Number Theory – group L4

Instructor: Dušan Djukić *Date: 21.2.2022.*

1. Find all primes p, q such that $p^2 - pq - q^3 = 1$.
   What if we do not require q to be prime?

2. A triple of positive integers (a, b, c) is *lame* if $c^2 + 1$ divides $(a^2 + 1)(b^2 + 1)$, but not $a^2 + 1$ and $b^2 + 1$. Given c, if there is a lame triple (a, b, c), prove that there is a lame triple in which $ab < c^3$.

3. The sequence (a_n) is defined by $a_1 = 1$, $a_2 = 2$ and $a_{n+2} = a_n(a_{n+1} + 1)$ for all $n \geqslant 1$. Prove that a_{a_n} is divisible by a_n^n for every $n \geqslant 100$.

4. A function $f : \mathbb{N} \to \mathbb{N}$ is such that $f(f(n)) = \tau(n)$, i.e. the number of divisors of n. Prove that if p is prime, then $f(p)$ is prime.

5. Prove that there are infinitely many positive integers n such that $\lfloor \tau(n)\sqrt{3} \rfloor$ divides n.

6. Suppose that $1 \leqslant a_1, a_2, \ldots, a_n \leqslant 2n$ are integers such that $\operatorname{lcm}(a_i, a_j) > 2n$ whenever $i < j$. Prove that $a_1 a_2 \cdots a_n$ divides $(n + 1)(n + 2) \cdots (2n)$.

7. If a positive integer $n > 20$ is not squarefree, prove that there exist positive integers a, b, c such that $ab + bc + ca = n$.

8. There are $n \geqslant 3$ integers on the board with the GCD equal to 1. In each step we are allowed to increase or decrease one of the numbers by a multiple of another number. Find the smallest k for which it is always possible to obtain number 1 by a sequence of k such steps.

Number Theory – group L4

Instructor: Dušan Djukić *Date: 23.2.2022.*

9. Rational numbers x, y satisfy $x^5 + y^5 = 2x^2y^2$. Prove that $1 - xy$ is a square of a rational number.
Are there infinitely many such pairs (x, y)?

10. Find all pairs of integers (m, n) such that $m^6 = n^{n+1} + n - 1$.

11. Coprime positive integers a, b, c are such that $a+b-c \mid a^2+b^2-c^2$, $b+c-a \mid b^2+c^2-a^2$ and $c + a - b \mid c^2 + a^2 - b^2$. Prove that $(a + b - c)(b + c - a)(c + a - b)$ is either a square or two times a square.

12. Positive integers a, b, c, d are such that $a + b = c + d = ab - cd$. Can both ab and cd be perfect squares?

13. Given positive integers a, b, for a prime p not dividing any of $a, b, a \pm b$ define $f(a, b)$ to be the number of integers x with $1 \leqslant x \leqslant p - 1$ for which either both ax and bx leave remainders $< \frac{p}{2}$ upon division by p, or both leave remainders $> \frac{p}{2}$. Prove that for p sufficiently large and any a, b we have $\frac{p-1}{3} \leqslant f(a, b) \leqslant \frac{2(p-1)}{3}$.

14. (a) What is the largest n for which there exist $2n$ positive integers $a_1, \dots, a_n, b_1, \dots, b_n$ that satisfy $a_ib_j - a_jb_i = 1$ whenever $i < j$?
(b) Same question if $1 \leqslant a_ib_j - a_jb_i \leqslant 2$ whenever $i < j$.

15. If $a_1, a_2, .., a_n \in \mathbb{N}$ are pairwise distinct, prove that $\sum_{k=1}^{n} \frac{1}{[a_1,\dots,a_k]} < 4$.
Can we improve the upper bound to 3? Or to 2?

Number Theory – group L4

Instructor: Dušan Djukić *Date: 24.2.2022.*

16. Let $x > 1$ be an integer. We are given the list of numbers $1, x+1, 2x+1, 3x+1, \dots, x^{99}+1$. In each step we erase the rightmost number existing on the board, along with all its divisors. Which number will be last deleted?

17. Suppose that p and $\frac{p-1}{2}$ are primes, and a, b, c integers not divisible by p. Prove that there are at most $\lceil\sqrt{2p}\rceil$ exponents n with $1 \leqslant n \leqslant p-1$ for which $p \mid a^n + b^n + c^n$.

18. We perform a sequence of operations of the following types: If the number is even, we divide it by 2, and if it is odd, we multiply it by some power of 3 (which we may choose, but it must be > 1) and add 1. Prove that, starting from any number, we can reach number 1 in finitely many such operations.

19. Given a squarefree integer $n > 2$, evaluate the sum $\sum_{k=1}^{n^2} \lfloor \sqrt[3]{kn} \rfloor$.

20. Let a, b, c be pairwise coprime positive integers. Denote by $g(a, b, c)$ the largest integer not representable in the form $xa + yb + zc$ for some $x, y, z \in \mathbb{N}$. Prove that $g(a, b, c) \geqslant \sqrt{2abc}$.

Number Theory – group L4

Instructor: Dušan Djukić *Date: 25.2.2022.*

18. We perform a sequence of operations of the following types: If the number is even, we divide it by 2, and if it is odd, we multiply it by some power of 3 (which we may choose, but it must be > 1) and add 1. Prove that, starting from any number, we can reach number 1 in finitely many such operations.

21. Find all triples of nonnegative integers a, b, c satisfying $a^2 + b^2 + c^2 = abc + 1$.

22. Positive integers x and $y < x$ are such that $x^2 + y^2 - 2$ is divisible by $x^2 - y^2$. Prove that $x^2 + y^2 - 2$ and $x^2 - y^2$ have the same sets of prime divisors.

Number Theory – group L4

Instructor: Dušan Djukić *Date: 26.2.2022.*

23. Find all positive integers that can be written as $\frac{x^2+y}{xy+1}$ with $x, y \in \mathbb{N}$ in at least two ways.

24. Let a, b, c be positive integers. If $(ab+1)(bc+1)(ca+1)$ is a perfect square, prove that each of the factors $ab+1$, $bc+1$, $ca+1$ is itself a square.

25. Determine all functions $f : \mathbb{N} \to \mathbb{N}$ such that $a^2 + f(a)f(b)$ is divisible by $f(a) + b$ for all $a, b \in \mathbb{N}$.

26. Find all surjective functions $f : \mathbb{N} \to \mathbb{N}$ such that, for every $m, n \in \mathbb{N}$, $f(m) + f(n)$ and $f(m+n)$ have the same set of prime divisors.

27. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $(m^2+n)^2$ is divisible by $f(m)^2 + f(n)$ for all $m, n \in \mathbb{N}$.

28. Determine all $f : \mathbb{N} \to \mathbb{N}$ such that $f(m) \geqslant m$ and $f(m+n) \mid f(m) + f(n)$ for all $m, n \in \mathbb{N}$.

Number Theory – group L4

Instructor: Dušan Djukić *Date: 28.2.2022.*

29. Find all functions $f : \mathbb{N} \to \mathbb{N}$ with the property that $f(m) + f(n) + 2mn$ is a perfect square for all $m, n \in \mathbb{N}$.

30. A sequence of positive integers $a_1, a_2, \ldots$ is such that $n \leqslant a_n \leqslant n + 2021$ for all n and $\gcd(a_m, a_n) = 1$ whenever $\gcd(m, n) = 1$. If a prime p divides a_n, prove also $p \mid n$.

31. Prove that every integer can be uniquely written in the form $a_0 + a_1(-\frac{4}{3}) + a_2(-\frac{4}{3})^2 + \cdots + a_k(-\frac{4}{3})^k$ for some integers $k \geqslant 0$ and $a_0, a_1, \ldots, a_k \in \{0, 1, 2, 3\}$.

Solutions – group L4

Instructor: Dušan Djukić *Feb.21–Mar.3, 2021*

1. The discriminant of the given quadratic $p^2 - q \cdot p - (q^3 + 1)$ must be a square, so $d^2 = q^2 + 4(q^3 + 1)$. This leads to $(d+2)(d-2) = q^2(4q+1)$, but since only one of the factors $d \pm 2$ can be divisible by q, that one is a multiple of q^2, while the other factor (which is less by at most 4) divides $4q + 1$. It follows that $q^2 - 4 \leqslant 4q + 1$ and hence $q \leqslant 5$. Testing these values of q yields two solutions: $(7, 3)$ and $(14, 5)$.

2. If $c^2 + 1 = 2m$ is even, then m is odd, so m divides $(c + m)^2 + 1$, but $2m$ does not (c is also odd). This enables us to take $a = 1$ and $b = c + m$; clearly, $ab = \frac{(c+1)^2}{2} < c^3$.

   Now let $c^2 + 1$ be odd. It must be composite, so let $c^2 + 1 = mn$, where $m < c < n$. We first choose a so that $a^2 + 1$ is divisible by m, but not by mn - this can be done by simply taking a to be the remainder of c when divided by m, as then $a^2+1 < m^2 < mn$.

   It remains to choose b. The numbers c^2+1, $(n-c)^2+1$ and $(n+c)^2+1$ are all divisible by n, but not all are divisible by mn (else $mn \mid (n + c)^2 - (n - c)^2 = 4cn$ and hence $mn \mid n$), so we can take b so that $b < 2n < c^2$. Then $ab < c^3$.

3. An easy induction yields $a_k = (a_{k-1} + 1)(a_{k-3} + 1) \cdots (a_{k-2i+1} + 1)a_{k-2i}$. We will show that $v_p(a_{a_n}) \geqslant nv_p(a_n)$ for every prime p.

   It follows from the recurrence relation that the sequence $v_p(a_i), v_p(a_{i+2}), v_p(a_{i+4}), \dots$ is nondecreasing. Moreover, if $p^k \mid a_i + 1$, then $p^k \mid a_{i+1}$ and $a_{i+2} = a_i(a_{i+1} + 1) \equiv -1 \pmod{p^k}$, which implies that the sequence $v_p(a_i + 1), v_p(a_{i+2} + 1), v_p(a_{i+4} + 1), \dots$ is nondecreasing as well.

   Now consider the largest ℓ for which $p \mid a_{n-2\ell}$. From $a_{n-2\ell} = a_{n-2\ell-2}(a_{n-2\ell-1} + 1)$ it follows that $p \mid a_{n-2\ell-1}+1$, so $v_p(a_{n-2\ell-1}+1) \leqslant v_p(a_{n-2\ell+1}+1) \leqslant \dots \leqslant v_p(a_{n-1}+1) \leqslant v_p(a_{n+1} + 1) \leqslant \dots$. So if $k = v_p(a_{n+1} + 1)$, it follows that $v_p(a_n) \leqslant \ell k < \frac{1}{2}nk$.

   On the other hand, a_n is inductively shown to have the same parity as n, so $a_{a_n} = a_n(a_{n+1} + 1)(a_{n+3} + 1) \cdots (a_{a_n-1} + 1)$ and hence $v_p(a_{a_n}/a_n) \geqslant \frac{1}{2}(a_n - n)k$. It remains to show that $\frac{1}{2}(a_n - n)k \geqslant (n - 1) \cdot \frac{1}{2}nk$, which reduces to $a_n \geqslant n^2$, and this holds by induction for $n \geqslant 6$.

4. Iterating one more f we obtain $f(\tau(n)) = f(f(f(n))) - \tau(f(n))$. Now setting $n = p$ to be prime yields $\tau(f(p)) = f(\tau(p)) = f(2)$, so it is enough to prove that $f(2) = 2$. However, we have $\tau(f(2)) = f(\tau(2)) = f(2)$, so $f(2)$ is either 1 or 2.

   It remains to show that $f(2) = 1$ is impossible. Otherwise we would have $f(p) = 1$ for all p, so $f(1) = f(f(p)) = \tau(p) = 2$. On the other hand, then $1 = f(3) = f(\tau(25)) = \tau(f(25))$, so also $f(25) = 1$, contradicting $f(f(25)) = 3$.

5. Setting e.g. $\tau(n) = 8$ we find that n must be divisible by $\lfloor 8\sqrt{3} \rfloor = 13$, which is achievable by taking $n = 13p^3$ for any prime $p \neq 13$ (then indeed $\tau(n) = 8$).

6. Each of the numbers a_i has a multiple in the set $\{n+1, \dots, 2n\}$, but no two share this multiple (because lcm $> 2n$), so each number from $n+1$ to $2n$ has a unique divisor among the a_i. The statement immediately follows.

7. Since $n = ab + bc + ca$ is equivalent to $n + a^2 = (a+b)(a+c)$, the problem reduces to finding a such that $n + a^2$ is a product of two integers greater than a.

   Let $n = p^2 m$, where p is a prime. We first try taking $a = p$, so that $n + p^2 = (m+1)p^2$. This clearly works if $m+1 > p$, or if $m+1$ is composite ($m+1 = uv \Rightarrow n+p^2 = up \cdot vp$).

   It remains to deal with the case when $m+1 = q \leqslant p$ is a prime. Then $n = p^2 q - p^2$, so we can take a to be the remainder of p modulo q: then $n + a^2 = p^2 q - (p^2 - a^2)$ is divisible by q and greater than $n + a^2 > n > pq$. This works unless $q = p$.

   We are left with the case $n = p^2(p-1)$. Then $a = 6$ works if $p > 3$ (which corresponds to $n > 20$), because $n + a^2 = (p+3)(p^2 - 4p + 12)$.

8. We start with a lemma:

   Lemma. If a, b, m are nonzero integers with $(a, b) = 1$, then there exists $k \in \mathbb{Z}$ such that $(a + kb, m) = 1$. $\square$

   We claim that n steps always suffice. If $(a_1, \dots, a_{n-1}) = 1$, then for some integers x_i we have $x_1 a_1 + \dots + x_{n-1} a_{n-1} = 1 - a_n$, so by adding the multiples $x_i a_i$ to a_n we obtain 1 in $n-1$ steps. We proceed to the general case: $d = (a_{n-1}, a_n)$ and $e = (a_1, \dots, a_{n-2})$. Clearly, $(d, e) = (\frac{a_{n-1}}{d}, \frac{a_n}{d}) = 1$, so by the Lemma there exists k such that $\frac{a_{n-1} + k a_n}{d}$ is coprime to e. Then we also have $(a_1, \dots, a_{n-2}, a_{n-1} + k a_n) = 1$. As before, we need further $n-1$ steps to replace the number a_n by 1.

   Let us prove that $n-1$ may not be enough. Suppose $p_1, \dots, p_n > 2$ are different primes. By the Chinese remainder theorem there exist integers $a_1, \dots, a_n$ such that $a_i \equiv 0 \pmod{p_j}$ for $j \neq i$ and $a_i \equiv 2 \pmod{p_i}$. Suppose that we have applied $n-1$ steps. Then there exists i such that no multiple of a_i was ever added. Thus the given numbers did not change modulo p_i, so none of them could become 1.

9. If $y = 0$, then $x = 0$. Else $t = \frac{x}{y}$ yields $y = \frac{2t^2}{t^5+1}$, $x = \frac{2t^3}{t^5+1}$, so $\sqrt{1 - xy} = \left| \frac{1-t^5}{1+t^5} \right|$.

10. If $2 \mid n+1$ or $3 \mid n+1$, then $n^{n+1} + n - 1$ falls between two consecutive squares or cubes and cannot be a sixth power. Now let n be even. Also, if $6 \mid n$, then $m^6 \equiv -1 \pmod{3}$. It remains to check $n \equiv 4 \pmod{6}$. Then $n+1 \mid m^6 + 3$ which is impossible, because -3 is not a quadratic residue modulo $n+1 \equiv 5 \pmod{6}$.

11. Denote $x = b + c - a$, $y = c + a - b$ and $z = a + b - c$. Since $2a = y + z$ etc, the numbers x, y, z have GCD at most 2. In terms of x, y, z we have $x \mid b^2 + c^2 - a^2 = \frac{1}{2}(x^2 + xy + xz - yz)$, so $x \mid yz$; similarly, $y \mid zx$ and $z \mid xy$.

    It suffices to prove that $v_p(x+y+z)$ is even for any odd prime p, so suppose $v_p(x) = k > 0$. W.l.o.g. $v_p(z) = 0$. Then from $x \mid 2yz$ we get $v_p(y) \geqslant k$, but $y \mid 2xz$ then implies $v_p(y) = k$, so $v_p(x+y+z) = 2k$.

12. If ab and cd were of different parity, then $a+b=c+d$ $(=ab-cd)$ would be odd, so both ab and cd would be even, a contradiction.

 Hence ab and cd are squares of the same parity, so $ab=(x+y)^2$, $cd=(x-y)^2$ and $a+b=c+d=4xy$ for some integers $x>y>0$. Since $(a-b)^2=(a+b)^2-4ab=4(4x^2y^2-(x+y)^2)$ and similarly $(c-d)^2=4(4x^2y^2-(x-y)^2)$, the product $(4x^2y^2-(x+y)^2)(4x^2y^2-(x-y)^2)=(4x^2y^2-x^2-y^2)^2-(2xy)^2$ is a square as well... although it lies strictly between $(4x^2y^2-x^2-y^2-1)^2$ and $(4x^2y^2-x^2-y^2)^2$.

13. By changing (a,b) to $(a\cdot b^{-1},1)$ modulo p and switching sign if needed - this does not change $|f(a,b)-\frac{p-1}{2}|$ - we can assume that $b=1$ and $2\leqslant a\leqslant\frac{p-1}{2}$. We say x is good if both residues are $<\frac{p}{2}$ or both $>\frac{p}{2}$.

 If $\frac{p}{4}<a<\frac{3p}{4}$, then among any three consecutive values of x at least one is good and at least one bad, implying $\frac{p-1}{3}<f(a)<\frac{2(p-1)}{3}$.

 Verifying $a=2,3,p-3,p-2$ is straightforward. It remains to deal with $4\leqslant a\leqslant\frac{p}{4}$. Then the difference between the good and bad values in each of the intervals $(\frac{(i-1)p}{a},\frac{ip}{a})$ is at most 1, except for the central interval that contains at most $\frac{p}{a}+1$ values. Hence the total difference is at least $a+\frac{p}{a}+1$ which is less than $\frac{p-1}{6}$ for p big enough.

14. (a) We can have three pairs, e.g. $(1,1),(1,2),(2,3)$. We cannot have four. Indeed, first of all, we cannot have a_i,b_i both even, so if $n>3$, there are two fractions with $a_i\equiv a_j$ and $b_i\equiv b_j \pmod 2$, but then $a_jb_i-a_ib_j$ is even.

 In part (b) the maximum is four: e.g. $(1,1),(1,2),(2,3),(3,5)$.

15. Recall that $\tau(m)<2\sqrt{m}$, for m can have as many divisors $<\sqrt{m}$ as those $>\sqrt{m}$. The number $[a_1,\dots,a_n]$ has n divisors, so it is not less than $n^2/4$. Now the given sum is less than $1+\frac{1}{2}+\frac{1}{4}+\sum_{n\geqslant 4}\frac{4}{n^2}<\frac{7}{4}+\sum_{n\geqslant 4}\frac{16}{4n^2-1}=\frac{7}{4}+\sum_{n\geqslant 4}(\frac{8}{2n-1}-\frac{8}{2n+1})<\frac{7}{4}+\frac{8}{7}<3$.

 The upper bound is greater than 2: e.g. take (a_n) to be $1,2,3,6,4,12,8,24,16,48,\dots$.

16. The last number is $y=\frac{x^{99}+1}{x+1}+x$. It does not divide any larger number on the list. Indeed, if y divides some number $z\equiv 1 \pmod x$, then $\frac{z}{y}\equiv 1 \pmod x$, so $\frac{z}{y}\geqslant x+1$ and hence $z\geqslant(x+1)y>x^{99}+1$. Thus y only gets deleted after all numbers greater than y. On the other hand, every number on the list less than y has a multiple on the list (other than y), so it will also get deleted before y.

17. Multiplying by $c^{-1} \pmod p$, we can assume w.l.o.g. that $c=1$. Now if $a\equiv\pm1$ or $b\equiv\pm1$ or $a\equiv\pm b$ modulo p, the statement is trivial, so we can also assume otherwise. Then the orders of a, b and ab^{-1} modulo p divide $2q$, so they are q or $2q$.

 Call n *good* if $p\mid a^n+b^n+1$, and denote by G the set of good exponents n. Given $q\nmid r$, we claim that there are at most two pairs of good numbers differing by r. To see this, assume that $p\mid a^n+b^n+1$ and $p\mid a^ra^n+b^rb^n+1$; these imply that $(a^r-b^r)a^n\equiv b^r-1 \pmod p$, which occurs for at most two values of n.

 Since for each $n\in G$ there are $|G|-2$ other elements of G not differing from n by q, so they produce $|G|(|G|-2)$ differences and hence $|G|(|G|-2)\leqslant 2(p-2)$, leading to $|G|\leqslant 1+\sqrt{2p}$.

18. We can assume the initial number n_0 is odd. For $i \geqslant 1$, from n_{i-1} we will obtain some number n_i such that $2^{r_i} n_i = 3^{s_i} n_{i-1} + 1$ for some $r_i, s_i > 0$. Combining these equations for $1 \leqslant i \leqslant k$, we can write the condition $n_k = 1$ as

$$m = 2^{a_{k-1}} 3^{b_0} + 2^{a_{k-2}} 3^{b_1} + \cdots + 2^{a_0} 3^{b_{k-1}}, \qquad (*)$$

where $a_0 = b_0 = 0$, $a_i = r_1 + \cdots + r_i$, $b_i = s_k + \cdots + s_{k+1-i}$ and $m = 2^{a_k} - 3^{b_k} n$.

<u>*Lemma.*</u> Every positive integer m can be written in the form $(*)$ for some integers $0 \leqslant a_0 < a_1 < \cdots < a_{k-1}$ and $0 \leqslant b_0 < b_1 < \cdots < b_{k-1}$.

To secure the conditions $a_{k-1} < a_k$ and $b_{k-1} < b_k$, it is enough to choose a_k and b_k so that $0 < m = 2^{a_k} - 3^{b_k} n < 3^{b_k}$, i.e. $b_k + \log_3 n < a_k \log_3 2 < b_k + \log_3(n+1)$. This choice is possible because $\log_3 2$ is irrational: Indeed, for some a_k we have $\{\log_3 n\} < \{a_k \log_3 2\} < \{\log_3(n+1)\}$.

Finally, having chosen a_k and b_k, we find a_i and b_i $(0 \leqslant i < k)$ by the Lemma for $m = 2^{a_k} - 3^{b_k} n$ and take $r_i = a_i - a_{i-1}$ and $s_i = b_{k+1-i} - b_{k-i}$.

19. Let A be the set of lattice points (x, y) with $1 \leqslant x \leqslant n^2$, $1 \leqslant y \leqslant n$. Our sum is the number T of points in A below the curve $y^3 = nx$.

Let us count points in A *above* the curve: given y, there are $[\frac{y^3}{n}]$ such points, for the total of $S = \sum_{y=1}^{n} [\frac{y^3}{n}]$. Since n is squarefree, no points from A other than (n^2, n) lie on the curve, so $S + T = n^3 + 1$. We have $[\frac{y^3}{n}] + [\frac{(n-y)^3}{n}] = \frac{y^3}{n} + \frac{(n-y)^3}{n} - 1 = n^2 - 3ny + 3y^2 - 1$ for $1 \leqslant y \leqslant n-1$, so summing over all y yields $2S = \sum_{y=0}^{n} (n^2 - 3ny + 3y^2) - (n-1) = n^2(n+1) - \frac{3n^2(n+1)}{2} + \frac{n(n+1)(2n+1)}{2} - (n-1) = \frac{(n+2)(n^2-1)}{2} + 2$.

The required sum is $T = n^3 + 1 - S = \frac{(n-1)(3n^2+n+2)}{4}$.

20. Let us count the numbers of the form $xa + yb$ $(x, y \in \mathbb{N})$ that do not exceed $2\sqrt{abc}$. It is (at most) the number of lattice points in the triangle in the first quadrant below the line $ax + by \leqslant 2\sqrt{abc}$, which is less than its area, and this area is $\frac{1}{2} \frac{\sqrt{2abc}}{a} \frac{\sqrt{2abc}}{b} = c$. Thus $ax + by$ cannot collect all residue classes modulo c, so $ax + by + cz$ cannot cover all integers $> \sqrt{2abc}$.

21. Assume $a \leqslant b \leqslant c$. Since $c^2 - ab \cdot c + (a^2 + b^2 - 1) = 0$, we can switch c to $ab - c$, thus obtaining a smaller solution, unless $a^2 + b^2 - 1 < 0$ (i.e. $a = b = 0$) or $c \leqslant \frac{ab}{2}$. If $a \leqslant b \leqslant c \leqslant \frac{ab}{2}$, then $0 = c^2 - ab \cdot c + a^2 + b^2 - 1 \leqslant b^2 - ab \cdot b + a^2 + b^2 - 1 = a^2 - (a-2)b^2 - 1$, which is possible only for $a < 2$. But then $c \leqslant \frac{ab}{2} < b \leqslant c$, a contradiction. Therefore the only solution is $(0, 0, 1)$.

22. We have $x^2 + y^2 - 2 = n(x^2 - y^2)$, i.e.

$$(n+1)y^2 - (n-1)x^2 = 2. \qquad (*)$$

It suffices to prove that n divides $x^2 - y^2$.

Suppose to the contrary that (x, y) is the solution of $(*)$ with $|y|$ minimal for which $n \nmid x^2 - y^2$. Then $(nx - (n+1)y, ny - (n-1)x)$ is also a solution, and moreover, $n \nmid (nx - (n+1)y)^2 - (ny - (n-1)x)^2 \equiv y^2 - x^2 \pmod{n}$. Hence this is a larger solution: $|ny - (n-1)x| \geqslant |y|$, i.e. $x \leqslant y$ or $x \geqslant \frac{n+1}{n-1} y$. Substituting in $(*)$ yields $|y| \leqslant 1$, so it would force $(x, y) = (1, 1)$. However, $n \mid 1^2 - 1^2$, which is a contradiction.

23. Let $x^2+y=n(xy+1)$. Then $x^2-ny\cdot x+y-n=0$ with the discriminant $D^2=n^2y^2+4(n-y)$, but $4(1-ny)\leqslant 4(n-y)<4(ny+1)$, so $ny-2\leqslant D<ny+2$. Since D is of the same parity as ny, we have either $D=ny$ (leading to $(x,y)=(n^2,n)$) or $D=ny-2$ (leading to $n=1$ and $x\in\{1,y-1\}$). Only for $n=1$ we have multiple solutions.

24. Write $4(ab+1)(ac+1)(bc+1)=(2abc+a+b+c-d)^2$. This reduces to the symmetric equation $a^2+b^2+c^2+d^2-2ab-2ac-2bc-2ad-2bd-2cd-4abcd-4=0$. We also observe that $4(ab+1)(cd+1)=(a+b-c-d)^2$ etc... so $ab+1$, $ac+1$, $bc+1$ are squares if and only if so are $ad+1$, $bd+1$, $cd+1$.

    We are now ready for Vieta jumping: if (a,b,c,d) is a solution, then so is (a,b,c,d') with $d'=4abc+2(a+b+c)-d$. Suppose (a,b,c,d) is a solution ($a\leqslant b\leqslant c\leqslant d$) with the smallest $a+b+c+d$ for which not all six products plus 1 are squares. The same applies for the solution (a,b,c,d'), so by minimality we must have $d'\geqslant d$ or $d\leqslant 0$. However, if $d=0$ then trivially $4(ab+1)=(a+b-c)^2$ etc, and if $d<0$, then from $cd+1\geqslant 0$ we deduce $c=1$, $d=-1$ and $a+b=0$ which is impossible. Therefore $d'\geqslant d$, i.e. $c\leqslant d\leqslant 2abc+a+b+c$, so $4(ab+1)(bc+1)(ca+1)\leqslant(2abc+a+b)^2$. But this expands into $4abc^2+4c(a+b)+4\leqslant(a-b)^2$, which is impossible (note that $2c\geqslant a+b$).

25. Plugging in $(a,b)=(1,1)$ we find that $f(1)=1$. Next, for a prime p, setting $(a,b)=(p,p)$ we get $f(p)+p\mid 2p^2$, so $f(p)\in\{p,p^2-p,2p^2-p\}$, but for $(a,b)=(p,1)$ we get $f(p)+1\mid p^2-1$, so for $p\geqslant 3$ only $f(p)=p$ is possible. Now for an arbitrary n and prime $p\geqslant 3$ we have $f(n)+p\mid n^2+pf(n)$ and hence $f(n)+p\mid n^2-f(n)^2$, and if p is big enough, we must have $f(n)=n$.

26. Fix a prime p and consider the smallest a with $p\mid f(a)$. By induction, $p\mid f(x)$ whenever $a\mid x$. On the other hand, if $a\nmid x$, i.e. $x\equiv k\pmod{p}$ with $0<k<p$, then $p\mid f(a-x)+f(x)$, so $p\mid f(x)$, a contradiction. Hence $p\mid f(x)$ if and only if $a\mid x$. Next, $x\equiv -z\pmod{a}$ is equivalent to $p\mid f(x+z)$, i.e. $f(x)\equiv -f(z)\pmod{p}$. This implies that $x\equiv y\pmod{a}$ if and only $f(x)\equiv f(y)\pmod{p}$. By surjectivity, $f(1),f(2),\dots,f(a)$ form a complete residue system modulo p, so $d=p$. Thus $p\mid f(x)\Leftrightarrow p\mid x$, and $p\mid f(x)-f(y)\Leftrightarrow p\mid x-y$. Hence f is also injective.

    Since no prime divides 1, we must have $f(1)=1$. Next, if $f(x)=x$ for all $x<n$, then $f(n)-f(n-1)$ and $n-(n-1)=1$ have the same prime divisors, so $f(n)-f(n-1)=\pm 1$. Now an easy induction together with injectivity leads to $f(n)=n$ for all n.

27. Setting $m=n=1$ gives $f(1)^2+f(1)\mid 4$, so $f(1)=1$. Next, if p is a prime, we have $f(1)^2+f(p-1)\mid p^2$, so $f(p-1)\in\{p-1,p^2-1\}$. However, if $f(p-1)=p^2-1$, then setting $(m,n)=(p-1,1)$ yields $(p^2-1)^2+1\mid((p-1)^2+1)^2$, which is impossible. Hence $f(p-1)=p-1$. Now, given $n\in\mathbb{N}$, $(p-1)^2+f(n)$ divides $((p-1)^2+n)^2\equiv(n-f(n))^2\pmod{(p-1)^2+f(n)}$ for every prime p, i.e. $(n-f(n))^2$ has infinitely many divisors, so $f(n)=n$.

28. Let $f(1)=c$. Then $f(n+1)\leqslant f(n)+c$ implies $f(n)\leqslant cn$.

    Next, $f(2^k)$ divides $2f(2^{k-1})=c_kf(2^k)$ for some integer c_k. Then $2^kf(1)=c_1\cdots c_kf(2^k)\geqslant 2^kc_1\cdots c_k$, so $c_1\cdots c_k\leqslant c$. Thus $c_k=1$ for all big enough k.

Now fix n and take k big enough, so that $f(2^{k+2}) = 2f(2^{k+1}) = 4f(2^k)$. We have $2f(2^k) \mid f(2^k+n)+f(2^k-n)$ and $f(2^k) \mid f(2^k-n)+f(n)$, so $f(2^k) \mid f(2^k+n)-f(n)$ and hence $f(2^k+n) \mid f(2^k)+f(n) \leqslant f(2^k+n)$, which is possible only if $f(2^k+n) = f(2^k)+f(n)$. Similarly, $f(2^k+1) = f(2^k)+c$. Now $f(2^{k+1}+n+1) = 2f(2^k)+f(n+1)$ divides $f(2^k+n)+f(2^k+1) = 2f(2^k)+f(n)+f(1)$, and for big k this implies $f(n+1) = f(n)+c$. Therefore $f(n) = cn$ for all n.

29. Fix n and let $f(n+1)-f(n) = k$. Now for any m, if $f(m)+2mn+f(n) = x^2$ and $f(m)+2m(n+1)+f(n+1) = y^2$, we have $y^2-x^2 = 2m+k$. Since a difference of two squares cannot be 2 (mod 4), we cannot have k even. But now as k is odd, we can take m so that $2m+k = p$ is a prime - then $y^2-x^2 = p$, and this is only possible if $x = \frac{p-1}{2}$ and $y = \frac{p+1}{2}$.

    Next, consider $f(m)+2m(n+2)+f(n+2) = z^2$. Then $z^2 - \left(\frac{p+1}{2}\right)^2 = 2m+(f(n+2)-f(n+1)) = p+c$, where $c = f(n+2)-2f(n+1)+f(n)$. But if p is big enough, this will imply $\left(\frac{p+1}{2}\right)^2 < z < \left(\frac{p+5}{2}\right)^2$ and thus force $z = \frac{p+3}{2}$. Consequently, $f(n+2)-2f(n+1)+f(n) = c = 2$ is constant, so $f(n) = n^2+An+B$ is a quadratic function.

    Now $f(n)+f(n)+2n^2 = 4n^2+2An+2B$ is a square for all n, so it must be $(2n+2a)^2$ and hence $A = 4a$, $B = 2a^2$. Therefore $f(n) = n^2+4an+2a^2$.

30. Denote by $g(n)$ the smallest prime divisor of a_n, and by P_n the set of primes not exceeding n. Consider any N such that $1000! \mid N-1$. Since $a_p \leqslant p+1000 \leqslant N+1000$ for $p \in P_N$, we have $g(p) \in P_{N+1000} = P_N$. Moreover, by the problem condition, $g(p) \neq g(q)$ whenever p and q are different primes, so g is a bijection on P_N. Since this holds for all N, g is a bijection on the set of all primes.

    Let q be a prime divisor of a_{p^k}, where p is a prime and $k \in \mathbb{N}$. Since g is a bijection, $g(r) = q$ for some prime r, so $q \mid (a_r, a_{p^k})$, and this implies $(r, p^k) > 1$, i.e. $r = p$. Hence a_{p^k} is a power of the prime $g(p) = q$. Assume now that $q \neq p$ and take $k, n \in \mathbb{N}$ so that $p^n > q^k > 2017$ and $\varphi(q^k) \mid n$. Then $p^n \equiv 1 \pmod{q}^k$, which secures that none of $p^n, p^n+1, \ldots, p^n+2016$ is a multiple of q^k. Thus $q^k \nmid a_{p^n}$, so a_{p^n} is not a power of q, a contradiction. Therefore $f(p)$ is in fact a power of p,

    Now if $p \mid a_n$, then $(a_n, a_p) > 1$ and hence $(p, n) > 1$, i.e. $p \mid n$.

31. Since all summands except a_0 are divisible by 4, a_0 is uniquely determined modulo 4. Subtract a_0, multiply by $-\frac{3}{4}$ (this should decrease its absolute value, except in very small cases) and continue.