
April Online Camp 2020

Number Theory

Level L2

Dominik Burek

CONTENTS

Covered topics	2
Problems	3
1. Class 1	3
1.1. Homework	4
2. Class 2	5
2.1. Homework	5
3. Class 3	7
3.1. Homework	7
4. Class 4	9
4.1. Homework	9
5. Class 5	10
5.1. Homework	10
6. Class 6	12
6.1. Homework	12
7. Class 6	13
7.1. Homework	13
8. Class 7	14
TEST	15
Solutions	16
References	43

Covered topics

- Divisibility
- Fermat's descent
- Guessing module
- Square between square
- Sum of two squares, Fermat theorem
- Chinese Remainder Theorem
- Quadratic residues

Problems

1. CLASS 1

Problem 1. Let a, b be integers such that $a + b \mid a^2$. Prove $a + b \mid b^2$.



Problem 2. Let m, n be integers such that $m + n \mid m + n^2$. Prove $m + n \mid m + n^3$.



Problem 3. Let m, n, d be integers such that $d \mid mn^2 + 1$ and $d \mid m^2n + 1$. Prove $d \mid m^3 + 1$ and $d \mid n^3 + 1$.



Problem 4. Prove that

$$133 \mid 11^{n+2} + 12^{2n+1}.$$



Problem 5. Prove the identity

$$\text{lcm}(a, b) \cdot \gcd(a, b) = ab.$$



Problem 6. Prove the identity

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


for all positive integers a, b, c .




Problem 7. Let a, b be positive integers and p, q distinct primes such that $aq \equiv 1 \pmod{p}$ and $bp \equiv 1 \pmod{q}$. Prove that

$$\frac{a}{p} + \frac{b}{q} > 1.$$




Problem 8. Let a, b be odd positive integers such that $a^b b^a$ is a perfect square. Prove that ab is a perfect square. 


Problem 9. Let a, b, c, d be positive integers such that $ab = cd$. Prove that $a^{2020} + b^{2020} + c^{2020} + d^{2020}$ is a composite number. 


Problem 10. Given are two integers $a > b > 1$ such that

$$a + b \mid ab + 1 \quad \text{and} \quad a - b \mid ab - 1.$$


Prove that $a < \sqrt{3}b$. 


1.1. Homework.


Homework 1. Let a, b, c be positive integers such that $\frac{a\sqrt{2} + b}{b\sqrt{2} + c}$ is rational. Prove that $a + b + c \mid ab + bc + ca$. 

Homework 2. Let a be a 8-digit number. Call b the number which was made by moving last digit of a to the beginning. Prove that if $101 \mid a$, then $101 \mid b$. 


Homework 3. Find all positive integers n for which $n^3 - 7n$ is a square. 

Homework 4. Let a_1, a_2, \dots, a_n be an arithmetic progression of integers such that $i \mid a_i$ for $i = 1, 2, \dots, n - 1$ and $n \nmid a_n$. Prove that n is a prime power. 

Homework 5. Are there exist four different positive integers a, b, c, d with $ad = bc$ and $n^2 \leq a, b, c, d < (n + 1)^2$ for some positive integer n ? 


Homework 6. Show that there exist infinitely many positive integers n such that $n^2 + 1$ divides $n!$. 

2. CLASS 2

Problem 11. Let a, b be positive integers such that $a + b \mid ab$. Prove that $\gcd(a, b) \geq \sqrt{a + b}$. 


Problem 12. Let x, y, z be positive integers such that

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

is an integer. Let d be the greatest common divisor of x, y and z . Prove that $d \leq \sqrt[3]{xy + yz + zx}$. 


Problem 13. Let a, b and c , be positive integers such that $\gcd(a, b, c) = 1$ and

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

Prove that all of a, b, c are perfect squares. 

Problem 14. Let a, b, c, d be non-zero integers, such that the only quadruple of integers (x, y, z, t) satisfying the equation

$$ax^2 + by^2 + cz^2 + dt^2 = 0$$

is $x = y = z = t = 0$. Does it follow that the numbers a, b, c, d have the same sign? 

Problem 15. Solve in integers the following equation

$$x^2 + y^2 + z^2 - 2xyz = 0.$$



2.1. Homework.

Homework 7. Solve in integers the following equation

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



Homework 8. Find all integer solutions of

$$x^3 + 3y^3 + 9z^3 - 3xyz = 0.$$



Homework 9. Find all integer solutions of the following equation


$$a^2 + b^2 + c^2 = 7d^2.$$



Homework 10. Solve in integers the following equation

$$x^4 + y^4 + z^4 = 9u^4.$$



 **Homework 11.** Let $p > 2$ be a prime number and consider numbers $x, y \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ are given. Prove that if $x(p-x)y(p-y)$ is a perfect square, then $x = y$.



3. CLASS 3

Problem 16. Solve in integers system of equations

$$\begin{cases} x^2 + 6y^2 = z^2 \\ 6x^2 + y^2 = t^2 \end{cases}$$



Problem 17. Solve in integers the following equation

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



Problem 18. Find all positive integers (k, m) for which $k^2 + 4m$ and $m^2 + 5k$ are perfect squares.



Problem 19. Find all solutions of the following equation in integers

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



Problem 20. Solve in integers the following equation

$$2^x + 17 = y^4.$$



Problem 21. Let $p > 3$ be a prime of the form $3k + 2$. Prove that

$$1^3, 2^3, \dots, (p-1)^3$$

gives different residues modulo p .



3.1. Homework.

Homework 12. Solve in integers the following equation

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



Homework 13. Find all rationals a, b such that

$$a^2 + ab + b^2 = 2.$$



Homework 14. Prove that for any prime $p \geq 3$ the following divisibility holds

$$p \mid \underbrace{11 \dots 1}_p \underbrace{22 \dots 2}_p \dots \underbrace{99 \dots 9}_p - 123456789.$$



Homework 15. Find all solutions of the following equation in integers

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




Homework 16. Find all positive integers (a, b) for which $a^3 + 6ab + 1$ and $b^3 + 6ab + 1$ are perfect cubes.




Homework 17. Solve in integers the following equation

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




 **Homework 18.** Prime number $p > 3$ is congruent to 2 modulo 3. Let $a_k = k^2 + k + 1$ for $k = 1, 2, \dots, p-1$. Prove that product $a_1 a_2 \dots a_{p-1}$ is congruent to 3 modulo p .



 **Homework 19.** 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.



4. CLASS 4

Problem 22. Prove that for any prime number $p > 3$ exist integers x, y, k that meet conditions: $0 < 2k < p$ and $kp + 3 = x^2 + y^2$. 

4.1. Homework.


Homework 20. Prove that

$$x^8 + 1 = n!$$

has only finitely many solutions in nonnegative integers. 


Homework 21. Prove that the equation

$$3^k - 1 = m^2 + n^2$$

has infinitely many solutions in positive integers. 


Homework 22. Prove that the equation

$$x^4 - 4 = y^2 + z^2$$

does not have integer solutions. 

Homework 23. Prove that there are no positive integers m, n such that

$$4mn - m - n$$

is a square. 

5. CLASS 5

Problem 23. Solve in integers the following equation

$$x^3 + 7 = y^2.$$



Problem 24. Find all n -tuples (a_1, a_2, \dots, a_n) of positive integers such that

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

is a perfect square.



Problem 25. Prove that there are infinitely many prime numbers of the form $4k + 3$ and $4k + 1$.



Problem 26. Prove that there exist 2020 consecutive integers which are divisible by a square of some integer greater than 1.



Problem 27. Prove that there exist 2020 consecutive integers which are not perfect powers.



Problem 28. Prove that there are arbitrary many consecutive integers, none of which can be written as a sum of perfect squares.



Problem 29 (Schur's lemma). Suppose that $f \in \mathbb{Z}[X]$. Prove that the set of primes numbers dividing at least one term of a sequence $(P(n))_{n \geq 1}$ is infinite.



5.1. Homework.

Homework 24. 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.



Homework 25. Prove that

$$\frac{x^2 + 1}{y^2 - 5}$$

is not an integer for any integers $x, y > 2$.




Homework 26. Prove that each prime p of the form $4k + 1$ can be represented in exactly one way as the sum of the squares of two integers, up to the order and signs of the terms.



Homework 27. Prove that for all $n \geq 1$ there is a positive integer a such that $a, 2a, 3a, \dots, na$ are all perfect powers.




 **Homework 28.** 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 2020 consecutive positive integers which are nice.



6. CLASS 6


Problem 30. Show that for any n we can find a set X of n distinct integers greater than 1, such that the average of the elements of any subset of X is a square, cube or higher power. 

Problem 31. Let f be a nonconstant polynomial with integer coefficients and let n and k be positive integers. Prove that there is a positive a such that

$$f(a), f(a+1), \dots, f(a+n-1)$$


has at least k distinct prime divisors. 


6.1. Homework.



Homework 29. Let P be a polynomial with integer coefficients such that there are two distinct integers at which P takes coprime values. Show that there exists an infinite set of integers, such that the values P takes at them are pairwise coprime. 

Homework 30. Prove that for any positive integer k , there exists an arithmetic sequence

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \dots, \frac{a_k}{b_k}$$

of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \dots, k$ such that the positive integers $a_1, b_1, a_2, b_2, \dots, a_k, b_k$ are all distinct. 

Homework 31. Prove that for each positive integer n , there are pairwise relatively prime integers k_0, k_1, \dots, k_n , all strictly greater than 1, such that $k_0 k_1 \dots k_n - 1$ is the product of two consecutive integers. 

 **Homework 32.** Find all positive integers n for which there is an integer m such that $2^n - 1 \mid m^2 + 9$. 

7. CLASS 6

Problem 32. Compute

$$\left(\frac{600}{953}\right), \quad \left(\frac{2020^3}{953}\right), \quad \left(\frac{-7000}{757}\right).$$



Problem 33. Prove that

- -2 is a quadratic residue modulo a prime $p > 2$ iff $p \equiv 1, 3 \pmod{8}$,
- 2 is a quadratic residue modulo a prime $p > 2$ iff $p \equiv \pm 1 \pmod{8}$,
- -3 is a quadratic residue modulo a prime $p > 2$ iff $p \equiv 1 \pmod{6}$,
- 3 is quadratic residue modulo a prime $p > 2$ iff $p \equiv \pm 1 \pmod{12}$.



7.1. Homework.

Homework 33. Let $p > 2$ be a prime. Compute

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \dots + \left(\frac{p-1}{p}\right).$$



Homework 34. Prove that if $p \equiv 1 \pmod{4}$, then the sum of quadratic residues \pmod{p} in $\{0, 1, \dots, p-1\}$ is $\frac{p(p-1)}{4}$.



Homework 35. Let $x_1 = 7$ and

$$x_{n+1} = 2x_n^2 - 1, \quad \text{for } n \geq 1.$$

Prove that 2003 does not divide any term of the sequence.




Homework 36. 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 $p \mid y^2 - y + 25$.



Homework 37. Prove that number $2^n + 1$ does not have prime divisor of the form $8k - 1$.





8. CLASS 7


Problem 34. Let $p \equiv 1 \pmod{4}$ be a prime and let $p = a^2 + b^2$ with a odd. Prove a is quadratic residue modulo p . 

Problem 35. Suppose that for some prime p and integers a, b, c the following are true

$$6 \mid p+1, \quad p \mid a+b+c, \quad p \mid a^4+b^4+c^4.$$

Prove that $p \mid a, p \mid b$ and $p \mid c$. 

Problem 36. Let c be an integer which is not perfect square. Then, there exists a prime $p > 2$ such that $\left(\frac{c}{p}\right) = -1$. 

Problem 37. Let a and b be integers such that $a \neq 0$ and the number $3 + a + b^2$ is divisible by $6a$. Prove that a is negative. 

Problem 38. Prove that for any positive integer n every prime divisor p of number

$$n^4 - n^2 + 1$$

is of the form $12k + 1$. 

Problem 39. Suppose that $p \equiv 1 \pmod{3}$ is a prime. Using Thue's lemma prove that there exists integers $0 < x, y < \sqrt{p}$ such that $p \mid 3x^2 + y^2$. Conclude that there are integers a, b such that

$$p = a^2 + ab + b^2.$$



TEST

Problem 1. Compute

$$\left(\frac{-12000}{821}\right), \quad \left(\frac{2^{2019}}{953}\right).$$

Problem 2. Let a and b be positive integers such that

$$\frac{\text{lcm}(a, b)}{\text{gcd}(a, b)} = a - b.$$

Prove that $\text{lcm}(a, b) = \text{gcd}(a, b)^2$.

Problem 3. Prove that 5 is quadratic residue modulo a prime $p > 2$ iff $p \equiv \pm 1 \pmod{10}$.

Problem 4. Find all positive integers such that $x^2 + 3y$ and $y^2 + 3x$ are squares.

Problem 5. Let k be a positive integer. Prove that there are distinct integers x, y such that

$$\text{gcd}(x + i, y + j) > 1 \quad \text{for any } 1 \leq i, j \leq k.$$

Problem 6. Solve in integers the following equation

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

Problem 7. Prove that if a is an integer, then $2a^2 - 1$ has no divisors of the form $b^2 + 2$, where b is an integer.


Problem 8. Let a, b, c be positive integers such that

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


is an integer. Prove that this integer is not divisible by 3.

Solutions

Problem 1. Let a, b be integers such that $a + b \mid a^2$. Prove $a + b \mid b^2$.

Proof.  Note that $b^2 = a(a + b) - a^2$. □

Problem 2. Let m, n be integers such that $m + n \mid m + n^2$. Prove $m + n \mid m + n^3$.

Proof.  Note that $m + n \mid m + n^2 - (m + n) = n(n - 1)$, so using the identity

$$m + n^3 = m + n^2 - n^2(n - 1)$$

we are done. □

Problem 3. Let m, n, d be integers such that $d \mid mn^2 + 1$ and $d \mid m^2n + 1$. Prove $d \mid m^3 + 1$ and $d \mid n^3 + 1$.

Proof.  We see that

$$d \mid n(m^2n + 1) - m(mn^2 + 1) = n - m.$$


Thus

$$d \mid m^2(m - n) + (m^2n + 1) \quad \text{and} \quad d \mid m^2(n - m) + (mn^2 + 1).$$

□

Problem 4. Prove that

$$133 \mid 11^{n+2} + 12^{2n+1}.$$


Proof. 

$$11^{n+2} + 12^{2n+1} = 121 \cdot 11^n + 12 \cdot 144^n \equiv -12 \cdot 11^n + 12 \cdot 11^n = 0 \pmod{133}.$$

□

Problem 5. Prove the identity


$$\text{lcm}(a, b) \cdot \text{gcd}(a, b) = ab.$$

Proof.  For an arbitrary prime p , suppose the exponent of p in the prime factorization of a is a' and define b' similarly. Assume WLOG $a' \geq b'$. Then v_p of LHS is equal to $a'b'$ and same with v_p of RHS. \square

Problem 6. Prove the identity

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

for all positive integers a, b, c .

Proof.  For an arbitrary prime p , suppose the exponent of p in the prime factorization of a is a' and define b', c' similarly. Assume WLOG $a' \geq b' \geq c'$. Take the reciprocal of both sides of the desired equation; then the exponent v_p of LHS

$$-2 \max(a', b', c') + \max(a', b') + \max(b', c') + \max(c', a') = -2a' + a' + b' + a' = b'$$


while the exponent v_p of the RHS is

$$-2 \min(a', b', c') + \min(a', b') + \min(b', c') + \min(c', a') = -2c' + b' + c' + c' = b'$$

so the two sides have the same prime factorization and are therefore equal. \square

Problem 7. Let a, b be positive integers and p, q distinct primes such that $aq \equiv 1 \pmod{p}$ and $bp \equiv 1 \pmod{q}$. Prove that

$$\frac{a}{p} + \frac{b}{q} > 1.$$

Proof.  Given conditions imply that $aq = pk + 1$ and $bp = ql + 1$ for some positive integers k and l . Since p, q are primes we see that $pq \mid pk + ql + 1$. Therefore

$$\frac{a}{p} + \frac{b}{q} = \frac{aq + bp}{pq} = \frac{pk + ql + 1}{pq} = \frac{pk}{pq} + \frac{ql}{pq} + \frac{1}{pq} \geq 1 + \frac{1}{pq} > 1.$$

\square

Problem 8. Let a, b be odd positive integers such that $a^b b^a$ is a perfect square. Prove that ab is a perfect square.

Proof.  Notice that


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

is a perfect square. Thus

$$ab = \frac{a^b b^a}{a^{b-1} b^{a-1}},$$

too. \square

Problem 9. Let a, b, c, d be positive integers such that $ab = cd$. Prove that $a^{2020} + b^{2020} + c^{2020} + d^{2020}$ is a composite number.

Proof.  We firstly shall prove the following lemma

Lemma 1. Let a, b, c , and d be positive integers such that $ab = cd$. Show that there exists positive integers p, q, r, s such that

$$a = pq, \quad b = rs, \quad c = ps, \quad d = qr.$$

Proof. Since $\frac{a}{c} = \frac{d}{b}$, one can find $q, s \in \mathbb{N}$ such that $\gcd(q, s) = 1$ and

$$\frac{a}{c} = \frac{d}{b} = \frac{q}{s}.$$

Since $\frac{a}{c} = \frac{q}{s}$ and since $\gcd(q, s) = 1$, we can write $a = qp$, $c = sp$ for some positive integer p . Also, since $\frac{d}{b} = \frac{q}{s}$ and since $\gcd(q, s) = 1$, we can write $d = qr$ and $b = sr$ for some positive integer r . \square

Notice that from the above lemma $a = mn$, $b = kl$, $c = km$, $d = ln$ for some integers k, l, m, n . Thus

$$a^{2020} + b^{2020} + c^{2020} + d^{2020} = (m^{2020} + l^{2020})(k^{2020} + n^{2020}).$$

\square

Problem 10. Given are two integers $a > b > 1$ such that

$$a + b \mid ab + 1 \quad \text{and} \quad a - b \mid ab - 1.$$

Prove that $a < \sqrt{3}b$.

Proof.  Notice that

$$b^2 - 1 = b(a + b) - (ab + 1) \equiv 0 \pmod{a + b},$$

and

$$b^2 - 1 = (ab - 1) - b(a - b) \equiv 0 \pmod{a - b}.$$

Since $\gcd(a - b, a + b) = 1, 2$, we get $(a - b)(a + b) \mid 2(b^2 - 1)$. Hence

$$(a^2 - b^2) \leq 2(b^2 - 1) < 2b^2,$$

so we have $a < \sqrt{3}b$. \square

Homework 1. Let a, b, c be a positive integers such that $\frac{a\sqrt{2} + b}{b\sqrt{2} + c}$ is rational.

Prove that $a + b + c \mid ab + bc + ca$.

Proof. 🧐 Notice that

$$\frac{a\sqrt{2}+b}{b\sqrt{2}+c} = \frac{2ab-bc}{2b^2-c^2} + \frac{b^2-ac}{2b^2-c^2}\sqrt{2} \in \mathbb{Q},$$

so $b^2 - ac = 0$. Therefore

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

□

Homework 2. Let a be a 8-digit number. Call b the number which was made by moving last digit of a to the beginning. Prove that if $101 \mid a$, then $101 \mid b$.

Proof. 🧐 Let $a = \overline{a_7a_6a_5a_4a_3a_2a_1a_0}$, then

$$b = \overline{a_0a_7a_6a_5a_4a_3a_2a_1} = a_0 \cdot 10^7 + \frac{a - a_0}{10},$$

thus

$$10b = a + a_0(10^8 - 1) = a + a_0 \cdot 101 \cdot 990099,$$

and the conclusion follows. □

Homework 3. Find all positive integers n for which $n^3 - 7n$ is a square.

Proof. 🧐 If $7 \nmid n$, then $\gcd(n, n^2 - 7) = 1$, thus $n = a^2$ and $n^2 - 7 = b^2$ for some nonnegative a, b . Therefore $(a^2 - b)(a^2 + b) = 7$, thus $n = a^2 = 4$.

If $7 \mid n$, then $n^3 - 7n = 49m(7m^2 - 1)$, hence $m(7m^2 - 1)$ is a square. Similar to the above case we derive $m = c^2$ and $7m^2 - 1 = d^2$ for some nonnegative c, d . Thus $7c^4 = d^2 + 1$, but $7 \nmid d^2 + 1$ – contradiction. □

Homework 4. Let a_1, a_2, \dots, a_n be an arithmetic progression of integers such that $i \mid a_i$ for $i = 1, 2, \dots, n-1$ and $n \nmid a_n$. Prove that n is a prime power.


Proof. 🧐 We have

$$a_1 = a_1, \quad a_2 = a_1 + d, \quad a_3 = a_1 + 2d, \quad \dots, \quad a_n = a_1 + (n-1)d.$$

Then since $i \mid a_i = a_1 + (i-1)d$ for $1 \leq i \leq n-1$, we have $i \mid a_1 - d$; but $n \nmid a_1 - d$.

If $n = ab$ for two coprime positive integers $1 < a, b < n$. Then $a \mid a_1 - d$ and $b \mid a_1 - d$ which implies $n \mid a_1 - d$, of course a contradiction. Therefore n is a prime power. □


Homework 5. Are there exist four different positive integers a, b, c, d with $ad = bc$ and $n^2 \leq a, b, c, d < (n+1)^2$ for some positive integer n ?

Proof.  If exist then take (by 1) $a = pq$, $d = rs$, $b = pr$, $c = qs$ (??) and suppose $a < b < c < d$. We have that $c > a$ implies $s \geq p + 1$ and $b > a$ implies $r \geq q + 1$, thus

$$\begin{aligned} d = rs &\geq (p + 1)(q + 1) = pq + p + q + 1 \geq pq + 2\sqrt{pq} + 1 = \\ &= (\sqrt{a} + 1)^2 \geq (n + 1)^2. \end{aligned}$$

□

Homework 6. Show that there exist infinitely many positive integers n such that $n^2 + 1$ divides $n!$.

Proof.  We try $n = 2k^2$ for some k :

$$n^2 + 1 = 4k^4 + 1 = (2k^2 + 2k + 1)(2k^2 - 2k + 1).$$

Now $\gcd(2k^2 + 2k + 1, 2k^2 - 2k + 1) = \gcd(4k, 2k^2 - 2k + 1) = 1$ and $2k^2 - 2k + 1 < 2k^2 = n$, so $2k^2 - 2k + 1 \mid n!$. Thus everything we still need to show is that $2k^2 + 2k + 1$ can be chosen such that it divides $n!$. For this, take for example $k = 25m + 1$, since then $2k^2 + 2k + 1 = 5 \cdot s$ for some s not divisible by 5. Thus $5 < n$, $s = \frac{2k^2 + 2k + 1}{5} < 2k^2 = n$ and $\gcd(5, s) = 1$, implying the result.


There is also one more construction. Let $n = 4k^2 + 2k + 1$, then

$$n^2 + 1 = (4k^2 + 1)^2 + 2(4k^2 + 1)2k + (2k)^2 + 1 = 2(4k^2 + 1)(2k^2 + 2k + 1).$$

If we suppose $2 < 2k^2 + 2k + 1 < 4k^2 + 1$, then $2(4k^2 + 1)(2k^2 + 2k + 1)$ divides $(4k^2 + 2k + 1)!$.

We have another solution: Consider the equation $n^2 - 5m^2 = -1$. Clearly, $\max\{m, 2m\} < n$. For $n > 5$, $m \neq 5$, we have that $n^2 + 1 = 5m^2 \mid n!$. The equation $n^2 - 5m^2 = -1$ is a Pell equation with infinitely many solutions. And the conclusion follows. □


Problem 11. Let a, b be a positive integers such that $a + b \mid ab$. Prove that $\gcd(a, b) \geq \sqrt{a + b}$.

Proof.  Let $d := \gcd(a, b)$. Then $a = dx$ and $b = dy$ for some coprime x, y . Given divisibility implies that $(a + b)z = ab$ for some integer z . It means that $d(x + y)z = d^2xy$ or $(x + y)z = dxy$ i.e. $x + y \mid dxy$. Since $\gcd(x, x + y) = \gcd(y, x + y) = 1$, then $x + y \mid d$. In particular $d \geq x + y$, i.e. $d \geq \sqrt{a + b}$. □

Problem 12. Let x, y, z be positive integers such that

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

is an integer. Let d be the greatest common divisor of x, y and z . Prove that $d \leq \sqrt[3]{xy + yz + zx}$.

Proof.  Let $x = ad$, $y = bd$, $z = cd$, then

$$\begin{aligned} \frac{x+1}{y} + \frac{y+1}{z} + \frac{z+1}{x} &= \frac{x^2z + xz + y^2x + yx + z^2y + zy}{xyz} = \\ &= \frac{d^3(a^2c + b^2a + c^2b) + xy + yz + zx}{d^3abc}. \end{aligned}$$

It follows that


$$d^3 \mid xy + yz + zx \implies d^3 \leq xy + yz + zx \implies d \leq \sqrt[3]{xy + yz + zx}.$$

□

Problem 13. Let a, b and c , be a positive integers such that $\gcd(a, b, c) = 1$ and

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

Prove that all of a, b, c are perfect squares.

Proof.  From the condition, we obtain:

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

$$(a - b + c)^2 = 4ac,$$

$$(-a + b + c)^2 = 4bc.$$


Hence ab, bc, ca are all perfect squares. Moreover, as $\gcd(a, b, c) = 1$, we see that a, b, c are pairwise coprime and hence perfect squares.

□

Problem 14. Let a, b, c, d be non-zero integers, such that the only quadruple of integers (x, y, z, t) satisfying the equation

$$ax^2 + by^2 + cz^2 + dt^2 = 0$$

is $x = y = z = t = 0$. Does it follow that the numbers a, b, c, d have the same sign?

Proof.  No, take $a = b = 1$, $c = d = -3$. Then we get an equation


$$x^2 + y^2 = 3z^2 + 3t^2,$$

which has only $(0, 0, 0, 0)$ solution from Fermat's descend method.

□

Problem 15. Solve in integers the following equation

$$x^2 + y^2 + z^2 - 2xyz = 0.$$

Proof.  Since $2 \mid x^2 + y^2 + z^2$ so we have 0 or 2 odd number within x, y, z . If there are 2 odd numbers then we get

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


but

$$4 \mid 2xyz = x^2 + y^2 + z^2$$

– contradiction. Therefore $2 \mid x$, $2 \mid y$ and $2 \mid z$ and Fermat's descend finishes problem. \square


Homework 7. Solve in integers the following equation

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

Proof.  Since $3 \mid x^2 + y^2$ we see that $3 \mid x$ and $3 \mid y$, so $x = 3x_1$ and $y = 3y_1$. After this substitution our equations is equivalent to $3x_1^2 + 3y_1^2 = z^2$, so $z = 3z_1$ and hence $x_1^2 + y_1^2 = 3z_1^2$. By Fermat descend $x = y = z = 0$. \square

Homework 8. Find all integer solutions of

$$x^3 + 3y^3 + 9z^3 - 3xyz = 0.$$

Proof.  From that equation you see that $3 \mid x^3$, so $x = 3x_1$. Putting it into given equation you will get

$$9x_1^3 + y^3 + 3z^3 - 3x_1yz = 0,$$

so $3 \mid y^3$ i.e. $y = 3y_1$. Then

$$3x_1^3 + 9y_1^3 + z^3 - 3x_1y_1z = 0,$$


so $3 \mid z^3$ i.e. $z = 3z_1$. Therefore

$$x_1^3 + 3y_1^3 + 9z_1^3 - 3x_1y_1z_1 = 0$$

which is the same equation as original one. Hence by Fermat's descend we get $x = y = z = 0$. \square

Homework 9. Find all integer solutions of the following equation

$$a^2 + b^2 + c^2 = 7d^2.$$

Proof.  We will do modulo 4. Since $x^2 \equiv 0, 1 \pmod{4}$ we see that if $2 \nmid d$, then a, b, c are odd. Therefore


$$a^2 + b^2 + c^2 \equiv 3 \pmod{8}$$

and $7d^2 \equiv 7 \pmod{8}$ – contradiction. Therefore $2 \mid d$ and so $2 \mid a, b, c$, so by descent argument we have $a = b = c = d = 0$.

There is theorem due to Euler which says that the number is a sum of three squares iff is not of the form $4^s(8\ell + 7)$, where s, ℓ are non-negative integers. \square

Homework 10. Solve in integers the following equation

$$x^4 + y^4 + z^4 = 9u^4.$$

Proof.  If $5 \nmid u$ then


$$x^4 + y^4 + z^4 = 9u^4 \equiv 4 \pmod{5}$$

from LFT, but again from LFT

$$x^4 + y^4 + z^4 \leq 3 \pmod{5}.$$

Therefore $5 \mid u$. Thus $5 \mid x^4 + y^4 + z^4$ and from LFT we see that $5 \mid x$, $5 \mid y$, $5 \mid z$. By Fermat's descend we are done. \square

Homework 11. Let $p > 2$ be a prime number and consider numbers $x, y \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ are given. Prove that if $x(p-x)y(p-y)$ is a perfect square, then $x = y$.

Proof.  Write $xy = ka^2$ and $(p-x)(p-y) = kb^2$. Then p divides $(p-x)(p-y) - xy = k(b-a)(b+a)$. Clearly $p \nmid k(b-a)$ so $p \mid a+b$.

Now, if $x \neq y$ then $a^2 \leq ka^2 = xy < \left(\frac{x+y}{2}\right)^2$. So $a < \frac{x+y}{2}$. Analogously $b < \frac{(p-x) + (p-y)}{2}$, thus

$$p \leq a + b < \frac{x+y}{2} + \frac{(p-x) + (p-y)}{2} = p,$$

a contradiction. Therefore $x = y$. \square

Problem 16. Solve in integers system of equations

$$\begin{cases} x^2 + 6y^2 = z^2 \\ 6x^2 + y^2 = t^2 \end{cases}$$

Proof.  After adding these equations we have

$$7x^2 + 7y^2 = z^2 + t^2,$$

so $7 \mid z^2 + t^2$ i.e. $z = 7z_1$, $t = 7t_1$ and so

$$7x^2 + 7y^2 = 49z_1^2 + 49t_1^2,$$

hence

$$x^2 + y^2 = 7z_1^2 + 7t_1^2,$$

so $7 \mid x^2 + y^2$ i.e. $x = 7x_1$ and $y = 7y_1$, so

$$49x_1^2 + 49y_1^2 = 7z_1^2 + 7t_1^2,$$


hence

$$7x_1^2 + 7y_1^2 = z_1^2 + t_1^2.$$

Therefore by Fermat's descent we see that $x = y = z = t = 0$. \square

Problem 17. 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. \square

Problem 18. 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 from 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. \square

Problem 19. 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

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

\square

Problem 20. Solve in integers the following equation

$$2^x + 17 = y^4.$$

Proof.  Since

$$17 = y^4 - 2^x \mid (y^4)^4 - (2^x)^4 = y^{16} - 16^x$$

we have y^{16} and 16^x give the same residue modulo 17.

If x is odd, then $16^x \equiv -1$, but $y^{16} \equiv 0, 1 \pmod{17}$ by LFT. Therefore x is even i.e. $x = 2m$. Hence


$$17 = y^4 - 2^{2m} = (y^2 - 2^m)(y^2 + 2^m),$$

so $y^2 - 2^m = 1$ and $y^2 + 2^m = 17$, so $y = 3$ and $m = 3$ i.e. $(x, y) = (6, 3)$. \square

Problem 21. Let $p > 3$ be a prime of the form $3k + 2$. Prove that


$$1^3, 2^3, \dots, (p-1)^3$$

gives different residues modulo p .

Proof.  Suppose that $a^3 \equiv b^3 \pmod{p}$. Then taking $\frac{p-2}{3} = k$ power of both sides we have $a^{p-2} \equiv b^{p-2} \pmod{p}$, so $ba^{p-1} \equiv ab^{p-1} \pmod{p}$, hence by LFT $b \equiv a \pmod{p}$ – contradiction. \square

Homework 12. Solve in integers the following equation

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


Proof.  If x is even, then y too, but then $x^2 + 4 \equiv 4, 8 \pmod{16}$ and $y^5 \equiv 0 \pmod{16}$ – contradiction. Therefore x is odd, then $x^2 + 4 \equiv 1 \pmod{4}$, so $y \equiv 1 \pmod{4}$. Hence

$$x^2 + 6^2 = y^5 + 2^5,$$

and $y + 2 \mid y^5 + 2^5$, so $y + 2 \mid x^2 + 6^2$, but $y + 2 \equiv 3 \pmod{4}$, so there exists prime $p \equiv 3 \pmod{4}$ of odd exponent ($\gcd(y + 2, \frac{y^5 + 2^5}{y + 2}) = 1$) which divides $x^2 + 6^2$ – contradiction. \square

Homework 13. Find all rationals a, b such that

$$a^2 + ab + b^2 = 2.$$

Proof.  We can find integers $x, y \neq 0, z$ such that $a = \frac{x}{y}, b = \frac{z}{y}$. Then

$$x^2 + xz + z^2 = 2y^2.$$

Easy to see that $2 \mid x, z$, so $x = 2x_1$ and $z = 2z_1$. Therefore

$$2x_1^2 + 2x_1z_1 + 2z_1^2 = y^2,$$


so $2 \mid y$ i.e. $y = 2y_1$, thus

$$x_1^2 + x_1z_1 + z_1^2 = 2y_1^2,$$

which is the same as original. Fermat's descend gives $x = y = z = 0$ – contradiction since $y \neq 0$. \square

Homework 14. Prove that for any prime $p \geq 3$ the following divisibility holds

$$p \mid \underbrace{11 \dots 1}_p \underbrace{22 \dots 2}_p \dots \underbrace{99 \dots 9}_p - 123456789.$$

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

$$\begin{aligned} & 9 \left(\underbrace{11 \dots 1}_p \underbrace{22 \dots 2}_p \dots \underbrace{99 \dots 9}_p - 123456789 \right) = \\ &= 9 \left(\underbrace{11 \dots 1}_{9p} + \underbrace{11 \dots 1}_{8p} + \dots + \underbrace{11 \dots 1}_p - \underbrace{11 \dots 1}_9 - \underbrace{11 \dots 1}_8 - \dots - 1 \right) = \\ &= 10^{9p} + 10^{8p} + \dots + 10^p - 10^9 - 10^8 - \dots - 10, \end{aligned}$$

which is divisible by p from LFT, because $10^{kp} \equiv 10^k \pmod{p}$ for $k = 1, 2, \dots, 9$. \square

Homework 15. 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

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

□

Homework 16. 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.


□

Homework 17. Solve in integers the following equation

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

Proof.  If we choose $p = 6 \cdot 7 + 1$ we see that there are only 7 nonzero residues of $y^6 \pmod{43}$ i.e. 1, 4, 11, 16, 21, 35, 41. Analogously, there are 6 nonzero residues of $y^7 \pmod{43}$ i.e. 1, 6, 7, 36, 37, 42. Easy to see that from above sets of residues the number $2x^6 + y^7$ cannot take 11 $\pmod{43}$. \square

Homework 18. Prime number $p > 3$ is congruent to 2 modulo 3. Let $a_k = k^2 + k + 1$ for $k = 1, 2, \dots, p-1$. Prove that product $a_1 a_2 \dots a_{p-1}$ is congruent to 3 modulo p .

Proof.  By 21 we see that

$$2^3 - 1, 3^3 - 1, \dots, (p-1)^3 - 1$$

are pairwise distinct in modulo p , so

$$\prod_{k=2}^{p-1} (k^3 - 1) \equiv (p-2)! \pmod{p}.$$

Since $k^3 - 1 = (k-1)a_k$ for $k = 2, \dots, p-1$, we see that


$$\prod_{k=2}^{p-1} (k^3 - 1) \equiv (p-2)! a_2 a_3 \dots a_{p-1} \pmod{p}.$$

Therefore we have

$$(p-2)! \equiv \prod_{k=2}^{p-1} (k^3 - 1) \equiv (p-2)! a_2 a_3 \dots a_{p-1} \pmod{p},$$

so $a_2 a_3 \dots a_{p-1} \equiv 1 \pmod{p} \implies a_1 a_2 \dots a_{p-1} \equiv 3 \pmod{p}$. \square

Homework 19. 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


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

is a perfect square. But

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

\square

Problem 22. Prove that for any prime number $p > 3$ exist integers x, y, k that meet conditions: $0 < 2k < p$ and $kp + 3 = x^2 + y^2$.

Proof.  Consider $p + 1$ numbers consist of

$$0^2, 1^2, \dots, \left(\frac{p-1}{2}\right)^2 \quad \text{and} \quad 3 - 0^2, 3 - 1^2, \dots, 3 - \left(\frac{p-1}{2}\right)^2.$$

There must be two with same residue modulo p , and easy to see that they must not come from same former/latter group. Hence, there exists $0 \leq i, j \leq \frac{p-1}{2}$ that $i^2 \equiv 3 - j^2 \pmod{p} \implies p \mid i^2 + j^2 - 3$. We also have

$$i^2 + j^2 - 3 \leq 2 \left(\frac{p-1}{2}\right)^2 - 3 < \frac{p^2}{2}.$$

Hence, $k = \frac{i^2 + j^2 - 3}{p} < \frac{p}{2}$. Also, $i^2 + j^2 \leq 3$ is impossible, this gives $0 < k$, done. □

Homework 20. Prove that

$$x^8 + 1 = n!$$

has only finitely many solutions in nonnegative integers.

Proof.  Note that

$$n! = (x^4)^2 + 1$$

cannot have divisor of the form $4k + 3$, so $n \leq 3$ and so we have only finitely many solutions. □

Homework 21. Prove that the equation

$$3^k - 1 = m^2 + n^2$$

has infinitely many solutions in positive integers.

Proof.  Note that

$$3^{2^\ell} - 1 = (1^2 + 1^2) \cdot 2^2 \cdot (3^2 + 1) \cdot \dots \cdot (3^{2^{\ell-1}} + 1),$$

which is a sum of 2 squares because all factors are sum of two squares. □

Homework 22. Prove that the equation

$$x^4 - 4 = y^2 + z^2$$

does not have integer solutions.

Proof.  Note that

$$x^4 - 4 = (x^2 + 2)(x^2 - 2).$$

If x is odd, then $x^2 + 2 \equiv 3 \pmod{4}$, so there exists prime $p \equiv 3 \pmod{4}$ with odd exponent in the prime decomposition of $x^2 + 2$. But $p \nmid x^2 - 2$ (otherwise $p = 2$), so p has odd exponent in $x^4 - 4$ – cannot divide sum of two squares.

If $x = 2k$ is even, then

$$x^4 - 4 = 4(2k^2 + 1)(2k^2 - 1).$$

If k is even, then $2k^2 - 1 \equiv 3 \pmod{4}$, so the above argument also works, if k is odd then $2k^2 + 1 \equiv 3 \pmod{4}$, so the above argument again works. \square

Homework 23. Prove that there are no positive integers m, n such that

$$4mn - m - n$$

is a square.

Proof.  Suppose that

$$4mn - m - n = x^2,$$


then

$$(4m - 1)(4n - 1) = (2x)^2 + 1.$$

But the number $4m - 1$ has a prime divisor p of the form $4\ell + 3$, so we have that $p \mid 2x$ and $p \mid 1$ – contradiction. \square

Problem 23. Solve in integers the following equation

$$x^3 + 7 = y^2.$$

Proof.  If x is even then y is odd, so $y^2 \equiv 1 \pmod{8}$. Therefore $x^3 \equiv 2 \pmod{8}$ – contradiction. If x is odd, then y is even, so $y^2 \equiv 0 \pmod{4}$, so $x^3 \equiv 1 \pmod{4}$ and thus $x \equiv 1 \pmod{4}$. But then the number

$$y^2 + 1 = x^3 + 2^3$$

is divisible by $x + 2 \equiv 3 \pmod{4}$ – contradiction. \square

Problem 24. Find all n -tuples (a_1, a_2, \dots, a_n) of positive integers such that

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

is a perfect square.

Proof.  Suppose

$$(a_1! - 1)(a_2! - 1) \dots (a_n! - 1) = k^2 + 4^2.$$


Of course $a_i \neq 1$. If $a_i > 3$, then $a_i! - 1 \equiv 3 \pmod{4}$, so some $p \equiv 3 \pmod{4}$ divides $k^2 + 4^2$ – contradiction. Therefore $a_i \in \{2, 3\}$. Let m be the number of 3's, then

the equations can be transform into $5^m - 16 = k^2$. As k is odd, modulo 8 argument shows that m is even. Therefore $m = 2s$, so

$$(5^s - k)(5^s + k) = 16.$$

Easy to see that $s = 1$, so $m = 2$. □

Problem 25. Prove that there are infinitely many prime numbers of the form $4k + 3$ and $4k + 1$.

Proof.  Suppose that p_1, p_2, \dots, p_k are all primes of the form $3 \pmod{4}$. Then the number

$$A := 4p_1p_2 \dots p_k - 1$$


has a prime divisor of the form $3 \pmod{4}$ different then p_i – contradiction.

Suppose that p_1, p_2, \dots, p_k are all primes of the form $1 \pmod{4}$. Then the number

$$A := (p_1p_2 \dots p_k)^2 + 1$$

has only prime divisor of the form $1 \pmod{4}$ different then p_i – contradiction. □

Problem 26. Prove that there exist 2020 consecutive integers which are divisible by a square of some integer greater then 1.

Proof.  Let $p_1, p_2, \dots, p_{2020}$ be arbitrary pairwise different primes. From CRT there exists n such that


$$\begin{cases} n \equiv 0 & (\text{mod } p_1^2) \\ n \equiv -1 & (\text{mod } p_2^2) \\ \vdots \\ n \equiv -2019 & (\text{mod } p_{2020}^2). \end{cases}$$

Easy to see that

$$n, n + 1, n + 2, \dots, n + 2019$$

are 2020 consecutive numbers which satisfy problem's assumptions. □

Problem 27. Prove that there exist 2020 consecutive integers which are not perfect powers.

Proof.  Let $p_1, p_2, \dots, p_{2020}$ be arbitrary pairwise different primes. From the CRT there exists n such that

$$\begin{cases} n \equiv p_1 & (\text{mod } p_1^2) \\ n \equiv -1 + p_2 & (\text{mod } p_2^2) \\ \vdots \\ n \equiv -2019 + p_{2020} & (\text{mod } p_{2020}^2). \end{cases}$$

Easy to see that

$$n, n+1, n+2, \dots, n+2019$$

are 2020 consecutive numbers which satisfy problem's assumptions. \square

Problem 28. Prove that there are arbitrary many consecutive integers, none of which can be written as a sum of perfect squares.

Proof.  Let p_1, p_2, \dots, p_n be arbitrary pairwise different primes which are $3 \pmod{4}$. From the CRT there exists x such that


$$\begin{cases} x \equiv p_1 - 1 & (\text{mod } p_1^2) \\ x \equiv p_2 - 2 & (\text{mod } p_2^2) \\ \vdots \\ x \equiv p_n - n & (\text{mod } p_n^2). \end{cases}$$

Easy to see that


$$x, x+1, x+2, \dots, x+2019$$

are n consecutive numbers which satisfy problem's assumptions (by criterion on sum of two squares). \square

Problem 29 (Schur's lemma). Suppose that $f \in \mathbb{Z}[X]$. Prove that the set of primes numbers dividing at least one term of a sequence $(P(n))_{n \geq 1}$ is infinite.

Proof.  Let $\{p_1, p_2, \dots, p_n\}$ be a set of all prime divisors. If f has free term equal to 0, then statement is obvious. Assume that $a_0 \neq 0$. Take $g(x) = \frac{f(a_0 x)}{a_0}$ and WLOG assume that $a_0 = 1$. Consider number $A = p_1 p_2 \dots p_n$, then $f(A)$ has a prime divisor outside the set $\{p_1, p_2, \dots, p_n\}$ – contradiction. \square

Homework 24. 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.

Proof.  One implication is trivial. Suppose that

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

hence $a^2 + b^2 = nc^2$, so for any $p \equiv 3 \pmod{4}$ we have


$$v_p(n) = v_p(a^2 + b^2) - 2v_p(c),$$

so is even (since $2 \mid v_p(a^2 + b^2)$), therefore n is sum of two squares of integers. \square


Homework 25. Prove that

$$\frac{x^2 + 1}{y^2 - 5}$$

is not an integer for any integers $x, y > 2$.

Proof.  If y is even, $y^2 - 5$ is of the form $4k + 3$, and thus cannot divide $x^2 + 1$.
If y is odd, then $y^2 - 5$ is divisible by 4, while $x^2 + 1$ is never a multiple of 4. \square

Homework 26. Prove that each prime p of the form $4k + 1$ can be represented in exactly one way as the sum of the squares of two integers, up to the order and signs of the terms.

Proof.  Suppose there are two solutions $p = a^2 + b^2 = c^2 + d^2$ for positive integers a, b, c, d . WLOG assume $a > c$. Subtracting from both sides and factoring gives

$$(a - c)(a + c) = (d - b)(d + b).$$

A factoring lemma (4 numbers theorem) says that there exist positive integers w, x, y, z such that

$$\begin{aligned} a - c &= xy, & d - b &= xw, \\ a + c &= wz, & d + b &= yz. \end{aligned}$$

Therefore $a = \frac{xy + wz}{2}$ and $b = \frac{yz - xw}{2}$. Plugging back in gives


$$4p = (x^2 + z^2)(y^2 + w^2).$$

Of course p must divide one of the sums on the left, so we have two cases

- If $p \mid y^2 + w^2$, then $x^2 + z^2 \mid 4$, which only has the solution $x = z = 1$. This gives $a = d = \frac{y + w}{2}$ and $b = -c = \frac{y - w}{2}$.
- If $p \mid x^2 + z^2$, then $y^2 + w^2 \mid 4$, which only has the solution $y = w = 1$. This gives $a = d = \frac{x + z}{2}$ and $b = c = \frac{z - x}{2}$.

Both cases yield the necessary contradiction. \square

Homework 38. Prove that for all $n \geq 1$ there is a positive integer a such that $a, 2a, 3a, \dots, na$ are all perfect powers.

Proof.  Choose pairwise coprime numbers s_1, s_2, \dots, s_n . We will prove that there is $a > 1$ such that ia is s_i perfect power for $1 \leq i \leq n$. There is set of primes p_1, p_2, \dots, p_k such that

$$i = p_1^{\alpha_{1,i}} p_2^{\alpha_{2,i}} \dots p_k^{\alpha_{k,i}}$$

for any i and some $\alpha_{\ell,i} \geq 0$. We look for a of the form

$$p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}.$$

Then


$$ia = p_1^{x_1 + \alpha_{1,i}} p_2^{x_2 + \alpha_{2,i}} \dots p_k^{x_k + \alpha_{k,i}}.$$

For any $1 \leq i \leq n$, by CRT there is a x_i such that $x_i \equiv -\alpha_{i,j} \pmod{p_j}$ for all $1 \leq j \leq k$, and we are done. \square

Homework 27. 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 2020 consecutive positive integers which are nice.

Proof.  We may choose such positive integers $x_1, x_2, \dots, x_{2020}$ that the numbers

$$y_1 = x_1^2(x_1 + 2), y_2 = x_2^2(x_2 + 2), \dots, y_{2020} = x_{2020}^2(x_{2020} + 2)$$

are pairwise coprime. For example, we may choose $x_1 = 1$ and $x_i = y_1 y_2 \dots y_{i-1} - 1$ for every consecutive i . This choice guarantees that for every integer $2 \leq i \leq 2020$ both x_i and $x_i + 2$ (hence, y_i as well) are coprime with any of the numbers y_1, y_2, \dots, y_{i-1} .

If a positive integer n is divisible by any of the numbers $y_1, y_2, \dots, y_{2020}$ then it is nice. Indeed, if, say, $n = y_i m = x_i^2(x_i + 2)m$ for some positive integers m and $1 \leq i \leq 2020$ 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 $y_1, y_2, \dots, y_{2020}$ are pairwise coprime, the CRT implies that there exists a positive integer k satisfying the equalities

$$k \equiv -i \pmod{y_i}, \quad \text{for } i = 1, 2, \dots, 2020.$$

This means that $k + i$ is divisible by y_i for any $1 \leq i \leq 2020$. Thus, the consecutive positive integers $k + 1, k + 2, \dots, k + 2020$ are all nice, and the statement of the problem is proved. \square

Problem 30. Show that for any n we can find a set X of n distinct integers greater than 1, such that the average of the elements of any subset of X is a square, cube or higher power.

Proof.  By 38 there is a positive integer a such that $a, 2a, \dots, n \cdot n!a$ are all perfect powers. Consider the set


$$A := \{n!a, 2n!a, \dots, n \cdot n!a\}.$$

If $x_1, \dots, x_k \in A$ and $1 \leq k \leq n$, then $\frac{x_1 + \dots + x_k}{k}$ is of the form $\frac{n!}{k} \cdot am$ with $1 \leq m \leq nk$. Thus $\frac{x_1 + \dots + x_k}{k}$ is indeed a perfect power by the choice of a . \square

Problem 31. Let f be a nonconstant polynomial with integer coefficients and let n and k be positive integers. Prove that there is a positive a such that

$$f(a), f(a+1), \dots, f(a+n-1)$$

has at least k distinct prime divisors.

Proof.  Choose pairwise distinct prime for $1 \leq i, j \leq k$ numbers p_{ij} such that $f(x_{ij}) \equiv 0 \pmod{p_{ij}}$ for some positive integers x_{ij} , which is possible using Schur's lemma 29. Thanks to the Chinese remainder theorem, we can find $a \geq 1$ such that


$$a + i - 1 \equiv x_{ij} \pmod{p_{ij}}$$

for all i, j . But then each of the numbers

$$f(a), f(a+1), \dots, f(a+n-1)$$

has at least k distinct prime divisors, since p_{ij} divides $f(a+i-1)$ for all $1 \leq i, j \leq k$. \square


Homework 28. Let P be a polynomial with integer coefficients such that there are two distinct integers at which P takes coprime values. Show that there exists an infinite set of integers, such that the values P takes at them are pairwise coprime.

Proof.  It suffices to prove that if a_1, a_2, \dots, a_k are integers such that $\gcd(f(a_i), f(a_j)) = 1$ for $1 \leq i \neq j \leq k$ then there is an integer a_{k+1} different from a_1, \dots, a_k such that $\gcd(f(a_{k+1}), f(a_i)) = 1$ for $1 \leq i \leq k$. Take by CRT a_{k+1} such that $a_{k+1} \equiv a_i \pmod{f(a_{i+1})}$ for $1 \leq i \leq k-1$ and $a_{k+1} \equiv a_k \pmod{f(a_1)}$. Then $f(a_{k+1}) \equiv f(a_i) \pmod{f(a_{i+1})}$ for $1 \leq i \leq k$ and $f(a_{k+1}) \equiv f(a_k) \pmod{f(a_1)}$. Thus $\gcd(f(a_{k+1}), f(a_{i+1})) = \gcd(f(a_i), f(a_j)) = 1$ for $1 \leq i < k$ and $\gcd(f(a_{k+1}), f(a_1)) = 1$ as desired. \square

Homework 29. Prove that for any positive integer k , there exists an arithmetic sequence

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \dots, \frac{a_k}{b_k}$$

of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \dots, k$ such that the positive integers $a_1, b_1, a_2, b_2, \dots, a_k, b_k$ are all distinct.

Proof.  Pick primes p_1, p_2, \dots, p_k such that $k < p_k < \dots < p_2 < p_1$ and let x be an integer such that:


$$\begin{aligned} x &\equiv -1 \pmod{p_1} \\ x &\equiv -2 \pmod{p_2} \\ &\vdots \\ x &\equiv -k \pmod{p_k} \end{aligned}$$

Let $M := \prod_{i=1}^k p_i$. By CRT the existence of such $x > M^2$ is guaranteed. Now consider the rational numbers


$$\frac{x}{M}, \frac{x+1}{M}, \dots, \frac{x+k}{M}.$$

Clearly, this sequence of rationals is an arithmetic progression. Moreover put $a_i = \frac{x+i}{p_i}$ and $b_i = \frac{M}{p_i}$. Easy to see that for each $i = 1, 2, \dots, k$, the numerator $x+i$ is divisible by p_i but not by p_j for $j \neq i$. Moreover $a_i > b_i$ and $a_j > a_i$ for all $i < j$. \square

Homework 30. Prove that for each positive integer n , there are pairwise relatively prime integers k_0, k_1, \dots, k_n , all strictly greater than 1, such that $k_0 k_1 \dots k_n - 1$ is the product of two consecutive integers.

Proof.  Follows from 31 for polynomial $t^2 + t + 1$. \square

Homework 31. Find all positive integers n for which there is an integer m such that $2^n - 1 \mid m^2 + 9$.

Proof.  Clearly $n = 1$ is a solution of the problem, so assume from now on that $n \geq 2$. If $2^n - 1 \mid m^2 + 9$ for some integer m , then $2^n - 1$ has no prime divisor $p > 3$ such that $p \equiv 3 \pmod{4}$. On the other hand, if $d > 1$ is an odd integer, then $2^d - 1 \equiv -1 \pmod{4}$ and 3 does not divide $2^d - 1$, thus $2^d - 1$ has a prime factor $p \equiv 3 \pmod{4}$ different from 3. We deduce that n cannot have any odd divisor $d > 1$ (otherwise $2^d - 1 \mid 2^n - 1 \mid m^2 + 9$, contradicting the previous observations) and so n is a power of 2.

Conversely, if n is a power of 2, then n is a solution of the problem. Indeed, write $n = 2^k$ and observe that

$$2^n - 1 = 3 \cdot (2^2 + 1)(2^4 + 1) \dots (2^{2^{k-1}} + 1).$$

Choosing $m = 3a$, it is enough to find a such that

$$(2^2 + 1)(2^4 + 1) \dots (2^{2^{k-1}} + 1) \mid a^2 + 1.$$

Since the Fermat numbers $2^{2^i} + 1$ are pairwise relatively prime (**EXERCISE**), by the Chinese remainder theorem there is an integer a such that $a \equiv 2^{2^i} \pmod{2^{2^i} + 1}$ for $1 \leq i \leq k - 1$. Then

$$a^2 + 1 \equiv 0 \pmod{2^{2^i} + 1}$$


for $1 \leq i \leq k - 1$ and so

$$(2^2 + 1)(2^4 + 1) \dots (2^{2^{k-1}} + 1) \mid a^2 + 1.$$

The solutions of the problem are therefore all powers of 2. \square


Problem 32. Compute

$$\left(\frac{600}{953}\right), \quad \left(\frac{2020^3}{953}\right), \quad \left(\frac{-7000}{757}\right).$$

Proof.  It's obvious. Answers: $-1, 1, 1$. □

Problem 33. Prove that

- -2 is a quadratic residue modulo a prime $p > 2$ iff $p \equiv 1, 3 \pmod{8}$,
- 2 is a quadratic residue modulo a prime $p > 2$ iff $p \equiv \pm 1 \pmod{8}$,
- -3 is a quadratic residue modulo a prime $p > 2$ iff $p \equiv 1 \pmod{6}$,
- 3 is quadratic residue modulo a prime $p > 2$ iff $p \equiv \pm 1 \pmod{12}$.

Proof.  Since all of the above dots are similar we prove only first and third.

Suppose that $\left(\frac{-2}{p}\right) = 1$ i.e.

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = 1.$$

If $p \equiv 5, 7 \pmod{8}$, then $\frac{p^2-1}{8} \equiv 1, 0 \pmod{2}$ and $\frac{p-1}{2} \equiv 0, 1 \pmod{2}$, respectively. Therefore in both cases $\frac{p-1}{2} + \frac{p^2-1}{8}$ is even. Hence $p \equiv 1, 3 \pmod{8}$.

On the other hand if $p \equiv 1, 3 \pmod{8}$, then

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = 1,$$

since $\frac{p-1}{2} + \frac{p^2-1}{8}$ is even.

Suppose that $\left(\frac{-3}{p}\right) = 1$ i.e.

$$(-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right) = 1.$$

If $p \equiv 5 \pmod{6}$, then by quadratic reciprocity

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{2}{3}\right) = (-1) \cdot (-1)^{\frac{p-1}{2}},$$

so

$$1 = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1) \cdot (-1)^{\frac{p-1}{2}} = -1,$$

contradiction.


On the other hand if $p \equiv 1 \pmod{6}$, then using quadratic reciprocity we get

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{1}{3}\right) = 1.$$


□

Homework 32. Let $p > 2$ be a prime. Compute

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \dots + \left(\frac{p-1}{p}\right).$$

Proof.  There are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p so the statement follows. \square

Homework 33. Prove that if $p \equiv 1 \pmod{4}$, then the sum of quadratic residues \pmod{p} in $\{0, 1, \dots, p-1\}$ is $\frac{p(p-1)}{4}$.

Proof.  Since $p \equiv 1 \pmod{4}$, easy to see that $\left(\frac{-1}{p}\right) = 1$, therefore if $\left(\frac{k}{p}\right) = 1$ then $\left(\frac{p-k}{p}\right) = 1$, too. Thus we can split all $\frac{p-1}{2}$ quadratic residues modulo p into $\frac{p-1}{4}$ pairs of quadratic residues with sum p . Therefore the sum of them is $\frac{p(p-1)}{4}$. \square

Homework 34. Let $x_1 = 7$ and

$$x_{n+1} = 2x_n^2 - 1, \quad \text{for } n \geq 1.$$

Prove that 2003 does not divide any term of the sequence.

Proof.  Note that 2003 is prime number. Suppose that $2003 \mid x_{n+1}$ for some n . Then


$$2x_n^2 \equiv 1 \pmod{2003} \implies (2x_n)^2 \equiv -2 \pmod{2003}.$$

Therefore $\left(\frac{-2}{2003}\right) = 1$, but

$$\left(\frac{-2}{2003}\right) = (-1)^{\frac{2003^2-1}{8}} = (-1)^{501501} = -1,$$

contradiction. \square

Homework 35. 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

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

□

Homework 36. Prove that number $2^n + 1$ does not have prime divisor of the form $8k - 1$.

Proof.  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

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


so $\left(\frac{-1}{p}\right) = 1$ i.e. $(-1)^{\frac{8k-1-1}{2}} = 1$ – contradiction.

Now, assume that n is odd. Then

$$-2 \equiv \left(2^{\frac{n+1}{2}}\right)^2 \pmod{p},$$

so $\left(\frac{-2}{p}\right) = 1$ – contradiction with problem 33. □

Problem 34. Let $p \equiv 1 \pmod{4}$ be a prime and let $p = a^2 + b^2$ with a odd. Prove a is quadratic residue modulo p .

Proof.  It suffices to prove that for any prime divisor q of a we have $\left(\frac{q}{p}\right) = 1$. But from reciprocity law it follows that


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

□

Problem 35. Suppose that for some prime p and integers a, b, c the following are true

$$6 \mid p + 1, \quad p \mid a + b + c, \quad p \mid a^4 + b^4 + c^4.$$

Prove that $p \mid a$, $p \mid b$ and $p \mid c$.

Proof.  Suppose that $p \nmid c$. Then


$$p \mid (b+c)^4 + b^4 + c^4 = 2(b^2 + bc + c^2)^2 \implies p \mid b^2 + bc + c^2 \implies p \mid (2b+c)^2 + 3c^2 \implies \left(\frac{-3}{p}\right) = 1.$$

Moreover using reciprocity law and the condition $6 \mid p+1$ we have that

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

contradiction. \square

Problem 36. Let c be an integer which is not perfect square. Then, there exists a prime $p > 2$ such that $\left(\frac{c}{p}\right) = -1$.

Proof.  WLOG assume that c is square-free 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 $2 \leq i \leq n$. From CRT and Dirichlet's Theorem we find prime p such that

$$\begin{cases} p \equiv r_1 \pmod{p_1} \\ p \equiv r_2 \pmod{p_2} \\ \dots \\ p \equiv r_n \pmod{p_n} \\ p \equiv 1 \pmod{4}. \end{cases}$$

Observe that

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

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 $2 \leq i \leq n$. Using again CRT 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 $2 \leq i \leq n$. 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 $\left(\frac{2}{p}\right) = -1$. Hence

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

□


Problem 37. Let a and b be integers such that $a \neq 0$ and the number $3 + a + b^2$ is divisible by $6a$. Prove that a is negative.

Proof.  Suppose that $3 + a + b^2 = 6ak$, then $3 + b^2 = a(6k - 1)$. Suppose that a is positive, therefore $6k - 1$ is also positive and so k is positive. Then $6k - 1$ 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. □

Problem 38. Prove that for any positive integer n every prime divisor p of number

$$n^4 - n^2 + 1$$

is of the form $12k + 1$.


Proof.  Observe that

$$n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2 \quad \text{and} \quad n^4 - n^2 + 1 = (n^2 + 1)^2 - 3n^2.$$

First equality gives that $p \equiv 1 \pmod{4}$ (because $\left(\frac{-1}{p}\right) = 1$) and second one gives $p \equiv \pm 1 \pmod{12}$, since $\left(\frac{3}{p}\right) = 1$. □

Problem 39. Suppose that $p \equiv 1 \pmod{3}$ is a prime. Using Thue's lemma prove that there exists integers $0 < x, y < \sqrt{p}$ such that $p \mid 3x^2 + y^2$. Conclude that there are integers a, b such that

$$p = a^2 + ab + b^2.$$

Proof.  If $p \equiv 1 \pmod{3}$, then $\left(\frac{-3}{p}\right) = 1$, so $-3 \equiv n^2 \pmod{p}$, for some n . Hence from Thue's lemma we see that there are integers $0 < x, y < \sqrt{p}$ such that $nx \equiv \pm y \pmod{p}$, so

$$-3x^2 \equiv (nx)^2 \equiv y^2 \pmod{p} \implies p \mid 3y^2 + x^2.$$

But

$$0 < 3y^2 + x^2 < 3(\sqrt{p})^2 + (\sqrt{p})^2 = 4p,$$

so $3y^2 + x^2 \in \{p, 2p, 3p\}$.

(1) If $p = 3y^2 + x^2$, then

$$p = (y - x)^2 + (y - x) \cdot 2x + (2x)^2,$$

so we can take $a := y - x$ and $y := 2x$.

(2) If $2p = 3y^2 + x^2$, then y and x have the same parity, so $4 \mid 3y^2 + x^2 = 2p$, contradiction.

(3) If $3p = 3y^2 + x^2$, then $3 \mid x$, so $x = 3x_1$ and hence $p = y^2 + 3x_1^2$ – this is the first case (1).

□

References

- Art of Problem Solving - <https://artofproblemsolving.com>
- Polish Mathematical Olympiad - <https://om.mimuw.edu.pl>
- Homepage of Dominik Burek - <http://dominik-burek.u.matinf.uj.edu.pl>