{c}{a+2b} \geq 1.$$

Czech-Slovak Competition, 1999

5. Prove that for any positive real numbers a, b, c satisfying $a+b+c = 1$,

$$\frac{a}{1+bc} + \frac{b}{1+ca} + \frac{c}{1+ab} \geq \frac{9}{10}.$$

India

6. Prove that for any positive real numbers a, b, c, d satisfying $ab + bc + cd + da = 1$ the following inequality is true

$$\frac{a^3}{b+c+d} + \frac{b^3}{c+d+a} + \frac{c^3}{d+a+b} + \frac{d^3}{a+b+c} \geq \frac{1}{3}.$$

IMO 1990 Shortlist

7. Prove that if the positive real numbers a, b, c satisfy $abc = 1$, then

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} \geq 1.$$

Vasile Cartoaje, Gazeta Matematica

8. Prove that for any positive real numbers a, b, c the following inequality holds

$$\frac{a^2+bc}{b+c} + \frac{b^2+ca}{c+a} + \frac{c^2+ab}{a+b} \geq a+b+c.$$

Cristinel Mortici, Gazeta Matematica

9. Prove that for any nonnegative real numbers $x_1, x_2, \ldots, x_n$,

$$\frac{x_1}{x_n+x_2} + \frac{x_2}{x_1+x_3} + \cdots + \frac{x_n}{x_{n-1}+x_1} \geq 2.$$

Tournament of the Towns, 1982

10. Prove that for any positive real numbers a, b, c, d, e satisfying $abcde = 1$,

$$\frac{a+abc}{1+ab+abcd} + \frac{b+bcd}{1+bc+bcde} + \frac{c+cde}{1+cd+cdea}$$
$$+\frac{d+dea}{1+de+deab} + \frac{e+eab}{1+ea+eabc} \geq \frac{10}{3}.$$

Waldemar Pompe, Crux Mathematicorum

11. Prove that for any positive real numbers a, b, c the following inequality holds

$$\left(\frac{a}{b+c}\right)^2 + \left(\frac{b}{c+a}\right)^2 + \left(\frac{c}{a+b}\right)^2 \geq \frac{3}{4} \cdot \frac{a^2+b^2+c^2}{ab+bc+ca}.$$

Gabriel Dospinescu

12. Let $n \geq 4$ an integer and let $a_1, a_2, \ldots, a_n$ be positive real numbers such that $a_1^2 + a_2^2 + \cdots + a_n^2 = 1$. Prove that

$$\frac{a_1}{a_2^2+1} + \frac{a_2}{a_3^2+1} + \cdots + \frac{a_n}{a_1^2+1} \geq \frac{4}{5}(a_1\sqrt{a_1} + a_2\sqrt{a_2} + \cdots + a_n\sqrt{a_n})^2.$$

Mircea Becheanu, Bogdan Enescu, TST 2002, Romania

13. Find the best constant $k(n)$ such that for any positive real numbers $a_1, a_2, \ldots, a_n$ satisfying $a_1 a_2 \ldots a_n = 1$ the following inequality holds

$$\frac{a_1 a_2}{(a_1^2+a_2)(a_2^2+a_1)} + \frac{a_2 a_3}{(a_2^2+a_3)(a_3^2+a_2)} + \cdots + \frac{a_n a_1}{(a_n^2+a_1)(a_1^2+a_2)} \leq k_n.$$

Gabriel Dospinescu, Mircea Lascu

14. Prove that for any positive real numbers a, b, c,

$$\frac{(2a+b+c)^2}{2a^2+(b+c)^2} + \frac{(2b+c+a)^2}{2b^2+(c+a)^2} + \frac{(2c+a+b)^2}{2c^2+(a+b)^2} \leq 8.$$

Titu Andreescu, Zuming Feng, USAMO 2003

ONLY GRAPHS, NO SUBGRAPHS!

There were so many strategies and useful ideas till now, that the reader might say: enough with this game of tricks! When shall we go to serious facts? Not only that we will "dissapoint" him again, but we will try also to convince him that these are more than simple tools and tricks. They help to create a good base, which is absolutely indispensable for someone who enjoys mathematics and moreover, they are the first step to some really beautiful and difficult theorems or problems. And the reader must admit that the last problems discussed in the previous units are quite serious facts. It is worth mentioning that they are not panacea. This assertion is proved by the fact that each year problems that are based on well-known "tricks" prove to be very difficult in contests.

We will focus in this unit on a very familiar theme: graphs without complete subgraphs. Why do we say familiar? Because there are hundreds of problems proposed to different contests around the world and in mathematical magazines that deal with this subject and each one seems to add something. Before passing to the first problem, we will assume that the basic knowledge about graphs is known and we will denote by $d(A)$ and $C(A)$ the number, respectively the set of vertices adjacent to A. Also, we will say that a graph does not have a complete k subgraph if there aren't k vertices any two of them connected. For simplicity, we will say that G is k-free. First, we will discuss probably the first classical result about triangles-free graphs, the famous Turan' theorem. But before that, an useful lemma, which is also known as Zarankiewicz lemma and which is the main idea in Turan' theorem' proof.

Example 1. If G is a k-free graph, then there exists a vertex having degree at most $\left[\frac{k-2}{k-1}n\right]$.

Zarankiewicz

Solution. Suppose not and take an arbitrary vertex A_1. Then

$$|C(A_1)| > \left[\frac{k-2}{k-1}n\right],$$

so there exists $A_2 \in C(A_1)$. Moreover,

$$\begin{aligned}|C(A_1) \cap C(A_2)| &= d(A_1) + d(A_2) - |C(A_1 \cup A_2)| \\ &\geq 2\left(1 + \left[\frac{k-2}{k-1}n\right]\right) - n > 0.\end{aligned}$$

Pick a vertex $A_3 \in C(A_1) \cap C(A_2)$. A similar argument shows that

$$|C(A_1) \cap C(A_2) \cap C(A_3)| \geq 3\left(1 + \left[\frac{k-2}{k-1}n\right]\right) - 2n.$$

Repeating this argument, we find

$$A_4 \in C(A_1) \cap C(A_2) \cap C(A_3), \ldots, A_{k-1} \in \bigcap_{i=1}^{k-2} C(A_i).$$

Also, we have

$$\left|\bigcap_{i=1}^{j} C(A_i)\right| \geq j\left(1 + \left[\frac{k-2}{k-1}n\right]\right) - (j-1)n.$$

This can be proved easily by induction. Thus,

$$\left|\bigcap_{i=1}^{k-1} C(A_i)\right| \geq (k-1)\left(1 + \left[\frac{k-2}{k-1}n\right]\right) - (k-2)n > 0$$

and consequently we can choose

$$A_k \in \bigcap_{i=1}^{k-1} C(A_i).$$

But it is clear that $A_1, A_2, \ldots, A_k$ form a complete k graph, which contradicts the assumption that G is k-free.

We are now ready to prove Turan' theorem.

Example 2. The maximal number of edges of a k-free graph with vertices is

$$\frac{k-2}{2} \cdot \frac{n^2 - r^2}{k-1} + \binom{r}{2},$$

where $r = n \pmod{k-1}$.

Turan' theorem

Solution. The theorem will be proved by induction on n. Since the first case is trivial, let us suppose the theorem true for all k-free graphs having $n-1$ vertices and let G a k-free graph with n vertices. Using Zarankiewicz' lemma, we can find a vertex A such that

$$d(A) \leq \left[\frac{k-2}{k-1}n\right].$$

Since the subgraph determined by the other $n-1$ vertices is obviously k-free, using the inductive hypothesis we find that G has at most

$$\left[\frac{k-2}{k-1}n\right] + \frac{k-2}{k-1} \cdot \frac{(n-1)^2 - r_1^2}{2} + \binom{r_1}{2}$$

edges, where $r_1 = n-1 \pmod{k-1}$.

Let $n = q(k-1)+r = q_1(k-1)+r_1+1$. Then $r_1 \in \{r-1, r+k-2\}$ (this is because $r - r_1 \equiv 1 \pmod{k-1}$) and it is easy to check that

$$\left[\frac{k-2}{k-1}n\right] + \frac{k-2}{k-1} \cdot \frac{(n-1)^2 - r_1^2}{2} + \binom{r_1}{2} = \frac{k-2}{2} \cdot \frac{n^2 - r^2}{k-1} + \binom{r}{2}$$

and the inductive step is proved. Now, it remains to construct a k-free graph with n vertices and $\frac{k-2}{2} \cdot \frac{n^2-r^2}{k-1} + \binom{r}{2}$ edges. This is not difficult. Just consider $k-1$ classes of vertices, r of them having $q+1$ elements and the rest q elements and join the vertices situated in different groups. It is immediate to prove that this graph is k-free, has $\frac{k-2}{2} \cdot \frac{n^2-r^2}{k-1} + \binom{r}{2}$ edges and also the minimal degree of the vertices is $\left[\frac{k-2}{k-1}n\right]$. This graph is called Turan' graph and it is denoted by $T(n,k)$.

These two examples generate lots of beautiful and difficult problems. For example, knowing them means a straightforward solution for the following bulgarian problem.

Example 3. There are 2001 towns in a country, every one of which is connected with at least 1600 towns by a direct bus line. Find the largest n for which it is always possible to find n towns, any two of which are connected by a direct bus line.

Spring Mathematics Tournament, 2001

Solution. Practically, the problem asks to find the maximal n such that any graph G with 2001 vertices and minimum degree at least 1600 is not n-free. But Zarankiewicz' lemma implies that if G is n-free, then at least one vertex has degree at most $\left[\frac{n-2}{n-1}2001\right]$. So, we need the maximal n for which $\left[\frac{n-2}{n-1}2001\right] < 1600$. It is immediate to see that it is $n = 5$. Thus, if $n = 5$ then any such graph G is not n-free. It suffices to construct a graph with all degrees of the vertices at least 1600, which is 6-free. We will take of course $T(2001, 6)$, whose minimal degree is $\left[\frac{4}{4}2001\right] = 1600$ and which is of course 6-free. Thus, the answer is $n = 5$.

Here is a beautiful application of Turan' theorem in combinatorial geometry.

Example 4. Given are 21 points on a circle. Show that at least 100 pairs of points subtend an angle smaller than or equal to 120 at the center.

Tournament of the Towns, 1986

Solution. In such problems, it is more important to choose the right graph than to apply the theorem, because as soon as the graph is appropriately chosen, the solution is more or less straightforward. Here, we will consider the graph with vertices in the points and we will connect two points if they subtend an angle smaller than or equal to 120 at the center. Therefore, we need to prove that this graph has at least 100 edges. It seems that this is a reversed form of Turan' theorem, which

maximizes the number of edges in a k-free graph. Yet, the reversed form of a reversed form is the natural one. In the aim of this principle, let us look at the "reversed" graph, the complementary one. We must show that it has at most $\binom{21}{2} - 100 = 110$ edges. But this is immediate, since it is clear that this new graph does not have triangles and so, by Turan' theorem it has at most $\frac{21^2 - 1}{4} = 110$ edges. And the problem is solved.

At first glance, the following problem seem to have no relation with the previously examples, but, as we will see, it is a simple consequence of Zarankiewicz' lemma. This problem is an adaptation of a USAMO 1978 problem. Anyway, this is trickier than the contest problem.

Example 5. There are n delegates at a conference, each of them knowing at most k languages. Anyway, among any three delegates, at least two speak a common language. Find the smallest number n (in terms of k) such that it is always possible to find a language spoken by at least three delegates.

Solution. We will prove that $n = 2k + 3$. First, we prove that if there are $2k + 3$ delegates,then the conclusion of the problem holds. The condition "among any three of them there are at least two who can communicate" suggests us to take the 3-free graph with vertices in the persons and whose edges join persons that cannot communicate. From Zarankiewicz' lemma, there exists a vertex whose degree is at most $\left[\frac{n}{2}\right] = k+1$. Thus, it is not connected with at least $k+1$ other vertices. Therefore, there exists a person A and $k + 1$ persons $A_1, A_2, \ldots, A_{k+1}$ that can communicate with A. Since A knows at most k languages, there are two persons among $A_1, A_2, \ldots, A_p$ that know a language also known by A. But that language is known by at least three delegates and we are done. It remains to prove now that we can create a situation in which there are $2k + 2$ delegates, but no language is known by more than two delegates. We use again Turan' graph, by creating two groups of $k + 1$

delegates. In each group a person will have a common language with each other person from the group and will not have common languages with the members of the other group. Of course, any language is spoken by at most two delegates and there are no triangles.

The following problem turned out to be a surprise at one of the Team Selection Tests for 2004 IMO, being solved by 4 contestants. The idea is even easier than in the previous problems, but this time we need a little observation, that is not so obvious.

Example 6. Let $A_1, A_2, \ldots, A_{101}$ be different subsets of the set $\{1, 2, \ldots, n\}$. Suppose that the union of any 50 subsets has more than $\frac{50}{51}n$ elements. Prove that there are three subsets among them, any two of them having common elements.

Gabriel Dospinescu, TST 2004 Romania

Solution. Of course, as the conclusion suggests, we should take a graph with vertices in the subsets, connecting two subsets if they have common elements. Let us assume that this graph is 3-free. The main idea is not to use Zarankiewicz' lemma, but to find much more vertices with small degrees. In fact, we will prove that there are at least 51 vertices whose degree are smaller than or equal to 50. Suppose this is not the case, thus there are at least 51 vertices whose degrees are greater than 51. Let us pick such a vertex A. It is connected with at least 51 vertices, thus it must be adjacent to a vertex B, whose degree is at least 51. Since A and B are each connected with at least 51 vertices, there is a vertex adjacent to both, so we have a triangle, contradicting our assumption. Therefore, we can find $A_{i_1}, \ldots, A_{i_{51}}$, all of them having degrees at most 50. Consequently, A_{i_1} is disjoint from at least 50 subsets. Since the union of these subsets has more than $\frac{50}{51}n$ elements, we infer that $|A_{i_1}| < n - \frac{50}{51}n = \frac{n}{51}$. In a similar way, we obtain that $|A_{i_j}| \leq \frac{n}{51}$

for all $j \in \{1, 2, \ldots, 51\}$ and so

$$|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_{50}}| \leq |A_{i_1}| + \cdots + |A_{i_{50}}| < \frac{50}{51}n,$$

which contradicts the hypothesis. And the solution ends here.

We end the discussion with an adaptation of a very nice and quite challenging problem from the American Mathematical Monthly.

Example 7. Prove that the complementary of any 3-free graph with n vertices and m edges has at least

$$\frac{n(n-1)(n-5)}{24} + \frac{2}{n}\left(m - \frac{n^2-n}{4}\right)^2$$

triangles.

A.W Goodman, AMM

Solution. Believe it or not, the number of triangles from the complementary graph can be expressed only in terms of the degrees of the vertices of the graph. More precisely, if G is the graph, then the number of triangles from the complementary graph is

$$\binom{n}{3} - \frac{1}{2}\sum_{x \in X} d(x)(n-1-d(x)),$$

where X is the set of vertices of G. Indeed, consider all triples (x, y, z) of vertices of G. We will count the triples that do not form a triangle in the complementary graph $\overline{G}$. Indeed, consider the sum $\sum_{x \in X} d(x)(n-1-d(x))$. It counts twice every triple (x, y, z) in which are connected, while z is not adjacent to any of x, y: once for x and once for y. But it also counts twice every triple (x, y, z) in which y is connected with both x, z: once for x and once for z. Therefore, $\frac{1}{2}\sum_{x \in X} d(x)(n-1-d(x))$ is exactly the number of triples (x, y, z) that do not form a triangle in the complementary graph (here we have used the fact that G is 3-free). Now, it is enough to prove

that

$$\binom{n}{3} - \frac{1}{2}\sum_{x\in X} d(x)(n-1-d(x)) \geq \frac{n(n-1)(n-5)}{24} + \frac{2}{n}\left(m - \frac{n^2-n}{4}\right)^2.$$

Using the observation that $\sum_{x\in X} d(x) = 2m$, after a few computations we find the equivalent form of the inequality

$$\sum_{x\in X} d^2(x) \geq \frac{4m^2}{n}.$$

But this is exactly the Cauchy-Schwarz inequality combined with the observation that

$$\sum_{x\in X} d(x) = 2m.$$

Problems for training

1. In a country there are 1998 cities. In each group of three cities, at least two are not directly connected. What is the maximal number of direct flights?

Japan, 1998

2. Let $x_1, x_2, \ldots, x_n$ be real numbers. Prove that there are at most $\frac{n^2}{4}$ pairs $(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,n\}$ such that $1 < |x_i - x_j| < 2$.

MOSP, CE AN?

3. If n points lie on a circle, then at most $\frac{n62}{3}$ segments connecting them have length greater than $\sqrt{2}$.

Poland, 1997

4. Let G be a graph with no triangles and such that no point is adjacent to all the other vertices. Also, if A and B are not joined by an edge, then there exists a vertex C such that AC and BC are edges. Prove that all vertices have the same degree.

APMO 1990

5. Show that a graph with n vertices and k edges has at least $\frac{k}{3n}(4k-n^2)$ triangles.

APMO 1989

6. Let A be a subset of the set $S = \{1, 2, \ldots, 1000000\}$ having exactly 101 elements. Prove that there exist $t_1, t_2, \ldots, t_{100} \in S$ such that the sets $A_j = \{x + t_j | x \in A\}$ are pairwise disjoint.

IMO 2003

6. There are 1999 people participating in an exhibition. Out of any 50 people, at least 2 do not know each other. Prove that we can find at least 41 people who each know at most 1958 other people.

Taiwan, 1999

7. A graph with n vertices and k edges is 3-free. Prove that we can choose a vertex such that the subgraph induced by the remaining vertices has at most $k\left(1 - \frac{4k}{n^2}\right)$ vertices.

USAMO 1995

8. Prove that for every n one can construct a graph with no triangles and whose chromatic number is at least n.

9. A graph with $n^2 + 1$ edges and $2n$ vertices is given. Prove that it contains two triangles sharing a common edge.

China TST, 1987

10. We are given $5n$ points in a plane and we connect some of them, so that $10n^2 + 1$ segments are drawn. We color these segments in 2 colours. Prove that we can find a monochromatic triangle.

COMPLEX COMBINATORICS

When reading the title, one will surely expect a hard unit, which will show what a complex field is combinatorics. Unfortunately, this was not our intention. We "just" want to discuss some combinatorial problems that can be solved elegantly using complex numbers. In this moment, the reader will probably say we are crazy, but we will continue our idea and say that complex numbers can play a very important role in counting problems and also in problems related to tilings. There are also numerous applications in combinatorial number theory, so our purpose is to present a little bit from each of these situations. After that, the reader will surely have the pleasure of solving the proposed problems using this technique. For fear of useless repetition, we will present in the beginning of the discussion a useful result

Lemma. *If p is a prime number and $a_0, a_1, \ldots, a_{p-1} \in Q$ satisfy the relation*

$$a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{p-1}\varepsilon^{p-1} = 0,$$

where

$$\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p},$$

then $a_0 = a_1 = \cdots = a_{p-1}$.

We will say just a few words about the proof, which is not difficult. It is enough to observe that the polynomials $a_0+a_1x+a_2x^2+\cdots+a_{p-1}x^{p-1}$ and $1+x+x^2+\cdots+x^{p-1}$ cannot be relatively prime-because they share a common root-and since $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over Q, $1 + x + x^2 + \cdots + x^{p-1}$ must divide $a_0 + a_1x + a_2x^2 + \cdots + a_{p-1}x^{p-1}$, which can only happen if $a_0 = a_1 = \cdots = a_{p-1}$. Therefore, the lemma is proved and it is time to solve some nice problems. Not before saying that in the following examples $m(A)$ will denote the sum of the elements of the set A. By convention $m(\emptyset) = 0$.

The first example is an adaptation from a problem given in the Inter-County Contest "Traian Lalescu". Of course, there is a solution using recurrent sequences, but it is by far less elegant than the following one.

Example 1. How many numbers with n digits, all equal to 1, 3, 4, 6, 7, 9 are divisible by 7?

Solution. Let $a_n^{(k)}$ be the number of n-digits numbers, formed using only the digits 1, 3, 4, 6, 7, 9 and which are congruent to k modulo 7. It is clear that

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k = \sum_{x_1,x_2,\ldots,x_n \in \{1,3,4,6,7,9\}} \varepsilon^{x_1+x_2+\cdots+x_n}$$

$$= (\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^9)^n,$$

where $\varepsilon = \cos\dfrac{2\pi}{7} + i \sin\dfrac{2\pi}{7}$. The remark that $1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^6 = 0$ helps us to bring $(\varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^6+\varepsilon^7+\varepsilon^9)^n$ to the simpler form $(-\varepsilon^5)^n$. Let us assume that n is divisible by 7, for example (the other cases can be discussed similarly). Then

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k = (-1)^n$$

and from the lemma we infer that $a_n^{(0)} - (-1)^n = a_n^{(1)} = \cdots = a_n^{(6)}$. Let k be the common value. Then $7k = \sum_{k=0}^{6} a_n^{(k)} - (-1)^n = 6^n - (-1)^n$ - this is because exactly 6^n numbers have n digits, all equal to 1, 3, 4, 6, 7, 9. Thus, in this case we have $a_n^{(0)} = (-1)^n + \dfrac{6^n - (-1)^n}{7}$. We leave to the reader the study of the other cases: $n \equiv 1, 2, 3, 4, 5, 6 \pmod 7$.

The same simple, but tricky idea can offer probably the most beautiful solution for the difficult IMO 1995 problem 6. It worth saying that Nikolai Nikolov won a special prize for the following magnificent solution.

Example 2. Let $p > 2$ be a prime number and $A = \{1, 2, \ldots, 2p\}$. Find the number of subsets of A, each having p elements and the sum of the elements divisible by p.

Marcin Kuczma, IMO 1995

Solution. Consider $\varepsilon = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$ and let x_j the number of subsets $x \subset A$ such that $|X| = p$ and $m(X) \equiv j \pmod p$. Then it is clear that

$$\sum_{j=0}^{p-1} x_j\varepsilon^j = \sum_{B\subset A, |B|=p} \varepsilon^{m(B)} = \sum_{1\le c_1<c_2<\cdots<c_p\le 2p} \varepsilon^{c_1+c_2+\cdots+c_p}.$$

But $\displaystyle\sum_{1\le c_1<c_2<\cdots<c_p\le 2p} \varepsilon^{c_1+c_2+\cdots+c_p}$ is exactly the coefficient of x^p in the expansion $(X+\varepsilon)(X+\varepsilon^2)\ldots(X+\varepsilon^{2p})$. Since $X^p - 1 = (X-1)(X-\varepsilon)\ldots(X-\varepsilon^{p-1})$, we easily find that $(X+\varepsilon)(X+\varepsilon^2)\ldots(X+\varepsilon^{2p}) = (X^p+1)^2$. Thus, $\displaystyle\sum_{j=0}^{p-1} x_j\varepsilon^j = 2$ and lemma implies the equality $x_0 - 2 = x_1 = \cdots = x_{p-1}$. Since there are $\dbinom{2p}{p}$ subsets with p elements, we have

$$x_0 + x_1 + \cdots + x_{p-1} = \binom{2p}{p}.$$

Therefore,

$$x_0 = 2 + \frac{1}{p}\left(\binom{2p}{p} - 2\right).$$

With a somewhat different, but closely related idea we can solve the following nice problem.

Example 3. Let $a_1, a_2, \ldots, a_m$ be natural numbers and let $f(k)$ the number of m-tuples $(c_1, c_2, \ldots, c_m)$ such that $1 \le c_i \le a_i$, $i = \overline{1,m}$ and $c_1 + c_2 + \cdots + c_m \equiv k \pmod n$, where $n > 1$ is a natural number.

Prove that $f(0) = f(1) = \cdots = f(n-1)$ if and only if there exists an index $i \in \{1, 2, \ldots, m\}$ such that $n|a_i$.

Reid Burton, Rookie Contest ,1999

Solution. It is not difficult to observe that

$$\sum_{k=0}^{n-1} f(k)\varepsilon^k = \sum_{1\le c_i\le a_i} \varepsilon^{c_1+c_2+\cdots+c_m} = \prod_{i=1}^{m}(\varepsilon+\varepsilon^2+\cdots+\varepsilon^{a_i})$$

for any complex number ε such that $\varepsilon^{n-1}+\varepsilon^{n-2}+\cdots+\varepsilon+1=0$. Thus, one part of the problem is already proved, since if $f(0)=f(1)=\cdots=f(n-1)$ then of course we can find $i\in\{1,2,\ldots,m\}$ such that $\varepsilon+\varepsilon^2+\cdots+\varepsilon^{a_i}=0$, where we have chosen here a primitive root of the unity ε. We infer that $\varepsilon^{a_i}=1$ and so $n|a_i$. Now, suppose there exists an index $i\in\{1,2,\ldots,m\}$ such that $n|a_i$. Then for any root ε of the polynomial $\sum_{k=0}^{n-1} X^k$ we have $\sum_{k=0}^{n-1} f(k)\varepsilon^k$ and so the polynomial $\sum_{k=0}^{n-1} X^k$ divides the polynomial $\sum_{k=0}^{n-1} f(k)X^k$. This is because the polynomial $\sum_{k=0}^{n-1} X^k$ has only simple roots. By a simple degree consideration, this is possible only if $f(0)=f(1)=\cdots=f(n-1)$. The solution ends here.

The enthusiasm determined by the above solutions will surely be ATENUAT by the following problem, in which e need some tricky manipulations.

Example 4. Let $p>2$ be a prime number and let m,n be multiples of p such that n is odd. For any function $f:\{1,2,\ldots,m\}\to\{1,2,\ldots,n\}$ that satisfies $p|f(1)+f(2)+\cdots+f(m)$, consider the product $f(1)f(2)\cdot f(m)$. Prove that the sum of these products is divisible by $\left(\frac{n}{p}\right)^m$.

Gabriel Dospinescu

Solution. Let $\varepsilon=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$ and x_k be the sum of all the numbers $f(1)f(2)\ldots f(m)$, after all functions $f:\{1,2,\ldots,m\}\to\{1,2,\ldots,n\}$ that satisfy $f(1)+f(2)+\cdots+f(m)\equiv k \pmod p$. It is

clear that:

$$\sum_{k=0}^{p-1} x_k \varepsilon^k = \sum_{c_1,c_2,\ldots,c_m \in \{1,2,\ldots,n\}} c_1 c_2 \ldots c_m \varepsilon^{c_1+c_2+\cdots+c_m}$$

$$= (\varepsilon + 2\varepsilon^2 + \cdots + n\varepsilon^n)^m.$$

Recall the identity

$$1 + 2x + 3x^2 + \cdots + nx^{n-1} = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}.$$

Plugging ε in the previous identity, we find that

$$\varepsilon + 2\varepsilon^2 + \cdots + n\varepsilon^n = \frac{n\varepsilon^{n+2} - (n+1)\varepsilon^{n+1} + \varepsilon}{(\varepsilon-1)^2} = \frac{n\varepsilon}{\varepsilon - 1}.$$

Consequently,

$$\sum_{k=0}^{p-1} x_k \varepsilon^k = \frac{n^m}{(\varepsilon-1)^m}.$$

On the other hand, it is not difficult to deduce the relations

$$\varepsilon^{p-1} + \varepsilon^{p-2} + \cdots + \varepsilon + 1 = 0 \Leftrightarrow$$

$$\frac{1}{\varepsilon - 1} = -\frac{1}{p}(\varepsilon^{p-2} + 2\varepsilon^{p-3} + \cdots + (p-2)\varepsilon + p - 1).$$

Thus, if we consider

$$(X^{p-2} + 2X^{p-3} + \cdots + (p-2)X + p - 1)^m = b_0 + b_1 X + \cdots + b_{m(p-2)} X^{m(p-2)},$$

then we have

$$\frac{n^m}{(\varepsilon-1)^m} = \left(-\frac{n}{p}\right)^m (c_0 + c_1\varepsilon + \cdots + c_{p-1}\varepsilon^{p-1}),$$

where

$$c_k = \sum_{k \equiv k \pmod p} b_j.$$

If $r = \left(-\frac{n}{p}\right)^m$, then we have the relation

$$x_0 - rc_0 + (x_1 - rc_1)\varepsilon + \cdots + (x_{p-1} - rc_{p-1})\varepsilon^{p-1} = 0.$$

From the lemma, it follows that $x_0 - rc_0 = x_1 - rc_1 = \cdots = x_{p-1} - rc_{p-1} = k$. Because clearly $c_0, c_1, \ldots, c_{p-1} \in \mathbb{R}$, it remains to prove that $r|k$. Since

$$pk = x_0 + x_1 + \cdots + x_{p-1} - r(c_0 + c_1 + \cdots + c_{p-1})$$

$$= (1 + 2 + \cdots + n)^m - r(b_0 + b_1 + \cdots + b_{m(p-2)})$$

$$= \left(\frac{n(n+1)}{2}\right)^m - r\left(\frac{p(p-1)}{2}\right)^m,$$

it is clear that $r|k$. Here we have used the hypothesis. The problem is solved.

It is time now to leave this kind of problems and to speak a little bit about some nice applications of complex numbers in tilings. The idea is to put a complex number in each square of a table and then to translate the hypothesis and the conclusion in terms of complex numbers. But we will better see how this technique works by solving a few problems. First, some easy problems.

Example 5. Consider a rectangle which can be tiled with a finite combination of $1 \times m$ or $n \times 1$ rectangles, where m, n are natural numbers. Prove that it is possible to tile this rectangle using only rectangles $1 \times m$ or only with rectangles $n \times 1$.

Gabriel Carrol ,BMC Contest,2000

Solution. It is obvious that the rectangle has natural dimensions, let them be a, b. Now, let us partition the rectangle into 1×1 squares and denote this squares

$$(1,1), (1,2), \ldots, (a,1), \ldots, (a,1), (a,2), \ldots, (a,b).$$

Next, put the number $\varepsilon_1^i \varepsilon_2^j$ in the square whose label is (i,j), where

$$\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},\ \varepsilon_2 = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}.$$

The main observation is that the sum of the numbers in any $1 \times m$ or $n \times 1$ rectangle is 0. This is immediate, but the consequence of this simple observation is really surprising. Indeed, it follows that the sum of the numbers from all the squares is 0 and so

$$0 = \sum_{\substack{1 \le i \le a \\ 1 \le j \le b}} \varepsilon_1^i \varepsilon_2^j = \sum_{i=1}^{a} \varepsilon_1^i \sum_{j=1}^{b} \varepsilon_2^j.$$

Thus, at least one of the numbers $\sum_{i=1}^{a} \varepsilon_1^i$ and $\sum_{j-1}^{b} \varepsilon_2^j$ is 0. But this means that $n|a$ or $m|b$. In any of these cases, it is clear that we can tile the rectangle using only horizontal or vertical rectangles.

The idea in the previous problem is quite useful, many tilings problems having straightforward solutions by using it. An example is the following problem, given in Baltic Contest in 1998.

Example 6. Can we tile a 13×13 table using only $1 \times 4, 4 \times 1$ rectangles, such that only the center of the table does not belong to any rectangle?

Baltic Contest,1998

Solution. Suppose such a tiling is possible and label the squares of the table as in the previous problem. Next, associate to square (k, j) the number i^{k+2j}. Obviously, the sum of the numbers from each $1 \times 4, 4 \times 1$ rectangle is 0. Therefore, the sum of all numbers from the squares of the table is equal to the number in the square situated at the center of the table. Thus,

$$i^{21} = (i + i^2 + \cdots + i^{13})(i^2 + i^4 + \cdots + i^{26}) = i \cdot \frac{i^{13} - 1}{i - 1} \cdot i^2 \cdot \frac{i^{26} - 1}{i^2 - 1} = i^3,$$

which clearly cannot hold. Thus, the assumption was wrong and such a tiling does not exist.

The following example we are going to discuss is based on the same idea, but here complex numbers are more involved.

Example 7. On a 8×9 table we put rectangles 3×1 and figures formed by rectangles 1×3 by cutting the median 1×1 square. The rectangles and the figures do not intersect and cannot be rotated. Prove that there exists a set S of 18 squares of the table such that if there are exactly two uncovered squares, then they belong to S.

Gabriel Dospinescu

Solution. Again, we label the squares of the table $(1,1)$, $(1,2), \ldots,$ $(8,9)$ by starting from the up-left corner. In the square labeled (k,j) we will put the number $i^j \cdot \varepsilon^k$, where $i^2 = -1$ and $\varepsilon^2 + \varepsilon + 1 = 0$. The sum of the numbers from any figure or rectangle is 0. The sum of the numbers from the table is

$$\left(\sum_{k=1}^{8} \varepsilon^k\right)\left(\sum_{j=1}^{9} i^j\right) = -i.$$

Let us suppose that the squares $(a_1, b_1), (a_2, b_2)$ are the only uncovered squares. Then we have of course $i^{b_1}\varepsilon^{a_1} + i^{b_2}\varepsilon^{a_2} = -i$. Let $z_1 = i^{b_1-1}\varepsilon^{a_1}$, $z_2 = i^{b_2-1}\varepsilon^{a_2}$. We have $|z_1| = |z_2| = 1$ and $z_1 + z_2 = -1$. It follows that $\dfrac{1}{z_1} + \dfrac{1}{z_2} = -1$ and so $z_1^3 = z_2^3 = 1$. This in turn implies the equalities $i^{3(b_1-1)} = i^{3(b_2-1)} = 1$, from where we conclude that $b_1 \equiv b_2 \equiv 1 \pmod 4$. Therefore, the relation $z_1 + z_2 = -1$ becomes $\varepsilon^{a_1} + \varepsilon^{a_2} = -1$, which is possible if and only if the remainders of the numbers a_1, a_2 when divided by 3 are 1 and 2. Thus, we can take S the set of squares that lie at the intersection of the lines 1, 2, 4, 5, 7, 8 with the columns 1, 5, 9. From the above argument, if two squares remain uncovered, then surely they belong to S. The conclusion is immediate.

Problems for training

1. Three persons A, B, C play the following game: a subset with k elements of the set $\{1, 2, \ldots, 1986\}$ is selected randomly, all selections having the same probability. The winner is A, B or C, according to the case when the sum of the elements of the selected subset is congruent to 0, 1, or 2 modulo 3. Find all values of k for which A, B, C have equal chances of winning.

Imo Shortlist, 1987

2. The faces of a die are labeled with the numbers 1, 2, 3, 4, 5, 6. We throw the die n times. What is the probability that the sum of the numbers shown by the die is a multiple of 5?

IMC, 1999

3. Let $a_k, b_k, c_k \in \mathbb{R}$, $k = \overline{1,n}$. Let $f(p)$ be the number of ordered triples (A, B, C) of subsets (not necessarily non-empty) of the set $M = \{1, 2, \ldots, n\}$ whose union is M and for which

$$\sum_{i \in M \setminus A} a_i + \sum_{i \in M \setminus B} b_i + \sum_{i \in M \setminus C} c_i \equiv 3 \pmod{p}.$$

We assume that

$$\sum_{i \in \emptyset} x_i = 0 \text{ and } f(0) = f(1) = f(2).$$

Prove that there exists $i \in M$ such that $3 | a_i + b_i + c_i$.

Gabriel Dospinescu, Recreaţii Matematice

4. How many subsets with 100 elements of the set $\{1, 2, \ldots, 2000\}$ have the sum of their elements divisible by 5?

Qihong Xie, High School-Mathematics

5. There are 2000 white balls in a box. There are also unlimited supplies of white, green and red balls, initially outside the box. At each step, we can replace two balls in the box with one or two balls according

to the following rules: two whites or two reds with a green, two greens with a white and red, a white and green with a red or a green and red with a white.

a) After some finite number of steps, in the box there are exactly three balls. Prove that at least one of them is green.

b) Is it possible that after a finite number of steps there is just one ball in the box?

Bulgaria, 2000

6. A 7×7 table is tiled with 16 rectangles 1×3 such that only one square remains uncovered. What is the position of this square?

Tournament of the Towns, 1984

7. Let $k > 2$ be an integer. For which odd natural numbers n can we tile a $n \times n$ table with $1 \times k$ or $k \times 1$ rectangles such that only the square in the center of the table does not belong to any rectangle?

Arhimede Magazine, Gabriel Dospinescu

8. Let $n \geq 2$ be an integer. In each point (i, j) having integer coordinates we write the number $i + j \pmod{n}$. Find all pairs (a, b) of natural numbers such that any residue modulo n appears the same number of times on the frontier of the rectangle of vertices $(0, 0)$, $(a, 0)$, (a, b), $(0, b)$ and also any residue modulo n appears the same number of times in the interior of the same rectangle.

Bulgaria, 2001

9. Let F be the family of the subsets of the set $A = \{1, 2, \ldots, 3n\}$ which have the sum of their elements divisible by 3. For each element of F, compute the square of sum of its elements. What is the value of the sum of all the obtained numbers?

Gabriel Dospinescu

10. Let $p > 3$ be a prime number and let h be the number of sequences $(a_1, a_2, \ldots, a_{p-1}) \subset \{0, 1, 2\}^{p-1}$ such that $p | \sum_{j=0}^{p-1} j a_j$. Also, let k be the number of sequences $(a_1, a_2, \ldots, a_{p-1}) \subset \{0, 1, 3\}^{p-1}$ such that $p | \sum_{j=0}^{p-1} j a_j$. Prove that $h \leq k$ and that the equality appears only for $p = 5$.

IMO 1999 Shortlist

FORMAL SERIES REVISITED

We start with a riddle and a challenge for the reader: what is the connection between the following problems:

1. The set of natural numbers (including 0) is partitioned into a finite number $n \geq 2$ of infinite arithmetic progressions having ratios $r_1, r_2, \ldots, r_n$ and first term $a_1, a_2, \ldots, a_n$. Then the following relation is satisfied:

$$\frac{a_1}{r_1} + \frac{a_2}{r_2} + \cdots + \frac{a_n}{r_n} = \frac{n-1}{2}.$$

2. The vertices of a regular polygon are colored in some fashion so that each set of vertices having the same colour is the set of vertices of a regular polygon. Then there are two congruent polygons among them.

The first problem was discussed during the preparation for IMO of the USA team, but it seems it is a classical result. As for the second one, well, it is a famous problem given in a Russian olympiad and proposed by N. Vasiliev.

If the reader has no clue, then let's give him one small hint: the methods used to solve both problems are very similar and can be included into a larger field, that of formal series. What is that? Well, given a commutative ring A, we can define another ring, called the ring of formal series with coefficients in A and denoted $A[X]$. An element of $A[X]$ is of the form $\sum_{n\geq 0} a_n X^n$, where $a_n \in A$. As we are going to see in what follows, these formal series have some very nice applications in different fields: algebra, combinatorics, number theory. But let's start working now, reminding that the reader is supposed to be familiar with some basic analysis tools:

Example 1. Let $a_1, a_2, \ldots, a_n$ be some complex numbers such that for any $1 \leq k \leq n$ we have $a_1^k + a_2^k + \cdots + a_n^k = 0$. Then all numbers are equal to 0.

Solution. Of course, experienced reader has already noticed that this problem is a trivial consequence of Newton's relations. But what can we do if don't know them? Here is a nice way to solve the problem (and a way to prove Newton's relations too).

First of all, observe that the given condition implies that

$$a_1^k + a_2^k + \cdots + a_n^k = 0$$

for all positive integer k. Indeed, let

$$f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$$

the polynomial $\prod_{i-1}^{n}(x - a_i)$. Then for all $k \geq n+1$ we have

$$a_i^k + b_{n-1}a_i^{k-1} + \cdots + b_0a_i^{k-n} = 0.$$

Then it suffices to add these relations and to prove the statement by strong induction.

Now, let us consider the function

$$f(z) = \sum_{i=1}^{n} \frac{1}{1 - za_i}.$$

Developing it by using

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots \text{(for } |x| < 1),$$

we obtain that $f(z) = n$ for all sufficiently small z (which means that $|z| \max(|a_i|) < 1$). Assume that not all numbers are zero and take $a_1, \ldots, a_s$ $(s \geq 1)$ to be the collection of numbers of maximal modulus among the n numbers. Let the common value of the modulus be r. By taking a sequence $z_p \to \frac{1}{r}$ such that $\left|\frac{z_p}{r}\right| < 1$, we obtain a contradiction with the relation $\sum_{i=1}^{n} \frac{1}{1 - z_p a_i} = n$ (indeed, it suffices to observe that the left-hand side is unbounded, while the second one is bounded). This shows that all numbers are equal to 0.

We are going to discuss a nice number theory problem, whose solution is practically based on the same idea. Yet, there are some details that make the problem more difficult.

Example 2. Let $a_1, a_2, \ldots, a_q, x_1, x_2, \ldots, x_q$ and m some integers such that $m|a_1x_1^k + a_2x_2^k + \cdots + a_qx_q^k$ for all $k \geq 0$. Then

$$m|a_1 \prod_{i=2}^{q}(x_1 - x_i).$$

Gabriel Dospinescu

Solution. Consider this time the formal series

$$f(z) = \sum_{i=1}^{q} \frac{a_i}{1 - zx_i}.$$

By using the same formula as in the first problem, we deduce immediately that

$$f(z) = \sum_{i=1}^{q} a_i + \left(\sum_{i=1}^{q} a_i x_i \right) z + \ldots,$$

which shows that all coefficients of this formal series are integers multiples of m. Obviously, it follows that the formal series

$$\sum a_1(1 - x_2z)\ldots(1 - x_qz)$$

also has all coefficients multiples of m. Now, consider $S_t^{(i)}$ the i-th fundamental symmetric sum in x_j $(j \neq i)$. Since all coefficients of $\sum a_1(1 - x_2z)\ldots(1 - x_qz)$ are multiples of m, a simple computation shows that we have the divisibility relation:

$$m|x_1^{q-1}\sum_{i=1}^{q} a_i - x_i^{q-2}\sum_{i=1}^{q} a_i S_1^{(i)} + \cdots + (-1)^{q-1}\sum_{i=1}^{q} a_i S_{q-1}^{(i)}.$$

This can also be rewritten in the nicer form

$$m|\sum_{i=1}^{q} a_i(x_1^{q-1} - x_1^{q-2}S_1^{(i)} + \cdots + (-1)^{q-1}S_{q-1}^{(i)}).$$

Now, the trivial identity

$$(x_1 - x_1)\dots(x_1 - x_{i-1}(x_1 - x_{i+1})\dots(x_1 - x_n) = 0$$

gives us the not-so obvious relation

$$x_1^{q-1} - x_1^{q-2}S_1^{(i)} + \dots + (-1)^{q-1}S_{q-1}^{(i)} = 0$$

for $i \geq 2$. Therefore we can conclude, since

$$x_1^{q-1} - x_q^{q-2}S_1^{(1)} + \dots + (-1)^{q-1}S_{q-1}^{(1)} = (x_1 - x_2)\dots(x_1 - x_n).$$

In order to solve the problem announced in the very beginning of the presentation, we need a little lemma, which is interesting itself and which we prefer to present as a separate problem:

Example 3. Suppose that the set of natural numbers (including 0) is partitioned into a finite number of infinite arithmetic progressions of ratios $r_1, r_2, \dots, r_n$ and first term $a_1, a_2, \dots, a_n$. Then the following relation is satisfied:

$$\frac{1}{r_1} + \frac{1}{r_2} + \dots + \frac{1}{r_n} = 1.$$

Solution. Let us observe that for any $|x| < 1$ we have the identity:

$$\sum_{k\geq 0} x^{a_1+kr_1} + \sum_{k\geq 0} x^{a_2+kr_2} + \dots + \sum_{k\geq 0} x^{a_n+kr_n} = \sum_{k\geq 0} x^k.$$

Indeed, all we did was to write the fact that each natural number is exactly in one of the arithmetic progressions. The above relation becomes of course the very useful relation:

$$\frac{x^{a_1}}{1-x^{r_1}} + \frac{x^{a_2}}{1-x^{r_2}} + \dots + \frac{x^{a_n}}{1-x^{r_n}} = \frac{1}{1-x} \tag{1}$$

Let us multiply the relation (1) with $1 - x$ and use the fact that $\lim\limits_{x\to 1} \dfrac{1-x^a}{1-x} = a$. We find of course the desired relation

$$\frac{1}{r_1} + \frac{1}{r_2} + \dots + \frac{1}{r_n} = 1.$$

It's time to solve the first problem. We will just a small, but not obvious step and we'll be done. The fundamental relation is again (1). So:

Example 4. The set of natural numbers (including 0) is partitioned into a finite number $n \geq 2$ of infinite arithmetic progressions having ratios $r_1, r_2, \ldots, r_n$ and first term $a_1, a_2, \ldots, a_n$. Then the following relation is satisfied:

$$\frac{a_1}{r_1} + \frac{a_2}{r_2} + \cdots + \frac{a_n}{r_n} = \frac{n-1}{2}.$$

MOSP

Solution. Let us write the relation (1) in the more appropriate form:

$$\frac{x^{a_1}}{1 + x + \cdots + x^{r_1 - 1}} + \cdots + \frac{x^{a_n}}{1 + x + \cdots + x^{r_n - 1}} = 1 \qquad (2)$$

Now, let us derive the relation (2) and then make $x \to 1$ in the resulting expression. A small computation let to the reader will show that

$$\sum_{i=1}^{n} \frac{a_i r_i - \dfrac{r_i(r_i - 1)}{2}}{r_i^2} = 0.$$

But it suffices to use the result proved in example 3 in order to conclude that we must have

$$\frac{a_1}{r_1} + \frac{a_2}{r_2} + \cdots + \frac{a_n}{r_n} = \frac{n-1}{2}.$$

Some commentaries about these two relations are necessary. First of all, using a beautiful and hard result due to Erdos, we can say that the relation

$$\frac{1}{r_1} + \frac{1}{r_2} + \cdots + \frac{1}{r_n} = 1$$

implies that $\max(r_1, r_2, \ldots, r_n) < 2^{2^{n-1}}$. Indeed, this remarkable theorem due to Erdos asserts that if $x_1, x_2, \ldots, x_k$ are natural numbers whose

sum of inverses is strictly smaller than 1, then

$$\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}\leq\frac{1}{u_1}+\frac{1}{u_2}+\cdots+\frac{1}{u_k},$$

where $u_1=2$, $u_{n+1}=u_n^2-u_n+1$. But the reader can verify immediately that

$$\frac{1}{u_1}+\frac{1}{u_2}+\cdots+\frac{1}{u_k}=1-\frac{1}{u_1u_2\ldots u_k}$$

(it is trivial by induction). Thus we can write

$$1-\frac{1}{r_n}\leq 1-\frac{1}{u_1u_2\ldots u_{n-1}},$$

or even better $r_n\leq u_1u_2\ldots u_{n-1}=u_n-1$ (the last relation being again a simple induction). Once again, the reader will do a short induction to prove that $u_n\leq 2^{2^{n-1}}$. And here is how we can prove that $\max(r_1,r_2,\ldots,r_n)<2^{2^{n-1}}$ (since of course any number among $r_1,r_2,\ldots,r_n$ can be taken as r_n). Using the relation proved in example 4, we also deduce that $\max(a_1,a_2,\ldots,a_n)<(n-1)\cdot 2^{2^{n-1}-1}$. This shows that for fixed n not only there is a finite number of ways to partition the set of natural numbers into n arithmetic progressions, but we also have some explicit (even though huge) bounds on ratios and first terms.

It is now time to solve the remarkable problem discussed in the beginning of this note. We will see that in the framework of the previous results proved here, the solution becomes natural. However, it is not at all true, the problem is really difficult.

Example 5. The vertices of a regular polygon are colored such that vertices having the same colour form regular polygons. Prove that there are at least two congruent polygons among them.

N. Vasiliev, Russian Olympiad

Solution. Let us assume that the initial polygon (which we will call big from now on) has n edges and that it is inscribed in the unit circle, the vertices having as affixes the numbers $1,\varepsilon,\varepsilon^2,\ldots,\varepsilon^{n-1}$, where $\varepsilon=$

$e^{\frac{2i\pi}{n}}$ (of course, we will not loose generality with all these restrictions). Consider now $n_1, n_2, \ldots, n_k$ the number of edges of each monochromatic polygon and let us assume that all these numbers are different. Let $\varepsilon_j = e^{\frac{2i\pi}{n_j}}$; observe that the affixes of the vertices of each monochromatic polygon are $z_j, z_j\varepsilon_j, \ldots, z_j\varepsilon_j^{n_j-1}$, for some z_j complex numbers on the unit circle. First, a technical result.

Lemma 1. *For any complex number z, if $\zeta = e^{\frac{2i\pi}{p}}$ then we have the identity*

$$\frac{1}{1-z} + \frac{1}{1-z\zeta} + \cdots + \frac{1}{1-z\zeta^{p-1}} = \frac{p}{1-z^p}.$$

Proving this lemma is a very simple task. Indeed, it suffices to observe that $z, z\zeta, \ldots, z\zeta^{p-1}$ are exactly the roots of $P(X) = X^p - z^p$. Or, we know that

$$\frac{P'(x)}{P(X)} = \frac{1}{X-z} + \cdots + \frac{1}{X-z\zeta^{p-1}}.$$

By taking $X = 1$, we obtain exactly the desired identity.

Now, the hypothesis of the problem and lemma 1 allow to write

$$\frac{n_1}{1-(zz_1)^{n_1}} + \cdots + \frac{n_k}{1-(zz_k)^{n_k}} = \frac{n}{1-z^n}.$$

Also, the simple observation that $n_1 + n_2 + \cdots + n_k = n$ allows the new identity

$$\frac{n_1 z_1^{n_1}}{1-(zz_1)^{n_1}} z^{n_1} + \frac{n_2 z_2^{n_2}}{1-(zz_2)^{n_2}} z^{n_2} + \cdots + \frac{n_k z_k^{n_k}}{1-(zz_k)^{n_k}} z^{n_k} = \frac{nz^n}{1-z^n}. \quad (1)$$

Let us assume now that $n_1 < \min(n_2, \ldots, n_k)$ and let us divide (1) by z^{n_1}. It follows that for non-zero z we have

$$\frac{n_1 z_1^{n_1}}{1-(zz_1)^{n_1}} + \frac{n_2 z_2^{n_2}}{1-(zz_2)^{n_2}} z^{n_2-n_1} + \cdots + \frac{n_k z_k^{n_k}}{1-(zz_k)^{n_k}} z^{n_k-n_1} = \frac{nz^{n-n_1}}{1-z^n}. \quad (2)$$

Well, we are done: it suffices to observe that if we make $z \to 0$ (by non-zero values) in (2) , we obtain that $z_1^{n_1} = 0$, which is surely impossible since $|z_1| = 1$. The proof ends here.

The following problem that we are going to discuss appeared in various contests under different forms. It is a very nice identity that can be proved elementary in a quite messy way. Here is a magical proof using formal series.

Example 6. For any complex numbers $a_1, a_2, \ldots, a_n \in \mathbb{C}$, the following identity holds:

$$\left(\sum_{i=1}^{n} a_i\right)^n - \sum_{i=1}^{n}\left(\sum_{j\neq i} a_j\right)^n$$

$$+ \sum_{1\leq i<j\leq n}\left(\sum_{k\neq i,j} a_k\right)^n - \cdots + (-1)^{n-1}\sum_{i=1}^{n} a_i^n = n!\prod_{i=1}^{n} a_i.$$

Solution. Consider the formal series

$$f(z) = \prod_{i=1}^{n}(e^{za_i} - 1).$$

We are going to compute it in two different ways. First of all, it is clear that

$$f(z) = \prod_{i=1}^{n}\left(za_i + \frac{z^2a_i^2}{2!} + \ldots\right)$$

thus we can say that the coefficient of z^n in this formal series is $\prod_{i=1}^{n} a_i$.

On the other hand, we can write

$$f(z) = e^{z\sum\limits_{i=1}^{n} a_i} - \sum_{i=1}^{n} e^{z\sum\limits_{j\neq i} a_j} + \cdots + (-1)^{n-1}\sum_{i=1}^{n} e^{za_i} + (-1)^n.$$

Indeed, the reader is right: now everything is clear, since the coefficient of z^n in e^{kz} is $\dfrac{k^n}{n!}$. The conclusion is clear: not only the identity is true, but it has a four-line solution!!!

There aren't only algebra problems that can be solved in an elegant manner using formal series, but also some beautiful concocts of numbers theory and combinatorics. We shall focus a little bit more on such type of problems in the sequel.

Example 7. Let $0 = a_0 < a_1 < a_2 < \dots$ be a sequence of positive integers such that the equation $a_i + 2a_j + 4a_k = n$ has a unique solution i, j, k. Find a_{1998}.

IMO Shortlist, 1998

Solution. Here is a very nice answer: 9817030729. Let $A = \{a_0, a_1, \dots\}$ and $b_n = 1$ if $n \in A$ and 0 otherwise. Next, consider the formal series $f(x) = \sum_{n\geq 0} b_n x^n$, the generating function of the set A (we can write in a more intuitive way $f(x) = \sum_{n\geq 0} x^{a_n}$). The hypothesis imposed on the set A translates into

$$f(x)f(x^2)f(x^4) = \frac{1}{1-x}.$$

Replace x by x^{2^k}. We obtain the recursive relation

$$f(x^{2^k})f(x^{2^{k+1}})f(x^{2^{k+2}}) = \frac{1}{1-x^{2^k}}.$$

Now, observe two relations:

$$\prod_{k\geq 0} f(x^{2^k}) = \prod_{k\geq 0}(f(x^{2^{3k}})f(x^{2^{3k+1}})f(x^{2^{3k+2}})) = \prod_{k\geq 0}\frac{1}{1-x^{2^{3k}}}$$

and

$$\prod_{k\geq 1} f(x^{2^k}) = \prod_{k\geq 0}(f(x^{2^{3k+1}})f(x^{2^{3k+2}})f(x^{2^{3k+3}})) = \prod_{k\geq 0}\frac{1}{1-x^{2^{3k+1}}}.$$

Therefore (the reader has observed that rigor was not the strong point in establishing these relations) we have

$$f(x) = \prod_{k\geq 0}\frac{1-x^{2^{3k+1}}}{1-x^{2^{3k}}} = \prod_{k\geq 0}(1+x^{8^k})f(x) = \prod_{k\geq 0}\frac{1-x^{2^{3k+1}}}{1-x^{2^{3k}}} = \prod_{k\geq 0}(1+x^{8^k}).$$

This shows that the set A is exactly the set of nonnegative integers that use only the digits 0 and 1 when written in base 8. A quick computation based on this observation shows that the magical term asked by the problem is 9817030729.

The following problem is an absolute classic. It appeared, under different forms, in Olympiads from all over the world. We will present the latest one, given in a Putnam competition:

Example 8. Find all partitions with two classes A, B of the set of nonnegative integers having the property that for all nonnegative integers n the equation $x + y = n$ with $x < y$ has as many solutions $(x, y) \in A \times A$ as in $B \times B$.

Solution. Consider f, g the generating functions of A, B and write them in explicit form

$$f(x) = \sum_{n \geq 0} a_n x^n, \quad g(x) = \sum_{n \geq 0} b_n x^n$$

(as in the previous problem, a_n equals 1 if $n \in A$ and 0 otherwise). The fact that A, B form a partition of the set of nonnegative integers can be also rewritten as

$$f(x) + g(x) = \sum_{n \geq 0} x^n = \frac{1}{1 - x}.$$

Also, the hypothesis made on the number of solutions of the equation $x + y = n$ imposes that

$$f^2(x) - f(x^2) = g^2(x) - g(x^2).$$

Therefore,

$$f(x^2) - g(x^2) = \frac{f(x) - g(x)}{1 - x},$$

which can also be rewritten as

$$\frac{f(x) - g(x)}{f(x^2) - g(x^2)} = 1 - x.$$

Now, the idea is the same as in the previous problems: replace x by x^{2^k} and iterate the process. After multiplication, we deduce that

$$f(x)-g(x)=\prod_{k\geq 0}(1-x^{2^k})\lim_{x\to\infty}\frac{1}{f(x^{2^n})-g(x^{2^n})}.$$

Let us assume without loss of generality that $0\in A$. Then the reader can easily verify that

$$\lim_{n\to\infty}f(x^{2^n})=1 \text{ and } \lim_{n\to\infty}g(x^{2^n})=0.$$

This shows that actually

$$f(x)-g(x)=\prod_{k\geq 0}(1-x^{2^k})=\sum_{k\geq 0}(-1)^{s_2(k)}x^k,$$

where $s_2(x)$ is the sum of digits of binary representation of x. Taking into account the relation

$$f(x)+g(x)=\sum_{n\geq 0}x^n=\frac{1}{1-x},$$

we finally deduce that A, B are respectively the set of nonnegative integers having even (respectively odd) sum of digits when written in binary.

We will discuss two nice problems in which formal series and complex numbers appear in a quite spectacular way:

Example 9. Let n,k be positive integers such that $n\geq 2^{k-1}$ and let $S=\{1,2,\ldots,n\}$. Prove that the number of subsets $A\subset S$ such that $\sum_{x\in A}x\equiv m \pmod{2^k}$ does not depend on $m\in\{0,1,\ldots,2^k-1\}$.

Balkan Olympiad Shortlist 2005

Solution. Let us consider the function (call it formal series, if you want)

$$f(x)=\prod_{i=1}^{n}(1+x^i).$$

If we prove that $1+x+\cdots+x^{2^k-1}$ divides $f(x)$, then we have certainly done the job. In order to prove this, it suffices of course to

prove that any 2^kth root of unity, except for 1 is a root of f. But it suffices to observe that for any $l \in \{1, 2, \ldots, 2^{k-1} - 1\}$ we have

$$\left(\cos \frac{2l\pi}{2^k} + i \sin \frac{2l\pi}{2^k}\right)^{2^{k-2-v_2(l)}} = -1$$

and so

$$f\left(\cos \frac{2l\pi}{2^k} + i \sin \frac{2l\pi}{2^k}\right) = 0,$$

which proves our claim and finishes the solution.

Example 10. Let $m, n \geq 2$ be positive integers and $a_1, a_2, \ldots, a_n$ integers, none of them divisible by m^{n-1}. Prove that one can find integers $e_1, e_2, \ldots, e_n$, not all zero, such that $|e_i| < m$ for all i and such that $m^n | e_1 a_1 + e_2 a_2 + \cdots + e_n a_n$.

IMO Shortlist 2002

Solution. Look at the set $A = \left\{ \sum_{i=1}^{n} e_i a_i |\ 1 \leq e_i \leq m \right\}$ and observe that we can assume that A is a complete system of residues modulo m^n (otherwise, the conclusion is immediate). Now, consider $f(x) = \sum_{p \in A} x^a$. On one hand, we have

$$f(x) = \prod_{i=1}^{n} \left(\sum_{j=0}^{m-1} x^{ja_i} \right) = \prod_{i=1}^{n} \frac{1 - x^{ma_i}}{1 - x^{a_i}}.$$

On the other hand, take $\varepsilon = e^{\frac{2i\pi}{m^n}}$. Since A is a complete system of residues modulo m^n, we must have $f(\varepsilon) = 0$. Therefore (the hypothesis ensures that $\varepsilon^{a_i} \neq 1$) we must have $\prod_{i=1}^{n} (1 - \varepsilon^{ma_i}) = 0$. But this surely contradicts the fact that none of the numbers $a_1, a_2, \ldots, a_n$ is a multiple of m^{n-1}.

Finally, it is time for a tough problem. Of course, it will be a combinatorial problem, whose nice solution below was found by Constantin Tanasescu.

Example 11. Let A be the set of all words which can be formed using $m \geq 2$ given letters. For any $c \in A$, let $l(c)$ be its length. Also, let $C \subseteq A$ be a set of words. We know that any word from A can be obtained in at most one way by concatenating words from C. Prove the inequality:

$$\sum_{c \in C} \frac{1}{m^{l(c)}} \leq 1.$$

Adrian Zahariuc

Solution. Let S be the set of all words which can be obtained by concatenating words from C. Let

$$f(x) = \sum_{c \in C} x^{l(c)}, \quad g(x) = \sum_{s \in S} x^{l(s)}.$$

By the definition of S, we have that:

$$g(x) = 1 + f(x) + f^2(x) + \cdots = \frac{1}{1 - f(x)}.$$

Therefore,

$$f(x)g(x) = g(x) - 1. \qquad (*)$$

Now, S (and C) has at most m^k elements of length k, thus $g(x) < \infty$ and $f(x) < \infty$ for $x < \dfrac{1}{m}$. Thus, for all $x \in \left(0, \dfrac{1}{m}\right)$:

$$f(x)g(x) = g(x) - 1 < g(x)$$

and so $f(x) < 1$ for all $x \in \left(0, \dfrac{1}{m}\right)$. All we need now is to make x tend to $\dfrac{1}{m}$ and we will obtain that $f\left(\dfrac{1}{m}\right) \leq 1$, which is nothing else than the desired inequality.

Proposed problems

1. Let $z_1, z_2, \ldots, z_n$ be some arbitrary complex numbers. Prove that for any $\varepsilon > 0$ there are infinitely many numbers n such that

$$\sqrt[k]{|z_1^k + z_2^k + \cdots + z_n^k|} > \max(|z_1|, |z_2|, \ldots, |z_n|) - \varepsilon.$$

2. Find the general formula for the sequence $(x_n)_{n\geq 1}$ given by

$$x_{n+k} = a_1 x_{n+k-1} + \cdots + a_k x_n$$

in function of $x_0, x_1, \ldots, x_{k-1}$. Here $a_1, \ldots, a_k$ are arbitrary complex numbers.

3. Prove that if we partition the natural numbers into a finite number of infinite arithmetic progressions, then there will be two of them having the same ratio.

4. How many polynomials P with coefficients 0, 1, 2 or 3 satisfy $P(2) = n$, where n is a given positive integer?

Romanian TST, 1994

5. Define $A_1 = \emptyset$, $B_1 = \{0\}$ and $A_{n+1} = \{1 + x |\ x \in B_n\}$, $B_{n+1} = (A_n \setminus B_n) \cup (B_n \setminus A_n)$. What are the positive integers n such that $B_n = \{0\}$?

AMM

6. In how many ways can we parenthesis a non-associative product $a_1 a_2 \ldots a_n$?

Catalan's problem

7. For which positive integers n can we find real numbers $a_1, a_2, \ldots, a_n$ such that

$$\{|a_i - a_j| \mid 1 \leq i < j \leq n\} = \left\{1, 2, \ldots, \binom{n}{2}\right\}?$$

China TST 2002

8. Let $a_1, a_2, \ldots, a_n$ relatively prime positive integers. Find in closed form a sequence $(x_n)_{n\geq 1}$ such that if $(y_n)_{n\geq 1}$ is the number of positive integral solutions to the equation $a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = k$, then $\lim\limits_{n\to\infty} \dfrac{x_n}{y_n} = 1$.

9. Let $A_1, A_2, \ldots, A_k \in M_n(C)$ be some complex $n\theta n$ matrices such that

$$\|A_1^p + A_2^p + \cdots + A_k^p\| \leq \frac{C}{p!}$$

for any natural number $p \geq 1$. Here C does not depend on $p \geq 1$ and $\|X\| = \max\limits_{1 \leq i,j \leq n} |x_{ij}|$. Then prove that $A_i^n = 0$ for all $1 \leq i \leq k$.

Gabriel Dospinescu

10. Is there an infinite set of natural numbers such that all sufficiently large integer can be represented in the same number of ways as the sum of two elements of the set?

D. Newman

11. Find all possibilities to color a regular polygon in the way presented in example 5.

12. Find all positive integers n with the following property: for any real numbers $a_1, a_2, \ldots, a_n$, knowing the numbers $a_i + a_j$, $i < j$, determines $a_1, a_2, \ldots, a_n$ uniquely.

Erdos and Selfridge

13. Suppose that $a_0 = a_1 = 1$, $(n+3)a_{n+1} = (2n+3)a_n + 3na_{n-1}$. Prove that all terms of this sequence are integers.

Komal

14. Define two sequences of integer numbers $(a_n), (b_n) : a_1 = b_1 = 0$ and

$$a_n = nb_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1.$$

Prove that for any prime number p we have $p | a_p$.

Komal

15. Is it possible to partition the set of all 12-digit numbers into groups of 4 numbers such that the numbers in each group have the same digits in 11 places and four consecutive digits in the remaining place?

16. Prove the following identity

$$\sum_{k=1}^{n} \sum_{1\le i_1<i_2<\cdots<i_k\le n} \sum_{\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n\in\{-1,1\}} \frac{(-1)^k}{2^k}(\varepsilon_1 a_{i_1} + \varepsilon_2 a_{i_2} + \cdots + \varepsilon_k a_{i_k})^{2n}$$
$$= \frac{(-1)^n (2n)! a_1^2 a_2^2 \ldots a_n^2}{2^n}$$

for any real numbers $a_1, a_2, \ldots, a_n$.

Gabriel Dospinescu

17. A set of positive integers A has the property that for some positive integers b_i, c_i, the sets $b_i A + c_i$, $1 \le i \le n$ are disjoint subsets of A. Prove that

$$\sum_{i=1}^{n} \frac{1}{b_i} \le 1.$$

IMO Shortlist 2004

NUMBERS AND LINEAR ALGEBRA

We have seen how analysis can help in solving number theory problems. But linear algebra has an important role as well, especially because it makes a beautiful connection between number theory and algebra. This discussion practically started from the following difficult problem that we solved in the chapter "Look at the exponent!" and which appeared in the American Mathematical Monthly a long time ago.

For any integers $a_1, a_2, \ldots, a_n$ the number $\prod_{1 \le i < j \le n} \frac{a_j - a_i}{j - i}$ is an integer.

You will see a nice and short solution to this problem. At the appropriate time... But first, we need some basic facts about matrices, determinants, and systems of linear equations. For example, the fact that any homogeneous linear system

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = 0 \end{cases}$$

in which

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} \neq 0$$

has only the trivial solution. Secondly, we need Vandermonde's identity

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i). \qquad (1)$$

With these basic facts (of course, for a better understanding, the reader should have some more knowledge on linear algebra), we are ready to begin the discussion. As usual, we start with an easy and classical problem. This time, we will prove a result from the theory of permutations. Here is a nice solution.

Example 1. Let σ be a permutation of the numbers $1, 2, \ldots, n$. Then

$$\left| \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) \right| = 1! \cdot 2! \ldots (n-1)!.$$

Solution. The formula in the left-hand side suggests that we might use Vandermonde's identity (1). But we also need a small trick. Using the fact that $\det A = \det {}^tA$ for any matrix A, we get

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \sigma(1)^{n-1} & \sigma(2)^{n-1} & \sigma(3)^{n-1} & \ldots & \sigma(n)^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)).$$

So, by multiplying the two determinants we find

$$\left(\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) \right)^2 =$$

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \sigma(1)^{n-1} & \sigma(2)^{n-1} & \sigma(3)^{n-1} & \ldots & \sigma(n)^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & \sigma(1) & \ldots & \sigma(1)^{n-1} \\ 1 & \sigma(2) & \ldots & \sigma(2)^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \sigma(n) & \ldots & \sigma(n)^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} S_0 & S_1 & \ldots & S_{n-1} \\ S_1 & S_2 & \ldots & S_n \\ \ldots & \ldots & \ldots & \ldots \\ S_{n-1} & \ldots & \ldots & S_{2n-2} \end{vmatrix},$$

where

$$S_i = \sigma(1)^i + \sigma(2)^i + \cdots + \sigma(n)^i.$$

But since σ is a permutation of the numbers $1, 2, \ldots, n$, we have $S_i = 1^i + 2^i + \cdots + n^i$ and repeating the arguments we conclude that

$$\left(\prod_{1 \le i < j \le n} (\sigma(j) - \sigma(i)) \right)^2 = \left(\prod_{1 \le i < j \le n} (j - i) \right)^2.$$

Hence

$$\left| \prod_{1 \le i < j \le n} (\sigma(j) - \sigma(i)) \right| = \prod_{1 \le i < j \le n} (j - i) = (n-1)!(n-2)! \ldots 1!.$$

Using this result, we can answer immediately the following question:

Example 2. Given a polynomial with complex coefficients, can we decide if it has a double zero only by performing additions, multiplications, and divisions on its coefficients?

Solution. Yes, we can. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then this polynomial has a double root if and only if

$$\left(\prod_{1 \le i < j \le n} (x_i - x_j) \right)^2 = 0,$$

where $x_1, x_2, \ldots, x_n$ are the zeros of the polynomial. But we have seen that

$$\left(\prod_{1 \le i < j \le n} (x_i - x_j) \right)^2 = \begin{vmatrix} S_0 & S_1 & \ldots & S_{n-1} \\ S_1 & S_2 & \ldots & S_n \\ \ldots & \ldots & \ldots & \ldots \\ S_{n-1} & \ldots & \ldots & S_{2n-2} \end{vmatrix},$$

where $S_i = x_1^i + x_2^i + \cdots + x_n^i$. So, we need to express $S_i = x_1^i + x_2^i + \cdots + x_n^i$ in terms of the coefficients of the polynomial. But this is a consequence of Newton's and Vieta's formulas, which combined yield

$$a_n S_i + a_{n-1} S_{i-1} + \cdots + a_{n-i+1} S_1 + i a_{n-i} S_i = 0, \quad i \in \{1, 2, \ldots, \}.$$

The last formula allows us to prove by induction that S_i can be expressed only in terms of the coefficients of the polynomial (this could have been shown much easier, since after all S_i is a symmetric polynomial in n variables, hence it can be expressed only in terms of the fundamental symmetric polynomials, which can also be expressed in terms of the coefficients due to Vieta's formulas). Consequently, we can decide whether

$$\left(\prod_{1\leq i<j\leq n}(x_i-x_j)\right)^2=0$$

only by using the described operations on the coefficients of the polynomial, which shows that the answer to the problem is positive.

You may know the following classical problem: if $a,b,c\in Q$ verify $a+b\sqrt[3]{2}+c\sqrt[3]{4}=0$, then $a=b=c=0$. Have you ever thought about the general case? This cannot be done only with simple tricks. We need much more. Of course, a direct solution could be the following: from Eisenstein's criterion, the polynomial $f(X)=X^n-2$ is irreducible, so if $a_0+a_1\sqrt[n]{2}+\cdots+a_{n-1}\sqrt[n-1]{2^{n-1}}=0$ for some rational numbers $a_0,a_1,\ldots,a_{n-1}$, then the polynomial $g(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ is not relatively prime with f. Hence $gcd(f,g)$ is a polynomial of degree at most $n-1$ that divides an irreducible polynomial f of degree n. This cannot happen, unless $g=0$, i.e. $a_0=a_1=\cdots=a_{n-1}=0$. But here is a beautiful proof using linear algebra. This time we will have to be careful to work in the most appropriate field.

Example 3. Prove that if $a_0,a_1,\ldots,a_{n-1}\in Q$ satisfy

$$a_0+a_1\sqrt[n]{2}+\cdots+a_{n-1}\sqrt[n-1]{2^{n-1}}=0,$$

then $a_0=a_1=\cdots=a_{n-1}=0$.

Solution. If $a_0+a_1\sqrt[n]{2}+\cdots+a_{n-1}\sqrt[n-1]{2^{n-1}}=0$, then

$$ka_0+ka_1\sqrt[n]{2}+\cdots+ka_{n-1}\sqrt[n-1]{2^{n-1}}=0$$

for any real number k. Thus, we may assume that $a_0, a_1, \ldots, a_{n-1} \in Z$ (for example, we can choose k to be the least common multiple of all denominators of the numbers $a_0, a_1, \ldots, a_{n-1}$). The idea is to choose n values for k so that to obtain a system of linear equations, having nontrivial solutions. Then, the determinant of the system must be zero and this will imply $a_0 = a_1 = \cdots = a_{n-1} = 0$. Now, let us fill in the blanks. What are the best values for k? This can be seen by noticing that $\sqrt[n]{2^{n-1}} \cdot \sqrt[n]{2} = 2 \in Z$. So, the values $(k_1, k_2, \ldots, k_n) = (1, \sqrt[n]{2}, \ldots, \sqrt[n]{2^{n-1}})$ are good and the system becomes

$$\begin{cases} a_0 + a_1 \cdot \sqrt[n]{2} + \cdots + a_{n-1} \cdot \sqrt[n]{2^{n-1}} = 0 \\ a_0 \cdot \sqrt[n]{2} + a_1 \cdot \sqrt[n]{2^2} + \cdots + 2a_{n-1} = 0 \\ \ldots \\ a_0 \cdot \sqrt[n]{2^{n-1}} + 2a_1 + \cdots + a_{n-1} \cdot \sqrt[n]{2^{n-2}} = 0 \end{cases}$$

Viewing $(1, \sqrt[n]{2}, \ldots, \sqrt[n]{2^{n-1}})$ as a nontrivial solution to the system, we conclude that

$$\begin{vmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ 2a_{n-1} & a_0 & \ldots & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots \\ 2a_1 & 2a_2 & \ldots & a_0 \end{vmatrix} = 0.$$

But what can we do now? Expanding the determinant leads nowhere. As we said before passing to the solution, we should always work in the most appropriate field. This time the field is Z_2, since in this case the determinant can be easily computed. It equals $\overline{a}_0^n = \overline{0}$. Hence a_0 must be even, that is $a_0 = 2b_0$ and we have

$$\begin{vmatrix} b_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & 2a_2 & \ldots & a_0 \end{vmatrix} = 0.$$

Now, we interchange the first two lines of the determinant. Its value remains 0, but when we expand it in Z_2, it is $\overline{a}_1^n = \overline{0}$. Similarly, we find that all a_i are even. Let us write $a_i = 2b_i$. Then we also have $b_0 + b_1 \cdot \sqrt[n]{2} + \cdots + b_{n-1} \cdot \sqrt[n-1]{2^{n-1}} = 0$ and with the same reasoning we conclude that all b_i are even. But of course, we can repeat this as long as we want. By the method of infinite descent, we find that $a_0 = a_1 = \cdots = a_{n-1} = 0$.

The above solution might seem exaggeratedly difficult compared with the one using Eisenstein's criterion, but the idea was too nice not to be presented here.

The following problem can become a nightmare despite its simplicity.

Example 4. Let $A = \{a^3 + b^3 + c^3 - 3abc |\ a, b, c \in Z\}$. Prove that if $x, y \in A$ then $xy \in A$.

Proof. The observation that

$$a^3 + b^3 + c^3 - 3abc = \begin{vmatrix} a & c & b \\ b & a & c \\ c & b & a \end{vmatrix}$$

leads to a quick solution. Indeed, it suffices to note that

$$\begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix} \begin{pmatrix} x & z & y \\ y & x & z \\ z & y & x \end{pmatrix} =$$

$$= \begin{pmatrix} ax + cy + bz & az + by + cx & ay + bx + cz \\ ay + bx + cz & ax + cy + bz & az + by + cx \\ az + by + cx & ay + bx + cz & ax + cy + bz \end{pmatrix}$$

and thus

$$(a^3 + b^3 + c^3 - 3abc)(x^2 + y^3 + z^3 - 3xyz) = A^3 + B^3 + C^3 - 3ABC,$$

where $A = ax + cy + bz$, $B = az + by + cx$, $C = ax + cy + bz$. You see, identities are not so hard to find...

We all know the famous Bezout's theorem, stating that if $a_1, a_2, \ldots,$ a_n are relatively prime, then one can find integers $k_1, k_2, \ldots, k_n$ such that $k_1a_1 + k_2a_2 + \cdots + k_na_n = 1$. The following problem claims more, at least for $n = 3$.

Example 5. Prove that if a, b, c are relatively prime integers, then there are integers x, y, z, u, v, w such that

$$a(yw - zv) + b(zu - xw) + c(xv - yu) = 1.$$

Solution. First of all, there is a crucial observation to be made: the given condition can be also written in the form $\det A = 1$, where

$$A = \begin{pmatrix} a & x & u \\ b & y & v \\ c & z & w \end{pmatrix}.$$

So, let us prove a much more general result.

Theorem. *Any vector v whose integer components are relatively prime is the first column of an integral matrix with determinant equal to 1.*

There is a simple proof of this theorem, using clever manipulations of determinant properties and induction on the dimension n of the vector v. Indeed, for $n = 2$ it is exactly Bezout's theorem. Now, assume that it is true for vectors in Z^{n-1} and take $v = (v_1, v_2, \ldots, v_n)$ such that v_i are relatively prime. Consider the numbers $\frac{v_1}{g}, \ldots, \frac{v_{n-1}}{g}$, where g is the greatest common divisor of $v_1, \ldots, v_{n-1}$. They are relatively prime and

thus we can find an integral matrix

$$\begin{pmatrix} \dfrac{v_1}{g} & a_{12} & \dots & a_{1,n-1} \\ \dots & \dots & \dots & \dots \\ \dfrac{v_{n-1}}{g} & a_{n-1,2} & \dots & a_{n-1,n} \end{pmatrix}$$

having determinant equal to 1. Now, using Bezout's theorem, we can find α, β such that $\alpha g + \beta v_n = 1$. In this case, it is not difficult to verify that the following matrix has integral entries and determinant equal to 1:

$$\begin{pmatrix} v_1 & a_{12} & \dots & a_{1,n-1} & (-1)^{n-1}\beta\dfrac{v_1}{g} \\ \dots & \dots & \dots & \dots & \dots \\ v_{n-1} & a_{n-1,2} & \dots & a_{n-1,n-1} & (-1)^{n-1}\beta\dfrac{v_{n-1}}{g} \\ v_n & 0 & \dots & 0 & (-1)^{n-1}\alpha \end{pmatrix}.$$

We said at the beginning that the discussion started from the difficult problem that appeared in AMM, but yet we did not present its solution yet. It is now time to do it.

Example 6. For any integers $a_1, a_2, \dots, a_n$ then

$$\prod_{1 \le i < j \le n} \frac{a_j - a_i}{j - i} \in Z.$$

Armond Spencer, AMM E 2637

Solution. With this introduction, the way to proceed is clear. What does the expression $\prod_{1 \le i < j \le n} (a_j - a_i$ suggest? It is the Vandermonde's identity (1), associated to $a_1, a_2, \dots, a_n$. But we have a hurdle here. We might want to use the same formula for the expression $\prod_{1 \le i < j \le n} (j - i)$. This is a dead end. But we have seen what is $\prod_{1 \le i < j \le n} (j - i)$ equal to in

the first problem. It equals $(n-1)!(n-2)!\ldots 1!$. Now, we can write

$$\prod_{1\le i<j\le n}\frac{a_j-a_i}{j-i}=\frac{1}{1!\cdot 2!\ldots(n-1)!}\begin{vmatrix} 1 & 1 & 1 & \ldots & 1\\ a_1 & a_2 & a_3 & \ldots & a_n\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & a_n^{n-1} & \end{vmatrix}.$$

As usual, the last step is the most important. The above formula can be rewritten as

$$\prod_{1\le i<j\le n}\frac{a_j-a_i}{j-i}=\begin{vmatrix} 1 & 1 & 1 & \ldots & 1\\ \frac{a_1}{1!} & \frac{a_2}{1!} & \frac{a_3}{1!} & \ldots & \frac{a_n}{1!}\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ \frac{a_1^{n-1}}{(n-1)!} & \frac{a_2^{n-1}}{(n-1)!} & \frac{a_2^{n-1}}{(n-1)!} & \ldots & \frac{a_n^{n-1}}{(n-1)!} \end{vmatrix}.$$

And now we recognize the form

$$\prod_{1\le i<j\le n}\frac{a_j-a_i}{j-i}=\begin{vmatrix} 1 & 1 & \ldots & 1\\ \binom{a_1}{1} & \binom{a_2}{1} & \ldots & \binom{a_n}{1}\\ \binom{a_1}{2} & \binom{a_2}{2} & \ldots & \binom{a_n}{2}\\ \ldots & \ldots & \ldots & \ldots\\ \binom{a_1}{n-1} & \binom{a_2}{n-1} & \ldots & \binom{a_n}{n-1} \end{vmatrix},$$

which can be proved easily by subtracting lines. Because each number $\binom{a_i}{j}$ is an integer, the determinant itself is an integer and the conclusion follows.

We end the unit with a very nice and difficult problem that also appeared in AMM in 1998. A variant of this problem was given in 2004 at a TST in Romania and turned out to be a hard problem.

Example 7. Consider the sequence $(x_n)_{n\geq 0}$ defined by $x_0 = 4$, $x_1 = x_2 = 0$, $x_3 = 3$ and $x_{n+4} = x_n + x_{n+1}$. Prove that for any prime p the number x_p is a multiple of p.

AMM

Solution. Let us consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and let trX be the sum of the entries of the main diagonal of the matrix X. We will first prove that $x_n = TrA^n$ (here $A^0 = I_4$). This is going to be the easy part of the solution. Indeed, for $n = 1, 2, 3$ it is not difficult to verify it. Now, assume that the statement is true for all $i = 1, 2, \ldots, n-1$ and prove that it is also true for n. This is true because

$$x_n = x_{n-4} + x_{n-3} = TrA^{n-4} + TrA^{n-3} = Tr(A^{n-4}(A + I_4)) = TrA^n.$$

We have used here the relation $A^4 = A + I_4$, which can be easily verified by a simple computation. Hence the claim is proved.

Now, let us prove an important result, that is $TrA^p \equiv TrA \pmod{p}$ for any integral matrix and any prime p. The proof is not trivial at all. A possible advanced solution is to start by considering the matrix $\overline{A}$ obtained by reducing all entries of A modulo p, then by placing ourselves in a field in which the characteristic polynomial of A has all its zeroes $\lambda_1, \lambda_2, \ldots, \lambda_n$. This field has clearly characteristic p (it contains Z_p) and so we have (using the binomial formula and the fact that all coefficients $\binom{p}{k}$, $1 \leq k \leq p-1$ are multiples of p)

$$trA^p = \sum_{i=1}^{n} \lambda_i^p = \left(\sum_{i=1}^{n} \lambda_i \right)^p = (TrA)^p,$$

from where the conclusion is immediate via Fermat's little theorem.

But there is a beautiful elementary solution. Let us consider two integral matrices A, B and write

$$(A+B)^p = \sum_{A_1,\ldots,A_p \in \{A,B\}} A_1 A_2 \ldots A_p.$$

Observe that for any A, B we have $Tr(AB) = Tr(BA)$ and by induction, for any $X_1, \ldots, X_n$ and any cyclic permutation σ,

$$Tr(X_1 \ldots X_n) = Tr(X_{\sigma(1)} \ldots X_{\sigma(n)}).$$

Now, note that in the sum $\sum_{A_1,\ldots,A_p \in \{A,B\}} A_1 A_2 \ldots A_p$ we can form $\frac{2^p - 2}{p}$ groups of p-cycles and we have two more terms A^p and B^p. Thus $\sum_{A_1,\ldots,A_p \in \{A,B\}} Tr(A_1 A_2 \ldots A_p) \equiv TrA^p + TrB^p$ modulo p (the reader has already noticed that Fermat's little theorem comes handy once again), since the sum of $Tr(A_1 A_2 \ldots A_p)$ is a multiple of p in any cycle. Thus we have proved that

$$Tr(A+B)^p \equiv TrA^p + TrB^p \pmod{p}$$

and by an immediate induction we also have

$$Tr(A_1 + \cdots + A_k)^p \equiv \sum_{i=1}^{k} TrA_i^p.$$

Next, consider the matrices E_{ij} that have 1 in position (i,j) and 0 elsewhere. For these matrices we clearly have $TrA^p \equiv TrA \pmod{p}$ and by using the above result we can write (using Fermat's little theorem one more time):

$$TrA^p = Tr\left(\sum_{i,j} a_{ij} E_{ij}\right)^p$$

$$\equiv \sum_{i,j} Tr(a_{ij}^p E_{ij}^p) \equiv \sum_{i,j} a_{ij} TrE_{ij} = TrA \pmod{p}.$$

The result is proved and with it the fact that x_p is a multiple of p.

Problems for training

1. Let $F_1 = 1$, $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 3$ be the Fibonacci sequence. Prove that

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n \text{ and } F_{m+n} = F_nF_{m-1} + F_{n+1}F_m.$$

2. Let the sequence of polynomials $(f_n)_{n\geq 1}$ be defined by $f_1(x) = 1$, $f_2(x) = x$ and $f_{n+1}(x) = xf_n(x) + f_{n-1}(x)$. Prove that this sequence satisfies the following Fibonacci-type relations $f_{m+n} = f_nf_{m-1}+f_{n+1}f_m$.

3. Prove that the number $\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7}$ is irrational.

4. Compute the product $\prod_{0\leq i<j\leq n-1} (\varepsilon_j - \varepsilon_i)^2$, where

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

for all $k \in \{0, 1, \ldots, n-1\}$.

5. Consider 2005 real numbers with the following property: whenever we eliminate one number, the rest can be divided into two groups of 1002 numbers each and having the same sum per group. Prove that all the 2005 numbers are equal.

6. Let a, b, c be relatively prime nonzero integers. Prove that for any relatively prime integers u, v, w satisfying $au + bv + cw = 0$, there are integers m, n, p such that

$$a = nw - pv,\ b = pu - mw,\ c = mv - nu.$$

Octavian Stanasila, TST 1989, Romania

7. Let p be a prime and suppose that the real numbers $a_1, a_2, \ldots, a_{p+1}$ have the property: no matter how we eliminate one of them, the rest of the numbers can be divided into at least two nonempty classes,

any two of them being disjoint and each class having the same arithmetic mean. Prove that $a_1 = a_2 = \cdots = a_{p+1}$.

Marius Radulescu, TST 1994 ,Romania

8. Let a, b, c be integers and define the sequence $(x_n)_{n\geq 0}$ by $x_0 = 4$, $x_1 = 0$, $x_2 = 2c$, $x_3 = 3b$ and $x_{n+3} = ax_{n-1} + bx_n + cx_{n+1}$. Prove that for any prime p and any positive integer m, the number x_{p^m} is divisible by p.

Calin Popescu, TST 2004, Romania

9. Prove that for any integers $a_1, a_2, \ldots, a_n$ the following number

$$\frac{lcm(a_1, a_2, \ldots, a_n)}{a_1 a_2 \ldots a_n} \prod_{1\leq i<j\leq n} (a_j - a_i)$$

is an integer divisible by $1!2!\ldots(n-2)!$. Moreover, we cannot replace $1!2!\ldots(n-2)!$ by any other multiple of $1!2!\ldots(n-2)!$.

10. Let $a_1, a_2, \ldots, a_n \in \mathbb{R}$. A move is transforming the n-tuple $(x_1, x_2, \ldots, x_n)$ into the n-tuple

$$\left(\frac{x_1 + x_2}{2}, \frac{x_2 + x_3}{2}, \ldots, \frac{x_{n-1} + x_n}{2}, \frac{x_n + x_1}{2}\right).$$

Prove that if we start with an arbitrary n-tuple $(a_1, a_2, \ldots, a_n)$, after finitely many moves we obtain an n-tuple $(A_1, A_2, \ldots, A_n)$ such that

$$\max_{1\leq i<j\leq n} |A_i - A_j| < \frac{1}{2^{2005}}.$$

11. Let $a_1^{(0)}, a_2^{(0)}, \ldots, a_n^{(0)} \in \mathbb{R}$ and define $a_i^{(k)} = \dfrac{a_i^{(k-1)} + a_{i+2}^{(k-1)}}{2}$ for all $k \geq 1$ and $1 \leq i \leq n$ (the indices are taken modulo n). Prove that

$$\sum_{k=0}^{n} (-2)^k \binom{n}{k} a_i^{(k)} = (-1)^n a_i^{(0)}$$

for all $1 \leq i \leq n$.

Gabriel Dospinescu

ARITHMETIC PROPERTIES OF POLYNOMIALS

Another topic with old fashioned tricks... will surely say the reader at first about this small note. Yet, how many times happened to pass too many time on a problem just because we neglected basic and trivial aspects of it? This is why we think that speaking about these "old fashioned tricks" is not lack of imagination, but rather an imperious need. In this small note we joined together some classical arithmetic properties of polynomials. Of course, as usual, the list is just a small and insignificant introduction to this field, but some basic things should become reflex and between them there are also some problems we shall discuss. As usual, we kept some chestnuts for the end of the note, so the tough solver will have his own part of lecture, especially in a chapter like this one, when extremely difficult problems with extremely simple statements can be asked...

There is one result that should be remembered, that is for any polynomial $f \in Z[X]$ and any different integers $a, b, a-b$ divides $f(a)-f(b)$. Practically, this is the fundamental result that we shall use continuously.

We will start with an essential result, due to Schur, and which appeared in many variants in contests. Although in the topic Analysis against number theory we proved an even more general result using a nice analytical argument, we prefer to present here a purely arithmetic proof.

Example 1. (Schur) Let $f \in Z[X]$ be a non constant polynomial. Then the set of prime numbers dividing at least one non-zero number between $f(1), f(2), \ldots, f(n), \ldots$ is infinite.

Proof. First, suppose that $f(0) = 1$ and consider the numbers $f(n!)$. For sufficiently large n, they are non-zero integers. Moreover, $f(n!) \equiv 1 \pmod{n!}$ and so if we pick a prime divisor of each of the numbers $f(n!)$. we obtain the conclusion (since in particular any such prime divisor is

greater than n). Now, if $f(0) = 0$, the conclusion is obvious. Suppose thus that $f(0) \neq 0$ and consider the polynomial $g(x) = \dfrac{f(xf(0))}{f(0)}$. Obviously, $g \in Z[X]$ and $g(0) = 1$. Applying now the first part of the solution, we easily get the conclusion.

This result has, as we have already said, important consequences. Here is a nice application.

Example 2. Suppose that $f, g \in Z[X]$ are monic non constant irreducible polynomials such that for all sufficiently large n, $f(n)$ and $g(n)$ have the same set of prime divisors. Then $f = g$.

Solution. Indeed, by Gauss's lemma, the two polynomials are irreducible in $Q[X]$. Even more, if they are not equal, then the above remark and the fact that they have the same leading coefficient implies they are relatively prime in $Q[X]$. Using Bezout's theorem we conclude instantly that we can find a non zero integer N and $P, Q \in Z[X]$ such that $fP + gQ = N$. This shows that for all sufficiently large n, all prime factors of $f(n)$ divide N. But, of course, this contradicts Schur's result.

The result of example 2 remains true if we assume the same property valuable for infinitely many numbers n. Yet, the proof uses some highly non elementary results of Erdos in this field. Interested reader will find a rich literature on this field.

A refinement of Schur's lemma is discussed in the following example. The ingredient is, as usual, the Chinese remainder theorem.

Example 3. Let $f \in Z[X]$ be a non constant polynomial and n, k some positive integers. Then prove that there exists a positive integer a such that each of the numbers $f(a), f(a+1), \ldots, f(a+n-1)$ has at least k distinct prime divisors.

Bulgarian Olympiad

Solution. Let us consider an array of different prime numbers $(p_{ij})_{i,j=\overline{1,k}}$ such that for some positive integers x_{ij} such that $f(x_{ij}) \equiv 0 \pmod{p_{ij}}$. We know that this is possible from Schur's theorem. Now, using the Chinese remainder theorem we can find a positive integer a such that $a_i - 1 \equiv x_{ij} \pmod{p_{ij}}$. Using the fundamental result, it follows that each of the numbers $f(a), f(a+1), \ldots, f(a+n-1)$ has at least k distinct prime divisors.

Classical arithmetic "tricks" and the fundamental result that $a-b$ divides $f(a)-f(b)$ are the main ingredients of the following problem.

Example 4. Find all polynomials with integer coefficients f such that for all sufficiently large n, $f(n)|n^{n-1}-1$.

Gabriel Dospinescu

Solution. Since clearly $f(X) = X - 1$ is a solution, let us consider an arbitrary solution and write it in the form $f(X) = (X-1)^r g(X)$ with $r \geq 0$ and $g \in Z[X]$ such that $g(1) \neq 0$. Thus, there exists M such that for all $n > M$ we have $g(n)|n^{n-1}-1$.

We will prove that g is constant. Supposing the contrary, then, since changing g and his opposite has no effect, we may assume that the leading coefficient of g is positive. Thus one can find $k > M$ such that for all $n > k$ we have $g(n) > 2$ and $g(n)|n^{n-1}-1$. Now, since $n + g(n) - n | g(n+g(n)) - g(n)$, we deduce that $g(n)|g(n+g(n))$ for all n. In particular, for all $n > k$ we have $g(n)|g(n+g(n))|(n+g(n))^{n+g(n)-1}-1$ and $g(n)|n^{n-1}-1$. Of course, this implies that $g(n)|n^{n+g(n)-1}-1 = (n^{n-1}-1)n^{g(n)} + n^{g(n)} - 1$, that is $g(n)|n^{g(n)}-1$ for all $n > k$. Now, let us consider a prime number $p > k$ and let us look at the smallest prime divisor of $g(p+1) > 2$. We clearly have $q|g(p+1)|(p+1)^{g(p+1)}-1$ and $q|(p+1)^{q-1}-1$. Since $gcd(g(p+1), q-1) = 1$ (by minimality) and $gcd((p+1)^{g(p+1)}-1, (p+1)^{q-1}-1) = (p+1)^{gcd(g(p+1),q-1)}-1 = p$, it follows that we actually have $p = q$. This shows that $p|g(p+q)$ and thus

(again using the fundamental result) $p|g(1)$. Since this happens for any prime number $p > k$, we must have $g(1) = 0$. This contradiction shows that g is indeed constant.

Let $g(X) = c$. Thus, $c|2^{n(2^n-1)-1} - 1$ for all $n > M$. $(2^n > M)$. Since $gcd(2^a-1, 2^b-1) = 2^{gcd(a,b)}-1$, in order to show that $|c| = 1$, it suffices to exhibit $k < m < n$ such that $gcd(m(2^m-1), n(2^n-1)) = 1$. This is very simple to realize. Indeed, it suffices to take m a prime number greater than M, k and to choose n a prime number greater than $m(2^m - 1)$. A simple argument shows that $gcd(m(2^m - 1), n(2^n - 1)) = 1$ and so $|c| = 1$.

Finally, let us prove that $r \leq 2$. Supposing the contrary, we deduce that

$$(n-1)^3|n^{n-1} - 1 \Leftrightarrow (n-1)^1|n^{n-2} + n^{n-3} + \cdots + n + 1$$

for all sufficiently large n and since

$$n^{n-2} + n^{n-3} + \cdots + n + 1 =$$

$$= n - 1 + (n-1)[n^{n-3} + 2n^{n-4} + \cdots + (n-3)n + (n-2)],$$

we obtain that $n - 1|n^{n-3} + 2n^{n-4} + \cdots + (n-3)n + (n-2) + 1$ for all sufficiently large n, which is clearly impossible, since

$$n^{n-3} + 2n^{n-4} + \cdots + (n-3)n + (n-2) + 1 \equiv 1 + 2 + \cdots + (n-2) + 1$$

$$\equiv \frac{(n-1)(n-2}{2} + 1 \pmod{n-1}.$$

Hence $r \leq 2$. Finally, the relation

$$n^{n-1} - 1 = (n-1)^2[n^{n-3} + 2m^{n-4} + \cdots + (n-3)n + (n-2) + 1]$$

shows that $(n-1)^2|n^{n-1} - 1$ for all $n > 1$ and allows to conclude that all solutions are the polynomials $\pm(X-1)^r$, with $r \in \{0, 1, 2\}$.

After reading the solution of the following problem, the reader will have the impression the problem is very simple. Actually, it is extremely

difficult. There are many possible approaches that fail and the time spent for solving such a problem can very well tend to infinity.

Example 5. Let $f \in Z[X]$ be a non constant polynomial and $k \geq 2$ a positive integer such that $\sqrt[k]{f(n)} \in Q$ for all positive integers n. Then there exists a polynomial $g \in Z[X]$ such that $f = g^k$.

Folklore

Solution. Let us assume the contrary and let us decompose $f = p_1^{k_1} \dots p_s^{k_s} g^k$ where $1 \leq k_i < k$ and p_i are different irreducible polynomials in $Q[X]$. Suppose that $s \geq 1$ (which is the same as denying the conclusion). Since p_1 is irreducible in $Q[X]$, it is relatively prime with $p_1 p_2 \dots p_s$ and thus (using Bezout's theorem and multiplication with integers) there exist some polynomials with integer coefficients Q, R and a positive integer c such that

$$Q(x)p_1(x) + R(x)p_1(x)p_2(x) \dots p_s(x) = c.$$

Now, using the result from example 1, we can take a prime number $q > |c|$ and a number n such that $q|p_1(n) \neq 0$. We shall have of course $q|p_1(n+q)$ (since $p_1(n+q) \equiv p_1(n) \pmod{q}$). The choice $q > |c|$ ensures that q does not divide $p_1(n)p_2(n) \dots p_s(n)$ and so $v_q(f(n)) = v_q(p_1(n)) + kv_q(g(n))$. But the hypothesis says that $k|v_q(f(n))$, so we must have $v_q(p_1(n)) > 2$. In exactly the same way we obtain $v_q(p_1(n+q)) \geq 2$. Yet, using the binomial formula, we can easily establish the congruency

$$p_1(n+q) \equiv p_1(n) + qp_1'(n) \pmod{q^2}.$$

Therefore, we must have $q|p_1(n)$, which contradicts $q > |c|$ and

$$Q(x)p_1(x) + R(x)p_1(x)p_2(x) \dots p_s(x) = c.$$

This contradiction shows that the hypothesis $s \geq 1$ was wrong and thus the result of the problem follows.

The next problem was given in the USA TST 2005 and uses a nice combination of arithmetic considerations and computations using complex numbers. There are many arithmetic properties of polynomials speculated in this problem, although the problem itself is not so difficult, if we find the good way to solve it, of course...

Example 6. Let us call a polynomial $f \in Z[X]$ special if for any positive integer $k > 1$, in the sequence $f(1), f(2), f(3), \ldots$ one can find numbers which are relatively prime with k. Prove that for any $n > 1$, at least 71% of all monic polynomials of degree n, with coefficient in the set $\{1, 2, \ldots, n!\}$ are special.

Titu Andreescu, Gabriel Dospinescu, USA TST 2005

Solution. Of course, before counting such polynomials, it would be better to find an easier characterization for them.

Let $p_1, p_2, \ldots, p_r$ all prime numbers at most equal to n and let us consider the sets $A_i = \{f \in M |\ p_i | f(m),\ \forall\ m \in \mathbb{N}^*\}$, where M is the set of monic polynomials of degree n, with coefficient in the set $\{1, 2, \ldots, n!\}$. We shall prove that the set T of special polynomials is exactly $M \setminus \bigcup_{i=1}^{r} A_i$. Obviously, we have $T \subset M \setminus \bigcup_{i \leq r} A_i$. The converse, however is not that easy. Let us suppose that $f \in Z[X]$ belongs to $M \setminus \bigcup_{i=1}^{r} A_i$ and let p be a prime number greater than n. Since f is monic, Lagrange's theorem ensures that we can find m such that p is not a divisor of $f(m)$. It follows then that for any prime number q at least one of the numbers $f(1), f(2), f(3), \ldots$ is not a multiple of q. Let now $k > 1$ and $q_1, q_2, \ldots, q_s$ its prime divisors. Then we know we can find $u_1, \ldots, u_s$ such that q_i does not divide $f(u_i)$. Using the Chinese remainder theorem, we can find a positive integer x such that $x \equiv u_i \pmod{q_i}$. Then $f(x) \equiv f(u_i) \pmod{q_i}$ and thus q_i does not divide $f(x)$, thus $gcd(f(x), k) = 1$. The equality of the two sets is thus proved.

Using a brutal estimation, we obtain

$$|T| = |M| - \left|\bigcup_{i=1}^{r} A_i\right| \geq |M| - \sum_{i=1}^{r} |A_i|.$$

Let's compute now $|A_i|$. Actually, we will show that $\frac{(n!)^n}{p_i^{p_i}}$. Let f a monic polynomial in A_i,

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Then for any $m > 1$ we have

$$0 \equiv f(m) \equiv a_0 + (a_1 + a_p + a_{2p-1} + a_{3p-2} + \dots)m$$

$$+(a_2+a_{p+1}+a_{2p}+\dots)m^2+\cdots+(a_{p-1}+a_{2p-2}+a_{3p-3}+\dots)m^{p-1} \pmod{p},$$

where, for simplicity, we put $p = p_i$. Using Lagrange's theorem it follows that $p|a_0, p|a_1 + a_p + a_{2p-1} + \dots, \dots, p|a_{p-1} + a_{2p-2} + \dots$ We are going to use this later, but we still need a small observation. Let us count the number of s-tuples $(x_1, x_2, \dots, x_s) \in \{1, 2, \dots, n!\}^s$ such that $x_1 + x_2 + \cdots + x_s \equiv u \pmod{p}$, where u is fixed. Let

$$\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}.$$

Let us observe that

$$0 = (\varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n!})^s$$

$$= \sum_{k=0}^{p-1} \varepsilon^k |\{(x_1, x_2, \dots, x_s) \in \{1, 2, \dots, n!\}^s |\ x_1 + \cdots + x_s \equiv k \pmod{p}\}|.$$

A simple argument related to the irreducibility of the polynomial $1 + X + X^2 + \cdots + X^{p-1}$ shows that all cardinals that appear in the above sum are equal and that their sum is $(n!)^s$, thus each cardinal equals $\frac{(n!)^s}{p}$.

We are now ready to finish the proof. Assume that among the numbers $a_1, a_p, a_{2p-1}, \dots$ there are exactly v_1 numbers that among

$a_{p-1}, a_{2p-2}, \dots$ there are v_{p-1} numbers. Using the above observations, it follows that we have

$$|A_i| = \frac{n!}{p} \cdot \frac{(n!)^{v_1}}{p} \dots \frac{(n!)^{v_{p-1}}}{p} = \frac{(n!)^n}{p^p}.$$

Hence, we obtain

$$|T| \geq (n!)^n - \sum_{p\, prime} \frac{(n!)^n}{p^p}.$$

But

$$\frac{1}{5^5} + \frac{1}{7^7} + \dots < \frac{1}{5^5}\left(1 + \frac{1}{5} + \frac{1}{5^2} + \dots\right) < \frac{1}{1000}$$

and so the percent of special polynomials is at least

$$100\left(1 - \frac{1}{4} - \frac{1}{27} - \frac{1}{1000}\right) = 75 - \frac{100}{27} - \frac{1}{10} > 71.$$

The solution of the problem ends here.

Example 7. Suppose that the non constant polynomial f with integer coefficients has no double roots. Then for any positive integer r there exists n such that $f(n)$ has at least r distinct prime divisors, all of them appearing with exponent 1 in the decomposition of $f(n)$ in prime factors.

Iran Olympiad

Solution. Already for $r = 1$ the problem is in no way obvious, so let's not try to attack it directly and concentrate at first on the case $r = 1$. Suppose the contrary, that is for all n, all prime divisors of $f(n)$ appear with exponent at least 2. Since f has no double root, we deduce that $gcd(f, f') = 1$ in $C[X]$ and thus also in $Q[X]$ (because of the division algorithm and Euclid's algorithm). Using Bezout's theorem in $Q[X]$, we deduce that we can find integer polynomials P, Q such that $P(n)f(n) + Q(n)f'(n) = c$ for a certain positive integer c. Using the result stated in the first example, we can choose $q > c$ a prime divisor

of a certain $f(n)$. The hypothesis made ensures that $q^2|f(n)$. But then we also have $q|f(n+q)$ and so $q^2|f(n+q)$. Using Newton's binomial formula, we deduce immediately that $f(n+q) \equiv f(n)+qf'(n) \pmod{q^2}$. We finally deduce that $q|p'(n)$ and so $q|c$, impossible since our choice was $q > c$. Thus the case $r = 1$ was proved.

Let us try to prove the property by induction and suppose it is true for r. Of course, the existence of P, Q such that $P(n)f(n)+Q(n)f'(n) = c$ for a certain positive integer c did not depend on r, so we keep the above notations. By inductive hypothesis, there is n such that at least r prime divisors of $f(n)$ appear with exponent 1. Let these prime factors be $p_1, p_2, \ldots, p_r$. But it is obvious that $n + kp_1^2p_2^2 \ldots p_r^2$ has the same property: all prime divisors $p_1, p_2, \ldots, p_r$ have exponent 1 in the decomposition of $f(n+kp_1^2p_2^2 \ldots p_r^2)$. Since at most a finite number among them can be roots of f, we may very well suppose from the beginning that n is not a root of f. Consider now the polynomial $g(X) = f(n + (p_1 \ldots p_r)^2X)$, which is obviously non constant. Thus, using again the result in example 1, we can find $q > \max\{|c|, p_1, \ldots, p_r, |p(n)|\}$ a prime number and a number u such that $q|g(u)$. If $v_q(g(u)) = 1$, victory is ours, since a trivial verification shows that $q, p_1, \ldots, p_r$ are different prime numbers whose exponents in $f(n + (p_1 \ldots p_r)^2u)$ are all 1. The difficult case is when $v_q(g(u)) \geq 2$. In this case, we shall consider the number $N = n+u(p_1 \ldots p_r)^2+uq(p_1 \ldots p_r)^2$. Let us prove that in the decomposition of $f(N)$, all prime numbers $q, p_1, \ldots, p_r$ appear with exponent 1. For any p_i, this is obvious since $f(N) \equiv f(n) \pmod{(p_1 \ldots p_r)^2}$. Using once again binomial formula, we easily obtain that $f(N) \equiv f(n + (p_1 \ldots p_r)^2u) + uq(p_1 \ldots p_r)^2f'(N) \pmod{q^2}$. Now, if $v_q(f(n)) \geq 2$, then since $v_q(f(n + (p_1 \ldots p_r)^2u)) = v_q(g(u)) \geq 2$, we have $q|u(p_1 \ldots p_r)^2f'(N)$. Remember that the choice was $q > \max\{|c|, p_1, \ldots, p_r, |p(n)|\}$ so necessarily $q|u$ (if $q|f'(N) \Rightarrow q|(f(N), f'(N))|c \Rightarrow q \leq |c|$, contradiction). But since $q|g(u)$,

we must have $q|g(0) = f(n)$. But hopefully, we ensured that n is not a roof of our polynomial and also that $q > \max\{|c|, p_1, \ldots, p_r, |p(n)|\}$ so that the last divisibility relation cannot hold. This allows to finish the induction step and to solve the problem.

Example 8. Find all non constant polynomials f with integer coefficients and with the following property: for any relatively prime positive integers a, b, the sequence $(f(an+b))_{n\geq 1}$ contains an infinite number of terms, any two of which are relatively prime.

Gabriel Dospinescu

Solution. We will prove that the only polynomials with the specified property are those of the form X^n, $-X^n$ with n a positive integer. Because changing f with its opposite does not modify the property of the polynomial, we can suppose that the leading coefficient of f is positive. Thus, there exists a constant M such that for any $n > M$ we have $f(n) > 2$. From now on, we consider only $n > M$. Let us prove that we have $gcd(f(n), n) \neq 1$ for any such n. Suppose that there is $n > M$ such that $gcd(f(n), n) = 1$. Consequently, the sequence $(f(n+kf(n))_{n\geq 1}$ will contain at least two relatively prime numbers. Let them be s, r. Since $f(n)|kf(n) = kf(n) + n - n|f(kf(n) + n) - f(n)$, we have $f(n)|f(n + kf(n))$ for any positive integer k. Hence ,we obtain that s, r are multiples of $f(n) > 2$, impossible. We have shown that $gcd(f(n), n) \neq 1$ for any $n > M$. Thus ,for any prime $p > M$ we have $p|f(p)$ and so $p|f(0)$. Since any integer different from zero has a finite number of divisors, we conclude that $f(0) = 0$. Thus, there is a polynomial q with integer coefficients such that $f(X) = Xq(X)$. It is obvious that q has positive leading coefficient and the same property as f. Repeating the above argument, we infer that if q is non-constant, then $q(0) = 0$ and $q(X) = Xh(X)$. Since f is not constant, the above argument cannot be repeated infinitely many times and thus one of the

polynomials g, h must be constant. Consequently, there are positive integers n, k such that $f(X) = kX^n$. But since the sequence $(f(2n+3))_{n\geq 1}$ contains at least two relatively prime integers, we must have $k = 1$. We have obtained that f must have the form X^n. But since f is a solution if and only if $-f$ is a solution, we infer that any solution of the problem is a polynomial of the form X^n, $-X^n$.

Now let us prove that the polynomials of the form X^n, $-X^n$ are solutions. It is enough to prove for X^n and even for X. But this follows trivially from Dirichlet's theorem. Let us observe that there is another, more elementary approach. Let us suppose that $x_1, x_2, \ldots, x_p$ are terms of the sequence, any two of which are relatively prime. We prove that we can add another term x_{p+1} so that $x_1, x_2, \ldots, x_{p+1}$ has the same property. It is clear that $x_1, x_2, \ldots, x_p$ are relatively prime with a, so we can apply the Chinese remainder theorem to find x_{p+1} greater than $x_1, x_2, \ldots, x_p$, such that $x_{p+1} \equiv (1-b)a_i^{-1} \pmod{x_i}$, $i \in \{1, 2, \ldots, p\}$, where a_i^{-1} is a's inverse in $Z_{x_i}^*$. Then $gcd(x_{p+1}, x_i) = 1$ for $i \in \{1, 2, \ldots, p\}$ and thus we can add x_{p+1}.

Here is an absolute classic, that appears in at least one Olympiad around the world each year. Very easy, it uses only the fundamental result.

Example. Suppose that

Fie n natural nenul. Care este gradul minim al unui polinom monic cu coeficienti intregi f astfel incat $n|f(k)$ pentru orice k natural?

Proposed problems

1. Let $(a_n)_{n\geq 1}$ be an increasing sequence of positive integers such that for a certain polynomial $f \in Z[X]$ we have $a_n \leq f(n)$ for all n. Suppose also that $m - n|a_m - a_n$ for all distinct positive integers m, n.

Prove that there exists a polynomial $g \in Z[X]$ such that $a_n = g(n)$ for all n.

USAMO 1995

2. We call the sequence of positive integers $(a_n)_{n\geq 1}$ relatively prime if $gcd(a_m, a_n) = 1$ for any different positive integers m, n. Find all integer polynomials $f \in Z[X]$ such that for any positive integer c, the sequence $(f^{[n]}(c))_{n\geq 1}$ is relatively prime. Here $f^{[n]}$ is the composition of f with itself n times.

Leo Mosser

3. Are there polynomials p, q, r with positive integer coefficients such that

$$p(x) + (x^2 - 3x + 2)q(x) \text{ and } q(x) = \left(\frac{x^2}{20} - \frac{x}{15} + \frac{1}{12}\right) r(x)?$$

Vietnam Olympiad

4. Given is a finite family of polynomials with integer coefficients. Prove that for infinitely many numbers n, if we evaluate any member of the family in n, we obtain only composite numbers.

Folklore

5. Find all polynomials with integer coefficients such that $f(n)|2^n - 1$ for any positive integer n.

Poland Olympiad

6. Suppose that $f \in Z[X]$ is a non constant polynomial. Also, suppose that for some positive integers r, k, the following property is satisfied: for any positive integer n, at most r prime factors of $f(n)$ have appear with exponent at most equal to k. Does it follow that any root of this polynomial appears with multiplicity at least equal to $k + 1$?

7. Is it true that any polynomial $f \in Z[X]$ that has a root modulo n for any positive integer n must necessarily have a rational root?

8. Let $f, g \in Z[X]$ some non zero polynomials. Let us consider the set $D_{f,g} = \{gcd(f(n), g(n))|\ n \in \mathbb{N}\}$. Prove that the two polynomials are relatively prime in $Q[X]$ if and only if $D_{f,g}$.

M. Andronache, Gazeta Matematica 1985

9. Prove that there are no polynomials $f \in Z[X]$ with the property: there exists $n > 3$ and integers $x_1, \ldots, x_n$ such that $f(x_i) = x_{i-1}, i = \overline{1,n}$ (indices are taken mod n).

10. Let $f \in Z[X]$ a polynomial of degree n at least 2, with integer coefficients. Prove that the polynomial $f(f(X))-X$ has at most n integer roots.

Gh. Eckstein, Romanian TST

11. Find all trinomials $f \in Z[X]$ with the property that for any relatively prime integers m, n, the numbers $f(M), f(n)$ are also relatively prime.

Sankt Petersburg Olympiad

12. For the die hard: find all polynomials with the above property.

13. Let $f \in Z[X]$ be a non constant polynomial. Show that the sequence $f(3^n) \pmod b$ is not bounded.

14. Is there a second degree polynomial $f \in Z[X]$ such that for any positive integer n all prime factors of $f(n)$ are of the form $4k + 3$?

AMM

15. Prove that for any n there exists a polynomial $f \in Z[X]$ such that all numbers $f(1) < f(2) < \cdots < f(n)$ are

a) prime numbers b) powers of 2.

Folklore

16. Find all integers $n > 1$ for which there exists a polynomial $f \in Z[X]$ such that for any integer k we have $f(k) \equiv 0, 1 \pmod n$ and both these congruences have solutions.

17. Let p be a prime number. Find the maximal degree of a polynomial $f \in Z[X]$ having coefficients in the set $\{0, 1, \ldots, p-1\}$, knowing that its degree is at most p and that if p divides $f(m) - f(n)$ then it also divides $m - n$.

18. Use example 1 and properties of the cyclotomic polynomials

$$\phi_n(X) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (X - e^{\frac{2i\pi k}{n}})$$

to prove that there are infinitely many prime numbers of the form $1 + kn$ for any given $n \geq 2$. You may be interested to characterize those numbers m, n for which $p | \phi_m(n)$, but p does not divide any other number of the form $\phi_d(n)$, where d is a divisor of m different from m

Classical result

LAGRANGE INTERPOLATION

Almost everyone knows the Chinese Remainder Theorem, which is a remarkable tool in number theory. But does everyone know the analogous form for polynomials? Stated like this, this question may seem impossible to answer. Then, let us make it easier and also reformulate it: is it true that given some pair wise distinct real numbers $x_0, x_1, x_2, \ldots, x_n$ and some arbitrary real numbers $a_0, a_1, a_2, \ldots, a_n$, we can find a polynomial f with real coefficients such that $f(x_i) = a_i$ for $i \in \{0, 1, \ldots, n\}$? The answer turns out to be positive and a possible solution to this question is based on Lagrange's interpolation formula. It says that an example of such polynomial is

$$f(x) = \sum_{i=0}^{n} a_i \prod_{0 \leq j \neq i \leq n} \frac{x - x_j}{x_i - x_j} \tag{1}$$

Indeed, it is immediate to see that $f(x_i) = a_i$ for $i \in \{0, 1, \ldots, n\}$. Also, from the above expression we can see that this polynomial has degree less than or equal to n. Is this the only polynomial with this supplementary property? Yes, and the proof is not difficult at all. Just suppose we have another polynomial g of degree smaller than or equal than n and such that $g(x_i) = a_i$ for $i \in \{0, 1, \ldots, n\}$. Then the polynomial $g - f$ also has degree smaller than or equal to n and vanishes at $0, 1, \ldots, n$. Thus, it must be null and the uniqueness is proved.

What is Lagrange's interpolation theorem good for? We will see in the following problems that it helps us to find immediately the value of a polynomial in a certain point if we know the values in some given points. And the reader has already noticed that this follows directly from the formula (1), which shows that if we know the value in $1 + \deg f$ points, then we can find easily the value in any other point without solving a complicated linear system. Also, we will see that it helps in establishing

some inequalities and bounds for certain special polynomials and will even help us in finding and proving some beautiful identities.

Now, let us begin the journey trough some nice examples of problems where this idea can be used. As promised, we will see first how we can compute rapidly the value in a certain point for some polynomials. This was one of the favorite's problems in the old Olympiads, as the following examples will show. The first example is just an immediate application of formula (1) and became a classical problem.

Example 1.

Let f be a polynomial of degree n such that

$$f(0) = 0,\ f(1) = \frac{1}{2},\ f(2) = \frac{2}{3}, \ldots, f(n) = \frac{n}{n+1}.$$

Find $f(n+1)$.

USAMO 1975, Great Britain 1989

Solution. A first direct approach would be to write

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

and to determine $a_0, a_1, \ldots, a_n$ from the linear system

$$f(0) = 0,\ f(1) = \frac{1}{2},\ f(2) = \frac{2}{3}, \ldots, f(n) = \frac{n}{n+1}.$$

But this is terrible, since the determinants that must be computed are really complicated. This is surely a dead end. But for someone who knows Lagrange's Interpolation Theorem, the problem is straightforward. Indeed, we have

$$f(x) = \sum_{i=0}^{n} \frac{i}{i+1} \prod_{j \neq i} \frac{x-j}{i-j},$$

so that

$$f(n+1) = \sum_{i=0}^{n} \frac{i}{i+1} \prod_{n \leq i} \frac{n+1-j}{i-j}.$$

Now, how do we compute this? The reader might say: but we have already found the value of $f(n+1)$! Well, it is tacit that the answer should be expressed in the closest possible form. But, after all, computing the above sum is not so difficult. Indeed, we can see that

$$\prod_{j\neq i}\frac{n+1-j}{i-j}=\frac{(n+1)!}{(n+1-i)\cdot i!\cdot(n-i)!}(-1)^{n-i}$$

just by writing

$$\prod_{j\neq i}\frac{n+1-j}{i-j}=\frac{(n+1)n\ldots(n+1-(i-1))(n+1-(i+1))\ldots 1}{i(i-1)\ldots 1\cdot(-1)\ldots(-(n-i))}.$$

According to these small observations, we can write

$$\begin{aligned}f(n+1)&=\sum_{i=0}^{n}\frac{i}{i+1}\cdot\frac{(n+1)!}{(n+1-i)\cdot i!\cdot(n-i)!}(-1)^{n-i}\\&=\sum_{i=1}^{n}\frac{(n+1)!}{(n+1-i)!\cdot(i-1)!}(-1)^{n-i}\\&=(n+1)\sum_{i=1}^{n}\binom{n}{i-1}(-1)^{n-i}=(n+1)\sum_{i=0}^{n-1}\binom{n}{i}(-1)^{n+1-i}.\end{aligned}$$

And we have arrived at a familiar formula: the binomial theorem. According to this,

$$\sum_{i=0}^{n-1}\binom{n}{i}(-1)^{n+1-i}=-\left(\sum_{i=0}^{n}\binom{n}{i}(-1)^{n-i}-1\right)=1.$$

This shows that $f(n+1)=n+1$.

The first example was straightforward because we didn't find any difficulties after finding the idea. It's not the case with the following problem.

Example 2. Let $F_1=F_2=1$, $F_{n+2}=F_n+F_{n+1}$ and let f be a polynomial of degree 990 such that $f(k)=F_k$ for $k\in\{992,\ldots,1982\}$. Show that $f(1983)=F_{1983}-1$.

Titu Andreescu, IMO 1983 Shortlist

Solution. So, we have $f(k+992) = F_{k+992}$ for $k = \overline{0,990}$ and we need to prove that $f(992+991) = F_{1983} - 1$. This simple observation shows that we don't have to bother too much with $k+992$, since we could work as well with the polynomial $g(x) = f(x+992)$, which also has degree 990. Now, the problem becomes: if $g(k) = F_{k+992}$, for $k = \overline{0,990}$, then $g(991) = F_{1983} - 1$. But we know how to compute $g(991)$. Indeed, looking again at the previous problem, we find that

$$g(991) = \sum_{k=0}^{990} g(k)\binom{991}{k}(-1)^k = \sum_{k=0}^{990}\binom{991}{k}F_{k+992}(-1)^k$$

which shows that we need to prove the identity

$$\sum_{k=0}^{990}\binom{991}{k}F_{k+992}(-1)^k = F_{1983} - 1.$$

This isn't so easy, but with a little bit of help it can be done. The device is: never complicate things more than necessary! Indeed, we could try to establish a more general identity that could be proved by induction. But why, since it can be done immediately with the formula for F_n. Indeed, we know that

$$F_n = \frac{a^n - b^n}{\sqrt{5}},$$

where $a = \dfrac{\sqrt{5}+1}{2}$ and $b = \dfrac{1-\sqrt{5}}{2}$. Having this in mind, we can of course try a direct approach:

$$\sum_{k=0}^{990}\binom{991}{k}F_{k+992}(-1)^k$$

$$= \frac{1}{\sqrt{5}}\left[\sum_{k=0}^{990}\binom{991}{k}a^{k+992}(-1)^k - \sum_{k=0}^{990}\binom{991}{k}b^{k+992}(-1)^k\right].$$

But using the binomial theorem, the above sums vanish:

$$\sum_{k=0}^{990}\binom{991}{k}a^{k+992}(-1)^k = a^{992}\sum_{k=0}^{990}\binom{991}{k}(-a)^k = a^{992}[(1-a)^{991} + a^{991}].$$

Since $a^2 = a + 1$, we have

$$a^{992}[(1-a)^{991} + a^{991}] = a(a-a^2)^{991} + a^{1983} = -a + a^{1983}.$$

Since in all this argument we have used only the fact that $a^2 = a+1$ and since b also verifies this relation, we find that

$$\sum_{k=0}^{990} \binom{991}{k} F_{k+992}(-1)^k = \frac{1}{\sqrt{5}}(a^{1983} - b^{1983} - a + b)$$

$$= \frac{a^{1983} - b^{1983}}{\sqrt{5}} - \frac{a-b}{\sqrt{5}} = F_{1983} - 1.$$

And this is how with the help of a precious formula and with some smart computations we could solve this problem and also find a nice property of the Fibonacci numbers.

The following example is a very nice problem proposed for IMO 1997. Here, the following steps after using Lagrange's Interpolation formula are even better hidden in some congruencies. It is the typical example of a good Olympiad problem: no matter how much the contestant knows in that field, it causes great difficulties in solving.

Example 3. Let f be a polynomial with integer coefficients and let p be a prime such that $f(0) = 0$, $f(1) = 1$ and $f(k) = 0, 1 \pmod{p}$ for all positive integer k. Show that $\deg f$ is at least $p - 1$.

IMO Shortlist 1997

Solution. As usual, such a problem should be solved indirectly, arguing by contradiction. So, let us suppose that $\deg f \leq p - 2$. Then, using the Interpolation formula, we find that

$$f(x) = \sum_{k=0}^{p-1} f(k) \prod_{j \neq k} \frac{x-j}{k-j}.$$

Now, since $\deg f \leq p-2$, the coefficient of x^{p-1} in the right-hand side of the identity must be zero. Consequently, we have

$$\sum_{k=0}^{p-1} \frac{(-1)^{p-k-1}}{k!(p-1-k)!} f(k) = 0.$$

From here we have one more step. Indeed, let us write the above relation in the form

$$\sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(k) = 0$$

and let us take this equality modulo p. Since

$$k! \binom{p-1}{k} = (p-k)(p-k+1)\dots(p-1) \equiv (-1)^k k! \pmod{p}$$

we find that

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

and so

$$\sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(k) \equiv \sum_{k=0}^{p-1} f(k) \pmod{p}.$$

Thus,

$$\sum_{k=0}^{p-1} f(k) \equiv 0 \pmod{p},$$

which is impossible, since $f(k) \equiv 0, 1 \pmod{p}$ for all k and not all of the numbers $f(k)$ have the same remainder modulo p (for example, $f(0)$ and $f(1)$). This contradiction shows that our assumption was wrong and the conclusion follows.

It's time now for some other nice identities, where polynomials do not appear at first sight. We will see how some terrible identities are simple consequences of the Lagrange Interpolation formula.

Example 4. Let $a_1, a_2, \ldots, a_n$ be pairwise distinct positive integers. Prove that for any positive integer k the number $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod_{j\neq i}(a_i - a_j)}$ is an integer.

Great Britain

Solution. Just by looking at the expression, we recognize the Lagrange Interpolation formula for the polynomial $f(x) = x^k$. But we may have some problems when the degree of this polynomial is greater than or equal to n. But this can be solved by working with the remainder of f modulo $g(x) = (x - a_1)(x - a_2)\ldots(x - a_n)$. So, let us proceed, by writing $f(x) = g(x)h(x) + r(x)$, where r is a polynomial of degree at most $n - 1$. This time we don't have to worry, since the formula works and we obtain

$$r(x) = \sum_{i=1}^{n} r(a_i) \prod_{j\neq i} \frac{x - a_j}{a_i - a_j}.$$

Now, we need three observations. The first one is $r(a_i) = a_i^k$, the second one is that the polynomial r has integer coefficients and the third one is that $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod_{j\neq i}(a_i - a_j)}$ is just the coefficient of x^{n-1} in the polynomial $\displaystyle\sum_{i=1}^{n} r(a_i) \prod_{j\neq i} \frac{x - a_j}{a_i - a_j}$. All these observations are immediate. Combining them, we find that $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod_{j\neq i}(a_i - a_j)}$ is the coefficient of x^{n-1} in r, which is an integer. Thus, not only that we have solved the problem, but we also found a rapid way to compute the sums of the form $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod_{j\neq i}(a_i - a_j)}$.

The following two problems we are going to discuss refer to combinatorial sums. If the first one is relatively easy to prove using a combinatorial argument (it is a very good exercise for the reader to find this argument), the second problem is much more difficult. But we will see that both are immediate consequences of the Interpolation Formula.

Example 5. Let $f(x) = \sum_{k=0}^{n} a_k x^{n-k}$. Prove that for any non-zero real number h and any real number A we have

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(A+kh) = a_0 \cdot h^n \cdot n!.$$

Alexandru Lupas

Solution. Since this polynomial has degree at most n, we have no problems in applying the Interpolation formula

$$f(x) = \sum_{k=0}^{n} f(A_k h) \prod_{j \neq k} \frac{x - A - jh}{(k-j)h}.$$

Now, let us identify the leading coefficients in both polynomials that appear in the equality. We find that

$$a_0 = \sum_{k=0}^{n} f(A+kh) \frac{1}{\prod_{j \neq k} [(k-j)h]} = \frac{1}{n! h^n} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(A+kh),$$

which is exactly what we had to prove. Simple and elegant! Notice that the above problem implies the well-known combinatorial identities

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} k^p = 0$$

for all $p \in \{0, 1, 2, \ldots, n-1\}$ and $\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n = n!$.

As we promised, we will discuss a much more difficult problem. The reader might say after reading the solution: but this is quite natural! Yes, it is natural for someone who knows very well the Lagrange Interpolation

formula and especially for someone who thinks that using it could lead to a solution. Unfortunately, this isn't always so easy.

Example 6. Prove the identity

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^{n+1}=\frac{n(n+1)!}{2}.$$

Solution. We take the polynomial $f(x)=x^n$ (why don't we take the polynomial $f(x)=x^{n+1}$? Simply because $(-1)^{n-k}\binom{n}{k}$ appears when writing the formula for a polynomial of degree at most n) and we write the Interpolation Formula

$$x^n=\sum_{k=0}^{n}k^n\frac{x(x-1)\dots(x-k-1)(x-k+1)\dots(x-n)}{(n-k)!k!}(-1)^{n-k}$$

Now, we identify the coefficient of x^{n-1} in both terms. We find that

$$0=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^n(1+2+\dots+n-k).$$

And now the problem is solved, since we found that

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^{n+1}=\frac{n(n+1)}{2}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^n$$

and we also know that

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^n=n!$$

from the previous problem.

Were Lagrange interpolation formula good only to establish identities and to compute values of polynomials, it wouldn't have been such a great discovery. Of course it is not the case, it plays a fundamental role in analysis. Yet, we are not going to enter this field and we prefer to concentrate on another elementary aspect of this formula and see how it can help us establish some remarkable inequalities. And some of them will be really tough.

We begin with a really difficult inequality, in which the interpolation formula is really well hidden. Yet, the denominators give sometimes precious indications...

Example 7. Prove that for any real numbers $x_1, x_2, \ldots, x_n \in [-1, 1]$ the following inequality is true:

$$\sum_{i=1}^{n} \frac{1}{\prod_{j \neq i} |x_j - x_i|} \geq 2^{n-2}.$$

Iran Olympiad

Solution. The presence of $\prod_{j \neq i} |x_j - x_i|$ is the only hint to this problem. But even if we know it, how do we choose the polynomial? The answer is simple: we will choose it to be arbitrary and only in the end we will decide which is one is optimal. So, let us proceed by taking $f(x) = \sum_{k=0}^{n-1} a_k x^k$ an arbitrary polynomial of degree $n-1$. Then we have

$$f(x) = \sum_{k=1}^{n} f(x_k) \prod_{j \neq k} \frac{x - x_j}{x_k - x_j}.$$

Combining this with the triangular inequality , we arrive at a new inequality

$$|f(x)| \leq \sum_{k=1}^{n} |f(x_k)| \prod_{j \neq k} \left| \frac{x - x_j}{x_k - x_j} \right|.$$

Only now comes the beautiful idea, which is in fact the main step. From the above inequality we find that

$$\left| \frac{f(x)}{x^{n-1}} \right| \leq \sum_{k=1}^{n} \frac{|f(x_k)|}{\prod_{j \neq k} |x_k - x_j|} \left| \prod_{j \neq k} \left(1 - \frac{x_j}{x}\right) \right|$$

and since this is true for all non-zero real numbers x, we may take the limit when $x \to \infty$ and the result is pretty nice

$$|a_{n-1}| \leq \sum_{k=1}^{n} \frac{|f(x_k)|}{\prod_{j \neq k} |x_k - x_j|}.$$

This is the right moment to decide what polynomial to take. We need a polynomial f such that $|f(x)| \leq 1$ for all $x \in [-1, 1]$ and such that the leading coefficient is 2^{n-2}. This time our mathematical culture will decide. And it says that Chebyshev polynomials are the best, since they are the polynomials with the minimum deviation on $[-1, 1]$ (the reader will wait just a few seconds and he will see a beautiful proof of this remarkable result using Lagrange's interpolation theorem). So, we take the polynomial defined by $f(\cos x) = \cos(n-1)x$. It is easy to see that such a polynomial exists, has degree $n-1$ and leading coefficient 2^{n-2}, so this choice solves our problem.

Note also that the inequality $|a_{n-1}| \leq \sum_{k=1}^{n} \frac{|f(x_k)|}{\prod_{j \neq k} |x_k - x_j|}$ can be proved by identifying the leading coefficients in the identity

$$f(x) = \sum_{k=1}^{n} f(x_k) \prod_{j \neq k} \frac{x - x_j}{x_k - x_j}$$

and then using the triangular inequality.

The following example is a fine concoct of ideas. The problem is not simple at all, since many possible approaches fail. Yet, in the framework of the previous problems and with the experience of Lagrange's interpolation formula, it is not so hard after all.

Example 8. Let $f \in R[X]$ be a polynomial of degree n with leading coefficient 1 and let $x_0 < x_1 < x_2 < \cdots < x_n$ be some integers. Prove

that there exists $k \in \{1, 2, \ldots, n\}$ such that

$$|f(x_k)| \geq \frac{n!}{2^n}.$$

Crux Matematicorum

Solution. Naturally (but would this be naturally without having discussed so many related problems before?), we start with the identity

$$f(x) = \sum_{k=0}^{n} f(x_k) \prod_{j \neq k} \frac{x - x_j}{x_k - x_j}.$$

Now, repeating the argument in the previous problem and using the fact that the leading coefficient is 1, we find that

$$\sum_{k=0}^{n} \frac{|f(x_k)|}{\prod_{j \neq k} |x_k - x_j|} \geq 1.$$

It is time to use that we are dealing with integers. This will allow us to find a good inferior bound for $\prod_{j \neq k} |x_k - x_j| \geq 1$. This is easy, since

$$\prod_{j \neq k} |x_k - x_j| = (x_k - x_0)(x_k - x_1) \ldots (x_k - x_{k-1})(x_{k+1} - x_k) \ldots (x_n - x_k)$$

$$\geq k(k-1)(k-2) \ldots 1 \cdot 1 \cdot 2 \ldots (n-k) = k!(n-k)!.$$

And yes, we are done, since using these inequalities, we deduce that

$$\sum_{k=0}^{n} \frac{|f(x_k)|}{k!(n-k)!|} \geq 1.$$

Now, since

$$\sum_{k=0}^{n} \frac{1}{k!(n-k)!} = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} = \frac{2^n}{n!},$$

it follows trivially that

$$|f(x_k)| \geq \frac{n!}{2^n}.$$

We shall discuss one more problem before entering in a more detailed study of Chebyshev polynomials and their properties, a problem given

in the Romanian mathematical Olympiad and which is a very nice application of Lagrange's interpolation formula. It is useless to say that it follows trivially using a little bit of integration theory and Fourier series.

Example 9. Prove that for any polynomial f of degree n and with leading coefficient 1 there exists a point z such that

$$|z| = 1 \text{ and } |f(z)| \geq 1.$$

Marius Cavachi, Romanian Olympiad

Solution. Of course, the idea is always the same, but this time it is necessary to find the good points in which we should write the interpolation formula. As usual, we shall be blind and we shall try to find these points. Till then, let us call them simply $x_0, x_1, x_2, \ldots, x_n$ and write

$$\sum_{k=0}^{n} \frac{|f(x_k)|}{\prod_{j\neq k} |x_k - x_j|} \geq 1.$$

This inequality was already proved in the two problems above. Now, consider the polynomial

$$g(x) = \prod_{i=0}^{n} (x - x_i).$$

We have then

$$|g'(x_i)| = \left| \prod_{j\neq i} (x_i - x_j) \right|.$$

Now, of course we would like, if possible, to have $|x_i| = 1$ and also $\sum_{k=0}^{n} \frac{1}{|g'(x_k)|} \leq 1$. In this case it would follow from $\sum_{k=0}^{n} \frac{|f(x_k)|}{\prod_{j\neq k} |x_k - x_j|} \geq 1$ that at least one of the numbers $|f(x_k)|$ is at least equal to 1 and the problem would be solved. Thus, we should find a monic polynomial g of degree $n+1$ with all roots of modulus 1 and such that $\sum_{k=0}^{n} \frac{1}{|g'(x_k)|} \leq 1$.

This is trivial: it suffices of course to consider $g(x) = x^{n+1} - 1$. The conclusion follows.

We have an explanation to give: we said the problem follows trivially with a little bit of integration theory tools. Indeed, if we write $f(x) = \sum_{k=0}^{n} a_k x^k$ then one can check with a trivial computation that

$$a_k = \frac{1}{2\pi} \int_0^{2\pi} f(e^{it}) e^{-ikt} dt$$

and from here the conclusion follows since we will have

$$2\pi = \left| \int_0^{2\pi} f(e^{it}) e^{-int} dt \right| \leq \int_0^{2\pi} |f(e^{it}| dt \leq 2\pi \max_{|z|=1} |f(z)|.$$

Of course, knowing already this in 10-th grade (the problem was given to students in 10-th grade) is not something common...

The next problems will be based on a very nice identity that will allow us to prove some classical results about norms of polynomials, to find the polynomials having minimal deviation on $[-1, 1]$ and also to establish some new inequalities. In order to do all this, we need two quite technical lemmas, which is not difficult to establish, but very useful.

Lemma 1. *If we put* $t_k = \cos \frac{k\pi}{n}$, $0 \leq k \leq n$, *then*

$$f(x) = \prod_{k=0}^{n} (x - t_k) = \frac{\sqrt{x^2 - 1}}{2^n} [(x + \sqrt{x^2 - 1})^n - (x - \sqrt{x^2 - 1})^n].$$

Proof. The proof is simple. Indeed, if we consider

$$g(x) = \frac{\sqrt{x^2 - 1}}{2^n} [(x + \sqrt{x^2 - 1})^n - (x - \sqrt{x^2 - 1})^n],$$

using the binomial formula we can establish immediately that it is a polynomial. Moreover, from the obvious fact that $\lim_{x \to \infty} \frac{g(x)}{x^{n+1}} = 1$, we deduce that it is actually a monic polynomial of degree $n + 1$. The fact

that $g(t_k) = 0$ for all $0 \leq k \leq n$ is easily verified using Moivre's formula. All this proves the first lemma.

A little bit more computational is the second lemma.

Lemma 2. *The following relations are true:*

i) $\prod_{j \neq k}(t_k - t_j) = \frac{(-1)^k n}{2^{n-1}}$ *if* $1 \leq k \leq n-1$;

ii) $\prod_{j=1}^{n}(t_0 - t_j) = \frac{n}{2^{n-2}}$;

iii) $\prod_{j=0}^{n-1}(t_n - t_j) = \frac{(-1)^n n}{2^{n-2}}$.

Proof. Simple computations, left to the reader, allow us to write:

$$f'(x) = \frac{n}{2^n}[(x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n]$$

$$+\frac{x}{2^n\sqrt{x^2-1}}[(x + \sqrt{x^2-1})^n - (x - \sqrt{x^2-1})^n].$$

Using this formula and Moivre's formula we easily deduce i). To prove ii) and iii) it suffices to compute $\lim_{x \to \pm 1} f'(x)$, using the above formula. We leave the computations to the reader.

Of course, the reader hopes that all these computations will have a honourable purpose. He's right, since these lemmas will allow us to prove some very nice results. The first one is a classical theorem of Chebyshev, about minimal deviation of polynomials on $[-1, 1]$.

Example 10. (Chebyshev theorem) Let $f \in R[X]$ be a monic polynomial of degree n. Then

$$\max_{x \in [-1,1]} |f(x)| \geq \frac{1}{2^{n-1}}$$

and this bound cannot be improved.

Solution. Using again the observation from problem 7, we obtain the identity:

$$I = \sum_{k=0}^{n} f(t_k) \prod_{j \neq k} \frac{1}{t_k - t_j}.$$

Thus, we have

$$1 \leq \max_{0\leq k\leq n} |f(t_k)| \sum_{k=0}^{n} \frac{1}{\left|\prod_{j\neq k}(t_k - t_j)\right|}.$$

Now, it suffices to apply lemma 2 to conclude that we actually have

$$\sum_{k=0}^{n} \frac{1}{\left|\prod_{j\neq k}(t_k - t_j)\right|} = 2^{n-1}.$$

This shows that $\max_{x\in[-1,1]} |f(x)| \geq \frac{1}{2^{n-1}}$ and so the result is proved. To prove that this result is optimal, it suffices to use the polynomial $T_n(x) = \cos(n \arccos(x))$. It is an easy exercise to prove that this is really a polynomial (called the nth polynomial of Chebyshev of the first kind) and that it has leading coefficient 2^{n-1} and degree n. Then the polynomial $\frac{1}{2^{n-1}}T_n$ is monic of degree n and

$$\max_{x\in[-1,1]} \left|\frac{1}{2^{n-1}}T_n(x)\right| = \frac{1}{2^{n-1}}.$$

There are many other proof of this result , many of them are much easier, but we chosen this one because it shows the power of Lagrange interpolation theory. Not to say that the use of the two lemmas allowed us to prove that the inequality presented in example 7 is actually the best.

Some years ago, Walther Janous presented in Crux the following problem as open problem. It is true that it is a very difficult one, but here is a very simple solution using the results already achieved.

Example 11. Suppose that $a_0, a_1, \ldots, a_n$ are real numbers such that for all $x \in [-1, 1]$ we have

$$|a_0 + a_1 x + \cdots + a_n x^n| \leq 1.$$

Then for all $x \in [-1,1]$ we also have

$$|a_n + a_{n-1}x + \cdots + a_0x^n| \leq 2^{n-1}.$$

Walther Janous, Crux Matematicorum

Solution. Actually, we are going to prove a stronger result, that is:

Lemma. *Denote*

$$\|f\| = \max_{x\in[-1,1]} |f(x)|.$$

Then for any polynomial $f \in R[X]$ of degree n the following inequality is satisfied:

$$|f(x)| \leq |T_n(x)| \cdot \|f\| \text{ for all } |x| \geq 1.$$

Proof. Using Lagrange's interpolation formula and modulus inequality, we deduce that for all $u \in [-1,1]$ we have:

$$\left|f\left(\frac{1}{u}\right)\right| \leq \frac{1}{|u|^n}\|f\| \sum_{k=0}^{n} \prod_{j\neq k} \frac{1-t_ju}{|t_k-t_j|}.$$

The very nice idea is to use now again Lagrange interpolation formula, this time for the polynomial T_n. We shall then have

$$\left|T_n\left(\frac{1}{u}\right)\right| = \frac{1}{|u|^n}\left|\sum_{k=0}^{n}(-1)^k \prod_{j\neq k}\frac{1-ut_j}{t_k-t_j}\right| = \frac{1}{|u|^n}\sum_{k=0}^{n}\prod_{j\neq k}\frac{1-ut_j}{|t_k-t_j|}$$

(the last identity being ensured by lemma 2). By combining the two results, we obtain

$$\left|f\left(\frac{1}{u}\right)\right| \leq \left|T_n\left(\frac{1}{u}\right)\right| \|f\| \text{ for all } u \in [-1,1]$$

and the conclusion follows.

Coming back to the problem and considering the polynomial $f(x) = \sum_{k=0}^{n} a_kx^k$, the hypothesis says that $\|f\| \leq 1$ and so by the lemma we have

$$|f(x)| \leq |T_n(x)| \text{ for all } |x| \geq 1.$$

We will then have for all $x \in [-1, 1]$:

$$|a_n + a_{n-1}x + \cdots + a_0x^n| = \left|x^n f\left(\frac{1}{x}\right)\right| \leq \left|x^n T_n\left(\frac{1}{x}\right)\right|.$$

It suffices to prove that

$$\left|x^n T_n\left(\frac{1}{x}\right)\right| \leq 2^{n-1},$$

which can be also written as

$$(1 + \sqrt{1 - x^2})^n + (1 - \sqrt{1 - x^2})^n \leq 2^n.$$

But this inequality is very easy to prove: just set $a = \sqrt{1 - x^2} \in [0, 1]$ and observe that $h(a) = (1-a)^n + (1+a)^n$ is a convex function on $[0, 1]$, thus its superior bound is attained in 0 or 1 and there the inequality is trivially verified. Therefore we have

$$|a_n + a_{n-1}x + \cdots + a_0x^n| \leq 2^{n-1}$$

and the problem is solved.

We end this topic with a very difficult problem, that refines a problem given in a Japanese mathematical Olympiad in 1994. The problem has a nice story: given initially in an old Russian Olympiad, it asked to prove that

$$\max_{x\in[0,2]} \prod_{i=1}^{n} |x - a_i| \leq 108^n \max_{x\in[0,1]} \prod_{i=1}^{n} |x - a_i|$$

for any real numbers $a_1, a_2, \ldots, a_n$. The Japanese problems asked only to prove the existence of a constant that could replace 108. A brutal choice of points in Lagrange interpolation theorem gives a better bound of approximately 12 for this constant. Recent work by Alexandru Lupas reduces this bound to $1 + 2\sqrt{6}$. In the following, we present the optimal bound.

Example 12. For any real numbers $a_1, a_2, \ldots, a_n$, the following inequality holds:

$$\max_{x\in[0,2]} \prod_{i=1}^{n} |x - a_i| \leq \frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2} \max_{x\in[0,1]} \prod_{i=1}^{n} |x - a_i|.$$

Gabriel Dospinescu

Solution. Let us denote

$$\|f\|_{[a,b]} = \max_{x\in[a,b]} |f(x)|$$

for a polynomial f and let, for simplicity,

$$c_n = \frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}.$$

We thus need to prove that $\|f\|_{[0,2]} \leq c_n \|f\|_{[0,1]}$ where

$$f(x) = \prod_{i=1}^{n} (x - a_i).$$

We shall prove that this inequality is true for any polynomial f, which allows us to suppose that $\|f\|_{[0,1]} = 1$. We shall prove that for all $x \in [1,2]$ we have $|f(x)| \leq x_n$. Let us fix $x \in [1,2]$ and consider the numbers $x_k = \dfrac{1+t_k}{2}$. Using Lagrange interpolation formula, we deduce that

$$|f(x)| \leq \sum_{k=0}^{n} \left| \prod_{j\neq k} \frac{x - x_k}{x_k - x_j} \right| = \sum_{k=0}^{n} \prod_{j\neq k} \frac{x - x_j}{|x_k - x_j|}$$

$$\leq \sum_{k=0}^{n} \prod_{j\neq k} \frac{2 - x_j}{|x_k - x_j|} = \sum_{k=0}^{n} \prod_{j\neq k} \frac{3 - t_j}{|t_k - t_j|}.$$

Using lemma 2, we can write

$$\sum_{k=0}^{n} \prod_{j\neq k} \frac{3 - t_j}{|t_k - t_j|} = \frac{2^{n-1}}{n} \sum_{k=1}^{n-1} \prod_{j\neq k} (3 - t_j)$$

$$+ \frac{2^{n-2}}{n} \left[\prod_{j=0}^{n-1} (3 - t_j) + \prod_{j=1}^{n} (3 - t_j) \right].$$

Using again the two lemmas, we obtain:

$$\frac{n}{2^n}[(3+2\sqrt{2})^n+(3-2\sqrt{2})^n]+\frac{3}{2^{n+1}\sqrt{2}}[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n]$$

$$=\sum_{k=1}^{n-1}\prod_{j\neq k}(3-t_j)+\prod_{j=0}^{n-1}(3-t_j)+\prod_{j=1}^{n}(3-t_j).$$

All we have to do now is to compute

$$\prod_{j=0}^{n-1}(3-t_j)+\prod_{j=1}^{n}(3-t_j)=6\prod_{j=1}^{n-1}(3-t_j).$$

But using lemma 1, we deduce immediately that

$$\prod_{j=1}^{n-1}(3-t_j)=\frac{1}{2^{n+1}\sqrt{2}}[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n].$$

Putting all these observations together and making a small computation, that we let to the reader, we easily deduce that $|f(x)|\leq c_n$. This proves that $\|f\|_{[0,2]}\leq c_n\|f\|_{[0,1]}$ and solves the problem.

Problems for training

1. A polynomial of degree $3n$ takes the value 0 at $2,5,8,\ldots,3n-1$, the value 1 at $1,4,7,\ldots,3n-2$ and the value 2 at $0,3,6,\ldots,3n$. It's value at $3n+1$ is 730. Find n.

USAMO 1984

2. A polynomial of degree n verifies $p(k)=2^k$ for all $k=1,n+1$. Find its value at $n+2$.

Vietnam 1988

3. Prove that for any real number a we have the following identity

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}(a-k)^n=n!.$$

Tepper's identity

4. Find $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}k^{n+2}$ and $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}k^{n+3}$.

AMM

5. Prove that

$$\sum_{k=0}^{n}\frac{x_k^{n+1}}{\prod_{j\neq k}(x_k-x_j)}=\sum_{k=0}^{n}x_k$$

and compute

$$\sum_{k=0}^{n}\frac{x_k^{n+2}}{\prod_{j\neq k}(x_k-x_j)}.$$

6. Prove the identity

$$\sum_{k=1}^{n}(-1)^{k-1}\frac{\binom{n}{k}}{k}(n-k)^n=n^n\sum_{k=2}^{n}\frac{1}{k}.$$

Peter Ungar, AMM E 3052

7. Let a,b,c be real numbers and let $f(x)=ax^2+bx+c$ such that $\max\{|f(\pm1)|,|f(0)|\}\leq 1$. Prove that if $|x|\leq 1$ then

$$|f(x)|\leq\frac{5}{4}\text{ and }\left|x^2f\left(\frac{1}{x}\right)\right|\leq 2.$$

Spain, 1996

8. Let $f\in R[X]$ a polynomial of degree n that verifies $|f(x)|\leq 1$ for all $x\in[0,1]$, then

$$\left|f\left(-\frac{1}{n}\right)\right|\leq 2^{n+1}-1.$$

9. Let $a,b,c,d\in R$ such that $|ax^3+bx^2+cx+d|\leq 1$ for all $x\in[-1,1]$. What is the maximal value of $|c|$? Which are the polynomials in which the maximum is attained?

Gabriel Dospinescu

10. Let $a \geq 3$ be a real number and p be a real polynomial of degree n. Prove that

$$\max_{i=\overline{0,n+1}} |a^i - p(i)| \geq 1.$$

India, 2001

11. Find the maximal value of the expression $a^2 + b^2 + c^2$ if $|ax^2 + bx + c| \leq 1$ for all $x \in [-1, 1]$.

Laurentiu Panaitopol

12. Let $a, b, c, d \in R$ such that $|ax^3 + bx^2 + cx + d| \leq 1$ for all $x \in [-1, 1]$. Prove that

$$|a| + |b| + |c| + |d| \leq 7.$$

IMO Shortlist, 1996

13. Let $A = \left\{ p \in R[X] |\ \deg p \leq 3,\ |p(\pm 1)| \leq 1,\ \left| p\left(\pm \frac{1}{2}\right) \right| \leq 1 \right\}$. Find $\sup\limits_{p \in A} \max\limits_{|x| \leq 1} |p''(x)|$.

IMC, 1998

14. a) Prove that for any polynomial f having degree at most n, the following identity is satisfied:

$$xf'(x) = \frac{n}{2} f(x) + \frac{1}{n} \sum_{k=1}^{n} f(xz_k) \frac{2z_k}{(1 - z_k)^2},$$

where z_k are the roots of the polynomial $|X^n + 1$.

b) Deduce Bernstein's inequality: $\|f'\| \leq n\|f\|$ where

$$\|f\| = \max_{|x| \leq 1} |f(x)|.$$

P.J. O'Hara, AMM

15. Define $F(a, b, c) = \max\limits_{x \in [0,3]} |x^3 - ax^2 - bx - c|$. What is the least possible value of this function over R^3?

China TST 2001

HIGHER ALGEBRA IN COMBINATORICS

Till now, we have seen numerous applications of analysis and higher algebra in number theory and algebra. It is time to see the contribution of this "non-elementary mathematics" to combinatorics. It is quite hard to imagine that behind a simple game, such as football for example or behind a quotidian situation such as handshakes there exists such complicated machinery, but this happens sometimes and we will prove it in the next. For the beginning of the discussion, the reader doesn't need any special knowledge, just imagination and the most basic properties of the matrices, but, as soon as we advance, things change. Anyway, the most important fact is not the knowledge, but the ideas and, as we will see, it is not easy to discover that "non-elementary" fact that hides after a completely elementary problem. Since we have clarified what is the purpose of the unit, we can begin the battle.

The first problem we are going to discuss is not classical, but it is easy and a very nice application of how linear-algebra can solve elementary problems. Here it is.

Example 1. Let $n \geq 3$ and let A_n, B_n be the sets of all even, respectively, odd permutations of the set $\{1, 2, \ldots, n\}$. Prove the equality

$$\sum_{\sigma \in A_n} \sum_{i=1}^{n} |i - \sigma(i)| = \sum_{\sigma \in B_n} \sum_{i=1}^{n} |i - \sigma(i)|.$$

Nicolae Popescu, Gazeta Matematica

Solution. Writing the difference

$$\sum_{\sigma \in A_n} \sum_{i=1}^{n} |i - \sigma(i)| - \sum_{\sigma \in B_n} \sum_{i=1}^{n} |i - \sigma(i)|$$

as

$$\sum_{\sigma \in S_n} \varepsilon(\sigma) \sum_{i=1}^{n} |i - \sigma(i)| = 0,$$

where

$$\varepsilon(\sigma) = \begin{cases} 1, & \text{if} \quad \sigma \in A_n \\ -1, & \text{if} \quad \sigma \in B_n \end{cases}$$

reminds us about the formula

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

We have taken here $S_n = A_n \cup B_n$. But we don't have any product in our sum! That is why we will take an arbitrary positive number a and we will consider the matrix $A = (a^{|i-j|})_{1 \leq i,j \leq n}$. This time,

$$\det A = \sum_{\sigma \in S_n} (-1)^{\varepsilon(\alpha)} a^{|1-\sigma(1)|} \dots a^{|-n\sigma(n)|}$$

$$= \sum_{\sigma \in A_n} a^{\sum_{i=1}^{n} |i-\sigma(i)|} - \sum_{\sigma \in B_n} a^{\sum_{i=1}^{n} |i-\sigma(i)|}$$

This is how we have obtained the identity

$$\begin{vmatrix} 1 & x & x^2 & \dots & x^{n-2} & x^{n-1} \\ x & 1 & x & \dots & x^{n-3} & x^{n-2} \\ x^2 & x & 1 & \dots & x^{n-4} & x^{n-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x^{n-1} & x^{n-2} & \dots & \dots & x & 1 \end{vmatrix}$$

$$= \sum_{\substack{\sigma \in S_n \\ \sigma \text{ pară}}} x^{\sum_{i=1}^{n} |i-\sigma(i)|} - \sum_{\substack{\sigma \in S_n \\ \sigma \text{ impară}}} x^{\sum_{i=1}^{n} |i-\sigma(i)|}. \qquad (1)$$

Anyway, we still do not have the desired difference. What can we do to obtain it? The most natural way is to derive the last relation, which is nothing else than a polynomial identity, and then to take $x = 1$. Before

doing that, let us observe that the polynomial

$$\begin{vmatrix} 1 & x & x^2 & \dots & x^{n-2} & x^{n-1} \\ x & 1 & x & \dots & x^{n-3} & x^{n-2} \\ x^2 & x & 1 & \dots & x^{n-4} & x^{n-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x^{n-1} & x^{n-2} & \dots & \dots & x & 1 \end{vmatrix}$$

is divisible by $(x-1)^2$. This can be easily seen by subtracting the first line from the second and the third one and taking from each of these line $x-1$ as common factor. Thus, the derivative of this polynomial is a polynomial divisible by $x-1$, which shows that after we derive the relation (1) and take $x=1$, in the left-hand side we will obtain 0. Since in the right-hand side we obtain exactly

$$\sum_{\sigma \in A_n} \sum_{i=1}^{n} |i - \sigma(i)| - \sum_{\sigma \in B_n} \sum_{i=1}^{n} |i - \sigma(i)|$$

the identity is established.

Here is another nice application of this trick. We have seen how many permutation do not have a fixed point. The question that arises is how many of them are even. Here is a direct answer to the question, using determinants.

Example 2. Find the number of even permutations of the set $\{1, 2, \dots, n\}$ that do not have fixed points.

Solution. Let us consider C_n, D_n, respectively, the sets of even and odd permutations of the set $\{1, 2, \dots, n\}$, that do not have any fixed points. We know how to find the sum $|C_n| + |D_n|$. We have seen it in the unit "Principiul includerii si excluderii" that it is equal to

$$n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + \frac{(-1)^n}{n!}\right).$$

Hence if we manage to compute the difference $|C_n| - |D_n|$, will be able to answer to the question. If we write

$$|C_n| - |D_n| = \sum_{\substack{\sigma \in A_n \\ \sigma(i) \neq i}} 1 - \sum_{\substack{\sigma \in B_n \\ \sigma(i) \neq i}} 1,$$

we observe that this reduces to computing the determinant of the matrix $T = (t_{ij})_{1 \leq i,j \leq n}$, where

$$t_{ij} = \begin{cases} 1, & \text{if} \quad i \neq j \\ 0, & \text{if} \quad i = j \end{cases}$$

That is,

$$|C_n| - |D_n| = \begin{vmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 0 \end{vmatrix}.$$

But it is not difficult to compute this determinant. Indeed, we add all columns to the first one and we give $n-1$ as common factor, then we subtract the first column from each of the other columns. The result is $|C_n| - |D_n| = (-1)^{n-1}(n-1)$ and the conclusion is quite surprising:

$$|C_n| = \frac{1}{2} n! \left(1 - \frac{1}{2!} + \frac{1}{3!} - \dots + \frac{(-1)^{n-2}}{(n-2)!} \right) + (-1)^{n-1}(n-1).$$

We will focus in the next problems on a very important combinatorial tool, that is the incidence matrix (cum se spune la matricea de incidenta?). What is this? Suppose we have a set $X = \{x_1, x_2, \dots, x_n\}$ and $X_1, X_2, \dots, X_k$ a family of subsets of X. Now, define the matrix $A = (a_{ij})_{\substack{i=1,n \\ j=1,k}}$, where

$$a_{ij} = \begin{cases} 1, & \text{if} \quad x_i \in X_j \\ 0, & \text{if} \quad x_i \notin X_j \end{cases}$$

This is the incidence matrix of the family $X_1, X_2, \ldots, X_k$ and the set X. In many situations, computing the product ${}^tA \cdot A$ helps us to modelate algebraically the conditions and the conclusions of a certain problem. From this point, the machinery activates and the problem is on its way of solving.

Let us discuss first a classical problem, though a difficult one. It appeared in USAMO 1979, Tournament of the Towns 1985 and in Bulgarian Spring Mathematical Competition 1995. This says something about the classical character and beauty of this problem.

Example 3. Let $A_1, A_2, \ldots, A_{n+1}$ be distinct subsets of the set $\{1, 2, \ldots, n\}$, each of which having exactly three elements. Prove that there are two distinct subsets among them that have exactly one point in common.

Solution. Of course, we argue by contradiction and suppose that $|A_i \cap A_j| \in \{0, 2\}$ for all $i \neq j$. Now, let T be the incidency matrix of the family $A_1, A_2, \ldots, A_{n+1}$ and compute the product

$$ {}^tT \cdot T = \begin{pmatrix} \sum_{k=1}^{n} t_{k1}^2 & \sum_{k=1}^{n} t_{k1}t_{k2} & \ldots & \sum_{k=1}^{n} t_k t_{kn+1} \\ \ldots & \ldots & \ldots & \ldots \\ \sum_{k=1}^{n} t_{kn+1}t_{k1} & \sum_{k=1}^{n} t_{kn+11}t_{k2} & \ldots & \sum_{k=1}^{n} t_{kn+1}^2 \end{pmatrix}. $$

But we have of course

$$ \sum_{k=1}^{n} x_{ki}^2 = |A_i| = 3 $$

and

$$ \sum_{k=1}^{n} x_{ki}x_{kj} = |A_i \cap A_j| \in \{0, 2\}. $$

Thus, considered in the field $(\mathbb{R}_2, +, \cdot)$, we have

$$\overline{{}^tT \cdot T} = \begin{pmatrix} \widehat{1} & \widehat{0} & \dots & \widehat{0} & \widehat{0} \\ \dots & \dots & \dots & \dots & \dots \\ \widehat{0} & \widehat{0} & \dots & \widehat{0} & \widehat{1} \end{pmatrix},$$

where $\overline{X}$ is the matrix having as elements the residues classes of the elements of the matrix X. Since of course $\det \overline{X} = \overline{\det X}$, the previous relation shows that $\det {}^tT \cdot T$ is odd, hence non-zero. This means that ${}^tT\mathbf{y}T$ is an invertible matrix of size $n+1$, thus $rank\, {}^tT \cdot T = n+1$ which contradicts the inequality $rank\, {}^tT \cdot T \leq rankT \leq n$. This shows that our assumption was wrong and there exist indeed indices $i \neq j$ such that $|A_i \cap A_j| = 1$.

The following problem is very difficult to solve by elementary means, but the solution using linear-algebra is straightforward.

Example 4. Let n be an even number and $A_1, A_2, \dots, A_n$ be distinct subsets of the set $\{1, 2, \dots, n\}$, each of them having an even number of elements. Prove that among these subsets there are two having an even number of elements in common.

Solution. Indeed, if T is the incidency matrix of the family $A_1, A_2, \dots, A_n$, we obtain as in the previous problem the following relation

$${}^tT \cdot T = \begin{pmatrix} |A_1| & |A_1 \cap A_2| & \dots & |A_1 \cap A_n| \\ \dots & \dots & \dots & \dots \\ |A_n \cap A_1| & |A_n \cap A_2| & \dots & |A_n| \end{pmatrix}.$$

Now, let us suppose that all the numbers $|A_i \cap A_j|$ are odd and interpret the above relation in the field $(\mathbb{R}_2, +, \cdot)$. We find that

$$\overline{{}^tT \cdot T} = \begin{pmatrix} \widehat{0} & \widehat{1} & \dots & \widehat{1} & \widehat{1} \\ \dots & \dots & \dots & \dots & \dots \\ \widehat{1} & \widehat{1} & \dots & \widehat{1} & \widehat{0} \end{pmatrix},$$

which means again that $\det {}^tT \dots T$ is odd. Indeed, if we work in $(\mathbb{R}_2, +, \cdot)$, we obtain

$$\begin{vmatrix} \widehat{0} & \widehat{1} & \dots & \widehat{1} & \widehat{1} \\ \dots & \dots & \dots & \dots & \dots \\ \widehat{1} & \widehat{1} & \dots & \widehat{1} & \widehat{0} \end{vmatrix} = \widehat{1}.$$

The technique used is exactly the same as in the second example, only this time we work in a different field. Note that this is the moment when we use the hypothesis that n is even. Now, since $\det {}^tT \cdot T = \det^2 T$, we obtain that $\det T$ is also an odd number. Hence we should try to prove that in fact $\det T$ is an even number and the problem will be solved. Just observe that the sum of elements of the column i of T is $|A_i|$, hence an even number. Thus, if we add all lines to the first line, we will obtain only even numbers on the first line. Since the value of the determinant doesn't change under this operation, the conclusion is plain: $\det T$ is an even number. Since a number cannot be both even and odd, our assumption was wrong and the problem is solved.

Working in a simple field such as $(\mathbb{R}_2, +, \cdot)$ can allow us to find quite interesting solutions. For example, we will discuss the following problem, used for the IMO preparation of the Romanian IMO team in 2004.

Example 5. The squares of a $n \times n$ table are colored with white and black. Suppose that there exists a non-empty set of lines A such that any column of the table has an even number of white squares that also belong to A. Prove that there exists a non-empty set of columns B such that any line of the table contains an even number of white squares that also belong to B.

Gabriel Dospinescu

Solution. This is just the combinatorial translation of the well-known fact that a matrix T is invertible in a field if and only if its transpose is also invertible in that field. But this is not that easy to see.

Let us proceed easily. In each white square we write the number 1 and in each black square we put a 0. We thus obtain a binary matrix $T = (t_{ij})_{1 \leq i,j \leq n}$. From now on, we work only in $(\mathbb{R}_2, +, \cdot)$. Suppose that A contains the columns $a_1, a_2, \ldots, a_k$. It follows that $\sum_{i=1}^{k} t_{a,j} = 0$ for all $j = \overline{1,n}$. Now, let us take

$$x_i = \begin{cases} 1, & \text{if} \quad i \in A \\ 0, & \text{if} \quad i \notin A \end{cases}$$

It follows that the system

$$\begin{cases} t_{11}z_1 + t_{21}z_2 + \cdots + t_{n1}z_n = 0 \\ t_{12}z_1 + t_{22}z_2 + \cdots + t_{n2}z_n = 0 \\ \ldots \\ t_{1n}z_1 + t_{2n}z_2 + \cdots + t_{nm}z_n = 0 \end{cases}$$

admits the non-trivial solution $(x_1, x_2, \ldots, x_n)$. Thus, $\det T = 0$ and consequently $\det {}^tT = 0$. But this means that the system

$$\begin{cases} u_{11}y_1 + u_{12}y_2 + \cdots + u_{1n}y_n = 0 \\ u_{21}y_1 + u_{22}y_2 + \cdots + u_{2n}y_n = 0 \\ \ldots \\ u_{n1}y_1 + u_{n2}y_2 + \cdots + u_{nn}y_n = 0 \end{cases}$$

also has a non-trivial solution in $\mathbb{R}_2$. Now, we take $B = \{i |\ y_i \neq 0\}$ and we will clearly have $B \neq \emptyset$ and $\sum_{x \in B} u_{ix} = 0$, $i = \overline{1,n}$. But this mean that any line of the table contains an even number of white squares that also belong to B and the problem is solved.

In the end of this sub-unit, we will discuss a very difficult problem, in which just knowing the trick of computing ${}^tA \cdot A$ does not suffice. It

is true that it is one of the main steps, but there are much more things to do after we compute ${}^tA \cdot A$. And if for these first problems we have used only intuitive or well-known properties of the matrices and fields, this time we need a more sophisticated machinery: the properties of the characteristic polynomial and eingenvalues of a matrix. It is exactly that kind of problem that kills you just when we feel most strong.

Example 6. Let $S = \{1, 2, \ldots, n\}$ and A be a family of pairs of elements from S with the following property: for any $i, j \in S$ there exist exactly m indices $k \in S$ for which $(i, k), (k, j) \in A$. Find all possible values of m, n for which this is possible.

Gabriel Carrol

Solution. This time, it is easy to see what hides after the problem. Indeed, if we take $T = (t_{ij})_{1 \leq i,j \leq n}$, where

$$a_{ij} = \begin{cases} 1, & \text{if } (i,j) \in A \\ 0, & \text{otherwise} \end{cases}$$

the existence of the family A reduces to

$$T^2 = \begin{pmatrix} m & m & \ldots & m \\ m & m & \ldots & m \\ \ldots & \ldots & \ldots & \ldots \\ m & m & \ldots & m \end{pmatrix}.$$

So, we must find all values of m, n for which there exist a binary matrix T such that

$$T^2 = \begin{pmatrix} m & m & \ldots & m \\ m & m & \ldots & m \\ \ldots & \ldots & \ldots & \ldots \\ m & m & \ldots & m \end{pmatrix}.$$

Let us consider

$$TB = \begin{pmatrix} m & m & \dots & m \\ m & m & \dots & m \\ \dots & \dots & \dots & \dots \\ m & m & \dots & m \end{pmatrix}.$$

and find the eigenvalues of B. This is not difficult, since if x is an eingenvalue, then

$$\begin{vmatrix} m-x & m & \dots & m \\ m & m & \dots & m \\ \dots & \dots & \dots & \dots \\ m & m & \dots & m-x \end{vmatrix}.$$

If we add all columns to the first one and then take the common factor $mn - x$, we obtain the equivalent form

$$(mn-x)\begin{vmatrix} 1 & m & \dots & m \\ 1 & m-x & \dots & m \\ \dots & \dots & \dots & \dots \\ 1 & m & \dots & m-x \end{vmatrix} = 0.$$

In this final determinant, we subtract from each column the first column multiplied by m and we obtain in the end the equation $x^{n-1}(mn - x) = 0$, which shows that the eigenvalues of B are precisely $\underbrace{0, 0, \dots, 0}_{n-1}, mn$. But these are exactly the squares of the eigenvalues of T. Thus, T has the eingevalues $\underbrace{0, 0, \dots, 0}_{n-1}, \sqrt{mn}$, because the sum of the eingenvalues is nonnegative (being equal to the sum of the elements of the matrix situated on the main diagonal). Since $TrT \in \mathbb{R}$, we find that mn must be a perfect square. Also, because $TrT \leq n$, we must have $m \leq n$.

Now, let us prove the converse. So, suppose that $m \leq n$ and mn is a perfect square and write $m = du^2$, $n = dv^2$. Let us take the matrices

$$I = (\underbrace{11\ldots11}_{dv}), \quad O = (\underbrace{00\ldots00}_{dv}).$$

Now, let us define the circulant matrix

$$S = \begin{pmatrix} \underbrace{111\ldots1}_{u}\underbrace{00\ldots0}_{v-u} \\ 0\underbrace{11\ldots1}_{u}\underbrace{00\ldots0}_{v-u-1} \\ \ldots \\ \underbrace{111\ldots1}_{u-1}\underbrace{00\ldots0}_{v-u}1 \end{pmatrix} \in M_{v,n}(\{0,1\}).$$

Finally, we take

$$A = \begin{pmatrix} S \\ S \\ \ldots \\ S \end{pmatrix} \in M_n(\{0,1\}).$$

It is not difficult to see that

$$A^2 = \begin{pmatrix} m & m & \ldots & m \\ m & m & \ldots & m \\ \ldots & \ldots & \ldots & \ldots \\ m & m & \ldots & m \end{pmatrix}.$$

The last idea that we present here (but certainly these are not all the methods of higher mathematics applied to combinatorics) is the use of vector spaces. Again, we will not insist on complicated notions from the theory of vector spaces, just the basic notions and theorems. Maybe the most useful fact is that if V is a vector space of dimension n (that is, V has a basis of cardinal n), then any $n+1$ or more vectors are linearly dependent. As a direct application, we will discuss the following problem,

which is very difficult to solve by means of elementary mathematics. Try first to solve it elementary and you will see how hard it is. The following example is classical, too, but few people know the trick behind it.

Example 7. Let n be a positive integer and let $A_1, A_2, \ldots, A_{n+1}$ be nonempty subsets of the set $\{1, 2, \ldots, n\}$. Prove that there exist nonempty and disjoint index sets $I_1 = \{i_1, i_2, \ldots, i_k\}$ and $I_2 = \{j_1, j_2, \ldots, j_m\}$ such that

$$A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k} = A_{j_1} \cup A_{j_2} \cup \cdots \cup A_{j_m}.$$

Solution. Let us associate to each subset A_i a vector $v_i \in \mathbb{R}^n$, where $v_i = (x_i^1, x_i^2, \ldots, x_i^n)$ and

$$x_i^j = \begin{cases} 0, & \text{if} \quad j \in A_i \\ 1, & \text{if} \quad j \notin A_i \end{cases}$$

Since $\dim \mathbb{R}^n = n$, these vectors we have just constructed must be linearly dependent. So, we can find $a_1, a_2, \ldots, a_{n+1} \in \mathbb{R}$, not all of them 0, such that

$$a_1 v_1 a_2 v_2 + \cdots + a_{n+1} v_{n+1} = 0.$$

Now, we take $I_1 = \{i \in \{1, 2, \ldots, n+1\} |\ a_i > 0\}$ and $I_2 = \{i \in \{1, 2, \ldots, n+1\} |\ a_i < 0\}$. It is plain that I_1, I_2 are nonempty and disjoint. Now, let us prove that $\bigcup_{i \in I_1} A_i = \bigcup_{i \in I_2} A_i$ and the solution will be complete. Let us take $x \in \bigcup_{i \in I_1} A_i$ and suppose that $x \notin \bigcup_{i \in I_2} A_i$. Then the vectors v_i with $i \in I_2$ have zero on their xth component, so the xth component of the vector $a_1 v_1 + a_2 v_2 + \cdots + a_{n+1} v_{n+1}$ is $\sum_{\substack{x \in A_j \\ j \in I_1}} a_j > 0$, which is impossible, since $a_1 v_1 + a_2 v_2 + \cdots + a_{n+1} v_{n+1} = 0$. This shows that $\bigcup_{i \in I_1} A_i \subset \bigcup_{i \in I_2} A_i$. But the reversed inclusion can be proved in exactly the same way, so we conclude that $\bigcup_{i \in I_1} A_i = \bigcup_{i \in I_2} A_i$.

In the end of this "non-elementary" discussion, we solve another problem, proposed for the TST 2004 in Romania, whose idea is also related to vector spaces.

Example 8. 30 boys and 20 girls are preparing for the 2004 Team Selection Test. They observed that any two boys have an even number of common acquaintances among the girls and exactly 9 boys know an odd number of girls. Prove that there exists a group of 16 boys such that any girls attending the preparation is known by an even number of boys from this group.

Gabriel Dospinescu

Solution. Let us consider the matrix $A = (a_{ij})$ where

$$a_{ij} = \begin{cases} 1, & \text{if } B_i \text{ knows } F_j \\ 0, & \text{otherwise} \end{cases}$$

We have considered here that $B_1, B_2, \ldots, B_{30}$ are the boys and $F_1, F_2, \ldots, F_{20}$ are the girls. Now, consider the matrix $T = A \cdot {}^tA$. We observe that all the elements of the matrix T, except those from the main diagonal are even (because $t_{ij} = \sum_{k=1}^{20} a_{ik}a_{jk}$ is the number of common acquaintances among the girls of the boys B_i, B_j). The elements on the main diagonal of T are exactly the number of girls known by each boy. Thus, if we consider the matrix T in $(\mathbb{R}_2, +, \cdot)$, it will be diagonal, with exactly nine non-zero elements on its main diagonal. From now on, we will work only in $(\mathbb{R}_2, +, \cdot)$. We have seen till now that $rankT = 9$. Using Sylvester inequality, it follows that

$$9 = rankT \geq rankA + rank\,{}^tA - 20 = 2rank\,{}^tA - 20$$

hence $r = rank\,{}^tA \leq 14$. Let us consider now the linear system in $(\mathbb{R}_2, +, \cdot)$:

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \cdots + a_{301}x_{30} = 0 \\ a_{12}x_1 + a_{22}x_2 + \cdots + a_{302}x_{30} = 0 \\ \cdots \\ a_{120}x_1 + a_{220}x_2 + \cdots + a_{3020}x_{30} = 0 \end{cases}$$

The set of solutions of this system is a vector space of dimension $30 - r \geq 16$. That is why we can choose a solution $(x_1, x_2, \ldots, x_{30})$ of the system, having at least 16 components equal to $\widehat{1}$. Finally, consider the set $M = \{i \in \{1, 2, \ldots, 30\} |\ x_i = \widehat{1}\}$. We have proved that $|M| \geq 16$ and also $\sum_{j \in M} a_{ji} = 0$ for all $i = \overline{1, 20}$. But we observe that $\sum_{j \in M} a_{ji}$ is just the number of boys B_k with $k \in M$ such that B_k knows F_i. Thus, if we choose the group of those boys B_k with $k \in M$, then each girl is known by an even number of boys from this group and the problem is solved.

Problems for training

1. Let $p > 2$ be an odd prime and let $n \geq 2$. For any permutation $\sigma \in S_n$, we consider

$$S(\sigma) = \sum_{k=1}^{n} k\sigma(k).$$

Let A_j, B_j, respectively, be the set of even, respectively odd permutations σ for which $S(\sigma) \equiv j \pmod{p}$. Prove that $n > p$ if and only if A_j and B_j have the same number of elements for all $j \in \{0, 1, \ldots, p-1\}$.

Gabriel Dospinescu

2. Let $n \geq 2$. Find the greatest number p such that for all $k \in \{1, 2, \ldots, p\}$ we have

$$\sum_{\sigma \in A_n} \left(\sum_{i=1}^{n} if(i) \right)^k = \sum_{\sigma \in B_n} \left(\sum_{i=1}^{n} if(i) \right)^k,$$

where A_n, B_n are, respectively, the sets of all even, respectively, odd permutations of the set $\{1, 2, \ldots, n\}$.

Gabriel Dospinescu

3. Is there in the plane a configuration of 22 circles and 22 points on their union (the union of their circumferences) such that any circle contains at least 7 points and any point belongs to at least 7 circles?

Gabriel Dospinescu, Moldova TST 2004

4. Let $A_1, A_2, \ldots, A_m$ be distinct subsets of a set A with $n \geq 2$ elements. Suppose that any two of these subsets have exactly one elements in common. Prove that $m \leq n$.

5. The edges of a regular 2^n-gon are colored red and blue. A step consists of recoloring each edge which is the same color as both of its neighbours in red, and recoloring each other edge in blue. Prove that after 2^{n-1} steps all of the edges will be red and show that this need not hold after fewer steps.

Iran Olympiad, 1998

6. Problema de la Vietnamezi cu cunostintele

7. $n \geq 2$ teams compete in a tournament and each team plays against any other team exactly once. In each game, 2 points are given to the winner, 1 point for a draw and 0 points for the looser. It is known that for any subset S of teams, one can find a team (possibly in S) whose total score in the games with teams in S is odd. Prove that n is even.

D. Karpov, Russian Olympiad,1972

8. On an $m \times n$ sheet of paper is drawn a grid dividing the sheet into unit squares. The two sides of length n are taped together to form a cylinder. Prove that it is possible to write a real number in each square, not all zero, so that each number is the sum of the numbers in the neighboring squares, if and only if there exist integers k, l such that

$n+1$ does not divide k and

$$\cos\frac{2l\pi}{m}+\cos\frac{k\pi}{n+1}=\frac{1}{2}.$$

Ciprian Manolescu, Romanian TST 1998

9. In a contest consisting of n problems, the jury defines the difficulty of each problem by assigning it a positive integral number of points (the same number of points may be assigned to different problems). Any participant who answers the problem correctly receives that number of points for the problem; any other participant receives 0 points. After the participants submitted their answers, the jury realizes that given any ordering of the participants (where ties are not permitted), it could have defined the problems' difficulty levels to make that ordering coincide with the participants' ranking according to their total scores. Determine, in terms of n, the maximum number of participants for which such a scenario could occur.

Russian Olympiad, 2001

10. Let $S=\{x_0,x_1,\ldots,x_n\}\subset[0,1]$ be a finite set of real numbers with $x_0=0$, $x_1=1$, such that every distance between pairs of elements occurs at least twice, except for the distance 1. Prove that S consists of rational numbers only.

Iran Olympiad

11. Let $x_1,\ldots,x_n$ be real numbers and suppose that the vector space spanned by x_i-x_j over the rationals has dimension m. Then the vector space spanned only by those x_i-x_j for which $x_i-x_j\neq x_k-x_l$ whenever $(i,j)\neq(k,l)$ also has dimension m.

Strauss theorem

12. Let $A_1, A_2, \ldots, A_m$ some subsets of $\{1, 2, \ldots, n\}$. Then there are disjoint sets I, J with non-empty union such that $\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$ and $\bigcap_{i \in I} A_i = \bigcap_{j \in J} A_j$.

Lindstrom theorem

13. There is no partition of the set of edges of the complete graph on n vertices into (strictly) fewer than $n - 1$ complete bipartite graphs.

Graham-Pollak theorem

14. Let $2n+1$ real numbers with the property that no matter how we eliminate one of them, the rest of them can be divided into two groups of n numbers, the sum of the numbers in the two groups being the same. Then all numbers are equal.

15. In a society, acquaintance is mutual and even more, any two persons have exactly one friend. Then there is a person that knows all the others.

Universal friend theorem

16. Let $A_1, \ldots, A_m$ and $B_1, \ldots, B_p$ subsets of $\{1, 2, \ldots, n\}$ such that $A_i \cap B_j$ is an odd number for all i, j. Then $mp \leq 2^{n-1}$.

Benyi Sudakov

17. Let $A_1, \ldots, A_n, B_1, \ldots, B_n \subset A = \{1, 2, \ldots, n\}$ with the properties:

a) for any nonempty subset T of A, there is $i \in A$ such that $|A_i \cap T|$ is odd.

b) for any $i, j \in A$, A_i and B_j have exactly one common element. Then prove that $B_1 = B_2 = \cdots = B_n$.

Gabriel Dospinescu

18. A symmetric matrix of zeros and ones has only ones on the main diagonal. Prove that we can find some rows in this matrix such that their sum is a vector having all of its components odd.

Iran Olympiad

GEOMETRY AND NUMBERS

Again an apparently paradoxical note!!! Indeed, it may look weird, but geometry it really useful in number theory and sometimes it can help proving difficult results with some extremely simple arguments. In the sequel we are going to show some applications of geometry in number theory, almost all of them playing around the celebrated Minkowski theorem. We will see that this theorem gives a very simple criterion for a nice region (we are also going to explain what we understand by nice) to have a non-trivial lattice point and the existence of this point will have important consequences in the theory of representation of numbers by quadratic forms or in approximation of real numbers with rational numbers. As usual, we will content to present only a mere introduction to this field, extremely well developed. The reader will surely have the pleasure to read some reference books about this fascinating field, mentioned in the bibliographies.

First of all, let us state the conditions in which we will work and what is a nice figure. In general, we will work in $\mathbb{R}^n$ and we will call convex body a bounded subset A of $\mathbb{R}^n$ which is convex (that is for all $a, b \in A$ and all $0 \leq t \leq 1$ we have $ta + (1-t)b \in A$), which is symmetric about the origin (that is, for all $x \in A$ we also have $-x \in A$). We will admit that convex bodies have volumes (just think about it in the plane or space, which will be practically always used in our applications).

Let us start by proving the celebrated Minkowski's theorem.

Theorem. (Minkowski) *Suppose that A is a convex body in $\mathbb{R}^n$ having volume strictly greater than 2^n. Then there is a lattice point in A different from the origin.*

The proof is surprisingly simple. Indeed, let us start by making a sort of partition of $\mathbb{R}^n$ in cubes of edge 2, having as centers the points that have all coordinates even numbers. It is clear that any two such cubes will

have disjoint interiors and that they cover all space. That is why we can say that the volume of the convex body is equal to the sum of volumes of the intersections of the body with each cube (since the body is convex, it is clear that the sum will be finite). But of course, one can bring any cube into the cube centered around the origin by using a translation by a vector all of whose coordinates are even. Since translations preserve volume, we will have now an agglomeration of bodies in the central cube (the one centered in the origin) and the sum of volumes of all these bodies is strictly greater that 2^n. Necessarily there will be two bodies which intersect in a point X. Now, look at the cubes where these two bodies where taken from and look at the points in these cubes that give by translations the point X. We have found two different points x, y in our convex body such that $x - y \in 2\mathbb{Z}^n$. But since A is centrally symmetric and convex, it follows that $\frac{x-y}{2}$ is a lattice point different from the origin and belonging to A. The theorem is thus proved.

Here is a surprising result that follows directly from this theorem.

Problem 1. Suppose that in each lattice point in space except for the origin one draws a ball of radius $r > 0$ (common for all the balls). Then any line that passes through the origin will intercept a certain ball.

Solution. Let us suppose the contrary and let us consider a very long cylinder having as axe the line and basis a circle of radius $\frac{r}{2}$. We choose it sufficiently long to ensure that it will have a volume strictly greater than 8. This is clearly a convex body in space and using Minkowski's theorem we deduce the existence of a non-trivial lattice point in this cylinder (or on the border). This means that the line will intercept the ball centered around this point.

Actually, the theorem proved before admits a more general formulation, which is even more useful.

Theorem 2. (Minkowski) *Let A is a convex body in $\mathbb{R}^n$ and $v_1, v_2, \ldots, v_n$ some linearly independent vectors in $\mathbb{R}^n$. Also consider the fundamental parallelepiped $P = \left\{ \sum_{i=1}^{n} x_i v_i |\ 0 \leq x_i \leq 1 \right\}$ and denote $Vol(P)$ its volume. Assuming that A has a volume strictly greater than $2^n \cdot Vol(P)$, A must contain at least a point of the lattice $L = Zv_1 + \cdots + Zv_n$ different from the origin.*

With all these terms, it would seem that this is extremely difficult to prove. Actually, it follows trivially from the first theorem. Indeed, by considering the linear application f sending v_i into the vector $e_i = (0, 0, \ldots, 1, 0, \ldots, 0)$ one can easily see that P is sent into the "normal" cube in $\mathbb{R}^n$ (that is, the set of vectors all of whose components are between 0 and 1) and that f maps L into $\mathbb{Z}^n$. Since the transformation is linear, it will send A into a convex body of volume $\frac{Vol(A)}{Vol(P)} > 2^n$. It suffices to apply the first theorem to this convex body and to look at the preimage of the lattice point (in $\mathbb{Z}^n$), in order to find a non-trivial point of $A \cap L$. The second theorem is thus proved.

We have already proved that any prime number of the form $4k + 1$ is the sum of two squares. Let us prove it differently, using Minkowski's theorem.

Problem 2. Any prime number of the form $4k+1$ is the sum of two squares.

Proof. We have already proved that for any prime number of the form $4k + 1$, call it p, one can find a such that $p|a^2 + 1$. Then let us consider $v_1 = (p, 0)$, $v_2 = (a, 1)$. Visibly, they are linearly independent and moreover for any point (x, y) in the lattice $L = Zv_1 + Zv_2$ we have $p|x^2 + y^2$. Indeed, there are $m, n \in \mathbb{Z}$ such that $x = mp + na$, $y = n$ and thus $x^2 + y^2 \equiv n^2(a^2 + 1) \equiv 0 \pmod{p}$. Moreover, the area of the fundamental parallelogram is $\|v_1 \wedge v_2\| = p$. Next, consider as convex

body the disc centered in the origin and having as radius $\sqrt{2p}$. Obviously, its area is strictly greater than four times the area of the fundamental parallelogram. Thus, there is a point (x, y) different from the origin that lies in this disc and also in the lattice $L = Zv_1 + Zv_2$. For this point we have $p|x^2 + y^2$ and $x^2 + y^2 < 2p$, which shows that $p = x^2 + y^2$.

Proving that a certain Diophantine equation has no solution is a very classical problem, but what can we do when we are asked to prove that a certain equation has solutions? Minkowski's theorem and in general geometry of numbers allow quick responses to such problems. Here is an example, taken from a polish Olympiad.

Problem 3. Consider positive integers such that $ac = b^2 + b + 1$. Then the equation $ax^2 - (2b + 1)xy + cy^2 = 1$ has integer solutions.

Poland Olympiad

Solution. Here is a very quick approach: consider in $\mathbb{R}^2$ the set of points verifying $ax^2 - (2b + 1)xy + cy^2 < 2$. A simple computation shows that it is an elliptical disc having as area $\dfrac{4\pi}{\sqrt{3}} > 4$. An elliptical disc is obviously a convex body and even more this elliptical disc is symmetric about the origin. Thus, by Minkowski's theorem we can find a point of this region different from the origin. Since $ac = b^2 + b + 1$, we have for all x, y not both 0 the inequality $ax^2 - (2b + 1)xy + cy^2 > 0$. Thus for $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ a lattice point of this region, we have $ax^2 - (2b+1)xy + cy^2 = 1$ and the existence of a solution of the equation is proved.

The following problem (as the above one) has a quite difficult elementary solution. The solution using geometry of numbers is more natural, but it is not at all obvious how to proceed. Yet... the experience of the preceding problem should ring a bell.

Problem 4. Suppose that n is a natural number for which the equation $x^2+xy+y^2=n$ has rational solutions. Then this equation has integer solutions as well.

Komal

Solution. Of course, the problem reduces to: if there are integer numbers a, b, c such that $a^2 + ab + b^2 = c^2 n$, then $x^2 + xy + y^2 = n$ has integer solutions. We will assume that a, b, c are non-zero (otherwise the conclusion follows trivially). Even more, a classical argument allows to assume that a, b are relatively prime. We will try again to find a couple of integers $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ such that $x^2 + xy + y^2 < 2n$ and n divides $x^2 + xy + y^2$. In this case we will have $x^2 + xy + y^2 = n$ and the conclusion will follow. First, let us look at the region defined by $x^2 + xy + y^2 < 2n$. Again, simple computations show that it is an elliptical disc of area $\frac{4\pi}{\sqrt{3}}n$. Next, consider the lattice formed by the points (x, y) such that n divides $ax - by$. The area of the fundamental parallelepiped is clearly at most n. By Minkowski's theorem, we can find $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ such that $x^2 + xy + y^2 < 2n$ and n divides $ax - by$. We claim that this will give an integer solution of the equation. Observe that $ab(x^2 + xy + y^2) = c^2xyn + (ax - by)(bx - ay)$ and so n also divides $x^2 + xy + y^2$ (since n is relatively prime with a, b). This allows us to conclude.

Before continuing with some more difficult problems, let us remind that for any symmetric real matrix A such that

$$\sum_{1 \le i,j \le n} a_{ij} x_i x_j > 0$$

for all $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \setminus \{0\}$ the set of points verifying

$$\sum_{1 \le i,j \le n} a_{ij} x_i x_j \le 1$$

has a volume equal to $\frac{Vol(B_n)}{\sqrt{\det A}}$, where

$$Vol(B_n) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1+\frac{n}{2}\right)}$$

(here $\Gamma(x) = \int_0^\infty e^{-t}t^{x-1}dt$ is Euler's gamma function). The proof of this result is non elementary and we invite the reader to read more about it in any decent book of multivariate integral calculus. In particular, the reader has noticed that these results can be applied to previous problems to facilitate the computations of different areas and volumes. With these results (that we will admit) in mind, let's attack some serious problems.

If we spoke about squares, why not present the beautiful classical proof of Lagrange's theorem on representations using 4 squares.

Problem 5. (Lagrange's theorem) Any natural number is a sum of 4 squares.

Proof. This is going to be much more complicated, but the idea is always the same. The main difficulty is finding the appropriate lattice and convex body. First of all, let us prove the result for prime numbers. Let thus $p > 2$ a prime number and consider the sets $A = \{x^2 |\ x \in \mathbb{Z}_p\}$, $B = \{-y^2 - 1 |\ y \in \mathbb{Z}_p\}$. Since there are $\frac{p+1}{2}$ squares in $\mathbb{Z}_p$ (as we have already seen in previous notes), these two sets cannot be disjoint. In particular, there are x, y such that $0 \leq x, y \leq p-1$ and $p|x^2+y^2+1$. This is the observation that will allow us to find a good lattice. Consider now the vectors

$$v_1 = (p, 0, 0, 0),\ v_2 = (0, p, 0, 0),\ v_3 = (x, y, 1, 0),\ v_4 = (y, -x, 0, 1)$$

and the lattice L generated by these vectors. A simple computation (using the above formulas) allows to prove that the volume of the fundamental parallelepiped is p^2. Moreover, one can easily verify that for all point $(x, y, z, t) \in L$ one has $p|x^2+y^2+z^2+t^2$. Even more, one can

also prove (by employing the non-elementary results stated before this problem) that the volume of the convex body $A = \{x = (a, b, c, d) \in \mathbb{R}^4 |\ a^2 + b^2 + c^2 + d^2 < 2p\}$ is equal to $2\pi^2 p^2 > 16Vol(P)$, thus $A \cap L$ is not empty. It suffices then to choose a point $(x, y, z, t) \in L \cap A$ and we will clearly have $x^2 + y^2 + z^2 + t^2 = p$. Thus the theorem is proved for prime numbers.

Of course, everything would be nice if the product of two sums of 4 squares is always a sum of 4 squares. Hopefully, it is the case, but the proof is not obvious at all. It follows form the miraculous identity:

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = (ax + by + cz + dt)^2$$

$$= (ay - bx + ct - dz)^2 + (az - bt + dy - cx)^2 + (at + bz - cy - dx)^2.$$

Of course, very nice, but how could one think at such an identity? The eternal question... Well, this time there is a very nice reason: instead of thinking in eight variables, let us reason only with four. Consider the numbers $z_1 = a + bi$, $z_2 = c + di$, $z_3 = x + yi$, $z_4 = z + ti$. Introduce the matrices

$$M = \begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix}, \quad N = \begin{pmatrix} z_3 & z_4 \\ -\overline{z}_4 & \overline{z}_3 \end{pmatrix}.$$

We have

$$\det(M) = |z_1|^2 + |z_2|^2 = a^2 + b^2 + c^2 + d^2$$

and similarly

$$\det(N) = x^2 + y^2 + z^2 + t^2.$$

It is then normal to try to express $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2)$ as $\det(MN)$. But surprise! We have

$$MN = \begin{pmatrix} z_1 z_3 - z_2 \overline{z}_4 & z_1 z_4 + z_2 \overline{z}_3 \\ \overline{-z_1 z_4 + z_2 \overline{z_3}} & \overline{z_1 z_3 - z_2 \overline{z}_4} \end{pmatrix}$$

and so $\det(MN)$ is again a sum of 4 squares. The identity appears thus naturally...

Let us concentrate a little bit more on approximations of real numbers. We have some beautiful results of Minkowski that deserve to be presented after this small introduction to geometry of numbers.

Problem 6. (Minkowski's linear forms' theorem) Let $A = (a_{ij})$ be a $n \times n$ invertible matrix of real numbers and suppose that $c_1, c_2, \ldots, c_n$ are positive real numbers such that $c_1 c_2 \ldots c_n > |\det A|$. Then there are integers $x_1, x_2, \ldots, x_n$, not all 0, such that $\left| \sum_{j=1}^{n} a_{ij} x_j \right| < c_i$ for all $i = 1, \ldots, n$.

Solution. We need to prove that there exists a non-zero vector X that also belongs to the region $\{Y \in \mathbb{R}^n |\ |A^{-1}Y|_i < c_i,\ i = 1, \ldots, n\}$ (here $A^{-1}Y = (|A^{-1}Y|_1, \ldots, |A^{-1}Y|_n)$. But observe that $\{Y \in \mathbb{R}^n |\ |A^{-1}Y|_i < c_i,\ i = 1, \ldots, n\}$ is exactly the image trough A^{-1} of the parallelepiped $\{Y \in \mathbb{R}^n |\ -c_i < Y_i < c_i,\ i = 1, \ldots, n\}$ which has volume $2^n c_1 \ldots c_n$, thus $\{Y \in \mathbb{R}^n |\ |A^{-1}Y|_i < c_i,\ i = 1, \ldots, n\}$ is a convex body of volume $\frac{1}{\det A} 2^n c_1 \ldots c_n > 2^n$. By Minkowski's theorem, this body will contain a non-zero lattice point, which will verify the conditions of the problem.

And here is a nice consequence of the previous theorem.

Problem 7. Suppose $A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is a matrix with m, n real numbers and $a \ge 1$ is a real number. Then one can find $x_1, x_2, \ldots, x_n$ integers between $-a$ and a, not all 0, such that

$$\left| \sum_{j=1}^{n} a_{ij} x_j \right| < a^{-\frac{n}{m}} \text{ for all } 1 \le i \le m.$$

Solution. All we need to do is to apply the result in problem 6 for the invertible matrix $\begin{pmatrix} A & I_m \\ I_n & 0 \end{pmatrix}$, whose determinant equals 1 or -1

and make the choice $c_1 = \cdots = c_m = a^{-\frac{n}{m}}$, $c_{m+i} = a$, $1 \leq i \leq n$. Incredibly, but the proof ends here!!!

Proposed problems

1. Suppose that a, b, c are positive integers such that $ac = b^2 + 1$. Then there exist x, y, z, t integers such that $a = x^2 + y^2$, $b = z^2 + t^2$, $c = xz + yt$.

Imo Shortlist

2. Suppose that a natural number is the sum of three squares of rational numbers. Then prove that it is also a sum of squares of three natural numbers (the use of three squares theorem is forbidden!).

Davenport-Cassels lemma

3. Consider a disc of radius R. At each lattice point of this disc, except for the origin, one plants a circular tree of radius r. Suppose that r is optimal with respect to the following property: if one regards from the origin, he can see at least a point situated at the exterior of the disc. Then prove that

$$\frac{1}{\sqrt{R^2+1}} \leq r < \frac{1}{R}.$$

AMM

4. Suppose that a, b, c are positive integers such that $a > b > c$. Prove that we can find three integers x, y, z, not all 0, such that

$$ax + by + cz = 0 \text{ and } \max\{|x|, |y|, |z|\} < \frac{2}{\sqrt{3}}a + 1.$$

Miklos Schweitzer competition

5. Suppose that a, b, c are positive integers such that $ac = b^2 + 1$. Prove that the equation $ax^2 + 2bxy + cy^2 = 1$ is solvable in integers.

6. Suppose that a_{ij} $(1 \leq i, j \leq n)$ are rational numbers such that for any $x = (x_1, \ldots, x_n) \in \mathbb{R}^n \setminus \{0\}$ we have $\sum_{1 \leq i,j \leq n} a_{ij} x_i x_j > 0$. Then

there are integers (not all zero) $x_1, \ldots, x_n$ such that

$$\sum_{1 \leq i,j \leq n} a_{ij} x_i x_j < n \sqrt[n]{\det A},$$

where $A = (a_{ij})$.

Minkowski

7. Suppose that $x_1, x_2, \ldots, x_n$ are algebraic integers such that for any $1 \leq i \leq n$ there is at least a conjugate of x_i which is not between $x_1, x_2, \ldots, x_n$. Then the set of n-tuples $(f(x_1), f(x_2), \ldots, f(x_n))$ with $f \in \mathbb{Z}[X]$ is dense in $\mathbb{R}^n$.

8. Suppose that a, b are rational numbers such that the equation $ax^2 + by^2 = 1$ has at least one rational solution. Then it has infinitely many rational solutions.

Kurschak contest

9. Let us denote $A(C, r)$ the set of points w on the unit sphere in $\mathbb{R}^n$ with the property that $|wk| \geq \dfrac{C}{\|k\|^r}$ for any non-zero vector $k \in \mathbb{Z}^n$ (here wk is the usual scalar product and $\|k\|$ is the Euclidean norm of the vector $k \in \mathbb{Z}^n$). Prove that if $r > n - 1$ there exists $C > 0$ such that $A(C, r)$ is non-empty, but if $r < n - 1$ there is no such $C > 0$.

Mathlinks contest (after an ENS entrance exam problem)

10. Using the non-elementary results presented in the topic, prove that if $A = (a_{ij})_{1 \leq i,j \leq n}$ is a symmetric integer matrix such that $\sum_{1 \leq i,j \leq n} a_{ij} x_i x_j > 0$ for all $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \setminus \{0\}$, then we can find an integer matrix B such that $A = B \cdot {}^tB$. Deduce the result from problem 1.

11. Let $n \geq 5$ and $a_1, \ldots, a_n, b_1, \ldots, b_n$ some integers verifying that all pairs (a_i, b_i) are different and $|a_i b_{i+1} - a_{i+1} b_i| = 1$, $1 \leq i \leq n$ (here $(a_{n+1}, b_{n+1}) = (a_1, b_1)$). Prove that one can find $1 < |i - j| < n - 1$ such that $|a_i b_j - a_j b_i| = 1$.

Korea TST

12. Let a, b, c, d be positive integers such that there are 2004 pairs (x, y) such that $x, y \in [0, 1]$ and $ax + by, cx + dy \in \mathbb{Z}$. If $(a, c) = 6$, find (b, d).

Nikolai Nikolov, Bulgaria Olympiad

13. A polygon of area greater than n is given in a plane. Prove that it contains $n + 1$ points $A_i(x_i, y_i)$ such that $x_i - x_j, y_i - y_j \in \mathbb{Z}$ for all $1 \leq i, j \leq n + 1$.

China TST 1988

THE SMALLER, THE BETTER

Often, a large amount of simple ideas can solve very difficult problems. We have seen or will see a few such examples in our journey through the world of numbers: clever congruences that readily solve Diophantine equations, properties of the primes of the form $4k+3$ or even complex numbers and analysis. All these can be called "tricks", but in fact they are much more, as you are going to see soon.

In this unit, we will discuss a fundamental concept in number theory, the order of an element. It may seem contradictory for us to talk about simple ideas and then say "a fundamental concept". Well, what we are going to discuss about is the bridge between simplicity and complexity. The reason for which we say it is a simple idea can be easily guessed from the definition: given are the positive integer $n > 1$ and the integer a such that $gcd(a, n) = 1$, the smallest possible integer d for which $n|a^d - 1$ is called the order of a modulo n. The definition is correct, since from Euler's theorem we have $n|a^{\varphi(n)} - 1$ so such numbers d indeed exist. The complexity of this concept will follow from the examples.

In what follows we will denote by $o_n(a)$ the order of a modulo n. There is a simple property of $o_n(a)$, which has important consequences: if k is a positive integer such that $n|a^k - 1$, then $d|k$. Indeed, because $n|a^k - 1$ and $n|a^d - 1$, we find that $n|a^{gcd(k,d)} - 1$. But from the definition of d it follows that $d \leq gcd(k, d)$, which cannot hold unless $d|k$. Nice and easy. But could such a simple idea be good at anything? The answer is positive and will follow from the solutions of the problems to come. But, before that, we note a first application of this simple observation: $o_n(a)|\varphi(n)$. This is a consequence of the above property and of Euler's theorem.

Now, an old and nice problem, which may seem really trivial after this introduction. But do not get excited so easily, the problem has an

extremely short solution, but this does not mean that it is obvious. It appeared in Saint Petersburg Mathematical Olympiad and also in Gazeta Matematica.

Example 1. Prove that $n|\varphi(a^n-1)$ for all positive integers a, n.

Solution. What is $o_{a^n-1}(a)$? It may seem a silly question, since of course $o_{a^n-1}(a) = n$. Using the observation in the introduction, we obtain exactly $n|\varphi(a^n-1)$.

Here is another beautiful application of the order of an element. It is the first case case of Dirichlet's theorem that we intend to discuss and is also a classical property.

Example 2. Prove that any prime factor of the nth Fermat number $2^{2^n}+1$ is congruent to 1 modulo 2^{n+1}. Show that there are infinitely many prime numbers of the form $2^n k+1$ for any fixed n.

Solution. Let us consider a prime p such that $p|2^{2^n}+1$. Then $p|2^{2^{n+1}}-1$ and consequently $o_p(2)|2^{n+1}$. This ensures the existence of a positive integer $k \leq n+1$ such that $o_p(2)+2^k$. We will prove that in fact $k = n+1$. The proof is easy. Indeed, if this is not the case, then $o_p(2)|2^n$ and so $p|2^{o_p(2)}-1|2^{2^n}-1$. But this is impossible, since $p|2^{2^n}+1$. Therefore, we have found that $o_p(2) = 2^{n+1}$ and we have to prove that $o_p(2)|p-1$ to finish the first part of the question. But this follows from the introduction.

The second part is a direct consequence of the first. Indeed, it is enough to prove that there exists an infinite set of Fermat's numbers $(2^{2^{n_k}}+1)_{n_k>a}$ any two relatively prime. Then we could take a prime factor of each such Fermat's number and apply the first part to obtain that each such prime is of the form $2^n k+1$. But not only it is easy to find such a sequence of Fermat's coprime numbers, but in fact any two different Fermat's numbers are relatively prime. Indeed, suppose that $d|gcd(2^{2^n}+1, 2^{2^{n+k}}+1)$. Then $d|2^{2^{n+1}}-1$ and so $d|2^{2^{n+k}}-1$. Combining

this with $d|2^{2^{n+k}}+1$, we obtain a contradiction. Hence both parts of the problem are solved.

We continue with another special case of the well-known difficult theorem of Dirichlet on arithmetical sequences. Though classical, the following problem is not straightforward and this explains probably its presence on a Korean TST in 2003.

Example 3. For a prime p, let $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

a) If $p|m$, prove that there exists a prime factor of $f_p(m)$ that is relatively prime with $m(m-1)$.

b) Prove that there are infinitely many numbers n such that $pn+1$ is prime.

Solution.

a) is straightforward. In fact, we will prove that any prime factor of $f_p(m)$ is relatively prime with $m(m-1)$. Take such a prime divisor q. Because $q|1+m+\cdots+m^{p-1}$, it is clear that $gcd(q,m)=1$. Moreover, if $gcd(q,m-1)\neq 1$, then $q|m-1$ and because $q|1+m+\cdots+m^{p-1}$, it follows that $q|p$. But $p|m$ and we find that $q|m$, which is clearly impossible.

More difficult is b). But we are tempted to use a) and to explore the properties of $f_p(m)$, just like in the previous problem. So, let us take a prime $q|f_p(m)$ for a certain positive integer m divisible by p. Then we have of course $q|m^p-1$. But this implies that $o_q(m)|q$ and consequently $o_q(m)\in\{1,p\}$. If $o_q(m)=p$, then $q\equiv 1 \pmod p$. Otherwise, $q|m-1$ and because $q|f_p(m)$, we deduce that $q|p$, hence $q=p$. But we have seen while solving a) that this is not possible, so the only choice is $p|q-1$. Now, we need to find a sequence $(m_k)_{k\geq 1}$ of multiples of p such that $f_p(m_k)$ are pairwise relatively prime. This is not as easy as in the first example. Anyway, just by trial and error, it is not difficult to find such a sequence. There are many other approaches, but we like the following one: take $m_1=p$ and $m_k=pf(m_1)f_p(m_2)\ldots f_p(m_{k-1})$. Let us prove that $f_p(m_k)$

is relatively prime to $f_p(m_1), f_p(m_2), \ldots, f_p(m_{k-1})$. Fortunately, this is easy, since $f_p(m_1)f_p(m_2)\ldots f_p(m_{k-1})|f_p(m_k) - f_p(0)|f_p(m_k) - 1$. The solution ends here.

The following problem became classical and variants of it have been given in contests for years. It seems to be a favorite Olympiad problem, since it uses elementary facts and the method is more than beautiful.

Example 4. Find the smallest number n with the property that $2^{2005}|17^n - 1$.

Solution. The problem actually asks for $o_{2^{2005}}(17)$. We know that $o_{2^{2005}}(17)|\varphi(2^{2005}) = 2^{2004}$, so $o_{2^{2005}}(17) = 2^k$, where $k \in \{1, 2, \ldots, 2004\}$. The order of an element has done its job. Now, it is time to work with exponents. We have $2^{2005}|17^{2^k} - 1$. Using the factoring

$$17^{2^k} - 1 = (17 - 1)(17 + 1)(17^2 + 1)\ldots(17^{2^{k-1}} + 1),$$

we proceed by finding the exponent of 2 in each factor of this product. But this is not difficult, because for all $i \geq 0$ the number $17^{2^t} + 1$ is a multiple of 2, but not a multiple of 4. Thus, $v_2(17^{2^k} - 1) = 4 + k$ and the order is found by solving the equation $k + 4 = 2005$. Thus, $o_{2^{2005}}(17) = 2^{2001}$ is the answer to the problem.

Another simple, but not straightforward application of the order of an element is the following divisibility problem. Here, we also need some properties of the prime numbers, that we have already studied in a previous unit.

Example 5. Find all primes p, q such that $p^2 + 1|2003^q + 1$ and $q^2 + 1|2003^p + 1$.

Gabriel Dospinescu

Solution. Let us suppose that $p \leq q$. We discuss first the trivial case $p = 2$. In this case, $5|2003^q + 1$ and it is easy to deduce that q is even,

hence $q = 2$, which is a solution of the problem. Now, suppose that $p > 2$ and let r be a prime factor of $p^2 + 1$. Because $r|2003^{2q} - 1$, it follows that $o_r(2003)|2q$. Suppose that $(q, o_r(2003)) = 1$. Then $o_r(2003)|2$ and $r|2003^2 - 1 = 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 167$. It seems that this is a dead end, since there are too many possible values for r. Another simple observation narrows the number of possible cases: because $r|p^2 + 1$, must be of the form $4k + 1$ or equal to 2 and now we do not have many possibilities: $r \in \{2, 13\}$. The case $r = 13$ is also impossible, because $2003^q + 1 \equiv 2 \pmod{13}$ and $r|2003^q + 1$. So, we have found that for any prime factor r of $p^2 + 1$, we have either $r = 2$ or $q|o_r(2003)$, which in turn implies $q|r-1$. Because p^2+1 is even, but not divisible by 4 and because any odd prime factor of it is congruent to 1 modulo q, we must have $p^2 + 1 \equiv 2 \pmod{q}$. This implies that $p^2 + 1 \equiv 2 \pmod{q}$, that is $q|(p-1)(p+1)$. Combining this with the assumption that $p \leq q$ yields $q|p + 1$ and in fact $q = p+1$. It follows that $p = 2$, contradicting the assumption $p > 2$. Therefore the only pair is (2,2).

More difficult is the following problem, proposed by Reid Barton for the USA TST in 2003. Anyway, using the order of an element, the problem is not very difficult and the solution follows naturally. Let us see...

Example 6. Find all ordered triples of primes (p, q, r) such that

$$p|q^r + 1, q|r^p + 1, r|p^q + 1.$$

Reid Barton, TST USA 2003

Solution. It is quite clear that p, q, r are distinct. Indeed, if for example $p = q$, then the relation $p|q^r + 1$ is impossible. We will prove that we cannot have $p, q, r > 2$. Suppose this is the case. The first condition $p|q^r + 1$ implies $p|q^{2r} - 1$ and so $o_p(q)|2r$. If $o_p(q)$ is odd, it follows that $p|q^r - 1$, which combined with $p|q^r + 1$ yields $p = 2$, which

is impossible. Thus, $o_p(q)$ is either 2 or $2r$. Could we have $o_p(q) = 2r$? No, since this would imply that $2r|p-1$ and so $0 \equiv p^q + 1 \pmod{r} \equiv 2 \pmod{r}$, that is $r = 2$, false. Therefore, the only possibility is $o_p(q) = 2$ and so $p|q^2-1$. We cannot have $p|q-1$, because $p|q^r+1$ and $p \neq 2$. Thus, $p|q+1$ and in fact $p|\frac{q+1}{2}$. In the same way, we find that $q|\frac{r+1}{2}$ and $r|\frac{p+1}{2}$. This is clearly impossible, just by looking at the largest among p, q, r. So, our assumption was wrong and indeed one of the three primes must equal 2. Suppose without loss of generality that $p = 2$. Then q is odd, $q|r^2+1$ and $r|2^q+1$. Similarly, $o_r(2)|2q$. If $q|o_r(2)$, then $q|r-1$ and so $q|r^2+1-(r^2-1) = 2$, which contradicts the already established result that q is odd. Thus, $o_r(2)|2$ and $r|3$. As a matter of fact, this implies that $r = 3$ and $q = 5$, yielding the triple (2,5,3). It is immediate to verify that this triple satisfies all conditions of the problem. Moreover, all solutions are given by cyclic permutations of the components of this triple.

Can you find the smallest prime factor of the number $2^{2^5}+1$. Yes, with a large amount of work, you will probably find it. But what about the number $12^{2^{15}}+1$? It has more than 30000 digits, so you will probably be bored before finding its smallest prime factor. But here is a beautiful and short solution, which does not need a single division.

Example 7. Find the smallest prime factor of the number $12^{2^{15}}+1$.

Solution. Let p be this prime number. Because $p|12^{2^{16}}-1$, we find that $o_p(12)|2^{16}$. Exactly as in the solution of the first example, we find that $o_p(12) = 2^{16}$ and so $2^{16}|p-1$. Therefore $p \geq 1+2^{16}$. But it is well-known that $2^{16}+1$ is a prime (and if you do not believe, you can check; it is not that difficult). So, we might try to see if this number divides $12^{2^{15}}+1$. Let $q = 2^{16}+1$. Then $12^{2^{15}}+1 = 2^{q-1} \cdot 3^{\frac{q-1}{2}} + 1 \equiv 3^{\frac{q-1}{2}} + 1 \pmod{q}$. It remains to see whether $\left(\frac{3}{q}\right) = -1$. But this is done in the unit Quadratic reciprocity and the answer is positive, so indeed

$3^{\frac{q-1}{2}} + 1 \equiv 0 \pmod 2$ and $2^{16} + 1$ is the smallest prime factor of the number $12^{2^{15}} + 1$.

Ok, you must be already tired of this old fashioned idea that any prime factor of $2^{2^n} + 1$ is congruent to 1 modulo 2^{n+1}. Yet, here is a problem that will keep you occupied for a certain period of time, even if it uses only this simple idea.

Example 8. Prove that for any $n > 1$ the largest prime factor of $2^{2^n} + 1$ is at least equal to $n \cdot 2^{n+2} + 1$.

China TST, 2005

Solution. The reader will not imagine how simple this problem really is. If the start is correct... Indeed, let us write $2^{2^n} + 1 = p_1^{k_1} \dots p_r^{k_r}$ with $p_1 < \dots, p_r$ prime numbers. We know that we can find $q_i \in \mathbb{N}$ such that $p_i = 1 + 2^{n+1}q_i$. Now, reduce the relation $2^{2^n} + 1 = p_1^{k_1} \dots p_r^{k_r}$ modulo 2^{2n+2}. It follows that $1 \equiv 1 + 2^{n+1} \sum_{i=1}^{r} k_i q_i \pmod{2^{2n+2}}$ and so $\sum_{i=1}^{r} k_i q_i \geq 2^{n+1}$. But then $q_r \sum_{i=1}^{r} k_i \geq 2^{n+1}$. Now everything becomes simple, since we have $2^{2^n}+1 > (1+2^{n+1})^{k_1+\dots+k_r}$ and so $k_1+\dots+k_r \leq \frac{2^n}{n+1}$. This shows that $q_r \leq 2(n+1)$ and the proof finishes here.

Problems for training

1. Let $a, n > 2$ be positive integers such that $n | a^{n-1} - 1$ and n does not divide any of the numbers $a^x - 1$, where $x < n - 1$ and $x | n - 1$. Prove that n is a prime number.

2. Let p be a nonzero polynomial with integral coefficients. Prove that there are at most finitely many numbers n for which $p(n)$ and $2^{2^n} + 1$ are not relatively prime.

3. Let $p > 3$ be a prime. Prove that any positive divisor of the number $\frac{2^p + 1}{3}$ is of the form $2kp + 1$.

Fermat

4. Let $a > b > 1$ and $n > 1$ be positive integers. Prove that any positive divisor of the number $a^n - b^n$ is either of the form $nk + 1$ or divides a number of the form $a^d - b^d$, with $d|n$, $d < n$.

5. Find all positive integers m, n for which $n|1 + m^{3^n} + m^{2 \cdot 3^n}$.

Bulgaria, 1997

6. Find the smallest repunit divisible by 19.

Gazeta Matematica

7. Let p be a prime and $q > 5$ a prime factor of the number $2^p + 3^p$. Prove that $q > p$.

Laurentiu Panaitopol, TST Romania

8. Let $m > 1$ be an odd number. Find the smallest number n such that $2^{1989}|m^n - 1$.

IMO 1989 Shortlist

9. Let $0 < m < n$ be integers such that 1978^m and 1978^n have the same last three digits. Find the least possible value of $m + n$.

IMO 1978

10. Let p be a prime number and let d a positive divisor of $p - 1$. Prove that there is a positive integer n such that $o_p(n) = d$.

11. Let $q = k \cdot 2^m + 1$ be a divisor of the number $2^{2^n} + 1$, where k is odd. Find $o_q(k)$ in terms of n and $v_2(m)$

J. van de Lune

12. Let n be a positive integer such that $n - 1 = FR$, where all the prime factors of F are known and $gcd(F, R) = 1$. Suppose further that there is an integer a such that $n|a^{n-1} - 1$ and for all primes p dividing $n - 1$ we have $gcd(n, a^{\frac{n-1}{p}} - 1) = 1$. Prove that any prime factor of n is congruent to 1 modulo F.

13. Let $a > 1$ be an integer and let us define $o_p(a) = 0$ if $p|a$. Prove that the function $f : \{2, 3, 5, 7, 11, \dots\} \to \mathbb{N}$, $f(p) = \dfrac{p-1}{o_p(a)}$ is unbounded.

Jon Froemke, Jerrold W Grossman, AMM

14. Let $d = o_p(n)$ and let $k = v_p(n^d - 1)$.

a) If $k > 1$ then $o_{p^j}(n) = d$ for $j \leq k$ and $o_{p^j}(n) = p^{j-k}d$ for all $j \geq k$.

b) If $k = 1$ then let $l = v_p(n^{pd}-1)$. Prove that $o_p(n) = d$, $o_{p^j}(n) = pd$ for $2 \leq j \leq l$ and $o_{p^j}(n) = p^{j-l+1}d$, for all $j \geq l$.

15. Let A be a finite set of prime numbers and let $a \geq 2$ be a positive integer. Prove that there are only finitely many positive integers n such that all prime factors of $a^n - 1$ are in A.

Iran Olympiad

16. Prove that for any prime p there is a prime number q that does not divide any of the numbers $n^p - p$, with $n \geq 1$.

IMO 2003

17. Let $a > 1$ be a positive integer. Prove that for infinitely many n the largest prime factor of $a^n - 1$ is greater than $n \log_a n$.

Gabriel Dospinescu

DENSITY AND REGULAR DISTRIBUTION

Everyone knows that $(\{na\})_{n\geq 1}$ is dense in [0,1] if a is an irrational number, a classical theorem of Kronecker. Various applications of this nice result have appeared in different contests and will probably make the object of Olympiad problems in the future. Yet, there are some examples in which this result is ineffective. A simple one is as follows: using Kronecker's theorem one can easily prove that for any positive integer a that is not a power of 10 there exists n such that a^n begins with 2006. The natural question: what fraction of numbers between 1 and n have this property (speaking here about large values of n) is much more difficult and to answer it we need some stronger tools. This is the reason for which we will try to discuss some classical approximation theorems, particularly the very efficient Weil criterion and its consequences. The proofs are non-trivial and require some heavy-duty analysis. Yet, the consequences that will be discussed here are almost elementary.

Of course, one cannot start a topic about approximation theorems without talking first about Kronecker's theorem. We skip the proof, not only because it is very well-known, but because we will prove a much stronger result about the sequence $(\{na\})_{n\geq 1}$. Instead, we will discuss two beautiful problems, consequences of this theorem.

Example 1. Prove that the sequence $([n\sqrt{2003}])_{n\geq 1}$ contains arbitrarily long geometric progressions with arbitrarily large ratio.

Radu Gologan, IMO TST Romania

Solution. Let us take p a very large number. We will prove that there are arbitrarily long geometric sequences with ratio p. Given $n \geq 3$, let us prove that we can find a positive integer m such that $[p^k m\sqrt{2003}] = p^k[m\sqrt{2003}]$ for all $1 \leq k \leq n$. If the existence of such a number is proved, then the conclusion is immediate. But observe that

$[p^k m\sqrt{2003}] = p^k[m\sqrt{2003}]$ is equivalent to $[p^k\{m\sqrt{2003}\}] = 0$, or to $\{m\sqrt{2003}\} < \dfrac{1}{p^n}$. The existence of a positive integer m with the last property is ensured by Kronecker's theorem.

Here is a problem that is apparently very difficult, but which is again a simple consequence of Kronecker's theorem.

Example 2. Consider $k \geq 1$ and a such that $\log a$ is irrational. Define the sequence x_n as the number formed by the first k digits of the number $[a^n]$ with $n \geq 1$. Prove that this sequence is not eventually periodical.

Gabriel Dospinescu, Mathlinks Contest

Solution. The solution is based on certain simple, but useful remarks. First of all, the number formed with the first k digits of a number m is $[10^{k-1+\{\log m\}}]$. The proof of this claim is not difficult. Indeed, let us write $m = \overline{x_1x_2\ldots x_p}$, with $p \geq k$. Then $m = \overline{x_1\ldots x_k}\cdot 10^{p-k} + \overline{x_{k+1}\ldots x_p}$, hence $\overline{x_1\ldots x_k}\cdot 10^{p-k} \leq m < (\overline{x_1\ldots x_k}+1)\cdot 10^{p-k}$. It follows that $\overline{x_1\ldots x_k} = \left[\dfrac{m}{10^{p-k}}\right]$ and, since $p = 1 + [\log m]$, the claim is proved.

Another remark is the following: there is a positive integer r such that $x_{rT} > 10^{k-1}$. Indeed, assuming the contrary, we find that for all $r > 0$ we have $x_{rT} = 10^{k-1}$. Using the first observation, it follows that $k - 1 + \{\log[a^{rT}]\} < \log(1 + 10^{k-1})$ for all r. Thus

$$\log\left(1 + \frac{1}{10^{k-1}}\right) > \log[a^{rT}] - [\log[a^{rT}]] > \log(a^{rT} - 1) - [\log a^{rT}]$$

$$= \{rT\log a\} - \log\frac{a^{rT}}{a^{rT}-1}.$$

It suffices now to consider a sequence of positive integers (r_n) such that $1 - \dfrac{1}{n} < \{r_nT\log a\}$ (the existence is a simple consequence of Kronecker's lemma) and we will deduce that:

$$\log\left(1 + \frac{1}{10^{k-1}}\right) + \frac{1}{n} + \log\frac{a^{r_nT}}{a^{r_nT}-1} > 1 \text{ for all } n.$$

The last inequality is clearly impossible.

Finally, assume the existence of such an r. It follows that for $n > r$ we have $x_{nT} = x_{rT}$, thus

$$\{\log[a^{nT}]\} \geq \log\left(1 + \frac{1}{10^{k-1}}\right).$$

This shows that

$$\log\left(1 + \frac{1}{10^{k-1}}\right) \leq \log[a^{nT}] - [\log[a^{nT}]] \leq nT\log a - [\log a^{nT}]$$

$$= \{nT\log a\} \text{ for all } n > r.$$

But this contradicts Kronecker's theorem.

Before passing to the quantitative results stated at the beginning of this chapter, we must speak about a simple, yet surprising result, which turns out to be very useful when dealing with real numbers and their properties. Sometimes, it can even help us reducing the problem to integers, as we will see in one of the examples. But first, let us state and prove this result.

Example 3. (Dirichlet) Let $x_1, x_2, \ldots, x_k$ be some real numbers and let $\varepsilon > 0$. There exists a positive integer n and integers $p_1, p_2, \ldots, p_k$ such that $|nx_i - p_i| < \varepsilon$ for all i.

Solution. Thus we need to prove that if we have a finite set of real numbers, we can multiply all its elements by a suitable integer such that the elements of the new set are as close to integers as we want.

Let us choose an integer $N > \dfrac{1}{\varepsilon}$ and partition the interval $[0, 1)$ in N intervals,

$$[0,1) = \bigcup_{s=1}^{N} J_s, \quad J_s = \left[\frac{s-1}{N}, \frac{s}{N}\right).$$

Now, choose $n = N^k + 1$ and associate to any positive integer $q \in \{1, 2, \ldots, n\}$ a sequence of k positive integers $\alpha_1, \alpha_2, \ldots, \alpha_k$, where

$\alpha_i = s$ if and only if $\{qx_i\} \in J_s$. We obtain at most N^k sequences corresponding to these numbers and so by Dirichlet's criterion we can find $1 \leq u < v \leq n$ such that the same sequence is associated to u and v. This means that for all $1 \leq i \leq k$ we have

$$|\{ux_i\} - \{vx_i\}| < \frac{1}{N} \leq \varepsilon.$$

It suffices thus to pick $n = v - u$, $p_i = [vx_i] - [ux_i]$.

And here is how we can use this result in problems where it is more comfortable to work with integers. But don't kid yourself, there are not many such problems. The one we are going to discuss has had a circuitous itinerary between world's Olympiads: proposed for IMO long time ago, it appeared next at the W.L. Putnam Competition and later on in a Japanese Mathematical Olympiad.

Example 4. Let $x_1, x_2, \ldots, x_{2n+1}$ be positive real numbers with the property: for any $1 \leq i \leq 2n+1$ one can make two groups of n numbers by using x_j, $j \neq i$, such that the sum of the numbers in each group is the same. Prove that all numbers are equal.

Solution. Of course, the problem for integers is very well-known and easy: it suffices to observe that in this case all numbers x_i have the same parity and the use of infinite descent solves the problem (either they are all even and in this case we divide each one by two and obtain a new set with smaller sum and the same properties; otherwise, we subtract 1 from each one and then divide by 2).

Now, assume that they are real numbers, which is clearly much more subtle. First of all, if they are all rational, it suffices to multiply by their common denominator and apply the first case. Thus assume that at least one of the numbers is irrational. Consider $\varepsilon > 0$, a positive integer n, and some integers $p_1, p_2, \ldots, p_k$ such that $|nx_i - p_i| < \varepsilon$ for all i. We claim that if $\varepsilon > 0$ is small enough, the corresponding $p_1, p_2, \ldots, p_k$ have

the same property as $x_1, x_2, \ldots, x_{2n+1}$. Indeed, take some i and write the partition condition in the form

$$\sum_{j\neq i} a_{ij} n x_j = 0 \text{ or } \sum_{j\neq i} a_{ij}(nx_j - p_j) = -\sum_{j\neq i} a_{ij} p_j$$

(where of course $a_{ij} \in \{-1, 1\}$). Then

$$\left|\sum_{j\neq i} a_{ij} p_j\right| = \left|\sum_{j\neq i} a_{ij}(nx_j - p_j)\right| \leq 2n\varepsilon.$$

Thus if we choose $\varepsilon < \dfrac{1}{2n}$, then $\displaystyle\sum_{j\neq i} a_{ij} p_j = 0$ and so $p_1, p_2, \ldots, p_k$ have the same property. Since they are all integers, they must be equal (again, because of the first case). Thus we have proved that for any $N > 2n$ there are integers n_N, p_N such that $|n_N x_i - p_N| \leq \dfrac{1}{N}$.

Because at least one of the numbers $x_1, x_2, \ldots, x_{2n+1}$ is irrational, it is not difficult to prove that the sequence $(n_N)_{N>2n}$ is unbounded. But $\dfrac{2}{N} > |n_N| \max\limits_{i,j} |x_i - x_j|$, hence $\max_{i,j} |x_i - x_j| = 0$ and the problem is solved.

Now, let us turn to more quantitative results about the set of fractional parts of natural multiples of different real numbers. The following criterion, due to Weil, is famous and deserves to be discussed because of its beauty and apparent simplicity.

Weil criterion. Let $(a_n)_{n\geq 1}$ be a sequence of real numbers from the interval [0,1]. Then the following statements are equivalent:

a) For any real numbers $0 \leq a \leq b \leq 1$,

$$\lim_{n\to\infty} \frac{|\{i|\ 1 \leq i \leq n,\ a_i \in [a, b]\}|}{n} = b - a;$$

b) For any continuous function $f : [0, 1] \to \mathbb{R}$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) = \int_0^1 f(x)dx;$$

c) For any positive integer $p \geq 1$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi p a_k} = 0.$$

In this case we will say that the sequence is equidistributed.

We will present just a sketch of the solution, containing yet all the necessary ingredients.

First of all, we observe that a) says precisely that b) is true for the characteristic function of any sub-interval of [0,1]. By linearity, this remains true for any piecewise function. Now, there is a well-known and easy to verify property of continuous functions: they can be uniformly approximated with piecewise functions. That is, given $\varepsilon > 0$, we can find a piecewise function g such that $|g(x) - f(x)| < \varepsilon$ for all $x \in [0, 1]$. But then if we write

$$\left| \frac{1}{n} \sum_{k=1}^{n} f(a_k) - \int_0^1 f(x)dx \right| \leq \frac{1}{n} \sum_{k=1}^{n} |f(a_k) - g(a_k)| + \int_0^1 |f(x) - g(x)|dx$$

$$+ \left| \frac{1}{n} \sum_{k=1}^{n} g(a_k) - \int_0^1 g(x)dx \right|$$

and apply the result in b) for the function g, we easily deduce that b) is true for any continuous function.

The fact that b) implies c) is immediate. More subtle is that b) implies a). Let us consider the subinterval $I = [a, b]$ with $0 < a < b < 1$. Next, consider two sequences of continuous functions f_k, g_k such that f_k is zero on $[0, a]$, $[b, 1]$ and 1 on $\left[a + \frac{1}{k}, b - \frac{1}{k}\right]$ (being affine otherwise), while g_k has "the same" properties but is greater than or equal to λ_I (the characteristic function of $I = [a, b]$). Therefore

$$\frac{1}{n} \sum_{j=1}^{n} f_k(a_j) \leq \frac{|\{i|\ 1 \leq i \leq n,\ a_i \in [a, b]\}|}{n} \leq \frac{1}{n} \sum_{j=1}^{n} g_k(a_j).$$

But from the hypothesis,

$$\frac{1}{n}\sum_{j=1}^{n} f_k(a_j) \to \int_0^1 f_k(x)dx = b - a - \frac{1}{k}$$

and

$$\frac{1}{n}\sum_{j=1}^{n} g_k(a_j) \to \int_0^1 g_k(x)dx = b - a + \frac{1}{k}.$$

Now, let us take $\varepsilon > 0$ and k sufficiently large. The above inequalities show that actually for all sufficiently large positive integer n

$$\left| \frac{|\{i|\ 1 \leq i \leq n,\ a_i \in [a,b]\}|}{n} - b + a \right| \leq 2\varepsilon$$

and the conclusion follows. The reader has already seen how to adapt this proof for the case $a = 0$ or $b = 1$.

Finally, let us prove that c) implies b). Of course, a linearity argument allows us to assume that b) is true for any trigonometric polynomials of any degree. Because any continuous function $f : [0,1] \to \mathbb{R}$ satisfying $f(0) = f(1)$ can be uniformly approximated by trigonometric polynomials (this is a really non-trivial result due to Weierstrass), we deduce that b) is true for continuous functions f for which $f(0) = f(1)$. Now, given $f : [0,1] \to \mathbb{R}$ continuous, it is immediate that for any $\varepsilon > 0$ we can find two continuous functions g, h, both having equal values at 0 and 1 and such that

$$|f(x) - g(x)| \leq h(x) \text{ and } \int_0^1 h(x)dx \leq \varepsilon.$$

Using the same arguments as those used to prove that b) implies a), one can easily see that b) is true for any continuous function.

The first problem that we discuss is in fact the most common result about equidistribution. We invite the reader to find an elementary proof in order to appreciate the power of Weil's criterion. Before presenting the second problem, we need another definition: we say that the sequence

$(a_n)_{n\geq 1}$ is uniformly distributed mod 1 if the sequence of fractional parts of a_n is equidistributed. So, here is the classical example.

Example 5. Let a be an irrational number. Then the sequence $(na)_{n\geq 1}$ is uniformly distributed mod 1.

Solution. Well, after so much work, we deserve a reward: this is a simple consequence of Weil's criterion. Indeed, it suffices to prove that c) is verified, which reduces to proving that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi pka} = 0 \qquad (*)$$

for all integers $p \geq 1$. But this is just a geometric series!!! A one-line computation shows that $(*)$ is trivially satisfied and thus we have the desired result.

It's probably time to solve the problem presented in the very beginning of this note: how to compute the density of those numbers n for which 2^n begins with 2006 (for example). Well, again a reward: this is going to be equally easy (of course, the reader needs some rest before looking at some deeper results...).

Example 6. What is the density of the set of positive integers n for which 2^n begins with 2006?

Solution. Indeed, 2^n begins with 2006 if and only if there is a $p \geq 1$ and some digits $a_1, a_2, \ldots, a_p \in \{0, 1, \ldots, 9\}$ such that $2^n - \overline{2006a_1a_2\ldots a_p}$, which is clearly equivalent to the existence of $p \geq 1$ such that

$$2007 \cdot 10^p > 2^n \geq 2006 \cdot 10^p.$$

This can be rewritten in the form

$$\log 2007 + p > n \log 2 \geq \log 2006 + p$$

This implies $[n \log 2] = p + 3$ hence $\log \dfrac{2007}{1000} > \{n \log 2\} > \log \dfrac{2006}{1000}$. Thus the density of the desired set is exactly the density of the set of

positive integers n satisfying

$$\log \frac{2007}{1000} > \{n \log 2\} > \log \frac{2006}{1000}.$$

From example 5, the last set has density $\log \frac{2007}{2006}$ and so this is the answer to our problem.

We have seen a beautiful proof of the fact that if a is irrational, then $(na)_{n\geq 1}$ is uniformly distributed mod 1. Actually, much more is true, but this much more is also much more difficult to prove. The next two examples are two important theorems. The first is due to Van der Corput and shows how a brilliant combination of algebraic manipulations and Weil's criterion can yield difficult and nice results.

Example 7. (Van der Corput) Let (x_n) be a sequence of real numbers such that the sequences $(x_{n+p} - x_n)_{n\geq 1}$ are equidistributed for all $p \geq 1$. Then the sequence (x_n) is also equidistributed.

This is not an Olympiad problem!!! But mathematics is not just Olympiad and from time to time (in fact, from a certain time on) one should try to discover what is behind such great results. This is the reason for which we present a proof of this theorem, a difficult proof that uses the "well-known" but not easy to remember inequality of Van der Corput.

Lemma. (Van der Corput) *For any complex numbers $z_1, z_2, \ldots, z_n$ and any $h \in \{1, 2, \ldots, n\}$, the following inequality is true (with the convention that $z_i = 0$ for any integer i not in $\{1, 2, \ldots, n\}$):*

$$h^2 \left| \sum_{i=1}^{n} z_i \right|^2 \leq (n + h - 1) \left[2 \sum_{r=1}^{p-1} (h - r) \mathrm{Re} \left(\sum_{i=1}^{n-r} z_i \overline{z_{i+r}} \right) + h \sum_{i=1}^{n} |z_i|^2 \right].$$

Unbelievable, but true! Not to mention that the proof of this inequality is anything but easy. We will limit to give the main idea of the

proof, the computations being very technical. The idea behind this fundamental inequality is another fundamental one. You would have never guessed: the Cauchy Schwarz inequality!!! The simple observation that

$$h\sum_{i=1}^{n} z_i = \sum_{i=1}^{n+h-1}\sum_{j=0}^{h-1} z_{i-j}$$

allows us to write (via Cauchy Schwarz's inequality):

$$h^2\left|\sum_{i=1}^{n} z_i\right|^2 \leq (n+h-1)\sum_{i=1}^{n+h-1}\left|\sum_{j=0}^{h-1} z_{i-j}\right|^2.$$

And next ? Well... this is where the readers will get some satisfaction... if they have the patience to expand $\sum_{i=1}^{n+p-1}\left|\sum_{j=0}^{p-1} z_{i-j}\right|^2$ and see that it is nothing else than

$$2\sum_{r=1}^{p-1}(p-r)\mathrm{Re}\left(\sum_{i=1}^{n-r} z_i\overline{z_{i+r}}\right) + p\sum_{i=1}^{n}|z_i|^2.$$

Wishing them good luck with the computations, we will now prove Van der Corput's theorem, by using this lemma and Weil's criterion.

Of course, the idea is to prove that

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n} e^{2i\pi p x_k} = 0 \text{ for all } p \geq 1.$$

Fix such a $p \geq 1$ and take for the moment a positive real number h and $\varepsilon \in (0,1)$ (h may depend on ε). Also, denote $z_j = e^{2i\pi p x_j}$. Using the lemma, we have:

$$\left|\frac{1}{n}\sum_{j=1}^{n} z_j\right|^2 \leq \frac{1}{n^2}\cdot\frac{n+h-1}{h^2}\left[hn + 2\sum_{i=1}^{h-1}(h-i)\mathrm{Re}\left(\sum_{j=1}^{n-i} z_j\cdot\overline{z_{i+j}}\right)\right].$$

Now, let us regard

$$\mathrm{Re}\left(\sum_{j=1}^{n-i} z_j \cdot \overline{z_{i+j}}\right) = \mathrm{Re}\left(\sum_{j=1}^{n-i} e^{2i\pi p(x_j - x_{i+j})}\right) \leq \left|\sum_{j=1}^{n-i} e^{2i\pi p(x_j - x_{i+j})}\right|.$$

Using Weil's criterion for the sequences $(x_{n+i} - x_n)$ for $i = 1, 2, \ldots, h-1$ we deduce that for all sufficiently large n we have

$$\left|\sum_{j=1}^{n-i} e^{2i\pi p(x_j - x_{i+j})}\right| \leq \varepsilon n.$$

Therefore

$$\left|\frac{1}{n}\sum_{j=1}^{n} z_j\right|^2 \leq \frac{1}{n^2} \cdot \frac{n+h-1}{h^2}\left[hn + 2\varepsilon n \sum_{i=1}^{h-1}(h-i)\right]$$

$$< \frac{n+h-1}{nh}(1+\varepsilon) < \frac{2(1+\varepsilon)}{h}$$

for all sufficiently large n. Now, by choosing $h > \dfrac{2(1+\varepsilon)}{\varepsilon^2}$, we deduce that for all sufficiently large n we have

$$\left|\frac{1}{n}\sum_{j=1}^{n} z_j\right| \leq \varepsilon.$$

This shows that Weil's criterion is verified and thus (x_n) is equidistributed.

This was surely the most difficult result of this unit, but why not taking one more step once we are already here? Let us prove the following weaker (but as the reader will probably agree, absolutely nontrivial) version of famous theorem of Weil. It is related to the equidistribution of the sequence $(\{f(n)\})_{n\geq 1}$ where is a real polynomial having at least one irrational coefficient except for the free term. We will not prove this here, but focus on the following result.

Example 8. (Weil) Let f be a polynomial with real coefficients and irrational leading coefficient. Then the sequence $(\{f(n)\})_{n\geq 1}$ is equidistributed.

The reader has probably noticed that this is an immediate consequence of Van der Corput's theorem (but just imagine the amount of work done to arrive at this conclusion!!!). Indeed, the proof by induction is immediate.

Indeed, if f has degree 1, then the conclusion is immediate (see example 5). Now, if the result holds for polynomials of degree at most k, it suffices (by Van der Corput's theorem) to prove that for all positive integers p, the sequence $(f(n+p)-(f(n))$ is equidistributed. But this is exactly the induction hypothesis applied to the polynomial (whose leading coefficient is clearly irrational) $f(X+p)-f(X)$. The proof by induction finishes here.

Problems for training

1. Compute $\sup\limits_{n\geq 1}\left(\min\limits_{\substack{p,q\in\mathbb{N}\\ p+q=n}}|p-q\sqrt{3}|\right)$.

Putnam Competition

2. Prove that by using different terms of the sequence $[n^2\sqrt{2006}]$ one can construct geometric sequences of any length.

3. Let x be an irrational number and let $f(t)=\min(\{t\},\{1-t\})$. Prove that given any $\varepsilon>0$ one can find a positive integer n such that $f(n^2x)<\varepsilon$.

Iran 2004

4. Prove that the sequence consisting of the first digit of 2^n+3^n is not periodical.

Tuymaada Olympiad

5. Suppose that $A = \{n_1, n_2, \dots\}$ is a set of positive integers such that the sequence $(\cos n_k)_{k\geq 1}$ is convergent. Then prove that A has zero density.

Marian Tetiva

6. Suppose that f is a real, continuous, and periodical function such that the sequence $\left(\sum_{k=1}^{n} \frac{|f(k)|}{k}\right)_{n\geq 1}$ is bounded. Prove that $f(k) = 0$ for all positive integers k. Give a necessary and sufficient condition ensuring the existence of a constant $c > 0$ such that $\sum_{k=1}^{n} \frac{|f(k)|}{k} > c \ln n$ for all n.

Gabriel Dospinescu

7. Does the sequence $\sin(n^2) + \sin(n^3)$ converge?

Gabriel Dospinescu

8. Let f be a polynomial with integral coefficients and let a be an irrational number. Can all numbers $f(k)$, $k = 1, 2, \dots$ be in the set $A = \{[na] |\ n \geq 1\}$? Is it true that any set of positive integers with positive density contains an infinite arithmetical sequence?

9. Let a, b be positive real numbers such that $\{na\} + \{nb\} < 1$ for all n. Then at least one of them is an integer.

10. Prove that for every k one can find distinct positive integers $n_1, n_2, \dots, n_k$ such that $[n_1\sqrt{2}]$, $[n_2\sqrt{2}], \dots, [n_k\sqrt{2}]$ and $[n_1\sqrt{3}]$, $[n_2\sqrt{3}], \dots, [n_k\sqrt{3}]$ are both geometrical sequences.

After a romanian IMO TST problem

11. A flea moves in the positive direction of an axis, starting from the origin. It can only jump over distances equal to $\sqrt{2}$ and $\sqrt{2005}$. Prove that there exists n_0 such that the flea will be able to arrive in any interval $[n, n+1]$ for all $n \geq n_0$.

Romanian Contest, 2005

12. Let a, b, c be positive real numbers. Prove that the sets

$$A = \{[na] |\ n \geq 1\},\ B = \{[nb] |\ n \geq 1\},\ C = \{[nc] |\ n \geq 1\}$$

cannot form a partition of the set of positive integers.

Putnam

13. Let $z_1, z_2, \ldots, z_n$ be arbitrary complex numbers. Prove that for any $\varepsilon > 0$ there are infinitely many positive integers n such that

$$\varepsilon + \sqrt[k]{|z_1^k + z_2^k + \cdots + z_n^k|} < \max\{|z_1|, |z_2|, \ldots, |z_n|\}.$$

THE SUM OF DIGITS OF A POSITIVE INTEGER

Problems about the sum of digits of a positive integer often occur in mathematical contests because of their difficulty and the lack of standard ways to tackle the problem. This is why a synthesis of the most frequent techniques that occur in such cases would be useful. We have selected several representative problems to show how the main results and techniques work and why they are so important.

We will work only in base 10 and we will denote the decimal sum of digits of the positive integer x by $s(x)$. The following "formula" can be checked easily:

$$s(n) = n - 9\sum_{k\geq 1}\left\lfloor \frac{n}{10^k}\right\rfloor \tag{1}$$

From (1) we can easily deduce some well-known results about $s(n)$ such as $s(n) \equiv n(\mathrm{mod}\, 9)$ and $s(m+n) \leq s(m)+s(n)$. Unfortunately, (1) is a clumsy formula, which can hardly be used in applications. On the other hand, there are several more or less known results about sum of digits, results which may offer simple ways to tackle hard problems. This is what we will discuss about in the following.

The easiest of these techniques is, probably, just the careful analysis of the structure of the numbers and their digits. This can work surprisingly well, as we will see in the following examples.

1. Prove that among any 79 consecutive numbers, one can choose at least one whose sum of digits is a multiple of 13.

Baltic, 1997

Solution. Note that among the first 40 numbers, there are exactly 4 multiples of 10. Also, it is clear that the last but one digit of one of them is at least 6. Let x be this number. Obviously, x, $x+1$,..., $x+39$ are among our numbers, so $s(x), s(x)+1$,...,$s(x)+12$ occur as sum of digits

in some of our numbers. Obviously, one of these numbers is a multiple of 13 and we are done.

We will continue with two harder problems, which still do not require any special result or technique.

2. Find the greatest N such that one can find N consecutive numbers with the property that the sum of digits of the k-th number is divisible by k, for $k = 1, 2, ..., N$.

Tournament of Towns, 2000

Solution. The answer here is not trivial at all, namely 21. The main idea is that among $s(n+2)$, $s(n+12)$ and $s(n+22)$ there are two consecutive numbers, which is impossible since they should all be even. In truth, we make transports at $a+10$ only when the last but one digit of a is 9, but this situation can occur at most once in our case. So, for $N > 21$, we have no solution. For $N = 21$, we can choose $N+1$, $N+2$,..., $N+21$, where $N = 291 \cdot 10^{11!} - 12$. For $i = 1$ we have nothing to prove. For $2 \leq i \leq 11$, $s(N+i) = 2+9+0+9(11!-1)+i-2 = i+11!$ while for $12 \leq i \leq 21$, $s(N+i) = 2+9+1+(i-12) = i$, so our numbers have the desired property.

3. How many positive integers $n \leq 10^{2005}$ can be written as the sum of 2 positive integers with the same sum of digits?

Adrian Zahariuc

Solution. Answer: $10^{2005} - 9023$. At first glance, it might seem almost impossible to find the exact number of positive integers with this property. In fact, the following is true: a positive integer cannot be written as the sum of two numbers with the same sum of digits iff all of its digits (eventually) excepting the first are 9 and the sum of its digits is odd.

Let n be such a number. Suppose there are $a, b \in \mathbb{Z}^+$ such that $n = a + b$ and $s(a) = s(b)$. The main fact is that when we add $a + b = n$, there are no transports. This is clear enough. It follows that $s(n) = s(a) + s(b) = 2s(a)$, which is impossible since $s(n)$ is odd.

Now we will prove that any number n which is not one of the numbers stated above, can be written as the sum of 2 positive integers with the same sum of digits. We will start with the following:

Lemma. *There is $a \leq n$ such that $s(a) \equiv s(n-a) (\mathrm{mod} 2)$.*

Proof. If the $s(n)$ is even, take $a = 0$. If $s(n)$ is odd, then n must have a digit which is not the first and is not equal to 9, otherwise it would have one of the forbidden forms. Let c be the value of this digit and p its position (from right to left). Then let us chose $a = 10^{p-1}(c+1)$. At the adding $a + (n-a) = n$ there is exactly one transport, so

$$s(a) + s(n-a) = 9 + s(n) \equiv 0 (\mathrm{mod} 2) \Rightarrow s(a) \equiv s(n-a) (\mathrm{mod} 2)$$

which proves our claim.

Back to the original problem. All we have to do now is take one-by-one a "unity" from a number and give it to the other until the 2 numbers have the same sum of digits. This will happen since they have the same parity. So, let us do this rigorously. Let

$$a = \overline{a_1 a_2 .. a_k}, n - a = \overline{b_1 b_2 ... b_k}$$

The lemma shows that the number of elements of the set $I = \{i \in \{1, 2, ..., k\} : 2 \text{ does not divide } a_i + b_i\}$ is even, so it can be divided into 2 sets with the same number of elements, say I_1 and I_2. For $i = 1, 2, ..., k$ define $A_i = (a_i + b_i)/2$ if $i \in I$, $(a_i + b_i + 1)/2$ if $i \in I_1$ or $(a_i + b_i - 1)/2$ if $i \in I_2$ and $B_i = a_i + b_i - A_i$. It is clear that the numbers

$$A = \overline{A_1 A_2 ... A_k}, B = \overline{B_1 B_2 ... B_k}$$

have the property that $s(A) = s(B)$ and $A + B = n$. The proof is complete.

We have previously seen that $s(n) \equiv n (\mathrm{mod}\, 9)$. This is probably the most famous property of the function s and it has a series of remarkable applications. Sometimes it is combined with some simple inequalities such as $s(n) \leq 9(\lfloor \lg n \rfloor + 1)$. Some immediate applications are the following:

4. Find all n for which one can find a and b such that

$$s(a) = s(b) = s(a + b) = n.$$

Vasile Zidaru and Mircea Lascu, JBMO TST, 2002

Solution. We have $a \equiv b \equiv a + b \equiv n (\mathrm{mod} 9)$, so 9 divides n. If $n = 9k$, we can take $a = b = 10^k - 1$ and we are done since $s(10^k - 1) = s(2 \cdot 10^k - 2) = 9k$.

5. Find all the possible values of the sum of digits of a perfect square.

Iberoamerican, 1995

Solution. What does sum of digits has to do with perfect squares? Apparently, nothing, but perfect squares do have something to do with remainders mod 9! In fact, it is very easy to prove that the only possible values of a perfect square mod 9 are 0, 1, 4 and 7. So, we deduce that the sum of digits of a perfect square must be congruent to 0, 1, 4 or 7 mod 9. To prove that all such numbers work, we will use a small and very common (but worth to remember!) trick: use numbers that consist almost only of 9-s. We have the following identities:

$$\underbrace{99...99}_{n}{}^2 = \underbrace{99...99}_{n-1} 8 \underbrace{00...00}_{n-1} 1 \Rightarrow s(\underbrace{99...99}_{n}{}^2) = 9n$$

$$\underbrace{99...99}_{n-1} 1^2 = \underbrace{99...99}_{n-2} 82 \underbrace{00...00}_{n-2} 81 \Rightarrow s(\underbrace{99..99}_{n-1} 1^2) = 9n + 1$$

$$\underbrace{99...99}_{n-1}2^2 = \underbrace{99...99}_{n-2}84\underbrace{00...00}_{n-2}64 \Rightarrow s(\underbrace{99..99}_{n-1}2^2) = 9n+4$$
$$\underbrace{99...99}_{n-1}4^2 = \underbrace{99...99}_{n-2}88\underbrace{00...00}_{n-2}36 \Rightarrow s(\underbrace{99..99}_{n-1}4^2) = 9n+7$$

and since $s(0) = 0$, $s(1) = 1$, $s(4) = 4$ and $s(25) = 7$ the proof is complete.

6. Compute $s(s(s(4444^{4444})))$.

IMO 1975

Solution. Using the inequality $s(n) \leq 9(\lfloor \lg n \rfloor + 1)$ several times we have

$$s(4444^{4444}) \leq 9(\lfloor \lg 4444^{4444} \rfloor + 1) < 9 \cdot 20,000 = 180,000;$$

$$s(s(4444^{4444})) \leq 9(\lfloor \lg s(4444^{4444}) \rfloor + 1) \leq 9(\lg 180,000 + 1) \leq 36,$$

so $s(s(s(4444^{4444}))) \leq 12$. On the other hand, $s(s(s(n))) \equiv s(s(n)) \equiv s(n) \equiv n(\mathrm{mod}9)$ and since

$$4444^{4444} \equiv 7^{4444} = 7 \cdot 7^{3^{1481}} \equiv 7(\mathrm{mod}9),$$

the only possible answer is 7.

Finally, we present a beautiful problem which appeared in the Russian Olympiad and, later, in *Kvant*.

7. Prove that for any N there is $n \geq N$ such that $s(3^n) \geq s(3^{n+1})$.

Solution. Suppose by way of contradiction that there is one N such that $s(3^{n+1}) - s(3^n) > 0, \forall n \geq N$. But, for $n \geq 2$, $s(3^{n+1}) - s(3^n) \equiv 0(\mathrm{mod}9)$, so $s(3^{n+1}) - s(3^n) \geq 9, \forall n \geq N$. It follows that

$$\sum_{k=N+1}^{n} \left(3^{k+1} - 3^k\right) \geq 9(n-N) \Rightarrow s(3^{n+1}) \geq 9(n-N), n \geq N+1.$$

But $s(3^{n+1}) \leq 9(\lfloor \lg 3^{n+1} \rfloor + 1)$, so $9n - 9N \leq 9 + 9(n+1)\lg 3$, for all $n \geq N+1$. This is obviously a contradiction.

If so far we have studied some remarkable properties of the function s, which were quite well-known, it is time to present some problems and

results which are less familiar, but interesting and hard. The first result is the following:

Statement. If $1 \leq x \leq 10^n$, then $s(x(10^n-1)) = 9n$.

Proof. The idea is very simple. All we have to do is write $x = \overline{a_1a_2...a_j}$ with $a_j \neq 0$ (we can ignore the final 0-s of x) and note that

$$x(10^n-1) = \overline{a_1a_2...a_{j-1}(a_j-1)\underbrace{99...99}_{n-j}(9-a_1)...(9-a_j)(10-a_j)},$$

which obviously has the sum of digits equal to $9n$.

The previous result is by no means hard, but we will see that it can be the key in many situations. A first application is:

8. Compute $s(9 \cdot 99 \cdot 999 \cdot ... \cdot \underbrace{99...99}_{2^n})$.

USAMO, 1992

Solution. The problem in trivial if we know the previous result. We have

$$N = 9 \cdot 99 \cdot 999 \cdot ... \cdot \underbrace{99...99}_{2^{n-1}} < 10^{1+2+...+2^{n-1}} < 10^{2^n} - 1$$

so $s(\underbrace{99...99}_{2^n} N) = 9 \cdot 2^n$.

However, there are very hard applications of this apparently unimportant result, such as the following problem.

9. Prove that for any n there is a positive integer n which is divisible by its sum of digits.

IMO Shortlist, 1998

Solution. Only to assure our readers that this problem did not appear on the ISL out of nowhere, such numbers are called Niven numbers and they are an important research source in number theory. Now, let's solve it. We will see that constructing such a number is hard. First, we

will get rid of the case $n = 3^k$, when we can take the number $\underbrace{11...11}_{n}$ (it can be easily proved by induction that $3^{k+2}|10^{3^k} - 1$).

Due to the trick that we should search numbers with many equal digits and the last result, we decide that the required number p should be $\underbrace{aa...aa}_{s}b \cdot (10^t - 1)$, with $\underbrace{aa...aa}_{s}b \leq 10^t - 1$. This number will have $s+t+1$ digits and its sum of digits will be $9t$. Therefore, we will require $s + t = n - 1$ and $9t|\underbrace{aa...aa}_{s}b \cdot (10^t - 1)$. We now use the fact that for t a power of 3, $9t|10^t - 1$. So, let us take $t = 3^k$ where k is chosen such that $3^k < n < 3^{k+1}$. If we also take in account the condition $\underbrace{aa...aa}_{s}b \leq 10^t - 1$, the choice $p = \underbrace{11...11}_{n-3^k-1}2(10^{3^k} - 1)$ when $n \leq 2 \cdot 3^k$ and $p = \underbrace{22...22}_{2 \cdot 3^k}(10^{2 \cdot 3^k} - 1)$ otherwise becomes natural.

We continue our investigations in finding suitable techniques for problems involving sum of digits with a very beautiful result. The following result turned out to have several consequences, most of them being very hard.

Statement. Any multiple of $\underbrace{11...11}_{k}$ has sum of digits at least k.

Proof. We will use the extremal principle. Suppose by way of contradiction that the statement is false and take M to be the smallest multiple of a such that $s(M) < k$, where $a = \underbrace{11...11}_{k}$. Note that $s(ia) = ik$ for $i = 1, 2, ..., 9$. So $M \geq 10a > 10^k$. Therefore, $M = \overline{a_1 a_2 ... a_p}$, with $p \geq k + 1$ and $a_p \neq 0$. Take the number $N = M - 10^{p-k}a$. Obviously, N is a multiple of a. We will try to prove that $s(N) < k$. In this way, we would contradict the minimality of M and the proof would be complete. But this is not hard at all since if $a_{k+1} < 9$, we have $s(N) = s(M) < k$ and if $a_{k+1} = 9$, we have $s(N) < s(M) < k$.

We will show 3 applications of this fact, which might seem simple, but which might be unsolvable without it.

10. Prove that for every k, we have

$$\lim_{n\to\infty} \frac{s(n!)}{\ln^k \ln n} = \infty$$

Gabriel Dospinescu

Solution. Due to the simple fact that $10^{\lfloor \lg n \rfloor} - 1 \leq n \Rightarrow 10^{\lfloor \lg n \rfloor} - 1 | n!$, we have that $s(n!) \geq \lfloor \lg n \rfloor$, from which our conclusion follows easily.

11. Let S be the set of positive integers whose decimal representation contains only of at most 1988 1-s and the rest 0-s. Prove that there is a positive integer which does not divide any member of S.

Tournament of Towns, 1988

Solution. Again, the solution follows directly from our result. We can choose the number $10^{1989} - 1$, whose multiples have sum of digits greater than 1988.

12. Prove that for any $k > 0$, there is an infinite arithmetical sequence having the ratio relatively prime to 10, such that all its members have the sum of digits greater than k.

IMO Shortlist, 1999

Solution. Let us remind that this is the last problem of ISL 1999, so the hardest. The official solution is indeed one for such a problem. But, due to our "theorem" we can chose the sequence $a_n = n(10^m - 1)$, where $m > k$ and we are done.

Now, as a final proof of the utility of these two results, we will present a hard, but beautiful, problem from the USAMO.

13. Let n be a fixed positive integer. Denote by $f(n)$ the smallest k for which one can find a set $X \subset \mathbb{Z}^+$ of cardinality n with the property

that

$$s\left(\sum_{x\in Y} x\right) = k$$

for all nonempty subsets Y of X. Prove that $C_1 \lg n < f(n) < C_2 \lg n$ for some constants C_1 and C_2.

Gabriel Dospinescu and Titu Andreescu, USAMO 2005

Solution. We will prove that

$$\lfloor \lg(n+1) \rfloor \leq f(n) \leq 9 \lg \left\lceil \frac{n(n+1)}{2} + 1 \right\rceil,$$

which is enough to establish our claim. Let l be the smallest integer such that

$$10^l - 1 \geq \frac{n(n+1)}{2}.$$

Consider the set $X = \{j(10^l - 1) : 1 \leq j \leq n\}$. By the previous inequality and our first statement, it follows that

$$s\left(\sum_{x\in Y} x\right) = 9l$$

for all nonempty subsets Y of X, so $f(n) \leq 9l$ and the RHS is proved. Let m be the largest integer such that $n \geq 10^m - 1$. We will use the following well-known

Lemma. *Any set $M = \{a_1, a_2, ..., a_m\}$ has a nonempty subset whose sum of elements is divisible by m.*

Proof. Consider the sums a_1, $a_1 + a_2$,..., $a_1 + a_2 + ... + a_m$. If one of then is a multiple of m, them we are done. Otherwise, there are 2 of them congruent mod m, say the i-th and the j-th. Then, $m | a_{i+1} + a_{i+2} + ... + a_j$ so we are done.

From the lemma, it follows that any set X with n elements has a subset, say Y, whose sum of elements is divisible by $10^m - 1$. By our

second statement, it follows that

$$s\left(\sum_{x\in Y} x\right) \geq m \Rightarrow f(n) \geq m,$$

and the proof is complete.

The last solved problem is one we consider to be very hard, and which uses different techniques than the ones we have mentioned so far.

14. Let $a, b \in \mathbb{Z}^+$ such that $s(an) = s(bn)$ for all $n \in \mathbb{Z}^+$. Prove that $\lg a - \lg b \in \mathbb{Z}$.

Adrian Zahariuc and Gabriel Dospinescu

Solution. We start with an observation. If $(\max\{a, b\}, 10) = 1$, then the problem becomes trivial. Suppose $a = \max\{a, b\}$. Then, by Euler's theorem, $a|10^{\varphi(a)} - 1$, so there is an n such that $an = 10^{\varphi(a)} - 1$ and since numbers consisting only of 9-s have the sum of digits greater than all previous numbers, it follows that $an = bn$, so $a = b$.

Let us solve now the harder problem. For any $k \geq 1$, there is a n_k such that $10^k \leq an_k \leq 10^k + a - 1$. It follows that $s(an_k)$ is bounded, so $s(bn_k)$ is bounded as well. On the other hand,

$$10^k \frac{b}{a} \leq bn_k < 10^k \frac{b}{a} + b,$$

so, for sufficiently large p, the first (nonzero) digits of b/a are exactly the same as the first p digits of bn_k for large enough k. This means the the sum of the first p digits of b/a is bounded, which could only happen when this fraction has finitely many decimals. Analogously, we can prove the same result about a/b.

Let $a = 2^x 5^y m$ and $b = 2^z 5^t m'$, where $(m, 10) = (m', 10)$=1. It follows that $m|m'$ and $m'|m$, so $m = m'$. Now, we can write the hypothesis as

$$s(2^z 5^u mn 2^{c-x} 5^{c-y}) = s(2^x 5^y mn 2^{c-x} 5^{c-y}) = s(mn), \forall c \geq \max\{x, y\}$$

Now, if $p = max\{z+c-x, u+c-y\} - min\{z+c-x, u+c-y\}$, we get that there is a $k \in \{2,5\}$ such that $s(mn) = s(mk^p n)$ for all $n \in \mathbb{Z}^+$. It follows that

$$s(m) = s(k^p m) = s(k^{2p} m) = s(k^{3p} m) = ...$$

Let $t = a^p$, so $\lg t \in \mathbb{R} - \mathbb{Q}$ unless $p = 0$. Now, we will use the following:

Lemma. *If $\lg t \in \mathbb{R} - \mathbb{Q}$, then for any sequence of digits, there is a $n \in \mathbb{Z}^+$, such that $t^n m$ starts with the selected sequence of digits.*

Proof. If we will prove that $\{\{\lg t^n m\} : n \in \mathbb{Z}^+\}$ is dense in $(0,1)$, then we are done. But $\lg t^n m = n \lg t + m$ and by Kronecker's theorem $\{\{n \lg t\} : n \in \mathbb{Z}^+\}$ is dense in $(0,1)$, so the proof is complete.

The lemma implies the very important result that $s(t^n m)$ is unbounded for $p \neq 0$, which is a contradiction. So $p = 0$ and hence $z + c - x = u + c - y$, so $a = 10^{x-z} b$ and the proof is complete.

This problem can be nicely extended to any base. The proof of the general case is quite similar, although there are some very important differences.

The upmetioned methods are just a point to start from in solving such problems since the variety of problems involving sum of digits is very large. The techniques are useful only when they are applied creatively. Finally, we invite our readers to solve this proposed problems:

Proposed Problems

1. Prove that among any 39 there is one whose sum of digits is divisible by 11.

USSR, 1961

2. Prove that among any 18 consecutive 2-digit numbers there is at least one Niven number.

Tournament of Towns, Training, 1997

3. Are there positive integers n such that $s(n) = 1,000$ and $s(n^2) = 1,000,000$?

USSR, 1985

4. Prove that for any positive integer n there are infinitely many numbers m which do not contain any zero, such that $s(n) = s(mn)$.

USSR, 1970

5. Find all x such that $s(x) = s(2x) = s(3x) = ... = s(x^2)$.

Kurschak, 1989

6. Are there arbitrarily long arithmetical sequences whose terms have the same sum of digits? What about infinite aritmetical sequences?

***

7. Prove that

$$\lim_{n\to\infty} s(2^n) = \infty.$$

***

8. Are there $p \in \mathbb{Z}[X]$ such that

$$\lim_{n\to\infty} s(p(n)) = \infty?$$

***

9. Prove that there are arbitrarily long sequences of consecutive numbers which do not contain any Niven number.

***

10. We start with a perfect number, different form 6 (which is equal to the sum of its divisors, except itself), and calculate its sum of digits. Then, we calculate the sum of digits of the new number and so on. Prove that we will eventually get 1.

***

11. Prove that there are infinitely many $x \in \mathbb{Z}^+$ such that

$$s(x) + s(x^2) = s(x^3).$$

Gabriel Dospinescu

12. a, b, c and d are primes such that $2 < a \leq c$ and $a \neq b$. We now that there is one $M \in \mathbb{Z}$ such that the numbers $an + b$ and $cn + d$ have the same sum of digits for any $n > M$ and base between 2 and $a - 1$. Prove that $a = c$ and $b = d$.

Gabriel Dospinescu

13. Let $(a_n)_{n \geq 1}$ be a sequence such that $s(a_n) \geq n$. Prove that for any n, we have

$$\frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n} < 3.2$$

Can we replace 3.2 by 3?

Laurentiu Panaitopol

14. Prove that one can find $n_1 < n_2 < ... < n_{50}$ such that

$$n_1 + s(n_1) = n_2 + s(n_2) = ... = n_{50} + s(n_{50})$$

Poland, 1999

15. Study whether we can choose the numbers in the previous problem such that $n_2 - n_1 = n_3 - n_2 = ... = n_{50} - n_{49}$.

Gabriel Dospinescu

16. Define $f(n) = n + s(n)$. A number m is called *special* if there is a k such that $f(k) = m$. Prove that there are infinitely many special numbers $10^n + b$ iff $b - 1$ is special.

Christopher D. Long

17. Find a Niven number with 100 digits.

Sankt Petersburg, 1990

18. Let S be a set such that for any $\alpha \in \mathbb{R}-\mathbb{Q}$, there is a number $n \in \mathbb{Z}^+$ such that $\lfloor \alpha^n \rfloor \in S$. Prove that S contains numbers with arbitrarily large sum of digits.

Gabriel Dospinescu

19. Let a be a positive integer such that $s(a^n + n) = 1 + s(n)$ for any $n > M$, where M is given. Prove that a is a power of 10.

Gabriel Dospinescu

20. Let $k \in \mathbb{Z}^+$. Prove that there is a positive integer m such that the equation $n + s(n) = m$ has exactly k solutions.

Mihai Manea, Romanian IMO TST, 2003

21. Are there 19 positive integers with the same sum of digits, which add up to 1999?

Rusia, 1999

22. Let $a, b > 0$. Prove that the sequence $s(\lfloor an + b \rfloor)$ contains a constant subsequence.

Laurentiu Panaitopol, Romanian IMO TST, 2002

23. If $s(n) = 100$ and $s(44n) = 800$, find $s(3n)$.

Rusia, 1999

24. Find the smallest positive integer which can be expressed at the same time as the sum of 2002 numbers with the same sum of digits and as the sum of 2003 numbers with the same sum of digits.

Rusia, 2002

25. Prove that

$$\sum_{n \geq 1} \frac{s(n)}{n(n+1)} = \frac{10}{9} \ln 10.$$

O. Shallit

Open Questions

1. For any $a > 1$, we have

$$\lim_{n\to\infty} s(a^n) = \infty$$

(proved only for a couple of values, namely 2, 4, 6, 8).

2. Is it true that

$$\lim_{n\to\infty} \frac{s(n!)}{n \ln\ln n} = \infty?$$

3. Let $a, b \in \mathbb{Z}^+$ such that $s(a^n) = s(b^n)$ for all $n \in \mathbb{Z}^+$. Prove that $\lg a - \lg b \in \mathbb{Z}$.

4. Prove that for any n, there are $a, b \in \mathbb{Z}$ such that $\lg a - \lg b \notin \mathbb{Z}$ with the property that $s(a^k) = s(b^k)$ for any $k \in \{1, 2, ..., n\}$.

5. Is it true that

$$\lim_{n\to\infty} \frac{s(2^n)}{\ln n} = \infty?$$

ANALYSIS AGAINST NUMBER THEORY?

"Olympiad problems can be solved without the aid of analysis or linear algebra" is a sentence always heard when speaking about the elementary problems given in contests. This is true, but the true nature and essence of some of these problems is in analysis and this is the reason for which such type of problems are always the highlight of a contest. Their elementary solutions are very tricky and sometimes extremely difficult, while using analysis they can be solved quickly. Well, of course, "quickly" only if you see the sequence that hides after each problem. Practically, our aim is to exhibit convergent sequences formed by integer numbers. These sequences must become constant and from here the problem is much easier. The difficulty is in finding those sequences. Sometimes, this is easy, but most of the time this is a very difficult task. We will develop our skills in "hunting" these sequences by solving first some easy problems (anyway, "easy" is a relative concept: try to solve them elementary and you will see if they really are easy) and after that we will attack the chestnuts.

As usual, we begin with a classic beautiful problem, which has lots of applications and extensions.

Example 1. Let $f, g \in Z[X]$ be two non-constant polynomials such that $f(n)|g(n)$ for an infinite natural numbers n. Prove that f divides g in $Q[X]$.

Solution. Indeed, we need to look at the remainder of g when divided with f in $Q[X]$! Let us write $g = fh + r$, were h, r are polynomials from $Q[X]$ and $\deg r < \deg f$. Now, multiplying by the common denominator of all coefficients of polynomials h, r, the hypothesis becomes: there exists two infinite sequences $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ of integer numbers and a positive integer N such that $b_n = N\dfrac{r(a_n)}{f(a_n)}$ (we could have some

problems with the roots of f, but they are in finite number and the sequence $(a_n)_{n\geq 1}$ tends to infinity, so from a certain point, a_n is not a root of f). Since $\deg r < \deg f$, it follows that $\dfrac{r(a_n)}{f(a_n)} \to 0$, thus $(b_n)_{n\geq 1}$ is a sequence of integer numbers that tends to 0. This implies that from a certain point, all the terms of these sequence are 0. Well, this is the same as $r(a_n) = 0$ from a certain point n_0, which is practically the same thing with $r = 0$ (don't forget that any non-zero polynomial has only a finite number of roots!). But in this moment the problem is solved.

The next problem we are going to discuss is a particular case of a much more general and classical result: if f is a polynomial with integer coefficients, $k > 1$ is a natural number and $\sqrt[k]{f(n)} \in Q$ for all natural numbers n, then there exists a polynomial $g \in Q[X]$ such that $f(x) = g^k(x)$. We won't discuss here this general result (the reader will find a proof in the chapter about arithmetic properties of polynomials).

Example 2. Let $a \neq 0, b, c$ be integers such that for any natural number n, the number $an^2 + bn + c$ is a perfect square. Prove that there exist $x, y \in Z$ such that $a = x^2$, $b = 2xy$, $c = y^2$.

Solution. Let us begin by writing $an^2 + bn + c = x_n^2$ for a certain sequence of nonnegative integers $(x_n)_{n\geq 1}$. We could expect that $x_n - n\sqrt{a}$ converges. And yes, it converges, but it's not a sequence of integers, so the convergence is useless. In fact, it's not that useless, but we need another sequence. The easiest way is to work with $(x_{n+1} - x_n)_{n\geq 1}$, since this sequence certainly converges to $\sqrt{a}$ (the reader has already noticed why it wasn't useless to find that $x_n - n\sqrt{a}$ is convergent; we used this to establish the convergence of $(x_{n+1} - x_n)_{n\geq 1}$). This time, the sequence is formed by integer numbers, so it is constant from a certain point. Thus, we can find a number M such that if $n \geq M$ then $x_{n+1} = x_n + \sqrt{a}$. Thus, a must be a perfect square, let us say $a = x^2$. A simple induction shows that $x_n = x_M + (n - M)x$ and so $(x_M - Mx + nx)^2 = x^2n^2 + bn + c$ for

all $n \geq M$. A simple identification of coefficients finishes the solution, since we can take $y = x_M - Mx$.

The following problem is based on the same idea, but it really doesn't seem to be related with mathematical analysis. In fact, as we will see, it is closely related to the concept of convergence.

Example 3. Let $a, b, c > 1$ be positive integers such that for any positive integer n there exists a positive integer k such that $a^k + b^k = 2c^n$. Prove that $a = b$.

Laurentiu Panaitopol

Solution. What does the problem say in fact? That we can find a sequence of positive integers $(x_n)_{n\geq 1}$ such that $a^{x_n} + b^{x_n} = 2c^n$. What could be the convergent sequence here? We see that $(x_n)_{n\geq 1}$ is appreciatively kn for a certain constant k. Thus, we could expect that the sequence $(x_{n+1} - x_n)_{n\geq 1}$ converges. Let us see if this is true or not. From where could we find $x_{n+1} - x_n$? Certainly, by writing that $a^{x_{n+1}} + b^{x_{n+1}} = 2c^{n+1}$ and after that considering the value $\dfrac{a^{x_{n+1}} + b^{x_{n+1}}}{a^{x_n} + b^{x_n}} = c$. Now, let us suppose that $a > b$ and let us write $\dfrac{a^{x_{n+1}} + b^{x_{n+1}}}{a^{x_n} + b^{x_n}} = c$ in the form

$$a^{x_{n+1}-x_n} \frac{1 + \left(\dfrac{b}{a}\right)^{x_{n+1}}}{1 + \left(\dfrac{b}{a}\right)^{x_n}} = c,$$

from where it is easy to see that $a^{x_{n+1}-x_n}$ converges to c. Why is it so easy? It would be easy if we could show that $x_n \to \infty$. Fortunately, this is immediate, since $2a^{x_n} > 2c^n \Rightarrow x_n > n \log_a c$. So, we found that $a^{x_{n+1}-x_n}$ converges. Being a sequence of integer numbers, it must become constant, so there exist M such that for all $n \geq M$ we have

$a^{x_{n+1}-x_n} = c$. This means that for all $n \geq M$ we also have

$$\frac{1+\left(\frac{b}{a}\right)^{x_{n+1}}}{1+\left(\frac{b}{a}\right)^{x_n}} = 1.$$

But this is impossible, since $a > b$. Thus, our assumption was wrong and we must have $a \leq b$. Due to symmetry in a and b, we conclude that $a = b$.

Another easy example is the following problem, in which finding the right convergent sequence of integers in not difficult at all. But, attention must be paid to details!

Example 4. Let $a_1, a_2, \ldots, a_k$ be positive real numbers such that at least one of them is not an integer. Prove that there exits infinitely many natural numbers n such that n and $[a_1 n] + [a_2 n] + \cdots + [a_k n]$ are relatively prime.

Gabriel Dospinescu, Arhimede Magazine

Solution. Of course, the solution of such a problem is better to be indirect. So, let us assume that there exists a number M such that for all $n \geq M$ the numbers n and $[a_1 n] + [a_2 n] + \cdots + [a_k n]$ are not relatively prime. Now, what are the most efficient numbers n to be used? Yes, they are the prime numbers, since if n is prime and it is not relatively prime with , $[a_1 n] + [a_2 n] + \cdots + [a_k n]$, then it must divide $[a_1 n] + [a_2 n] + \cdots + [a_k n]$. This suggests us to consider the sequence of prime numbers $(p_n)_{n \geq 1}$. Since this sequence is infinite, there is a number N such that if $n \geq N$ then $p_n \geq M$. According to our assumption, this implies that for all $n \geq N$ there exist a natural number x_n such that $[a_1 p_n] + [a_2 p_n] + \cdots + [a_k p_n] = x_n p_n$. And now, you have already guessed what is the convergent sequence! Yes, it is $(x_n)_{n \geq N}$. This is obvious, since $\dfrac{[a_1 p_n] + [a_2 p_n] + \cdots + [a_k p_n]}{p_n}$ tends to $n \geq N a_1 + a_2 + \cdots + a_k$.

Thus, we can find a number P such that for $x_n = a_1 + a_2 + \cdots + a_k$ for all $n \geq P$. But this is the same as $\{a_1 p_n\} + \{a_2 p_n\} + \cdots + \{a_k p_n\} = 0$. Of course, this says that $a_i p_n \in Z$ for all $i = \overline{1,k}$ and $n \geq P$. Well, the conclusion is immediate: $a_i \in Z$ for all $i = \overline{1,k}$, which contradicts the hypothesis. Consequently, we were wrong again and the problem statement is right!

Step by step, we start to have some experience in "guessing" the sequences. Thus, it's time to solve some more difficult problems. The next problem we are going to discuss may seem obvious after reading the solution. In fact, it's just that type of problem whose solution is very short, but very hard to find.

Example 5. Let $a, b \in Z$ such that for all natural numbers n the number $a \cdot 2^n + b$ is a perfect square. Prove that $a = 0$.

Poland TST

Solution. Again, we argue by contradiction. Suppose that $a \neq 0$. Then, of course, $a > 0$, otherwise for large values of n the number $a \cdot 2^n + b$ is negative. According to the hypothesis, there exists a sequence of positive integers $(x_n)_{n \geq 1}$ such that for all natural numbers n, $x_n = \sqrt{a \cdot 2^n + b}$. Then, a direct computation shows that $\lim\limits_{n \to \infty} (2x_n - x_{n+2}) = 0$. This implies the existence of a natural number N such that for all $n \geq P$ we have $2x_n = x_{n+2}$. But $2x_n = x_{n+2}$ is equivalent with $b = 0$. Then, a and $2a$ are both perfect squares, which is impossible for $a \neq 0$. This shows, as usually, that our assumption was wrong and indeed $a = 0$.

A classical result of Schur states that for any non-constant polynomial f with integer coefficients, the set of prime numbers dividing at least one of the numbers $f(1), f(2), f(3), \ldots$ is infinite. The following problem is a generalization of this result.

Example 6. Suppose that f is a polynomial with integer coefficients and (a_n) is a strictly increasing sequence of natural numbers such that

$a_n \leq f(n)$ for all n. Then the set of prime numbers dividing at least one term of the sequence is infinite.

Solution. The idea is very nice: for any finite set of prime numbers $p_1, p_2, \ldots, p_r$ and any $k > 0$, we have

$$\sum_{\alpha_1,\alpha_2,\ldots,\alpha_N \in Z_+} \frac{1}{p_1^{k\alpha_1} \ldots p_N^{k\alpha_N}} < \infty.$$

Indeed, it suffices to remark that we have actually

$$\sum_{\alpha_1,\alpha_2,\ldots,\alpha_N \in Z_+} \frac{1}{p_1^{k\alpha_1} \ldots p_N^{k\alpha_N}} \prod_{j=1}^{N} \sum_{i \geq 0} \frac{1}{p_j^{ki}} = \prod_{j=1}^{n} \frac{p_j^k}{p_j^k - 1}.$$

On the other hand, by taking $k = \dfrac{1}{2\deg(f)}$ we clearly have

$$\sum_{n \geq 1} \frac{1}{(f(n))^k} = \infty.$$

Thus, if the conclusion of the problem is not true, we can find $p_1, p_2, \ldots, p_r$ such that any term of the sequence is of the form $p_1^{k\alpha_1} \ldots p_N^{k\alpha_N}$ and thus

$$\sum_{n \geq 1} \frac{1}{a_n^k} \leq \sum_{\alpha_1,\alpha_2,\ldots,\alpha_N \in Z_+} \frac{1}{p_1^{k\alpha_1} \ldots p_N^{k\alpha_N}} < \infty.$$

On the other hand, we also have

$$\sum_{n \geq 1} \frac{1}{a_n^k} \geq \sum_{n \geq 1} \frac{1}{(f(n))^k} = \infty,$$

which is clearly impossible.

The same idea is employed in the following problem.

Example 7. Let $a, b \geq 2$ be natural numbers. Prove that there is a multiple of a which contains all digits $0, 1, \ldots, b-1$ when written in base b.

Adapted after a Putnam problem

Solution. Let's suppose the contrary. Then any multiple of a misses at least a digit when written in base b. Since the sum of inverses of all multiples of a diverges (because $1+\frac{1}{2}+\frac{1}{3}+\cdots=\infty$), it suffices to show that the sum of inverses of all natural numbers missing at least one digit in base b is convergent and we will reach a contradiction. But of course, it suffices to prove it for a fixed (but arbitrary) digit j. For any $n \geq 1$, there are at most $(b-1)^n$ numbers which have n digits in base b, all different from j. Thus, since each one of them is at least equal to b^{n-1}, the sum of inverses of numbers that miss the digit j when written in base b is at most equal to $\sum_n b\left(\frac{b-1}{b}\right)^n$, which converges. The conclusion follows.

We return to classical problems to discuss a beautiful problem, that appeared in the Tournament of the Towns in 1982, in a Russian Team Selection Test in 1997 and also in the Bulgarian Olympiad in 2003. It's beauty explains probably the preference for this problem.

Example 8. Let $f \in Z[X]$ be a polynomial with leading coefficient 1 such that for any natural number n the equation $f(x) = 2^n$ has at least one natural solution. Prove that $\deg f = 1$.

Solution. So, the problem states that there exists a sequence of positive integers $(x_n)_{n\geq 1}$ such that $f(x_n) = 2^n$. Let us suppose that $\deg f = k > 1$. Then, for large values of x, $f(x)$ behaves like x^k. So, trying to find the right convergent sequence, we could try first to "think big": we have $x_n^k \cong 2^n$, that is for large n, x_n behaves like $2^{\frac{n}{k}}$. Then, a good possibly convergent sequence could be $x_{n+k} - 2x_n$. Now, the hard part: proving that this sequence is indeed convergent. First, we will show that $\frac{x_{n+k}}{x_n}$ converges to 2. This is easy, since the relation

$f(x_{n+k}) = 2^k f(x_n)$ implies

$$\frac{f(x_{n+k})}{x_{n+k}^k}\left(\frac{x_{n+k}}{x_n}\right)^k = 2^k \cdot \frac{f(x_n)}{x_n^k}$$

and since

$$\lim_{x\to\infty}\frac{f(x)}{x^k} = 1 \text{ and } \lim_{n\to\infty} x_n = \infty$$

(do you see why?), we find that indeed

$$\lim_{n\to\infty}\frac{x_{n+k}}{x_n} = 2.$$

We will see that this will help us a lot. Indeed, let us write

$$f(x) = x^k + \sum_{i=0}^{k-1} a_i x^i.$$

Then $f(x_{n+k}) = 2^k f(x_n)$ can be also written

$$x_{n+k} - 2x_n = \frac{\sum_{i=0}^{k-1} a_i(2^k x_n^i - x_{n+k}^i)}{\sum_{i=0}^{k-1}(2x_n)^i x_{n+k}^{k-i-1}}$$

But from the fact that $\lim_{n\to\infty}\frac{x_{n+k}}{x_n} = 2.$ it follows that the right-hand side in the above relation is also convergent. So, $(x_{n+k} - 2x_n)_{n\geq 1}$ is convergent and it follows that there exist M, N such that for all $n \geq M$ we have $x_{n+k} = 2x_n + N$. But now the problem is almost done, since the last result combined with $f(x_{n+k}) = 2^k f(x_n)$ yields $f(2x_n + N) = 2^k f(x_n)$ for $n \geq M$, that is $f(2x + N) = 2^k f(x)$. So, an arithmetical property of the polynomial turned into an algebraic one using analysis. This algebraic property helps us to immediately solve the problem. Indeed, we see that if z is a complex root of f, then $2z + N, 4z + 3N, 8z + 7N, \ldots$ are all roots of f. Since f is non-zero, this sequence must be finite and this can happen only for $z = -N$. Since $-N$ is the only root of f, we deduce that $f(x) = (x + N)^k$. But since the equation $f(x) = 2^{2k+1}$ has

natural roots, we find that $2^{\frac{1}{k}} \in N$, which implies, contradiction. Thus, our assumption was wrong and $\deg f = 1$.

The idea of the following problem is so beautiful, that after reading the solution the reader will have the impression that the problem is trivial. Wrong! The problem is really difficult and to make again an experiment, we will ask the reader to struggle a lot before reading the solution. He will see the difficulty.

Example 9. Let $\pi(n)$ be the number of prime numbers smaller than or equal to n. Prove that there exist infinitely many numbers n such that $\pi(n)|n$.

AMM

Solution. First, let us prove the following result, which is the key of the problem.

Lemma. *For any increasing sequence of positive integers* $(a_n)_{n\geq 1}$ *such that* $\lim\limits_{n\to\infty} \dfrac{a_n}{n} = 0$, *the sequence* $\left(\dfrac{n}{a_n}\right)_{n\geq 1}$ *contains all natural numbers. In particular, for infinitely many* n *we have that* n *divides* a_n.

Proof. Even if it seems unbelievable, this is true and moreover the proof is extremely short. Let $m \geq 1$ be a natural number. Consider the set $A = \left\{ n \geq 1 | \ \dfrac{a_{mn}}{mn} \geq \dfrac{1}{m} \right\}$. This set contains and it is bounded, since $\lim\limits_{n\to\infty} \dfrac{a_{mn}}{mn} = 0$. Thus it has a maximal element k. If $\dfrac{a_{mk}}{mk} = \dfrac{1}{m}$, then m is in the sequence $\left(\dfrac{n}{a_n}\right)_{n\geq 1}$. Otherwise, we have $a_{m(k+1)} \geq a_{mk} \geq k+1$, which shows that $k+1$ is also in the set, contradiction with the maximality of k. The lemma is proved.

Thus, all we need to show is that $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n} = 0$. Fortunately, this is well-known and not difficult to prove. There are easier proofs than the following one, but we prefer to deduce it from a famous and beautiful result of Erdos.

Erdos's theorem. *We have* $\prod_{\substack{p\leq n\\ p\,prime}} p \leq 4^n$.

The proof of this result is magnificient. The proof is by induction. For small values of n it is clear. Now, assume the inequality true for all values smaller than n and let us prove that $\prod_{\substack{p\leq n\\ p\,prime}} p \leq 4^n$. If $n$is even, we have nothing to prove, since

$$\prod_{\substack{p\leq n\\ p\,prime}} = \prod_{\substack{p\leq n-1\\ p\,prime}} p \leq 4^{n-1} < 4^n.$$

Now, assume that $n = 2k+1$ and consider the binomial coefficient

$$\binom{2k+1}{k} = \frac{(k+2)\ldots(2k+1)}{k!}.$$

A simple application of the fact that

$$2^{2k+1} = \sum_{i\geq 0} \binom{2k+1}{i}$$

shows that

$$\binom{2k+1}{k} \leq 4^k.$$

Thus, using the inductive hypothesis, we find that

$$\prod_{\substack{p\leq n\\ p\,prime}} p \leq \prod_{\substack{p\leq k+1\\ p\,prime}} p \prod_{\substack{k+2\leq p\leq 2k+1\\ p\,prime}} p \leq 4^{k+1}\cdot 4^k = 4^n.$$

Now, the fact that $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$ is trivial. Indeed, fix $k \geq 1$. We have for all large n the inequality

$$n \lg 4 \geq \sum_{\substack{k\leq p\leq n\\ p\,prime}} \lg p \geq \lg k(\pi(n) - \pi(k)),$$

which shows that

$$\pi(n) \leq \frac{\pi(k)}{n} + \frac{\lg 4}{\lg k}.$$

This shows of course that $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$. The problem is solved.

It is time now for the last problem, which is, as usual, very hard. We don't exaggerate if we say that the following problem is exceptionally difficult.

Example 10. Let $a, b > 1$ be natural numbers such that for any natural number n, $a^n - 1 | b^n - 1$. Prove that b is a natural power of a.

Marius Cavachi, AMM

Solution. This time we will be able to find the right convergent sequence only after some double recurrences. Let us see. So, initially we are given that there exists a sequence of positive integers $(x_n^1)_{n\geq 1}$ such that $x_n^1 = \frac{b^n - 1}{a^n - 1}$ Then, $x_n^1 \cong \left(\frac{b}{a}\right)^n$ for large values of n. So, we could expect that the sequence $(x_n^2)_{n\geq 1}$, $x_n^2 = bx_n^1 - ax_{n+1}^2$ is convergent. Unfortunately,

$$x_n^2 = \frac{b^{n+1}(a-1) - a^{n+1}(b-1) + a - b}{(a^n - 1)(a^{n+1} - 1)},$$

which is not necessarily convergent. But... if we look again at this sequence, we see that for large values of n it grows like $\left(\frac{b}{a^2}\right)^n$, so much slower. And this is the good idea: repeat this procedure until the final sequence behaves like $\left(\frac{b}{a^{k+1}}\right)^n$, where k is chosen such that $a^k \leq b < a^{k+1}$. Thus, the final sequence will converge to 0. Again, the hard part has just begun, since we have to prove that if we define $x_n^{i+1} = bx_n^i - a^i x_{n+1}^i$ then $\lim_{n\to\infty} x_n^{k+1} = 0$. This isn't easy at all. The idea is to compute x_n^3 and after that to prove the following statement: for any $i \geq 1$ the sequence $(x_n^i)_{n\geq 1}$ has the form

$$\frac{c_i b^n + c_{i-1} a^{(i-1)n} + \cdots + c_1 a^n + c_0}{(a^{n+i-1} - 1)(a^{n+i-2} - 1)\ldots(a^n - 1)}$$

for some constants $c_0, c_1, \ldots, c_i$. Proving this is not so hard, the hard part was to think about it. How can we prove the statement otherwise than by

induction? And induction turns out to be quite easy. Supposing that the statement is true for i, then the corresponding statement for $i+1$ follows from $x_n^{i+1} = bx_n^i - a^i x_{n+1}^i$ directly (note that to make the difference, we just have to multiply the numerator $c_i b^n + c_{i-1} a^{(i-1)n} + \cdots + c_1 a^n + c_0$ with b and $a^{n+i} - 1$. Then, we proceed in the same way with the second fraction and the term $b^{n+1} a^{n+i}$ will vanish). So, we have found a formula which shows that as soon as $a^i > b$ we have $\lim_{n\to\infty} x_n^i = 0$. So, we have deduced that $\lim_{n\to\infty} x_n^{k+1} = 0$. Another step of the solution is to take the minimal index j such that $\lim_{n\to\infty} x_n^j = 0$. Obviously, $j > 1$ and the recurrence relation $x_n^{i+1} = bx_n^i - a^i x_{n+1}^i$ shows that $x_n^i \in Z$ for all n, i. Thus, there exists M such that whenever $n \geq M$ we have $x_n^j = 0$. This is the same as $bx_n^{j-1} = a^j x_{n+1}^{j-1}$ for all $n \geq M$, which implies $x_n^{j-1} = \left(\frac{b}{a^j}\right)^{n-M} x_M^{j-1}$ for all $n \geq M$. Let us suppose that b is not a multiple of a. Since $\left(\frac{b}{a^j}\right)^{n-M} x_M^{j-1} \in Z$ for all $n \geq M$, we must have $x_M^{j-1} = 0$ and so $x_n^{j-1} = 0$ for $n \geq M$, which means $\lim_{n\to\infty} x_n^j = 0$. But this contradicts the minimality of j. Since we have reached a contradiction, we must have $a|b$. Let us write $b = ca$. Then, the relation $a^n - 1|b^n - 1$ implies $a^n - 1|c^n - 1$. And now are finally done. Why? We have just seen that $a^n - 1|c^n - 1$ for all $n \geq 1$. But our previous argument applied for c instead of b shows that $a|c$. Thus, $c = ad$ and we deduce again that $a|d$. Since this process cannot be infinite, b must be a power of a.

It worth saying that there exist an even stronger result: it is enough to suppose that $a^n - 1|b^n - 1$ for an infinite number n, but this is a much more difficult problem. It follows from a result found by Bugeaud, Corvaja and Zannier in 2003:

If $a, b > 1$ are multiplicatively independent in Q^* (that is $\log_a b \notin Q$), then for any $\varepsilon > 0$ there exists $n_0 = n_0(a, b, \varepsilon)$ such that $gcd(a^n - 1, b^n -$

1) $< 2^{\varepsilon n}$ for all $n \geq n_0$. Unfortunately, the proof is too advanced to be presented here.

Problems for training

1. Let $f \in Z[X]$ be a polynomial of degree k such that for all $n \in \mathbb{N}$ we have $\sqrt[k]{f(n)} \in Z$. Prove that there exists integer numbers a, b such that $f(x) = (ax + b)^k$.

2. Find all arithmetic progressions of positive integers $(a_n)_{n \geq 1}$ such that for all $n \geq 1$ the number $a_1 + a_2 + \cdots + a_n$ is a perfect square.

Laurentiu Panaitopol, Romanian Olympiad 1991

3. Let p be a polynomial with integer coefficients such that there exists a sequence of pair wise distinct positive integers $(a_n)_{n \geq 1}$ such that $p(a_1) = 0$, $p(a_2) = a_1$, $p(a_3) = a_2, \ldots$. Find the degree of this polynomial.

Tournament of the Towns, 2003

4. Let $f, g : \mathbb{N}^* \to \mathbb{N}^*$ two functions such that $|f(n) - n| \leq 2004\sqrt{n}$ and $n^2 + g^2(n) = 2f^2(n)$. Prove that if f or g is surjective, then these functions have infinitely many fixed points.

Gabriel Dospinescu, Moldova TST 2004

5. Let a, b be natural numbers such that for any natural number n, the decimal representation of $a + bn$ contains a sequence of consecutive digits which form the decimal representation of n (for example, if $a = 600$, $b = 35$, $n = 16$ we have $600 + 16 \cdot 35 = 1160$). Prove that b is a power of 10.

Tournament of the Towns, 2002

6. Let $a, b > 1$ be positive integers. Prove that for any given $k > 0$ there are infinitely many numbers n such that $\varphi(an + b) < kn$, where φ is the Euler totient function.

Gabriel Dospinescu

7. Let b an integer at least equal to 5 and define the number $x_n = \underbrace{11\ldots1}_{n-1}\underbrace{22\ldots2}_{n}5$ in base b. Prove that x_n is a perfect square for all sufficiently large n if and only if $b = 10$.

Laurentiu Panaitopol, IMO Shortlist 2004

8. Find all triplets of integer numbers a, b, c such that for any positive integer n, $a \cdot 2^n + b$ is a divisor of $c^n + 1$.

Gabriel Dospinescu

11. Suppose that a is a real number such that all numbers $1^a, 2^a, 3^a, \ldots$ are integers. Then prove that a is also integer.

Putnam

12. Find all complex polynomials f having the property: there exists $a \geq 2$ a natural number such that for all sufficiently large n, the equation $f(x) = a^{n^2}$ has at least a positive rational solution.

Gabriel Dospinescu, Revue de Mathematiques Speciales

13. Let f be a complex polynomial having the property that for all natural number n, the equation $f(x) = n$ has at least a rational solution. Then f has degree at most 1.

Mathlinks Contest

14. Let A be a set of natural numbers, which contains at least one number among any 2006 consecutive natural numbers and let f a non-constant polynomial with integer coefficients. Prove that there exists a number N such that for any $n \geq N$ there are at least $\sqrt{\ln \ln n}$ different prime numbers dividing the number $\prod_{\substack{N \leq k \leq n \\ k \in A}} f(k)$.

Gabriel Dospinescu

15. Prove that in any strictly increasing sequence of positive integers $(a_n)_{n\geq 1}$ which satisfies $a_n < 100n$ for all n, one can find infinitely many terms containing at least 1986 consecutive 1.

Kvant

16. Any infinite arithmetical progression contains infinitely many terms that are not powers of integers.

17. Find all a, b, c such that for all sufficiently large n, the number $a \cdot 4^n + b \cdot 6^n + c \cdot 9^n$ is a perfect square.

18. Let f, g two real polynomials of degree 2 such that for any real x, if $f(x)$ is integer, so is $g(x)$. Then there are integers m, n such that $g(x) = mf(x) + n$ for all x.

Bulgarian Olympiad

19. Try to generalize the preceding problem (this is for the die-hards!!!).

20. Find all pairs of natural numbers a, b such that for every positive integer n the number $an + b$ is triangular if and only if n is triangular.

After a Putnam problem

21. Let $(a_n)_{n\geq 1}$ be an infinite and strictly increasing sequence of positive integers such that for all $n \geq 2002$, $a_n | a_1 + a_2 + \cdots + a_{n-1}$. Prove that there exists n_0 such that for all $n \geq n_0$ we have $a_n = a_1 + a_2 + \cdots + a_{n-1}$.

Tournament of the Towns, 2002

22. Find all real polynomials such that the image of any repunit is also a repunit.

After a problem from Kvant

23. Fie doua multimi finite de numere reale pozitive cu proprietatea ca

$$\left\{\sum_{x\in A} x^n |\ n\in\mathbb{R}\right\}\subset\left\{\sum_{x\in B} x^n |\ n\in\mathbb{R}\right\}.$$

Sa se arate ca exista $k\in\mathbb{R}$ astfel incat $A=\{x^k|\ x\in B\}$.

Gabriel Dospinescu

QUADRATIC RECIPROCITY

For an odd prime p, define the function $\left(\frac{a}{p}\right) : Z \to \{-1, 1\}$ by $\left(\frac{a}{p}\right) = 1$ if the equation $x^2 = a$ has at least a solution in Z_p and, otherwise, $\left(\frac{a}{p}\right) = -1$. In the first case, we say that a is a quadratic residue modulo p, otherwise we say that it is a non quadratic residue modulo p. This function is called Legendre's symbol and plays a fundamental role in number theory. Perhaps the most remarkable result involving this symbol is Gauss's quadratic reciprocity law. This states that for different odd prime numbers p, q the following equality holds:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

This is a nontrivial result whose proof will be sketched later. Until then, we will unfold some easier properties of Legendre's symbol. First, let us present an useful theoretical (but not practical at all) way of computing $\left(\frac{a}{p}\right)$ due to Euler.

Theorem. *The following identity is true:*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

We will prove this result and many other simple remarks concerning quadratic residues in what follows. First, let us assume that $\left(\frac{a}{p}\right) = 1$ and consider x a solution of the equation $x^2 = a$ in Z_p. Using Fermat's theorem, we find that $a^{\frac{p-1}{2}} = x^{p-1} = 1 \pmod{p}$. Thus the equality $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$ holds for all quadratic residues a modulo p. In addition, for any quadratic residue we have $a^{\frac{p-1}{2}} = 1 \pmod{p}$. Now, we will prove that there are exactly $\frac{p-1}{2}$ quadratic residues in $Z_p \setminus \{0\}$. This will enable us to conclude that quadratic residues are precisely the

roots of the polynomial $X^{\frac{p-1}{2}} - 1$ and also that non quadratic residues are exactly the roots of the polynomial $X^{\frac{p-1}{2}} + 1$ (from Fermat's little theorem). Note that Fermat's little theorem implies that the polynomial $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$ has exactly $p-1$ roots in the field Z_p. But in a field, the number of different zeros of a polynomial cannot exceed its degree. Thus each of the polynomials $X^{\frac{p-1}{2}} - 1$ and $X^{\frac{p-1}{2}} + 1$ has at most $\frac{p-1}{2}$ zeros in Z_p. These two observations show that in fact each of these polynomials has exactly $\frac{p-1}{2}$ zeros in Z_p. Let us observe next that there are at least $\frac{p-1}{2}$ quadratic residues modulo p. Indeed, all numbers $i^2 \pmod p$ with $1 \leq i \leq \frac{p-1}{2}$ are quadratic residues and they are all different. This shows that there are exactly $\frac{p-1}{2}$ quadratic residues in $Z_p \setminus \{0\}$ and also proves Euler's criterion.

We have said that Euler's criterion is a very useful result. Indeed, it allows a very quick proof of the fact that $\left(\frac{a}{p}\right) : Z \to \{-1, 1\}$ is a group morphism. Indeed, we have

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \pmod p = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

The relation $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ shows that while studying Legendre's symbol, it suffices to focus on the prime numbers only. Also, the same Euler's criterion implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ whenever $a \equiv b \pmod p$.

It is now time to come back to Gauss's celebrated quadratic reciprocity law. First of all, we will prove a lemma (due to Gauss).

Lemma. *Let p be an odd prime and let $a \in Z$ such that $gcd(a, p) = 1$. If m is the number of positive integers x such that $x < \frac{p}{2}$ and $\frac{p}{2} < ax \pmod p < p$, then $\left(\frac{a}{p}\right) = (-1)^m$.*

Proof. Let $x_1, x_2, \ldots, x_m$ be those numbers x for which $x < \frac{p}{2}$ and $\frac{p}{2} < ax \pmod p < p$. Let $k = \frac{p-2}{2} - m$ and $y_1, \ldots, y_k$ all numbers smaller than $\frac{p}{2}$, different from $x_1, x_2, \ldots, x_m$.

Observe that

$$\prod_{x=1}^{\frac{p-1}{2}}(ax) = a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right)\left(\frac{p-1}{2}\right)! \pmod p.$$

On the other hand,

$$\prod_{x=1}^{\frac{p-1}{2}}(ax) = \prod_{ax \pmod p > \frac{p}{2}}(ax) \pmod p \prod_{ax \pmod p < \frac{p}{2}}(ax) \pmod p.$$

We clearly have

$$\prod_{ax \pmod p > \frac{p}{2}}(ax) \pmod p \prod_{ax \pmod p < \frac{p}{2}}(ax) \pmod p$$

$$= \prod_{i=1}^{m} ax_i \pmod p \prod_{j=1}^{k} ay_i \pmod p.$$

On the other hand, the numbers $p - ax_i \pmod p$ and $ay_i \pmod p$ give a partition of $1, 2, \ldots, \frac{p-1}{2} \pmod p$. Indeed, it suffices to prove that $p - ax_i \pmod p \neq ay_j \pmod p$, which is clearly true by the definition of $x_i, y_j < \frac{p}{2}$. Hence we can write

$$\prod_{i=1}^{m} ax_i \pmod p \prod_{j=1}^{k} ay_i \pmod p$$

$$= (-1)^m \prod_{i=1}^{m}(p - ax_i \pmod p) \prod_{j=1}^{k} ay_j \pmod p$$

$$\equiv (-1)^m \prod_{i=1}^{\frac{p-1}{2}} i \pmod p = (-1)^m \left(\frac{p-1}{2}\right)! \pmod p.$$

Combining these facts, we finally deduce that $\left(\frac{a}{p}\right) = (-1)^m$.

Using Gauss's lemma, the reader will enjoy proving the next two classical results.

Theorem. *The identity* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *holds for any odd prime number* p.

Theorem. (quadratic reciprocity law) *For any different odd primes* p, q, *the following identity holds:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Using this powerful arsenal, we are now able to solve some interesting problems. Most of them are merely direct applications of the above results, but we think that they are still worthy not necessarily because they appeared in various contests.

Example 1. Prove that the number $2^n + 1$ does not have prime divisors of the form $8k - 1$.

Vietnam TST 2004

Solution. Indeed, assume that p is a prime divisor of the form $8k-1$ that divides $2^n + 1$. Of course, if n is even, the contradiction is immediate, since in this case we would have $-1 \equiv (2^{\frac{n}{2}})^2 \pmod{p}$ and so $-1 = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right) = 1$. Now, assume that n is odd. Then $-2 \equiv (2^{\frac{n+1}{2}})^2 \pmod{p}$ and so $\left(\frac{-2}{p}\right) = 1$. This can be also written in the form $\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$, or $(-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}} = 1$. Fortunately, if p is of the form $8k - 1$ the later cannot hold and this is the contradiction that solves the problem.

Based on the same idea and with a bit more work, we arrive at the following result.

Example 2. Prove that for any positive integer n, the number $2^{3^n}+1$ has at least n prime divisors of the form $8k + 3$.

Solution. Using the result of the previous problem, we deduce that 2^n+1 does not have prime divisors of the form $8k+7$. We will prove that if n is odd, then it has no prime divisors of the form $8k+5$ either. Indeed, let p be a prime divisor of 2^n+1. Then $2^n \equiv -1 \pmod p$ and so $-2 \equiv (2^{\frac{n+1}{2}})^2 \pmod p$. Using the same argument as the one in the previous problem, we deduce that $\frac{p^2-1}{8}+\frac{p-1}{2}$ is even, which cannot happen if p is of the form $8k+5$.

Now, let us solve the proposed problem. We will assume $n>2$ (otherwise the verification is trivial). The essential observation is the identity:

$$2^{3^n}+1=(2+1)(2^2-2+1)(2^{2\cdot 3}-2^3+1)\ldots(2^{2\cdot 3^{n-1}}-2^{3^{n-1}}+1)$$

Now, we will prove that for all $1 \leq i<j \leq n-1$, $gcd(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1)=3$. Indeed, assume that p is a prime number dividing $gcd(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1)$ We will then have $p|2^{3^{i+1}}+1$. Thus,

$$2^{3^j} \equiv (2^{3^{i+1}})^{3^{j-i-1}} \equiv (-1)^{3^{j-i-1}} \equiv -1 \pmod p,$$

implying

$$0 \equiv 2^{2\cdot 3^j}-2^{3^j}+1 \equiv 1-(-1)+1 \equiv 3 \pmod p.$$

This cannot happen unless $p=3$. But since $v_3(gcd(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1))=1$ (as one can immediately check), it follows that

$$gcd(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1)=3$$

and the claim is proved.

It remains to show that each of the numbers $2^{2\cdot 3^i}-2^{3^i}+1$, with $1 \leq i \leq n-1$ has at least a prime divisor of the form $8k+3$ different from 3. It would follow in this case that $2^{3^n}+1$ has at least $n-1$ distinct prime divisors of the form $8k+3$ (from the previous remarks) and since it

is also divisible by 3, the conclusion would follow. Fix $i \in \{1, 2, \ldots, n-1\}$ and observe that any prime factor of $2^{2\cdot 3^i} - 2^{3^i} + 1$ is also a prime factor of $2^{3^n} + 1$ and thus, from the first remark, it must be of the form $8k+1$ or $8k+3$. Because $v_3(2^{2\cdot 3^i} - 2^{3^i} + 1) = 1$, it follows that if all prime divisors of $2^{2\cdot 3^i} - 2^{3^i} + 1$ except for 3 are of the form $8k+1$, then $2^{2\cdot 3^i} - 2^{3^i} + 1 \equiv 8 \pmod 8$, which is clearly impossible. Thus at least a prime divisor of $2^{2\cdot 3^i} - 2^{3^i} + 1$ is different from 3 and is of the form $8k+3$ and so the claim is proved. The conclusion follows.

At first glance, the following problem seems trivial. Far from being true! It is actually very tricky, because brute force will take us nowhere. In the framework of the above results, this should not be so difficult now.

Example 3. Find a number n between 100 and 1997 such that $n|2^n + 2$.

APMO, 1997

Solution. If we search for odd numbers, then we will certainly fail (actually, this result due to Sierpinski has been proved in the topic "Look at the exponent!"). So let us search for even numbers. The first step would be choosing $n = 2p$, for some prime number p. Unfortunately this cannot work by Fermat's little theorem. So let us try setting $n = 2pq$, with p, q different prime numbers. We need $pq|2^{2pq-1} + 1$ and so we must have $\left(\frac{-2}{p}\right) = \left(\frac{-2}{q}\right) = 1$. Also, using Fermat's little theorem, $p|2^{2q-1} + 1$ and $q|2^{2p-1} + 1$. A small verification shows that $q = 3, 5, 7$ are not good choices, so let us try $q = 11$. In this case we find $p = 43$ and so it suffices to show that $pq|2^{2pq-1} + 1$ for $q = 11$ and $p = 43$. This is immediate, since the hard work has already been completed: we have shown that it suffices to have $p|q^{2q-1}$, $q|2^{2p-1} + 1$, and $\left(\frac{-2}{p}\right) =$

$\left(\frac{-2}{q}\right) = 1$ in order to have $pq|2^{2pq-1}+1$. But as one can easily check, all these conditions are verified and the number $2 \cdot 11 \cdot 43$ is a valid answer.

Were we wrong when choosing to present the following example? It apparently has no connection with quadratic reciprocity, but let us take a closer look.

Example 4. Let $f, g : Z^+ \to Z^+$ functions with the properties:

i) g is surjective;

ii) $2f^2(n) = n^2 + g^2(n)$ for all positive integers n.

If, moreover, $|f(n)-n| \leq 2004\sqrt{n}$ for all n, prove that f has infinitely many fixed points.

Gabriel Dospinescu, Moldova TST, 2005

Solution. Let p_n be the sequence of prime numbers of the form $8k+3$ (the fact that there are infinitely many such numbers is a trivial consequence of Dirichlet's theorem, but we invite the reader to find an elementary proof). It is obvious that for all n we have

$$\left(\frac{2}{p_n}\right) = (-1)^{\frac{p_n^2-1}{8}} = -1.$$

Using the condition i) we can find x_n such that $g(x_n) = p_n$ for all n. It follows that $2f^2(x_n) = x_n^2 + p_n^2$, which can be rewritten as $2f^2(x_n) \equiv x_n^2 \pmod{p_n}$. Because $\left(\frac{2}{p_n}\right) = -1$, the last congruence shows that $p_n|x_n$ and $p_n|f(x_n)$. Thus there exist sequences of positive integers a_n, b_n such that $x_n = a_n p_n$, $f(x_n) = b_n p_n$ for all n. Clearly, ii) implies the relation $2b_n^2 = a_n^2 + 1$. Finally, using the property $|f(n) - n| \leq 2004\sqrt{n}$ we infer that

$$\frac{2004}{\sqrt{x_n}} \geq \left|\frac{f(x_n)}{x_n} - 1\right| = \left|\frac{b_n}{a_n} - 1\right|,$$

that is

$$\lim_{n\to\infty} \frac{\sqrt{a_n^2+1}}{a_n} = \sqrt{2}.$$

The last relation immediately implies that $\lim\limits_{n\to\infty} a_n = 1$. Therefore, starting from a certain rank, we have $a_n = 1 = b_n$ that is $f(p_n) = p_n$. The conclusion now follows.

We continue with a difficult classical result, that often proves very useful. It characterizes numbers that are quadratic residues modulo all sufficiently large prime numbers. Of course, perfect square are such numbers, but how to prove that they are the only ones?

Example 5. Suppose that $a \in \mathbb{N}$ is not a perfect square. Then $\left(\frac{a}{p}\right) = -1$ for infinitely many prime numbers p.

Solution. One may assume that a is square-free. Let us write $a = 2^e q_1 q_2 \dots q_n$, where q_i are different odd primes and $e \in \{0, 1\}$. Let us assume first that $n \geq 1$ and consider some odd distinct primes $r_1, \dots, r_k$ each of them different from $q_1, \dots, q_n$. We will show that there exists a prime p, different from $r_1, \dots, r_k$, such that $\left(\frac{a}{p}\right) = -1$. Let s be a non quadratic residue modulo q_n.

Using the Chinese remainder theorem, we can find a positive integer b such that

$$\begin{cases} b \equiv 1 \pmod{r_i},\ 1 \leq i \leq k \\ b \equiv 1 \pmod{8}, \\ b \equiv 1 q_i,\ 1 \leq i \leq n-1 \\ b \equiv s \pmod{q_n} \end{cases}$$

Now, write $b = p_1 \dots p_m$ with p_i odd primes, not necessarily distinct. Using the quadratic reciprocity law, it follows immediately that

$$\prod_{i=1}^{m} \left(\frac{2}{p_i}\right) = \prod_{i=1}^{m} (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\frac{b^2-1}{8}} = 1$$

and

$$\prod_{j=1}^{m} \left(\frac{q_i}{p_j}\right) = \prod_{j=1}^{m} (-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}} \left(\frac{p_j}{q_i}\right) = (-1)^{\frac{q_i-1}{2}\cdot\frac{b-1}{2}} \left(\frac{b}{q_i}\right) = \left(\frac{b}{q_i}\right)$$

for all $i \in \{1, 2, \ldots, n\}$. Hence

$$\prod_{i=1}^{m} \left(\frac{a}{p_i}\right) = \left[\prod_{j=1}^{m} \left(\frac{2}{p_j}\right)\right]^2 \prod_{i=1}^{n} \prod_{j=1}^{m} \left(\frac{q_i}{p_j}\right)$$

$$= \prod_{i=1}^{n} \left(\frac{b}{q_i}\right) = \left(\frac{b}{q_n}\right) = \left(\frac{s}{q_n}\right) = -1.$$

Thus, there exists $i \in \{1, 2, \ldots, m\}$ such that $\left(\frac{a}{p_i}\right) = -1$. Because $b \equiv 1 \pmod{r_i}$, $1 \leq i \leq k$ we also have $p_i \in \{1, 2, \ldots\} \setminus \{r_1, \ldots, r_k\}$ and the claim is proved.

The only remaining case is $a = 2$. But this one is very simple, since it suffices to use Dirichlet's theorem to find infinitely many primes p such that $\frac{p^2 - 1}{8}$ is odd.

As in other units, we will now focus on a special case. This time it is a problem almost trivial in the above framework and almost impossible to solve otherwise (we say almost because there is a beautiful, but very difficult solution using analytical tools, that we will not present here).

Example 6. Suppose that $a_1, a_2, \ldots, a_{2004}$ are nonnegative integers such that $a_1^n + a_2^n + \cdots + a_{2004}^n$ is a perfect square for all positive integers n. What is the minimal number of such integers that must equal 0?

Gabriel Dospinescu, Mathlinks Contest

Solution. Suppose that $a_1, a_2, \ldots, a_k$ are positive integers such that $a_1^n + a_2^n + \cdots + a_k^n$ is a perfect square for all n. We will show that k is a perfect square. In order to prove this, we will use the above result and show that $\left(\frac{k}{p}\right) = 1$ for all sufficiently large prime p. This is not a difficult task. Indeed, consider a prime p, greater than any prime divisor of $a_1 a_2 \ldots a_k$. Using Fermat's little theorem, $a_1^{p-1} + a_2^{p-1} + \cdots + a_k^{p-1} \equiv k \pmod{p}$, and since $a_1^{p-1} + a_2^{p-1} + \cdots + a_k^{p-1}$ is a perfect square, it follows that $\left(\frac{k}{p}\right) = 1$. Thus k is a perfect square. And now the problem becomes

trivial, since we must find the greatest perfect square smaller than 2004. A quick computation shows that this is $44^2 = 1936$ and so the desired minimal number is 68.

Here is another nice application of this idea. The following example is adapted after a problem given in Saint Petersburg Olympiad.

Example 7. Suppose that $f \in Z[X]$ is a second degree polynomial such that for any prime p there exists at least an integer n for which $p|f(n)$. Prove that f has rational zeros.

Solution. Let $f(x) = ax^2 + bx + c$ be this polynomial. It suffices of course to prove that $b^2 - 4ac$ is a perfect square. This boils down to proving that it is a quadratic residue modulo any sufficiently large prime. Pick a prime number p and an integer n such that $p|f(n)$. Then

$$b^2 - 4ac \equiv (2an + b)^2 \pmod{p}$$

and so

$$\left(\frac{b^2 - 4ac}{p}\right) = 1.$$

This shows that our claim is true and finishes the solution.

Some of the properties of Legendre's symbol can be also found in the following problem.

Example 8. Let p be an odd prime and let

$$f(x) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) X^{i-1}.$$

a) Prove that f is divisible by $X - 1$ but not by $(X-1)^2$ if and only if $p \equiv 3 \pmod 4$;

b) Prove that if $p \equiv 5 \pmod 8$ then f is divisible by $(X-1)^2$ and not by $(X-1)^3$.

Romanian TST, 2004

Solution. The first question is not difficult at all. Observe that

$$f(1) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$$

by the simple fact that there are exactly $\frac{p-1}{2}$ quadratic and non quadratic residues in $\{1, 2, \ldots p-1\}$. Also,

$$f'(1) = \sum_{i=1}^{p-1} (i-1) \left(\frac{i}{p}\right) = \sum_{i=1}^{p-1} i \left(\frac{i}{p}\right),$$

because $f(1) = 0$. The same idea of summing up in reversed order allows us to write:

$$\sum_{i=1}^{p-1} i \left(\frac{i}{p}\right) = \sum_{i=1}^{p-1} (p-i) \left(\frac{p-i}{p}\right)$$

$$= (-1)^{\frac{p-1}{2}} \sum_{i=1}^{p-1} 2(p-i) \left(\frac{i}{p}\right) = -(-1)^{\frac{p-1}{2}} f'(1)$$

(we used again the fact that $f(1) = 0$).

Hence for $p \equiv 1 \pmod 4$ we must also have $f'(1) = 0$. In this case f is divisible by $(X-1)^2$. On the other hand, if $p \equiv 3 \pmod 4$, then

$$f'(1) = \sum_{i=1}^{p-1} i \left(\frac{i}{p}\right) \equiv \sum_{i=1}^{p-1} i = \frac{p(p-1)}{2} \equiv 1 \pmod 2$$

and so f is divisible by $X-1$ but not by $(X-1)^2$.

The second question is much more technical, even though it uses the same main idea. Observe that

$$f''(1) = \sum_{i=1}^{p-1} (i^2 - 3i + 2) \left(\frac{i}{p}\right) = \sum_{i=1}^{p-1} i^2 \left(\frac{i}{p}\right) - 3 \sum_{i=1}^{p-1} i \left(\frac{i}{p}\right)$$

(once again we use the fact that $f(1) = 0$). Observe that the condition $p \equiv 5 \pmod 8$ implies, by a), that f is divisible by $(X-1)^2$ so actually

$$f''(1) = \sum_{i=1}^{p-1} i^2 \left(\frac{i}{p}\right).$$

Let us break this sum into two pieces and treat each of them independently. Let us deal with

$$\sum_{i=1}^{\frac{p-1}{2}}(2i)^2\left(\frac{2i}{p}\right)=4\left(\frac{2}{p}\right)\sum_{i=1}^{\frac{p-1}{2}}i^2\left(\frac{i}{p}\right).$$

Note that

$$\sum_{i=1}^{\frac{p-1}{2}}i^2\left(\frac{i}{p}\right)\equiv\sum_{i=1}^{\frac{p-1}{2}}i^2\equiv\sum_{i=1}^{\frac{p-1}{2}}i=\frac{p^2-1}{8}\equiv 1 \pmod 2,$$

so

$$\sum_{i=1}^{\frac{p-1}{2}}(2i)^2\left(\frac{2i}{p}\right)\equiv\pm \pmod 8$$

(actually, using the fact that $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, we obtain that its value is -4). On the other hand,

$$\sum_{i=1}^{\frac{p-1}{2}}(2i-1)^2\left(\frac{2i-1}{p}\right)\equiv\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right) \pmod 8.$$

If we prove that the last quantity is a multiple of 8, then the problem will be solved. But note that $f(1)=0$ implies

$$0=\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i}{p}\right)+\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right).$$

Also,

$$\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i}{p}\right)=1+\sum_{i=1}^{\frac{p-3}{2}}\left(\frac{2i}{p}\right)=1+\sum_{i=1}^{\frac{p-3}{2}}\left(\frac{2\left(\frac{p-1}{2}-i\right)}{p}\right)$$

$$=1+\sum_{i=1}^{\frac{p-3}{2}}\left(\frac{2i+1}{p}\right)=\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right).$$

Therefore $\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right)=0$ and the problem is finally solved.

Finally, a difficult problem.

Example 9. Find all positive integers n such that $2^n - 1 | 3^n - 1$.

Solution. We will prove that $n = 1$ is the only solution to the problem. Suppose that $n > 1$ is a solution. Then $2^n - 1$ cannot be a multiple of 3, hence n is odd. Therefore, $2^n \equiv 8 \pmod{12}$. Because any odd prime different from 3 is of one of the forms $12k \pm 1$, $12k \pm 5$ and since $2^n - 1 \equiv 7 \pmod{12}$, it follows that $2^n - 1$ has at least a prime divisor of the form $12k \pm 5$, call it p. Obviously, we must have $\left(\frac{3}{p}\right) = 1$ and using the quadratic reciprocity law, we finally obtain $\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$. On the other hand $\left(\frac{p}{3}\right) = \left(\frac{\pm 2}{3}\right) = -(\pm 1)$. Consequently, $-(\pm 1) = (-1)^{\frac{p-1}{2}} = \pm 1$, which is the desired contradiction. Therefore the only solution is $n = 1$.

Problems for training

1. Prove that for any odd prime p, the smallest positive quadratic non residue modulo p is smaller than $1 + \sqrt{p}$.

2. Let p be a prime number. Prove that the following statements are equivalent:

i) there is a positive integer n such that $p | n^2 - n + 3$;

ii) there is a positive integer m such that $p | m^2 - m + 25$.

Polish Olympiad

3. Let $x_1 = 7$ and let $x_{n+1} = 2x_n^2 - 1$. Prove that 2003 does not divide any term of the sequence.

Valentin Vornicu, Mathlinks Contest

4. Let p be a prime of the form $4k + 1$. Compute

$$\sum_{k=1}^{p-1} \left(\left[\frac{2k^2}{p} \right] - 2 \left[\frac{k^2}{p} \right] \right).$$

Korea TST 2000

5. Prove that the number $3^n + 2$ does not have prime divisors of the form $24k + 13$.

Laurentiu Panaitopol, Gazeta Matematica

6. What is the number of solutions to the equation $a^2 + b^2 = 1$ in $Z_p \times Z_p$. What about the equation $a^2 - b^2 = 1$?

7. Suppose that p is an odd prime and that A, B are two different non empty subsets of $\{1, 2, \ldots, p-1\}$ for which

i) $A \cup B = \{1, 2, \ldots, p-1\}$;

ii) If a, b are in the same set among A, B, then $ab \pmod{p} \in A$;

iii) If $a \in A,\ b \in B$, then $ab \in B$.

Find all such subsets A, B.

India

8. Let a, b, c be positive integers such that $b^2 - 4ac$ is not a perfect square. Prove that for any $n > 1$ there are n consecutive positive integers, none of which can be written in the form $(ax^2 + bxy + cy^2)^z$ for some integers x, y and some positive integer z.

Gabriel Dospinescu

9. Let be integers relatively prime with an odd prime p. Prove that:

$$\sum_{i=1}^{p-1} \left(\frac{ai^2 + bi}{p} \right) = -\left(\frac{a}{p} \right).$$

10. Compute $\displaystyle\sum_{k=1}^{p-1} \left(\frac{f(k)}{p} \right)$, where f is a polynomial with integral coefficients and p is an odd prime.

11. Suppose that for a certain prime p, the values the polynomial with integral coefficients $f(x) = ax^2 + bx + c$ takes at $2p-1$ consecutive integers are perfect squares. Prove that $p | b^2 - 4ac$.

IMO Shortlist

12. Suppose that $\phi(5^m - 1) = 5^n - 1$ for a pair (m, n) of positive integers. Here ϕ is Euler's totient function. Prove that $gcd(m, n) > 1$.

Taiwan TST

13. Let p be a prime of the form $4k+1$ such that $p^2|2^p-2$. Prove that the greatest prime divisor q of $2^p - 1$ satisfies the inequality $2^q > (6p)^p$.

Gabriel Dospinescu

SOLVING ELEMENTARY INEQUALITIES WITH INTEGRALS

Why are integral pertinent for solving inequalities? Well, when we say integral, we say in fact area. And area is a measurable concept, a comparable one. That is why there are plenty of inequalities which can be solved with integrals, some of them with a completely elementary statement. They seem elementary, but sometimes finding elementary solutions for them is a real challenge. Instead, there are beautiful and short solutions using integrals. Of course, the hard part is to find the integral that hides after the elementary form of the inequality (and to be sincere, the idea of using integrals to solve elementary inequalities is practically inexistent in Olympiad books). First, let us state some properties of integrals that we will use here.

1) For any integrable function $f : [a, b] \to \mathbb{R}$ we have

$$\int_a^b f^2(x)dx \geq 0.$$

2) For any integrable functions $f, g : [a, b] \to \mathbb{R}$ such that $f \leq g$ we have

$$\int_a^b f(x)dx \leq \int_a^b g(x)dx \text{ (monotony for integrals).}$$

3) For any integrable functions $f, g : [a, b] \to \mathbb{R}$ and any real numbers α, β we have

$$\int_a^b (\alpha f(x)+\beta g(x))dx = \alpha \int_a^b f(x)dx+\beta \int_a^b g(x) \text{ (linearity of integrals).}$$

Also, the well-known elementary inequalities of Cauchy-Schwarz, Chebyshev, Minkowski, Hölder, Jensen, Young have corresponding integral inequalities, which are derived immediately from the algebraic inequalities (indeed, one just have to apply the corresponding inequalities for the numbers $f\left(a+\frac{k}{n}(b-a)\right)$, $g\left(a+\frac{k}{n}(b-a)\right), \ldots$ with

$k \in \{1, 2, \ldots, n\}$ and to use the fact that

$$\int_a^b f(x)dx = \lim_{n\to\infty} \frac{b-a}{n} \sum_{k=1}^{n} f\left(a + \frac{k}{n}(b-a)\right).$$

The reader will take a look at the glossary if he doesn't manage to state them.

It seems at first glance that this is not a very intricate and difficult theory. Totally false! We will see how strong is this theory of integration and especially how hard it is to look beneath the elementary surface of a problem. To convince yourself of the strength of the integral, take a look at the following beautiful proof of the AM-GM inequality using integrals. This magnificent proof was found by H. Alzer and published in the American Mathematical Monthly.

Example 1. Prove that for any $a_1, a_2, \ldots, a_n \geq 0$ we have the inequality

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n}.$$

Solution. Let us suppose that $a_1 \leq a_2 \leq \cdots \leq a_n$ and let

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n}, \ B = \sqrt[n]{a_1 a_2 \ldots a_n}.$$

Of course, we can find an index $k \in \{1, 2, \ldots, n-1\}$ such that $a_k \leq G \leq a_{k+1}$. Then it is immediate to see that

$$\frac{A}{G} - 1 = \frac{1}{n} \sum_{i=1}^{k} \int_{a_i}^{G} \left(\frac{1}{t} - \frac{1}{G}\right) dt + \frac{1}{n} \sum_{i=k+1}^{n} \int_{G}^{a_i} \left(\frac{1}{G} - \frac{1}{t}\right) dt$$

and the last quantity is clearly nonnegative, since each integral is nonnegative.

Truly wonderful, isn't it? So, after all, integrals are nice! This is also confirmed by the following problem, an absolute classic whose solution by induction can be a real nightmare.

Example 2. Prove that for any real numbers $a_1, a_2, \ldots, a_n$ the following inequality holds:

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_i a_j}{i+j} \geq 0.$$

Poland Mathematical Olympiad

Solution. Now, we will see how easy is this problem if we manage to handle integrals and especially to see from where they come. The essential suggestion is the observation that

$$\frac{a_i a_j}{i+j} = \int_0^1 a_i a_j t^{i+j-1} dt.$$

And now the problem is solved. What follows are just formalities; the hard part was translating the inequality. After that, we will decide what is better to do. So,

$$\sum_{i,j=1}^{n}\frac{a_i a_j}{i+j} \geq 0$$

is equivalent to

$$\sum_{i,j=1}^{n}\int_0^1 a_i a_j t^{i+j-1} dt \geq 0,$$

or, using the linearity of the integrals, to

$$\int_0^1 \left(\sum_{i,j=1}^{n} a_i a_j t^{i+j-1}\right) dt \geq 0.$$

This form suggests us that we should use the first property, that is we should find an integrable function f such that

$$f^2(t) = \sum_{i,j=1}^{n} a_i a_j t^{i+j-1} dt.$$

This isn't hard, because the formula

$$\left(\sum_{i=1}^{n} a_i x_i\right)^2 = \sum_{i,j=1}^{n} a_i a_j x_i x_j$$

solves the task. We just have to take

$$f(x) = \sum_{i=1}^{n} a_i x^{i-\frac{1}{2}}.$$

We continue the series of direct applications of classical integral inequalities with a problem proposed by Walther Janous and which may also put serious problems if not attacked appropriately.

Example 3. Let $t \geq 0$ and the sequence $(x_n)_{n\geq 1}$ defined by

$$x_n = \frac{1 + t + \cdots + t^n}{n+1}.$$

Prove that

$$x_1 \leq \sqrt{x_2} \leq \sqrt[3]{x_3} \leq \sqrt[4]{x_4} \leq \ldots$$

Walther Janous, Crux Mathematicorum

Solution. It is clear that for $t > 1$ we have

$$x_n = \frac{1}{t-1} \int_1^t u^n du$$

and for $t < 1$ we have

$$x_n = \frac{1}{1-t} \int_1^t u^n du.$$

This is how the inequality to be proved reduces to the more general inequality

$$\sqrt[k]{\frac{\int_a^b f^k(x)dx}{b-a}} \leq \sqrt[k+1]{\frac{\int_a^b f^{k+1}(x)dx}{b-a}}$$

for all $k \geq 1$ and any nonnegative integrable function $f : [a, b] \to \mathbb{R}$. And yes, this is a consequence of the Power Mean Inequality for integral functions.

The following problem has a long and quite complicated proof by induction. Yet, using integrals it becomes trivial.

Example 4. Prove that for any positive real numbers x, y and any positive integers m, n

$$(n-1)(m-1)(x^{m+n}+y^{m+n})+(m+n-1)(x^m y^n+x^n y^m)$$

$$\geq mn(x^{m+n-1}y+y^{m+n-1}x).$$

Austrian-Polish Competition ,1995

Solution. We transform the inequality as follows:

$$mn(x-y)(x^{m+n-1}-y^{m+n-1})\geq(m+n-1)(x^m-y^m)(x^n-y^n)\Leftrightarrow$$

$$\frac{x^{m+n-1}-y^{m+n-1}}{(m+n-1)(x-y)}\geq\frac{x^m-y^m}{m(x-y)}\cdot\frac{x^n-y^n}{n(x-y)}$$

(we have assumed that $x>y$). The last relations can be immediately translated with integrals in the form

$$(y-x)\int_y^x t^{m+n-2}dt\geq\int_y^x t^{m-1}dt\int_y^x t^{n-1}dt.$$

And this follows from the integral form of Chebyshev inequality.

A nice blending of arithmetic and geometric inequality as well as integral calculus allows us to give a beautiful short proof of the following inequality.

Example 5. Let $x_1, x_2, \ldots, x_k$ be positive real numbers and m, n positive real numbers such that $n \leq km$. Prove that

$$m(x_1^n+x_2^n+\cdots+x_k^n-k)\geq n(x_1^m x_2^m\ldots x_k^m-1).$$

IMO Shortlist 1985, proposed by Poland

Solution. Applying AM-GM inequality, we find that

$$m(x_1^n+\cdots+x_k^n-k)\geq m(k\sqrt[k]{(x_1x_2\ldots x_k)^n}-k).$$

Let

$$P=\sqrt[k]{x_1x_2\ldots x_k}.$$

We have to prove that

$$mkP^n - mk \geq nP^{mk} - n,$$

which is the same as

$$\frac{P^n - 1}{n} \geq \frac{P^{mk} - 1}{mk}.$$

This follows immediately from the fact that

$$\frac{P^x - 1}{x \ln P} = \int_0^1 e^{xt \ln P} dt.$$

We have seen a rapid but difficult proof for the following problem, using the Cauchy-Schwarz inequality. Well, the problem originated by playing around with integral inequalities and the following solution will show how one can create difficult problems starting from trivial ones.

Example 6. Prove that for any positive real numbers a, b, c such that $a + b + c = 1$ we have

$$(ab + bc + ca)\left(\frac{a}{b^2 + b} + \frac{b}{c^2 + c} + \frac{c}{a^2 + a}\right) \geq \frac{3}{4}.$$

Gabriel Dospinescu

Solution. As in the previous problem, the most important aspect is to translate the expression $\frac{a}{b^2 + b} + \frac{b}{c^2 + c} + \frac{c}{a^2 + a}$ in the integral language. Fortunately, this isn't difficult, since it is just

$$\int_0^1 \left(\frac{a}{(x + b)^2} + \frac{b}{(x + c)^2} + \frac{c}{(x + a)^2}\right) dx.$$

Now, using the Cauchy-Schwarz inequality, we infer that

$$\frac{a}{(x + b)^2} + \frac{b}{(x + c)^2} + \frac{c}{(x + a)^2} \geq \left(\frac{a}{x + b} + \frac{b}{x + c} + \frac{c}{a + x}\right)^2.$$

Using again the same inequality, we minor $\frac{a}{x + b} + \frac{b}{x + c} + \frac{c}{a + x}$ with $\frac{1}{x + ab + bc + ca}$. Consequently,

$$\frac{a}{(x + b)^2} + \frac{b}{(x + c)^2} + \frac{c}{(x + a)^2} \geq \frac{1}{(x + ab + bc + ca)^2}$$

and we can integrate this to find that

$$\frac{a}{b^2+b}+\frac{b}{c^2+c}+\frac{c}{a^2+a}\geq\frac{1}{(ab+bc+ca)(ab+bc+ca+1)}.$$

Now, all we have to do is to notice that

$$ab+bc+ca+1\leq\frac{4}{3}.$$

Now, another question for the interested reader: can we prove the general case (solved in Cauchy Schwarz's inequality topic) using integral calculus? It seems a difficult problem.

There is an important similarity between the following problem and example 2, yet here it is much more difficult to see the relation with integral calculus.

Example 7. Let $n\geq 2$ and S the set of the sequences $(a_1,a_2,\ldots,a_n)\subset[0,\infty)$ which verify

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1-a_ia_j}{1+j}\geq 0.$$

Find the maximum value of the expression $\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_i+a_j}{i+j}$, over all sequences from S.

Gabriel Dospinescu

Solution. Consider the function $f:\mathbb{R}\to\mathbb{R}$, $f(x)=a_1+a_2x+\cdots+a_nx^{n-1}$. Let us observe that

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_ia_j}{i+j}=\sum_{i=1}^{n}a_i\left(\sum_{j=1}^{n}\frac{a_j}{i+j}\right)=\sum_{i=1}^{n}a_i\int_0^1x^if(x)dx$$

$$=\int_0^1\left(xf(x)\sum_{i=1}^{n}a_ix^{i-1}\right)dx=\int_0^1xf^2(x)dx.$$

So, if we denote $M = \sum_{1 \le i,j \le n} \frac{1}{i+j}$, we infer that

$$\int_0^1 x f^2(x) dx \le M.$$

On the other hand, we have the identity

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \frac{a_i + a_j}{i+j} = 2\left(\frac{a_1}{2} + \cdots + \frac{a_n}{n+1} + \cdots + \frac{a_1}{n+1} + \cdots + \frac{a_n}{2n} \right)$$

$$= 2 \int_0^1 (x + x^2 + \cdots + x^n) f(x) dx.$$

This was the hard part: translating the properties of the sequences in S and also the conclusion. Now, the problem becomes easy, since we must find the maximal value of

$$2 \int_0^1 (x + x^2 + \cdots + x^n) f(x) dx$$

where

$$\int_0^1 x f^2(x) dx \le M.$$

Well, Cauchy-Schwarz inequality for integrals is the way to proceed. Indeed, we have

$$\left(\int_0^1 (x + x^2 + \cdots + x^n) f(x) dx \right)^2$$

$$= \left(\int_0^1 \sqrt{x f^2(x)} \sqrt{x(1 + x + \cdots + x^{n-1})^2} dx \right)^2$$

$$= \int_0^1 x f^2(x) dx \int_0^1 (1 + x + \cdots + x^{n-1})^2 dx \le M^2.$$

This shows that $\sum_{i=1}^{n} \sum_{j=1}^{n} \frac{a_i + a_j}{i+j} \le 2M$ and now the conclusion easily follows: the maximal value is $2 \sum_{1 \le i,j \le n} \frac{1}{i+j}$, attained for $a_1 = a_2 = \cdots = a_n = 1$.

Two more words about fractions. We have already said that bunching is a mathematical crime. It is time to say it again. This is why we designed this topic, to present a new method of treating inequalities involving fractions. Some relevant examples will be treated revealing that bunching could be a great pain for the reader wanting to use it.

Example 8. Prove that for any positive real numbers a, b, c the following inequality holds:

$$\frac{1}{3a}+\frac{1}{3b}+\frac{1}{3c}+\frac{3}{a+b+c}\geq \frac{1}{2a+b}+\frac{1}{2b+a}+\frac{1}{2b+c}$$
$$+\frac{1}{2c+b}+\frac{1}{2c+a}+\frac{1}{2a+c}.$$

Gabriel Dospinescu

Solution. Of course, the reader has noticed that this is stronger than Popoviciu's inequality, so it seems that classical methods will have no chances. And what if we say that this is Schur's inequality revisited? Indeed, let us write Schur's inequality in the form:

$$x^3+y^3+z^3+3xyz\geq x^2y+y^2x+y^2z+z^2y+z^2x+x^2z$$

where $x=t^{a-\frac{1}{3}}$, $y=t^{b-\frac{1}{3}}$, $z=t^{c-\frac{1}{3}}$ and integrate the inequality as t ranges between 0 and 1. And surprise... since what we get is exactly the desired inequality.

In the same category, here is another application of this idea.

Example 9. Prove that for any positive real numbers a, b, c the following inequality holds:

$$\frac{1}{3a}+\frac{1}{3b}+\frac{1}{3c}+2\left(\frac{1}{2a+b}+\frac{1}{2b+c}+\frac{1}{2c+a}\right)$$
$$\geq 3\left(\frac{1}{a+2b}+\frac{1}{b+2c}+\frac{1}{c+2a}\right).$$

Gabriel Dospinescu

Solution. If the previous problem could be solved using bunching (or not? Anyway, we haven't tried), this one is surely impossible to solve in this manner. With the experience from the previous problem, we see that the problem asks in fact to prove that

$$x^3+y^3+z^3+2(x^2y+y^2z+z^2x)\geq 3(xy^2+yz^2+zx^2)$$

for any positive real numbers x, y, z.

Let us assume that $x=\min(x,y,z)$ and write $y=x+m$, $z=x+n$ for some nonnegative real numbers m, n. Simple computations show that the inequality is equivalent to

$$2x(m^2-mn+n^2)+(n-m)^3+m^3\geq (n-m)m^2.$$

Therefore, it suffices to prove that

$$(n-m)^3+m^3\geq (n-m)m^2,$$

which is the same as (via the substitution $t=\dfrac{n-m}{m}$) $t^3+1\geq t$ for all $t\geq -1$, which is immediate.

Starting this topic, we said that there is a deep relation between integrals and areas, but in the sequel we seemed to neglect the last concept. We ask the reader to accept our apologizes and bring to their attention two mathematical gems, in which they will surely have the occasion to play around with areas. If only this was easy to see... In fact, these problems are discrete forms of Young and Steffensen inequalities for integrals.

Example 10. Let $a_1\geq a_2\geq\cdots\geq a_{n+1}=0$ and let $b_1, b_2, \ldots, b_n\in[0,1]$. Prove that if

$$k=\left[\sum_{i=1}^{n} b_i\right]+1,$$

then

$$\sum_{i=1}^{n} a_i b_i \leq \sum_{i=1}^{k} a_i.$$

Saint Petersburg Olympiad, 1996

Solution. The very experienced reader has already seen a resemblance with Steffensen's inequality: for any continuous functions $f, g : [a, b] \to \mathbb{R}$ such that f is decreasing and $0 \leq g \leq 1$ we have

$$\int_a^{a+k} f(x)dx \geq \int_a^b f(x)g(x)dx,$$

where

$$k = \int_a^b f(x)dx.$$

So, probably an argument using areas (this is how we avoid integrals and argue with their discrete forms, areas!!!) could lead to a neat solution. So, let us consider a coordinate system XOY and let us draw the rectangles $R_1, R_2, \ldots, R_n$ such that the vertices of R_i are the points $(i-1, 0)$, $(i, 0)$, $(i-1, a_i)$, (i, a_i) (we need n rectangles of heights $a_1, a_2, \ldots, a_n$ and weights 1, so that to view $\sum_{i=1}^{k} a_i$ as a sum of areas) and the rectangles $S_1, S_2, \ldots, S_n$, where the vertices of S_i are the points $\left(\sum_{j=1}^{i-1} b_j, 0\right)$, $\left(\sum_{j=1}^{i} b_j, 0\right)$, $\left(\sum_{j=1}^{i-1} b_j, a_i\right)$, $\left(\sum_{j=1}^{i} b_j, a_i\right)$ (where $\sum_{j=1}^{0} b_j = 0$). We have made this choice because we need two sets of pair wise disjoint rectangles with the same heights and areas $a_1, a_2, \ldots, a_n$ and $a_1b_1, a_2b_2, \ldots, a_nb_n$ so that we can compare the areas of the unions of the rectangles in the two sets. Thus, looking in a picture, we find immediately what we have to show: that the set of rectangles $S_1, S_2, \ldots, S_n$ can be covered with the rectangles $R_1, R_2, \ldots, R_{k+1}$. Intuitively, this is evident, by looking again at the picture. Let us make it rigorous. Since

the weight of the union of $S_1, S_2, \ldots, S_n$ is $\sum_{j=1}^{n} b_j < k+1$ (and the weight of $R_1, R_2, \ldots, R_{k+1}$ is $k+1$), it is enough to prove this for any horizontal line. But if we consider a horizontal line $y = p$ and an index r such that $a_r \geq p > a_{r+1}$, then the corresponding weight for the set $R_1, R_2, \ldots, R_{k+1}$ is p, which is at least $b_1 + b_2 + \cdots + b_p$, the weight for $S_1, S_2, \ldots, S_n$. And the problem is solved.

And now the second problem, given this time in a Balkan Mathematical Olympiad.

Example 11. Let $(x_n)_{n\geq 0}$ be an increasing sequence of nonnegative integers such that for all $k \in \mathbb{N}$ the number of indices $i \in \mathbb{N}$ for which $x_i \leq k$ is $y_k < \infty$. Prove that for any $m, n \in \mathbb{N}$ we have the inequality

$$\sum_{i=0}^{m} x_i + \sum_{j=0}^{n} y_j \geq (m+1)(n+1).$$

Balkan Mathematical Olympiad, 1999

Solution. Again, experienced reader will see immediately a similarity with Young's inequality: for any strictly increasing one to one map $f : [0, A] \to [0, B]$ and any $a \in (0, A)$, $b \in (0, B)$ we have the inequality

$$\int_0^a f(x)dx + \int_0^b f^{-1}(x)dx \geq ab.$$

Indeed, it suffices to take the given sequence $(x_n)_{n\geq 0}$ as the one to one increasing function in Young's inequality and the sequence $(y_n)_{n\geq 0}$ as the inverse of f. Just view $\sum_{i=0}^{m} x_i$ and $\sum_{j=0}^{m} y_j$ as the corresponding integrals and the similarity will be obvious.

Thus, probably again a geometrical solution is hiding behind some rectangles. Indeed, consider the vertical rectangles with weight 1 and heights $x_0, x_1, \ldots, x_m$ and the rectangles with weight 1 and heights $y_0, y_1, \ldots, y_n$. Then in a similar way one can prove that the set of these

rectangles covers the rectangle of sides $m+1$ and $n+1$. Thus, the sum of their areas is at least the are of this rectangle.

It will be difficult to solve the following beautiful problems using integrals, since the idea is very well hidden. Yet, there is such a solution and it is more than beautiful.

Example 12. Prove that for any $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \geq 0$ the following inequality holds

$$\sum_{1\leq i<j\leq n} (|a_i - a_j| + |b_i - b_j|) \leq \sum_{1\leq i,j\leq n} |a_i - b_j|.$$

Poland, 1999

Solution. Let us define the functions $f_i, g_i : [0,\infty) \to \mathbb{R}$,

$$f_i(x) = \begin{cases} 1, & t \in [0, a_i], \\ 0, & t > a_i \end{cases} \quad \text{and } g_i(x) = \begin{cases} 1, & x \in [0, b_i], \\ 0, & x > b_i. \end{cases}$$

Also, let us define

$$f(x) = \sum_{i=1}^{n} f_i(x), \quad g(x) = \sum_{i=1}^{n} g_i(x).$$

Now, let us compute $\displaystyle\int_0^\infty f(x)g(x)dx$. We see that

$$\int_0^\infty f(x)g(x)dx = \int_0^\infty \left(\sum_{1\leq i,j\leq n} f_i(x)g_j(x) \right) dx$$

$$= \sum_{1\leq i,j\leq n} \int_0^\infty f_i(x)g_j(x)dx = \sum_{1\leq i,j\leq n} \min(a_i, b_j).$$

A similar computation shows that

$$\int_0^\infty f^2(x)dx = \sum_{1\leq i,j\leq n} \min(a_i, a_j)$$

and

$$\int_0^\infty g^2(x)dx = \sum_{1\leq i,j\leq n} \min(b_i, b_j).$$

Since

$$\int_0^\infty f^2(x)dx+\int_0^\infty g^2(x)dx=\int_0^\infty (f^2(x)+g^2(x))dx\geq 2\int_0^\infty f(x)g(x)dx,$$

we find that

$$\sum_{1\leq i,j\leq n}\min(a_i,a_j)+\sum_{1\leq i,j\leq n}\min(b_i,b_j)\geq 2\sum_{1\leq i,j\leq n}\min(a_i,b_j).$$

Now, remember that $2\min(x,y)=x+y-|x-y|$ and the last inequality becomes

$$\sum_{1\leq i,j\leq n}|a_i-a_j|+\sum_{1\leq i,j\leq n}|b_i-b_j|\leq 2\sum_{1\leq i,j\leq n}|a_i-b_j|$$

and since

$$\sum_{1\leq i,j\leq n}|a_i-a_j|=2\sum_{1\leq i<j\leq n}|a_i-a_j|,$$

the problem is solved.

Using this idea, here is a difficult problem, whose elementary solution is awful and which has a 3-lines solution using the above idea... Of course, this is easy to find for the author of the problem, but in a contest things change!

Example 13. Let $a_1,a_2,\ldots,a_n>0$ and let $x_1,x_2,\ldots,x_n$ be real numbers such that

$$\sum_{i=1}^n a_ix_i=0.$$

a) Prove that the inequality $\sum_{1\leq i<j\leq n}x_ix_j|a_i-a_j|\leq 0$ holds;

b) Prove that we have equality in the above inequality if and only if there exist a partition $A_1,A_2,\ldots,A_k$ of the set $\{1,2,\ldots,n\}$ such that for all $i\in\{1,2,\ldots,k\}$ we have $\sum_{j\in A_i}x_j=0$ and $a_{j_1}=a_{j_2}$ if $j_1,j_2\in A_i$.

Gabriel Dospinescu, Mathlinks Contest

Solution. Let λ_A be the characteristic function of the set A. Let us consider the function

$$f : [0, \infty) \to \mathbb{R}, \quad f = \sum_{i=1}^{n} x_i \lambda_{[0,a_i]}.$$

Now, let us compute

$$\int_0^\infty f^2(x)dx = \sum_{1\le i,j\le n} x_i x_j \int_0^\infty \lambda_{[0,a_i]}(x)\lambda_{[0,a_a]}(x)dx$$

$$= \sum_{1\le i,j\le n} x_i x_j \min(a_i, a_j).$$

Hence

$$\sum_{1\le i,j\le n} x_i x_j \min(a_i, a_j) \ge 0.$$

Since

$$\min(a_i, a_j) = \frac{a_i + a_j - |a_i - a_j|}{2}$$

and

$$\sum_{1\le i,j\le n} x_i x_j (a_i + a_j) = 2\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} a_i x_i\right) = 0,$$

we conclude that

$$\sum_{1\le i<j\le n} x_i x_j |a_i - a_j| \le 0.$$

Let us suppose that we have equality. We find that

$$\int_0^\infty f^2(x)dx = 0$$

and so $f(x) = 0$ almost anywhere. Now, let $b_1, b_2, \ldots, b_k$ the distinct numbers that appear among $a_1, a_2, \ldots, a_n > 0$ and let $A_i = \{j \in \{1, 2, \ldots, n\} |\ a_j = b_i\}$. Then $A_1, A_2, \ldots, A_k$ is a partition of the set $\{1, 2, \ldots, n\}$ and we also have

$$\sum_{i=1}^{k} \left(\sum_{j\in A_i} x_j\right) \lambda_{[0,b_i]} = 0$$

almost anywhere, from where we easily conclude that

$$\sum_{i\in A_i} x_j = 0 \text{ for all } i \in \{1, 2, \ldots, k\}.$$

The conclusion follows.

And since we have proved the nice inequality

$$\sum_{1\le i,j\le n} x_i x_j \min(a_i, a_j) \ge 0$$

for any numbers $x_1, x_2, \ldots, x_n, a_1, a_2, \ldots, a_n > 0$ let's make a step further and give the magnificent proof found by Ravi B. (see mathlinks site) for one of the most difficult inequalities ever given in a contest, solution based on this result:

Example 14. Prove the following inequality

$$\sum_{1\le i,j\le n} \min(a_i a_j, b_i b_j) \le \sum_{1\le i,j\le n} \min(a_i b_j, a_j b_i).$$

G. Zbaganu, USAMO, 1999

Solution. Let us define the numbers $r_i = \dfrac{\max(a_i, b_i)}{\min(a_i, b_i)} - 1$ and $x_i = \operatorname{sgn}(a_i - b_i)$ (if, by any chance, one of $a_i, b_j = 0$, we can simply put $r_i = 0$). The crucial observation is the following identity:

$$\min(a_i b_j, a_j b_i) - \min(a_i a_j, b_i b_j) = x_i x_j \min(r_i, r_j).$$

Proving this relation can be achieved by distinguishing 4 cases, but let us remark that actually we may assume that $a_i \ge b_i$ and $a_j \ge b_j$, which leaves us with only two cases. The first one is when at least one of the two inequalities $a_i \ge b_i$ and $a_j \ge b_j$ becomes an equality. This case is trivial, so let us assume the contrary. Then

$$x_i x_j \min(r_i, r_j) = b_i b_j \min\left(\frac{a_i}{b_i} - 1, \frac{a_j}{b_j} - 1\right) = b_i b_j \left(\min\left(\frac{a_i}{b_i}, \frac{a_j}{b_j}\right) - 1\right)$$

$$= \min(a_i b_j, a_j b_i) - b_i b_j = \min(a_i b_j, a_j b_i) - \min(a_i a_j, b_i b_j).$$

Now, we can write

$$\sum_{1\le i,j\le n}\min(a_ib_j,a_jb_i)-\sum_{1\le i,j\le n}\min(a_ia_j,b_ib_j)=\sum_{i,j}x_ix_j\min(r_i,r_j)\ge 0,$$

the last inequality being nothing else than the main ingredient of the preceding problem.

Finally, here is a very funny problem, which is a consequence of this last hard inequality. Consider this a hint and try to solve it, since otherwise the problem is really extremely hard.

Example 15. Let $x_1,x_2,\ldots,x_n$ some positive real numbers such that

$$\sum_{1\le i,j\le n}|1-x_ix_j|=\sum_{1\le i,j\le n}|x_i-x_j|.$$

Prove that $\sum_{i=1}^{n}x_i=n$.

Gabriel Dospinescu

Solution. Consider $b_i=1$ in the inequality from example 14. We obtain:

$$\sum_{1\le i,j\le n}\min(x_i,x_j)\ge\sum_{1\le i,j\le n}\min(1,x_ix_j).$$

Now, use the formula $\min(u,v)=\dfrac{u+v-|u-v|}{2}$ and rewrite the above inequality in the form

$$2n\sum_{i=1}^{n}x_i-\sum_{1\le i,j\le n}|x_i-x_j|\ge n^2+\left(\sum_{i=1}^{n}x_i\right)^2-\sum_{1\le i,j\le n}|1-x_ix_j|.$$

Taking into account that

$$\sum_{1\le i,j\le n}|1-x_ix_j|=\sum_{1\le i,j\le n}|x_i-x_j|,$$

we finally obtain

$$2n\sum_{i=1}^{n}x_i\ge n^2+\left(\sum_{i=1}^{n}x_i\right)^2,$$

which can be rewritten as

$$\left(\sum_{i=1}^{n} x_i - n\right)^2 \leq 0$$

Therefore

$$\sum_{i=1}^{n} x_i = n.$$

Problems for practice

1. Show that for all $a, b \in \mathbb{N}^*$

$$\ln\left(\frac{bn+1}{an+1}\right) < \frac{1}{an+1} + \frac{1}{an+2} + \cdots + \frac{1}{bn} < \ln\frac{b}{a}.$$

2. Prove that for any $a > 0$ and any positive integer n the inequality

$$1^a + 2^a + \cdots + n^a < \frac{(n+1)^{a+1} - 1}{a+1}$$

holds. Also, for $a \in (-1, 0)$ we have the reversed inequality.

Folklore

3. Prove that for any real number x

$$n\sum_{k=0}^{n} x^{2k} \geq (n+1)\sum_{k=1}^{n} x^{2k-1}.$$

Harris Kwong, College Math. Journal

4. Let a continuous and monotonically increasing function $f : [0, 1] \to \mathbb{R}$ such that $f(0) = 0$ and $f(1) = 1$. Prove that

$$\sum_{k=1}^{9} f\left(\frac{k}{10}\right) + \sum_{k=1}^{10} f^{-1}\left(\frac{k}{10}\right) \leq \frac{99}{10}.$$

Sankt Petersburg, 1991

5. Prove the following inequality

$$\frac{a^n + b^n}{2} + \left(\frac{a+b}{2}\right)^n \geq 2 \cdot \frac{a^n + a^{n-1}b + \cdots + ab^{n-1} + b^n}{n+1}$$

for any positive integer n and any nonnegative real numbers a, b.

Mihai Onucu Drambe

6. Prove that if $a_1 \leq a_2 \leq \cdots \leq a_n \leq 2a_1$ the the following inequality holds

$$a_n \sum_{1 \leq i,j \leq n} \min(a_i, a_j) \geq \left(\sum_{i=1}^{n} a_i \right)^2 + \left(2n - \sum_{i=1}^{n} a_i \right)^2 .$$

Gabriel Dospinescu

7. For all positive real number x and all positive integer n we have:

$$\frac{\binom{2n}{0}}{x} - \frac{\binom{2n}{1}}{x+1} + \frac{\binom{2n}{2}}{x+2} - \cdots + \frac{\binom{2n}{2n}}{x+2n} > 0.$$

Komal

8. Prove that the function $f : [0, 1) \to \mathbb{R}$ defined by

$$f(x) = \log_2(1 - x) + x + x^2 + x^4 + x^8 + \ldots$$

is bounded.

Komal

9. Prove that for any real numbers $a_1, a_2, \ldots, a_n$

$$\sum_{i,j=1}^{n} \frac{ij}{i + j - 1} a_i a_j \geq \left(\sum_{i=1}^{n} a_i \right)^2 .$$

10. Let $k \in \mathbb{N}$, $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} = \alpha_1$. Prove that

$$\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq k}} \alpha_i^{k-j} \alpha_{i+1}^{j-1} \geq \frac{k}{n^{k-2}} \left(\sum_{i=1}^{n} \alpha_i \right)^{k-1} .$$

Hassan A. Shah Ali, Crux Mathematicorum

11. Prove that for any positive real numbers a, b, c such that $a + b = c = 1$ we have:

$$\left(1 + \frac{1}{a}\right)^b \left(1 + \frac{1}{b}\right)^c \left(1 + \frac{1}{c}\right)^a \geq 1 + \frac{1}{ab + bc + ca}.$$

Marius and Sorin Radulescu

12. Prove that for all $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \geq 0$ the inequality holds

$$\left(\sum_{1\leq i,j\leq n} \min(a_i, a_j)\right)\left(\sum_{1\leq i,j\leq n} \min(b_i, b_j)\right) \geq \left(\sum_{1\leq i,j\leq n} \min(a_i, b_j)\right).$$

Don Zagier

13. Prove that for any $x_1 \geq x_2 \geq \cdots \geq x_n > 0$ we have

$$\sum_{i=1}^{n} \sqrt{\frac{x_i^2 + x_{i+1}^2 + \cdots + x_n^2}{i}} \leq \pi \sum_{i=1}^{n} x_i.$$

Adapted after an IMC 2000 problem

14. Let φ be Euler's totient function, where $\varphi(1) = 1$. Prove that for any positive integer n we have

$$1 > \sum_{k=1}^{n} \frac{\varphi(k)}{k} \ln \frac{2^k}{2^k - 1} > 1 - \frac{1}{2^n}.$$

Gabriel Dospinescu

15. Let $p_1, p_2, \ldots, p_n$ some positive numbers which add up to 1 and $x_1, x_2, \ldots, x_n$ some positive real numbers. Let also

$$A = \sum_{i=1}^{n} a_i x_i \text{ and } G = \prod_{i=1}^{n} x_i^{p_i}.$$

a) Let us denote

$$I(x, a) = \int_0^\infty \frac{tdt}{(1+t)(x+at)^2}.$$

Prove that

$$\ln \frac{A}{G} = \sum_{i=1}^{n} p_i (x_i - A)^2 I(x_i, A).$$

Deduce the arithmetic-geometric inequality.

b) Suppose that $x_i \leq \dfrac{1}{2}$ and define A', G' the corresponding means for $1 - x_i$. Prove that $\dfrac{A}{G} \geq \dfrac{A'}{G'}$.

Oral examination ENS

16. Prove that for any positive real numbers $x_1, x_2, \ldots, x_n$ such that

$$\sum_{i=1}^{n} \frac{1}{1+x_i} = \frac{n}{2},$$

we have the inequality

$$\sum_{1 \le i,j \le n} \frac{1}{x_i + x_j} \ge \frac{n^2}{2}.$$

Gabriel Dospinescu

17. Prove that we can find a constant c such that for any $x \ge 1$ and any positive integer n we have

$$\left| \sum_{k=1}^{n} \frac{kx}{(k^2+x)^2} - \frac{1}{2} \right| \le \frac{c}{x}.$$

IMC, 1996

18. Let $0 = x_1 < \cdots < x_{2n+1} = 1$ some real numbers. Prove that if $x_{i+1} - x_i \le h$ for all $1 \le i \le 2n$ then

$$\frac{1-h}{2} < \sum_{i=1}^{2n} x_{2i}(x_{2i+1} - x_{2i-1}) < \frac{1+h}{2}.$$

Turkey TST, 1996

19. Prove that for any $a_1, a_2, \ldots, a_n \ge 0$ we have the following inequality

$$\sum_{1 \le i,j \le n} \frac{a_i a_j}{i+j} \le \pi \sum_{i=1}^{n} a_i^2.$$

Hilbert's inequality