March camp 2019 - Number Theory

Dominik Burek

1. Exponent (L2 only)

Problem 1. Prove the identity

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

for all positive integers a,b,c.

Proof. For an arbitrary prime p, suppose the exponent on 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 on p in the prime factorization of the LHS is

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

while the exponent on p in the prime factorization 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. □

Problem 2. Suppose that a,b,c are positive integers such that a^b divides b^c, and a^c divides c^b. Prove that a^2 divides bc.

Proof. The condition implies that for any prime p, we have $b\cdot\nu_p(a)\leq c\cdot\nu_p(b)$ and $c\cdot\nu_p(a)\leq b\cdot\nu_p(c)$. Hence,

$$\nu_p(bc)=\nu_p(b)+\nu_p(c)\geq\left(\frac{b}{c}+\frac{c}{b}\right)\nu_p(a)\geq 2\nu_p(a).$$

This means that $a^2\mid bc$. □

Problem 3. Let a,b,c be positive integers such that

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

are integers and $\gcd(a,b)=\gcd(b,c)=\gcd(c,a)=d$. Prove that

$$d\geq\sqrt{2\min\{a,b,c\}}.$$

Proof. Let $a\geq b\geq c$, $a=dx$, $b=dy$ and $c=dz$. Thus, $\gcd(x,y)=\gcd(x,z)=\gcd(y,z)=1$, $x\geq y\geq z$ and we need to prove that $d\geq 2z$. Indeed, since

$$\frac{ab}{a+b}=\frac{dxy}{x+y}\in\mathbb{N}$$

and $\gcd(xy, x+y) = 1$, we obtain that $x + y$ divides d, which gives

$$d \geq x + y \geq 2z.$$

□

Problem 4. Let $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$ be positive integers such that $\gcd(a_i, b_i) = 1$ for all $i \in \{1, 2, \dots, k\}$. Let $m = \operatorname{lcm}(b_1, b_2, \dots, b_k)$. Prove that

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

Proof. For arbitrary prime p, let $v_p(a_i) = c_i$, $v_p(b_i) = d_i$. We have $\min(c_i, d_i) = 0$ for each i. Let $m' = \max(d_1, d_2, \dots, d_k)$. We must show $\min(c_1 - d_1 + m', c_2 - d_2 + m', \dots, c_k - d_k + m') = \min(c_1, c_2, \dots, c_n)$. We consider the following 2 cases:

- $c_i = 0$ for some i. Then $RHS = 0$. If $m' = 0$, then we are done; otherwise, consider d_j such that $d_j = m'$. Then $c_j = 0$, so $c_j - d_j + m' = 0$, so $LHS = 0$.
- $c_i \neq 0$ for all i. Then $d_i = 0$ for all d_i, so both sides are equal. Extending this argument to all primes, we see that the prime factorization of both sides are equal, so we are done.

□

Problem 5. Let a, b, c, d be positive integers such that $ab = cd$. Prove that

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

Proof. Let p be any prime, and let $p^{a'} \parallel a$, and define b', c', d' similarly. We have $a' + b' = c' + d'$, and now wish to show $\min(a', c') + \min(a', d') = a' + \min(a', b', c', d')$. WLOG, we may let $c' \leq d'$. Then we have 3 cases: Case 1: $a' \leq c' \leq d'$. Since $b' = c' + d' - a' \geq a' + a' - a' = a'$, we have $\min(a', b', c', d') = a'$. Then both sides are equal to $2a'$. Case 2: $c' \leq a' \leq d'$. Then $LHS = a' + c'$, and $RHS = a' + \min(a', b', c', d') = a' + \min(b', c')$. Suppose that $b' < c'$. Then $b' + a' \leq b' + d' < c' + d'$, contradiction. Thus, $\min(b', c') = c'$, and $RHS = a' + c'$. Case 3: $c' \leq d' \leq a'$. Then $LHS = c' + d'$, and $RHS = a' + \min(b', c')$. Suppose that $b' > c'$. Then $a' + b' \geq d' + b' > d' + c'$, contradiction. Thus, $\min(b', c') = b'$, and $RHS = a' + b' = LHS$. Applying this argument for all primes, we see that each side has the same prime factorization, so they are equal. □

Problem 6. Let m, n be a positive integers such that

$$\operatorname{lcm}(m, n) + \gcd(m, n) = m + n.$$

Prove that either $m \mid n$ or $n \mid m$.

Proof. Let $a = gcd(m, n)$, $b = lcm(m, n)$. We know $ab = mn$ and so $a + b = m + n$. Hence

$$a + b = m + \frac{ab}{m} \iff (m - a)(m - b) = 0.$$

WLOG $m = a$, then $n = b$ and the conclusion follows. □

Problem 7. Let a_1, b_1, c_1 be natural numbers. We define

$$a_2 = \gcd(b_1, c_1), \qquad b_2 = \gcd(c_1, a_1), \qquad c_2 = \gcd(a_1, b_1),$$

and

$$a_3 = \operatorname{lcm}(b_2, c_2), \qquad b_3 = \operatorname{lcm}(c_2, a_2), \qquad c_3 = \operatorname{lcm}(a_2, b_2).$$

Show that $\gcd(b_3, c_3) = a_2$.

Proof. Let $(a_1, b_1, c_1) = g$ with $a_1 = xg, b_1 = yg, c_1 = zg$ with $(x, y, z) = 1$. Let $(x, y) = d$, let $(y, z) = e$, let $(z, x) = f$. Note that $(d, e) = (e, f) = (f, d) = 1$, so $x = adf$, $y = bde$, $z = cef$ for some a, b, c. Note that $(a, b) = (a, c) = (a, e) = (b, c) = (b, f) = (c, d) = 1$.

Then $a_1 = adfg$, $b_1 = bdeg$, $c_1 = cefg$. So $a_2 = eg$, $b_2 = fg$, $c_2 = dg$. Then $a_3 = dfg$, $b_3 = deg$, $c_3 = efg$. Then $\gcd(b_3, c_3) = eg = a_2$. □

2. Divisibility

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

$$\operatorname{lcm}(a, b) \neq \operatorname{lcm}(a + c, b + c).$$

Proof. Suppose we do find a, b, c admitting the equality. We prove that $\gcd(a, b) \mid c$. Indeed; pick p^e to be a maximal prime power divisor of $d = \gcd(a, b)$. Then

$$\begin{aligned} \max\{v_p(a + c), v_p(b + c)\} &= v_p\left(\operatorname{lcm}(a + c, b + c)\right) \\ &= v_p\left(\operatorname{lcm}(a, b)\right) \geq e \end{aligned}$$

so $p^e \mid a + c$ or $p^e \mid b + c$. Either way, $p^e \mid c$; proving the claim.

Let $a = dx, b = dy, c = dz$ with $(x, y) = 1$. Suppose $q \mid x + z, q \mid y + z$ is a prime number. Then $q \mid xy = \operatorname{lcm}(x + z, y + z)$ so $q \mid x$ and $q \mid y$; contradiction! Hence, $\gcd(x + z, y + z) = 1$. So

$$\begin{aligned} xy &= \operatorname{lcm}(x + z, y + z) \\ &= \frac{(x + z)(y + z)}{\gcd(x + z, y + z)} \\ &= (x + z)(y + z) \end{aligned}$$

clearly false! □

Problem 9. Let x, y be a positive integers, such that $x^2 - 4y + 1$ is a multiple of $(x - 2y)(1 - 2y)$. Prove that $|x - 2y|$ is a square number.

Proof. Let $a = x - 2y \neq 0$ (otherwise all is trivial) and $b = 2y - 1$. Then

$$x^2 - 4y + 1 = (a + b + 1)^2 - 2b - 1 = a^2 + b^2 + 2ab + 2a.$$

Hence, the number

$$t = \frac{a^2 + b^2 + 2a}{ab}$$

must be integer. Particularly, $a \mid b^2$. Let $a = c^2 f$, where c and f are non-zero integers and f is square-free. Then $b = cfd$ for some integer d. Now rewrite t as

$$t = \frac{c^4 f^2 + c^2 f^2 d^2 + 2c^2 f}{c^3 f^2 d} = \frac{c^2 f + f d^2 + 2}{cfd}$$

From it, $f \mid 2$. But f is odd because so is b, so $f = \pm 1$ and $a = \pm c^2$. □

Problem 10. 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 perfect squares. □

Problem 11. Let $a_1, a_2, \ldots, a_n$ be positive integers with product P, where n is an odd positive integer. Prove that
$$\gcd(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \leq 2\gcd(a_1, \ldots, a_n)^n.$$

Proof. Suppose $\gcd(a_1, a_2, \cdots, a_n) = x$, and set $b_1 = \frac{a_1}{x}, b_2 = \frac{a_2}{x}, \cdots, b_n = \frac{a_n}{x}$. Clearly $\gcd(b_1, \cdots, b_n) = 1$.

Note that this means $a_i^n + P = a_i^n + a_1a_2 \cdots a_n = x^n(b_i^n + b_1b_2 \cdots b_n)$, so
$$\gcd(a_1^n + P, \cdots, a_n^n + P) = x^n \gcd(b_1^n + b_1b_2 \cdots b_n, \cdots, b_n^n + b_1b_2 \cdots b_n).$$
To prove the given inequality, we need to show
$$\gcd(b_1^n + b_1b_2 \cdots b_n, \cdots, b_n^n + b_1b_2 \cdots b_n) \leq 2.$$
Let $d := \gcd(b_1^n + b_1b_2 \cdots b_n, \cdots, b_n^n + b_1b_2 \cdots b_n)$; we claim that d is relatively prime of each of the b_i's. To see this, note that if there a b_i and a prime p so that $p \mid b_i$ and $p \mid d$, then $p \mid b_1b_2 \cdots b_n$, and since $p \mid d \mid b_j^n + b_1 \cdots b_n$, we have $p \mid b_j^n \implies p \mid b_j$, implying that p divides each of the b_i's. This contradicts $\gcd(b_1, \cdots, b_n) = 1$.

Now for $1 \leq i \leq n$, we have
$$d \mid b_i^n + b_1b_2 \cdots b_n \implies b_i^n \equiv -b_1b_2 \cdots b_n \pmod{d}.$$
Multiplying these congruences for $1 \leq i \leq n$, and noting that n is odd we have
$$(b_1b_2 \cdots b_n)^n \equiv -(b_1b_2 \cdots b_n)^n \pmod{d} \implies d \mid 2(b_1b_2 \cdots b_n)^n.$$
But since d is relatively prime to $b_1, \cdots, b_n$, this implies $d \mid 2 \implies d \leq 2$, as required. □

Example 12. Let $a, b, c \in \mathbb{N}$ with $\gcd(a^2 - 1, b^2 - 1, c^2 - 1) = 1$. Prove that,
$$\gcd(ab + c, bc + a, ca + b) = \gcd(a, b, c)$$

Proof. Let
$$G = \gcd(ab + c, bc + a, ca + b) = \gcd(ab + c, (b - 1)(c - a), (a - 1)(c - b)).$$
Since
$$\gcd(ab + c, b - 1, a - 1) = \gcd(c + 1, b - 1, a - 1) = 1 \text{ and}$$
$$\gcd(ab + c, c - a, a - 1) = \gcd(b + 1, c - 1, a - 1) = 1,$$

and symmetry of a, b, we have

$$G = \gcd(ab + c, c - a, c - b) = \gcd(a(b + 1), c - a, c - b).$$

Moreover

$$\gcd(b + 1, c - a, c - b) = \gcd(b + 1, a + 1, c + 1) = 1,$$

so we have $G = \gcd(a, c - a, c - b)$, which implies $G = \gcd(a, b, c)$. ☐

Problem 13. Let m, n be distinct positive integers. Prove that

$$\gcd(m, n) + \gcd(m + 1, n + 1) + \gcd(m + 2, n + 2) \leq 2|m - n| + 1.$$

Further, determine when equality holds.

Proof. WLOG $m > n$. Let $k = m - n$, we have

$$LHS = \gcd(m, k) + \gcd(m + 1, k) + \gcd(m + 2, k)$$

and $RHS = 2k + 1$.

If $k = 1, 2$, then inequality is obvious.

If $k > 2$, not all of the gcd's are equal to k. Therefore

$$\gcd(m, k) + \gcd(m + 1, k) + \gcd(m + 2, k) \leq k + \frac{k}{2} + \frac{k}{2} < 2k + 1.$$

Equality holds for consecutive m, n; $m - n = 2$ or $n - m = 2$ and m, n even. ☐

Problem 14. Let a, b, c be a non-zero integers such that

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$$

is integer. Prove that abc is a perfect cube.

Proof. Take any prime p. Let $x = v_p(a)$, $y = v_p(b)$ and $z = v_p(c)$. It is enough to prove that $3 \mid x + y + z$. If no two of $2x + z$, $2y + x$, $2z + y$ are equal then

$$v_p(a^2c + b^2a + c^2b) = \min\{2x + z, 2y + x, 2z + y\} := m$$

. Since $p^{x+y+z} \mid abc$, we have $m \geq x + y + z$ and

$$3(x + y + z) = (2x + z) + (2y + x) + (2z + y) \geq m + (m + 1) + (m + 2) > 3m,$$

contradiction.

Therefore we may assume that $2x + z = 2y + x$, then

$$x + y + z = x + y + z - (2x + z) + (2y + x) = 3y$$

is divisible by 3. ☐

Problem 15. Let a and b be a positive integers such that

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

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

Proof. Let $d = \gcd(a, b)$, then $a = a_1 d$ and $b = b_1 d$ where $\gcd(a_1, b_1) = 1$. Thus $\operatorname{lcm}(a, b) = da_1 b_1$ so the given identity can be written as $a_1 b_1 = d(a_1 - b_1)$. Therefore $a_1 \mid d$ and $b_1 \mid d$. Thus $a_1 b_1 \mid d$, so $a_1 - b_1 = 1$ and $d = a_1 b_1$. Hence

$$\operatorname{lcm}(a, b) = da_1 b_1 = d^2 = \gcd(a, b)^2.$$

□

Problem 16. Let x, y, z be pairwise different positive integers such that

$$\operatorname{lcm}(x, y) - \operatorname{lcm}(x, z) = y - z.$$

Prove that $x \mid y$ and $x \mid z$.

Proof. We see that $y - z = kx$ for some integer k. Then

$$\operatorname{lcm}(x, y) = \frac{xy}{\gcd(x, y)} = \frac{xy}{\gcd(x, z + kx)} = \frac{xy}{\gcd(x, z)}.$$

Since

$$\operatorname{lcm}(x, z) = \frac{xz}{\gcd(x, z)},$$

we can rewrite the equation as

$$\frac{x(y - z)}{\gcd(x, z)} = y - z.$$

Since $y \neq z$ we deduce that $x = \gcd(x, z)$ and so $x \mid z$. Since $x \mid y - z$, we conclude $x \mid y$. □

Problem 17. Find all positive integers which can be written as $\operatorname{lcm}(a, b) + \operatorname{lcm}(b, c) + \operatorname{lcm}(c, a)$ for some positive integers a, b, c.

Proof. Clearly if we can write n in such a way then $2n$ also. By choosing $b = c = 1$ we see that all odd integers satisfies problem assumptions.

Suppose that

$$2^k = \operatorname{lcm}(a, b) + \operatorname{lcm}(b, c) + \operatorname{lcm}(c, a),$$

then $k > 1$. Take $a = 2^A a_1$, $b = 2^B b_1$ and $c = 2^C c_1$ with $A \geq B \geq C$ and odd a_1, b_1, c_1. Then

$$2^k = 2^A(\operatorname{lcm}(a_1, b_1) + \operatorname{lcm}(a_1, c_1)) + 2^B \operatorname{lcm}(b_1, c_1).$$

Dividing by 2^B we wil lhave contradiction by dfferent parity of both sides. □

Example 18. Does there exist any integer a, b, c such that $a^2bc + 2$, $ab^2c + 2$, $abc^2 + 2$ are perfect squares?

Proof. If any of a, b, c is even, one of these is $2 \pmod 4$ which is impossible. So, all are odd. Therefore, a^2, b^2, c^2 are all $1 \pmod 4$ and also, the given square numbers are odd. So, $bc + 2$, $ca + 2$, $ab + 2$ all are $2 \pmod 4$. Therefore, ab, bc, ca are all $3 \pmod 4$. So,

$$(abc)^2 = (ab)(bc)(ca) \equiv 3^3 \equiv 3 \pmod 4,$$

contradiction. □

3. Integer sequences

Example 19. An integer sequence $\{a_n\}_{n\geq 1}$ is defined by

$$a_1 = 2,\ a_{n+1} = \left\lfloor \frac{3}{2} a_n \right\rfloor.$$

Show that it has infinitely many even and infinitely many odd integers.

Proof. Consider two cases:

(1) Let us suppose that the set of odd integers in a_n is finite. It means that there is an m so that for all $n \geq m$, a_n is even. Then for all $n \geq m$

$$a_{n+1} = \frac{3}{2} a_n \quad \text{so} \quad a_{m+k} = \left(\frac{3}{2}\right)^k a_m.$$

But if r is the greatest number such that $2^r \mid a_m$ then a_{m+r+1} is not an integer – contradiction!

(2) Now suppose that the set of even numbers in a_n is finite. That means we can find an m so that for all $n \geq m$, a_n is odd, which means that all the numbers $b_n = a_n - 1$ are even integers. Then for all $n \geq m$

$$a_{n+1} = \frac{3a_n - 1}{2} = \frac{3}{2}(a_n - 1) + 1 \quad \text{so} \quad b_{n+1} = \frac{3}{2} b_n,$$

but this case was discussed above.

□

Example 20. Determine all positive integers M such that the sequence $a_0, a_1, a_2, \ldots$ defined by

$$a_0 = M + \frac{1}{2} \qquad \text{and} \qquad a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{for} \quad k = 0, 1, 2, \ldots$$

contains at least one integer term.

Proof. The answer is all $M > 1$. Clearly $M = 1$ fails, as the sequence is just going to be all $\frac{3}{2}$. To show that all $M > 1$ work, we induct on $v_2(M-1)$. If $v_2(M-1) = 0$, then M is even, and we have that $a_1 = M\left(M + \frac{1}{2}\right)$ is an integer as desired. If $v_2(M-1) = k > 0$, then

$$a_1 = M\left(M + \frac{1}{2}\right) = \frac{2M^2 + M - 1}{2} + \frac{1}{2} =: N + \frac{1}{2},$$

and

$$v_2(N-1) = v_2\left(\frac{2M^2 + M - 3}{2}\right) = v_2\left(\frac{(2M+3)(M-1)}{2}\right) = k - 1,$$

so we can shift the sequence and reduce to the case of $v_2(M-1) = k-1$. Hence, a_{k+1} will be an integer as desired. □

3.1. Kobayashi Theorem.

Theorem 21 (Kobayashi Theorem)**.** *If the set of prime divisors of the terms of an unbound sequence $(a_n)_{n\geq 1}$ is finite, then the set of prime divisors of the terms of any translate $(a_n + t)_{n\geq 1}$, for $0 \neq t \in \mathbb{Z}$, is infinite.*

Proof. Let $p_1, p_2, \ldots, p_s$ be the prime factors of the terms of the initial sequence, and assume only finitely many prime factors $q_1, q_2, \ldots, q_r$ exist for the terms of the translated sequence (these sets may overlap). For any positive integer N using primes from the union of these sets, consider the largest cube K^3 dividing it, so $N = M \cdot K^3$, where M is made of (some of) those primes, at exponents 1 or 2, therefore may only take finitely many values.

But now the equation $(a_n + t) = a_n + t$ writes as $Ax^3 = By^3 + t$, with A, B taking finitely many values. According to Thue's result (HIGH END FACT), each of these equations has finitely many solutions. But this is in disaccord with the fact that the sequences are infinite, and, being unbounded, provide infinitely many solutions. ☐

Problem 22. Let a be a fix natural number . Prove that the set of prime divisors of $2^{2^n} + a$ for $n = 1, 2, \ldots$ is infinite.

Proof. Obvious from Kobayashi theorem. ☐

Proof. Assume that this set be finite i.e there exist $p_1, p_2, \cdots p_k$ which they are all the prime divisor of $2^{2^n} + a$. Now consider numbers

$$a^2 + a,\ a^4 + a,\ \ldots a^{2^k} + a$$

and assume r is a number such that none of this number is divisible by p_i^r for all $i = 1, 2, \ldots, k$

We know if n is sufficiently large then if we factorize $2^{2^n} + a$ by $p_1, p_2, \cdots p_k$ one of this prime number has a power bigger than r. Thus if we consider $k+1$ consecutive number n which are sufficient big then by Pigeonhole theorem there exist two of this number which one of these prime number (for example) p_1 has a power bigger than r in both. Therefore $p_1^r \mid 2^{2^u} + a$ and $p_1^r \mid 2^{2^{u+s}} + a$, for $1 \leq s \leq k$. Thus $p_1^r \mid a^{2^s} + a$ - contradiction. ☐

Problem 23. Define the sequence of integers a_n $n \geq 0$ such that a_0 is equal to an integer $a > 1$ and $a_{n+1} = 2^{a_n} - 1$. Let A be the set such that x belongs to A if and only if x is a prime and x divides a_n for some $n \geq 0$. Show that the number of elements of A is infinite.

Proof. Apply Kobayashi theorem to the set $\{2^{a_n} \mid n \geq 0\} - 1$. ☐

Problem 24. Fedya writes from left to right an infinite sequence of nonzero digits. After every digit, he considers the prime factors of the natural number that is written until this moment. Prove that sooner or later one of these prime numbers will be > 100.

Proof. Suppose the digit k was used infinitely many times, then we consider the subsequence of natural numbers $\{a_n\}$, but by Kobayashi one of

$$\{a_n\}, \quad \left\{\frac{a_n - k}{10}\right\}$$

has infinitely many prime factors, therefore the original sequence has infinitely many prime factors. ☐

Problem 25. Let m, n be positive integer numbers. Prove that there exist infinite many couples of positive integer nubmers (a, b) such that

$$a + b \mid am^a + bn^b, \quad \gcd(a, b) = 1.$$

Proof. Consider the sequence $a_k = (mn)^k - n$. By Kobayashi's theorem, the set of prime divisor of this sequence is infinite. Pick any prime that divides a_k i.e. $p \mid (mn)^k - n$ but not divides either m or n. Set $k = r(p-t)+1$, then

$$(mn)^k = (mn)^{r(p-1)+t} \equiv (mn)^t \pmod{p}.$$

Then, $t < p$. Now set $a = t$, $b = p - t$ ($a + b = p$, so we can make sure that $(a, b) = 1$), and them we have $p \mid (mn)^t - n$, so $p \mid (mn)^a - n^p = n^a(m^a - n^b)$. Thus $a + b = p \mid m^a - n^b$

Therefore $m^a \equiv n^b \pmod{a+b}$. From here we have

$$am^a + bn^b \equiv am^a + bm^a \equiv m^a(a+b) \equiv 0 \pmod{a+b}.$$

so we are done. □

Problem 26. Let us consider positive integers $p \neq q$. Prove that there are finitely many pairs $(n + p, n + q)$ such that both terms only have prime divisors from a finite set P of primes.

Proof. Aassume there are infinitely many such pairs, for indices n equal to $n_1, n_2, \ldots$. Then the terms of the unbounded sequence $(n_k + p)_{k \geq 1}$ only have prime divisors from the finite set P. By the Kobayashi theorem, there are infinitely many primes dividing at least one term of the translated sequence $(n_k + q = (n_k + p) + (q - p))_{k \geq 1}$, contradiction. □

4. Polynomials in $\mathbb{Z}[X]$

4.1. $a - b \mid P(a) - P(b)$ trick.

Problem 27. Let $W(x)$ be a polynomial with integer coefficients such that there are two distinct integer at which W takes coprime values. Prove that there exists an infinite set of integers such that the values W takes at them are pairwise coprime.

Proof. Let these two integers be a, b, then by the *Chinese Remainder Theorem* we can find X such that

$$X \equiv a \pmod{W(b)}, \quad X \equiv b \pmod{W(a)},$$

then obviously $W(X) \equiv W(a) \pmod{W(b)}$ and it's the same for $W(a)$ which implies that $W(X)$ is relatively prime to both $W(a)$ and $W(b)$. Now we can use again *Chinese Remainder Theorem* and proceed inductively. □

Problem 28. Let $f \in \mathbb{Z}[X]$. Prove that there are no $n \geq 3$ distinct integers $x_1, x_2, \ldots, x_n$ such that $f(x_i) = x_{i-1}$ for $i \in \{1, 2, \ldots, n\}$ (we put $x_0 := x_n$).

Proof. Suppose that such numbers exist. Then

$$x_i - x_{i-1} = f(x_{i+1}) - f(x_i)$$

is divisible by $x_{i+1} - x_i$ for $i \in \{1, 2, \dots, n\}$ (we put $x_{n+1} := x_1$). In particular

$$|x_1 - x_n| \geq |x_2 - x_1| \geq |x_3 - x_2| \geq \ldots \geq |x_{n-1} - x_n| \geq |x_n - x_1|$$

. Since the first and last numbers are equal then

$$|x_i - x_{i-1}| = |x_{i+1} - x_i| \text{ for } i \in \{1, 2, \dots, n\}.$$

Now, observe that

$$\sum_{i=1}^{n} (x_{i+1} - x_i) = 0,$$

so we can find $j \in \{1, 2, \dots, n-1\}$ such that $x_{j+1} - x_j$ and $x_{j+2} - x_{j+1}$ have different signs. By the above equality we have $x_{j+1} - x_j = -(x_{j+2} - x_{j+1})$ — thus $x_j = x_{j+2}$, contradiction. □

Problem 29. Find all polynomials $f \in \mathbb{Z}[X]$ such that $f(n) \mid 2^n - 1$ for any positive integer n.

Proof. Let $p \mid f(n)$ be a prime. Then

$$p = n + p - p \mid f(n+p) - f(n),$$

so $p \mid f(n+p)$. Hence $p \mid 2^n - 1$ and $p \mid 2^{n+p} - 1$ so $p \mid 2^p - 1$ ($p \neq 2$). But we know that $p \mid 2^p - 2$ – contradiction. □

Problem 30. Let $f \in \mathbb{R}[X]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$. Prove that there are $a_0, a_1, \dots, a_n$ such that for any real x the following equality holds

$$f(x) = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \ldots + a_1 \binom{x}{1} + a_0.$$

Proof. We induct on degree n of f. For $n = 1$ it is obvious, assume $n > 1$. Consider polynomial

$$g(x) := f(x+1) - f(x).$$

We see that $g(\mathbb{Z}) \subseteq \mathbb{Z}$ and $\deg g = n - 1$. From the induction assumption we find integers $a_0, a_1, \dots, a_{n-1}$ such that

$$f(x+1) - f(x) = g(x) = a_{n-1} \binom{x}{n-1} + a_{n-2} \binom{x}{n-2} + \ldots + a_1 \binom{x}{1} + a_0.$$

Fix $m \in \mathbb{Z}$ and notice that

$$f(m) = f(0) + g(1) + g(2) + \ldots + g(m-1). \tag{1}$$

Using (1) and well known identity

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{m-1} = \binom{n+1}{m} \text{ for } m, n \in \mathbb{N}$$

we see that

$$f(x) = a_{n-1} \binom{x}{n} + a_{n-2} \binom{x}{n-1} + \ldots + a_0 \binom{x}{1} + f(0) \text{ for } x \in \mathbb{Z}.$$

Since the last equality holds for infinitely many arguments, it holds for any real argument. □

Problem 31. Let $f \in \mathbb{R}[X]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$. Prove that for any integers m and n the number

$$\operatorname{lcm}\{1, 2, \ldots, \deg(f)\} \cdot \frac{f(m) - f(n)}{m - n}$$

is integer.

Proof. Assume $\deg f = \ell$. Taking $g(x) := f(x + \ell)$ we see that $\deg g = \ell$, $g \in \mathbb{Q}[X]$ and $g(\mathbb{Z}) \subseteq \mathbb{Z}$. It is enough to prove that

$$\operatorname{lcm}\{1, 2, \ldots, \ell\} \cdot \frac{g(d) - g(0)}{d}$$

is integer, for $d := m - \ell$.

By the above problem there are integers $a_1, a_2, \ldots, a_n$ such that

$$g(x) = a_\ell \binom{x}{\ell} + a_{\ell-1} \binom{x}{\ell - 1} + \ldots + a_1 \binom{x}{1} + a_0,$$

thus it is enough to show that

$$\operatorname{lcm}\{1, 2, \ldots, \ell\} \cdot \frac{1}{d} \binom{d}{i}$$

is integer for $i \in \{1, 2, \ldots, \ell\}$. But

$$\operatorname{lcm}\{1, 2, \ldots, \ell\} \cdot \frac{1}{d} \binom{d}{i} = \frac{\operatorname{lcm}\{1, 2, \ldots, \ell\}}{i} \cdot \binom{d-1}{i-1} \in \mathbb{Z}.$$

□

Problem 32. Let $f \in \mathbb{Z}[X]$ with $\deg f = n$. Suppose that d divides $f(1), f(2), \ldots, f(n)$. Prove that $d \mid n!$.

Proof. Applying problem 30 to polynomial $g(x) := \dfrac{f}{d}$ we are done. □

Problem 33. Let $a_1, a_2, \ldots, a_n$ be different positive integers such that

$$a_1 a_2 \ldots a_n \mid (k + a_1)(k + a_2) \ldots (k + a_n) \quad \text{for } k \geq 1.$$

Prove that

$$\{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, n\}.$$

Proof. Applying problem 32 to polynomial

$$f(x) = (x + a_1)(x + a_2) \ldots (x + a_n)$$

we see that

$$a_1 a_2 \ldots a_n \mid n!.$$

Since $a_1, a_2, \ldots, a_n$ are different positive integers we are done. □

4.2. Prime divisors of polynomials.

Problem 34. Suppose that $f \in \mathbb{Z}[X]$. Prove that the set of primes numbers dividing at least one term of a sequance $(P(n))_{n\geq 1}$ is infinite.

Proof. Let $\{p_1, p_2, \ldots, p_n\}$ 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 $A = p_1 p_2 \ldots p_n$, then $f(A)$ has a prime divisor outside the set $\{p_1, p_2, \ldots, p_n\}$ – contradiction. □

Problem 35. Suppose that $f \in \mathbb{Z}[X]$ and $(a_n)_{n\geq 1}$ is a strictly increasing sequence of positive integers such that $a_n \leq f(n)$ for any n. Prove that the set of primes numbers dividing at least one term of a sequance $(a_n)_{n\geq 1}$ is infinite.

Proof. Notice that for $k = (\deg(f))^{-1} < 1$ we have

$$\sum_{n=1}^{\infty} \frac{1}{(f(n))^k} = \infty.$$

Now, for any finite collection of primes $p_1, p_2, \ldots, p_N$ we have:

$$\sum_{x_1, x_2, \ldots, x_N \geq 0} \frac{1}{p_1^{kx_1} p_2^{kx_2} \ldots p_N^{kx_N}} = \prod_{j=1}^{N} \sum_{i\geq 0} \frac{1}{p_j^{ki}} = \prod_{j=1}^{N} \frac{p_j^k}{p_j^k - 1} < \infty.$$

If the statement does not hold, ten any term of a sequence $\{a_n\}_{n=1}^{\infty}$ will be of the form $p_1^{kx_1} p_2^{kx_2} \ldots p_N^{kx_N}$ for some $x_i \in \mathbb{Q}$ $(i \in \{1, \ldots, N\})$. Thus

$$\infty = \sum_{n=1}^{\infty} \frac{1}{(f(n))^k} \leq \sum_{n=1}^{\infty} \frac{1}{a_n^k} \leq \sum_{x_1, x_2, \ldots, x_N \geq 0} \frac{1}{p_1^{kx_1} p_2^{kx_2} \ldots p_N^{kx_N}} < \infty.$$

Contradiction. □

5. Thue Lemma

Example 36. Let A be the set of positive integers of the form $a^2 + 2b^2$, where a and b are integers and $b \neq 0$. Show that if p is a prime number and $p^2 \in A$, then $p \in A$.

Proof. Let $p^2 = a^2 + 2b^2$ for some positive integers a and b. Reading the equation modulo p yields $a^2 \equiv -2b^2 \pmod{p}$. Multiplying the inverse of b modulo p we get

$$\left(ab^{-1}\right)^2 \equiv -2 \pmod{p}.$$

Let $ab^{-1} \equiv \alpha \pmod{p}$. From *Thue's Lemma,* we can find a pair (m, n) of integers such that

$$n \equiv \alpha m \pmod{p} \quad \text{and} \quad 0 < |m|, |n| < \sqrt{p}.$$

After squaring the congruence, we have

$$n^2 \equiv \alpha^2 m^2 \equiv -2m^2 \pmod{p}.$$

In other words, $n^2 + 2m^2$ is divisible by p. Since $0 < |m|, |n| < \sqrt{p}$ we see that $0 < n^2+2m^2 < 3p$, thus $n^2+2m^2 \in \{p, 2p\}$. If $p = n^2+2m^2$, then $p \in A$. Otherwise, the relation $2p = n^2 + 2m^2$ implies that n is even, so $p = m^2 + 2\left(\frac{n}{2}\right)^2 \in A$. □

Example 37. Let S be a set of all positive integers which can be represented as $a^2 + 5b^2$ for some coprime integers a, b. Let p be a prime number such that $p = 4n + 3$ for some integer n. Show that if for some positive integer k the number kp is in S, then $2p$ is in S as well.

Proof. From the condition we have property, there exist $x, y \in \mathbb{N}$ such that $p \mid x^2 + 5y^2$ thus $p \mid a^2 + 5$ for $\alpha := xy^{-1} \pmod{p}$.

Using *Thue's lemma* we find integers m, n such that

$$n \equiv \alpha m \pmod{p} \quad \text{and} \quad 0 < |m|, |n| < \sqrt{p}.$$

Therefore

$$n^2 \equiv x^2 y^{-2} m^2 \equiv -5m^2 \pmod{p}, \quad \text{and so} \quad n^2 + 5m^2 \in \{p, 2p, 3p, 4p, 5p\}.$$

Since $4 \nmid n^2+5m^2$ and $5 \nmid n^2+5m^2$, it follows that in fact $n^2+5m^2 \in \{p, 2p, 3p\}$.

(1) If $p = x^2 + 5y^2$ then $p \equiv 1(\mod 4)$ – contradiction.
(2) If $2p = x^2 + 5y^2$ then we are done.
(3) If $x^2 + 5y^2 = 3p$, then we consider the following subcases
- $x \equiv 1 \pmod{3}$, $y \equiv 1 \pmod{3}$, then exist $k, l \in \mathbb{N}$ such that $x = 3k + 1$, $y = 3l + 1$, so
$$\begin{aligned} p &= 3k^2 + 2k + 5(3l^2 + 2l) + 2 \Longrightarrow \\ &\Longrightarrow 2p = 6k^2 + 4k + 10(3l^2 + 2l) + 4 = \\ &= (k + 2 + 5l) + 5(k - l)^2. \end{aligned}$$
- $x \equiv 1 \pmod{3}$, $y \equiv -1(\mod 3)$ then $x = 3k + 1$, $y = 3l - 1$, so
$$2p = (k + 2 - 5l)^2 + 5(k + l)^2.$$
- $x \equiv -1 \pmod{3}$, $y \equiv 1 \pmod{3}$, thus $x = 3k - 1$, $y = 3l + 1$, hence
$$2p = (k - 2 - 5l)^2 + 5(k + 5l)^2.$$
- $x \equiv -1 \pmod{3}$, $y \equiv -1 \pmod{3}$, thus $x = 3k - 1$, $y = 3l - 1$, hence
$$2p = (k - 2 + 5l) + 5(k - 5l)^2$$

□

6. Integer functions, sequences

Problem 38. Let k be a positive integer. Find all functions $f : \mathbb{N} \to \mathbb{N}$ satisfying the following two conditions:
- For infinitely many prime numbers p there exists a positve integer c such that $f(c) = p^k$.
- For all positive integers m and n, $f(m) + f(n)$ divides $f(m + n)$.

Proof. We prove by induction that $f(n) = nf(1)$. Let $c_1, c_2, \ldots,$ be the sequence of naturals such that $f(c_i) = p_i^k$. Then one has

$$f(c_i - (d + 1)) + f(d + 1) \mid f(c_i) = p_i^k$$

and hence $f(c_i - (d+1)) = p_i^j - f(d+1)$ for some natural number $j < k$. By pigeonhole, there are infinitely many i that gives us the same j and hence we can assume that j is fixed since we can just consider that sequence instead. Similarly, one has $f(c_i - k) = p_i^{j'} - f(k)$ for some fixed natural number j'. Now we have

$$f(1) + f(c_i - (d+1)) \mid f(c_i - d) \implies p_i^j - f(d+1) + f(1) \mid p_i^{j'} - f(d).$$

Let $j' = aj + b$ where $0 \leq b < j$. Then our divisibility condition becomes

$$p_i^j - f(d+1) + f(1) \mid (f(d+1) - f(1))^a p_i^b - f(d)$$

but since $b < j$ and $a < k$, the RHS is less than the LHS when p_i is large enough which is a contradiction unless the LHS is zero. In which case one has

$$(f(d+1) - f(1))^a p_i^b = f(d)$$

and so $b = 0$, giving us $(f(d+1) - f(1))^a = f(d)$. On the other hand, one also has

$$f(1) + f(d) \mid f(d+1)$$

giving us

$$(f(d+1) - f(1))^a + f(1) \mid f(d+1).$$

Letting $f(d+1) - f(1) = c$, one has

$$c^a + f(1) \mid c + f(1)$$

which is impossible unless $c^a = c$, in which case either $c = 1$ or $a = 1$. If $c = 1$, then $f(d) = 1$ and $f(1) + f(d-1) \mid f(d)$ is impossible. Thus it must be that $a = 1$ which gives us $f(d+1) = f(d) + f(1)$. By induction, $f(n) = nf(1)$ as desired.

Now clearly any function satisfying $f(n) = nf(1)$ satisfies the second condition. For the first condition, it is clear that one must have $f(1) = 1$. Hence the only solution is $f(n) = n$ for all $n \in \mathbb{N}$. □

Problem 39. Let $\mathbb{Z}_{>0}$ be the set of positive integers. Find all functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such that

$$m^2 + f(n) \mid mf(m) + n$$

for all positive integers m and n.

Proof. Let $m = n$ and we get $m^2 + f(m) \mid mf(m) + m$ so we have

$$m^2 + f(m) \leq mf(m) + m$$

which rearranges to $f(m) \geq m$ for all $m \geq 2$. Now let $m = f(n)$ and we get

$$f(n)^2 + f(n) \mid f(f(n)) \cdot f(n) + n$$

so $f(n) \mid n$ but $f(n) \geq n$, so the only viable possibility is $f(n) = n$ for $n \geq 2$. For $n = 1$, we have $f(1) \mid 1$, so $f(1) = 1$. It is easy to check that $f(n) = n$ satisfies the condition. □

Problem 40. Let $\mathbb{N}$ denote the set of positive integers. Find all functions $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that

$$n + f(m) \mid f(n) + nf(m)$$

for all $m, n \in \mathbb{N}$

Proof. Note that the condition implies $n + f(m) \mid f(n) - n^2$ $(*)$. In particular, $1 + f(1) \mid f(1) - 1$ so $f(1) = 1$. Obviously, $f(n) = n^2$ for all positive integers satisfies the hypothesis, so supppose there is $n_0 \in \mathbb{N}$ such that $f(n_0) \neq n_0^2$. We have that $n_0 + f(m) \mid f(n_0) - n_0^2$, so $f(m) \leq n_0 + f(m) \leq \mid f(n_0) - n_0^2 \mid$, i.e. f is bounded. Take $m = 1$ in the initial relation to get $n + 1 \mid f(n) + n$ or equivalently $n+1 \mid f(n) - 1$ for all positive integers n. However, f is bounded, so we have that $f(n) = 1$ for all n big enough, say $n > N$.

Take $n > N$ in the hypothesis and note that $n + f(m) \mid 1 + nf(m)$ implies $n + f(m) \mid f(m)^2 - 1$. Take n large enough to infer that $f(m) = 1$ for all positive integers m, which indeed is a solution of the problem. □

Problem 41. Let $\mathbb{N}$ denote the set of positive integers. Find all functions $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that

$$n + f(m) \mid f(n) + nf(m)$$

for all $m, n \in \mathbb{N}$.

Proof. First note that $1 + f(1) \mid 2f(1)$ so $f(1) = 1$.

Suppose that there exists an integer k such that $f(k) \neq k^2$. By the condition we have $k + f(m) \mid k^2 - f(k)$ so f is bounded. Furthermore we know that $n+1 \mid f(n)+n$ from $m = 1$ in the condition so $f(n) \equiv 1 \pmod{n+1}$ but since f is bounded we have $f(n) = 1$ for n sufficiently large.

To finish note that $n+f(m) \mid nf(m)+f(m)^2$ so $n+f(m) \mid f(m)^2 - f(n)$. Take a very large n in the previous relationship to get $n + f(m) \mid f(m)^2 - 1$ thus $f(m) = 1$ for all $m \in \mathbb{N}$ and we get the solution $f(n) \equiv 1$. If such a k doesn't exist we get the solution $f(n) \equiv n^2$. □

Problem 42. Find all functions $f : \mathbb{N} \to \mathbb{N}$ satisfying

$$f(mn) = \operatorname{lcm}(m, n) \cdot \gcd(f(m), f(n))$$

for all positive integer m, n.

Proof. Let $f(1) = k$, and denote

$$f(mn) = \operatorname{lcm}(a, b) \cdot \gcd(f(m), f(n))$$

by $P(m, n)$. Then

$$P(m,1) \implies f(m) = m \cdot \gcd(f(m), k), \quad P(km, 1) \implies f(km) = km \cdot \gcd(f(km), k) = k^2 m,$$

$$P(m, kn) \implies f(kmn) = \operatorname{lcm}(m, kn) \cdot \gcd(f(m), k^2 n) = \frac{kmn}{\gcd(m, kn)} \cdot \gcd(f(m), k^2 n) \implies$$

$$\implies \gcd(f(m), k^2 n) = k\gcd(m, kn).$$

Hence, $k \mid f(m) \implies \gcd(f(m), k) = k$.

Therefore, we have $f(m) = km$ for all m.

□

7. Miscellaneous

Problem 43. Let p, q be two consecutive odd prime numbers. Prove that $p+q$ is a product of at least 3 natural numbers greater than 1 (not necessarily different).

Proof. Since $p < q$ are odd, it means $p < \frac{p+q}{2} < q$, with $\frac{p+q}{2} = ab$ integer, and moreover, not a prime (sitting between two consecutive primes). Thus $p + q = 2ab$ with $a, b > 1$ (notice that for $(p, q) = (3, 5)$ we have $p + q = 2^3$, so all three of the factors may in fact be equal). ☐

Problem 44. 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

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

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

Problem 45. 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 46. Let a and b be two positive integers such that $2ab$ divides $a^2 + b^2 - a$. Prove that a is perfect square

Proof. Let $d = \gcd(a, b)$, then $(a, b) = (sd, td)$, where s and t are two positive coprime integers. Consequently

$$\frac{a^2 + b^2 - a}{2ab} = \frac{(sd)^2 + (td)^2 - sd}{2 \cdot (sd) \cdot (td)} = \frac{d(s^2 + t^2) - s}{2dst} \in \mathbb{N}. \tag{7-1}$$

Therefore $s \mid dt^2$ by 7-1, yielding $s \mid d$ since $\gcd(s, t) = 1$. Futhermore $d \mid s$ by 7-1, which means $d = s$. Hence $a = sd = s \cdot s = s^2$, i.e. a is a perfect square. ☐

Problem 47. Prove that the equation $x^x = y^3 + z^3$ has infinitely many positive integer solutions x, y, z.

Proof. Let m, n be a positive integers such that $3 \mid m + n - 1$.

For any integer c we have that $3 \mid c^3 - c = c(c-1)(c+1)$, so from the identity

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

we see that $3 \mid m^3 + n^3 - 1$.

Now, take $x = m^3 + n^3$. Then $3 \mid x - 1$, so x^{x-1} is a cube. Moreover

$$x^x = x \cdot x^{x-1} = (m^3 + n^3)x^{x-1} = m^3 x^{x-1} + n^3 x^{x-1}$$

is a sum of two cubes.

□

Example 48.

(1) Given a positive integer k, prove that there do not exist two distinct integers in the open interval $\left(k^2, (k+1)^2\right)$ whose product is a perfect square.

(2) Given an integer $n > 2$, prove that there exist n distinct integers in the open interval $(k^n, (k+1)^n)$ whose product is the n-th power of an integer, for all but a finite number of positive integers k.

Proof.

(1) Suppose $a, b \in (k^2, (k+1)^2)$ have a product which is a perfect square. Write $a = m^2 x$ and $b = n^2 y$ where x, y are squarefree. Observe then that $x = y$ if ab is a perfect square, so $a = m^2 x, b = n^2 x$. WLOG $b > a$, so $n \geq m + 1 \implies b - a \geq x(2m + 1)$. However, we know

$$k^2 < m^2 x = a, \quad b = n^2 x < k^2 + 2k + 1$$

so $b - a \leq 2k - 1$. We also know $m > \frac{k}{\sqrt{x}}$. Thus

$$b - a \geq x \cdot \left(\frac{2k}{\sqrt{x}} + 1\right) > 2k - 1,$$

contradiction, so a, b do not exist.

(2) We are done if there exists

$$k^n < a_1^{n-1} < a_2^{n-1} < \ldots < a_{n-1}^{n-1} < (k+1)^n,$$

such that a_i are positive integers, $k^n < a_1 a_2 \ldots a_{n-1} < (k+1)^n$ and $a_1 a_2 \ldots a_{n-1}$ differ than a_i^{n-1}. Then the product of

$$a_1^{n-1},\ a_2^{n-1}, \ldots, a_{n-1}^{n-1},\ a_1 a_2 \ldots a_{n-1}$$

is n-th power.

We claim that $a_1 = \left\lceil k^{\frac{n}{n-1}} \right\rceil$, and $a_{i+1} = a_i + 1$ for all $1 \leq i \leq n - 2$, will work for sufficiently large k. Indeed, easy to see that we will obtain n different numbers and the condition that needs to be fulfilled is $(a_1 + n - 2)^{n-1} < (k+1)^n$. The latter is true if

$$\left(k^{\frac{n}{n-1}} + n - 1\right)^{n-1} < (k+1)^n \iff n - 1 < (k+1)^{\frac{n}{n-1}} - k^{\frac{n}{n-1}}$$

which holds for sufficiently large k.

□

Example 49. Determine all arithmetic sequences $a_1, a_2, \ldots$ for which there exists integer $N > 1$ such that for any positive integer k the following divisibility holds

$$a_1 a_2 \ldots a_k \mid a_{N+1} a_{N+2} \ldots a_{N+k}.$$

Proof. Let $a_n = a_0 + nd$. If $a_0 = 0$ or $d = 0$, then $\{a_n\}_{n \geq 0}$ satisfy given condition. WLOG, assume that $a_0 \cdot d \neq 0$ and $\gcd(a_0, d) = 1$.

Notice that for $k > N$ we have

$$M := a_1 \cdot a_2 \cdots a_N \mid a_{k+1} \cdot a_{k+2} \cdots a_{k+N} =: R.$$

Since $M > N!$, then exists prime p such that $v_p(M) > v_p(N!)$.

Therefore, pick k such that $p^{v_p(M)} \mid M \mid a_0 + dk$, then

$$0 \equiv R \equiv d^N N! \pmod{p^{v_p(M)}},$$

which is impossible since $\gcd(p, d) = 1$.

Finally only sequences satisfying given condition are such that $a_0 = 0$ or $d = 0$ i.e. $a_n = nd$ or $a_n = \text{const}$. □

Example 50. Prove that there exist infinitely many positive integer pairs (a, b) satisfying the condition $ab \mid a^8 + b^4 + 1$.

Proof. If (a, b) is a solution then both

$$\left(\frac{b^4+1}{a}, b\right) \quad \text{and} \quad \left(a, \frac{a^8+1}{b}\right)$$

are solutions. We have therefore infinitely many solutions. □

Problem 51. Let b be a positive integer. Show that there exists integer $a > 0$ auch that $a > b$ and

$$3^b + 2^b + 1 \mid 3^a + 2^a + 1.$$

Proof. Let $m = 3^b + 2^b + 1$ and take $e = \nu_2(m)$ and $f = \nu_3(m)$. Since

$$\nu_2\left(3^b + 1\right) = \begin{cases} 1 & \text{if } 2 \mid b \\ 2 & \text{if } 2 \nmid b \end{cases},$$

we have $e \leq b$.

Assume that $f \geq b + 1$. Since $3^{b+1} \mid m$, we have

$$3^b + 2^b + 1 \geq 3^{b+1},$$

It follows that

$$2^b + 1 > 2 \cdot 3^b > 2 \cdot 2^b = 2^b + 2^b \;\Rightarrow\; 1 > 2^b,$$

contradiction. So we must have $f \leq b$.

Take $a = \varphi(m) + b$ and we claim that a satisfies problem's assumptions. Indeed, we can take $c \in \mathbb{N}$ with $\gcd(c, 6) = 1$ for which $m = 2^e \cdot 3^f \cdot c$.

Since

$$2^{\varphi\left(a \cdot 3^f\right)} \equiv 1 \pmod{a \cdot 3^f},$$

we have

$$2^{\varphi(m)} \equiv 1 \pmod{a \cdot 3^f}.$$

It follows that $2^a \equiv 2^b \pmod{a \cdot 2^b \cdot 3^f}$, which implies $2^a \equiv 2^b \pmod{m}$ because $e \leq b$. Similarly, we have $3^a \equiv 3^b \pmod{m}$. Thus,

$$3^a + 2^a + 1 \equiv 3^b + 2^b + 1 \equiv 0 \pmod{m}.$$

□