November camp

by

Dominik Burek

Magic module

Example 1. Solve in integers the following equation

$$y^4 = x^3 + 7.$$

Proof. Consider all possible residues modulo 13. RHS leads to residues

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 \pmod{13}$	0	1	8	1	12	8	8	5	5	1	12	5	12
$x^3+7 \pmod{13}$	7	8	12	8	6	2	2	12	12	8	6	12	6

while LHS produces the following residues

y	0	1	2	3	4	5	6	7	8	9	10	11	12
$y^4 \pmod{13}$	0	1	3	3	9	1	9	9	1	9	3	3	1

Both sets of residues are disjoint thus the equation has not integer solutions. □

Example 2. Decide whether the equation $x^4 + y^3 = z! + 7$ has an infinite number of positive integer solutions.

Proof. We prove that for $z \geq 13$, the given equation has no integer solutions. Indeed, if $z \geq 13$ and $x^4 + y^3 = z! + 7$, then $x^4 + y^3 \equiv 7 \pmod{13}$. Consider all possible residues modulo 13 of $7 - x^4$ and y^3:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^4 \pmod{13}$	0	1	3	3	9	1	9	9	1	9	3	3	1
$7 - x^4$	7	6	4	4	11	6	11	11	6	11	4	4	6
y	0	1	2	3	4	5	6	7	8	9	10	11	12
$y^3 \pmod{13}$	0	1	8	1	12	8	8	5	5	1	12	5	12

From these tables we read that $x^4 + y^3 \not\equiv 7 \pmod{13}$.

Therefore the equation $x^4 + y^3 = z! + 7$ forces $z \leq 12$. Thus $x \leq x^4 \leq 12! + 7$ and $y \leq y^3 \leq 12! + 7$. It means that the number of solution is finite. □

The following theorem may be helpful in finding of "magic" modulo (like 13 in above cases).

Theorem 3. *Let $p > 2$ be a prime and k be a positive integer. Then the numbers*

$$1^k, 2^k, \ldots, (p-1)^k$$

give $\dfrac{p-1}{\gcd(p-1,k)}$ *different residues modulo p.*

Homework.

Problem 4. Solve in integers the following equation

$$x^5 = y^2 + 4.$$

Proof. We have $y^{10} \equiv 0, 1 \pmod{11}$; thus $y^5 \equiv -1, 0, 1 \pmod{11}$. Also, $x^2 \equiv 0, 1, 3, 4, 5, 9 \pmod{11}$; thus $x^2 + 4 \equiv 2, 4, 5, 7, 8, 9 \pmod{11}$. Hence $x^2 + 4$ and y^{10} are different mod 11. □

Problem 5. Solve in positive integers the following equation

$$2x^6 + y^7 = 11.$$

Proof. The possible residues of $x^6 \mod 43$ and $y^7 \mod 43$ are 1,21,41,11,16 and 1,42,37 respectively. □

Square between square

Example 6. Find all solutions of the following equation in integers

$$x^2 + x + 1 = y^2.$$

Proof. If $x > 0$, then

$$(x+1)^2 > x^2 + x + 1 > x^2.$$

Thus $x^2 + x + 1$ lies between squares, hence cannot be a perfect square.

If $x \leq -2$, then

$$x^2 > x^2 + x + 1 > (x+1)^2,$$

and again we get a contradiction.

It remains to check $x = 0, -1$, which lead to solutions

$$(x, y) = (0, 1), (0, -1), (-1, 1), (-1, -1).$$

□

Example 7. Find all solutions of the following equation in integers

$$x^4 + y = x^3 + y^2.$$

Proof. We see that

$$x^4 + y = x^3 + y^2 \implies x^4 - x^3 = y^2 - y \implies 4x^4 - 4x^3 + 1 = (2y-1)^2.$$

But, whenever $x \geq 2$ or $x \leq -2$, then

$$(2x^2 - x - 1)^2 < 4x^4 - 4x^3 + 1 < (2x^2 - x)^2.$$

Therefore $(2y-1)^2$ it lies between 2 consecutive squares and cannot – contradiction.

So, $x \in \{-1, 0, 1\}$, this gives the solutions

$$(x, y) = (0, 0), (0, 1), (1, 0), (1, 1), (-1, 2), (-1, -1).$$

□

Example 8. Find all positive integers (a, b) for which $a^3 + 6ab + 1$ and $b^3 + 6ab + 1$ are perfect cubes.

Proof. WLOG $a \leq b$, then

$$b^3 < b^3 + 6ab + 1 \leq b^3 + 6b^2 + 1 < b^3 + 6b^2 + 12b + 8 = (b+2)^3.$$

Since $b^3 + 6ab + 1$ is a perfect cube, we must have

$$b^3 + 6ab + 1 = (b+1)^3$$

or equivalently $2ab = b(b+1)$ i.e. $b = 2a - 1$.

It remains to check whether $a^3 + 6ab + 1$ is a cube if $b = 2a - 1$. Thus we need to find all integers a for which $a^3 + 12a^2 - 6a + 1$ is a cube. From the inequality

$$a^3 \leq a^3 + 6a^2 - 6a < a^3 + 12a^2 - 6a + 1 < a^3 + 12a^2 + 48a + 64 = (a+4)^3$$

we get that

$$a^3 + 12a^2 - 6a + 1 \in \{(a+1)^3, (a+2)^3, (a+3)^3\}$$

. Therefore we are left with three cases:

- $a^3 + 12a^2 - 6a + 1 = (a+1)^3$, then $9a^2 - 9a = 0$, so $a = 0$ or $a = 1$.
- $a^3 + 12a^2 - 6a + 1 = (a+2)^3$, then $6a^2 - 18a - 7 = 0$ – no solutions.
- $a^3 + 12a^2 - 6a + 1 = (a+3)^3$, then $3a^2 - 33a - 26 = 0$ – no solutions.

Finally $(a, b) = (1, 1)$ is the only pair satisfying given conditions. □

Example 9. Find all positive integers (k, m) for which $k^2 + 4m$ and $m^2 + 5k$ are perfect squares.

Proof. If $m \geq k$, then

$$(m+3)^2 = m^2 + 6m + 9 > m^2 + 5m \geq m^2 + 5k > m^2,$$

since $m^2 + 5k$ is a perfect square, it follows that $m^2 + 5k = (m+1)^2$ or $m^2 + 5k = (m+2)^2$.

If $m^2 + 5k = (m+1)^2 = m^2 + 2m + 1$, then $2m = 5k - 1$ and form problem condition $k^2 + 4m = k^2 + 2(5k-1) = k^2 + 10k - 2$ is a perfect square. But $k^2 + 10k - 2 < k^2 + 10k + 25 = (k+5)^2$, so

$$k^2 + 10k - 2 \leq (k+4)^2 = k^2 + 8k + 16.$$

Therefore $2k \leq 18$ and $k \leq 9$. Since $2m = 5k - 1$, k must be odd. Values of $k^2 + 10k - 2$ at $k = 1, 3, 5, 7, 9$ are equal 9, 37, 73, 117, 169, respectively. Thus only $k = 1$ and $k = 9$ provide squares. Respective values of $m = \frac{1}{2}(5k - 1)$ are equal 2 and 22.

If$m^2 + 5k = (m+2)^2 = m^2 + 4m + 4$, then $4m = 5k - 4$, so $k^2 + 4m = k^2 + 5k - 4$ is a perfect square. But

$$k^2 + 5k - 4 < k^2 + 6k + 9 = (k+3)^2,$$

hence $k^2 + 5k - 4 \leq (k+2)^2 = k^2 + 4k + 4$, which gives $k \leq 8$. Moreover $m = \frac{5}{4}k - 1$ is an integer, so $4 \mid k$. Again $k^2 + 5k - 4$ for $k = 4, 8$ equals 32, 100, respectively and only for $k = 8$ we get a square. Also $m = \frac{5}{4}k - 1 = 9$.

It remains to consider the case $m < k$. Then

$$(k+2)^2 = k^2 + 4k + 4 > k^2 + 4k > k^2 + 4m > k^2,$$

and so $k^2+4m=(k+1)^2=k^2+2k+1$, thus $2k=4m-1$ – contradiction since $2\nmid 4m-1$.

Finally $(k,m)=(1,1),(9,22),(8,9)$ are only pairs satisfying given conditions. □

Homework.

Problem 10. Prove that there are no positive integers a,b such that $2a^2+1$, $2b^2+1$, $2(ab)^2+1$ are all perfect squares.

Proof. Assume that such a,b exist. Clearly $a,b>1$ and WLOG $a\geq b$. Then

$$4(2a^2+1)(2(ab)^2+1)=(4a^2b+b)^2+8a^2-b^2+4$$

is a perfect square. But

$$(4a^2b+b)^2<(4a^2b+b)^2+8a^2-b^2+4<(4a^2b+b+1)^2=(4a^2b+b)^2+8a^2b+2b+1.$$

□

Problem 11. Find all integers $a>1$, $b>1$ such that $a\mid b+1$ and $b\mid a^3-1$.

Proof. Let $b=ka-1$ and $a^3-1=\ell b=\ell ka-\ell$, for some integers k and ℓ. Then $a\mid \ell-1$, so $\ell=ma+1$ for some integer m. Therfore

$$a^2-mka+m-k=0.$$

Now we see that

$$\Delta=m^2k^2-4m+4k.$$

- If $m<k$, then $(mk)^2<\Delta$. Moreover $\Delta<(mk+2)^2$ iff $(m-1)(k+1)>-2$. Thus if $m\neq 0$, then $(mk)^2<\Delta<(mk+2)^2$, so $\Delta=(mk+1)^2$. Hence $-4m+4k=2mk+1$, – impossible since both sides have different parity. Therefore $m=0$ and then $a=k^2$ and $b=ka-1=k^3-1$. Thus (s,s^3-1), where $s\geq 2$ is an integer satisfy problem.
- If $m>k$, then $\Delta<(mk)^2$ and $\Delta>(mk-2)^2$ iff $(m+1)(k-1)>0$. Therefore if $k\neq 1$, then $(mk-2)^2<\Delta<(mk)^2$, so $\Delta=(mk-1)^2$, i.e. $-4m+4k=-2mk+1$ and again we have contradiction because of parity. Therefore $k=1$ and then $a=m-1$ and $b=ka-1=a-1=m-2$. Therefore $(s,s-1)$, where $s\geq 3$ is an integer satisfy problem assumption.
- If $m=k$, then (s^2,s^3-1), where $s\geq 2$ satisfy problem.

□

Vieta jumping, descent and rational root theorem

Example 12. Solve in integers the following equation $x^2+y^2=3z^2$.

Proof. Consider nontrivial solution (x,y,z) with $|x|+|y|+|z|$ minimal. Since $3\mid x^2+y^2$ we see that $x=3x_1$, $y=3y_1$ for some x_1 and y_1 in $\mathbb{Z}$. Plugging this into the equation, we get $z^2=3(x_1^2+y_1^2)$, hence $z=3z_1$ for some $z_1\in\mathbb{Z}$. Observe that $x_1^2+y_1^2=3z_1^2$, therefore (x_1,y_1,z_1) is also solution of the given equation. Moreover

$$|x_1|+|y_1|+|z_1|=\frac{|x|+|y|+|z|}{3}<|x|+|y|+|z|,$$

contradiction. □

Example 13. Let $W(x)$ be a polynomial of integer coefficients such that for any pair of different rational number r_1, r_2 dependence $W(r_1) \neq W(r_2)$ is true. Decide, whether the assumptions imply that for any pair of different real numbers t_1, t_2 dependence $W(t_1) \neq W(t_2)$ is true.

Proof. Take $W(x) = x^3 - 2x$. Clearly, the second statement is not true, so it suffices to prove that the first is.

Assume for the sake of contradiction that $r^3 - 2r = s^3 - 2s$. Rearranging, we get $r^3 - s^3 = 2(r - s)$. Dividing by $(r - s)$, we get $r^2 + rs + s^2 = 2$.

Since r and s are rational, we write $r = \frac{a}{b}$ and $s = \frac{c}{d}$ in lowest terms. So our equation becomes $\frac{a^2}{b^2} + \frac{ac}{bd} + \frac{b^2}{d^2} = 2$, or

$$a^2d^2 + b^2c^2 + abcd = 2b^2d^2$$

Note that the equation implies that at least one of a or d is even and that at least one of b or c is even. If a was even, then c would have to be even as well (a and b are relatively prime). So b and d are odd. But that would mean that the LHS is divisible by 4 but the RHS is not, contradiction.

So we know d was even, which implies that b is even. So we let $d = 2d'$ and $b = 2b'$ So our equation is now

$$4(a^2d'^2 + b'^2c^2 + ab'cd') = 32b'^2d'^2$$

We divide by 4 to get

$$a^2d'^2 + b'^2c^2 + ab'cd' = 8b'^2d'^2$$

Since we know that a and c are odd, that implies that b' and d' are even. From here, we can use infinite descent to conclude that b and d have infinite powers of 2 in their prime factorization, which is a contradiction. □

Example 14. Let a, b be positive integers such that $ab+1$ divides a^2+b^2. Prove that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Proof. Consider the following equation with fixed positive integer k

$$\frac{a^2 + b^2}{ab + 1} = k. \tag{0-1}$$

Let $\mathcal{A}$ be a set of all pairs (a, b) of nonegative integers a and b such that (0-1) holds i.e.

$$\mathcal{A} = \left\{(a, b) \in \mathbb{N} \times \mathbb{N} \colon \frac{a^2 + b^2}{ab + 1} = k\right\}.$$

Suppose that k is not a perfect square.

Let $(a_0, b_0) \in \mathcal{A}$ be an element of $\mathcal{A}$ with a minimal sum $a_0 + b_0$ among all elements of $\mathcal{A}$. We may assume that $a_0 \geq b_0 > 0$.

The equations

$$\frac{x^2 + b_0^2}{xb_0 + 1} = k,$$

is equivalent to a quadratic equation in x

$$x^2 - kb_0x + b_0^2 - k = 0. \tag{0-2}$$

Note that $x_1 = a_0$ is a root of (0-2). From *Vieta's formulas* we get another root x_2 of (0-2) i.e.

$$x_2 = kb_0 - a_0 = \frac{b_0^2 - k}{a_0}.$$

From (0-2) follows that, x_2 is a nonzero integer $x_2 \neq 0$, (otherwise $k = b_0^2$ which contradicts to assumption about k.)

Moreover $x_2 > 0$. Indeed, if $x_2 < 0$ then

$$0 = x_2^2 - kb_0x_2 + b_0^2 - k \geq x_2^2 + k + b_0^2 - k > 0,$$

contradiction. Therefore $x_2 \geq 0$, hence $(x_2, b_0) \in \mathcal{A}$. By the formula (0-2) and inequality $a_0 \geq b_0$ we have

$$x_2 = \frac{b_0^2 - k}{a_0} \leq \frac{a_0^2 - k}{a_0} < a_0.$$

It means that $x_2 + b_0 < a_0 + b_0$which contradicts to minimality of $a_0 + b_0$. □

Example 15. Let a and b be positive integers, such that $4ab - 1$ divides $(4a^2 - 1)^2$. Prove that $a = b$.

Proof. Firstly, observe that

$$4ab - 1 | b^2(4a^2 - 1)^2 - (4ab - 1)(4a^3b - 2ab + a^2) = (a - b)^2.$$

Consider the following equation with fixed positive integer k

$$\frac{(a - b)^2}{4ab - 1} = k. \tag{0-3}$$

Let $\mathcal{A}$ be a set of all pairs (a, b) of nonegative integers a and b such that (0-1) holds i.e.

$$\mathcal{A} = \left\{(a, b) \in \mathbb{N} \times \mathbb{N} \colon \frac{(a - b)^2}{4ab - 1} = k\right\}.$$

Let $(a_0, b_0) \in \mathcal{A}$ be an element of $\mathcal{A}$ with a minimal sum $a_0 + b_0$ among all elements of $\mathcal{A}$. We may assume that $a_0 \geq b_0 > 0$.

The equations

$$\frac{(x + b_0)^2}{4xb_0 - 1} = k,$$

is equivalent to a quadratic equation in x

$$x^2 - (2b_0 + 4kb_0)x + b_0^2 + k = 0. \tag{0-4}$$

Note that $x_1 = a_0$ is a root of (0-2). From *Vieta's formulas* we get another root x_2 of (0-4) i.e.

$$x_2 = 2b_0 + 4kb_0 - a_0 = \frac{b_0^2 + k}{a_0}. \tag{0-5}$$

From (0-5) follows that, x_2 is a positive integer, hence $(x_2, b_0) \in \mathcal{A}$.

Now we have the following inequality

$$k = \frac{(a_0 - b_0)^2}{4a_0b_0 - 1} \leq \frac{(a_0 - b_0)(a_0 + b_0)}{4a_0b_0 - 1} = \frac{(a_0^2 - b_0^2)}{4a_0b_0 - 1} < a_0^2 - b_0^2.$$

Therefore

$$x_2 = \frac{b_0^2 + k}{a_0} \leq \frac{b_0^2 + (a_0^2 - b_0^2)}{a_0} = a_0,$$

which means that $x_2 + b_0 < a_0 + b_0$ – contradiction. Thus $a_0 = b_0$ and $k = 0$ i.e. $a = b$. □

Example 16. Let $n \geq 2$ be an integer such that the equation
$$x_1^2 + x_2^2 + \ldots + x_n^2 = x_1 x_2 \ldots x_n$$
has at least one solution in positive integers. Prove that this equation has infinitely many solutions in positive integers.

Proof. Let $a_1 = \min\{x_1, x_2, \ldots, x_n\}$. Given equation may be considered as a quadratic equation in t :
$$t^2 + x_2^2 + \ldots + x_n^2 = t x_2 \ldots x_n.$$
This equation has a root $t_1 = x_1$ and from Vieta's formulas we derive another root $t_2 = x_2 \ldots x_n - x_1$. Therefore n-tuple
$$(x_2 \ldots x_n - x_1, x_2, \ldots, x_n)$$
satisfies given equation.

Now we prove that new n-tuple has greater sum. Indeed, it is equivalent to the inequality $x_2 \ldots x_n > 2x_1$. Suppose that it does not hold. Then $2x_1 \geq x_2 \ldots x_n \geq x_1^{n-1}$, so $2 \geq x_1^{n-2}$. Thus $n = 2$ or $x_1 = 1$ or $n = 3$ and $x_1 = 2 = x_2 = x_3$.

In the first case we have an equation $x_1^2 + x_2^2 = x_1 x_2$ which has not even real roots. In the second one, $x_2 \ldots x_n \leq 2x_1 = 2$, thus n-tuple $(x_1, x_2, \ldots, x_n)$ consists of all one's or $n - 1$ one's except one 2. These sequences does not satisfy given equation.

The last case cannot hold because $(2, 2, 2)$ does not satisfy equation $x_1^2 + x_2^2 + x_3^2 = x_1 x_2 x_3$.

□

Homework.

Problem 17. Prove that the equation
$$6(6a^2 + 3b^2 + c^2) = 5n^2$$
has no solutions in integers except $a = b = c = n = 0$.

Proof. Suppose that there is nontrivial solution. The RHS is divisible by 3, so 3 must divide n i.e. $n = 3m$ for some integer m. Moreover $9 \mid 5n^2 - 36a^2 - 18b^2$ so $c = 3d$, for some integer d. We can now divide out the factor 9 to get
$$5m^2 = 4a^2 + 2b^2 + 6d^2.$$
Now take m, a, b, d to be the solution with the smallest sum and consider residues (mod 16).

Observe that perfect squares gives residues 0, 1, 4, or 9 (mod 16). Clearly m is even so $5m^2 = 0, 4 \pmod{16}$. Similarly, $4a^2 = 0, 4 \pmod{16}$. Hence $2b^2 + 6d^2 = 0, 4, 12 \pmod{16}$. But $2b^2 = 0, 2, 8 \pmod{16}$ and $6d^2 = 0, 6, 8 \pmod{16}$. Therfore
$$2b^2 + 6d^2 = 0, 2, 6, 8, 10, 14 \pmod{16}.$$
So it must be $0 \pmod{16}$. Thus b and d are both even. But a cannot be even, otherwise $\frac{m}{2}; \frac{a}{2}; \frac{b}{2}; \frac{c}{2}$ would be a solution – contradiction.

So we can divide out the factor 4 and get
$$5k^2 = a^2 + 2e^2 + 6f^2$$
for some integers k, e, f with a odd. Hence k is also odd. So $5k^2 - a^2 = 4, 12 \pmod{16}$. But we have just seen that $2e^2 + 6f^2$ cannot be 4 or 12 (mod 16). So there are no solutions. □

Problem 18. Let x, y be integers different -1 such that

$$\frac{x^4-1}{y+1}+\frac{y^4-1}{x+1}\in\mathbb{Z}.$$

Prove that $x+1 \mid x^4y^{44}-1$.

Proof. Let $a=\frac{x^4-1}{y+1}$ and $b=\frac{y^4-1}{x+1}$. By assumption $a,b\in\mathbb{Q}$ and $a+b, ab\in\mathbb{Z}$. Thus

$$(X-a)(X-b)=X^2-(a+b)X+ab\in\mathbb{Z}[X],$$

so $a,b\in\mathbb{Z}$. Therefore $x+1 \mid y^4-1$, then clearly $x+1 \mid y^{44}-1$. Since $x^4\equiv 1 \pmod{x+1}$, the result follows. □

Problem 19. Find all positive integers a, b, c such that $\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$ and $\frac{b}{a}+\frac{c}{b}+\frac{a}{c}$ are both integers.

Proof. Notice that $\frac{a}{b}, \frac{b}{c}, \frac{c}{a}$ are rational roots of polynomial

$$X^3-\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{a}\right)X^2+\left(\frac{b}{a}+\frac{c}{b}+\frac{a}{c}\right)X-1=\left(X-\frac{a}{b}\right)\left(X-\frac{b}{c}\right)\left(X-\frac{c}{a}\right),$$

so they are integers. Since their product equals 1, then $a=b=c$. □

Problem 20. Suppose that a, b are two odd positive integers such that $2ab+1 \mid a^2+b^2+1$. Prove that $a=b$.

Proof. Note that $2ab+1 \mid a^2+b^2+1$ implies that $2ab+1 \mid (a-b)^2$.

Now consider the positive integer solution set (a,b) of the equation

$$\frac{(a-b)^2}{2ab+1}=k$$

where k is a fixed positive integer. Let (a_0,b_0) be a solution for which the sum is minimal. Without loss of generality let $a_0>b_0$. Now we consider another equation

$$\frac{(x-b_0)^2}{2xb_0+1}=k \Longleftrightarrow x^2-2xb_0(k+1)+{b_0}^2-k=0.$$

Obviously one of the roots is a_0. The other root $\alpha_0=2b_0(k+1)-a_0$ is a positive integer. We also have that $\alpha_0=\frac{{b_0}^2-k}{a_0}$. But

$$\frac{{b_0}^2-k}{a_0}<\frac{{b_0}^2}{a_0}<a_0 \Longrightarrow a_0+b_0>a_0+\alpha_0$$

– contradiction to our assumption. Therefore $a_0=b_0$, so $k=0$ i.e. $a=b$. □

Example 21. Positive rational number a and b satisfy the equality

$$a^3+4a^2b=4a^2+b^4.$$

Prove that the number $\sqrt{a}-1$ is a square of a rational number.

Proof. Note that

$$a(a+2b)^2 = a^3 + 4a^2b + 4ab^2 = 4a^2 + b^4 + 4ab^2 = (2a+b^2)^2,$$

thus

$$a = \frac{(2a+b^2)^2}{(a+2b)^2} \quad \text{and} \quad \sqrt{a} = \frac{2a+b^2}{a+2b}.$$

Therefore $\sqrt{a} \in \mathbb{Q}$. Moreover $x = b$ is a root of quadratic equation

$$x^2 - 2\sqrt{a}x + 2a - a\sqrt{a} = 0.$$

Simultanously coefficients of these equation are rational, hence its discriminant too. Thus

$$\Delta = (2\sqrt{a})^2 - 4(2a - a\sqrt{a}) = 4a(\sqrt{a} - 1)$$

is a perfect square, in particular

$$\frac{\Delta}{(2\sqrt{a})^2} = \sqrt{a} - 1$$

is a perfect square, too.

□

Proof. As in the above solution we have that $\sqrt{a} \in \mathbb{Q}$. Let $c := \sqrt{a}$, then our equality becomes $c^6 + 4c^4b = 4c^4 + b^4$. Hence

$$c^2 + 4b = 4 + \left(\frac{b}{c}\right)^4 = \left(\left(\frac{b}{c}\right)^2 + 2\right)^2 - 4 \cdot \frac{b^2}{c^2},$$

so

$$\left(\frac{2b}{c} + c\right)^2 = c^2 + 4 \cdot \frac{b^2}{c^2} + 4b = \left(\left(\frac{b}{c}\right)^2 + 2\right)^2,$$

thus

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

i.e.

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

□

Proof. As in the previous solutions we get that

$$\sqrt{a} = \frac{(2a+b^2)^2}{(a+2b)},$$

so we are left with proving that

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

is a square of a rational number. Since a is a perfect square of some rational, it is enaugh to prove that $a(b^2 - 2b + a)(a+2b)$ a square of a rational number. But

$$\begin{aligned} a(b^2 - 2b + a)(a+2b) &= a^2b^2 + a^3 + 2b^3a - 4b^2a = \\ &= a^2b^2 + 4a^2 + b^4 + 2b^3a - 4a^2b - 4b^2a = (2a - b^2 - ab)^2. \end{aligned}$$

□

Fact 22. *Let a, b be integers, then there exists integers x, y such that*

$$ax + by = \gcd(a, b).$$

Fact 23 ($\mathbb{Z}/p\mathbb{Z}$ is a field)**.** *Any number $a \in \{1, 2, \ldots, p-1\}$ has an inverse, where p is a prime.*

Theorem 24 (Little Fermat's Theorem)**.** *For any integer a and prime p the following holds*

$$a^p \equiv a \pmod{p}.$$

Theorem 25 (Euler Theorem)**.** *For any integers a and n such that $\gcd(a, n) = 1$ the following holds*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Theorem 26 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_k$ be integers pairwise coprime and let $a_1, a_2, \ldots, a_k$ be an arbitrary integers, then the system of congruences*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has exactly one solution modulo $n_1 n_2 \ldots n_k$.

1.1. Problems.

Example 27. Prove that if $p \mid a^p - b^p$, then $p^2 \mid a^p - b^p$, where a, b are positive integers and p is a prime.

Proof. From *Little Fermat's Theorem* $a^p \equiv a \pmod{p}$ and $b^p \equiv b \pmod{p}$, thus $a \equiv b \pmod{p}$. Therefore

$$a^{p-1} + a^{p-2}b + \ldots + b^{p-1} \equiv a^{p-1} + a^{p-1} + \ldots + a^{p-1} \equiv pa^{p-1} \equiv 0 \pmod{p},$$

so

$$a^p - b^p = (a - b)(a^{p-1} + a^{p-2}b + \ldots + b^{p-1})$$

is divisible by p^2. □

Example 28. Let a, b be integers such $p \mid a^2 + b^2$, where p is a prime of the form $4k + 3$. Prove that $p \mid a$ and $p \mid b$.

Proof. Suppose that $p \nmid a$, then $p \nmid b$ too. Assume $a^2 \equiv -b^2 \pmod{p}$. Taking $\frac{p-1}{2}$ power of both sides we get

$$a^{p-1} \equiv -b^{p-1} \pmod{p} \quad \text{(here we used the fact that } \frac{p-1}{2} \text{ is an odd number).}$$

But from the *Little Fermat's Theorem* we get that

$$1 \equiv a^{p-1} \equiv -b^{p-1} \equiv -1 \pmod{p},$$

contradiction, since $p > 2$. □

Example 29. Let a, b be a positive integers such that $\gcd(a, b) = 1$. Prove that there exists m, n such that $a^m + b^n \equiv 1 \pmod{ab}$.

Proof. Take $m = \phi(b)$ and $n = \phi(a)$ and use *Euler Theorem* . □

Example 30. Prove that for $n \geq 3$

$$1989 \mid n^{n^{n^n}} - n^{n^n}.$$

Proof. Observe that if $\gcd(n, m) = 1$, then the congruence $n^{n^{n^n}} \equiv n^{n^n} \pmod{m}$ is equivalent to $n^{n^{n^n} - n^n} \equiv 1 \pmod{m}$, which is implying by divisibility $\phi(m) \mid n^{n^n} - n^n$ (*Euler Theorem*).

Since $1989 = 3^2 \cdot 13 \cdot 17$ we need to prove the following divisibilities:

- by 9: if $3 \mid n$ then it is obvious. Suppose that $3 \nmid n$, then we need to show that $6 \mid n^{n^n} - n^n$. But it follows from parity and the fact that $n^2 \equiv 1 \pmod{3}$.
- by 13: if $13 \mid n$ then it is obvious. Suppose that $13 \nmid n$. We show that $12 \mid n^{n^n} - n^n$. For even n divisibility by 4 is clear. Now for odd n we use $n^2 \equiv 1 \pmod{4}$. Divisibility by 3 was done in previous point.
- by 17: for $17 \mid n$ clear. If $17 \nmid n$ then we prove that $n^{n^n} \equiv n^n \pmod{16}$. Indeed it is clear for even n because $n \geq 4$. For odd n we use $n^2 \equiv 1 \pmod{8}$ to get that $n^n \equiv n \pmod{8}$.

□

Example 31. Prove that if $p = 3k + 2$ is a prime, then $1^3, 2^3, \ldots, (p-1)^3$ are distinct modulo p.

Proof. Suppose that $a^3 \equiv b^3 \pmod{p}$ for some $a, b \in \{1, 2, \ldots, p-1\}$. Taking $\frac{p-2}{3}$ power of both sides we get that $a^{p-2} \equiv b^{p-2} \pmod{p}$, hence $a^{p-1}b \equiv b^{p-1}a \pmod{p}$. From the *Little Fermat's Theorem* follows that $b \equiv a \pmod{p}$, which is impossible. □

Example 32. Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, \quad \text{for } n \geq 1.$$

Proof. Take any prime $p > 3$. Then from *Little Fermat's Theorem* we get

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0 \pmod{p}.$$

For $n = 2$ we have $a_n = 48$ which is divisible by 6. □

Example 33. Prove that for any prime $p \geq 3$ the following divisibility holds

$$p \mid \underbrace{11\ldots1}_{p}\underbrace{22\ldots2}_{p}\ldots\underbrace{99\ldots9}_{p} - 123456789.$$

Proof. Observe that $\underbrace{11\ldots1}_{n} = \frac{10^n-1}{9}$, thus

$$9\left(\underbrace{11\ldots1}_{p}\underbrace{22\ldots2}_{p}\ldots\underbrace{99\ldots9}_{p} - 123456789\right) =$$

$$= 9\left(\underbrace{11\ldots1}_{9p} + \underbrace{11\ldots1}_{8p} + \ldots + \underbrace{11\ldots1}_{p} - \underbrace{11\ldots1}_{9} - \underbrace{11\ldots1}_{8} - \ldots - 1\right) =$$

$$= 10^{9p} + 10^{8p} + \ldots + 10^p - 10^9 - 10^8 - \ldots - 10,$$

which is divisible by p from *Little Fermat's Theorem* , because $10^{kp} \equiv 10^k \pmod{p}$ for $k = 1, 2, \ldots, 9$. □

Example 34. Suppose that p is an odd prime such that $2p+1$ is also prime. Show that the equation $x^p + 2y^p + 5z^p = 0$ has no solutions in integers other than $(0, 0, 0)$.

Proof. We will prove that it doesn't have any others. From the *Little Fermat's Theorem* :

$$2p + 1 \mid a^{2p+1} - a = a(a^p - 1)(a^p + 1)$$

so for every integer a we have $a^p \equiv 0$ or 1 or $-1 \bmod p$. By verifying manually all cases we can see that the only possibility is $p = 3$ (since $x^p + 2y^p + 5z^p \equiv 0 \bmod 2p + 1$). Alternatively we can observe that $x^p + 2y^p + 5z^p$ gives residue not gretaer then 8 modulo $2p + 1$, so only 5 and 7 are possible.

So we are left with proving that the equation $x^3 + 2y^3 + 5z^3 = 0$ has no solutions in integers. To do this consider this equation modulo 9. One can easily check that we must have $x \equiv y \equiv z \equiv 0 \pmod 3$ but in this case just divide by 27 and repeat the process. It will terminate unless $x = y = z = 0$. □

Example 35. Prove that there exist 2018 consecutive integers which are divisible by a square of some integer greater then 1.

Proof. From the *Chinese Remainder Theorem* there exists n such that

$$\begin{cases} n \equiv 0 & \pmod{p_1^2} \\ n \equiv -1 & \pmod{p_2^2} \\ \vdots & \\ n \equiv -2018 & \pmod{p_{2018}^2}. \end{cases}$$

□

Example 36. Prove that there exist 2018 consecutive integers which are not perfect powers.

Proof. From the *Chinese Remainder Theorem* there exists n such that

$$\begin{cases} n \equiv p_1 & (\text{mod } p_1^2) \\ n \equiv -1 + p_2 & (\text{mod } p_2^2) \\ \vdots & \\ n \equiv -2017 + p_{2018} & (\text{mod } p_{2018}^2). \end{cases}$$

□

Example 37. We call a positive integer n *nice* if there exist positive integers a, b, c such that the equality

$$n = \gcd(b,c)\gcd(a,bc) + \gcd(c,a)\gcd(b,ca) + \gcd(a,b)\gcd(c,ab)$$

holds. Prove that there exist 2018 consecutive positive integers which are *nice*.

Proof. We may choose such positive integers $x_1, x_2, \ldots, x_{2018}$ that the numbers

$$y_1 = x_1^2(x_1+2), y_2 = x_2^2(x_2+2), \ldots, y_{2018} = x_{2018}^2(x_{2018}+2)$$

are pairwise coprime. For example, we may choose $x_1 = 1$ and $x_i = y_1 y_2 \ldots y_{i-1} - 1$ for every consecutive i. This choice guarantees that for every integer $2 \leq i \leq 2018$ both x_i and $x_i + 2$ (hence, y_i as well) are coprime with any of the numbers $y_1, y_2, \ldots, y_{i-1}$.

If a positive integer n is divisible by any of the numbers $y_1, y_2, \ldots, y_{2018}$ then it is nice. Indeed, if, say, $n = y_i m = x_i^2(x_i+2)m$ for some positive integers m and $1 \leq i \leq 2018$ then

$$n = \gcd(b,c)\gcd(a,bc) + \gcd(c,a)\gcd(b,ca) + \gcd(a,b)\gcd(c,ab)$$

for $a = mx_i^2,\ b = mx_i,\ c = x_i$.

Since the numbers $y_1, y_2, \ldots, y_{2018}$ are pairwise coprime, the *Chinese Remainder Theorem* implies that there exists a positive integer k satisfying the equalities

$$k \equiv -i \pmod{y_i}, \quad \text{for } i = 1, 2, \ldots, 2015.$$

This means that $k+i$ is divisible by y_i for any $1 \leq i \leq 2018$. Thus, the consecutive positive integers $k+1, k+2, \ldots, k+2018$ are all nice, and the statement of the problem is proved. □

2. Quadratic residues

Definicja 38. For an integer a and prime p such that $\gcd(a,p) = 1$, we say that a is a *quadratic residue* if $a \equiv x^2 \pmod{p}$ for some x. Otherwise x is to be *nonquadratic residue*.

Put

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if a is quadratic residue} \\ -1 & \text{if a is not a quadratic residue} \\ 0 & \text{if } p \mid a \end{cases}$$

which is called Legandre's symbol of $a \pmod{p}$.

Fact 39. *Assume that a, b are integers coprime with p. The following are true*

- *There exists exactly $\frac{p-1}{2}$ quadratic residues among $1, 2, \ldots, p-1$*
- $\left(\frac{a^2}{p}\right) = 1$
- $\left(\frac{a}{p}\right) = \left(\frac{a \pmod p}{p}\right)$
- $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Theorem 40. *Let $p, q > 2$ be a distinct primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

2.1. Some problems.

Example 41. Let p be a prime number. Prove that there exists $x \in \mathbb{Z}$ for which $p \mid x^2 - x + 3$ if and only if there exists $y \in \mathbb{Z}$ for which $p \mid y^2 - y + 25$.

Proof. The statement is trivial for $p \leq 3$, so we can assume that $p \geq 5$. Since $p \mid x^2 - x + 3$ is equivalent to

$$p \mid 4(x^2 - x + 3) = (2x - 1)^2 + 11,$$

integer x exists if and only if 11 is a quadratic residue modulo p. Likewise, since

$$4(y^2 - y + 25) = (2y - 1)^2 + 99,$$

y exists if and only if 99 is a quadratic residue modulo p. Now the statement of the problem follows from

$$\left(\frac{-11}{p}\right) = \left(\frac{-11 \cdot 3^2}{p}\right) = \left(\frac{-99}{p}\right).$$

□

Example 42. There are given integers a and b such that a is different from 0 and the number $3 + a + b^2$ is divisible by $6a$. Prove that a is negative.

Proof. Suppose that $b^2 + 3 = ak$, where $6 \mid k + 1$. We claim that k is negative. If not, then k has a prime divisor p of the form $6\ell + 5$. But $p \mid b^2 + 3$, hence $\left(\frac{-3}{p}\right) = 1$ – contradiction. □

Example 43. Let c be an integer which is not perfect square. Then, there exists prime $p > 2$ such that $\left(\frac{c}{p}\right) = -1$.

Proof. WLOG assume that c is squarefree i.e. $c = p_1 p_2 \dots p_n$, where $p_1 < p_2 < \dots < p_n$ are primes. Consider two cases:

- p_1 is odd. Let $r_1, r_2, \dots, r_n$ be such that $\left(\frac{r_1}{p_1}\right) = -1$ and $\left(\frac{r_i}{p_i}\right) = 1$ for $2 \le i \le n$. Form *Chinese Remainder Theorem* and *Dirichlet's Theorem* we find prime p such that

$$\begin{cases} p \equiv r_1 \pmod{p_i} \\ p \equiv r_2 \pmod{p_2} \\ \dots \\ p \equiv r_n \pmod{p_n} \\ p \equiv 1 \pmod{4}. \end{cases}$$

  Observe that

$$\left(\frac{p}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = \begin{cases} -1 & \text{where } i = 1, \\ 1 & \text{where } 2 \le i \le n. \end{cases}$$

  Since $p \equiv 1 \pmod 4$, then from the *Gauss Theorem* we now that $\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right)$, so

$$\left(\frac{c}{p}\right) = \left(\frac{p_1}{p}\right) \cdot \left(\frac{p_2}{p}\right) \cdot \dots \cdot \left(\frac{p_n}{p}\right) = -1.$$

- $p_1 = 2$. Let $r_2, \dots, r_n$ be such that $\left(\frac{r_i}{p_i}\right) = 1$ for $2 \le i \le n$. Using again the *Chinese Remainder Theorem* and *Dirichlet's Theorem* we find prime p for which

$$\begin{cases} p \equiv r_2 \pmod{p_2} \\ p \equiv r_3 \pmod{p_3} \\ \dots \\ p \equiv r_n \pmod{p_n} \\ p \equiv 5 \pmod{8}. \end{cases}$$

  Therefore

$$\left(\frac{p}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = 1$$

  for $2 \le i \le n$. Since $p \equiv 1 \pmod 4$ we know that $\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right)$. But $p \equiv 5 \pmod 8$ implies that $\left(\frac{2}{p}\right) = -1$. Hance

$$\left(\frac{c}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{p_2}{p}\right) \cdot \dots \cdot \left(\frac{p_n}{p}\right) = -1.$$

□

3. For infinity naturals

In many problems with assumptions holding for infinity many naturals, the good strategy is to find special (tricky) natural number which fits to the problem statement and derives contradiction. Also limit argument (some basic analysis) is allowed and often kills problem.

Example 44. Let $a, b \in \mathbb{N}$ be naturals such that for any $n \in \mathbb{N}$ divisibility $a^n + n \mid b^n + n$ holds. Show that $a = b$.

Proof. Suppose that $a \neq b$. Consider prime p which does not divide $a - b$. From *Chinese Remainder Theorem* there exists natural n satisfying

$$\begin{cases} n \equiv 1 & (\mathrm{mod}\ p-1) \\ n \equiv -a & (\mathrm{mod}\ p). \end{cases}$$

Then from *Little Fermat's Theorem*

$$a^n + n \equiv a + n \equiv 0 \pmod{p} \text{ oraz } b^n + n \equiv b + n \equiv b - a \pmod{p},$$

so $p \mid a^n + n$ and $p \nmid b^n + n$, which is contradiction with problem assumption. □

Sometimes we don't need such a tricky n.

Example 45. Let a be a positive integer such that $4(a^n + 1)$ is cube of some integral for any natural number n. Show that $a = 1$.

Proof. Since $4(a^3 + 1)$ and $4(a^9 + 1)$ are cubes, then their quotient $a^6 - a^3 + 1$ is a cube, too. If $a > 1$, then $a^6 - a^3 + 1 < (a^2)^3$, thus $a^6 - a^3 + 1 \leq (a^2 - 1)^3$, hence $(a-1)(3a^3 - 2a^2 - 1) + 1 \leq 0$ – contradiction. □

Now its time for analysis...

Example 46. Let a and b be integers such that $2^n a + b$ is a perfect square for all positive integers n. Prove that $a = 0$.

Proof. Suppose $a \neq 0$. Then $a > 0$, otherwise for large enough, the number $2^n a + b$ is negative. There exists a sequence of positive integers $\{x_n\}_{n \geq 1}$ such that $x_n = \sqrt{2^n a + b}$ for all n. Easy to see that

$$\lim_{n \to +\infty} (2x_n - x_{n+2}) = 0.$$

Thus there exists positive integer N such that $2x_n = x_{n+2}$ for all $n \geq N$. But equality $2x_n = x_{n+2}$ is equivalent to $b = 0$. Hence a and $2a$ are both perfect squares, which is impossible for $a \neq 0$. □

Homework

Problem 47. Let a, b be positive integers such that for any positive integer n the number $(n + a)(n + b)$ is a product of even number of primes. Prove that $a = b$.

Proof. For any positive integer ℓ define

$$\lambda(\ell) = \begin{cases} 0 & \text{if } \ell \text{ is a product of even number of primes} \\ 1 & \text{if } \ell \text{ is a product of odd number of primes.} \end{cases}$$

Assume (wlog) that $a < b$. Let k be a sufficiently large integer such that $n := k(b-a) - a > 0$. Then

$$(n+a)(n+b) = k(k+1)(b-a)^2$$

is a product of even number of primes, thus $\lambda(k(k+1)) = 0$, hence $\lambda(k) = \lambda(k+1)$. It means that for large enough numbers, value of λ is constant. This is impossible, since $\lambda(p) = 1$ for any prime p and $\lambda(m^2) = 0$ for any integer m. □

Problem 48. 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 $a = x^2$, $b = 2xy$ and $c = y^2$.

Proof. Define sequence of positive integers $x_n = \sqrt{an^2 + bn + c}$. Then

$$\lim_{n \to +\infty} (x_{n+1} - x_n) = \sqrt{a}.$$

Thus there exists positive integer N such that $x_{n+1} = x_n + \sqrt{a}$ for all $n \geq N$. Thus $a = x^2$ for some x. A simple induction shows that $x_n = x_N + (n-N)x$ for $n \geq N$, so

$$(x_N - Nx + nx)^2 = x^2n^2 + bn + c \tag{3-1}$$

for all $n \geq N$. From that equality we get

$$(N-n)(2aN + b - 2x_N x) = 0,$$

thus $b = 2x(x_N - Nx)$. Putting b into 3-1 we compute $c = (x_N - Nx)^2$. Therefore $y := x_N - Nx$ works. □

4. Special problems

Problem 49. Integers $a_1, a_2, \ldots, a_n$ satisfy

$$1 < a_1 < a_2 < \ldots < a_n < 2a_1.$$

If m is the number of distinct prime factors of $a_1 a_2 \ldots a_n$, then prove that

$$(a_1 a_2 \cdots a_n)^{m-1} \geq (n!)^m.$$

Example 50. Let $C > 1$ be a real number. Define sequence of positive real numbers $a_1, a_2, a_3, \ldots$, satisfying $a_1 = 1$, $a_2 = 2$ and also

$$a_{mn} = a_m a_n \quad \text{and} \quad a_{m+n} \leq C(a_m + a_n) \quad \text{for} \quad m, n \in \mathbb{N}^*.$$

Show that $a_n = n$ for any $n \in \mathbb{N}^*$.

Problem 51. Prove that for any $\varepsilon > 0$ there exists integer n such that the greatest prime divisor of $n^2 + 2018$ is smaller than εn.