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 $x + y + z \geq \frac{3}{2}$. 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

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

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 $xyz \leq \frac{s^3}{27}$, so $\frac{s^3}{27} \geq s+2$, 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 $\frac{b+c}{a}+\frac{c+a}{b}+\frac{a+b}{c}+3$ 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:

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

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

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

Titu Andreescu, Zuming Feng, USAMO 2003

Solution. The desired inequality is equivalent to

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

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

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

This is in fact the same as

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

Now, we transform this inequality into

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

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

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

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 will see 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 $xyz(x-1)(y-1)(z-1) \leq 8$.

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

$$9(a+b)(b+c)(c+a) \leq \frac{8}{3}(a+b+c)^3.$$

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 contest 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

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

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 $p(x) = a_0 + a_1 x + \cdots + a_n x^n$. The desired inequality becomes

$$(a_0 + a_1 x^2 + \cdots + a_n x^{2n})(a_0 + a_1 y^2 + \cdots + a_n y^{2n})$$

$$\geq (a_0 + a_1 xy + \cdots + a_n x^n y^n)^2.$$

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

$$(a_0 + a_1 xy + \cdots + a_n x^n y^n)^2$$

$$= (\sqrt{a_0} \cdot \sqrt{a_0} + \sqrt{a_1x^2} \cdot \sqrt{a_2y^2} + \cdots + \sqrt{a_nx^n} \cdot \sqrt{a_ny^n})^2$$
$$\leq (a_0 + a_1x^2 + \cdots + a_nx^{2n})(a_0 + a_1y^2 + \cdots + a_ny^{2n}).$$

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 this function is nonnegative. We will not prove this here, but we note a simple consequence: the more general inequality

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

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.[Aczel] 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.[Titu Andreescu and Dorin Andrica] 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 $b_1^2 + b_2^2 + \cdots + b_n^2 > 1$.

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

$$\begin{aligned}(a_1^2+a_2^2+\cdots+a_n^2-1)&(b_1^2+b_2^2+\cdots+b_n^2-1)\\ &\le (a_1b_1+a_2b_2+\cdots+a_nb_n-1)^2 \qquad (1)\end{aligned}$$

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.[Gabriel Dospinescu] 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:

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

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

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

which is equivalent to

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

Now, if $kT(n,k)-n>0$, we can take a k-tuple $(x_1, x_2, \ldots, x_k)$ such that $\sum\limits_{i=1}^{k} x_i = 0$ and $\sum\limits_{i=1}^{k} x_i^2 \neq 0$ 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 $\sum\limits_{i=k+1}^{n} x_i$. 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 $A = \sum\limits_{i=k+1}^{n} x_i$ and $B = \sum\limits_{i=1}^{k} x_i$. 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: $T(n,k) = \dfrac{n}{k}$ 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.[Murray Klamkin] 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 $x^2+y^2+z^2=1$.

Crux Mathematicorum

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

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

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

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

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

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

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

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

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

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

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

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

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

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. Do not worry if the time you pass on them is much more important than the time spent for the other examples: these problems are difficult!
There are inequalities where you can immediately see that you should apply the Cauchy-Schwarz inequality. Yet, applying it wrong can be very annoying. This is the case with the following example, where there is only one possibility to solve the problem using Cauchy-Schwarz:

Example 8. 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

Solution. It is quite clear that a direct application of the Cauchy-Schwarz inequality for

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

has no chance to work. Instead, if we develop $\frac{2}{3}(a+b+c)(x+y+z)$ we may group a,b,c and therefore try again the same method. Let us see:

$$\frac{2}{3}(a+b+c)(x+y+z)-(ax+by+cz)=a\cdot\frac{2y+2z-x}{3}+b\cdot\frac{2x+2z-y}{3}+c\cdot\frac{2x+2y-z}{3}$$

and the later can me bounded by $\sqrt{a^2+b^2+c^2}\cdot\sqrt{\sum\left(\frac{2x+2y-z}{3}\right)^2}$. All we have to do now is to prove the easy inequality $\sum\left(\frac{2x+2y-z}{3}\right)^2\leq x^2+y^2+z^2$, which is actually an equality!

Example 9.[Vasile Cartoaje] 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

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

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 $f''(x) = \frac{-6x}{(1-x)^4} \leq 0$. Hence we can apply Jensen's inequality to complete the solution.

We continue 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 10.[Gabriel Dospinescu] Let $a_1, a_2, \ldots, a_n$ be real numbers and let S be a non-empty subset of $\{1, 2, \ldots, n\}$. Prove that

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

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 $0 \le i_1 < i_2 < \cdots < i_k \le n$, $j_1 < j_2 < \cdots < j_k$ and also $i_1 < j_1, \dots, i_k < j_k$. 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 $a_1 = s_{i_1}$, $a_2 = s_{j_1}, \dots,$ $a_{2k-1} = s_{i_k}$, $a_{2k} = s_{j_k}$ 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

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

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

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

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

The following is remarkable inequality where Cauchy-Schwarz inequality is extremely well hiden. We must confess that the following solution was found after several weeks of trial and error:

Example 11.[Titu Andreescu, Gabriel Dospinescu] Prove that for any positive real numbers a, b, c, x, y, z such that $xy + yz + zx = 3$,

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

Solution. This is probably the best example of how finding the good homogenuous inequality simplifies the solution. In our case, it suffices to prove the homogenuous inequality

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

And now we can assume that $x+y+z=1$! Let us apply then the Cauchy-Schwarz inequality:

$$\frac{a}{b+c}x+\frac{b}{c+a}y+\frac{c}{a+b}z+\sqrt{3(xy+yz+zx)}\leq\sqrt{\sum(\frac{a}{b+c})^2}\cdot\sqrt{\sum x^2}+$$

$$\sqrt{\frac{3}{4}(xy+yz+zx)}+\sqrt{\frac{3}{4}(xy+yz+zx)}\leq\sqrt{\frac{3}{2}+\sum(\frac{a}{b+c})^2}\cdot\sqrt{(x+y+z)^2}$$

Therefore, the problem will be solved if we manage to prove that

$$\sqrt{\frac{3}{2}+\sum(\frac{a}{b+c})^2}\leq\sum\frac{a}{b+c},$$

which is the same as

$$\sum\frac{ab}{(a+c)(b+c)}\geq\frac{3}{4}.$$

Fortunately, this one reduces immediately to $(a+b+c)(ab+bc+ca)\geq 9abc$ which is true.

Finally, the incredible Hilbert's inequality shows the power of a correct application of the Cauchy-Schwarz inequality combined with some analytic tools:

Example 12.[Hilbert] Prove that for any real numbers $a_1,a_2,...,a_n$ the following inequality holds:

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_ia_j}{i+j}\leq\pi\cdot\sum_{i=1}^{n}a_i^2$$

Solution

Here is a beautiful way to apply the Cauchy-Schwarz inequality:

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_ia_j}{i+j}\right)^2=\left(\sum_{i,j=1}^{n}\frac{\sqrt[4]{i}a_i}{\sqrt[4]{j}\sqrt{i+j}}\cdot\frac{\sqrt[4]{j}a_j}{\sqrt[4]{i}\sqrt{i+j}}\right)^2$$

$$\leq\left(\sum_{i,j=1}^{n}\frac{\sqrt{i}a_i^2}{\sqrt{j}(i+j)}\right)\cdot\left(\sum_{i,j=1}^{n}\frac{\sqrt{j}a_j^2}{\sqrt{i}(i+j)}\right).$$

By rearranging terms in both sums, it is enough to prove that for any positive integer m

$$\sum_{n\geq 1}\frac{\sqrt{m}}{(m+n)\sqrt{n}}\leq \pi.$$

Fortunately, this is not difficult, because the inequality

$$\frac{1}{(n+m+1)\sqrt{n+1}}\leq \int_n^{n+1}\frac{dx}{(x+m)\sqrt{x}}$$

holds as a consequence of the monotony of $f(x)=\frac{1}{(x+m)\sqrt{x}}$. By adding up these inequalities, we deduce that

$$\sum_{n\geq 0}\frac{1}{(n+m+1)\sqrt{n+1}}\leq \int_0^{\infty}\frac{dx}{(x+m)\sqrt{x}}.$$

With the change of variable $x=mu^2$, a simple computation shows that the last integral is $\frac{\pi}{\sqrt{m}}$ and this finishes the solution.

Problems for training

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

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

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

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

Prove the inequality

$$\left(\sum_{1 \le i \ne j \le n} a_i b_j \right)^2 \ge \left(\sum_{1 \le i \ne j \le n} a_i a_j \right) \left(\sum_{1 \le i \ne j \le n} b_i b_j \right)$$

Alexandru Lupas, AMM

7. Let $n \ge 2$ 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

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

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

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

Saint Petersburg, 2001

11. 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

12. 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

13. 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

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

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

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

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 $\max\{|x|, |y|, |z|\} > 2$ and satisfying (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 $x = u + \frac{1}{u}$, (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 $y = v + \frac{1}{v}$. 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) and such that $\max\{|x|, |y|, |z|\} > 2$, 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 nontrivial 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 $x^2 + y^2 + z^2 - xyz - 4$.

Of 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 "Two useful substitutions". 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

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

(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 $f(x) = g(x) + \frac{1}{g(x)}$. 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

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

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 $x_{n+1} = x_nx_{n-1}$ (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 $\lambda^{2k} + \dfrac{1}{\lambda^{2k}} \in \mathbf{N}$ for all $k \in \mathbf{N}$. But this isn't difficult, since

$$\lambda^2 + \frac{1}{\lambda^2} \in \mathbf{N}, \quad \lambda^4 + \frac{1}{\lambda^4} \in \mathbf{N}$$

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 or to the famous theorems such as those of 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? One thing is sure: the above methods fail. Yet, another smart idea appears: if we have to prove that $a|b$, then it suffices to show that the exponent of any prime number in the prime factorization of a is at most the exponent of that prime in the prime factorization of b. For simplicity, let us denote by $v_p(a)$ the exponent of the prime number p in the prime factorization of a. Of course, if p does not divide a, then $v_p(a) = 0$. Also, it is easy to prove the following properties of $v_p(a)$:

1) $v_p(a+b) \geq min\{v_p(a), v_p(b)\}$
2) $v_p(ab) = v_p(a) + v_p(b)$

for any positive integers a and b. Now, let us rephrase the above idea in terms of $v_p(a)$: $a|b$ if and only if for any prime p we have $v_p(a) \leq v_p(b)$ and $a = b$ if and only if for any prime 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) $v_p(lcm(a_1, a_2, \ldots, a_n)) = \max\{v_p(a_1), v_p(a_2), \ldots, v_p(a_n)\}$
5) $v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \frac{n - s_p(n)}{p-1}$.

Here, $s_p(n)$ is the sum of digits of n when written in base p. Observe that 3) and 4) are simple consequences of the definitions. Less straightforward is 5). It 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

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = a_1 + a_2 p + \cdots + a_k p^{k-1} + a_2 + a_3 p + \cdots + a_k p^{k-2} + \cdots + a_k,$$

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 us see this idea in action.

Example 1. Let a and 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. We will prove that $v_p(a) = v_p(b)$ for any prime p. 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 positive integers n. But the relation $a^{4n+1}|b^{4n+2}$ can be written 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 now follows.

We have mentioned at the beginning of the discussion a nice and easy problem, so probably it is time to solve it, although you might have already done this.

Example 2. 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 by symmetry we may assume that $x \geq y \geq z$ and the inequality becomes $2x + y \geq 2x$ and everything is clear.

It is time for some difficult problems. The ones we chose to present are all based on the observations from the beginning of the chapter.

Example 3.[Paul Erdos] Prove that there exists a constant c such that for any positive integers a, b, n that verify $a! \cdot b!|n!$ we have $a + b < n + c\ln n$.

Solution.
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 also written 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). Hence 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. It took quite a long time before an Olympian, S. Konyagin, found an extraordinary solution. We will not present his solution here, but another one, even simpler.

Example 4. Is there an infinite set of positive integers such that no matter how we choose some elements of this set, their sum is not a perfect power?

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 for sure not a perfect power, 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 we are about to present is truly beautiful. You might also want to try a combinatorial approach by counting the invertible matrices with entries in the field $\mathbf{Z}_2$.

Example 5. Prove that for any positive integer n, $n!$ is a divisor of

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

Solution. Let us take a prime number p. We may assume that $p \leq n$. First, let us see what happens if $p = 2$. 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 $k \geq 1$). Now, let us assume that $p > 2$. From Fermat's theorem we have $p | 2^{p-1} - 1$, so $p | 2^{k(p-1)} - 1$ 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 from the above remarks we infer that

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

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

Because

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

we find that

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

But

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

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 the problem is solved.

Diophantine equations can also be solved using the method described in this chapter. Here is a difficult one, given at a Russian Olympiad.

Example 6 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 Olympiad

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. It follows that $v_2(n_k!) = v_5(n_k!)$. This implies $\left[\frac{n_k}{2^j}\right] = \left[\frac{n_k}{5^j}\right]$ 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 simple verification 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 yields no solution. Thus $x = 0$. 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 odd and thus we find again that $v_2(n_k!) = n \leq v_5(n_k!)$, impossible. Hence $n_k = n_{k-1} + 1$. But then, taking into account that n_k is a power of 5, we deduce that $(n_1+1)\dots(n_k-1)n_k + \dots + (n_{k-1}+1)\dots(n_k-1)n_k + 1$ 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 $n_k \leq 6$. Because n_k is a power of 5, we find that $n_k = 5$, $n_{k-1} \leq 4$ and exhausting all of the possibilities shows that there are no solutions.

A tricky APMO 1997 problem asked to prove that there is a number $100 < n < 1997$ such that $n|2^n + 2$. We will invite you to verify that $2 \cdot 11 \cdot 43$ is a solution and especially to find how we arrived at this number. 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 Schinzel.

Example 7.[Schinzel] 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 $p_1 < \dots < p_s$ 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 $n \equiv 1 \pmod{2^{m_i}}$ and we can write $n - 1 = 2^m t$. We have $2^{2^m t} \equiv -1 \pmod{p_i}$, thus $-1 \equiv 2^{2^m t m_i} \equiv 2^{(p_i-1)t} \equiv 1 \pmod{p_i}$ (the last congruence being derived from Fermat's little theorem). Thus $p_i = 2$, which is clearly impossible.

We continue with a very nice and difficult problem, in which the idea of looking at the exponents is really helpful. It seems to have appeared for the first time in AMM, but over the last few years, it was proposed to various national and international contests.

Example 8.[Armond E. Spencer] Prove that for any integers $a_1, a_2, \dots, a_n$ the number

$$\prod_{1 \leq i < j \leq n} \frac{a_i - a_j}{i - j}$$

is an integer.

AMM E 2637

Solution. We consider a prime number p and 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 $(i-j)_{1 \leq i < j \leq n}$. Because

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

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

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

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

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

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; each of them is of the form $i+jp$, with $0\le j\le\frac{n-i}{p}$, and, of course, if $i=0$, we have $1\le j\le\frac{n}{p}$). Hence

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

and it suffices to prove that

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

Now, observe that we need to find the minimum 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 $x_1\le x_2\le\cdots\le x_{p^k-1}$ is the n-tuple for which the minimum is reached(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 $(x_0+1,x_1,\dots,x_{p^k-2},x_{p^k-1}-1)$ 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 to $x_{p^k-1}>x_0+1$. But this contradicts the minimality of $(x_0,x_1,\dots,x_2,\dots,x_{p^k-1})$. So, $x_{p^k-1}\le x_0+1$

and from here it follows that $x_i \in \{x_0, x_0+1\}$ for all $i \in \{0,1,2,\dots,p^k-1\}$. Hence there is $j \in \{0,1,2,\dots,p^k-1\}$ 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 clearly implies that the n-tuple for which the minimum is attained is in fact $\left(\left[\dfrac{n+i}{p^k}\right]\right)_{i=0,p^k-1}$ and the problem is solved.

Finally, it is time for a challenge.

Example 9.[Gabriel Dospinescu] Let a and b be two distinct positive rational numbers such that for infinitely many integers n, $a^n - b^n$ is an integer. Prove that a and b are also integers.

Mathlinks Contest

Solution. Let us start by writing $a = \dfrac{x}{z}$, $b = \dfrac{y}{z}$, where x, y, z are distinct relatively prime positive integers. We are given that $z^n | x^n - y^n$ for infinitely many positive integers 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 follows that it cannot divide y. We have thus two cases:

i) If $p = 2$, then let n such that $2^n | x^n - y^n$. 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 $x^{v_n-1} + x^{v_n-2}y + \cdots + xy^{v_n-2} + y^{v_n-1}$ is clearly 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

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

Because

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

for $k > 0$, we finally deduce that

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

Consequently, $(2^{u_n})_{n\in M}$ is bounded, a simple reason being the inequality $2^{u_n} \le v_2(x+y) + v_2(x-y) + u_n - 1$. 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 be the least positive integer k such that $p|x^k - y^k$. Then for any n in M we have $p|x^n - y^n$. Let $x = tu$, $y = tv$, where $(u, v) = 1$. Clearly, tuv is not a multiple of p. It follows 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 $n = md$, for some positive integer m. Let $A = x^d$ and $B = y^d$. Then $p^m|p^n|x^n - y^n = A^m - B^m$ and this happens for infinitely many m. Moreover, $p|A - B$. Let R be the infinite set of those m. For any m in R we have $m \leq v_p(A^m - B^m)$. Now, let us write $m = p^i j$, where j is relatively prime to 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 otherwise). An essential observation is that we cannot have $p^2|\dfrac{A^{jp^k} - B^{jp^k}}{A^{jp^{k-1}} - B^{jp^{k-1}}}$ for a certain $k > 1$. Otherwise we would have $p^2|A^{jp^k} - B^{jp^k} \Rightarrow p^2|A^{pj} - B^{pj}$ (by Euler's theorem). Yet, $p^2|A^{jp^{k-1}(p-1)} + A^{jp^{k-1}(p-2)}B^{jp^{k-1}} + \cdots + B^{jp^{k-1}(p-1)}$. 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 $p|A$, that is $p|x$, false.

Let us prove now that we cannot have $p^2|\dfrac{A^{pj} - B^{pj}}{A^j - B^j}$. 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

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

which proves the equality

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

Thus, for infinitely many m we have

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

which is clearly impossible.

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

If you thought this is the last challenge on this chapter, you are wrong! The following problem was especially kept for the end of the chapter, because of its beauty and difficulty:

Example 10.[Paul Erdos] a) Prove that for any positive integer n there exist positive integers $a_1 < a_2 < ... < a_n$ such that $a_i - a_j | a_i$ for all $i \leq j$.
b) Prove that there exists a positive constant c such that for any n and any sequence $a_1 < a_2 < ... < a_n$ which satisfies the conditions of a), $a_1 > n^{cn}$.

Miklos Schweitzer Competition

Solution. If a) is not so difficult, b) needs culture and ingenuity. The proof of a) is of course by induction on n. For $n = 1$ it is enough to take $a_1 = 1$. Suppose that $a_1 < a_2 < ... < a_n$ is a good sequence and let us take $b = a_1 a_2 ... a_n$. The sequence $b, b + a_1, b + a_2, ..., b + a_n$ is also good and shows how the inductive step works.
Now, let us discuss b). Take any prime number $p \leq n$ and observe that if $a_i = a_j (mod p)$ then $a_i = a_j = 0 (mod p)$. Therefore at most $p - 1$ among the numbers $a_1, a_2, ..., a_n$ are not multiples of p. Consider the multiples of p among $a_1, a_2, ..., a_n$ and divide them by p. We obtain another good sequence and the previous argument shows that this new sequence has at most $p - 1$ terms not divisible by p. Repeating this argument yields $v_p(a_1 a_2 ... a_n) \geq (n - (p-1)) + (n - 2(p-1)) + ... + (n - [\frac{n}{p-1}](p-1)$. A small computation shows that if $p \leq \sqrt{n}$, then the last quantity exceeds $\frac{n^2}{3p}$. Therefore $a_1 a_2 ... a_n \geq \prod\limits_{p \leq \sqrt{n}} p^{\frac{n^2}{3p}}$. But it is clear that $a_1 \geq a_n - a_1$, so $a_1 \geq \frac{a_n}{2} \geq \frac{\sqrt[n]{a_1 a_2 ... a_n}}{2}$, which shows that

$$a_1 \geq \frac{1}{2} \cdot e^{\frac{n}{3}}$$

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 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

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

IMO 1974 Shortlist

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

5. Prove the identity

$$(n+1)lcm\left(\binom{n}{0}, \binom{n}{1}, ..., \binom{n}{n}\right) = lcm(1, 2, \ldots, n+1)$$

for any positive integer n.

Peter L Montgomery, AMM E 2686

6. Let $0 < a_1 < \cdots < a_n$ be integers. Find the greatest m for which we can find the integers $0 < b_1 < \cdots < b_m$ 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

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

Laurentiu Panaitopol, TST 1990 Romania

8. 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

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

IMO 1985 Shortlist

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

Poland Olympiad

11. 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

12. Let $a_1, \dots, a_n > 0$ 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 $i \in \{1, 2, \dots, n\}$ such that $a_1 + \cdots + a_n < 1 + [a_i]$.

13. Find the exponent of 2 in the prime factorization of the number

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

J. Desmong, W.R.Hastings, AMM E 2640

14. Prove that $(x_n)_{n\geq 1}$ the exponent of 2 in the decomposition of the numerator of $\dfrac{2}{1} + \dfrac{2^2}{2} + \cdots + \dfrac{2^n}{n}$, goes to infinity as $n \to \infty$. Even more, prove that $x_{2^n} \geq 2^n - n + 1$.

Adapted after a Kvant problem

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

Narumi's theorem

15. Let $a_1, a_2, ..., a_k$ be positive integers not exceeding n such that a_i does not divide $\prod\limits_{i \neq j} a_j$ for all i. Prove that $k \leq \pi(n)$ where $\pi(n)$ is the number of primes not exceeding n.

Erdos

16. Find $v_2(A)$, where A is the numerator of $1 + \frac{1}{3} + \frac{1}{5} + ... + \frac{1}{2k-1}$.

J.L.Selfridge, AMM E 1408

17. Prove that the number $\sum\limits_{k=1}^{m} \frac{k}{1+k(p-1)}$ is not integer for any prime number p and any positive integer m.

Toma Albu, AMM E 3249

Primes and squares

The study of the properties of the prime numbers is very well-developed, yet many old conjectures and open questions are still waiting to be solved. In this unit, we present a unitary view of the properties of some classes of primes and also of some classical results related to representations as sum of two squares. At the end of the unit, we will discuss, as usual, some nonstandard and surprising problems.

Because we will use some facts several times, we prefer to make some notations before discussing the problems. So, we will consider the sets A and B of all prime numbers of the form $4k+1$ and $4k+3$, respectively. Also, C will be the set of all numbers that can be written as the sum of two perfect squares. Our purpose is to present some classical results related to A, B, C. The most spectacular property of the set A is the fact that any of its elements is the sum of the squares of two positive integers. This is not a trivial property and we will present a beautiful proof of it next.

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

Solution. 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 $x = x_1 - x_2$ and $y = |y_1 - y_2|$, all the conditions will be satisfied, so 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 find the existence of positive integers $0 < x, y < \sqrt{p}$ (since $\sqrt{p} \notin \mathbb{Q}$) 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.

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

Example 2. Let $p \in B$ and suppose that x and y are integers such that $p|x^2 + y^2$. Then $p|gcd(x, y)$. 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 $p|gcd(x, y)$ 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 $gcd(x, p) = gcd(y, p) = 1$ and with Fermat's little 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 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 are 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 $i = 1, 2, ..., n$, 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 the elements of A and then simply apply the result from the second question. The conclusion is clear.

It is not difficult now 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 example and we will not insist more. Having presented some basic results that we will further use in this unit, it is time to see some applications that these two examples have.

As a simple application of the first example, we consider the following problem, which is certainly 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 equivalent to $2x^2 + 2x + 1 \equiv 0 \pmod{1997}$, which in turn becomes $(2x+1)^2+1 \equiv 0 \pmod{1997}$. Because $1997 \in A$, the congruence $n^2 \equiv -1 \pmod{1997}$ 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, then so is $1997 - n_0$ and it is clear thatthis equation it has at most two noncongruent solutions mod 1997. Because $gcd(2, 1997) = 1$, the function $x \to 2x + 1$ is a permutation of $\mathbb{Z}_{1997}$, and so the initial congruence has exactly two solutions with $x \in \{1, 2, \dots, 1996\}$. In a similar way, we find that there are exactly two solutions with $x \in \{-1997, -1996, \dots, -1\}$. Therefore there are exactly four numbers $x \in \{-1997, \dots, 1997\}$ 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 rather sparse. This conclusion can be translated into the following nice problem.

Example 4. Prove that C does not have bounded gaps, that is there are arbitrarily long sequences of integers, none 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 we have just discussed about: $C = \{n \in \mathbb{Z}|$ if $p|n$ and $p \in B,$ then $v_p(n) \in 2\mathbb{Z}\}$. 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 be $p_1, p_2, \dots, p_n$ (we can take as many as we need, since B is infinite) and then we look for a solution to 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 $x+i$. Because 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 by Erdos and Selfridge. 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. For any p in B, prove that no set of $p-1$ consecutive positive integers can 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 the $p-1$ numbers is a multiple of p, then there must be another one divisible by p (since in this case both 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 the remainders of these numbers when divided by p is exactly $1, 2, \ldots, p-1$. Also from the hypothesis it follows that there exists a positive integer n such that

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

Hence $n^2 \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1 \pmod{p}$, the last congruence following from 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 in the second example are useful tools in solving nonstandard Diophantine equations. You can see this in the following two examples.

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

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 prime factorization 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 is worth noting that the equation $x^2 + y^2 = 4k + 3$ can be solved directly, by working modulo 4.

The following problem is much more difficult, but the basic idea is the same. Yet, the details are not so obvious and, most importantly, it is not clear how to begin.

Example 7.[Barry Powel] 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.

AMM

Solution. Without loss of generality, we may assume that x, y, z, t are relatively prime. Next, we prove that t is odd. Supposing the contrary, we obtain $x^{2p} + y^{2p} + z^{2p} \equiv 0 \pmod{4}$. Because $a^2 \pmod{4} \in \{0, 1\}$, the latter implies that x, y, z are even, contradicting the assumption that $gcd(x, y, z, t) = 1$. Hence t is odd. This implies that at least one of the numbers x, y, z is odd. Suppose that z is odd. 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 look for a prime $q \in B$ 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 (mod 4). This follows from the hypothesis $p \in B$ and the fact that $a^2 \equiv 1 \pmod 4$ for any odd number a. Hence there is $q \in B$ such that $v_q\left(\frac{t^{2p}-z^{2p}}{t^2-z^2}\right)$ is odd. Because $x^{2p}+y^{2p} \in C$, 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 $q|gcd(x,y,z,t)=1$, 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.

Finally, a challenge!

Example 8.[Gabriel Dospinescu] Find the least nonnegative integer n for which there exists a nonconstant 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 $x, y \in \mathbf{Z}$.
For this n, find all functions with the above properties.

Crux Mathematicorum

Solution. We will use all results proved of the beginning of the unit. 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 satisfies the conditions of the problem. Hence f_p is a solution for all $p \in B$.

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

We will now prove that any nonconstant function f which satisfies a) and b) must be of the form f_p. We have already seen that $f(0)=0$. Since $f(1)^2 = f(1)$

and f is nonconstant, we must have $f(1) = 1$. Also, $2f(x)^2 - f(x) = 2f(x^2 + 0^2) - f(x) - f(0) \in \{0, 1\}$ for every integer x. Thus $f(x) \in \{0, 1\}$.

Because $f(-1)^2 = f(1) = 1$ 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 suffices to find $f(p)$ for any prime p. We prove that there is exactly one prime p for which $f(p) = 0$. Because f is nonconstant, there is 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: $0 = 2f(a^2 + b^2)f(p^2 + q^2) = 2f((ap + bq)^2 + (aq - bp)^2)$. Observe that $0 \leq f(x) + f(y) \leq 2f(x^2 + y^2)$ for any x and y, so we must have $f(ap + bq) = f(aq - bp) = 0$. But p and q are relatively prime, so there are integers a and b such that $aq - bp = 1$. Then $1 = f(1) = f(aq - bp) = 0$, a contradiction. So, there is exactly one prime 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 example 1, 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.

Pune problema de pe shortlist 1996 India cu f(3mn+m+n)=4f(m)f(n)+f(m)+f(n).

Problems for training

1. Prove that each $p \in A$ can be represented in exactly one way as the sum of the squares of two integers, up to 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 for which the equation $n = x^2 + y^2$, with $0 \leq x \leq y$ and $gcd(x, y) = 1$ 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 $\max\{|x|, |y|\} < \dfrac{p}{2}$ and $2x\varepsilon\dbinom{2k}{k}$ (mod p), $y \equiv (2k)!x \pmod{p}$. Prove that $p = x^2 + y^2$.

Gauss

5. Find all pairs (m, n) of positive integers 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 1996

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

IMO 1984 Shortlist

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

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

is a perfect square.

Gabriel Dospinescu

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

Bulgaria 1995

10. Prove that the equation $y^2 = x^5 - 4$ has no integer solutions.

Balkan Olympiad 1998

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

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

IMO 1999 Shortlist

13. Prove that there are infinitely many pairs of consecutive numbers, no two of which have 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, AMM 6583

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

b) Suppose that a is a divisor of a number of the form $n^2 + 1$. Prove that $a \in C$.

17. Find all functions $f : \mathbb{Z}^+ \to \mathbb{Z}$ with the properties:
1. $f(a) \geq f(b)$ whenever a divides b.
2. for all positive integers a and b,

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

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 $n > 1$ for which L_n is a perfect square is $n = 3$.

Cohn's theorem

T2'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 $a_1, a_2, \dots, a_n$ and any positive real numbers $x_1, x_2, \dots, x_n$ 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 $\frac{a_1}{x_1} = \frac{a_2}{x_2}$. 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:

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

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

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 $\dfrac{1}{n(n-1)}$ attained when $x_1 = x_2 = \cdots = x_n = \dfrac{1}{\sqrt{n}}$. Indeed, by using the lemma, it follows that the left-hand side is greater than or equal to

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

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

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

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

$$\frac{r_a r_b}{m_a m_b} + \frac{r_b r_c}{m_b m_c} + \frac{r_c r_a}{m_c m_a} \geq 3.$$

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 $\dfrac{a_1^2}{a_1a_2} + \dfrac{a_2^2}{a_2a_3} + \cdots + \dfrac{a_n^2}{a_na_1}$ 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 $\dfrac{a_1}{a_2} + \dfrac{a_2}{a_3} + \cdots + \dfrac{a_n}{a_1}$ as

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

After applying T_2's lemma, we find that

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

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

And we are left with an easy problem: if $t = \dfrac{a_1}{a_2} + \cdots + \dfrac{a_n}{a_1}$, then $\dfrac{t^2}{1+t} \geq \dfrac{nt}{n+1}$, 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, Romania 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 and Bogdan Enescu, TST Romania 2002

13. Find the best constant $k(n)$ such that for any positive real numbers $a_1, a_2, \ldots, a_n$ satisfying $a_1a_2\ldots a_n=1$ the following inequality holds

$$\frac{a_1a_2}{(a_1^2+a_2)(a_2^2+a_1)}+\frac{a_2a_3}{(a_2^2+a_3)(a_3^2+a_2)}+\cdots+\frac{a_na_1}{(a_n^2+a_1)(a_1^2+a_2)}\leq k_n.$$

Gabriel Dospinescu and 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 and Zuming Feng, USAMO 2003

Only graphs, no subgraphs

You have already seen quite a few strategies and ideas so far and you might say: "Enough with these tricks! When will we go to serious facts?" We will try to convince you that these are more than simple tools or tricks. They help to create a good base, which is absolutely indispensable for someone who enjoys mathematics and moreover, they are the first steps to some really beautiful and difficult theorems or problems. And you must admit that the last problems discussed in the previous units are quite serious facts. It is worth mentioning that these strategies are not panacea. This assertion is proved by the fact that every year problems that are based on well-known "tricks" prove to be very difficult in contests.

We will "dissapoint" you again in this unit by focusing on a very familiar theme: graphs without complete subgraphs. Why do we say familiar? Because there are hundreds of problems proposed to different mathematics competitions around the world and in professional journals that deal with this subject. And each such problem 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 $d(V)$ and $C(V)$ the number, respectively the set of vertices adjacent to V. Also, we will say that a graph does not have a complete k subgraph if there are no k vertices any two of which are connected. For simplicity, we will say that G is k-free. First, we will discuss probably the first classical result about k-free graphs, the famous Turan's theorem. But before that, an useful lemma, which is also known as Zarankiewicz's lemma and which is the main step in the proof of Turan's theorem.

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

Solution. Suppose not and take an arbitrary vertex V_1. Then

$$|C(V_1)| > \left[\frac{k-2}{k-1}n\right],$$

so there exists $V_2 \in C(V_1)$. Moreover,

$$\begin{aligned}|C(V_1) \cap C(V_2)| &= d(V_1) + d(V_2) - |C(V_1 \cup V_2)| \\ &\geq 2\left(1 + \left[\frac{k-2}{k-1}n\right]\right) - n > 0.\end{aligned}$$

Pick a vertex $V_3 \in C(V_1) \cap C(V_2)$. A similar argument shows that

$$|C(V_1) \cap C(V_2) \cap C(V_3)| \geq 3\left(1 + \left[\frac{k-2}{k-1}n\right]\right) - 2n.$$

Repeating this argument, we find

$$V_4 \in C(V_1) \cap C(V_2) \cap C(V_3), \ldots, V_{k-1} \in \bigcap_{i=1}^{k-2} C(V_i).$$

Also,

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

This can be proved easily by induction. Thus

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

, and, consequently, we can choose

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

But it is clear that $V_1, V_2, \ldots, V_k$ form a complete k graph, which contradicts the assumption that G is k-free.

We are now ready to prove Turan's theorem.

Example 2.[Turan] The greatest number of edges of a k-free graph with n vertices is

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

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

Solution. We will use induction on n. The first case is trivial, so let us assume the result true for all k-free graphs having $n-1$ vertices. Let G be a k-free graph with n vertices. Using Zarankiewicz's lemma, we can find a vertex V such that

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

Because the subgraph determined by the other $n-1$ vertices is clearly 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

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

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 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's graph and is denoted by $T(n,k)$.

These two examples generate numerous beautiful and difficult problems. For example, using these results yields a straightforward solution for the following Bulgarian problem.

Example 3. There are 2001 towns in a country, each 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 greatest n such that any graph G with 2001 vertices and minimum degree at least 1600 is not n-free. But Zarankiewicz's 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 greatest n for which $\left[\frac{n-2}{n-1}2001\right] < 1600$. It is immediate to see that $n=5$. Thus for $n=5$ 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 $\left[\frac{4}{5}2001\right] = 1600$ and which is of course 6-free. Thus, the answer is $n=5$.

Here is a beautiful application of Turan's 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 at the given 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's theorem, which maximizes the number of edges in a k-free graph. Yet, the reversed form of the reversed form is the natural one. Applying 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's theorem it has at most $\frac{21^2-1}{4} = 110$ edges. And the problem is solved.

At first glance, the following problem seems to have no connection with the previous examples, but, as we will see, it is a simple consequence of Zarankiewicz's lemma. It is an adaptation of an USAMO 1978 problem. Anyway, this is trickier than the actual contest problem.

Example 5. There are n delegates at a conference, each of them knowing at most k languages. Among any three delegates, at least two speak a common language. Find the least number n 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 speak the same language" suggests taking the 3-free graph with vertices the persons and whose edges join persons that do not speak the same language. From Zarankiewicz's 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. Hence there exists a person A and $k + 1$ persons $A_1, A_2, \ldots, A_{k+1}$ that can communicate with A. Because A speaks at most k languages, there are two persons among $A_1, A_2, \ldots, A_{k+1}$ that speak a language also spoken by A. But that language is spoken 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 spoken by more than two delegates. We use again Turan's graph, by creating two groups of $k + 1$ delegates. In each group a person speak 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 an upset at one of the Romanian Team Selection Tests for 2004 IMO, being solved by only four 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.[Gabriel Dospinescu] 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 among them there are three, any two of which having common elements.

TST 2004 Romania

Solution. As the conclusion suggests, we should take a graph with vertices 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's 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. Because 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 $A_{i_1}, \dots, A_{i_{51}}$, all of them having degrees at most 50. Consequently, A_{i_1} is disjoint from at least 50 subsets. Because the union of these fifty 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 $|A_{i_j}| \leq \frac{n}{51}$ for all $j \in \{1, 2, \dots, 51\}$ 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.

We continue with an adaptation of a very nice and quite challenging problem from the American Mathematical Monthly.

Example 7.[A.W Goodman] 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.

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 $\sum\limits_{x \in X} d(x)(n-1-d(x))$. It counts twice every triple (x, y, z) in which x and y are connected, while z is not adjacent to any of x and 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 and 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

$$\sum_{x\in X} d(x)=2m.$$

Finally, two chestnuts. The following problem is not probably directly related to our topic, but since it involves complete subgraphs and since it is a very general and useful result, we prefer to discuss it:

Example 8.[T.S.Motzkin, E.G.Strauss]

Let G be a simple graph. To every vertex of G one assigns a nonnegative real number such that the sum of the numbers assigned to all vertices is 1. For any two connected vertices (by an edge), compute the product of the numbers associated to these vertices. What is the maximal value of the sum of these products?

Solution.

The answer is not obvious at all, so let us start by making a few remarks. If the graph is complete of order n then the problem reduces to finding the maximum of $\sum\limits_{1\leq i<j\leq n} x_i x_j$ knowing that $x_1+x_2+...+x_n=1$. This is easy, since

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

The last inequality is just the Cauchy-Schwarz inequality and we have equality when all variables are $\frac{1}{n}$. Unfortunately, the problem is much more difficult in other cases, but at least we have an idea of a possible answer: indeed, it is easy now to find a lower bound for the maximum: if H is the complete subgraph with maximal number of vertices k , then by assigning these vertices $\frac{1}{k}$ and to all other vertices 0, we find that the desired maximum is at least $frac12(1-\frac{1}{k})$. We still have to solve the difficult part: showing that the desired maximum is at most $frac12(1-\frac{1}{k})$. Let us proceed by induction on the number n of vertices of G. If $n = 1$ everything is clear, so assume the result true for all graphs with at most $n-1$ vertices and take a graph G with n vertices, numbered $1, 2, ..., n$. Let A be the set of vectors with nonnegative coordinates and whose components add up to 1 and E the set of edges of G. Because the function $f(x_1, x_2, ..., x_n) = \sum\limits_{(i,j)\in E} x_i x_j$ is continuous on the compact set A , it attains its maximum in a point $(x_1, x_2, ..., x_n)$. If at least one of the x_i is zero, then $f(G) = f(G_1)$ where G_1 is the graph obtained by erasing vertex i and all edges that are incident to this vertex. It suffices to apply the induction hypothesis to G_1 (clearly, the maximal complete subgraph of G_1 has at most as many vertices as the maximal complete subgraph of G). So, suppose that all x_i are positive. We may assume that G is not complete, since this case has already been discussed. So, let us assume for example that vertices 1 and 2 are not connected. Choose any number $0 < a \leq x_1$ and assign to vertices $1, 2, ..., n$ of G the numbers $x_1 - a, x_2 + a, x_3, ..., x_n$. By maximality of $f(G)$, we must have

$$\sum_{i\in C_1} x_i \leq \sum_{i\in C_2} x_i$$

, where C_1 is the set of vertices that are adjacent to vertex 2 and not adjacent to vertex 1 (the definition of C_2 being clear). By symmetry, we deduce that we must actually have

$$\sum_{i\in C_1} x_i = \sum_{i\in C_2} x_i$$

, which shows that $f(x_1, x_2, ..., x_n) = f(0, x_1 + x_2, x_3, ..., x_n)$. Hence we can apply the previous case and the problem is solved.

The final problem is a very beautiful result on the number of complete subgraphs of a graph:

Example 9.[Leo Moser, J.W.Moon]
What is the maximal number of complete maximal subgraphs that a graph on n vertices can have?

Solution. Let us suppose that $n \geq 5$, the other cases being easy to check. Let $f(n)$ be the desired number and G a graph for which this maximum is attained. Clearly, this graph is not complete, so there are two vertices x and y not connected by an edge. In order to simplify the solution, we need several notations. Let $V(x)$ be the set of vertices that are adjacent to x, $G(x)$ the subgraph obtained by erasing vertex x and $G(x, y)$ the graph obtained by erasing all edges incident to x and replacing them with edges from x to any vertex in $V(y)$. Finally, let $a(x)$ be the number of complete subgraphs with vertices in $V(x)$, maximal with respect to $G(x)$ and let $c(x)$ be the number of complete maximal subgraphs of G that contain x.
Now, we pass to serious things: by erasing edges incident to x , exactly $c(x) -$

$a(x)$ complete maximal subgraphs vanish and by joining x with all vertices of $V(y)$ exactly $c(y)$ complete maximal subgraphs appear. So, if $c(G)$ is the number of complete maximal subgraphs in the graph G, then we have the relation

$$c(G(x,y)) = c(G) + c(y) - c(x) + a(x).$$

By symmetry, we can assume that $c(y) \geq c(x)$. By maximality of $c(G)$, $c(G(x,y)) \leq c(G)$, which is the same as $c(y) = c(x)$ and $a(x) = 0$. Therefore $G(x,y)$ also has $f(n)$ complete maximal subgraphs. In the same way, we deduce that $c(G(x,y)) = c(G(y,x)) = c(G)$. Take now a vertex x and let $x_1, x_2, ..., x_k$ be the vertices not adjacent to x. By performing the previous operations, we change G into $G_1 = G(x_1, x)$, then into $G_2 = G_1(x_2, x)$ and so on until $G_k = G_{k-1}(x_k, x)$, by conserving the number $f(n)$ of maximal complete subgraphs. Observe now that G_k has the property that $x, x_1, ..., x_k$ are not joined by edges, yet $V(x_1) = V(x_2) = ... = V(x_k) = V(x)$. Now, we know what to do: if $V(x)$ is void, we stop the process. Otherwise, consider a vertex of $V(x)$ and apply the previous transformation. In the end, we obtain a complete multipartite graph G' whose vertices can be partitioned into r classes with $n_1, n_2, ..., n_r$ vertices, two vertices being connected by an edge if and only if they do not belong to the same class. Because G' has $f(n)$ maximal complete subgraphs, we deduce that

$$f(n) = max_r(max_{n_1+n_2+...+n_r=n} n_1 n_2 ... n_r).$$

This value can be easily computed. Indeed, let $(n_1, n_2, ..., n_r)$ the r-tuple for which the maximum is attained. If one of these numbers is at least equal to 4, let us say n_1, we consider $(2, n_1 - 2, n_3, ..., n_r)$ for which he product of the components is at least the desired maximum. So, all n_i do not exceed 3. Even more, since $2 \cdot 2 \cdot 2 < 3 \cdot 3$, there are at most two numbers equal to 2 among $n_1, n_2, ..., n_r$. This shows that $f(n) = 3^{\frac{n}{3}}$ if n is a multiple of 3, $f(n) = 4 \cdot 3^{\frac{n-4}{3}}$ if $n - 1$ is a multiple of 3 and $f(n) = 2 \cdot 3^{\frac{n-2}{3}}$ otherwise.

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 greatest number of direct flights?

Japan 1998

2. Let $x_1, x_2, \dots, x_n$ be real numbers. Prove that there are at most $\dfrac{n^2}{4}$ pairs $(i,j) \in \{1, 2, \dots, n\}^2$ such that $1 < |x_i - x_j| < 2$.

MOSP

3. Prove that if n points lie on a circle, then at most $\dfrac{n^2}{3}$ 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 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. Prove that a graph with n vertices and k edges has at least $\dfrac{k}{3n}(4k - n^2)$ 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

7. There are 1999 people participating in an exhibition. Out of any 50 people, at least two do not know each other. Prove that we can find at least 41 people who each know at most 1958 other people.

Taiwan 1999

8. 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 $k\left(1 - \dfrac{4k}{n^2}\right)$ vertices.

USAMO 1995

9. Prove that for every n one can construct a graph with no triangles and whose chromatic number is at least n.

10. 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

11. 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 colors. Prove that we can find a monochromatic triangle.

12. Let G be a regular graph of degree k (every vertex is adjacent to k other vertices) with n vertices. Prove that G and its complementary graph contain together at least $\frac{n(n-1)(n-2)}{6} - \frac{nk(n-k-1)}{2}$ triangles.

13. G is a finite graph such that it does not contain a complete subgraph with 5 vertices and any two triangles have at least point in common. Show that there are at most two points X such that removing X leaves no triangles.

IMO 2001 Shortlist

Complex combinatorics

When reading the title, you will perhaps expect a difficult unit, reflecting the complexity of combinatorics. But, this was not our intention. We just wanted to discuss some combinatorial problems that can be solved elegantly by using complex numbers. At this moment, the reader will probably say that we are crazy, but we will support our idea and prove that complex numbers can play a significant role in solving counting problems and also in problems related to tilings. They also have numerous applications in combinatorial number theory, so our purpose is to illustrate a little bit from each of these situations. After that, you will surely have the pleasure of solving the proposed problems using this technique. To avoid repetition, we will present in the beginning of the discussion a useful result

Lemma. *If p is a prime number and $a_0, a_1, \dots, a_{p-1}$ are rational numbers satisfying*

$$a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{p-1}\varepsilon^{p-1} = 0,$$

where

$$\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p},$$

then $a_0 = a_1 = \cdots = a_{p-1}$.

We will just sketch 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 $1+x+x^2+\cdots+x^{p-1}$ are not relatively prime-because they share a common root-and since $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbf{Q}$, $1 + x + x^2 + \cdots + x^{p-1}$ 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 Romanian Contest "Traian Lalescu". Of course, there is a solution using recursive sequences, but it is by far less elegant than the following one.

Example 1. How many n-digit numbers, all of whose digits are 1, 3, 4, 6, 7, or 9 have the sum of their digits a multiple of 7?

Solution. Let $a_n^{(k)}$ be the number of n-digit numbers, all of whose digits are 1, 3, 4, 6, 7, 9 and whose sum of their digits is congruent to k modulo 7. It is clear that

$$\sum_{k=0}^{6} a_n^{(k)}\varepsilon^k = \sum_{x_1,x_2,\dots,x_n\in\{1,3,4,6,7,9\}} \varepsilon^{x_1+x_2+\cdots+x_n}$$

$$= (\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^9)^n,$$

where $\varepsilon = \cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$. Observing that $1+\varepsilon+\varepsilon^2+\cdots+\varepsilon^6 = 0$ and $\epsilon^9 = \epsilon^2$ helps us bring $(\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^9)^n$ to the simpler form $(-\varepsilon^5)^n$. Let us assume, for example, that n is divisible by 7 (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 q be the common value. Then $7q = \sum_{k=0}^{6} a_n^{(k)} - (-1)^n = 6^n - (-1)^n$ - this is because exactly 6^n numbers have n digits, all equal to 1, 3, 4, 6, 7, 9. In this case we have $a_n^{(0)} = (-1)^n + \frac{6^n - (-1)^n}{7}$. We leave you with 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 is worth mentioning that Nikolai Nikolov won a special prize for the following magnificent solution.

Example 2.[Marcin Kuczma] Let $p > 2$ be a prime number and let $A = \{1, 2, \ldots, 2p\}$. Find the number of subsets of A each having p elements and the sum of the elements divisible by p.

IMO 1995

Solution. Consider $\varepsilon = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ and let x_j be the number of subsets X of A such that $|X| = p$ and $m(X) \equiv j \pmod p$. Then it is not difficult to see 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 $\sum_{1 \le c_1 < c_2 < \cdots < c_p \le 2p} \varepsilon^{c_1 + c_2 + \cdots + c_p}$ is precisely the coefficient of X^p in the expansion $(X + \varepsilon)(X + \varepsilon^2) \ldots (X + \varepsilon^{2p})$. Because $X^p - 1 = (X - 1)(X - \varepsilon) \ldots (X - \varepsilon^{p-1})$, we easily find that $(X + \varepsilon)(X + \varepsilon^2) \ldots (X + \varepsilon^{2p}) = (X^p + 1)^2$. Thus $\sum_{j=0}^{p-1} x_j \varepsilon^j = 2$ and the lemma implies the equality $x_0 - 2 = x_1 = \cdots = x_{p-1}$. Since there are $\binom{2p}{p}$ subsets with p elements, it follows that

$$x_0 + x_1 + \cdots + x_{p-1} = \binom{2p}{p}.$$

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.[Reid Barton] Let n be an integer greater than 1 and let $a_1, a_2, \ldots, a_m$ be positive integers. Denote by $f(k)$ the number of m-tuples $(c_1, c_2, \ldots, c_m)$ such that $1 \leq c_i \leq a_i$, $i = 1, ..., m$ and $c_1 + c_2 + \cdots + c_m \equiv k \pmod{n}$.

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 $n|a_i$.

Rookie Contest 1999

Solution. It is not difficult to observe that

$$\sum_{k=0}^{n-1} f(k)\varepsilon^k = \sum_{1 \leq c_i \leq a_i} \varepsilon^{c_1+c_2+\cdots+c_m} = \prod_{i=1}^{m}(\varepsilon + \varepsilon^2 + \cdots + \varepsilon^{a_i})$$

for any complex number ε such that $\varepsilon^{n-1}+\varepsilon^{n-2}+\cdots+\varepsilon+1 = 0$. Hence one implication of the problem is already showed, since if $f(0) = f(1) = \cdots = f(n-1)$ then clearly 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 ε of the unity. 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 $\sum\limits_{k=0}^{n-1} X^k$ we have $\sum\limits_{k=0}^{n-1} f(k)\varepsilon^k = 0$ and so the polynomial $\sum\limits_{k=0}^{n-1} X^k$ divides $\sum\limits_{k=0}^{n-1} f(k)X^k$. This is because $\sum\limits_{k=0}^{n-1} X^k$ 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 generated by the above solutions might be inhibited by the following problem, where we need in addition several tricky manipulations.

Example 4.[Gabriel Dospinescu] Let $p > 2$ be a prime number and let m and n be multiples of p, with n odd. For any function $f : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ satisfying $p|f(1)+f(2)+\cdots+f(m)$, consider the product $f(1)f(2) \cdot ... \cdot f(m)$. Prove that the sum of these products is divisible by $\left(\dfrac{n}{p}\right)^m$.

Solution. Let $\varepsilon = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$ and let x_k be the sum of $f(1) \cdot f(2) \cdot \cdots \cdot f(m)$, over all functions $f : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ such that $f(1) + f(2) + \cdots + f(m) \equiv k \pmod{p}$. It is clear that

$$\begin{aligned}\sum_{k=0}^{p-1} x_k\varepsilon^k &= \sum_{c_1, c_2, \ldots, c_m \in \{1, 2, \ldots, n\}} c_1 c_2 \ldots c_m \varepsilon^{c_1+c_2+\cdots+c_m} \\ &= (\varepsilon + 2\varepsilon^2 + \cdots + n\varepsilon^n)^m.\end{aligned}$$

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 justify that

$$\varepsilon^{p-1} + \varepsilon^{p-2} + \cdots + \varepsilon + 1 = 0 \Leftrightarrow$$

$$\frac{1}{\varepsilon - 1} = -\frac{1}{p}(\varepsilon^{p-2} + 2\varepsilon^{p-3} + \cdots + (p-2)\varepsilon + p - 1).$$

Considering

$$(X^{p-2} + 2X^{p-3} + \cdots + (p-2)X + p - 1)^m = b_0 + b_1 X + \cdots + b_{m(p-2)} X^{m(p-2)},$$

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

$$c_k = \sum_{j \equiv k \pmod p} b_j.$$

Setting $r = \left(-\dfrac{n}{p}\right)^m$, we have

$$x_0 - rc_0 + (x_1 - rc_1)\varepsilon + \cdots + (x_{p-1} - rc_{p-1})\varepsilon^{p-1} = 0.$$

From the lemma, it follows that $x_0 - rc_0 = x_1 - rc_1 = \cdots = x_{p-1} - rc_{p-1} = k$. Because clearly $c_0, c_1, \ldots, c_{p-1}$ are integers, it remains to prove that $r|k$. Because

$$\begin{aligned} pk &= x_0 + x_1 + \cdots + x_{p-1} - r(c_0 + c_1 + \cdots + c_{p-1}) \\ &= (1 + 2 + \cdots + n)^m - r(b_0 + b_1 + \cdots + b_{m(p-2)}) \\ &= \left(\frac{n(n+1)}{2}\right)^m - r\left(\frac{p(p-1)}{2}\right)^m, \end{aligned}$$

it is clear that $r|k$. Here we have used the conditions in the hypothesis. The problem is solved.

It is time now to leave this kind of problems and to talk 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 reformulate 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 examples.

Example 5.[Gabriel Carrol] Consider a rectangle that can be tiled by a finite combination of $1 \times m$ or $n \times 1$ rectangles, where m, n are positive integers. Prove that it is possible to tile this rectangle using only rectangles $1 \times m$ or only rectangles $n \times 1$.

BMC Contest 2000

Solution. Let the dimensions of the initial rectangle be the positive integers a and b. Now, let us partition the rectangle into 1×1 squares and denote these squares by

$$(1,1),(1,2),\dots,(1,b),\dots,(a,1),(a,2),\dots,(a,b).$$

Next, put the number $\varepsilon_1^x\varepsilon_2^y$ in the square labeled (x,y), 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 in all the squares is 0 and so

$$0 = \sum_{\substack{1\le x\le a\\1\le y\le b}} \varepsilon_1^x\varepsilon_2^y = \sum_{i=1}^{a}\varepsilon_1^i \cdot \sum_{j=1}^{b}\varepsilon_2^j.$$

Hence at least one of the numbers $\displaystyle\sum_{i=1}^{a}\varepsilon_1^i$ and $\displaystyle\sum_{j-1}^{b}\varepsilon_2^j$ is 0. But this means that $n|a$ or $m|b$. In any of these cases, the conclusion of the problem follows.

The idea in the previous problem is quite useful, many tiling problems becoming straightforward. Here is an example:

Example 6. Can we tile a 13×13 table from which we remove the central unit square using only 1×4 or 4×1 rectangles?

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}. Clearly, the sum of the numbers from each 1×4 or 4×1 rectangle is

0. Therefore the sum of all labels is equal to the number corresponding to the central unit square. Hence

$$i^{21} = (i + i^2 + \cdots + i^{13})(i^2 + i^4 + \cdots + i^{26}) = i \cdot \frac{i^{13} - 1}{i - 1} \cdot i^2 \cdot \frac{i^{26} - 1}{i^2 - 1} = i^3,$$

which clearly cannot hold. Thus the assumption we made is wrong and such a tiling is not possible.

The example we are going to discuss now is based on the same idea and here complex numbers are even more involved.

Example 7.[Gabriel Dospinescu] On an 8×9 table we place 3×1 rectangles and "broken" 3×1 rectangles, obtained by removing their central unit square. The rectangles and the "broken" rectangles do not overlap and cannot be rotated. Prove that there exists a set S consisting of 18 squares of the table such that if 70 unit squares are covered, then the remaining two belong to S.

Solution. Again, we label the squares of the table $(1,1)$, $(1,2), \ldots,$ $(8,9)$ by starting from the upper left corner. In the square labeled (k,j) we will place the number $i^j \cdot \varepsilon^k$, where $i^2 = -1$ and $\varepsilon^2 + \varepsilon + 1 = 0$. The sum of the numbers from any rectangle or "broken" rectangle is 0. The sum of all numbers is

$$\left(\sum_{k=1}^{8} \varepsilon^k\right)\left(\sum_{j=1}^{9} i^j\right) = -i.$$

Let us suppose that (a_1, b_1) and (a_2, b_2) are the only uncovered squares. Then $i^{b_1}\varepsilon^{a_1} + i^{b_2}\varepsilon^{a_2} = -i$. Let $z_1 = i^{b_1-1}\varepsilon^{a_1}$ and $z_2 = i^{b_2-1}\varepsilon^{a_2}$. We have $|z_1| = |z_2| = 1$ and $z_1 + z_2 = -1$. It follows that $\frac{1}{z_1} + \frac{1}{z_2} = -1$ 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 a_1, a_2 when divided by 3 are 1 and 2. Thus we can choose S to be 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 they belong to S. The conclusion is immediate.

Finally, a chestnut:

Example 8. Let m and n be integers greater than 1 and let $a_1, a_2, \ldots, a_n$ be integers, none of which is divisible by m^{n-1}. Prove that we can find integers $e_1, e_2, \ldots, e_n$, not all zero, such that $|e_i| < m$ for all i and $m^n | e_1a_1 + e_2a_2 + \cdots + e_na_n$.

IMO 2002 Shortlist

Solution. Look at the numbers $\sum\limits_{i=1}^{n} e_i a_i$, where $1 \leq e_i \leq m$ for all i. Observe that we have a collection of m^n numbers. We can assume that this is a complete system of residues modulo m^n (otherwise, the conclusion is immediate). Now, consider $f(x) = \sum\limits_{a \in A} x^a$. On one hand,

$$f(x) = \prod_{i=1}^{n} \left(\sum_{j=0}^{m-1} x^{j a_i} \right) = \prod_{i=1}^{n} \frac{1 - x^{m a_i}}{1 - x^{a_i}}.$$

On the other hand, take $\varepsilon = e^{\frac{2i\pi}{m^n}}$. Since the m^n numbers we previosly considered form a complete system of residues modulo m^n, we must have $f(\varepsilon) = 0$. Therefore (the hypothesis ensures that $\varepsilon^{a_i} \neq 1$) $\prod\limits_{i=1}^{n}(1 - \varepsilon^{m a_i}) = 0$. But this clearly contradicts the fact that none of the numbers $a_1, a_2, \ldots, a_n$ is a multiple of m^{n-1}.

Problems for training

1 Can we tile a 9×9 table from which we remove the central unit square using only 1×4 or 4×1 rectangles?

2. 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 1987 Shortlist

3. We roll a regular die n times. What is the probability that the sum of the numbers shown is a multiple of 5?

IMC 1999

4. Let a_k, b_k, c_k be integers, $k = 1, 2, ..., n$ and let $f(x)$ be the number of ordered triples (A, B, C) of subsets (not necessarily nonempty) of the set $S = \{1, 2, \ldots, n\}$ whose union is S and for which

$$\sum_{i \in S \setminus A} a_i + \sum_{i \in S \setminus B} b_i + \sum_{i \in S \setminus C} c_i \equiv 3 \pmod{x}.$$

Suppose that $f(0) = f(1) = f(2)$. Prove that there exists $i \in S$ such that $3 | a_i + b_i + c_i$.

Gabriel Dospinescu

5. How many 100-element subsets of the set $\{1, 2, \ldots, 2000\}$ have the sum of their elements a multiple of 5?

Qihong Xie

6. There are 2000 white balls in a box. There is also an unlimited supply of white, green, and red balls, initially outside the box. At each step, we can replace two balls in the box by one or two balls as follows: two whites or two reds by a green; two greens by a white and a red; a white and a green by a red or a green and a red by a white.

a) After a finite number of steps, there are exactly three balls in the box. Prove that at least one of them is green.

b) Is it possible that after a finite number of steps there is only one ball in the box?

Bulgaria 2000

7. A 7×7 table is tiled by sixteen 1×3 rectangles such that only one square remains uncovered. What are the possible positions of this square?

Tournament of the Towns 1984

8. Let k be an integer greater than 2. For which odd positive integers n can we tile a $n \times n$ table by $1 \times k$ or $k \times 1$ rectangles such that only the central unit square is uncovered?

Gabriel Dospinescu

9. Let $n \geq 2$ be an integer. At each point (i, j) having integer coordinates we write the number $i + j \pmod{n}$. Find all pairs (a, b) of positive integers such that any residue modulo n appears the same number of times on the sides of the rectangle with 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 this rectangle.

Bulgaria 2001

10. Let $\mathcal{F}$ be the family of subsets of the set $A = \{1, 2, \ldots, 3n\}$ having the sum of their elements a multiple of 3. For each member of $\mathcal{F}$, compute the square of the sum of its elements. What is the value of the numbers obtained?

Gabriel Dospinescu

11. 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 $p | \displaystyle\sum_{j=0}^{p-1} ja_j$. Also, let k be the number of sequences $(b_1, b_2, \ldots, b_{p-1}) \subset \{0, 1, 3\}^{p-1}$ such that $p | \displaystyle\sum_{j=0}^{p-1} jb_j$. Prove that $h \leq k$ and that the equality holds only for $p = 5$.

IMO 1999 Shortlist

Formal series revisited

We start with a riddle and a challenge: what is the connection between the following problems?

1. The set of nonnegative integers is partitioned into $n \geq 2$ infinite arithmetical sequences with common differences $r_1, r_2, \ldots, r_n$ and first terms $a_1, a_2, \ldots, a_n$. Then

$$\frac{a_1}{r_1} + \frac{a_2}{r_2} + \cdots + \frac{a_n}{r_n} = \frac{n-1}{2}.$$

2. The vertices of a regular polygon are colored such that each set of vertices having the same color is the set of vertices of a regular polygon. Prove that there are two congruent polygons among them.

The first problem was discussed during the preparation of the USA IMO team, but it seems to be a classical result. As for the second one, well, it is a famous problem given at a Russian Olympiad, proposed by N. Vasiliev.

If you have no clue, then we will give you a 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 are those? 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 $\sum\limits_{n\geq 0} a_n X^n$, where $a_n \in A$, and it is also called the generating function of the sequence $(a_n)_{n\geq 0}$. As we are going to see in what follows, formal series have some very nice applications in different fields: algebra, combinatorics, number theory. But let's start working now, assuming familiarity with some basic analysis tools.

Example 1. Let $a_1, a_2, \ldots, a_n$ be complex numbers such that $a_1^k + a_2^k + \cdots + a_n^k = 0$ for all $1 \leq k \leq n$. Then all numbers are equal to 0.

Solution. The experienced reader has already noticed that this problem is an immediate consequence of Newton's relations. But what can we do if we are not familiar with these relations? 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

$$a_1^k + a_2^k + \cdots + a_n^k = 0$$

for all positive integers k. Indeed, let

$$f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 = \prod_{i=1}^{n}(X - a_i).$$

Then

$$a_i^k + b_{n-1}a_i^{k-1} + \cdots + b_0 a_i^{k-n} = 0$$

for all $k \geq n+1$. 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 absolute value among the n numbers. Let the common value of the absolute value be r. By taking a sequence $z_p\to\frac{1}{r}$ such that $|z_p\cdot r|<1$, we obtain a contradiction with the relation $\sum_{i=1}^{n}\frac{1}{1-z_pa_i}=n$ (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.[Gabriel Dospinescu] Let $a_1,a_2,\ldots,a_q,x_1,x_2,\ldots,x_q$ and m be integers such that $m|a_1x_1^k+a_2x_2^k+\cdots+a_qx_q^k$ for all $k\geq 0$. Then

$$m|a_1\prod_{i=2}^{q}(x_1-x_i).$$

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 obtain

$$f(z)=\sum_{i=1}^{q}a_i+\left(\sum_{i=1}^{q}a_ix_i\right)z+\ldots,$$

which shows that all coefficients of this formal series are integers divisible by m. It follows that the formal series

$$\sum a_1(1-x_2z)\ldots(1-x_qz)$$

also has all of its coefficients divisible by m. Now, consider $S_t^{(i)}$ the t-th fundamental symmetric sum in x_j $(j\neq i)$. Because all coefficients of $\sum a_1(1-$

$x_2z)\dots(1-x_qz)$ are multiples of m, a simple computation shows that we have the divisibility relation

$$m|x_1^{q-1}\sum_{i=1}^{q}a_i - x_i^{q-2}\sum_{i=1}^{q}a_iS_1^{(i)}+\dots+(-1)^{q-1}\sum_{i=1}^{q}a_iS_{q-1}^{(i)}.$$

This can also be rewritten as

$$m|\sum_{i=1}^{q}a_i(x_1^{q-1}-x_1^{q-2}S_1^{(i)}+\dots+(-1)^{q-1}S_{q-1}^{(i)}).$$

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

$$x_1^{q-1}-x_1^{q-2}S_1^{(1)}+\dots+(-1)^{q-1}S_{q-1}^{(1)}=(x_1-x_2)\dots(x_1-x_n)$$

and we are done.

In order to solve the problem announced at the very beginning of the presentation, we need a lemma, which is interesting itself and which we prefer to present as a separate problem.

Example 3. Suppose that the set of nonnegative integers is partitioned into a finite number of infinite arithmetical sequences of common differences $r_1, r_2, \dots, r_n$ and first terms $a_1, a_2, \dots, a_n$. Then

$$\frac{1}{r_1}+\frac{1}{r_2}+\dots+\frac{1}{r_n}=1.$$

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 nonnegative integer is exactly in one of the arithmetical sequences. The above relation becomes 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 (1) by $1-x$ and use the fact that $\lim\limits_{x\to 1}\dfrac{1-x^a}{1-x}=a$. We find the desired relation

$$\frac{1}{r_1}+\frac{1}{r_2}+\cdots+\frac{1}{r_n}=1.$$

It's now time to solve the first problem. We will just take a small, but not obvious step and we'll be done. The fundamental relation is again (1).

Example 4. The set of nonnegative integers is partitioned into $n\geq 2$ infinite arithmetical sequences with common differences $r_1,r_2,\ldots,r_n$ and first terms $a_1,a_2,\ldots,a_n$. Then

$$\frac{a_1}{r_1}+\frac{a_2}{r_2}+\cdots+\frac{a_n}{r_n}=\frac{n-1}{2}.$$

MOSP

Solution. Let us write the relation (1) in the more appropriate form:

$$\frac{x^{a_1}}{1+x+\cdots+x^{r_1-1}}+\cdots+\frac{x^{a_n}}{1+x+\cdots+x^{r_n-1}}=1 \tag{2}$$

Now, let us differentiate (2) and then make $x\to 1$ in the resulting expression. An easy computation left to the reader shows that

$$\sum_{i=1}^{n}\frac{a_ir_i-\dfrac{r_i(r_i-1)}{2}}{r_i^2}=0.$$

It suffices now to use the result proved in example 3 in order to conclude that

$$\frac{a_1}{r_1}+\frac{a_2}{r_2}+\cdots+\frac{a_n}{r_n}=\frac{n-1}{2}.$$

Some comments about these two relations are necessary. First of all, using a beautiful and difficult 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 positive integers whose sum of reciprocals is less 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 by induction that

$$\frac{1}{u_1}+\frac{1}{u_2}+\cdots+\frac{1}{u_k}=1-\frac{1}{u_1u_2\ldots u_k}.$$

Thus we can write
$$1-\frac{1}{r_n}\le 1-\frac{1}{u_1u_2\dots u_{n-1}},$$
or, even better, $r_n \le u_1u_2\dots u_{n-1}=u_n-1$ (the last relation following again by a simple induction). Another inductive argument proves that $u_n\le 2^{2^{n-1}}$. And here is how we can prove that $\max(r_1,r_2,\dots,r_n)<2^{2^{n-1}}$. Using the relation proved in example 4, we also deduce that $\max(a_1,a_2,\dots,a_n)<(n-1)\cdot 2^{2^{n-1}-1}$. This shows that for fixed n not only there is a finite number of ways to partition the set of positive integers into n arithmetical sequences, but we also have some explicit (even though huge) bound on the common differences and first terms.

It is now time to solve the remarkable problem discussed at the beginning of this note. We will see that using the previous results proved here, the solution becomes natural. However, the problem is really difficult.

Example 5.[N. Vasiliev] The vertices of a regular polygon are colored such that each set of vertices having the same color is the set of vertices of a regular polygon. Prove that there are two congruent polygons among them.

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 coordinates the numbers $1,\varepsilon,\varepsilon^2,\dots,\varepsilon^{n-1}$, where $\varepsilon=e^{\frac{2i\pi}{n}}$ (of course, we will not lose generality with all these restrictions). Let $n_1,n_2,\dots,n_k$ be the number of edges of each monochromatic polygon and assume that all these numbers are distinct. Let $\varepsilon_j=e^{\frac{2i\pi}{n_j}}$ and observe that the coordinates of the vertices of each monochromatic polygon are $z_j,z_j\varepsilon_j,\dots,z_j\varepsilon_j^{n_j-1}$, for some complex numbers z_j on the unit circle. First, a technical result.

Lemma For any complex number z and $\zeta=e^{\frac{2i\pi}{p}}$ we have the identity
$$\frac{1}{1-z}+\frac{1}{1-z\zeta}+\dots+\frac{1}{1-z\zeta^{p-1}}=\frac{p}{1-z^p}.$$

Proving this lemma is a simple task. Indeed, it suffices to observe that $z,z\zeta,\dots,z\zeta^{p-1}$ are exactly the zeros of $P(X)=X^p-z^p$. Or, observe that
$$\frac{P'(X)}{P(X)}=\frac{1}{X-z}+\dots+\frac{1}{X-z\zeta^{p-1}}.$$

By taking $X=1$ we obtain exactly the desired result.

Now, the hypothesis of the problem and lemma allow us to write
$$\frac{n_1}{1-(zz_1)^{n_1}}+\dots+\frac{n_k}{1-(zz_k)^{n_k}}=\frac{n}{1-z^n}.$$

Also, the simple observation $n_1 + n_2 + \cdots + n_k = n$ yields 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 divide (1) by z^{n_1}. It follows that for any nonzero z we have

$$\frac{n_1 z_1^{n_1}}{1-(zz_1)^{n_1}} + \frac{n_2 z_2^{n_2}}{1-(zz_2)^{n_2}} z^{n_2-n_1} + \cdots + \frac{n_k z_k^{n_k}}{1-(zz_k)^{n_k}} z^{n_k-n_1} = \frac{nz^{n-n_1}}{1-z^n}. \quad (2)$$

We are done: it suffices to observe that if we make $z \to 0$ (by nonzero values) in (2), we obtain $z_1^{n_1} = 0$, which is clearly impossible, since $|z_1| = 1$. The proof ends here.

The problem that we are going to discuss now appeared in various contests under different forms. It is a very nice identity that can be proved elementarily in quite messy ways. Here is a magical proof using formal series.

Example 6. For any complex numbers $a_1, a_2, \ldots, a_n$ 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

$$f(z) = \prod_{i=1}^{n}\left(za_i + \frac{z^2 a_i^2}{2!} + \ldots\right),$$

hence the coefficient of z^n 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: everything is now clear, since the coefficient of z^n in e^{kz} is $\frac{k^n}{n!}$. The conclusion follows. Not only that 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 numbers theory and combinatorics concocts. 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 nonnegative integers such that for all n the equation $a_i + 2a_j + 4a_k = n$ has a unique solution (i, j, k). Find a_{1998}.

IMO 1998 Shortlist

Solution. Here is the very nice answer: 9817030729. Let $A = \{a_0, a_1, \dots\}$ and let $b_n = 1$ if $n \in A$ and 0 otherwise. Next, consider the formal series $f(x) = \sum\limits_{n\geq 0} b_n x^n$, the generating function of the set A (we can write it in a more intuitive way $f(x) = \sum\limits_{n\geq 0} x^{a_n}$). 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 that

$$\prod_{k\geq 0} f(x^{2^k}) = \prod_{k\geq 0}(f(x^{2^{3k}})f(x^{2^{3k+1}})f(x^{2^{3k+2}})) = \prod_{k\geq 0}\frac{1}{1-x^{2^{3k}}}$$

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 (you have observed that rigor was not the strong point in establishing these relations)

$$f(x) = \prod_{k\geq 0}\frac{1-x^{2^{3k+1}}}{1-x^{2^{3k}}} = \prod_{k\geq 0}(1+x^{8^k})$$

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 at the 2003 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. Let f and g be the generating functions of A and B respectively. Then

$$f(x) = \sum_{n \geq 0} a_n x^n, \quad g(x) = \sum_{n \geq 0} b_n x^n$$

where, as in the previous problem, a_n equals 1 if $n \in A$ and 0 otherwise. The fact that A and 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 on the number of solutions of the equation $x + y = n$ imposes that

$$f^2(x) - f(x^2) = g^2(x) - g(x^2).$$

Hence

$$f(x^2) - g(x^2) = \frac{f(x) - g(x)}{1 - x},$$

which can 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. After multiplication, we deduce that

$$f(x) - g(x) = \prod_{k \geq 0} (1 - x^{2^k}) \lim_{n \to \infty} \frac{1}{f(x^{2^n}) - g(x^{2^n})}.$$

Let us assume without loss of generality that $0 \in A$. You 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 the digits in the binary representation of x. Taking into account the relation

$$f(x) + g(x) = \frac{1}{1-x},$$

we finally deduce that A and B are respectively the set of nonnegative integers having even (respectively odd) sum of digits when written in base 2.

We will discuss a nice problem in which formal series and complex numbers appear in a quite spectacular way:

Example 9. Let n and 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 $\sum\limits_{x \in A} x \equiv m \pmod{2^k}$ does not depend on $m \in \{0, 1, \ldots, 2^k - 1\}$.

Balkan Olympiad 2005 Shortlist

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 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 settles our claim and finishes the proof.

Finally, it is time for a tough problem. Of course, it will be a combinatorial one, whose nice solution below was found by Constantin Tanasescu.

Example 10.[Adrian Zahariuc] Let S be the set of all words which can be formed using $m \geq 2$ given letters. For any $w \in S$, let $l(w)$ be its length. Also, let $W \subseteq S$ be a set of words. We know that any word in S can be obtained in at most one way by concatenating words from W. Prove that

$$\sum_{w \in W} \frac{1}{m^{l(w)}} \leq 1.$$

Solution. Let A be the set of all words which can be obtained by concatenating words from W. Let

$$f(x) = \sum_{w \in W} x^{l(w)}, \quad g(x) = \sum_{w \in A} x^{l(w)}.$$

By the definition of A,

$$g(x) = 1 + f(x) + f^2(x) + \cdots = \frac{1}{1 - f(x)}.$$

Hence

$$f(x)g(x) = g(x) - 1. \tag{$*$}$$

Now, A (and W) 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 $f\left(\dfrac{1}{m}\right) \leq 1$, which is nothing else than the desired inequality.

Problems for training

1. Let $z_1, z_2, \ldots, z_n$ be arbitrary complex numbers. Prove that for any $\varepsilon > 0$ there are infinitely many numbers k 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 term of the sequence $(x_n)_{n \geq 1}$ given by

$$x_{n+k} = a_1 x_{n+k-1} + \cdots + a_k x_n$$

with respect to $x_1, \ldots, x_k$. Here $a_1, \ldots, a_k$ and $x_1, \ldots, x_k$ are arbitrary complex numbers.

3. Prove that if we partition the set of nonnegative integers into a finite number of infinite arithmetical sequences, then there will be two of them having the same common difference.

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. Let $A_1 = \emptyset$, $B_1 = \{0\}$ and $A_{n+1} = \{1 + x|\ x \in B_n\}$, $B_{n+1} = (A_n \setminus B_n) \cup (B_n \setminus A_n)$. Find all positive integers n such that $B_n = \{0\}$?

AMM

6. In how many ways can we parenthesize a non-associative product $a_1 a_2 \ldots a_n$?

Catalan

7. For which positive integers n can we find real numbers $a_1, a_2, \ldots, a_n$ such that

$$\{|a_i - a_j| \mid 1 \le i < j \le n\} = \left\{1, 2, \ldots, \binom{n}{2}\right\}?$$

China TST 2002

8. Let $a_1, a_2, \ldots, a_n$ be relatively prime positive integers. Find in closed form a sequence $(x_k)_{k \ge 1}$ such that if y_k 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 $\lim\limits_{k \to \infty} \dfrac{x_k}{y_k} = 1$.

9. Let $A_1, A_2, \ldots, A_k$ be $n \times n$ matrices with complex entries such that

$$\|A_1^p + A_2^p + \cdots + A_k^p\| \le \frac{C}{p!}$$

for any integer $p \ge 1$. Here C does not depend on p and $\|X\| = \max\limits_{1 \le i,j \le n} |x_{ij}|$. Prove that $A_i^n = 0$ for all $1 \le i \le k$.

Gabriel Dospinescu

10. Is there an infinite set of nonnegative integers 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 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

12. Suppose that $a_0 = a_1 = 1$ and $(n + 3)a_{n+1} = (2n + 3)a_n + 3na_{n-1}$ for $n \ge 1$. Prove that all terms of this sequence are integers.

Komal

13. Define the sequences of integers (a_n) and (b_n) as follows :$a_1 = b_1 = 0$ and

$$a_n = nb_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1,$$

for all $n \geq 2$.

Prove that $p|a_p$ for any prime number p.

Komal

14. Is it possible to partition the set of all 12-digit numbers into groups of four numbers such that the numbers in each group have the same digits in 11 places and four consecutive digits in the remaining place?

Saint Petersburg Olympiad

15. Prove the identity

$$\sum_{k=1}^{n} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \sum_{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{-1,1\}} \frac{(-1)^k}{2^k} (\varepsilon_1 a_{i_1} + \varepsilon_2 a_{i_2} + \cdots + \varepsilon_k a_{i_k})^{2n}$$

$$= \frac{(-1)^n (2n)! a_1^2 a_2^2 \ldots a_n^2}{2^n}$$

holds for any complex numbers $a_1, a_2, \ldots, a_n$.

Gabriel Dospinescu

16. A set A of positive integers has the property that for some positive integers b_i, c_i, the sets $b_i A + c_i$, $1 \leq i \leq n$ are disjoint subsets of A. Prove that

$$\sum_{i=1}^{n} \frac{1}{b_i} \leq 1.$$

IMO 2004 Shortlist

17.[R. Stong] Determine whether there is a subset X of the integers with the following property: for any integer n there is exactly one solution of $a + 2b = n$ with $a, b \in X$.

USAMO 1996

A little introduction to algebraic number theory

We have already seen some topics where algebra, number theory and combinatorics were mixed in order to obtain some beautiful results. We are aware that such topics are not so easy to digest by the unexperienced reader, but we also think that it is fundamental to have a unitary vision of elementary mathematics. This is why we decided to combine in this chapter algebra and number theory. Your effort and patience will be tested again. The purpose of this chapter to survey some classical results concerning algebraic numbers and their applications, as well as some connections between number theory and linear algebra.

First, we recall 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

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \neq 0$$

has only the trivial solution. Second, we need Vandermonde's identity

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1\leq i<j\leq n} (x_j - x_i). \qquad (1).$$

Finally, when studying the algebraic numbers, we will need two more specific results. The first one is due to Hamilton and Cayley, while the second one is known as the fundamental theorem of symmetric polynomials

Theorem 1

For any field F and any matrix $A \in M_n(F)$, if p_A is the characteristic polynomial of A: $p_A(X) = det(XI_n - A)$, then $p_A(A) = O_n$.

Theorem 2

Let A be a ring and let $f \in A[X_1, X_2, ..., X_n]$ be a symmetric polynomial with coefficients in A, that is for any permutation $\sigma \in S_n$ we have $f(X_1, X_2, ..., X_n) = f(X_\sigma(1), X_\sigma(2), ..., X_\sigma(n))$. Then we can find a polynomial $g \in A[X_1, X_2, ..., X_n]$ such that $f(X_1, X_2, ..., X_n) = g(X_1 + X_2 + ... + X_n, X_1X_2 + X_1X_3 + ... + X_{n-1}X_n, ..., X_1X_2...X_n)$.

This means that any symmetric polynomial with coefficients in a ring is a polynomial (with coefficients in the same ring) in the symmetric fundamental sums:

$$S_k(X_1, ..., X_n) = \sum_{1\leq i_1<i_2<...<i_k\leq n} X_{i_1} \cdot ... \cdot X_{i_k}$$

.

As usual we start with some easy examples. Here is a nice (and direct) application of theorem 2:

Example 1. Given a polynomial with complex coefficients, can one decide if it has a double zero only by performing additions, multiplications, and divisions on its coefficients?

Solution. Yes, one can, even though at first glance this does not seem natural. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then this polynomial has a double zero if and only if

$$\left(\prod_{1\leq i<j\leq n} (x_i - x_j)\right)^2 = 0,$$

where $x_1, x_2, \ldots, x_n$ are the zeros of the polynomial. But the polynomial

$$\prod_{1\leq i<j\leq n} (x_i - x_j)^2$$

is symmetric with respect to $x_1, x_2, ..., x_n$, so by theorem 2 it is a polynomial in the fundamental symmetric sums in $x_1, x_2, ..., x_n$. By Vieta's formulas, these fundamental sums are just the coefficients of f (up to a sign), so

$$\left(\prod_{1\leq i<j\leq n} (x_i - x_j)\right)^2$$

is a polynomial on the coefficients of f. Consequently, we can decide whether

$$\left(\prod_{1\leq i<j\leq n} (x_i - x_j)\right)^2 = 0$$

only by using the operations on the coefficients of the polynomial mentioned in the hypothesis. This shows that the answer to the problem is positive.

You may know the following classical problem: if $a, b, c \in \mathbf{Q}$ satisfy $a+b\sqrt[3]{2}+c\sqrt[3]{4} = 0$, 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, there is a direct solution using Eisenstein's criterion applied to the polynomial $f(X) = X^n - 2$, but here is a beautiful proof using linear algebra. This time we need to be careful and work in the most appropriate field.

Example 2. Prove that if $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}$ satisfy

$$a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2^{n-1}} = 0,$$

then $a_0 = a_1 = \cdots = a_{n-1} = 0$.

Solution. If $a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2^{n-1}} = 0$, then

$$ka_0 + ka_1 \sqrt[n]{2} + \cdots + ka_{n-1} \sqrt[n]{2^{n-1}} = 0$$

for any real number k. Hence we may assume that $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}$. The idea is to choose n values for k 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 good values for k? This can be seen by noticing that $\sqrt[n]{2^{n-1}} \cdot \sqrt[n]{2} = 2 \in \mathbf{Z}$. 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 $\mathbf{Z}_2$, 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 $\mathbf{Z}_2$, it yields $\overline{a}_1^n = \overline{0}$. 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 3. 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 $A = ax + bz + cy$, $B = ay + bx + cz$, $C = az + by + cx$. 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 $v = (v_1, v_2, \dots, v_n)$ such that v_i are relatively prime. Consider the numbers $\frac{v_1}{g}, \frac{v_2}{g}, \dots, \frac{v_{n-1}}{g}$, where g is the greatest common divisor of $v_1, v_2, \dots, v_{n-1}$. They are relatively prime and thus we can find an integral matrix

$$\begin{pmatrix} \frac{v_1}{g} & a_{12} & \dots & a_{1,n-1} \\ \dots & \dots & \dots & \dots \\ \frac{v_{n-1}}{g} & a_{n-1,2} & \dots & a_{n-1,n} \end{pmatrix}$$

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:

$$\begin{pmatrix} v_1 & a_{12} & \dots & a_{1,n-1} & (-1)^{n-1}\beta\frac{v_1}{g} \\ \dots & \dots & \dots & \dots & \dots \\ v_{n-1} & a_{n-1,2} & \dots & a_{n-1,n-1} & (-1)^{n-1}\beta\frac{v_{n-1}}{g} \\ v_n & 0 & \dots & 0 & (-1)^{n-1}\alpha \end{pmatrix}.$$

In chapter **Look at the exponent** we have seen a rather complicated solution for the following problem. Here is one much easier, yet difficult to find:

Example 6.[Armond Spencer] For any integers $a_1, a_2, \dots, a_n$ then

$$\prod_{1 \le i < j \le n} \frac{a_j - a_i}{j - i} \in \mathbf{Z}.$$

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 it is easy to prove that $\prod_{1 \le i < j \le n} (j - i)$ equals $(n-1)!(n-2)!\dots 1!$. Now, we can write

$$\prod_{1 \le i < j \le n} \frac{a_j - a_i}{j - i} = \frac{1}{1! \cdot 2! \dots (n-1)!} \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ \dots & \dots & \dots & \dots & \dots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{vmatrix}.$$

As usual, the last step is the most important. The above formula can be rewritten as

$$\prod_{1\le i<j\le n}\frac{a_j-a_i}{j-i}=\begin{vmatrix} 1 & 1 & 1 & \dots & 1\\ \dfrac{a_1}{1!} & \dfrac{a_2}{1!} & \dfrac{a_3}{1!} & \dots & \dfrac{a_n}{1!}\\ \dots & \dots & \dots & \dots & \dots\\ \dfrac{a_1^{n-1}}{(n-1)!} & \dfrac{a_2^{n-1}}{(n-1)!} & \dfrac{a_3^{n-1}}{(n-1)!} & \dots & \dfrac{a_n^{n-1}}{(n-1)!}\end{vmatrix}.$$

And now we recognize the form

$$\prod_{1\le i<j\le n}\frac{a_j-a_i}{j-i}=\begin{vmatrix} 1 & 1 & \dots & 1\\ \dbinom{a_1}{1} & \dbinom{a_2}{1} & \dots & \dbinom{a_n}{1}\\ \dbinom{a_1}{2} & \dbinom{a_2}{2} & \dots & \dbinom{a_n}{2}\\ \dots & \dots & \dots & \dots\\ \dbinom{a_1}{n-1} & \dbinom{a_2}{n-1} & \dots & \dbinom{a_n}{n-1}\end{vmatrix},$$

which can be proved easily by subtracting lines. Because each number $\dbinom{a_i}{j}$ is an integer, the determinant itself is an integer and the conclusion follows.

At this point, you might dissapointed because we did not keep our promise: no trace of algebraic numbers appeared until now! Yet, we considered that a small introduction featuring easy problems and applications of linear algebra in number theory was absolutely necessary. Now, we can pass to the real purpose of this chapter, a small study of algebraic numbers. But what are they? Let us start with some definitions: we say that a complex number x is algebraic if it is a zero of a polynomial with rational coefficients. The monic polynomial of least degree, with rational coefficients and having x as a zero is called the minimal polynomial of x. Its other complex zeros are called the conjugates of x. Using the division algorithm, it is not difficult to prove that any polynomial with rational coefficients which has x as zero is a multiple of the minimal polynomial of x. Also, it is clear that the minimal polynomial of an algebraic number is irreducible in $\mathbf{Q}[X]$. We say that the complex number x is an algebraic integer if it is zero of a monic polynomial with integer coefficients. You can prove, using Gauss's lemma that an algebraic number is an algebraic integer if and only if its minimal polynomial has integer coefficients. In order to avoid confusion, we will call the usual integers rational integers in this chapter. There are two very important results concerning algebraic integers that you should know:

Theorem 3

The sum or product of two algebraic numbers is algebraic. The sum or product of two algebraic integers is an algebraic integer.

The result is extremely important, because it shows that the algebraic integers form a ring. Denote by AI this ring. None of the known proofs is really easy. The one that we are going to present uses the fundamental theorem of symmetric polynomials. Consider two algebraic numbers x and y and let $x_1, x_2, ..., x_n$ and $y_1, y_2, ..., y_m$ be all zeros of the minimal polynomials of x and y respectively. Next, look at the polynomial $f(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - x_i - y_j)$. We claim that is has rational coefficients (the fact that $x + y$ is a zero of f being obvious). This follows from theorem 2, because the coefficients of f are symmetric polynomials in $x_1, x_2, ..., x_n$ and $y_1, y_2, ..., y_m$ and therefore they are polynomials in the symmetric fundamental sums of x_i and y_j, which are (up to a sign) the coefficients of the minimal polynomials of x and y. Hence f has rational coefficients and $x + y$ is an algebraic number. Clearly, the proof can be adapted for algebraic integers, since theorem 2 works for any ring, not only for fields. The proof that xy is algebraic (respectively algebraic integer) is identical, by considering the polynomial $g(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - x_i \cdot y_j)$.

The next result is also very important and we will see some of its applications in the following examples.

Theorem 4

The only rational numbers which are also algebraic integers are the rational integers.

The proof of this result is much easier. Indeed, suppose that $x = \frac{p}{q}$ is a rational number (with $gcd(p, q) = 1$) which is also a zero of the polynomial with integer coefficients $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$. Then $p^n + a_{n-1}p^{n-1}q + ... + a_1pq^{n-1} + a_0q^n = 0$. Therefore q divides p^n and since $gcd(q, p^n) = 1$, we must have $q = \pm 1$, which shows that x is a rational integer. Clearly, any rational integer x is an algebraic integer.

Here is a very nice and difficult problem that appeared in AMM in 1998 and which is a consequence of these results. We prefer to give two solutions, one using the previous results and another one using linear algebra. A variant of this problem was given in 2004 at a TST in Romania and turned out to be a difficult 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 $x_{n+4} = x_{n+1} + x_n$. Prove that for any prime p the number x_p is a multiple of p.

AMM

Solution 1. Naturally, we start by considering the caracteristic polynomial of the recursive relation: $X^4 - X - 1$. It is easy to see that it cannot have a double zero. Using the theory of linear recursive sequences, it follows that the general term of the sequence is of the form $Ar_1^n + Br_2^n + Cr_3^n + Dr_4^n$ for some constants A, B, C, D. Here r_i are the distinct zeros of the caracteristic polynomial. Because this polynomial has no rational zero, it is natural to suppose that $Ar_1^n + Br_2^n + Cr_3^n + Dr_4^n$ is symmetric in r_1, r_2, r_3, r_4 and thus $A = B = C = D$. Because $x_0 = 4$, we should take $A = B = C = D = 1$. Now, let us see whether we can prove that $x_n = r_1^n + r_2^n + r_3^n + r_4^n$ for all n. Using Vieta's formulas, we can check that this holds for n less than 4. But since $r_i^{n+4} = r_i^{n+1} + r_i^n$, an inductive argument shows that the formula is true for any n. Hence we need to prove that p divides $r_1^p + r_2^p + r_3^p + r_4^p$ for any prime number p. This follows from the more general result (which is also a generalization of Fermat's little theorem):

Theorem

Let f be a monic polynomial with integer coefficients and let $r_1, r_2, ..., r_n$ be its zeros (not necessarily distinct). Then $A = (r_1+r_2+...+r_n)^p - (r_1^p+r_2^p+...+r_n^p)$ is a rational integer divisible by p for any prime number p.

Theorem 2 shows that A is a rational integer, because it is a symmetric polynomial in $r_1, r_2, ..., r_n$, therefore a poynomial with integer coefficients in the coefficients of f. The difficulty is to prove that it is a multiple of p. First of all, let us prove by induction that if $a_1, a_2, ..., a_n$ are algebraic integers then $\frac{1}{p} \cdot ((a_1 + a_2 + ... + a_n)^p - (a_1^p + a_2^p + ... + a_n^p))$ is an algebraic integer. For $n = 2$, this follows from the binomial formula $\frac{1}{p} \cdot ((a + b)^p - a^p - b^p) = \sum_{i=1}^{p-1} \frac{1}{p} \cdot \binom{p}{i} \cdot a^{p-i} b^i$. Indeed, $\frac{1}{p} \cdot \binom{p}{i}$ is an integer and we obtain a sum of products of algebraic integers, therefore an algebraic integer. Now, if the assertion is true for $n-1$, consider $a_1, a_2, ..., a_n$ algebraic integers. By the inductive hypothesis, $(a_1 + a_2 + ... + a_{n-1})^p - (a_1^p + a_2^p + ... + a_{n-1}^p) \in p \cdot AI$. The case $n = 2$ shows that $(a_1 + a_2 + ... + a_n)^p - (a_1 + a_2 + ... + a_{n-1})^p - a_n^p \in p \cdot AI$. Therefore, $(a_1 + a_2 + ... + a_n)^p - (a_1^p + a_2^p + ... + a_n^p) \in p \cdot AI$, which is exactly what we needed to finish the inductive step. Now, finishing the proof of the theorem is easy: we know that $\frac{1}{p} \cdot ((a_1 + a_2 + ... + a_n)^p - (a_1^p + a_2^p + ... + a_n^p))$ is a rational number which is also an algebraic integer. By theorem 4, it must be a rational integer.

¡pune problema cu $\sqrt{k+1} - \sqrt{k}$ nu a partea reala a vreounei radacini a unitatii. (training of the Chinese IMO team).

Solution 2.

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 $tr(X)$ be the sum of the entries of the main diagonal of the matrix X. We will first prove that $x_n = Tr(A^n)$ (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 $i = 1, 2, \dots, n-1$ and prove that it is also true for n. This follows from

$$x_n = x_{n-4} + x_{n-3} = Tr(A^{n-4}) + Tr(A^{n-3}) = Tr(A^{n-4}(A + I_4)) = Tr(A^n).$$

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 $Tr(A^p) \equiv Tr(A) \pmod{p}$ 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 working in a field in which the characteristic polynomial of A has all its zeroes $\lambda_1, \lambda_2, \dots, \lambda_n$. This field has clearly characteristic p (it contains Z_p) and so we have (using the binomial formula and the fact that all coefficients $\binom{p}{k}$, $1 \le k \le p-1$ are multiples of p)

$$tr(A^p) = \sum_{i=1}^{n} \lambda_i^p = \left(\sum_{i=1}^{n} \lambda_i \right)^p = (TrA)^p,$$

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

$$(A + B)^p = \sum_{A_1, \dots, A_p \in \{A, B\}} A_1 A_2 \dots A_p.$$

Observe that for any A, B we have $Tr(AB) = Tr(BA)$, and, by induction, for any $X_1, X_2, \dots, X_n$ and any cyclic permutation σ,

$$Tr(X_1 X_2 \dots X_n) = Tr(X_{\sigma(1)} X_{\sigma(2)} \dots X_{\sigma(n)}).$$

Now, note that in the sum $\displaystyle\sum_{A_1, \dots, A_p \in \{A, B\}} A_1 A_2 \dots A_p$ we can form $\dfrac{2^p - 2}{p}$ groups of p-cycles and that we have two more terms, A^p and B^p. Thus

$$\sum_{A_1, \dots, A_p \in \{A, B\}} Tr(A_1 A_2 \dots A_p) \equiv Tr(A^p) + Tr(B^p)$$

modulo p (you have already noticed that Fermat's little theorem comes handy once again), since the sum of $Tr(A_1A_2\dots A_p)$ is a multiple of p in any cycle. Thus we have proved that

$$Tr(A+B)^p \equiv Tr(A^p) + Tr(B^p) \pmod p$$

and by an immediate induction we also have

$$Tr(A_1 + \cdots + A_k)^p \equiv \sum_{i=1}^{k} Tr(A_i^p).$$

Next, consider the matrices E_{ij} that have 1 in the position (i,j) and 0 elsewhere. For these matrices we clearly have $Tr(A^p) \equiv Tr(A) \pmod p$ and by using the above result we can write (using Fermat's little theorem one more time):

$$TrA^p = Tr\left(\sum_{i,j} a_{ij}E_{ij}\right)^p$$

$$\equiv \sum_{i,j} Tr(a_{ij}^p E_{ij}^p) \equiv \sum_{i,j} a_{ij} Tr E_{ij} = TrA \pmod p.$$

The result is proved and with it the fact that x_p is a multiple of p.

The example we are about to discuss next generated a whole mathematical theory and even an important area of research in transcendental number theory. Let us start by introducing a definition: for a complex polynomial

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 = a_n(X-x_1)\cdot(X-x_2)\cdot ...\cdot(X-x_n)$$

define the Mahler measure of f to be

$$M(f) = |a_n| \cdot max(1, |x_1|) \cdot ... \cdot max(1, |x_n|).$$

You can immediately see that $M(fg) = M(f)\cdot M(g)$ for any polynomials f and g. Using complex analysis tools, one can prove the following beautiful identity:

$$M(f) = e^{\int_0^1 ln|f(e^{2i\pi t})|dt}.$$

The next problem shows that a monic polynomial with integer coefficients and Mahler measure 1 has necessarily all of its zeros roots of the unity. Stated otherwise, the only algebraic integers all of whose conjugates lie on the unit circle of the complex plane are the roots of the unity. This result is the celebrated Kronecker's theorem.

Example 8.[Kronecker] Let f be a monic polynomial with integer coefficients such that $f(0) \neq 0$ and $M(f) = 1$. Then for each zero z of f there exists n such that $z^n = 1$.

Solution What you are going to read now is one of those mathematical jewels that you do not come across every day, so enjoy the following proof. Let $f(X) = (X - x_1) \cdot (X - x_2) \cdot \ldots \cdot (X - x_n)$ be the factorization of f in $\mathbf{C}[X]$. Consider now the polynomials $f_k(X) = (X - x_1^k) \cdot (X - x_2^k) \cdot \ldots \cdot (X - x_n^k)$. The coefficients of these polynomials are symmetric polynomials in $x_1, x_2, ..., x_n$ and since all symmetric fundamental sums of $x_1, x_2, ..., x_n$ are integers, all f_k have integer coefficients (we used theorem 2 here). What is really awesome is that there is a uniform bound on the coefficients of f_k. Indeed, because all x_i have absolute values at most 1, all symmetric fundamental sums in $x_1^k, x_2^k, ..., x_n^k$ have absolute values at most $\binom{n}{[\frac{n}{2}]}$. Therefore, all coefficients of all polynomials f_k are integers between $-\binom{n}{[\frac{n}{2}]}$ and $\binom{n}{[\frac{n}{2}]}$. This shows that there are two identical polynomials among $f_1, f_2, f_3, \ldots$. Let $i > j$ such that $f_i = f_j$. Consequently, there is a permutation σ of $1, 2, ..., n$ such that $x_1^i = x_{\sigma(1)}^j, ..., x_n^i = x_{\sigma(n)}^j$. An easy induction shows that $x_1^{i^r} = x_{\sigma^r(1)}^j$ for all $r \geq 1$. Because $\sigma^{n!}(1) = 1$, we deduce that $x_1^{i^{n!} - j} = 1$ and so x_1 is a root of the unity. Clearly, we can similarly prove that $x_2, x_3, ..., x_n$ are roots of the unity.

Some more comments on the previous examples are needed. First of all, it is not difficult to deduce from this result that the only monic polynomials with integer coefficients whose Mahler measure is 1 are products of X and some cyclotomic polynomials. A famous conjecture of Lehmer says that there exists a constant $c > 1$ such that if a polynomial with integer coefficients has Mahler measure greater than 1, then its Mahler measure is actually greater than c. The polynomial with least Mahler measure found until now is $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$, whose Mahler measure is about 1.176.

Showing that a sum of square roots of positive integers is not a rational number is not difficult as long as the number of square roots is less than 3. Otherwise, this is much more complicated. Actually, one can prove the very beautiful result saying that if $a_1, ..., a_n$ are positive integers such that $\sqrt{a_1} + \ldots + \sqrt{a_n}$ is a rational number, then all a_i are perfect squares. The following problem claims much less, without being simple. We will see how easy it becomes in the framework of the above results.

Example 9. Prove that the number $\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \ldots + \sqrt{2000^2 + 1}$ is irrational.

Chinese TST 2005

Solution

Let us suppose that the number is rational. Because it is a sum of algebraic integers, it is also an algebraic integer. By theorem 4, it follows that $\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \ldots + \sqrt{2000^2 + 1}$ is a rational integer. Hence

$$\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \ldots + \sqrt{2000^2 + 1} - (1001 + 1002 + \ldots + 2000)$$

is a rational integer. But this cannot hold, because

$$\sqrt{1001^2+1}+\sqrt{1002^2+1}+...+\sqrt{2000^2+1}-(1001+1002+...+2000)=$$
$$\frac{1}{1001+\sqrt{1001^2+1}}+\frac{1}{1002+\sqrt{1002^2+1}}+...+\frac{1}{2000+\sqrt{2000^2+1}}$$
is greater than 0 and smaller than 1.

Here is an extremely beautiful and difficult problem, where properties of algebraic integers come to the spotlight.

Example 10.
Let $a_1, a_2, ..., a_k$ be positive real numbers such that $\sqrt[n]{a_1}+\sqrt[n]{a_2}+...+\sqrt[n]{a_k}$ is a rational number for all $n \geq 2$. Prove that $a_1 = a_2 = ... = a_k = 1$.

Solution
First of all, we will prove that $a_1, a_2, ..., a_k$ are algebraic numbers and that $a_1 \cdot a_2 \cdot ... \cdot a_k = 1$. Take an integer $N > k$ and put $x_1 = \sqrt[N!]{a_1}, x_2 = \sqrt[N!]{a_2}, ..., x_k = \sqrt[N!]{a_k}$. Then clearly $x_1^j + x_2^j + ... + x_k^j$ is rational for all $1 \leq j \leq N$. Using Newton's formula, we can easily deduce that all symmetric fundamental sums of $x_1, x_2, ..., x_k$ are rational numbers. Hence $x_1, x_2, ..., x_k$ are algebraic numbers and so $a_1 = x_1^{N!}, a_2 = x_2^{N!}, ..., a_k = x_k^{N!}$ are algebraic numbers as well. Also, by the argument above, we know that $x_1 \cdot x_2 \cdot ... \cdot x_k = \sqrt[N!]{a_1 \dot{a}_2 \cdot ... \cdot a_k}$ is rational and this happens for all $N > k$. This implies immediately that $a_1 \cdot a_2 \cdot ... \cdot a_k = 1$. Let now $f(x) = b_r X^r + b_{r-1} X^{r-1} + ... + b_0$ be a polynomial with integer coefficients which vanishes at $a_1, a_2, ..., a_k$. Clearly, $b_r a_1, ..., b_r a_k$ are algebraic integers. But then

$$b_r(\sqrt[n]{a_1}+\sqrt[n]{a_2}+...+\sqrt[n]{a_k}) = \sqrt{b_r^{n-1}} \cdot (\sqrt[n]{b_r a_1}+\sqrt[n]{b_r a_2}+...+\sqrt[n]{b_r a_k})$$

is also an algebraic integer. Because it is clearly a rational number, it follows that it is a rational integer. Consequently, $(b_r(\sqrt[n]{a_1}+\sqrt[n]{a_2}+...+\sqrt[n]{a_k}))_{n\geq 1}$ is a sequence of positive integers. Because it clearly converges to kb_r, it becomes eventually equal to kb_r. Thus there is n such that $\sqrt[n]{a_1}+\sqrt[n]{a_2}+...+\sqrt[n]{a_k} = k$. Because $a_1 \cdot a_2 \cdot ... \cdot a_k = 1$, the AM-GM inequality implies $a_1 = a_2 = ... = a_k = 1$ and the problem is solved.

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

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n \text{ and } F_{m+n} = F_n F_{m-1} + F_{n+1} F_m.$$

2. Compute the product $\prod\limits_{0\leq i<j\leq n-1} (\varepsilon_j - \varepsilon_i)^2$, where

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

for all $k \in \{0, 1, \ldots, n-1\}$.

3. 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

4. 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

5. Let a, b, c be integers. 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

6. 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 $1!2!\ldots(n-2)!$.

7. 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

$$\max_{1\leq i<j\leq n} |A_i - A_j| < \frac{1}{2^{2005}}.$$

8. Let $a_1^{(0)}, a_2^{(0)}, \ldots, a_n^{(0)} \in \mathbb{R}$ and let $a_i^{(k)} = \dfrac{a_i^{(k-1)} + a_{i+2}^{(k-1)}}{2}$ 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... you will probably say at first glance. Yet, we might spend too much time on a problem just because we ignore obvious clues or basic aspects of it. This is why we think that talking about these "old fashioned tricks" is not because of lack of imagination, but rather an imperious need. In this note we combine some classical arithmetic properties of polynomials. Of course, as usual, the list is just an unsophisticated introduction to this field, but some basic things should become second nature and among them there will be some problems we will discuss further. As usual, we keep some chestnuts for the end of the unit, so the hard core solver will get satisfaction, especially when extremely difficult problems with particularly simple statements can be asked...

There is one result that should be remembered, that is for any polynomial $f \in \mathbf{Z}[X]$ and any distinct integers a and b, $a-b$ divides $f(a)-f(b)$. Practically, this is the essential result that we will use relentlessly.

We will start with an important result, due to Schur, that appeared in many variants in contests. Even though in the topic **At the border between analysis and number theory** we prove an even more general result based on a nice analytical argument, we prefer to present here a purely arithmetical proof.

Example 1. [Schur] Let $f \in \mathbf{Z}[X]$ be a non constant polynomial. Then the set of prime numbers dividing at least one nonzero number among

$$f(1), f(2), \dots, f(n), \dots$$

is infinite.

Proof. First, suppose that $f(0) = 1$ and consider the numbers $f(n!)$. For sufficiently large n, they are nonzero integers. Moreover, $f(n!) \equiv 1 \pmod{n!}$ and so if we pick a prime divisor of each of the numbers $f(n!)$, the conclusion follows (since in particular any such prime divisor is greater than n). Now, if $f(0) = 0$, everything is clear. Suppose that $f(0) \neq 0$ and consider the polynomial $g(x) = \dfrac{f(xf(0))}{f(0)}$. Clearly, $g \in \mathbf{Z}[X]$ and $g(0) = 1$. Applying now the first part of the solution, the problem is solved.

This result has, as we have already said, important consequences. Here is a nice application.

Example 2. Suppose that $f, g \in \mathbf{Z}[X]$ are monic nonconstant 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 $\mathbf{Q}[X]$. In addition, if they are not equal, then the above remark and the fact that they have the same leading coefficient implies that the two polynomials are relatively prime in $\mathbf{Q}[X]$. Using Bezout's theorem we conclude that there is a nonzero integer N and $P, Q \in \mathbf{Z}[X]$ such that $fP + gQ = N$. This shows that for n large enough, 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 valid for infinitely many numbers n. Yet, the proof uses some highly nonelementary results of Erdos. The interested reader will find a rich literature on this field.

A refinement of Schur's theorem is discussed in the following example. The key ingredient is, as usual, the Chinese remainder theorem.

Example 3. Let $f \in \mathbf{Z}[X]$ be a nonconstant polynomial and let n, k be positive integers. Prove that there exists a positive integer a such that each of the numbers $f(a), f(a+1), \dots, f(a+n-1)$ has at least k distinct prime divisors.

Bulgarian Olympiad

Solution. Let us consider an array of distinct prime numbers $(p_{ij})_{i,j=1,k}$ such that $f(x_{ij}) \equiv 0 \pmod{p_{ij}}$ for some positive integers x_{ij}. This is just a direct consequence of Schur's theorem. Now, using the Chinese remainder theorem we can find a positive integer a such that $a - i \equiv x_{ij} \pmod{p_{ij}}$. Using the fundamental result mentioned above, it follows that each of the numbers $f(a), f(a+1), \dots, f(a+n-1)$ has at least k distinct prime divisors.

We continue with two more difficult examples of problems whose solutions are based on combinations of Schur's theorem with various classical arguments.

Example 4.[Titu Andreescu and Gabriel Dospinescu] For integral m, let $p(m)$ be the greatest prime divisor of m. By convention we set $p(1) = p(-1) = 0$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence $(p(f(n^2)) - 2n)_{n \geq 0}$ is bounded above.

USAMO 2006

Solution.

When searching the possible answer, one should start with easy examples. Here, the quadratic polynomials might give an insight. Indeed, observe that if u is an odd integer then the polynomial $f(X) = 4X - u^2$ is a solution of the problem. This suggests that any polynomial of the form $c(4X - a_1^2)(4X - a_2^2)...(4X - a_k^2)$ is a solution if c is a nonzero integer and $a_1, a_2, ..., a_k$ are odd integers. Indeed, any prime divisor p of $f(n)$ is either a divisor of c (and thus in a finite set) or a divisor of some $(2n - a_j)(2n + a_j)$. In this case $p - 2n \leq max(a_1, a_2, ..., a_k)$ and so f is a solution of the problem.

We deal now with the much more difficult part: showing the converse. Take f a polynomial that satisfies the conditions of the problem and suppose that $p(f(n^2)) - 2n \leq 2A$ for some constant A. Using Schur's theorem for the polynomial $f(X^2)$, we deduce the existence of a sequence of different prime numbers p_j and nonnegative integers k_j such that $p_j | f(k_j^2)$. Define the sequence $r_j = min(k_j(modp_j), p_j - k_j(modp_j))$ and observe that p_j divides $f(r_j^2)$ and also that $0 \leq r_j \leq \frac{p_j-1}{2}$. Hence $1 \leq p_j - 2r_j \leq A$ and so the sequence $(p_j - 2r_j)_{j\geq 1}$ must take some value a_1 infinitely many times. Let $p_j - 2r_j = a_1$ for j in an infinite set X. Then, if $m = deg(f)$, we have $p_j|4^m \cdot f((\frac{p_j-a_1}{2})^2)$ for all $j \in X$ and also the polynomial $4^m \cdot f((\frac{x-a_1}{2})^2)$ has integer coefficients. This shows that p_j divides $4^m \cdot f(\frac{a_1^2}{4})$ for infinitely many j. Hence $\frac{a_1^2}{4}$ is a root of f. Because $f(n^2)$ does not vanish, a_1 must be odd. This means that there exists a polynomial g with integer coefficients and a rational number r such that $f(X) = r(4X - a_1^2)g(X)$. Of course, g has the same property as f and applying the previous arguments finitely many times we deduce that f must be of the form $c(4X - a_1^2)(4X - a_2^2)...(4X - a_k^2)$ for a certain rational number c and odd integers $a_1, a_2, ..., a_k$. But do not forget that all coefficients of f are integers! Therefore the denominator of c is a divisor of both 4^m and $a_1^2a_2^2...a_k^2$, thus it is 1. This shows that c is an integer and the solution finishes here.

The next problem, which uses Schur's theorem needs also a classical result, a very particular case of Hensel's lemma. Let us first state and prove this result and then concentrate on the following problem. So, let us prove first the:

Hensel's lemma Let f be a polynomial with integer coefficients, p a prime number and n an integer such that p divides $f(n)$ and p does not divide $f'(n)$. Then there exists a sequence $(n_k)_{k\geq 1}$ of integers such that $n_1 = n$, p^k divides $n_{k+1} - n_k$ and p^k divides $f(n_k)$.

The proof is surprisingly simple. Indeed, let us suppose that we have found k and search $n_{k+1} = n_k + b \cdot p^k$ such that p^{k+1} divides $f(n_{k+1})$. Because $2k \geq k+1$, using the binomial formula yields

$$f(n_k + b \cdot p^k) = f(n_k) + bp^k f'(n_k)(modp^{k+1})$$

. Let $f(n_k) = cp^k$ for some integer c. Because $n_k = n(modp)$, we have $f'(n_k) = f'(n)(modp)$ and so $f'(n_k)$ is invertible modulo p. Let m be an inverse of $f'(n_k)$ modulo p. It is enough to choose $b = -mc$ in order to finish the inductive step.

We can discuss now a difficult problem used for the preparation of the iranian IMO team:

Example 5[Mohsen Jamali] Find all polynomials f with integer coefficients such that $n|m$ whenever $f(n)|f(m)$.

Iranian TST

Solution.[Adrian Zahariuc] With this preparation, the solution will be short, which does not mean that the problem is easy. First of all, observe that for a nonconstant polynomial with integer coefficients such that $f(0) \neq 0$ and for any k there are infinitely many prime numbers p such that $p^k|f(n)$ for some integer n. Indeed, by working with an irreducible divisor of f, we can assume

that f is irreducible. Thus f and f' are relatively prime in the ring of polynomials with rational coefficients. Bezout's theorem shows in this case that there exist integer polynomials S, Q and an integer $A \neq 0$ such that $Sf + Qf' = A$. Therefore, if p is a sufficiently large prime such that $p|f(n)$ for some n (the existence follows from Schur's theorem), p will not divide $f'(n)$ and we can apply Hensel's lemma to finish the proof of this result.
Next, observe that $X|f(X)$. Indeed, we have $f(n)|f(n + f(n))$ for all n, so $n|n + f(n)$ for all n, which easily implies $f(0) = 0$. So, let us write $f(X) = X^k g(X)$ with $g(0) \neq 0$. Assume that g is nonconstant. By the previous result, there exists a prime p such that $p > |g(0)|$ and $p^k|g(m)$ for some integer m. Clearly, p does not divide $g(p)$, so by the Chinese remainder theorem there exists an integer n such that $n = m(modp^k)$ and $n = p(modg(p))$. Thus $p^k|g(n)$ and $g(p)|g(n)$, from where $f(p)|f(n)$. This implies that $p|n$ and this is impossible, because it would follow that $p|g(0)$. Thus g is constant and the answer is: all polynomials of the form aX^n.

Classical arithmetics "tricks" and the fundamental result $a - b|f(a) - f(b)$ are the main ideas of the following problems.

Example 6.[Gabriel Dospinescu] Find all nonconstant polynomials f with integer coefficients and 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.

Solution. We will prove that the only polynomials with this 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 assume that the leading coefficient of f is positive. Hence there exists a constant M such that $f(n) > 2$ for all $n > M$. 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 $(f(n + kf(n))_{k\geq 1}$ will contain at least two relatively prime numbers. Let them be s and r. Because $f(n)|kf(n) = kf(n) + n - n|f(kf(n) + n) - f(n)$, we have $f(n)|f(n + kf(n))$ for any positive integer k. It follows that s and r are multiples of $f(n) > 2$, which is 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 $p|f(0)$. Because any nonzero integer has a finite number of divisors, we conclude that $f(0) = 0$. Hence there is a polynomial q with integer coefficients such that $f(X) = Xq(X)$. It is clear that q has positive leading coefficient and the same property as f. Repeating the above argument, we infer that if q is nonconstant, then $q(0) = 0$ and $qb(X) = Xh(X)$. Because f is nonconstant, the above argument cannot be repeated infinitely many times and thus one of the polynomials g and 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 obtain that f is of the form X^n. Because 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 it 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. Suppose that $x_1, x_2, \dots, x_p$ are pairwise relatively prime terms of the sequence. We prove that we can add another term x_{p+1} so that $x_1, x_2, \dots, x_{p+1}$ has the same property. It is clear that $x_1, x_2, \dots, x_p$ are relatively prime to a, so we can apply the Chinese remainder theorem to find an x_{p+1} greater than $x_1, x_2, \dots, x_p$, such that $x_{p+1} \equiv (1-b)a_i^{-1} \pmod{x_i}$, $i \in \{1, 2, \dots, p\}$, where a_i^{-1} is a's inverse in $Z_{x_i}^*$. Then $gcd(x_{p+1}, x_i) = 1$ for $i \in \{1, 2, \dots, p\}$ and thus we can add x_{p+1}.

Example 7. Let f, g be relatively prime polynomials with integer coefficients. Define the sequence $a_n = gcd(f(n), g(n))$. Prove that this sequence is periodic.

AMM

Solution.

As we have seen in previous problems, there exist polynomials F, G with integer coefficients and a positive integer A such that $fF + gG = A$.Thus a_n is a divisor of A for all n. Actually, we will prove that A is a period for the sequence $(a_n)_{n|geq1}$. Let us prove that $a_n|a_{n+A}$. We know that $f(n+A) = f(n)(modA)$ and since a_n divides A and $f(n)$, it will also divide $f(n+A)$. Similarly, a_n divides $g(n+A)$ and so $a_n|a_{n+A}$. But the same relations show that a_{n+A} divides a_n and so $a_n = a_{n+A}$.

Example 8.[Gabriel Dospinescu] Find all polynomials f with integer coefficients such that $f(n)|n^{n-1} - 1$ for all sufficiently large n.

Solution. Clearly, $f(X) = X - 1$ is a solution, so let us consider an arbitrary solution and write it in the form $f(X) = (X-1)^r g(X)$ with $r \geq 0$ and $g \in \mathbf{Z}[X]$ with $g(1) \neq 0$. Thus there exists M such that $g(n)|n^{n-1} - 1$ for all $n > M$.

We will prove that g is constant. Assuming the contrary, we may assume without loss of generality that the leading coefficient of g is positive. Thus there is $k > M$ such that $g(n) > 2$ and $g(n)|n^{n-1} - 1$ for all $n > k$. 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 $p|g(p+1)$ and thus (again using the fundamental result) $p|g(1)$. Because this occurs 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 $c|2^{n(2^n-1)} - 1$ for all $n > M$. Given that $gcd(2^a - 1, 2^b - 1) = 2^{gcd(a,b)} - 1$, 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 easy to achieve. Indeed, it suffices to take a prime number m greater than M, k and to choose a prime number n 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 $r \leq 2$. Assuming the contrary, we deduce that

$$(n-1)^3|n^{n-1} - 1 \Leftrightarrow (n-1)^2|n^{n-2} + n^{n-3} + \cdots + n + 1$$

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 $n - 1|n^{n-3} + 2n^{n-4} + \cdots + (n-3)n + (n-2) + 1$ 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 $r \leq 2$. 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 us 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, you might think that 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 be sufficiently large.

Example 9. Let $f \in \mathbf{Z}[X]$ be a nonconstant polynomial and let $k \geq 2$ be a positive integer such that $\sqrt[k]{f(n)} \in \mathbf{Q}$ for all positive integers n. Then there exists a polynomial $g \in \mathbf{Z}[X]$ such that $f = g^k$.

Solution. Let us assume the contrary and let us factor $f = p_1^{k_1} \dots p_s^{k_s} g^k$ where $1 \leq k_i < k$ and p_i are different irreducible polynomials in $\mathbf{Q}[X]$. Suppose that $s \geq 1$ (which is the same as negating the conclusion). Because p_1 is irreducible in $\mathbf{Q}[X]$, it is relatively prime with $p_1' p_2 \dots p_s$ and thus (using Bezout's theorem and multiplication by integers) there exist polynomials Q, R with integer coefficients and a positive integer c such that

$$Q(x)p_1(x) + R(x)p_1'p_2(x) \dots p_s(x) = c.$$

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 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 $v_q(p_1(n)) > 2$. In a similar manner we obtain $v_q(p_1(n+q)) \geq 2$. Yet, using the binomial formula, we can easily establish the congruence

$$p_1(n+q) \equiv p_1(n) + qp_1'(n) \pmod{q^2}.$$

Hence we must have $q|p_1(n)$, which contradicts the fact that $q > |c|$ 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 $s \geq 1$ is false and the result of the problem follows.

The next problem was given at the USA TST 2005 and uses a nice combination of arithmetics considerations and complex numbers computations. We take advantage of many arithmetical properties of polynomials in this problem, although the problem itself is not so difficult (if we find a good way to solve it, of course...)

Example 10.[Titu Andreescu, Gabriel Dospinescu] A polynomial $f \in \mathbf{Z}[X]$ is called special if for any positive integer $k > 1$, the sequence $f(1), f(2), f(3), \dots$ contains numbers which are relatively prime to k. Prove that for any $n > 1$, at least 71% of all monic polynomials of degree n with coefficients in the set $\{1, 2, \dots, n!\}$ are special.

USA TST 2005

Solution. Of course, before counting such polynomials, it would be better to find an easier characterization for them.

Let $p_1, p_2, \dots, p_r$ all prime numbers not exceeding n and 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 coefficients in the set $\{1, 2, \dots, n!\}$. We will prove that the set T of special polynomials is exactly $M \setminus \bigcup_{i=1}^{r} A_i$. Clearly, $T \subset M \setminus \bigcup_{i \leq r} A_i$. The converse, however, is not that easy. Let us suppose that $f \in \mathbf{Z}[X]$ belongs to $M \setminus \bigcup_{i=1}^{r} A_i$ and let p be a prime number greater than n. Because f is monic, Lagrange's theorem ensures that we can find m such that p is not a divisor of $f(m)$. It follows that for any prime number q at least one of the numbers $f(1), f(2), f(3), \dots$ is not a multiple of q. Let $k > 1$ and let $q_1, q_2, \dots, q_s$ be its prime divisors. Then we can find $u_1, \dots, u_s$ such that q_i does not divide $f(u_i)$. Using the Chinese remainder theorem, there is a positive integer x such that $x \equiv u_i \pmod{q_i}$. Consequently, $f(x) \equiv f(u_i) \pmod{q_i}$ and thus q_i does not divide $f(x)$, thus $gcd(f(x), k) = 1$. The equality of the two sets is now proved.

Using a raw estimation, we obtain

$$|T| = |M| - \left|\bigcup_{i=1}^{r} A_i\right| \geq |M| - \sum_{i=1}^{r} |A_i|.$$

Let us compute now $|A_i|$. Actually, we will show that $\dfrac{(n!)^n}{p_i^{p_i}}$. 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 $m > 1$,

$$0 \equiv f(m) \equiv a_0 + (a_1 + a_p + a_{2p-1} + a_{3p-2} + \dots)m$$

$$+(a_2 + a_{p+1} + a_{2p} + \dots)m^2 + \cdots + (a_{p-1} + a_{2p-2} + a_{3p-3} + \dots)m^{p-1} \pmod{p},$$

where, for simplicity, we put $p = p_i$. Using again 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 a small observation is still needed. 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

$$\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

and 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 $\dfrac{(n!)^s}{p}$.

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

$$|A_i| = \frac{n!}{p} \cdot \frac{(n!)^{v_1}}{p} \dots \frac{(n!)^{v_{p-1}}}{p} = \frac{(n!)^n}{p^p}.$$

Hence

$$|T| \geq (n!)^n - \sum_{p\, prime} \frac{(n!)^n}{p^p}.$$

But

$$\frac{1}{5^5} + \frac{1}{7^7} + \cdots < \frac{1}{5^5}\left(1 + \frac{1}{5} + \frac{1}{5^2} + \dots\right) < \frac{1}{1000}$$

and so the percent of special polynomials is at least

$$100\left(1-\frac{1}{4}-\frac{1}{27}-\frac{1}{1000}\right)=75-\frac{100}{27}-\frac{1}{10}>71.$$

Example 11. Suppose that the nonconstant polynomial f with integer coefficients has no double zeros. Then for any positive integer r there exists n such that in the prime decomposition of $f(n)$ there are at least r distinct prime divisors, all of them with exponent 1.

Iran Olympiad

Solution. Already for $r=1$ the problem is in no way obvious. So let's not attack it directly, but rather concentrate first on the case $r=1$. Suppose the contrary, that is for all n the prime divisors of $f(n)$ have exponent at least 2. Because f has no double zero, $gcd(f,f')=1$ in $\mathbf{C}[X]$ and thus also in $\mathbf{Q}[X]$ (because of the division and Euclid's algorithms). Using Bezout's theorem in $\mathbf{Q}[X]$, we can find polynomials P,Q with integer coefficients such that $P(n)f(n)+Q(n)f'(n)=c$ for some positive integer c. Using the result in the first example, we can take $q>c$ a prime divisor of some $f(n)$. Our hypothesis ensures that $q^2|f(n)$. But then, also, $q|f(n+q)$ 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 find $q|p'(n)$ and so $q|c$, which is impossible, since our choice was $q>c$. Thus the case $r=1$ is proved.

Let us now 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 some positive integer c did not depend on r, so we keep the above notations. By the inductive hypothesis, there is n such that at least r prime divisors of $f(n)$ have exponent 1. Let these prime factors be $p_1,p_2,\dots,p_r$. But it is clear that $n+kp_1^2p_2^2\dots p_r^2$ has the same property: all prime divisors $p_1,p_2,\dots,p_r$ have exponent 1 in the decomposition of $f(n+kp_1^2p_2^2\dots p_r^2)$. Because at most a finite number among them can be zeros of f, we may very well assume from the beginning that n is not a zero of f. Consider now the polynomial $g(X)=f(n+(p_1\dots p_r)^2X)$, which is obviously nonconstant. Thus using again the result in example 1, we find a prime number $q>\max\{|c|,p_1,\dots,p_r,|p(n)|\}$ and a number u such that $q|g(u)$. If $v_q(g(u))=1$, victory is ours, since a trivial verification shows that $q,p_1,\dots,p_r$ are different prime numbers whose exponents in $f(n+(p_1\dots p_r)^2u)$ are all 1. The difficult case is when $v_q(g(u))\geq 2$. In this case, we will consider the number $N=n+u(p_1\dots p_r)^2+uq(p_1\dots p_r)^2$. Let us prove that in the decomposition of $f(N)$, all prime numbers $q,p_1,\dots,p_r$ have exponent 1. For any p_i, this is obvious since $f(N)\equiv f(n) \pmod{(p_1\dots p_r)^2}$. Using once again the binomial formula, we obtain $f(N)\equiv f(n+(p_1\dots p_r)^2u)+uq(p_1\dots p_r)^2f'(N) \pmod{q^2}$. Now, if $v_q(f(n))\geq 2$, then since $v_q(f(n+(p_1\dots p_r)^2u))=v_q(g(u))\geq 2$, we have $q|u(p_1\dots p_r)^2f'(N)$. Recall that the choice was $q>\max\{|c|,p_1,\dots,p_r,|p(n)|\}$

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 $q|g(0) = f(n)$. Hopefully, we ensured that n is not a zero of our polynomial and also that $q > \max\{|c|, p_1, \ldots, p_r, |p(n)|\}$ so that the last divisibility cannot hold. This finishes the induction step and solves the problem.

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?

Problems for training

1. Let $(a_n)_{n\geq 1}$ be an increasing sequence of positive integers such that for some polynomial $f \in \mathbf{Z}[X]$ 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 $g \in \mathbf{Z}[X]$ 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 $f \in \mathbf{Z}[X]$ 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 taken 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 a finite family of polynomials with integer coefficients, prove that for infinitely many integers n, they assume at n only composite numbers.

5. Find all polynomials f with integer coefficients such that $f(n)|2^n - 1$ for all positive integer n.

Polish Olympiad

6. Suppose that $f \in \mathbf{Z}[X]$ is a nonconstant polynomial. Also, suppose that for some positive integers r, k, the following property holds: for any positive integer n, at most r prime factors of $f(n)$ have exponent at most equal to k. Does it follow that any zero of this polynomial has multiplicity at least $k+1$?

7. Is it true that any polynomial $f \in \mathbf{Z}[X]$ that has a zero modulo n for any positive integer n must have a rational zero?

8. Let f and $g \in \mathbf{Z}[X]$ be some nonzero polynomials. Consider the set $D_{f,g} = \{gcd(f(n), g(n))|\ n \in \mathbb{N}\}$. Prove that f and g are relatively prime in $\mathbf{Q}[X]$ if and only if $D_{f,g}$ is finite.

Gazeta Matematica 1985

9. Prove that there are no polynomials $f \in \mathbf{Z}[X]$ with the property: there exists $n > 3$ and integers $x_1, \dots, x_n$ such that $f(x_i) = x_{i-1}$, $i = 1, ..., n$ (indices are taken mod n).

10. Let $f \in \mathbf{Z}[X]$ be a polynomial of degree $n \geq 2$. Prove that the polynomial $f(f(X)) - X$ has at most n integer zeros.

Gh. Eckstein, Romanian TST

11. Find all quadratic polynomial $f \in \mathbf{Z}[X]$ with the property that for any relatively prime integers m, n, the numbers $f(m), f(n)$ are also relatively prime.

Saint Petersburg Olympiad

12. For the die hards: find all polynomials with the above property.

13. Let $f \in \mathbf{Z}[X]$ be a nonconstant polynomial. Prove that the sequence $f(3^n) \pmod{n}$ is not bounded.

14. Prove that for each positive integer n there is a polynomial $f \in \mathbf{Z}[X]$ such that all numbers $f(1) < f(2) < \cdots < f(n)$ are a) prime numbers b) powers of 2.

15. Find all integers $n > 1$ for which there is a polynomial $f \in \mathbf{Z}[X]$ such that for any integer k we have $f(k) \equiv 0, 1 \pmod{n}$ and both these congruences have solutions.

16. Let p be a prime number. Find the greatest degree of a polynomial $f \in \mathbf{Z}[X]$ having coefficients in the set $\{0, 1, \dots, p-1\}$, such that its degree is at most p and if p divides $f(m) - f(n)$ then it also divides $m - n$.

17. Use example 1 and properties of the cyclotomic polynomials

$$\phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (X - e^{\frac{2i\pi k}{n}})$$

to prove that there are infinitely many prime numbers of the form $kn+1$ for any given $n \geq 2$. You may want to first 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.

Lagrange interpolation formula

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

$$f(x) = \sum_{i=0}^{n} a_i \prod_{0 \le j \ne i \le n} \frac{x - x_j}{x_i - x_j} \tag{1}$$

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 example will show.

Example 1. 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 $a = \frac{\sqrt{5}+1}{2}$ and $b = \frac{1-\sqrt{5}}{2}$. 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 2. 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

$$k! \binom{p-1}{k} = (p-k)(p-k+1) \ldots (p-1) \equiv (-1)^k k! \pmod{p}$$

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 3. Let $a_1, a_2, \ldots, a_n$ be pairwise distinct positive integers. Prove that for any positive integer k the number $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod\limits_{j\neq i}(a_i - a_j)}$ 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 $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod\limits_{j\neq i}(a_i - a_j)}$ 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 $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod\limits_{j\neq i}(a_i - a_j)}$ 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 $\displaystyle\sum_{i=1}^{n} \frac{a_i^k}{\prod\limits_{j\neq i}(a_i - a_j)}$.

The following two problems we are going to discuss concern 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 4. Let $f(x) = \sum\limits_{k=0}^{n} a_k x^{n-k}$. 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

$$f(x) = \sum_{k=0}^{n} f(A+kh) \prod_{j \neq k} \frac{x-A-jh}{(k-j)h}.$$

Now, let us identify the leading coefficients in both polynomials that appear in the equality. We find that

$$a_0 = \sum_{k=0}^{n} f(A+kh) \frac{1}{\prod\limits_{j \neq k} [(k-j)h]} = \frac{1}{n!h^n} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(A+kh),$$

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 $p \in \{0, 1, 2, \dots, n-1\}$ and $\sum\limits_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n = n!.$

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 5. 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

$$0=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^{n}(1+2+\cdots+n-k).$$

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 6. Prove that for any real numbers $x_1,x_2,\dots,x_n\in[-1,1]$ the following inequality is true:

$$\sum_{i=1}^{n}\frac{1}{\prod\limits_{j\neq i}|x_j-x_i|}\geq 2^{n-2}.$$

Iran Olympiad

Solution. The presence of $\prod\limits_{j\neq i}|x_j-x_i|$ 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 one is optimal. So, let us proceed by taking $f(x)=\sum\limits_{k=0}^{n-1}a_kx^k$ 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

$$\left|\frac{f(x)}{x^{n-1}}\right| \leq \sum_{k=1}^{n} \frac{|f(x_k)|}{\prod\limits_{j\neq k} |x_k - x_j|} \left|\prod_{j\neq k}\Big(1 - \frac{x_j}{x}\Big)\right|$$

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

$$|a_{n-1}| \leq \sum_{k=1}^{n} \frac{|f(x_k)|}{\prod\limits_{j\neq k} |x_k - x_j|}.$$

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 $|a_{n-1}| \leq \sum\limits_{k=1}^{n} \dfrac{|f(x_k)|}{\prod\limits_{j\neq k} |x_k - x_j|}$ 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 7. 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

$$\sum_{k=0}^{n} \frac{|f(x_k)|}{\prod\limits_{j\neq k} |x_k - x_j|} \geq 1.$$

It is time to use the fact that we are dealing with integers. This will allow us to find a good inferior bound for $\prod\limits_{j\neq k} |x_k - x_j|$ This is easy, since

$$\prod_{j\neq k} |x_k - x_j| = (x_k - x_0)(x_k - x_1)\dots(x_k - x_{k-1})(x_{k+1} - x_k)\dots(x_n - x_k)$$

$$\geq k(k-1)(k-2)\dots 1 \cdot 1 \cdot 2 \dots (n-k) = k!(n-k)!.$$

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 8. 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 $x_0, x_1, x_2, \dots, x_n$ and write

$$\sum_{k=0}^{n} \frac{|f(x_k)|}{\prod\limits_{j\neq k} |x_k - x_j|} \geq 1.$$

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 are 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 $\lim\limits_{x\to\infty} \frac{g(x)}{x^{n+1}} = 1$, we deduce that it is actually a monic polynomial of degree $n+1$. The fact that $g(t_k) = 0$ for all $0 \le k \le n$ 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) $\prod\limits_{j\neq k}(t_k - t_j) = \frac{(-1)^k n}{2^{n-1}}$ *if* $1 \le k \le n-1$*;*

ii) $\prod\limits_{j=1}^{n}(t_0 - t_j) = \frac{n}{2^{n-2}}$*;*

iii) $\prod\limits_{j=0}^{n-1}(t_n - t_j) = \frac{(-1)^n n}{2^{n-2}}$.

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 $\lim\limits_{x\to\pm1} f'(x)$, 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 9. (Chebyshev theorem) Let $f \in R[X]$ be a monic polynomial of degree n. Then

$$\max_{x\in[-1,1]} |f(x)| \ge \frac{1}{2^{n-1}}$$

and this bound cannot be improved.

Solution. Using again the observation from problem 7, we obtain the identity:

$$1 = \sum_{k=0}^{n} f(t_k) \prod_{j\neq k} \frac{1}{t_k - t_j}.$$

Thus, we have

$$1 \le \max_{0\le k\le n} |f(t_k)| \sum_{k=0}^{n} \frac{1}{\left|\prod_{j\neq k}(t_k - t_j)\right|}.$$

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 $\max\limits_{x\in[-1,1]} |f(x)| \ge \frac{1}{2^{n-1}}$ 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 10. Suppose that $a_0, a_1, \dots, a_n$ are real numbers such that for all $x \in [-1, 1]$ we have

$$|a_0 + a_1x + \cdots + a_nx^n| \le 1.$$

Then for all $x \in [-1, 1]$ we also have

$$|a_n + a_{n-1}x + \cdots + a_0x^n| \le 2^{n-1}.$$

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:

$$|f(x)| \le |T_n(x)| \cdot \|f\| \text{ for all } |x| \ge 1.$$

Proof. Using Lagrange's interpolation formula and modulus inequality, we deduce that for all $u \in [-1,1]$ we have:

$$\left|f\left(\frac{1}{u}\right)\right| \leq \frac{1}{|u|^n}\|f\|\sum_{k=0}^{n}\prod_{j\neq k}\frac{1-t_j u}{|t_k-t_j|}.$$

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 $f(x) = \sum_{k=0}^{n} a_k x^k$, 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 $x \in [-1,1]$:

$$|a_n + a_{n-1}x + \cdots + a_0 x^n| = \left|x^n f\left(\frac{1}{x}\right)\right| \leq \left|x^n T_n\left(\frac{1}{x}\right)\right|.$$

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

$$|a_n + a_{n-1}x + \cdots + a_0 x^n| \leq 2^{n-1}$$

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

$$\max_{x\in[0,2]}\prod_{i=1}^{n}|x-a_i|\le 108^n\max_{x\in[0,1]}\prod_{i=1}^{n}|x-a_i|$$

for any real numbers $a_1, a_2, \dots, a_n$. 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 11. For any real numbers $a_1, a_2, \dots, a_n$, the following inequality holds:

$$\max_{x\in[0,2]}\prod_{i=1}^{n}|x-a_i|\le\frac{(3+2\sqrt{2})^n+(3-2\sqrt{2})^n}{2}\max_{x\in[0,1]}\prod_{i=1}^{n}|x-a_i|.$$

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 $\|f\|_{[0,2]}\le c_n\|f\|_{[0,1]}$ 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 $|f(x)|\le x_n$. 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

$$|f(x)|\le\sum_{k=0}^{n}\left|\prod_{j\ne k}\frac{x-x_k}{x_k-x_j}\right|=\sum_{k=0}^{n}\prod_{j\ne k}\frac{x-x_j}{|x_k-x_j|}$$

$$\le\sum_{k=0}^{n}\prod_{j\ne k}\frac{2-x_j}{|x_k-x_j|}=\sum_{k=0}^{n}\prod_{j\ne k}\frac{3-t_j}{|t_k-t_j|}.$$

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 $k=\overline{1,n+1}$. 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 $\sum_{k=0}^{n}(-1)^k\binom{n}{k}k^{n+2}$ and $\sum_{k=0}^{n}(-1)^k\binom{n}{k}k^{n+3}$.

AMM

5. Prove that

$$\sum_{k=0}^{n}\frac{x_k^{n+1}}{\prod\limits_{j\neq k}(x_k-x_j)}=\sum_{k=0}^{n}x_k$$

and compute

$$\sum_{k=0}^{n}\frac{x_k^{n+2}}{\prod\limits_{j\neq k}(x_k-x_j)}.$$

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 $\max\{|f(\pm 1)|, |f(0)|\} \leq 1$. Prove that if $|x| \leq 1$ then

$$|f(x)| \leq \frac{5}{4} \text{ and } \left|x^2 f\left(\frac{1}{x}\right)\right| \leq 2.$$

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

$$\max_{\overline{i=0,n+1}}|a^i - p(i)| \geq 1.$$

India, 2001

11. Find the maximal value of the expression $a^2+b^2+c^2$ if $|ax^2+bx+c| \le 1$ for all $x \in [-1,1]$.

Laurentiu Panaitopol

12. Let $a, b, c, d \in R$ such that $|ax^3+bx^2+cx+d| \le 1$ for all $x \in [-1,1]$. Prove that

$$|a|+|b|+|c|+|d| \le 7.$$

IMO Shortlist, 1996

13. Let $A = \left\{p \in R[X] | \ \deg p \le 3, \ |p(\pm 1)| \le 1, \ \left|p\left(\pm\frac{1}{2}\right)\right| \le 1\right\}$. Find $\sup\limits_{p\in A} \max\limits_{|x|\le 1} |p''(x)|$.

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: $\|f'\| \le n\|f\|$ where

$$\|f\| = \max_{|x|\le 1} |f(x)|.$$

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

It is probably time to see the contribution of nonelementary mathematics in combinatorics. It is quite difficult to imagine that behind a simple game, such as football, for example, or behind a day to day situation such as handshakes there exists such a complicated machinery, but this happens sometimes and we will prove it in the next. In the beginning of the discussion, the reader does not need any special knowledge, just imagination and the most basic properties of the matrices, but, as soon as we advance, things may 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 nonelementary fact that hides behind a completely elementary problem. Because we have clarified what is the purpose of the unit, we can begin.

The first problem we are going to discuss is not classical, but it is easy and shows how a very nice application of linear-algebra can solve elementary problems.

Example 1.[Nicolae Popescu] 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 that

$$\sum_{\sigma \in A_n} \sum_{i=1}^{n} |i - \sigma(i)| = \sum_{\sigma \in B_n} \sum_{i=1}^{n} |i - \sigma(i)|.$$

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

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}.$$

We have taken here $S_n = A_n \cup B_n$. But we have no product in our sum! This is why we take an arbitrary positive number a and consider the matrix $A = (a^{|i-j|})_{1 \leq i,j \leq n}$. We have

$$\det A = \sum_{\sigma \in S_n} (-1)^{\varepsilon(\alpha)} a^{|1-\sigma(1)|} \ldots a^{|n-\sigma(n)|}$$

$$= \sum_{\sigma\in A_n} a^{\sum\limits_{i=1}^{n}|i-\sigma(i)|} - \sum_{\sigma\in B_n} a^{\sum\limits_{i=1}^{n}|i-\sigma(i)|}$$

This is how obtain the identity

$$\begin{vmatrix} 1 & x & x^2 & \dots & x^{n-2} & x^{n-1} \\ x & 1 & x & \dots & x^{n-3} & x^{n-2} \\ x^2 & x & 1 & \dots & x^{n-4} & x^{n-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x^{n-1} & x^{n-2} & \dots & \dots & x & 1 \end{vmatrix}$$

$$= \sum_{\substack{\sigma\in S_n \\ \sigma \text{ even}}} x^{\sum\limits_{i=1}^{n}|i-\sigma(i)|} - \sum_{\substack{\sigma\in S_n \\ \sigma \text{ odd}}} x^{\sum\limits_{i=1}^{n}|i-\sigma(i)|}. \tag{1}$$

Anyway, we do not have the desired difference yet. What can we do to get it? The most natural way is to differentiate 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 differentiate (1) and take $x = 1$, the left-hand side vanishes, while the right-hand side becomes

$$\sum_{\sigma\in A_n}\sum_{i=1}^{n}|i-\sigma(i)| - \sum_{\sigma\in B_n}\sum_{i=1}^{n}|i-\sigma(i)|.$$

This completes the proof.

Here is another nice application of this idea. You know how many permutations do not have a fixed point. The question that arises is how many of them are even. Using determinants provides a direct answer to the question.

Example 2. Find the number of even permutations of the set $\{1, 2, \dots, n\}$ that do not have fixed points.

Solution. Let C_n and D_n be the sets of even and odd permutations of the set $\{1, 2, \dots, n\}$, that do not have any fixed points, respectively. You may recall how to find the sum $|C_n| + |D_n|$: using the inclusion-exclusion principle, it is not difficult to establish 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 $|C_n| - |D_n|$, we will be able to answer to the question. Write

$$|C_n| - |D_n| = \sum_{\substack{\sigma\in A_n\\ \sigma(i)\neq i}} 1 - \sum_{\substack{\sigma\in B_n\\ \sigma(i)\neq i}} 1$$

and 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 computing this determinant is not difficult. Indeed, we add all columns to the first and factor $n-1$, 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:

$$|C_n| = \frac{1}{2}n!\left(1 - \frac{1}{2!} + \frac{1}{3!} - \dots + \frac{(-1)^{n-2}}{(n-2)!}\right) + (-1)^{n-1}(n-1).$$

In the next problems we will focus on a very important combinatorial tool, that is the incidence matrix. 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 $X_1, X_2, \dots, X_k$ and the set X. In many situations, computing the product ${}^tA \cdot A$ helps translating algebraically the conditions and the conclusion of certain problems. From this point, we turn on this machinery and solving the problem is on its way.

Let us discuss first a classical problem. It appeared at the USAMO 1979, Tournament of the Towns 1985 and in the 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 subsets among them that have exactly one common element.

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

$$ {}^tT \cdot T = \begin{pmatrix} \sum\limits_{k=1}^{n} t_{k,1}^2 & \sum\limits_{k=1}^{n} t_{k,1}t_{k,2} & \ldots & \sum\limits_{k=1}^{n} t_{k,1}t_{k,n+1} \\ \ldots & \ldots & \ldots & \ldots \\ \sum\limits_{k=1}^{n} t_{k,n+1}t_{k,1} & \sum\limits_{k=1}^{n} t_{k,n+1}t_{k,2} & \ldots & \sum\limits_{k=1}^{n} t_{k,n+1}^2 \end{pmatrix}. $$

But $\sum\limits_{k=1}^{n} x_{ki}^2 = |A_i| = 3$ and $\sum\limits_{k=1}^{n} x_{ki}x_{kj} = |A_i \cap A_j| \in \{0, 2\}$.

Thus, considered in the field $(\mathbb{Z}_2, +, \cdot)$, we have

$$ \overline{{}^tT \cdot T} = \begin{pmatrix} \widehat{1} & \widehat{0} & \ldots & \widehat{0} & \widehat{0} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \widehat{0} & \widehat{0} & \ldots & \widehat{0} & \widehat{1} \end{pmatrix}, $$

where $\overline{X}$ is the matrix having as elements the residues classes of the elements of the matrix X. Because $\det \overline{X} = \overline{\det X}$, the previous relation shows that $\det {}^tT \cdot T$ is odd, hence nonzero. This means that ${}^tTT$ is an invertible matrix of order $n + 1$, thus $rank\, {}^tT \cdot T = n + 1$ which contradicts the inequality $rank\, {}^tT \cdot T \leq rankT \leq n$. This shows that our assumption is 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 even and let $A_1, A_2, \ldots, A_n$ be distinct subsets of the set $\{1, 2, \ldots, n\}$, each of them having an even number of elements. Prove that among these subsets there are two having an even number of common elements.

Solution. Indeed, if T is the incidency matrix of the family $A_1, A_2, \ldots, A_n$, we obtain as in the previous problem the following relation

$$ {}^tT \cdot T = \begin{pmatrix} |A_1| & |A_1 \cap A_2| & \ldots & |A_1 \cap A_n| \\ \ldots & \ldots & \ldots & \ldots \\ |A_n \cap A_1| & |A_n \cap A_2| & \ldots & |A_n| \end{pmatrix}. $$

Now, let us suppose that all the numbers $|A_i \cap A_j|$ are odd and interpret the above relation in the field $(\mathbb{Z}_2,+,\cdot)$. We find that

$$\overline{{}^tT\cdot T}=\left(\begin{array}{ccccc}\widehat{0} & \widehat{1} & \dots & \widehat{1} & \widehat{1}\\ \dots & \dots & \dots & \dots & \dots\\ \widehat{1} & \widehat{1} & \dots & \widehat{1} & \widehat{0}\end{array}\right),$$

which means again that det ${}^tT\cdot T$ is odd. Indeed, if we work in $(\mathbb{Z}_2,+,\cdot)$, we obtain

$$\left|\begin{array}{ccccc}\widehat{0} & \widehat{1} & \dots & \widehat{1} & \widehat{1}\\ \dots & \dots & \dots & \dots & \dots\\ \widehat{1} & \widehat{1} & \dots & \widehat{1} & \widehat{0}\end{array}\right|=\widehat{1}.$$

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, we will obtain only even numbers on the first line. Because the value of the determinant does not change under this operation, it follows that $\det T$ is an even number. But a number cannot be both even and odd, so our assumption is wrong and the problem is solved.

Working in a simple field such as $(\mathbb{Z}_2,+,\cdot)$ can allow us to find quite interesting solutions. For example, we will discuss the following problem, used in the preparation of the Romanian IMO team in 2004.

Example 5.[Gabriel Dospinescu] The squares of a $n\times n$ table are colored with white and black. Suppose that there exists a nonempty 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 nonempty set of columns B such that any line of the table contains an even number of white squares that also belong to B.

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 so easy to see. In each white square we write the number 1 and in each black square we put a 0. We thus obtain a binary matrix $T=(t_{ij})_{1\le i,j\le n}$. From now on, we work only in $(\mathbb{Z}_2,+,\cdot)$. Suppose that A contains the columns $a_1,a_2,\dots,a_k$. It follows that $\sum\limits_{i=1}^{k}t_{a,j}=0$ for all $j=1,2,...,n$. 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

$$\begin{cases} t_{11}z_1 + t_{21}z_2 + \cdots + t_{n1}z_n = 0 \\ t_{12}z_1 + t_{22}z_2 + \cdots + t_{n2}z_n = 0 \\ \dots \\ t_{1n}z_1 + t_{2n}z_2 + \cdots + t_{nn}z_n = 0 \end{cases}$$

has the nontrivial solution $(x_1, x_2, \ldots, x_n)$. Thus, $\det T = 0$ and consequently $\det {}^tT = 0$. But this means that the system

$$\begin{cases} u_{11}y_1 + u_{12}y_2 + \cdots + u_{1n}y_n = 0 \\ u_{21}y_1 + u_{22}y_2 + \cdots + u_{2n}y_n = 0 \\ \dots \\ u_{n1}y_1 + u_{n2}y_2 + \cdots + u_{nn}y_n = 0 \end{cases}$$

has also a nontrivial solution in $\mathbb{Z}_2$. Now, we take $B = \{i|\ y_i \neq 0\}$ and we clearly have $B \neq \emptyset$ and $\sum\limits_{x \in B} u_{ix} = 0$, $i = 1, 2, ..., n$. But this means that any line of the table contains an even number of white squares that also belong to B and the problem is solved.

The cherry on the cake is the following very difficult problem, where 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 many 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 arsenal: the properties of the characteristic polynomial and the eingenvalues of a matrix. It is exactly the kind of problem that knocks you down when you feel most confident.

Example 6.[Gabriel Carrol] Let $S = \{1, 2, \ldots, n\}$ and let A be a family of pairs of elements in 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 and n for which this is possible.

Solution. It is not difficult to see what hides behind this 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 and n for which there exist a binary matrix T such that

$$T^2 = \begin{pmatrix} m & m & \dots & m \\ m & m & \dots & m \\ \dots & \dots & \dots & \dots \\ m & m & \dots & m \end{pmatrix}.$$

Let us consider

$$B = \begin{pmatrix} m & m & \dots & m \\ m & m & \dots & m \\ \dots & \dots & \dots & \dots \\ m & m & \dots & m \end{pmatrix}.$$

and find the eigenvalues of B. This is not difficult, since if x is an eingenvalue, then

$$\begin{vmatrix} m-x & m & \dots & m \\ m & m & \dots & m \\ \dots & \dots & \dots & \dots \\ m & m & \dots & m-x \end{vmatrix} = 0$$

If we add all columns to the first 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 last 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. Hence 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 $Tr(T) \in \mathbb{R}$, we find that mn must be a perfect square. Also, because $Tr(T) \le n$, we must have $m \le n$.

Now, let us prove the converse. Suppose that $m \le n$ and mn is a perfect square and write $m = du^2$, $n = dv^2$. Let us take the matrices

$$I = (\underbrace{11\dots11}_{dv}), \quad O = (\underbrace{00\dots00}_{dv}).$$

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 concepts from the theory of vector spaces, just the basic facts 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

$$A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k} = A_{j_1} \cup A_{j_2} \cup \cdots \cup A_{j_m}.$$

Chinese Olympiad

Solution. Let us assign 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

$$x_i^j = \begin{cases} 0, & \text{if} \quad j \in A_i \\ 1, & \text{if} \quad j \notin A_i \end{cases}$$

Because $\dim \mathbb{R}^n = n$, the 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, 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 clear that I_1 and I_2 are nonempty and disjoint. Let us prove that $\bigcup\limits_{i \in I_1} A_i = \bigcup\limits_{i \in I_2} A_i$ and the solution will be complete. Take $x \in \bigcup\limits_{i \in I_1} A_i$ and suppose that $x \notin \bigcup\limits_{i \in I_2} A_i$. Then the vectors v_i with $i \in I_2$ have zero on their xth component, so the xth component of the vector $a_1v_1 + a_2v_2 + \cdots + a_{n+1}v_{n+1}$ is $\sum\limits_{\substack{x \in A_j \\ j \in I_1}} a_j > 0$, which is impossible, since $a_1v_1 + a_2v_2 + \cdots + a_{n+1}v_{n+1} = 0$. This shows that $\bigcup\limits_{i \in I_1} A_i \subset \bigcup\limits_{i \in I_2} A_i$. But the reversed inclusion can be proved in exactly the same way, so we conclude that $\bigcup\limits_{i \in I_1} A_i = \bigcup\limits_{i \in I_2} A_i$.

We conclude this discussion with another problem, proposed for the TST 2004 in Romania, whose idea is also related to vector spaces.

Example 8.[Gabriel Dospinescu] Thirty boys and twenty girls are preparing for the 2006 Team Selection Test. They observed that any two boys have an even number of common acquaintances among the girls and exactly nine boys know an odd number of girls. Prove that there exists a group of sixtien boys such that any girls attending the preparation is known by an even number of boys from this group.

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 $T = A \cdot {}^tA$. Observe that all the elements of the matrix T, except those from the main diagonal, are even (because $t_{ij} = \sum\limits_{k=1}^{20} a_{ik}a_{jk}$ is the number of common acquaintances among the girls of the boys B_i, B_j). Each element on the main diagonal of T is precisely the number of girls known by corresponding boy. Thus, if we consider the matrix T in $(\mathbb{Z}_2, +, \cdot)$, it will be diagonal, with exactly nine nonzero elements on its main diagonal. From now on, we will work only in $(\mathbb{Z}_2, +, \cdot)$. We have seen that $rank(T) = 9$. Using Sylvester inequality, we have

$$9 = rank(T) \geq rank(A) + rank\,({}^tA) - 20 = 2rank\,({}^tA) - 20$$

hence $r = rank\,({}^tA) \leq 14$. Let us consider now the linear system in $(\mathbb{Z}_2, +, \cdot)$:

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \cdots + a_{30,1}x_{30} = 0 \\ a_{12}x_1 + a_{22}x_2 + \cdots + a_{30,2}x_{30} = 0 \\ \cdots \\ a_{1,20}x_1 + a_{2,20}x_2 + \cdots + a_{30,20}x_{30} = 0 \end{cases}$$

The set of solutions of this system is a vector space of dimension $30 - r \geq 16$. This 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 $\sum\limits_{j \in M} a_{ji} = 0$ for all $i = 1, 2, ..., 20$. But observe that $\sum\limits_{j \in M} a_{ji}$ 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.

We continue our journey with a problem that has no combinatorial proof until now: the famous Graham-Pollak theorem. The solution, due to Tverberg, is taken from the execellent book **Proofs from The Book**.

Example 9.[R. Graham and O.Pollak]
There exists no partition of the complete graph on n vertices with fewer than $n - 1$ complete bipartite subgraphs.

Solution. Denote by $1, 2, ..., n$ the vertices of the complete graph on n vertices and suppose that $B_1, B_2, ..., B_m$ is a partition of this graph with complete bipartite subgraphs. Every such subgraph B_i is defined by two sets of vertices L_j and R_j. Put a real number x_i in each vertex of the complete graph K_n. The hypothesis implies that

$$\sum_{1 \leq i < j \leq n} x_i x_j = \sum_{k=1}^{m} (\sum_{i \in L_k} x_i \cdot \sum_{j \in R_k} x_j).$$

The marvelous idea is that if $m < n - 1$ then we can choose the real numbers $x_1, x_2, ..., x_n$ such that not all of them are zero, $x_1 + x_2 + ... + x_n = 0$ and $\sum\limits_{i \in L_k} x_i = 0$ for all k. Indeed, this linear system has a nontrivial solution, because the number of equations exceeds the number of variables. Using the above identity and the fact that $\sum\limits_{i=1}^{n} x_i^2 = (\sum\limits_{i=1}^{n} x_i)^2 - 2 \sum\limits_{1 \leq i < j \leq n} x_i x_j$, we infer that $x_1^2 + x_2^2 + ... + x_n^2 = 0$, which contradicts the choice of $x_1, x_2, ..., x_n$.

Problems for training

1. Let p 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 and B_j be the set of even and odd permutations σ for which $S(\sigma) \equiv j \pmod{p}$ respectively. 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 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 the sets of all even and odd permutations of the set $\{1, 2, \ldots, n\}$ respectively.

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 has 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 that need not hold after fewer steps.

Iran Olympiad, 1998

7. A number of $n \geq 2$ 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 loser. 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 a grid dividing the sheet into unit squares is drawn. 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, TST Romania 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 $x_1, x_2, \ldots, x_n$ 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's theorem

12. Let $A_1, A_2, \ldots, A_m$ be subsets of $\{1, 2, \ldots, n\}$. Then there are disjoint sets I, J with nonempty union such that $\bigcup\limits_{i\in I} A_i = \bigcup\limits_{j\in J} A_j$ and $\bigcap\limits_{i\in I} A_i = \bigcap\limits_{j\in J} A_j$.

Lindstrom's theorem

13. There is no partition of the set of edges of the complete graph on n vertices into fewer than $n-1$ complete bipartite graphs.

Graham-Pollak's theorem

14. Consider $2n+1$ real numbers with the property that no matter how we eliminate one of them, the rest 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 common friend. Then there is a person who knows all the others.

Universal friend theorem

16. Let $A_1, A_2, \ldots, A_m$ and $B_1, B_2, \ldots, B_p$ subsets of $\{1, 2, \ldots, n\}$ such that $A_i \cap B_j$ is an odd number for all i and j. Then $mp \leq 2^{n-1}$.

Benyi Sudakov

17. Let $A_1, A_2, \ldots, A_n, B_1, B_2, \ldots, B_n \subset A = \{1, 2, \ldots, n\}$ 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.

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

19. The squares of an n times n board are filled with 0 or 1 such that any two lines differ in exactly $\frac{n}{2}$ positions. Prove that there are at most $n \cdot \sqrt{n}$ ones on the board.

Komal

20. A handbook classifies plants by 100 attributes (each plant either has a given attribute or does not have it). Two plants are dissimilar if they differ in at least 51 attributes. Show that the handbook cannot give 51 plants all dissimilar from each other. Can it give 50?

Tournament of the Towns 1993

21. A simple graph has the property: given any nonempty set H of its vertices, there is a vertex x of the graph such that the number of edges connecting x with the points in H is odd. Prove that the graph has an even number of vertices.

Komal

22. A figure composed of 1 by 1 squares has the property that if the squares of a fixed m by n rectangle are filled with numbers the sum of all of which is positive, the figure can be placed on the rectangle (possibly after being rotated) so that the numbers it covers also have positive sum (however, the figure may not have any of its squares outside the rectangle). Prove that a number of such figures can be placed on the rectangle such that each square is covered by the same number of figures.

Russian Olympiad 1998

23. In a table m by n real numbers are written such that for any two lines and any two columns, the sum of the numbers situated in the opposite vertices of the rectangle formed by them is equal to the sum of the numbers situated in the other two opposite vertices. Some of the numbers are erased, but the remaining ones allow to find the erased numbers. Prove that at least $n+m-1$ numbers remained on the table.

Russian Olympiad 1971

24. Let A be a finite set of real numbers between 0 and 1 such that for all $x \in A$ there exist a, b different from x, which belong to A or which are equal to 0 or 1 such that $x = \frac{a+b}{2}$. Prove that all elements of A are rational.

Bay Area Competition

Geometry and numbers

It may seem 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 exhibit a few applications of geometry in number theory, almost all of them revolving around the celebrated Minkowski's theorem. We will see that this theorem gives an efficient criterion for a nice and convex region to have a nontrivial lattice point(we are going to explain what we understand by nice, but not by convex). The existence of this point has important consequences in the theory of representation of numbers by quadratic forms or in the approximation of real numbers by rational numbers. As usual, we will present only a mere introduction to this extremely well-developed field. You will surely have the pleasure to consult some reference books about this fascinating field.

First of all, let us specify the context of this unit and what a nice figure is. Generally, we will work in $\mathbb{R}^n$ and call convex body a bounded subset A of $\mathbb{R}^n$ which is convex and symmetric with respect to 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).

We 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, begin by making a sort of a partition of $\mathbb{R}^n$ in cubes of edge 2, having as centers the points that have all coordinates even integers. It is clear that any two such cubes 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 the volumes of the intersections of the body with each cube (because 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 at the origin) and the sum of volumes of all these bodies is greater than 2^n. It follows that there are two bodies which intersect at a point X. Now, look at the cubes where these two bodies where taken from and look at the points in these cubes whose image under these translations is 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 proved.

Here is a surprising result that follows directly from this theorem.

Example 1. Suppose that at 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 some ball.

Solution. Let us suppose the contrary and consider a cylinder having as axis that very line and base a circle of radius $\frac{r}{2}$. We choose it sufficiently long to ensure that it has a volume greater than 8. This is clearly a convex body in space and using Minkowski's theorem we deduce the existence of a nontrivial 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 be a convex body in $\mathbb{R}^n$ and let $v_1, v_2, \dots, v_n$ be linearly independent vectors in $\mathbb{R}^n$. 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. If A has a volume greater than $2^n \cdot Vol(P)$, A must contain at least a point of the lattice $L = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n$ 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 $e_i = (0, 0, \dots, 1, 0, \dots, 0)$, 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 $\mathbb{Z}^n$. Because 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 nontrivial point of $A \cap L$. This finishes the proof of the second theorem.

We proved in chapter **Primes and squares** that any prime number of the form $4k + 1$ is the sum of two squares. Let us prove it differently, using this time Minkowski's theorem.

Example 2. Any prime number of the form $4k+1$ is the sum of two squares.

Solution. We have already proved that for any prime number of the form $4k + 1$, call it p, we can find an integer a such that $p | a^2 + 1$. Consider then $v_1 = (p, 0)$ and $v_2 = (a, 1)$. Visibly, they are linearly independent and moreover for any point (x, y) in the lattice $L = \mathbf{Z}v_1 + \mathbf{Z}v_2$ we have $p | x^2 + y^2$. Indeed, there are $m, n \in \mathbb{Z}$ such that $x = mp + na$, $y = n$ and thus $x^2 + y^2 \equiv n^2(a^2 + 1) \equiv 0 \pmod{p}$. In addition, the area of the fundamental parallelogram is $\|v_1 \wedge v_2\| = p$. Next, consider as convex body the disc centered at the origin and having radius

$\sqrt{2p}$. Clearly, 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 $L = \mathbf{Z}v_1 + \mathbf{Z}v_2$. 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 some Diophantine equation has no solution is a classical problem, but what can we do when we are asked to prove that some equation has solutions? Minkowski's theorem and, in general, the geometry of numbers give responses to such problems. Here is an example:

Example 3. Consider positive integers a, b, c such that $ac = b^2 + b + 1$. Prove that the equation $ax^2 - (2b + 1)xy + cy^2 = 1$ has integer solutions.

Polish Olympiad

Solution. Here is a very quick approach: consider in $\mathbb{R}^2$ the set of points satisfying $ax^2 - (2b + 1)xy + cy^2 < 2$. A simple computation shows that it is an elliptical disc having area $\frac{4\pi}{\sqrt{3}} > 4$. An elliptical disc is obviously a convex body and even more this elliptical disc is symmetric about the origin. Thus by Minkowski's theorem there is a point in this region different from the origin. Since $ac = b^2 + b + 1$, we have for all x, y not both equal to 0 the inequality $ax^2 - (2b + 1)xy + cy^2 > 0$. Thus for $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, we have $ax^2 - (2b+1)xy + cy^2 = 1$ and the existence of a solution of the given equation is proved.

The following problem (like the one above) 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 gained by solving the previous problem should ring a bell.

Example 4. Suppose that n is a positive integer 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 integers a, b, c such that $a^2 + ab + b^2 = c^2n$, then $x^2 + xy + y^2 = n$ has integer solutions. We will assume that a, b, c are nonzero (otherwise the conclusion follows trivially). Even more, a classical argument allows us to assume that a and b are relatively prime. We try again to find a pair $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ such that $x^2+xy+y^2 < 2n$ and such that n divides x^2+xy+y^2. In this case we will have $x^2+xy+y^2 = n$ and the conclusion follows. 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 yields an integer solution to 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 and b). The conclusion now follows.

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 $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n \setminus \{0\}$ the set of points satisfying

$$\sum_{1 \le i,j \le n} a_{ij} x_i x_j \le 1$$

has volume equal to $\dfrac{Vol(B_n)}{\sqrt{\det A}}$, where

$$Vol(B_n) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1 + \dfrac{n}{2}\right)}$$

(here $\Gamma(x) = \displaystyle\int_0^{\infty} e^{-t} t^{x-1} dt$ is the Euler's gamma function). The proof of this result is not elementary and we invite you to read more about it in any decent book of multivariate integral calculus. In particular, you should notice that these results can be applied to previous problems to facilitate the computations of different areas and volumes. With these fact in mind, let us attack some serious problems.

If we talked about squares, why not present the beautiful classical proof of Lagrange's theorem on representations using four squares?

Example 5. [Lagrange] Any natural number is a sum of four perfect squares.

Solution. 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 p be an odd 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 $\dfrac{p+1}{2}$ squares in $\mathbb{Z}_p$ (as we have already seen in previous chapters), these two sets cannot be disjoint. In particular, there are x and y such that $0 \le x, y \le p-1$ and $p | x^2 + y^2 + 1$. This is the observation that will enable 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 us to prove that the volume of the fundamental parallelepiped is p^2. Moreover, one can easily verify that for each point $(x, y, z, t) \in L$ we have $p | x^2 + y^2 + z^2 + t^2$. Even more, we can also prove (by employing the nonelementary results stated before) 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 $x^2 + y^2 + z^2 + t^2 = p$. This finishes the proof for prime numbers.

Of course, everything would be nice if the product of two sums of four squares is always a sum of four squares. Hopefully, this is the case, but the proof is not obvious at all. It follows form the miraculous identity:

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = (ax + by + cz + dt)^2$$

$$+(ay - bx + ct - dz)^2 + (az - bt + dy - cx)^2 + (at + bz - cy - dx)^2.$$

This is very nice, but how could one answer the eternal question: how on earth should I think of such an identity? Well, this time there is a very nice reason: instead of thinking in eight variables, let us reason only with four. Consider the numbers $z_1 = a + bi$, $z_2 = c + di$, $z_3 = x + yi$, $z_4 = z + ti$ and 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 natural 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 four squares. The identity is now motivated.

For someone who knows the three-squares theorem, the following problem is trivial. But what would someone do in the opposite case? Without such an advanced result, the problem is not easy at all, but as we will see a good geometric argument is the key of a very elementary solution:

Example 6. [Davenport-Cassels] Prove that any positive integer which can be written as the sum of the squares of three rational numbers can also be written as the sum of the squares of three integers.

Solution. Let us suppose by contradiction that the property does not hold. We will use a geometric argument combined with the extremal principle. Let S be the sphere of radius $\sqrt{n}$ in $\mathbb{R}^3$ and suppose that $a \in S$ has all coordinates rational numbers. There exist an integer vector $v \in \mathbb{Z}^3$ and an integer $d > 1$ such that $a = \frac{v}{d}$. Choose the pair (a, v) for which d is minimal. We claim that there exists a vector $b \in \mathbb{Z}^3$ such that $||a - b|| < 1$, where $||x||$ is the euclidean norm of the vector x. Indeed, it is enough to write $a = (x, y, z)$ and to consider $b = (X, Y, Z)$, where integers X, Y, Z are such that

$$|X - x| \leq \frac{1}{2}, |Y - y| \leq \frac{1}{2}, |Z - z| \leq \frac{1}{2}.$$

Now, since a is assumed to have at least one non-integer coordinate, $a \neq b$. Consider the line ab . It will cut the sphere S in a and another point c. Let us determine precisely this point. Writing $c = b + \lambda \cdot (a - b)$ and imposing the condition $||c||^2 = n$ yields a quadratic equation in λ , with an obvious solution $\lambda = 1$. Using Vieta's formula for this equation, we deduce that another solution is $\lambda = \frac{||b||^2 - n}{||a-b||^2}$. On the other hand, the identity

$$||a - b||^2 = n + ||b||^2 - \frac{2}{d} < b, v >$$

and the fact that $0 < ||a - b|| < 1$ show that $||a - b||^2 = \frac{A}{d}$ for a certain positive integer A smaller than d . Therefore, $\lambda = \frac{d}{A}(||b||^2 - n)$ and $c = b + \frac{||b||^2 - n}{A}(v - db) = \frac{w}{A}$ for an integer vector w. This shows that the pair (c, w) contradicts the minimality of (a, v) and proves the result.

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.

Example 7. [Minkowski's linear forms theorem] Let $A = (a_{ij})$ be an $n \times n$ invertible matrix with real entries and let $c_1, c_2, \ldots, c_n$ be 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 an integer nonzero 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 $\{Y \in \mathbb{R}^n |\ |A^{-1}Y|_i < c_i,\ i = 1, \ldots, n\}$ is exactly the image through 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 nonzero lattice point, which satisfies the conditions of the problem.

And here is a nice consequence of the previous example.

Example 8. Suppose $A = (a_{ij})_{\substack{1\leq i\leq m\\1\leq j\leq n}}$ is a matrix with real entries and let $a \geq 1$ be a real number. Then we can find $x_1, x_2, \ldots, x_n$ integers between $-a$ and a, not all 0, such that

$$\left|\sum_{j=1}^{n} a_{ij}x_j\right| < a^{-\frac{n}{m}}$$

for all $1 \leq i \leq m$.

Solution. All we need to do is to apply the result in example 6 for the invertible matrix $\begin{pmatrix} A & I_m \\ I_n & 0 \end{pmatrix}$, whose determinant equals 1 or -1 and choose $c_1 = \cdots = c_m = a^{-\frac{n}{m}}$, $c_{m+i} = a$, $1 \leq i \leq n$. Incredibly, but the proof ends here!

Finally, the highlight of the IMO 1997, the very beautiful problem 6 also has a magnificient solution using geometry of numbers. Actually, we will prove much more than the result asked in the contest, which shows that for large values of one of the bounds asked by the IMO problem is very weak:

Example 9.

For each positive integer n , let $f(n)$ denote the number of ways of representing n as a sum of powers of two with nonnegative integer coefficients. Representations that differ only in the ordering of their summands are considered to be the same. For instance, $f(4) = 4$. Prove that there are two constants a, b such that

$$2^{\frac{n^2}{2}-anlogn} < f(2^n) < 2^{\frac{n^2}{2}-bnlogn}$$

for all sufficiently large n.

Adapted after IMO 1997

Solution: It is clear that $f(2^n)$ is just the number of nonnegative integer solutions of the equation $a_0+2a_1+...+2^na_n = 2^n$, which is the same as the number of solutions in nonnegative integers of the inequation $2a_1+4a_2+...+2^na_n \leq 2^n$ .For any such solution, we will consider the hypercube $H(a_1, a_2, ..., a_n)$ defined by the set of points $(x_1, x_2, ..., x_{n-1}) \in \mathbb{R}_+^{n-1}$ for which $a_i \leq x_i < a_i+1$. We need to estimate the sum of volumes of these hypercubes, which is clearly between the volumes of the regions $R_1 = \{(x_1, ..., x_{n-1}) \in \mathbb{R}_+^{n-1} | \sum\limits_{i=1}^{n-1} 2^i x_i \leq 2^n\}$ and $R_1 = \{(x_1, ..., x_{n-1}) \in \mathbb{R}_+^{n-1} | \sum\limits_{i=1}^{n-1} 2^i(x_i - 1) \leq 2^n\}$. Consider more generally the region $R(a_1, a_2, ..., a_n, b) = \{(x_1, ..., x_n) \in \mathbb{R}_+^n | \sum\limits_{i=1}^{n} a_i x_i \leq b\}$. Using integral calculus, we can establish that this region has a volume equal to $\frac{b^n}{n!a_1a_2\ldots a_n}$. Hence

$$1+\frac{2^{\frac{n^2-n}{2}}}{(n-1)!}\leq f(2^n)\leq 1+\frac{(2^{n+1}-2)^{n-1}}{2^{\frac{n^2-n}{2}}\cdot(n-1)!}$$

Because $lnn! = nlnn+O(n)$, the conclusion follows immediately from the above inequalities.

Problems for training

1.[Fermat] Suppose that a, b, c are positive integers such that $ac = b^2 + 1$. Then there exist integers x, y, z, t such that $a = x^2+y^2$, $b = z^2+t^2$, $c = xz+yt$.

3.[G.Polya] 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 looks from the origin, he can see at least a point situated at the exterior of the disc. Then

$$\frac{1}{\sqrt{R^2+1}}\leq r<\frac{1}{R}.$$

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 $\sum\limits_{1\leq i,j\leq n} a_{ij}x_ix_j > 0$. Then there are integers (not all zero) $x_1, \ldots, x_n$ such that

$$\sum_{1\leq i,j\leq n} a_{ij}x_ix_j < n\sqrt[n]{\det A},$$

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 among $x_1, x_2, \ldots, x_n$. Prove that 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 and 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 Competition

9. Let us denote by $A(C, r)$ the set of points w on the unit sphere in $\mathbb{R}^n$ with the property that $|wk| \geq \frac{C}{\|k\|^r}$ for any nonzero 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 nonempty, but if $r < n-1$ there is no such C.

Mathlinks contest (after an ENS entrance exam problem)

10. Using the nonelementary results presented in this chapter, prove that if $A = (a_{ij})_{1 \leq i,j \leq n}$ is a symmetric matrix with integer entries 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 there is a matrix B with integer entries such that $A = B \cdot {}^tB$.

11. Let $n \geq 5$ and let $a_1, \ldots, a_n, b_1, \ldots, b_n$ be integers such that 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 we can find $1 < |i - j| < n - 1$ such that $|a_i b_j - a_j b_i| = 1$.

Korean TST

12.[Nikolai Nikolov] Let a, b, c, d be positive integers such that there are 2004 pairs (x, y) with $x, y \in [0, 1]$ for which $ax + by, cx + dy \in \mathbb{Z}$. If $gcd(a, c) = 6$, find $gcd(b, d)$.

Bulgaria Olympiad

13. In the plane consider a polygon of area greater than n. 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

14. Prove that there is no position in which an n by n square can cover more than $(n+1)^2$ integral lattice points.

D.J.Newman, AMM E 1954

The smaller, the better

Quite often, a collection of simple ideas can make very difficult problems look easy. We have seen or will see a few such examples in our journey through the world of numbers: congruences that readily solve Diophantine equations, properties of the primes of the form $4k+3$ or even facts about complex numbers, analysis or higher algebra, cleverly applied. 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 the integer $n > 1$ and the integer a such that $gcd(a, n) = 1$, the least positive 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 exist. The complexity of this concept will be illustrated in the examples to follow.

We will denote by $o_n(a)$ the order of a modulo n. A simple property of $o_n(a)$ 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 $n|a^d - 1$, it follows that $n|a^{gcd(k,d)} - 1$. But from the definition of d we have $d \leq gcd(k, d)$, which cannot hold unless $d|k$. Nice and easy. But could such a simple idea be of any use? The answer is positive and the solutions of the problems to come will vouch for it. 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. 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 n-th Fermat number $2^{2^n}+1$ is congruent to 1 modulo 2^{n+1}. Then 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 divides $(2^{2^n} + 1)(2^{2^n} - 1) = 2^{2^{n+1}} - 1$ 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 $k = n + 1$. 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 $p|2^{2^n}+1$. Hence we found that $o_p(2)=2^{n+1}$ and we need to prove that $o_p(2)|p-1$ to finish the first part of the question. But this follows from the introduction of this chapter.

The second part is a direct consequence of the first. Indeed, it is enough to prove that there exists an infinite set of pairwise relatively prime Fermat's numbers $(2^{2^{n_k}}+1)_{n_k>0}$. Then we could take a prime factor of each such number and apply the first part to obtain that each such prime is of the form 2^nk+1. But not only it is easy to find such a sequence of 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 and 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 positive integers n such that $pn+1$ is prime.

Solution.

a) In fact, we will prove that any prime factor of $f_p(m)$ is relatively prime to $m(m-1)$. 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 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 that is divisible by p. Then we have $q|m^p-1$. But this implies that $o_q(m)|p$ 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, while solving a), we have seen 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 $m_k=pf(m_1)f_p(m_2)\dots f_p(m_{k-1})$. Let us prove that $f_p(m_k)$ is relatively prime to $f_p(m_1), f_p(m_2),\dots,f_p(m_{k-1})$. But this is easy, since $f_p(m_1)f_p(m_2)\dots f_p(m_{k-1})|f_p(m_k)-f_p(0)|f_p(m_k)-1$. The solution ends here.

The following problem became classical and variants of it have been subject of mathematics competitions for years. It seems to be a favorite Olympiad problem, since it uses elementary facts and the method is nothing less than beautiful.

Example 4. Find the least n such 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 factorization

$$17^{2^k} - 1 = (17 - 1)(17 + 1)(17^2 + 1) \ldots (17^{2^{k-1}} + 1),$$

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. Hence $v_2(17^{2^k} - 1) = 4 + k$ 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.

Example 5.[Gabriel Dospinescu] Find all primes $p$and q such that $p^2 + 1|2003^q + 1$ and $q^2 + 1|2003^p + 1$.

Solution. Without loss of generality, we may assume 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 to 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 $gcd(q, o_r(2003)) = 1$. 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 $r|p^2 + 1$, it 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).

A bit 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.[Reid Barton] Find all ordered triples of primes (p, q, r) such that

$$p|q^r + 1, q|r^p + 1, r|p^q + 1.$$

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 $p|\dfrac{q+1}{2}$. In the same way, we find that $q|\dfrac{r+1}{2}$ and $r|\dfrac{p+1}{2}$. This is clearly impossible, just by looking at the greatest among p, q, r. So, our assumption is wrong and 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 this triple.

Can you find the least 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 least prime factor. But here is a beautiful and short solution, which does not need a single division.

Example 7. Find the least prime factor of the number $12^{2^{15}} + 1$.

Solution. Let p be this prime number. Because p divides $\left(12^{2^{15}} + 1\right) \cdot \left(12^{2^{15}} - 1\right) = 12^{2^{16}} - 1$, 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 it, you can check it!). 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 $\left(\dfrac{3}{q}\right) = -1$. But this is done in the chapter **Quadratic reciprocity** and the answer is positive, so indeed $3^{\frac{q-1}{2}} + 1 \equiv 0$

(mod q) and $2^{16}+1$ is the least 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, you might find the energy to devote attention to the following interesting problems.

Example 8. Prove that for any $n>1$ the greatest prime factor of $2^{2^n}+1$ is greater than or equal to $n\cdot 2^{n+2}+1$.

China TST 2005

Solution. You will not imagine how simple this problem really is. If the start is right... Indeed, let us write $2^{2^n}+1=p_1^{k_1}\dots p_r^{k_r}$ where $p_1<\dots<p_r$ are prime numbers. We know that we can find positive integers q_i 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 $1\equiv 1+2^{n+1}\sum\limits_{i=1}^{r}k_iq_i \pmod{2^{2n+2}}$ and so $\sum\limits_{i=1}^{r}k_iq_i\geq 2^{n+1}$. But then $q_r\sum\limits_{i=1}^{r}k_i\geq 2^{n+1}$. Now everything becomes clear, since $2^{2^n}+1>(1+2^{n+1})^{k_1+\dots+k_r}$ and so $k_1+\dots+k_r\leq\dfrac{2^n}{n+1}$. This shows that $q_r\geq 2(n+1)$ and the proof finishes here.

Example 9 [Paul Erdos] It is not known whether there are infinitely many primes of the form $2^{2^n}+1$. Yet, prove that if x_n is the sum of the reciprocals of the proper divisors of $2^{2^n}+1$, then x_n converges to 0.

AMM, 4590

Solution Observe that the sum of the reciprocals of all the divisors of an integer n is $\frac{\sigma(n)}{n}$, where $\sigma(n)$ is the sum of all the divisors of n. Therefore it suffices to prove that $\frac{\sigma(2^{2^n}+1)}{2^{2^n}+1}$ converges to 1. Let $p_1^{k_1}\cdot\ldots\cdot p_r^{k_r}$ be the prime factorization of $2^{2^n}+1$ and observe that $1>\frac{\sigma(2^{2^n}+1)}{2^{2^n}+1}>\prod\limits_{i=1}^{r}(1-\frac{1}{p_i})>(1-\frac{1}{2^n})^r$. Because $2^{2^n}+1>2^{n(k_1+\ldots+k_r)}\geq 2^{rn}$, we can easily establish that $\prod\limits_{i=1}^{r}(1-\frac{1}{p_i})$ converges to 1 for sufficiently large n. The conclusion follows.

We have seen that the order of a modulo n is a divisor of $\varphi(n)$. Therefore a natural question appears: given a positive integer n, can we always find an integer a whose order modulo n is exactly $\varphi(n)$?. We call such a number a a primitive root modulo n. The answer to this question turns out to be negative, but in some cases primitive roots exist. We will prove here that primitive roots mod p^n exist whenever $p>2$ is a prime number and n is a positive integer. The proof is quite long and complicated, but breaking it into smaller pieces will make it easier to understand. So, let us start with a lemma due to Gauss:

Lemma For any positive integer $n > 1$, $\sum\limits_{d|n} \varphi(d) = n$.

One of the (many) proofs goes like this: imagine that you are trying to reduce the fractions $\frac{1}{n}, \frac{2}{n}, ..., \frac{n}{n}$ in lowest terms. The denominator of any new fraction will be a divisor of n and it is clear that for any divisor d of n we obtain $\varphi(d)$ fractions with denominator d. By counting in two different ways the total number of fractions obtained, we can conclude.

Take now $p > 2$ a prime number and observe that any element of Z_p has an order which divides $p-1$. Consider d a divisor of $p-1$ and define $f(d)$ as the number of elements in Z_p that have order d. Suppose that x is an element of order d. Then $1, x, ..., x^{d-1}$ are distinct solutions of the equation $u^d = 1$, equation which has at most d solutions in the field Z_p. Therefore $1, x, ..., x^{d-1}$ are all solutions of this equation and any element of order d is among these elements. Clearly, x^i has order d if and only if $gcd(i, d) = 1$. Thus at most $\varphi(d)$ elements have order d, which means that $f(d) \leq \varphi(d)$ for all d. But since any nonzero elements has an order which divides $p-1$, we deduce that $\sum\limits_{d|p-1} f(d) = p-1 = \sum\limits_{d|p-1} \varphi(d)$ (we used in the last equality the lemma above). This identity combined with the previous inequality shows that $f(d) = \varphi(d)$ for all $d|p-1$. We have thus proved the following:

Theorem For any divisor d of $p-1$ there are exactly $\varphi(d)$ elements of order d in Z_p.

The above theorem implies the existence of primitive roots modulo any prime p (the case $p = 2$ being obvious). Observe that if a is a primitive root mod p, then the p elements $0, 1, a, a^2, ..., a^{p-2}$ are distinct and so they represent a permutation of Z_p.

Let us fix now a prime number $p > 2$ and a positive integer k and show the existence of a primitive root mod p^k. First of all, let us observe that for any $j \geq 2$ and any integer x we have $(1+xp)^{p^{j-2}} = 1 + xp^{j-1}(modp^j)$. Establishing this property is immediate by induction on j and the binomial formula. With this preparatory result, we will prove now the following:

Theorem
If p is an odd prime, then for any positive integer k there exists a primitive root mod p^k.

Indeed, take a a primitive root mod p. Clearly, $a+p$ is also a primitive root mod p. Using again the binomial formula, it is easy to prove that one of the two elements a and $a+p$ is not a root of $X^{p-1} - 1$ mod p^2. This shows that there exists y a primitive root mod p for which $y^{p-1} \neq 1(modp^2)$.

Let $y^{p-1} = 1 + xp$. Then by using the previous observation we can write $y^{p^{k-2}(p-1)} = (1 + xp)^{p^{k-2}} = 1 + xp^{k-1}(modp^k)$ and so p^k does not divide $y^{p^{k-2}(p-1)} - 1$. Thus the order of y mod p^k is a multiple of $p - 1$ (because y is a primitive root mod p) which divides $p^{k-1}(p - 1)$ but does not divide $p^{k-2}(p - 1)$. So, y is a primitive root mod p^k.

In order to finish this (long) theoretical part, let us present a very efficient criterion for primitive roots modulo p^k:

Theorem
Any primitive root mod p and p^2 is a primitive root modulo any power of p.

Let us prove first that if a is a primitive root mod p and p^2 then it is also a primitive root mod p^3. Let k be the order of a mod p^3. Then k is a divisor of $p^2(p-1)$. Because p^2 divides $a^k - 1$, k must be a multiple of $p(p-1)$. It remains to prove that k is not $p(p-1)$. Supposing the contrary, let $a^{p-1} = 1 + rp$, then we know that $p^3|(1 + rp)^p - 1$. Using again the binomial formula, we deduce that p divides r and so p^2 divides $a^{p-1} - 1$, which is contradictory with the fact that a is a primitive root mod p^2. Now, we use induction. Suppose that $n \geq 4$ and that a is a primitive root mod p^{n-1}. Let k be the order of a mod p^n. Because p^{n-1} divides $a^k - 1$, k must be a multiple of $p^{n-2}(p - 1)$. Also, k is a divisor of $p^{n-1}(p - 1) = \varphi(p^n)$. So, all we have to do is to prove that k is not $p^{n-2}(p-1)$. Otherwise, by Euler's theorem we can write $a^{p^{n-3}(p-1)} = 1 + rp^{n-2}$ and from the binomial formula it follows that r is a multiple of p and so p^{n-1} divides $a^{p^{n-3}(p-1)} - 1$, contradiction with the fact that a has order $p^{n-2}(p - 1)$ modulo p^{n-1}. The theorem is thus proved.

Problems for training

1. Let $a, n > 2$ be 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 $\dfrac{2^p + 1}{3}$ is of the form $2kp + 1$.

Fermat

4. Find all positive integers m, n for which $n|m^{2 \cdot 3^n} + m^{3^n} + 1$.

Bulgaria 1997

5. Find the least multiple of 19 all of whose digits are 1.

Gazeta Matematica

6. Let p be a prime and let $q > 5$ be a prime factor of $2^p + 3^p$. Prove that $q > p$.

Laurentiu Panaitopol, TST Romania

7. Let $m > 1$ be an odd number. Find the least n such that $2^{1989} | m^n - 1$.

IMO 1989 Shortlist

8. Let $0 < m < n$ be integers such that 1978^m and 1978^n have the same last three digits. Find the least value of $m + n$.

IMO 1978

9. Let p be a prime number and let d be a positive divisor of $p - 1$. Prove that there is a positive integer n such that $o_p(n) = d$.

10. Let $q = k \cdot 2^m + 1$ be a divisor of $2^{2^n} + 1$, where k is odd. Find $o_q(k)$ in terms of n and $v_2(m)$

J. van de Lune

11. 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.

Proth, Pocklington, Lehmer Test

12. Let a be an integer greater than 1. 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 E 3216

13. Let $d = o_p(n)$ and let $k = v_p(n^d - 1)$. Prove that
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 $l = v_p(n^{pd} - 1)$. In addition, $o_p(n) = d$, $o_{p^j}(n) = pd$ for $2 \leq j \leq l$ and $o_{p^j}(n) = p^{j-l+1}d$, for all $j \geq l$.

14. Let A be a finite set of prime numbers and let a be an integer greater than 1. Prove that there are only finitely many positive integers n such that all prime factors of $a^n - 1$ are in A.

Iran Olympiad

15. Prove that for any prime p there is a prime q that does not divide any of the numbers $n^p - p$, with $n \geq 1$.

IMO 2003

16. Let a be an integer greater than 1. Prove that for infinitely many n the greatest 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 many more Olympiad problems in the future. Yet, there are some examples in which this result is inefficient. 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 effective Weil criterion and its consequences. The proofs of these results are nontrivial 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, corollaries of this theorem.

Example 1.[Radu Gologan] Prove that the sequence $([n\sqrt{2003}])_{n\geq 1}$ contains arbitrarily long geometric progressions with arbitrarily large ratio.

IMO TST, Romania, 2003

Solution. Let us take a very large number p. We will prove that there are arbitrarily long geometric sequences with ratio p. Given $n \geq 3$, we will 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. 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.[Gabriel Dospinescu] Consider a positive integer k and a real number a such that $\log a$ is irrational. For each $n \geq 1$ let x_n be the number formed by the first k digits of $[a^n]$. Prove that the sequence $(x_n)_{n\geq 1}$ is not eventually periodical.

Mathlinks Contest

Solution. The solution is based on some 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 $m = \overline{x_1x_2\dots x_p}$, with $p \geq k$. Then $m = \overline{x_1\dots x_k} \cdot 10^{p-k} + \overline{x_{k+1}\dots x_p}$, hence $\overline{x_1\dots x_k} \cdot 10^{p-k} \leq m < (\overline{x_1\dots x_k} + 1) \cdot 10^{p-k}$. It follows that $\overline{x_1\dots x_k} = \left[\dfrac{m}{10^{p-k}}\right]$ 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 direct consequence of Kronecker's theorem) and we 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.

We continue with two more subtle results, based on Kronecker's lemma. However, the way to proceed is not clear in these problems.

Example 3.[Roy Streit] For a pair (a, b) of real numbers let $F(a, b)$ denote the sequence of general term $c_n = [an + b]$. Find all pairs (a, b) such that $F(x, y) = F(a, b)$ implies $(x, y) = (a, b)$.

AMM, E 2726

Solution. Let us see what happens when $F(x, y) = F(a, b)$. We must have $[an + b] = [nx + y]$ for all positive integers n. Dividing by n this equality and taking the limit, we infer that $a = x$. Now, if a is rational, the sequence of fractional parts of $an + b$ takes only a finite number of values, so if r is chosen sufficiently small (but positive) we will have $F(a, b + r) = F(a, b)$, so no pair (a, b) can be a solution of the problem. On the other hand, we claim that any irrational number a is a solution for any real number b. Indeed, take $x_1 < x_2$ and a positive integer n such that $na + x_1 < m < na + x_2$ for a certain integer m. The existence of such an n follows immediately from Kronecker's theorem. But the last inequality shows that $F(a, x_1) \neq F(a, x_2)$ and so a is a solution. Therefore the answer is: all couples (a, b) with a irrational.

Finally, a very beautiful equivalent condition for the irrationality of a real number:

Example 4.[Klark Kimberling] Let r be a real number in $(0, 1)$ and let $S(r)$ be the set of positive integers n for which the interval $(nr, nr + r)$ contains exactly one integer. Prove that r is irrational if and only if for all integers M there exists a complete system of residues modulo M, contained in $S(r)$.

Solution.

One part of the solution is very easy: if r is rational, let M be its denominator. Then clearly if n is a multiple of M there is no k integer in the desired interval. Now, suppose that r is irrational and take integers m, M such that $0 \leq m < M$. By Kronecker's theorem, the integer multiples of $\frac{1}{r}$ form a dense set modulo M. So, there exists an integer k such that the image of $\frac{k}{r}$ is in $(m, m + 1)$, that is for a certain integer s we have $sM + m < \frac{k}{r}, sM + m + 1$. It is then clear that if we take $n = sM + m$ we have $n = m(modM)$ and $nr < k < nr + r$. This finishes the solution.

Before passing to the quantitative results stated at the beginning of this chapter, we must talk 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 reduce a complicated problem concerning real numbers to integers, as we will see in one of the examples. But first, let us state and prove this result.

Example 5. [Dirichlet] Let $x_1, x_2, \ldots, x_k$ be 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. 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 assign each q in the set $\{1, 2, \ldots, n\}$ 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 the pigeonhole principle we can find $1 \le u < v \le n$ such that the same sequence is assigned to u and v. This means that for all $1 \le i \le k$ we have

$$|\{ux_i\} - \{vx_i\}| < \frac{1}{N} \le \varepsilon.$$

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 next has meandered between world's Olympiads: proposed at the 1949 Moscow Olympiad, it appeared next at the W.L. Putnam Competition in 1973 and later on in an IMO Shortlist, proposed by Mongolia.

Example 6. Let $x_1, x_2, \ldots, x_{2n+1}$ be real numbers with the property: for any $1 \le i \le 2n+1$ one can make two groups of n numbers by using x_j, $j \ne i$, 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 well-known and not difficult: 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 number by 2 and obtain a new set with smaller sum of magnitudes and the same properties; otherwise, we subtract 1 from each number and then divide by 2).

Now, assume that they are real numbers, which is definitely more subtle a case. 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 condition in the statement as

$$\sum_{j \ne i} a_{ij} n x_j = 0 \text{ or } \sum_{j \ne i} a_{ij}(nx_j - p_j) = -\sum_{j \ne i} a_{ij} p_j$$

(where $a_{ij} \in \{-1, 1\}$). Then

$$\left|\sum_{j \ne i} a_{ij} p_j\right| = \left|\sum_{j \ne i} a_{ij}(nx_j - p_j)\right| \le 2n\varepsilon.$$

Thus if we choose $\varepsilon < \dfrac{1}{2n}$, then $\sum\limits_{j\neq i} a_{ij}p_j = 0$ and so $p_1, p_2, \ldots, p_k$ have the same property. Because they are all integers, $p_1, p_2, ..., p_k$ must be all equal (again, because of the first case). Hence 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, yet containing all the necessary ingredients.

First, we observe that a) says precisely that b) is true for the characteristic function of any subinterval 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. You 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 polynomial. 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 nontrivial result due to Weierstrass), we deduce that b) is true for continuous functions f for which $f(0) = f(1)$. Now, given a continuous $f : [0, 1] \to \mathbb{R}$, 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. So, here is the classical example.

Example 7. Let a be an irrational number. Then the sequence $(na)_{n\geq 1}$ is uniformly distributed mod 1.

Solution. Well, after so much work, you deserve a reward: this is a simple consequence of Weyl's criterion. Indeed, it suffices to prove that c) is true, 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 clearly satisfied and thus we obtain the desired result.

Before presenting the next 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. It is probably now the time to solve the problem mentioned at the very beginning of this note: how to compute the density of those numbers n for which 2^n begins with (for example) 2006. Well, again a reward: this is going to be equally easy (of course, you need some rest before looking at some deeper results...).

Example 8. 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 as

$$\log 2007 + p > n \log 2 \geq \log 2006 + p$$

and mplies $[n \log 2] = p + 3$. Hence $\log \frac{2007}{1000} > \{n \log 2\} > \log \frac{2006}{1000}$. 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 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 Weyl's criterion can yield difficult and important results.

Example 9. [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 (x_n) is also equidistributed.

This is not an Olympiad problem!!! But mathematics is not just about Olympiads 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 not well-known and 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 $\{1, 2, \ldots, n\}$):*

$$h^2 \left|\sum_{i=1}^{n} z_i\right|^2 \leq (n+h-1)\left[2\sum_{r=1}^{h-1}(h-r)\mathrm{Re}\left(\sum_{i=1}^{n-r} z_i\overline{z_{i+r}}\right) + h\sum_{i=1}^{n}|z_i|^2\right].$$

Unbelievable, but true! Not to mention that the proof of this inequality is anything but easy. We will limit ourselves 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 you will get some satisfaction... if you have the patience to expand $\displaystyle\sum_{i=1}^{n+h-1}\left|\sum_{j=0}^{h-1} z_{i-j}\right|^2$ and see that it is nothing else than

$$2\sum_{r=1}^{h-1}(h-r)\mathrm{Re}\left(\sum_{i=1}^{n-r} z_i\overline{z_{i+r}}\right) + h\sum_{i=1}^{n}|z_i|^2.$$

Wishing you good luck with the computations, we will now prove Van der Corput's theorem, by using this lemma and Weyl's criterion.

Of course, the idea is to show that

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} e^{2i\pi p x_k} = 0$$

for all $p \geq 1$. Fix such a p 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, observe that

$$\mathrm{Re}\left(\sum_{j=1}^{n-i} z_j\cdot\overline{z_{i+j}}\right) = \mathrm{Re}\left(\sum_{j=1}^{n-i} e^{2i\pi p(x_j - x_{i+j})}\right) \leq \left|\sum_{j=1}^{n-i} e^{2i\pi p(x_j - x_{i+j})}\right|.$$

Using Weyl's criterion for the sequences $(x_{n+i} - x_n)_{n\geq 1}$ 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 n large enough. 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 Weyl's criterion is satisfied and thus $(x_n)_{n\geq 1}$ 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 a famous theorem of Weyl. It is related to the equidistribution of the sequence $(f(n))_{n\geq 1}$ where f is a real polynomial having at least one irrational coefficient other than the free term. We will not prove this here, but focus on the following result.

Example 10 [Weyl] Let f be a polynomial with real coefficients and irrational leading coefficient. Then the sequence $(f(n))_{n\geq 1}$ is equidistributed.

You have 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 $(f(n+p)-f(n))_{n\geq 1}$ is equidistributed. But this is exactly the induction hypothesis applied to the polynomial $f(X+p)-f(X)$ (whose leading coefficient is clearly irrational). The proof by induction finishes here.
We end the discussion with a very useful criterion for uniform distribution, due to Fejer and which turns out to be very general. The proof is however very involved:

Example 10[Fejer]

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. 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. Prove that 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 each $n\geq n_0$.

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 Competition

13. Let $z_1,z_2,\dots,z_n$ be arbitrary complex numbers. Prove that for any $\varepsilon>0$ there are infinitely many positive integers n such that

$$\varepsilon+\sqrt[k]{|z_1^k+z_2^k+\cdots+z_n^k|}>\max\{|z_1|,|z_2|,\dots,|z_n|\}.$$

The sum of the digits of a positive integer

Problems about the sum of the digits of a positive integer often occur in mathematical contests because of their difficulty and lack of standard ways to tackle them. This is why a synthesis of the most frequent techniques used in such problems is useful. We have selected several representative problems to illustrate how the main results and techniques work and why they are so important.

We will only work in base 10 and will denote the decimal sum of the digits of the positive integer x by $s(x)$. The following "formula" can be easily checked:

$$s(n) = n - 9\sum_{k\geq 1}\left\lfloor \frac{n}{10^k}\right\rfloor \tag{1}$$

From (1) we can deduce immediately some well-known results about $s(n)$, such as $s(n) \equiv n(\bmod 9)$ 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 the sum of the digits, results which may offer simple ways to attack harder problems.

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.

Example 1. Prove that among any 79 consecutive numbers, we can choose at least one whose sum of digits is a multiple of 13.

Baltic Contest 1997

Solution. Note that among the first 40 numbers, there are exactly four multiples of 10. Also, it is clear that the next to last digit of one of them is at least 6. Let x be this number. Clearly, 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. 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.

Example 2. Find the greatest N such that there are N consecutive positive integers such 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 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 all of them should be even. Indeed, we carry over at $a+10$ only when the next to last 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 $2 \leq i \leq 11$, $s(N+i) = 2+9+0+9(11!-1)+i-2 = i+9\cdot 11!$ while for $12 \leq i \leq 21$, $s(N+i) = 2+9+1+(i-12) = i$, so our numbers have the desired property.

Example 3.[Adrian Zahariuc] How many positive integers $n \leq 10^{2005}$ can be written as the sum of two positive integers with the same sum of digits?

Solution. Answer: $10^{2005} - 9023$. At first glance, it is seemingly 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 except for the first are 9 and the sum of its digits is odd.

Let n be such a number. Suppose there are positive integers a and b such that $n = a+b$ and $s(a) = s(b)$. The main fact is that when we add $a+b = n$, there are no carry overs. 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 above, can be written as the sum of two positive integers with the same sum of digits. We will start with the following:

Lemma. There is $a \leq n$ such that $s(a) \equiv s(n-a)(\text{mod}2)$.

If $s(n)$ is even, take $a = 0$. If $s(n)$ is odd, then n must have a digit which is not the first one and is not equal to 9, otherwise it would have one of the forbidden forms mentioned in the beggining of the solution. Let c be this digit and let p be its position (from right to left). Choose $a = 10^{p-1}(c+1)$. In the addition $a + (n-a) = n$ there is exactly one carry over, so

$$s(a) + s(n-a) = 9 + s(n) \equiv 0(\text{mod}2) \Rightarrow s(a) \equiv s(n-a)(\text{mod}2)$$

which proves our claim.

Back to the original problem. All we have to do now is take one-by-one a "unit" from a number and give it to the other until the two numbers have the same sum of digits. This will happen because they have the same parity. So, let us do this rigorously. Set

$$a = \overline{a_1 a_2 .. a_k}, n - a = \overline{b_1 b_2 ... b_k}.$$

Let I be the set of those $1 \leq i \leq k$ for which $a_i + b_i$ is odd. The lemma shows that the number of elements of I is even, so it can be divided into two sets with the same number of elements, say I_1 and I_2. For $i = 1, 2, ..., k$ define $A_i = \frac{a_i+b_i}{2}$ if $i \in I$, $\frac{a_i+b_i+1}{2}$ if $i \in I_1$ or $\frac{a_i+b_i-1}{2}$ 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 properties $s(A) = s(B)$ and $A + B = n$. The proof is complete.

We have previously seen that $s(n) \equiv n(\text{mod}9)$. This is probably the most known property of the function s and it has a series of remarkable applications. Sometimes it is combined with simple inequalities such as $s(n) \leq 9(\lfloor \log n \rfloor + 1)$. Some immediate applications are the following:

Example 4.[Vasile Zidaru, Mircea Lascu] Find all n for which one can find a and b such that

$$s(a) = s(b) = s(a+b) = n.$$

JBMO TST 1999

Solution. We have $a \equiv b \equiv a + b \equiv n(\text{mod}9)$, so 9 divides n. If $n = 9k$, we can take $a = b = 10^k - 1$ and we are done, since $s(10^k - 1) = s(2 \cdot 10^k - 2) = 9k$.

Example 5. Find all the possible values of the sum of the digits of a perfect square.

Iberoamerican Contest 1995

Solution. What does the sum of the 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 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 the 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 $s(16) = 7$ the proof is complete.

Example 6. Compute $s(s(s(4444^{4444})))$.

IMO 1975

Solution. Using the inequality $s(n) \leq 9(\lfloor \log n \rfloor + 1)$ several times we have

$$s(4444^{4444}) \leq 9(\left\lfloor \log 4444^{4444} \right\rfloor + 1) < 9 \cdot 20000 = 180000;$$

$$s(s(4444^{4444})) \leq 9(\left\lfloor \log s(4444^{4444}) \right\rfloor + 1) \leq 9(\lg 180000 + 1) \leq 36,$$

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

$$4444^{4444} \equiv 7^{4444} = 7 \cdot 7^{3 \cdot 1481} \equiv 7(\mathrm{mod} 9),$$

the only possible answer is 7.

Finally, we present two beautiful problems which appeared in the Russian Olympiad and, later, in Kvant.

Example 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 an N such that $s(3^{n+1}) - s(3^n) > 0$ for all $n \geq N$. But, for $n \geq 2$, $s(3^{n+1}) - s(3^n) \equiv 0(\mathrm{mod} 9)$, so $s(3^{n+1}) - s(3^n) \geq 9$ for all $n \geq N$. It follows that

$$\sum_{k=N+1}^{n} \left(3^{k+1} - 3^k\right) \geq 9(n-N) \Rightarrow s(3^{n+1}) \geq 9(n-N)$$

for all $n \geq N+1$. But $s(3^{n+1}) \leq 9(\lfloor \log 3^{n+1} \rfloor + 1)$, so $9n - 9N \leq 9 + 9(n+1)\log 3$, for all $n \geq N+1$. This is obviously a contradiction.

Example 8.[I.N. Bernstein] Find all positive integers k for which there exists a positive constant c_k such that $\frac{s(kN)}{s(N)} \geq c_k$ for all positive integers N. For any such k, find the best c_k.

Solution. It is not difficult to observe that any k of the form $2^r \cdot 5^q$ is a solution of the problem. Indeed, in that case we have (by using the properties presented in the beginning of the chapter):

$$s(N) = s(10^{r+q}N) \leq s(2^q \cdot 5^r)s(kN) = \frac{1}{c_k}s(kN)$$

where clearly $c_k = \frac{1}{s(2^q \cdot 5^r)}$ is the best constant (we have equality for $N = 2^q \cdot 5^r$). Now, assume that $k = 2^r \cdot 5^q \cdot Q$ with $Q > 1$ relatively prime to 10. Let $m = \varphi(Q)$ and write $10^m - 1 = QR$ for some integer R. If $R_n = R(1 + 10^m + \ldots + 10^{m(n-1)}$ then $10^{mn} - 1 = QR_n$ and so $s(Q(R_n + 1)) = s(10^{mn} + Q - 1) = s(Q)$ and $s(R_n + 1) \geq (n-1)s(R)$. By taking n sufficiently large, we conclude that for any $\epsilon > 0$ there exists $N = R_n + 1$ such that

$$\frac{s(kN)}{s(N)} \leq \frac{s(2^r \cdot 5^q)s(Q)}{(n-1)s(R)} < \epsilon.$$

This shows that the numbers found in the first part of the solution are the only solutions of the problem.

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:

Lemma 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 $x = \overline{a_1 a_2 ... a_j}$ with $a_j \neq 0$ (we can ignore the trailing 0's of x) and note that

$$x(10^n - 1) = \overline{a_1 a_2 ... a_{j-1}(a_j - 1)\underbrace{99...99}_{n-j}(9 - a_1)...(9 - a_{j-1})(10 - a_j)},$$

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:

Example 9. Compute $s(9 \cdot 99 \cdot 9999 \cdot ... \cdot \underbrace{99...99}_{2^n})$.

USAMO 1992

Solution. The problem is 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.

Example 10. Prove that for any n there is a positive integer with n digits, all of them nonzero and which is divisible by the sum of its digits.

IMO 1998 Shortlist

Solution. Only to assure our readers that this problem did not appear on the IMO Shortlist out of nowhere, such numbers are called Niven numbers and they are an important research source in number theory. Now, let us solve it. We will see that constructing such a number is difficult. 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 $3^{k+2} | 10^{3^k} - 1$).

From the idea that we should search numbers with many equal digits and the last result, we decide that the required number p should be of the form $\underbrace{aa...aa}_{s} b \cdot (10^t - 1)$, with $\underbrace{aa...aa}_{s} b \leq 10^t - 1$. This number has $s + t + 1$ digits and its sum of digits is $9t$. Therefore, we require $s + t = n - 1$ and $9t | \underbrace{aa...aa}_{s} b \cdot (10^t - 1)$. We now use the fact that if t is a power of 3, then $9t | 10^t - 1$. So, let us take

$t = 3^k$ where k is chosen such that $3^k < n < 3^{k+1}$. If we also take into account the condition $\underbrace{aa...aa}_{s}b \le 10^t - 1$, the choice $p = \underbrace{11...11}_{n-3^k-1}2(10^{3^k} - 1)$ when $n \le 2 \cdot 3^k$ and $p = \underbrace{22...22}_{2 \cdot 3^k}(10^{2 \cdot 3^k} - 1)$ otherwise becomes natural.

We continue our investigations of finding suitable techniques for problems involving sum of digits with a very beautiful result, which has several interesting and difficult consequences.

Lemma. Any multiple of $\underbrace{11...11}_{k}$ has sum of its 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 $M \ge 10a > 10^k$. Hence $M = \overline{a_1a_2...a_p}$, with $p \ge k+1$ and $a_p \ne 0$. Take $N = M - 10^{p-k}a$. Clearly, N is a multiple of a. We will 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 difficult 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 three applications of this fact, which might seem simple, but seemingly unsolvable without it. But before that, let us insist a little bit on a very similar (yet more difficult) problem proposed by Radu Todor for the 1993 IMO: if $b > 1$ and a is a multiple of $b^n - 1$, then a has at least n nonzero digits when expressed in base b. The solution uses the same idea, but the details are not obvious, so we will present a full solution. Arguing by contradiction, assume that there exists A a multiple of $b^n - 1$ with less than n nonzero digits in base b and among all these numbers consider that number A with minimal number of nonzero digits in base b and with minimal sum of digits in base b. Suppose that a has exactly s nonzero digits (everything is in base b) and let $A = a_1b^{n_1} + a_2b^{n_2} + ... + a_sb^{n_s}$ with $n_1 > n_2 > ... > n_s$. We claim that $s = n$. First of all, we will prove that any two numbers among $n_1, n_2, ..., n_s$ are not congruent mod n. It will follow that $s \le n$. Indeed, if $n_i = n_j (mod n)$ let $0 \le r \le n-1$ be the common value of n_i and n_j modulo n. The number $B = A - a_ib^{n_i} - a_jb^{n_j} + (a_i + a_j)b^{nn_1+r}$ is clearly a multiple of $b^n - 1$. If $a_i + a_j < b$ then B has $s-1$ nonzero digits, which contradicts the minimality of s. So $b \le a_i + a_j < 2b$. If $q = a_i + a_j - b$, then

$$B = b^{nn_1+r+1} + qb^{nn_1+r} + a_1b^{n_1} + ... + a_{i-1}b^{n_{i-1}}$$

$$+a_{i+1}^{n_{i+1}} + ... + a_{j-1}b^{n_{j-1}} + a_{j+1}b^{n_{j+1}} + .. + a_sb^{n_s}$$

. Therefore the sum of digits of B in base b is $a_1+a_2+...+a_s+1+q-(a_i+a_j) < a_1+a_2+...+a_s$. This contradiction shows that $n_1, n_2, ..., n_s$ give distinct remainders $r_1, r_2, ..., r_s$ when divided by n. Finally, suppose that $s < n$ and consider the number $C = a_1 b^{r_1} + ... + a_s b^{r_s}$. Clearly, C is a multiple of $b^n - 1$. But $C < b^n - 1$! This shows that $s = n$ and finishes the solution.

Example 11. Prove that for every k, we have

$$\lim_{n\to\infty} \frac{s(n!)}{\log^k \log n} = \infty.$$

Solution. Due to the simple fact that $10^{\lfloor \log n \rfloor} - 1 \leq n \Rightarrow 10^{\lfloor \log n \rfloor} - 1 | n!$, we have $s(n!) \geq \lfloor \log n \rfloor$, from which our conclusion follows.

Example 12. Let S be the set of positive integers whose decimal representation contains only of at most 1988 ones and the rest zeros. Prove that there is a positive integer which does not divide any element 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.

Example 13. Prove that for any $k > 0$, there is an infinite arithmetical sequence having the common difference relatively prime to 10, such that all its terms have the sum of digits greater than k.

IMO 1999 Shortlist

Solution. Let us remind you that this is the last problem of IMO 1999 Shortlist, so one of the hardest. The official solution seems to confirm this. 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 problem from the USAMO.

Example 14.[Gabriel Dospinescu and Titu Andreescu] Let n be a fixed positive integer. Denote by $f(n)$ the smallest k for which one can find a set X of n positive integers with the property

$$s\left(\sum_{x\in Y} x\right) = k$$

for all nonempty subsets Y of X. Prove that $C_1 \log n < f(n) < C_2 \log n$ for some constants C_1 and C_2.

USAMO 2005

Solution. We will prove that

$$\lfloor \log(n+1) \rfloor \leq f(n) \leq 9 \log \left\lceil \frac{n(n+1)}{2} + 1 \right\rceil ,$$

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 lemma, 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 upper bound is proved. Now, let m be the greatest 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 two of them congruent mod m, say the i-th and the j-th. Then, $m | a_{i+1} + a_{i+2} + ... + a_j$ and we are done.

From the lemma, it follows that any set n-element set X has a subset Y whose sum of elements is divisible by $10^m - 1$. By our second lemma, 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.

Example 15.[Adrian Zahariuc and Gabriel Dospinescu] Let a and b be positive integers such that $s(an) = s(bn)$ for all n. Prove that $\log \frac{a}{b}$ is an integer.

Solution. We start with an observation. If $gcd(\max\{a, b\}, 10) = 1$, then the problem becomes trivial. Indeed, suppose that $a = \max\{a, b\}$. 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 an 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 k, the first p nonzero digits of $\frac{b}{a}$ are exactly the same as the first p digits of bn_k. This means that the sum of the first p digits of $\frac{b}{a}$ is bounded, which could only happen when this fraction has finitely many decimals. Analogously, we can prove the same result about $\frac{a}{b}$.

Let $a = 2^x 5^y m$ and $b = 2^z 5^t m'$, where $gcd(m, 10) = gcd(m', 10) = 1$. It follows that $m|m'$ and $m'|m$, so $m = m'$. Now, we can write the hypothesis as

$$s(2^z 5^u mn2^{c-x}5^{c-y}) = s(2^x 5^y mn2^{c-x}5^{c-y}) = s(mn)$$

for all $c \geq \max\{x, y\}$. Now, if $p = max\{z + c - x, u + c - y\} - min\{z + c - x, u + c - y\}$, we find that there is a $k \in \{2, 5\}$ such that $s(mn) = s(mk^p n)$ for all positive integer n. It follows that

$$s(m) = s(k^p m) = s(k^{2p} m) = s(k^{3p} m) = ...$$

Let $t = a^p$, so $\log t \in \mathbb{R} - \mathbb{Q}$ unless $p = 0$. Now, we will use the following:

Lemma. If $\log t \in \mathbb{R} - \mathbb{Q}$, then for any sequence of digits, there is a positive integer n such that $t^n m$ starts with the selected sequence of digits.

Proof. If we prove that $\{\{\log t^n m\} | n \in \mathbb{Z}^+\}$ is dense in $(0, 1)$, then we are done. But $\log t^n m = n \log t + m$ and by Kronecker's theorem $\{\{n \log t\} | n \in \mathbb{Z}^+\}$ 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. Hence $p = 0$ and $z + c - x = u + c - y$, so $a = 10^{x-z} b$. 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 aforementioned methods are just a starting point in solving such problems since the spectrum of problems involving the sum of the digits is very large. The techniques are even more useful when they are applied creatively...

Problems for training

1. Prove that among any 39 consecutive positive integers there is one whose sum of digits is divisible by 11.

Russian Olympiad 1961

2. Prove that among any 18 consecutive two-digit numbers there is at least one Niven number.

Tournament of Towns 1997

3. Are there positive integers n such that $s(n) = 1000$ and $s(n^2) = 1000000$?

Russian Olympiad 1985

4. Prove that for any positive integer n there are infinitely many numbers m not containing any zero, such that $s(n) = s(mn)$.

Russian Olympiad 1970

5. Find all x such that $s(x) = s(2x) = s(3x) = ... = s(x^2)$.

Kurschak Competition 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 polynomials $p \in \mathbb{Z}[X]$ 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 positive integers n such that

$$s(n) + s(n^2) = s(n^3).$$

Gabriel Dospinescu

12. Let a, b, c,d be prime numbers such that $2 < a \leq c$ and $a \neq b$. Suppose that for sufficiently large n, the numbers $an + b$ and $cn + d$ have the same sum of digits in any 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 the following inequality holds

$$\frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n} < 3.2.$$

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. 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 of the form $10^n + b$ if and only if $b - 1$ is special.

Christopher D. Long

16. Find a Niven number with 100 digits.

Saint Petersburg 1990

17. Let S be a set of positive integers such that for any $\alpha \in \mathbb{R} - \mathbb{Q}$, there is a positive integer n such that $\lfloor \alpha^n \rfloor \in S$. Prove that S contains numbers with arbitrarily large sum of digits.

Gabriel Dospinescu

18. Let a be a positive integer such that $s(a^n + n) = 1 + s(n)$ for any sufficiently large n. Prove that a is a power of 10.

Gabriel Dospinescu

19. Let k be a positive integer. 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

20. Are there 19 positive integers with the same sum of digits, which add up to 1999?

Rusia, 1999

21. Let a and b be positive integers. Prove that the sequence $s(\lfloor an + b \rfloor)$ contains a constant subsequence.

Laurentiu Panaitopol, Romanian IMO TST 2002

22. If $s(n) = 100$ and $s(44n) = 800$, find $s(3n)$.

Rusia 1999

23. 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

24. Prove that

$$\sum_{n\geq 1} \frac{s(n)}{n(n+1)} = \frac{10}{9} \ln 10.$$

O. Shallit, AMM

25. Prove that the sum of digits of 9^n is at least 18 for $n > 1$.

AMM

26. Call a positive integer m special if it can be written in the form $n+s(n)$ for a certain positive integer n. Prove that there are infinitely many positive integers that are not special, but among any two consecutive numbers, at least one is special.

Kvant

At the border of analysis and number theory...

"Olympiad problems can be solved without using concepts from analysis (or linear algebra)" is a sentence often heard when talking about elementary problems given at various mathematics competitions. This is true, but the true nature and essence of some of these problems lies 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 to design, while when using analysis they can fall apart rather quickly. Well, of course, "quickly" only if you see the right sequence (or function) that hides behind each such problem. Practically, in this chapter our aim is to exhibit convergent integer sequences. These sequences will eventually become constant and from here the problem becomes much easier. The difficulty lies in finding those sequences. Sometimes, this is not so challenging, but most of the time it turns out to be a very difficult task. We develop skills in "hunting" for these sequences by solving first some easier problems and after that we attack the chestnuts.

As usual, we begin with a classical and beautiful problem, which has many applications and extensions.

Example 1. Let $f, g \in \mathbf{Z}[X]$ be two nonconstant polynomials such that $f(n)|g(n)$ for infinitely many n. Prove that f divides g in $\mathbf{Q}[X]$.

Solution. Indeed, we need to look at the remainder of g when divided by f in $\mathbf{Q}[X]$. Let us write $g = f \cdot q + r$, were q, r are polynomials in $\mathbf{Q}[X]$ with $\deg r < \deg f$. Now, multiplying by the common denominator of all coefficients of the polynomials q and r, the hypothesis becomes: there exist two infinite integer sequences $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ and a positive integer N such that $b_n = N\dfrac{r(a_n)}{f(a_n)}$ (we could have some problems with the zeros of f, but they are only finitely many, so for n large enough, a_n is not a zero of f). Because $\deg r < \deg f$, it follows that $\dfrac{r(a_n)}{f(a_n)} \to 0$, thus $(b_n)_{n\geq 1}$ is a sequence of integers that converges to 0. This implies that this sequence will eventually become the zero sequence. Well, this is the same as $r(a_n) = 0$ from a certain point n_0, which is practically the same as $r = 0$ (do not forget that any nonzero polynomial has only finitely many zeros). The problem is solved.

The next problem is a special case of a much more general and classical result: if f is a polynomial with integer coefficients, k is an integer greater than 1, and $\sqrt[k]{f(n)} \in \mathbf{Q}$ for all n, then there exists a polynomial $g \in \mathbf{Q}[X]$ such that $f(x) = g^k(x)$. We will not discuss here this general result (the reader will find a proof in the chapter **Arithmetic properties of polynomials**)

.

Example 2. Let a, b, c be integers with $a \neq 0$ such that $an^2 + bn + c$ is a perfect square for any positive integer n. Prove that there exist integers x and y 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 $(x_n)_{n\geq 1}$ of nonnegative integers. We could expect that $x_n - n\sqrt{a}$ converges. And yes, it does, but it is not a sequence of integers, so its convergence is more or less useless. In fact, 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 $\sqrt{a}$ (you have already noticed why it was not 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 consists of integers, so it is eventually constant. Hence we can find a positive integer M such that $x_{n+1} = x_n + \sqrt{a}$ for all $n \geq M$. Thus a must be a perfect square, that $a = x^2$ for some integer x. A simple induction shows that $x_n = x_M + (n - M)x$ for $n \geq M$ and so $(x_M - Mx + nx)^2 = x^2n^2 + bn + c$ for all $n \geq M$. Identifying the coefficients finishes the solution, since we can take $y = x_M - Mx$.

The next 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.

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.[Gabriel Dospinescu] 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 positive integers n such that n and $[a_1n] + [a_2n] + \cdots + [a_kn]$ are relatively prime.

Solution. The solution of such a problem is better to be indirect. So, let us assume that there exists a number M such that n and $[a_1n] + [a_2n] + \cdots + [a_kn]$ are not relatively prime for all $n \geq M$. Now, what are the most efficient numbers n to be used? They are the prime numbers, since if n is prime and it is not relatively prime with $[a_1n] + [a_2n] + \cdots + [a_kn]$, then it must divide $[a_1n] + [a_2n] + \cdots + [a_kn]$. This suggests considering the sequence of prime numbers $(p_n)_{n\geq 1}$. Since this sequence is infinite, there is N such that $p_n \geq M$ for all $n \geq N$. According to our assumption, this implies that for all $n \geq N$ there exist a positive integer x_n such that $[a_1p_n] + [a_2p_n] + \cdots + [a_kp_n] = x_np_n$. And now, you have already guessed what is the convergent sequence! Yes, it is $(x_n)_{n\geq N}$. This is clear, since $\frac{[a_1p_n] + [a_2p_n] + \cdots + [a_kp_n]}{p_n}$ converges to $a_1 + a_2 + \cdots + a_k$. Thus we can find P such that $x_n = a_1 + a_2 + \cdots + a_k$ for all $n \geq P$. But this is the same as $\{a_1p_n\} + \{a_2p_n\} + \cdots + \{a_kp_n\} = 0$. This says that a_ip_n are integers for all $i = 1, 2, ..., k$ and $n \geq P$ and so a_i are integers for all i, contradicting the hypothesis.

Step by step, we start to build some experience in "guessing" the sequences.

It is then time to solve some more difficult problems. The next one may seem obvious after reading its solution. In fact, it is just that type of problem whose solution is very short, but difficult to find.

Example 5. Let a and b be integers such that $a \cdot 2^n + b$ is a perfect square for all positive integers n. 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. From the hypothesis, there exists a sequence of positive integers $(x_n)_{n\geq 1}$ such that $x_n = \sqrt{a \cdot 2^n + b}$ for all n. Then, a direct computation shows that $\lim\limits_{n\to\infty}(2x_n - x_{n+2}) = 0$. This implies the existence of a positive integer N such that $2x_n = x_{n+2}$ for all $n \geq P$. 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 is wrong and indeed $a = 0$.

A classical result of Schur states that for any nonconstant 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 that (a_n) is a strictly increasing sequence of positive integers 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

$$\sum_{\alpha_1,\alpha_2,\ldots,\alpha_N\in\mathbf{Z}_+} \frac{1}{p_1^{k\alpha_1}\ldots p_N^{k\alpha_N}} < \infty.$$

Indeed, it suffices to remark that we actually have

$$\sum_{\alpha_1,\alpha_2,\ldots,\alpha_N\in\mathbf{Z}_+} \frac{1}{p_1^{k\alpha_1}\ldots p_N^{k\alpha_N}} = \prod_{j=1}^{N}\sum_{i\geq 0}\frac{1}{p_j^{ki}} = \prod_{j=1}^{n}\frac{p_j^k}{p_j^k - 1}.$$

On the other hand, by taking $k = \dfrac{1}{2\deg(f)}$ we 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

$$\sum_{n\geq 1} \frac{1}{a_n^k} \leq \sum_{\alpha_1,\alpha_2,\ldots,\alpha_N \in \mathbf{Z}_+} \frac{1}{p_1^{k\alpha_1} \ldots p_N^{k\alpha_N}} < \infty.$$

On the other hand, we also have

$$\sum_{n\geq 1} \frac{1}{a_n^k} \geq \sum_{n\geq 1} \frac{1}{(f(n))^k} = \infty,$$

a contradiction.

The same idea is used in the following problem.

Example 7. Let a and b be integers greater than 1. 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 Competition problem

Solution. Let us 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 positive integers 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 $\sum_{n\geq 1} b\left(\frac{b-1}{b}\right)^n$, which converges. The conclusion follows.

We return to classical mathematics and 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. Its beauty explains why the problem was so popular among the exam writters.

Example 8. Let f be a monic polynomial with integer coefficients such that for any positive integer n the equation $f(x) = 2^n$ has at least one positive integer solution. Prove that $\deg(f) = 1$.

Solution. 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 possible 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 $\dfrac{x_{n+k}}{x_n}$ 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

$$\lim_{x\to\infty} \frac{f(x)}{x^k} = 1 \text{ and } \lim_{n\to\infty} x_n = \infty,$$

we find that indeed

$$\lim_{n\to\infty} \frac{x_{n+k}}{x_n} = 2.$$

We see that this will help us a lot. Indeed, 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 as

$$x_{n+k} - 2x_n = \frac{\sum_{i=0}^{k-1} a_i(2^k x_n^i - x_{n+k}^i)}{\sum_{i=0}^{k-1} (2x_n)^i x_{n+k}^{k-i-1}}$$

But from the fact that $\lim_{n\to\infty} \dfrac{x_{n+k}}{x_n} = 2$, it follows that the right-hand side of the above relation is also convergent. Hence $(x_{n+k} - 2x_n)_{n\geq 1}$ converges and so there exist M, N such that for all $n \geq M$ we have $x_{n+k} = 2x_n + N$. But now the solution is almost over, 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 by using analysis. This algebraic property helps us to finish the solution. Indeed, we see that if z is a complex zero of f, then $2z+N, 4z+3N, 8z+7N, \ldots$ are all zeros of f. Since f is nonzero, this sequence must be finite and this can happen only for $z = -N$. Because $-N$ is the only zero of f, we deduce that $f(x) = (x+N)^k$. But since the equation $f(x) = 2^{2k+1}$ has positive integer roots, we find that $2^{\frac{1}{k}} \in \mathbf{Z}$, which implies $k = 1$, a contradiction. Thus, our assumption was wrong and $\deg(f) = 1$.

The idea of the following problem is so beautiful that any reader who attempts to solve it will feel generously rewarded by discovering this mathematical gem either by himself or in the solution provided.

Example 9.[S. Golomb] Let $\pi(n)$ be the number of prime numbers not exceeding n. Prove that there exist infinitely many n such that $\pi(n)|n$.

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 $\lim\limits_{n\to\infty} \frac{a_n}{n} = 0$, the sequence $\left(\frac{n}{a_n}\right)_{n\geq 1}$ contains all positive integers. In particular n divides a_n for infinitely many n.

Proof. Even if it seems unbelievable, this is true. Moreover, the proof is extremely short. Let m be a positive integer. Consider the set

$$A = \left\{ n \geq 1 | \ \frac{a_{mn}}{mn} \geq \frac{1}{m} \right\}.$$

This set contains 1 and it is bounded, since $\lim\limits_{n\to\infty} \frac{a_{mn}}{mn} = 0$. Thus it has a maximal element k. If $\frac{a_{mk}}{mk} = \frac{1}{m}$, then m is in the sequence $\left(\frac{n}{a_n}\right)_{n\geq 1}$. Otherwise, we have $a_{m(k+1)} \geq a_{mk} \geq k+1$, which shows that $k+1$ is also in the set, in contradiction with the maximality of k. The lemma is proved.

Thus, all we need to show now is that $\lim\limits_{n\to\infty} \frac{\pi(n)}{n} = 0$. 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 $\prod\limits_{p\leq n} p \leq 4^{n-1}$.

The proof of this result is magnificient. We use 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 $\prod\limits_{p\leq n} p \leq 4^n$. If n is even, we have nothing to prove, since

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p \leq 4^{n-2} < 4^{n-1}.$$

Now, assume that $n = 2k+1$ and consider the binomial coefficient

$$\binom{2k+1}{k} = \frac{(k+2)\dots(2k+1)}{k!}.$$

A simple application of the identity

$$2^{2k+1} = \sum_{i\geq 0} \binom{2k+1}{i}$$

shows that

$$\binom{2k+1}{k} \leq 4^k.$$

Thus, using the inductive hypothesis, we find

$$\prod_{p\le n} p \le \prod_{p\le k+1} p \cdot \prod_{k+2\le p\le 2k+1} p \le 4^k \cdot 4^k = 4^{n-1}.$$

Now, the fact that $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n} = 0$ follows easily. Indeed, fix $k \ge 1$. We have for all large n the inequality

$$(n-1)\log 4 \ge \sum_{k\le p\le n} \log p \ge \log k(\pi(n)-\pi(k)),$$

which shows that

$$\pi(n) \le \ \pi(k) + \frac{(n-1)\log 4}{\log k}.$$

This proves that $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n} = 0$. The problem is finally solved.

It is time now for the last problem, which is, as usual, very hard. We do not exaggerate if we say that the following problem is exceptionally difficult.

Example 10.[Marius Cavachi] Let a and b be integers greater than 1 such that $a^n - 1|b^n - 1$ for any positive integer n. Prove that b is a natural power of a.

AMM

Solution. This time we will be able to find the right convergent sequence only after examining a few recursive sequences. Let us see. So, initially we are given that there exists a sequence of positive integers $(x_n^{(1)})_{n\ge 1}$ such that $x_n^{(1)} = \dfrac{b^n-1}{a^n-1}$ Then, $x_n^{(1)} \cong \left(\dfrac{b}{a}\right)^n$ for large values of n. So, we could expect that the sequence $(x_n^{(2)})_{n\ge 1}$, $x_n^{(2)} = bx_n^{(1)} - ax_{n+1}^{(1)}$ 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 $\left(\dfrac{b}{a^2}\right)^n$, so much slower. And this is the good idea: repeat this procedure until the final sequence behaves like $\left(\dfrac{b}{a^{k+1}}\right)^n$, where k is chosen such that $a^k \le b < a^{k+1}$. 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 $\lim\limits_{n\to\infty} x_n^{(k+1)} = 0$. This isn't easy at all. The idea is to compute $x_n^{(3)}$ and after that to prove the following statement: for any $i \ge 1$ the sequence $(x_n^{(i)})_{n\ge 1}$ has the form

$$\frac{c_i b^n + c_{i-1}a^{(i-1)n} + \cdots + c_1 a^n + c_0}{(a^{n+i-1}-1)(a^{n+i-2}-1)\dots(a^n-1)}$$

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 other 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 in order to compute the difference, we just have to multiply the numerator $c_i b^n + c_{i-1} a^{(i-1)n} + \cdots + c_1 a^n + c_0$ by 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 $\lim\limits_{n\to\infty} x_n^{(i)} = 0$. So, $\lim\limits_{n\to\infty} x_n^{(k+1)} = 0$. Another step of the solution is to take the minimal index j such that $\lim\limits_{n\to\infty} x_n^{(j)} = 0$. Clearly, $j > 1$ and the recursive relation $x_n^{(i+1)} = bx_n^{(i)} - a^i x_{n+1}^{(i)}$ shows that $x_n^{(i)} \in \mathbf{Z}$ for all n and 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. Because $\left(\frac{b}{a^j}\right)^{n-M} x_M^{(j-1)} \in \mathbf{Z}$ 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 $\lim\limits_{n\to\infty} x_n^{(j)} = 0$. But this contradicts the minimality of j. Thus 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 we 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 is worth saying that an even stronger result holds: it is enough to suppose that $a^n - 1|b^n - 1$ for infinitely many n. But this is a much more difficult problem and it follows from a result found by Bugeaud, Corvaja and Zannier in 2003:

If $a, b > 1$ are multiplicatively independent in $\mathbf{Q}^*$ (that is $\log_a b \notin \mathbf{Q}$), 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 $f \in \mathbf{Z}[X]$ be a polynomial of degree k such that $\sqrt[k]{f(n)} \in \mathbf{Z}$ for all n. Prove that there exist integers a and b such that $f(x) = (ax + b)^k$.

2. Find all arithmetical sequences $(a_n)_{n\geq 1}$ of positive integers $(a_n)_{n\geq 1}$ such that $a_1 + a_2 + \cdots + a_n$ is a perfect square for all $n \geq 1$.

Laurentiu Panaitopol, Romanian Olympiad 1991

3. Let p be a polynomial with integer coefficients such that there exists a sequence of pairwise 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 a and b be positive integers such that for any 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

5. Let a and b be integers greater than 1. 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

6. Let b be an integer greater than 4 and define the number $x_n = \underbrace{11\dots1}_{n-1}\underbrace{22\dots2}_{n}5$ 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 2004 Shortlist

8. Find all triplets (a, b, c) of integers such that $a \cdot 2^n + b$ is a divisor of $c^n + 1$ for any positive integer n.

Gabriel Dospinescu, Mathematical Reflections

9. Suppose that a is a positive real number such that all numbers $1^a, 2^a, 3^a, \dots$ are integers. Then prove that a is also integer.

Putnam Competition

10. Find all complex polynomials f with the property: there exists an integer a greater than 1 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

11. Let f be a complex polynomial such that for all positive integers n, the equation $f(x) = n$ has at least a rational solution. Prove that f has degree at most 1.

Mathlinks Contest

12. Let A be a set of positive integers containing at least one number among any 2006 consecutive positive integers and let f a nonconstant polynomial with integer coefficients. Prove that for sufficiently large n there are at least $\sqrt{\ln \ln n}$ different prime numbers dividing the number $\prod_{\substack{1 \le k \le n \\ k \in A}} f(k)$.

Gabriel Dospinescu

13. Prove that in any increasing sequence $(a_n)_{n\geq 1}$ of positive integers satisfying $a_n < 100n$ for all n, one can find infinitely many terms containing at least 1986 consecutive 1.

Kvant

14. Prove that any infinite arithmetical sequence contains infinitely many terms that are not perfect powers.

15. Find all a, b, c such that $a \cdot 4^n + b \cdot 6^n + c \cdot 9^n$ is a perfect square for all sufficiently large n.

16. Let f and g be two real polynomials of degree two such that for any real number x, if $f(x)$ is integer, then so is $g(x)$. Prove that there are integers m, n such that $g(x) = mf(x) + n$ for all x.

Bulgarian Olympiad

19. Try to generalize the previous problem (this is for the die-hards!).

20. Find all pairs (a, b) of positive integers such that $an + b$ is triangular if and only if n is triangular.

After a Putnam Competition problem

21. Let $(a_n)_{n\geq 1}$ be an increasing sequence of positive integers such that $a_n | a_1 + a_2 + \cdots + a_{n-1}$ for all $n \geq 2002$. Prove that there exists n_0 such that $a_n = a_1 + a_2 + \cdots + a_{n-1}$ for all $n \geq n_0$.

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 $A = \{x^k |\ x \in B\}$.

23. 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 $a = b$.

Gabriel Dospinescu

Quadratic reciprocity

For an odd prime p, define the function $\left(\frac{a}{p}\right) : \mathbf{Z} \to \{-1, 1\}$ by $\left(\frac{a}{p}\right) = 1$ if the equation $x^2 = a$ has at least a solution in $\mathbf{Z}_p$ and $\left(\frac{a}{p}\right) = -1$, otherwise. In the first case, we say that a is a quadratic residue modulo p, otherwise we say that it is a quadratic non-residue modulo p. This function is called Legendre's symbol and plays a fundamental role in number theory. We will unfold some easy properties of Legendre's symbol first, in order to prove a highly nontrivial result, the famous Gauss's quadratic reciprocity law. 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 facts concerning quadratic residues in what follows. First, let us assume that $\left(\frac{a}{p}\right) = 1$ and let x be a solution to the equation $x^2 = a$ in $\mathbf{Z}_p$. Using Fermat's little 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 $\mathbf{Z}_p \setminus \{0\}$. This will enable us to conclude that quadratic residues are precisely the zeros of the polynomial $X^{\frac{p-1}{2}} - 1$ and also that non quadratic residues are exactly the zeros 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 $p - 1$ zeros in the field $\mathbf{Z}_p$. 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 $\mathbf{Z}_p$. These two observations show that in fact each of these polynomials has exactly $\frac{p-1}{2}$ zeros in $\mathbf{Z}_p$. 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 $\mathbf{Z}_p \setminus \{0\}$ 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 $\left(\frac{a}{p}\right) : \mathbf{Z} \to \{-1, 1\}$ is a group morphism.

Indeed,

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \pmod p = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

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 discuss Gauss's celebrated quadratic reciprocity law. First of all, we will prove a lemma (also due to Gauss).

Lemma. Let p be an odd prime and let $a \in \mathbf{Z}$ 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 $k = \frac{p-1}{2} - m$ and let $y_1, \ldots, y_k$ be all numbers less than $\frac{p}{2}$ and 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,

$$\prod_{x=1}^{\frac{p-1}{2}} (ax) = \prod_{ax \pmod p > \frac{p}{2}} (ax) \pmod p \cdot \prod_{ax \pmod p < \frac{p}{2}} (ax) \pmod p.$$

We clearly have

$$\prod_{ax \pmod p > \frac{p}{2}} (ax) \pmod p \cdot \prod_{ax \pmod p < \frac{p}{2}} (ax) \pmod p$$

$$= \prod_{i=1}^{m} ax_i \pmod p \cdot \prod_{j=1}^{k} ay_i \pmod p.$$

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

$$\prod_{i=1}^{m} ax_i \pmod p \cdot \prod_{j=1}^{k} ay_i \pmod p$$

$$= (-1)^m \prod_{i=1}^{m}(p - ax_i) \pmod p \cdot \prod_{j=1}^{k} ay_j \pmod p$$

$$\equiv (-1)^m \cdot \prod_{i=1}^{\frac{p-1}{2}} i \pmod p = (-1)^m \left(\frac{p-1}{2}\right)! \pmod p.$$

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 distinct 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. For the sake of contradiction, assume that p is a prime 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 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 $(-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}} = 1$. But 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 obtain the following result.

Example 2.[Gabriel Dospinescu] 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 assume $n > 2$ (otherwise the verification is trivial). The essential observation is the identity

$$2^{3^n} + 1 = (2+1)(2^2-2+1)(2^{2\cdot 3} - 2^3 + 1)\dots(2^{2\cdot 3^{n-1}} - 2^{3^{n-1}} + 1)$$

Now, we prove that for all $1 \le i < j \le n-1$, $gcd(2^{2\cdot 3^i} - 2^{3^i} + 1, 2^{2\cdot 3^j} - 2^{3^j} + 1) = 3$. 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 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 you 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 $1 \le i \le n-1$ has at least a prime divisor of the form $8k+3$ different from 3. From the previous remarks,it will follow that $2^{3^n}+1$ has at least $n-1$ distinct prime divisors of the form $8k+3$ and since it is also divisible by 3, the solution will be complete. Fix $i \in \{1, 2, \dots, n-1\}$ and observe that any prime factor of $2^{2\cdot 3^i} - 2^{3^i} + 1$ is also a prime factor of $2^{3^n}+1$. Thus, from the first remark, this factor must be of the forms $8k+1$ or $8k+3$. Because $v_3(2^{2\cdot 3^i} - 2^{3^i} + 1) = 1$, all prime divisors of $2^{2\cdot 3^i} - 2^{3^i} + 1$ except for 3 are of the form $8k+1$, so $2^{2\cdot 3^i} - 2^{3^i} + 1 \equiv 8 \pmod{8}$, 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 $8k+3$. The claim is proved and the conclusion follows.

At first glance, the following problem seems trivial. It is actually very tricky, because brute force takes us nowhere. Yet, in the framework of the above results, this should not be so difficult.

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 has been proved in the topic **Look at the exponent!** and is due to Schinzel). So let us search for even numbers. The first step is choosing $n = 2p$, for some prime number p. Unfortunately, this choice is ruled out by Fermat's little theorem. So let us try settig $n = 2pq$, 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 case analysis 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 done: 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 satisfied 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.[Gabriel Dospinescu] Let $f, g : \mathbf{Z}^+ \to \mathbf{Z}^+$ functions with the properties:
i) g is surjective;
ii) $2f(n)^2 = n^2 + g(n)^2$ for all positive integers n.
If, in addition, $|f(n) - n| \leq 2004\sqrt{n}$ for all n, prove that f has infinitely many fixed points.

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 clear 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 $2f(x_n)^2 = x_n^2 + p_n^2$, which can be rewritten as $2f(x_n)^2 \equiv x_n^2 \pmod{p_n}$. 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 $x_n = a_n p_n$ and $f(x_n) = b_n p_n$ 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 have

$$\frac{2004}{\sqrt{x_n}} \geq \left|\frac{f(x_n)}{x_n} - 1\right| = \left|\frac{b_n}{a_n} - 1\right|.$$

That is

$$\lim_{n\to\infty}\frac{\sqrt{a_n^2+1}}{a_n}=\sqrt{2}.$$

The last relation implies $\lim\limits_{n\to\infty} a_n = 1$. 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 the numbers that are quadratic residues modulo all sufficiently large prime numbers. Of course, perfect squares are such numbers, but how to prove that they are the only ones?

Example 5. Suppose that a is a nonsquare positive integer. Then $\left(\dfrac{a}{p}\right) = -1$ 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 $r_1, r_2, \dots, r_k$, each of them different from $q_1, q_2, \dots, q_n$. We will show that there is a prime p, different from $r_1, r_2, \dots, r_k$, such that $\left(\dfrac{a}{p}\right) = -1$. Let s be a quadratic non-residue modulo q_n.

Using the Chinese remainder theorem, we can find a positive integer b such that

$$\begin{cases} b \equiv 1 \pmod{r_i},\ 1 \leq i \leq k \\ b \equiv 1 \pmod{8}, \\ b \equiv 1 \pmod{q_i},\ 1 \leq i \leq n-1 \\ b \equiv s \pmod{q_n} \end{cases}$$

Now, write $b = p_1 \cdot p_2 \cdot \ldots \cdot p_m$, with p_i odd primes, not necessarily distinct. Using the quadratic reciprocity law, it follows 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 $i \in \{1, 2, \dots, n\}$. 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 $i \in \{1, 2, \dots, m\}$ such that $\left(\dfrac{a}{p_i}\right) = -1$. Because $b \equiv 1 \pmod{r_i}$, $1 \le i \le k$, we also have $p_i \in \{1, 2, \dots\} \setminus \{r_1, r_2, \dots, r_k\}$ and the claim is proved.

The only case left is $a = 2$. But this is very simple, since it suffices to use Dirichlet's theorem to find infinitely many primes p such that $\dfrac{p^2-1}{8}$ is odd.

As in other units, we will now focus on some special case. This time it is a problem almost trivial in the above framework and seemingly impossible to solve otherwise (we say this because there is a beautiful, but very difficult solution using analytical tools, which we will not present here).

Example 6.[Gabriel Dospinescu] Suppose that $a_1, a_2, \dots, a_{2004}$ 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 least number of such integers that must equal 0?

Mathlinks Contest

Solution. Suppose that $a_1, a_2, \dots, a_k$ 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 $\left(\dfrac{k}{p}\right) = 1$ for all sufficiently large primes p. This is not a difficult task. Indeed, consider a prime p, greater than any prime divisor of $a_1 a_2 \dots a_k$. 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 $\left(\dfrac{k}{p}\right) = 1$. Thus k is a perfect square. And now the problem becomes trivial, since we must find the greatest perfect square less 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. It is adapted after a problem given at the Saint Petersburg Olympiad.

Example 7. Suppose that $f \in \mathbf{Z}[X]$ is a second degree polynomial such that for any prime p there is 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 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 also be found in the following problem.

Example 8.[Calin Popescu] 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 quadratic nonresidues 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 used 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. We have

$$\sum_{i=1}^{\frac{p-1}{2}}(2i)^2\left(\frac{2i}{p}\right) = 4\left(\frac{2}{p}\right)\sum_{i=1}^{\frac{p-1}{2}} i^2\left(\frac{i}{p}\right).$$

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

$$\sum_{i=1}^{\frac{p-1}{2}}(2i)^2\left(\frac{2i}{p}\right) \equiv \pm 4 \pmod 8$$

(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.[J.L.Selfridge] Find all positive integers n such that $2^n-1|3^n-1$.

AMM

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 $12k \pm 1$ or $12k \pm 5$ 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. Clearly, 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 least 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 $x_{n+1} = 2x_n^2 - 1$, for $n \geq 1$. 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 and 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 and B, then $ab \pmod{p} \in A$;
iii) If $a \in A,\ b \in B$, then $ab \in B$.
Find all such subsets A and B.

India Olympiad

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$a$ and b 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 $\sum_{k=1}^{p-1} \left(\frac{f(k)}{p} \right)$, 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 all 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 using 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 $a_1, a_2, \dots, a_n \geq 0$ we have the inequality

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n}.$$

Solution. Let us suppose that $a_1 \leq a_2 \leq \cdots \leq a_n$ and let

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n},\ B = \sqrt[n]{a_1 a_2 \dots a_n}.$$

Of course, we can find an index $k \in \{1, 2, \dots, n-1\}$ 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 $a_1, a_2, \dots, a_n$ 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

$$\sqrt[k]{\frac{\displaystyle\int_a^b f^k(x)dx}{b-a}} \leq \sqrt[k+1]{\frac{\displaystyle\int_a^b f^{k+1}(x)dx}{b-a}}$$

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

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \frac{1 - a_i a_j}{1 + j} \geq 0.$$

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 $f : \mathbb{R} \to \mathbb{R}$, $f(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}$. Let us observe that

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \frac{a_i a_j}{i + j} = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n} \frac{a_j}{i + j} \right) = \sum_{i=1}^{n} a_i \int_0^1 x^i f(x) dx$$

$$= \int_0^1 \left(x f(x) \sum_{i=1}^{n} a_i x^{i-1} \right) dx = \int_0^1 x f^2(x) dx.$$

So, if we denote $M = \displaystyle\sum_{1 \leq i,j \leq n} \frac{1}{i + j}$, we infer that

$$\int_0^1 x f^2(x) dx \leq M.$$

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

$$\int_0^1 x f^2(x) dx \leq M.$$

Well, Cauchy-Schwarz inequality for integrals is the way to proceed. Indeed, we have

$$\left(\int_0^1 (x + x^2 + \cdots + x^n) f(x) dx \right)^2$$

$$= \left(\int_0^1 \sqrt{xf^2(x)}\sqrt{x(1+x+\cdots+x^{n-1})^2}dx\right)^2$$

$$= \int_0^1 xf^2(x)dx \int_0^1 (1+x+\cdots+x^{n-1})^2 dx \leq M^2.$$

This shows that $\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_i+a_j}{i+j} \leq 2M$ and now the conclusion easily follows: the maximal value is $2\displaystyle\sum_{1\leq i,j\leq n}\frac{1}{i+j}$, 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

$$\sum_{i=1}^{n} a_ib_i\leq\sum_{i=1}^{k} a_i.$$

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 $\sum\limits_{i=1}^{k} a_i$ as a sum of areas) and the rectangles $S_1, S_2, \ldots, S_n$, where the vertices of S_i are the points $\left(\sum\limits_{j=1}^{i-1} b_j, 0\right)$, $\left(\sum\limits_{j=1}^{i} b_j, 0\right)$, $\left(\sum\limits_{j=1}^{i-1} b_j, a_i\right)$, $\left(\sum\limits_{j=1}^{i} b_j, a_i\right)$ (where $\sum\limits_{j=1}^{0} b_j = 0$). 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 $\sum\limits_{j=1}^{n} b_j < k+1$ (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 $\sum\limits_{i=0}^{m} x_i$ and $\sum\limits_{j=0}^{m} y_j$ 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 $x_0, x_1, \dots, x_m$ and the rectangles with weight 1 and heights $y_0, y_1, \dots, y_n$. 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 $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \geq 0$ 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

$$\sum_{1\le i,j\le n}\min(a_i,a_j)+\sum_{1\le i,j\le n}\min(b_i,b_j)\ge 2\sum_{1\le i,j\le n}\min(a_i,b_j).$$

Now, remember that $2\min(x,y)=x+y-|x-y|$ and the last inequality becomes

$$\sum_{1\le i,j\le n}|a_i-a_j|+\sum_{1\le i,j\le n}|b_i-b_j|\le 2\sum_{1\le i,j\le n}|a_i-b_j|$$

and since

$$\sum_{1\le i,j\le n}|a_i-a_j|=2\sum_{1\le i<j\le n}|a_i-a_j|,$$

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 $a_1,a_2,\dots,a_n>0$ and let $x_1,x_2,\dots,x_n$ be real numbers such that

$$\sum_{i=1}^{n}a_ix_i=0.$$

a) Prove that the inequality $\displaystyle\sum_{1\le i<j\le n}x_ix_j|a_i-a_j|\le 0$ holds;

b) Prove that we have equality in the above inequality if and only if there exist a partition $A_1,A_2,\dots,A_k$ of the set $\{1,2,\dots,n\}$ such that for all $i\in\{1,2,\dots,k\}$ we have $\displaystyle\sum_{j\in A_i}x_j=0$ 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

$$\int_0^\infty f^2(x)dx=\sum_{1\le i,j\le n}x_ix_j\int_0^\infty\lambda_{[0,a_i]}(x)\lambda_{[0,a_a]}(x)dx$$

$$=\sum_{1\le i,j\le n}x_ix_j\min(a_i,a_j).$$

Hence

$$\sum_{1\le i,j\le n}x_ix_j\min(a_i,a_j)\ge 0.$$

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 $a_i \geq b_i$ and $a_j \geq b_j$, which leaves us with only two cases. The first one is when at least one of the two inequalities $a_i \geq b_i$ and $a_j \geq b_j$ 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

$$\sum_{1\leq i,j\leq n} \min(a_i b_j, a_j b_i) - \sum_{1\leq i,j\leq n} \min(a_i a_j, b_i b_j) = \sum_{i,j} x_i x_j \min(r_i, r_j) \geq 0,$$

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

$$\sum_{1\leq i,j\leq n} |1 - x_i x_j| = \sum_{1\leq i,j\leq n} |x_i - x_j|.$$

Prove that $\sum_{i=1}^{n} x_i = n$.

Gabriel Dospinescu

Solution. Consider $b_i = 1$ in the inequality from example 14. We obtain:

$$\sum_{1\leq i,j\leq n} \min(x_i, x_j) \geq \sum_{1\leq i,j\leq n} \min(1, x_i x_j).$$

Now, use the formula $\min(u, v) = \frac{u + v - |u - v|}{2}$ and rewrite the above inequality in the form

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

Taking into account that

$$\sum_{1\leq i,j\leq n} |1 - x_i x_j| = \sum_{1\leq i,j\leq n} |x_i - x_j|,$$

we finally obtain

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

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

$$f(x) = \log_2(1-x) + x + x^2 + x^4 + x^8 + \dots$$

is bounded.

Komal

9. Prove that for any real numbers $a_1, a_2, \dots, a_n$

$$\sum_{i,j=1}^{n} \frac{ij}{i+j-1} a_i a_j \geq \left(\sum_{i=1}^{n} a_i\right)^2.$$

10. Let $k \in \mathbb{N}$, $\alpha_1, \alpha_2, \dots, \alpha_{n+1} = \alpha_1$. 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 $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \geq 0$ 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 $x_i \leq \frac{1}{2}$ and define A', G' the corresponding means for $1 - x_i$. Prove that $\frac{A}{G} \geq \frac{A'}{G'}$.

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

$$\sum_{1 \leq i,j \leq n} \frac{1}{x_i + x_j} \geq \frac{n^2}{2}.$$

17. Prove that we can find a constant c such that for any $x \geq 1$ and any positive integer n we have

$$\left|\sum_{k=1}^{n} \frac{kx}{(k^2+x)^2} - \frac{1}{2}\right| \leq \frac{c}{x}.$$

IMC, 1996

18. Let $0 = x_1 < \cdots < x_{2n+1} = 1$ some real numbers. Prove that if $x_{i+1} - x_i \leq h$ for all $1 \leq i \leq 2n$ 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 $a_1, a_2, \ldots, a_n \geq 0$ we have the following inequality

$$\sum_{1 \leq i,j \leq n} \frac{a_i a_j}{i+j} \leq \pi \sum_{i=1}^{n} a_i^2.$$

Hilbert's inequality

Some useful irreducibility criteria

Example 1. Let $f(X) = a_0 + a_1X + ... + a_nX^n$ be a polynomial with integer coefficients such that a_0 is prime and $|a_0| > |a_1| + |a_2| + ... + |a_n|$. Prove that f is irreducible in $\mathbb{Z}[X]$.

Solution.

By the previous arguments, it is enough to prove that all zeros of f are outside the closed unit disk of the complex plane. But this is not difficult, because if z is a zero of f and if $|z| \leq 1$ then

$$|a_0| = |a_1z + a_2z^2 + ... + a_nz^n| \leq |a_1| + |a_2| + ... + |a_n|$$

, which contradicts the hypothesis of the problem. This solves the problem.

The previous example may look a bit artificial, but it is quite powerful for theoretic purposes. For example, it immediately implies a Goldbach theorem for polynomials with integer coefficients: any such polynomial can be written as the sum of two irreducible polynomials. Actually, it proves much more: for any polynomial f with integer coefficients there are infinitely many positive integers a such that $f + a$ is irreducible in $\mathbb{Z}[X]$.

We have already discussed about algebraic numbers and their properties. We will see that they play a fundamental role in proving the irreducibility of a polynomial. However, we will work with an extension of the notion of algebraic number: for any field $K \subset \mathbb{C}$, we say that the number $z \in \mathbb{C}$ is algebraic over K if there exists a polynomial $f \in K[X]$ such that $f(z) = 0$. Exactly the same arguments as those presented for algebraic numbers over $\mathbb{Q}$ allow to deduce the same properties of the minimal polynomial of an algebraic number over K. Also, if the minimal polynomial of the algebraic number α has degree n, the set $K(\alpha)$ of numbers of the form $g(\alpha)$ with $g \in K[X]$ is a field included in $mathbbC$. After this introduction, we will discuss a fundamental result that will be used in the next examples:

Example 2. Let K be a subfield of $\mathbb{C}$, p a prime number and $a \in K$. The polynomial $X^p - a$ is reducible in $K[X]$ if and only if there exists $b \in K$ such that $a = b^p$.

Solution.

One implication being obvious, let us concentrate on the more difficult part. Suppose that $X^p - a$ is reducible in $K[X]$ and consider α such that $\alpha^p = a$. Let f be the minimal polynomial of α over K and let $m = deg(f)$. Clearly $m < p$. Let $f(X) = (X - \alpha_1)(X - \alpha_2)...(X - \alpha_m)$ and introduce the numbers $r_1 = \alpha, r_i = \frac{\alpha_i}{\alpha}$ for $i \geq 2$. Because f divides $X^p - a$, we have $r_i^p = 1$. Hence $(-1)^m f(0) = c\alpha^m$ for some c, root of unity of order p. Since $m < p$, there exist integers u, v such that $um + vp = 1$. It follows that $(-1)^{um} f^u(0) = c^u\alpha^{1-vp}$. Combining this observation with the fact that $\alpha^p = a$, we deduce that $c^u\alpha = (-1)^{mu} f(0)^u a^v = b \in K$, thus $a = \alpha^p = b^p$. This finishes the proof of the hard part of the problem.

The following example turns out to be very efficient when studying the irreducibility of polynomials of the form $f(g(X))$, even though the proof is really elementary.

Example 3. Let K be a subfield of $\mathbb{C}$ and $f, g \in K[X]$. Let α be a complex root of f and assume that f is irreducible in $K[X]$ and $g(X) - \alpha$ is irreducible in $K(\alpha)[X]$. Then $f(g(X))$ is irreducible in $K[X]$.

Solution.
Define $h(X) = g(X) - \alpha$ and consider β a zero of the polynomial h. Because $f(g(\beta)) = f(\alpha) = 0$, β is algebraic over K. Let $deg(f) = n, deg(h) = m$ and s be the minimal polynomial of β over K. If we manage to prove that $deg(s) = mn$, then we are done, since s is irreducible over K and s divides $f(g(X))$, which has degree mn. So, let us suppose the contrary. By using a repeated division algorithm, we can write $s = r_{n-1}g^{n-1} + r_{n-2}g^{n-2} + ... + r_1 g + r_0$, where $deg(r_i) < m$. Hence $r_{n-1}(\beta)\alpha^{n-1} + ... + r_1(\beta)\alpha + r_0(\beta) = 0$. By grouping terms according to increasing powers of β, we deduce from the last relation an equation $k_{m-1}(\alpha)\beta^{m-1} + ... + k_1(\alpha)\beta + k_0(\alpha) = 0$. Here the polynomials k_i have coefficients in K and degree at most $n - 1$. Because h is irreducible in $K(\alpha)[X]$, the minimal polynomial of β over $K(\alpha)$ is h and thus it has degree m. Therefore the last relation implies $k_{m-1}(\alpha) = ... = k_1(\alpha) = k_0(\alpha) = 0$. Now, because f is irreducible in $K[X]$, the minimal polynomial of α has degree n and since $deg(k_i) < n$, we must have $k_{m-1} = ... = k_1 = k_0 = 0$. This shows that $r_{n-1} = ... = r_1 = r_0 = 0$ and thus $s = 0$, which is clearly a contradiction. This shows that s has degree mn, thus it is equal (up to a multiplicative constant) to $f(g(X))$ and this polynomial is irreducible.

Using the previous result, we obtain a generalization (and a more general statement) of two difficult problems given in Romanian TST:

Example 4.
Let f be a monic polynomial with integer coefficients and let p be a prime number. If f is irreducible in $\mathbb{Z}[X]$ and $\sqrt[p]{(-1)^{deg(f)}f(0)}$ is not rational, then $f(X^p)$ is also irreducible in $\mathbb{Z}[X]$.

Solution.
Consider α a complex zero of f and let $n = deg(f)$ and $g(X) = X^p$ and $h = g - \alpha$. By the previous result, it is enough to prove that h is irreducible in $\mathbb{Q}(\alpha)[X]$. Because $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{C}$, by a previous result it suffices to prove that α is not the p-th power of an element of $\mathbb{Q}(\alpha)$. Supposing the contrary, there exists $u \in \mathbb{Q}[X]$ of degree at most $n - 1$ such that $\alpha = u^p(\alpha)$. Let $\alpha_1, \alpha_2, ..., \alpha_n$ be the zeros of f. Because f is irreducible and α is one of its zeros, f is the minimal polynomial of α, so f must divide $u^p(X) - X$. Therefore $\alpha_1 \alpha_2 \cdot ... cdot \alpha_n = (u(\alpha_1) \cdot u(\alpha_2) \cdot ... \cdot u(\alpha_n))^p$. Finally, using the fundamental

theorem of symmetric polynomials, $uj(\alpha_1) \cdot u \cdot ... \cdot u(\alpha_n)$ is rational. Because $\alpha_1 \cdot \alpha_2 \cdot ... \cdot \alpha_n = (-1)^n f(0)$, it follows that $\sqrt[p]{(-1)^n f(0)} \in \mathbb{Q}$, a contradiction.

Sophie Germain's identity $m^4 + 4n^4 = (m^2 - 2mn + 2n^2)(m^2 + 2mn + 2n^2)$ shows that the polynomial $X^4 + 4a^4$ is reducible in $\mathbb{Z}[X]$ for all integers a. However, finding an irreducibility criterion for polynomials of the form $X^n + a$ is not an easy task. The following result, even though very particular, shows that this problem is not an easy one. Actually, there exists a general criterion, known as Capelli's criterion: for rational a and $m \geq 2$, the polynomial $X^m - a$ is irreducible in $\mathbb{Q}[X]$ if and only if $\sqrt[p]{a}$ is not rational for any prime p dividing m and also, if $4|m$, a is not of the form $-4b^4$ with b rational.

Example 5.

Let $n \geq 2$ be an integer and let K be a subfield of $\mathbb{C}$. If the polynomial $f(X) = X^{2^n} - a \in K[X]$ is reducible in $K[X]$, then either there exists $b \in K$ such that $a = b^2$ or there exists $c \in K$ such that $a = -4c^4$.

Solution.

Supposing the contrary, $X^2 - a$ is irreducible in $K[X]$. Let α be a zero of this polynomial. First, we will prove that $X^4 - a$ is irreducible in $K[X]$. Using the result in example 3, it is enough to prove that $X^2 - \alpha$ is irreducible in $K(\alpha)[X]$. If this is not true, then there are $u, v \in K$ such that $\alpha = (u + \alpha v)^2$, which can be also written as $v^2\alpha^2 + (2uv - 1)\alpha + u^2 = 0$. Because $\alpha^2 \in K$ and α is not in K, it follows that $2uv = 1$ and $u^2 + av^2 = 0$. Thus $a = -4u^4$ and we can take $c = u$, a contradiction. Therefore $X^2 - \alpha$ is irreducible in $K(\alpha)[X]$ and $X^4 - a$ is irreducible in $K[X]$. Now, we will prove by induction on n the following assertion: for any subfield K of $\mathbb{C}$ and any $a \in K$ not of the form b^2 or $-4c^4$ with $b, c \in K$, the polynomial $X^{2^n} - a$ is irreducible in $K[X]$. Assume it is true for $n - 1$ and take α a zero of $X^2 - a$. Let K^t be the set of x^t when $x \in K$. Then with the same argument as above one can prove that α does not belong to $-K^2(\alpha)$ (thus it is not in $-4K^4(\alpha)$) and it does not belong to $K^2(\alpha)$. Therefore $X^{2^{n-1}} - \alpha$ is irreducible over $K(\alpha)$. By applying once again the result of example 3, we deduce that $X^{2^n} - a$ is irreducible in $K[X]$. This finishes the inductive step and also the solution.

We continue with another example of how strong the criterion in example 3 is.

Example 6.

Prove that the polynomial $f(X) = (X^2 + 1^2)(X^2 + 2^2)...(X^2 + n^2) + 1$ is irreducible in $\mathbb{Z}[X]$ for all positive integers n.

Japan Olympiad 1999

Solution.

Consider the polynomial $g(x) = (X+1^2)(X+2^2)...(x+n^2)+1$. Let us prove first that this polynomial is irreducible in $\mathbb{Z}[X]$. Suppose that $g(X) = F(X)G(X)$ with $F, G \in \mathbb{Z}[X]$ are nonconstant. Then $F(-i^2)G(-i^2) = 1$ for any $1 \le i \le n$. Therefore $F(-i^2)$ and $G(-i^2)$ are equal to 1 or -1 and since their product is 1, we must have $F(-i^2) = G(-i^2)$ for all $1 \le i \le n$. This means that $F - G$ is divisible by $(X+1^2)(X+2^2)...(X+n^2)$ and because it has degree at most $n-1$, it must be the zero polynomial. Therefore $f = F^2$ and so $n!^2 + 1 = g(0)$ must be a perfect square. This is clearly impossible, so g is irreducible. All we have to do now is to apply the result in example 4.

Example 7.[Perron's criterion] Let $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ be a polynomial with integer coefficients. If $|a_{n-1}| > 1 + |a_0| + |a_1| + ... + |a_{n-2}|$ and $f(0) \neq 0$ then f is irreducible in $\mathbb{Q}[X]$.

Solution.

We will prove that f has exactly one zero outside the closed unit disk of the complex plane. This will show that f is irreducible in $\mathbb{Z}[X]$ and by Gauss's lemma it will also be irreducible in $\mathbb{Q}[X]$. It is quite clear that no zero of f is on the unit circle, because if z is such a zero, then

$$|a_{n-1}| = |a_{n-1}z^{n-1}| = |z^n + a_{n-2}z^{n-2} + ... + a_1z + a_0| \le 1 + |a_0| + ... + |a_{n-2}|$$

, contradiction. On the other hand, $|f(0)| \ge 1$, so by Viete's formula at least one zero of f lies outside the unit disk. Call this zero x_1 and let $x_2, ..., x_n$ be the other zeros of f. Let

$$g(x) = X^{n-1} + b_{n-2}X^{n-2} + ... + b_1X + b_0 = \frac{f(X)}{X - x_1}.$$

By identifying coefficients in the formula $f(X) = (X - x_1)g(X)$, we deduce that

$$a_{n-1} = b_{n-2} - x_1, a_{n-2} = b_{n-3} - b_{n-2}x_1, ..., a_1 = b_0 - b_1x_1, a_0 = -b_0x_1.$$

Therefore the hypothesis $|a_{n-1}| > 1 + |a_0| + |a_1| + ... + |a_{n-2}|$can be rewritten as

$$|b_{n-2} - x_1| > 1 + |b_{n-3} - b_{n-2}x_1| + ... + |b_0x_1|.$$

Taking into account that $|b_{n-2}| + |x_1| \ge |b_{n-2} - x_1|$ and

$$|b_{n-3} - b_{n-2}x_1| \ge |x_1||b_{n-2}| - |b_{n-3}|, ..., |b_0 - b_1x_1| \ge |b_1||x_1| - |b_0|,$$

we deduce that $|x_1| - 1 > (|x_1| - 1)(|b_0| + |b_1| + ... + |b_{n-2}|)$ and since $|x_1| > 1$, it follows that $|b_0| + |b_1| + ... + |b_{n-2}| < 1$. Using an argument based on the triangular inequality, similar to the one in the first part of the solution, we immediately infer that g has only zeros inside the unit disk, which shows that f has one zero outside the unit disk. This finishes the proof of this criterion.

Observe that this criterion instantaneously solve the following old IMO problem: the polynomial $X^n + 5X^{n-1} + 3$ is irreducible in $\mathbb{Q}[X]$, just because $5 > 4$!

Here are two nicer examples, where this criterion turns out to be extremely efficient. The solution of the first problem is due to Mikhail Leipnitski.

Example 7. Let $f_1, f_2, ..., f_n$ be polynomials with integer coefficients. Prove that there exists a reducible polynomial $g \in \mathbb{Z}[X]$ such that all polynomials $f_1 + g, f_2 + g, ..., f_n + g$ are irreducible in $\mathbb{Q}[X]$.

Iranian Olympiad

Solution.

Using Perron's criterion, it is clear that if M is sufficiently large and m is greater than $2 + max(deg(f_1), deg(f_2), ..., deg(f_n))$, the polynomials $X^{m+1} - MX^m + f_i(X)$ are all irreducible in $\mathbb{Q}[X]$. Therefore we can choose $g(X) = X^{m+1} - MX^m$.

Example 8.[Valentin Vornicu] Let $(f_n)_{n\geq 0}$ be the Fibonacci sequence, defined by $f_0 = f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$. Prove that for any $n \geq 3$ the polynomial $X^n + f_{n-1}f_nX^{n-1} + ... + f_1f_2X + f_0f_1$ is irreducible in $\mathbb{Q}[X]$.

Mathlinks Contest

Solution.

By Perron's criterion, it suffices to verify the inequality $f_nf_{n-1} > f_{n-1}f_{n-2} + ... + f_1f_0 + 1$ for all $n \geq 3$. For $n = 3$ it is obvious. Supposing the inequality true for n, we have $f_nf_{n-1} + f_{n-1}f_{n-2} + ... + f_1f_0 + 1 < f_nf_{n-1} + f_nf_{n-1} < f_{n+1}f_n$ because this is equivalent to $2f_{n-1} < f_{n+1} = f_n + f_{n-1}$ and this one is obvious. The inductive step is proved and so is the proof for $n \geq 3$.

A very efficient method for proving that a certain polynomial is irreducible is working modulo p for suitable prime numbers p. There are several criteria involving this idea and Eisenstein's criterion is probably the easiest to state and verify. It asserts that if $f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ is a polynomial with integer coefficients for which there exists a prime p such that p divides all coefficients except a_n and p^2 does not divide a_0 then f is irreducible in $\mathbb{Z}[X]$. The proof is not complicated. Suppose that $f = gh$ for some nonconstant integer polynomials g, h and look at this equality in the field $\mathbb{Z}_p$. Let f^* be the polynomial f reduced modulo p. We have $g^*h^* = a_nX^n$ (by convention, a_n will also denote $a_n(modp)$). This implies that $g^*(X) = bX^r$ and $h^*(X) = cX^{n-r}$ for some $0 \leq r \leq n$, with $bc = a_n$. Suppose for example that $r = 0$. Then $h(X) = cX^n + pu(X)$ for a certain polynomial with integer coefficients u. Because p does not divide a_n, it does not divide c and so $deg(h) \geq n$, contradiction. This shows that $r > 0$ and similarly $r < n$. Thus there exist polynomials u, v with integer coefficients such that $g(X) = bX^r + pu(X)$ and $h(X) = cX^{n-r} + pv(X)$. This shows that $a_0 = f(0) = p^2u(0)v(0)$ is a multiple of p^2, contradiction. The following example is more general than Eisenstein's criterion and even older!

Example 9.[Schonemann's criterion] Let $F = f^n + pg$ with $n \geq 1$ and f, g polynomials with integer coefficients. If there exists a prime number p such that $deg(f^n) > deg(g)$, f^* is irreducible in $\mathbb{Z}_p[X]$ and f^* does not divide g^*, then F is irreducible in $\mathbb{Z}[X]$.

Solution.

Suppose that $F = F_1 F_2$ is a nontrivial factorization. By passing in $\mathbb{Z}_p[X]$ we deduce that $F_1^* F_2^* = (f^*)^n$. From the hypothesis and this equality, it follows that there exist nonnegative integers u, v with $u + v = n$ and polynomials with integer coefficients g_1, g_2 such that $F_1 = f^u + pg_1$ and $F_2 = f^v + pg_2$, with $deg(g_1) < udeg(f)$ and $deg(g_2) < vdeg(f)$. From here we infer that $g = f^u g_2 + f^v g_1 + pg_1 g_2$. Because F_1 is not identical 1, we have $u > 0$ and $v > 0$. Let us assume that $u \leq v$. From the previous relation there exists a polynomial h with integer coefficients such that $g = f^u h + pg_1 g_2$. It is enough to pass again in $\mathbb{Z}_p[X]$ this last relation to deduce that f^* divides g^*, which contradicts the hypothesis. Therefore F is irreducible.

Before passing to the next example, observe two important consequences of Eisenstein's criterion. First of all, if p is a prime number, then $f(X) = 1 + X + X^2 + ... + X^{p-1}$ is irreducible in $\mathbb{Q}[X]$. This follows from Gauss's lemma and the observation that $f(X+1) = \frac{1}{X}((1+X)^p - 1)$ verifies the conditions of Eisenstein's criterion. Secondly, for any n there exists a polynomial of degree n which is irreducible in $\mathbb{Q}[X]$. Indeed, for $X^n - 2$ Eisenstein's criterion can be applied with $p = 2$ and Gauss's lemma allows to conclude.

Problems for training

1. Let f be a monic irreducible (in $\mathbb{Z}[X]$) polynomial with integer coefficients and suppose that there exists a positive integer m such that $f(X^m)$ is reducible in $\mathbb{Z}[X]$. Then for any prime p dividing $f(0)$ we have $v_p(f(0)) \geq 2$.

2. Let f be a monic polynomial in $K[X]$, where K is a subfield of $\mathbb{C}$. Suppose that $deg(f)$ is even and that for any prime divisor p of m, a does not belong to K^p. Then $f(X^m)$ is irreducible in $K[X]$.

3. Let $p_1, p_2, ..., p_n$ be distinct prime numbers. Prove that the polynomial

$$f(X) = \prod_{e_1, e_2, \ldots, e_n = \pm 1} (X + e_1\sqrt{p_1} + e_2\sqrt{p_2} + ... + e_n\sqrt{p_n})$$

is irreducible in $\mathbb{Z}[X]$.

4. Let $f(X) = 5X^9 + 6X^8 + 3X^6 + 8X^5 + 9X^3 + 6X^2 + 8X + 3$. Prove that $X^n f(X) + 12$ is reducible in $\mathbb{Z}[X]$ for any positive integer n.

Schinzel

5. Prove that for any positive integer n, the polynomial $(X^2+2)^n+5(X^{2n-1}+10X^n+5$ is irreducible in $\mathbb{Z}[X]$.

Laurentiu Panaitopol, Doru Stefanescu

6. Let p be an odd prime and $k > 1$. Prove that for any partition of the set of positive integers with k classes there exists a class and infinitely many polynomials of degree $p-1$ with all coefficients in that class and which are irreducible in $\mathbb{Z}[X]$.

Marian Andronache, Ion Savu, Unesco Contest 1995

7. Let f be an irreducible polynomial in $\mathbb{Q}[X]$ of degree p, where $p > 2$ is prime. Let $x_1, x_2, ..., x_p$ be the zeros of f. Prove that for any nonconstant polynomial g with rational coefficients, of degree smaller than p, the numbers $g(x_1), g(x_2), ..., g(x_p)$ are pairwise distinct.

Toma Albu, Romanian TST 1983

8. Find all positive integers n such that $X^n + 64$ is reducible in $\mathbb{Q}[X]$.

Bulgarian Olympiad

9. Let $a_1, a_2, ..., a_k$ be distinct integers. Prove that the polynomials $(X-a_1)^2(X-a_2)^2...(X-a_k)^2+1$ and $(X-a_1)^4(X-a_2)^4...(X-a_k)^4+1$ are irreducible in $\mathbb{Z}[X]$.

10. Let $f(X) = a_mX^m + a_{m-1}X^{m-1} + ... + a_1X + a_0$ be a polynomial of degree m in $\mathbb{Z}[X]$ and define $H = max_{0\leq i\leq m-1}|\frac{a_i}{a_m}|$. If $f(n)$ is prime for some integer $n \geq H+2$ then f is irreducible in $\mathbb{Z}[X]$.

AMM