Number Theory – level L4

Instructor: Dušan Djukić *Date: 2.6.2022.*

1. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that, whenever $a_1 + a_2 + \cdots + a_n$ is a square (for some n), $f(a_1) + f(a_2) + \cdots + a(a_n)$ is also a square.

2. Can every positive integer greater than 100^{100} be written as a sum of 15 fourth powers (some of which may be zero)?

3. Find all triples of positive integers a, b, c such that $ab + bc + ca = 4 \cdot \operatorname{lcm}(a, b, c)$.

4. Find all positive integers n for which one can find several (at least two) positive rational numbers $a_1, a_2, \ldots, a_k$ such that $a_1 + a_2 + \cdots + a_k = a_1 a_2 \cdots a_k = n$.

Number Theory – level L4

Instructor: Dušan Djukić *Date: 3.6.2022.*

5. Are there integers a, b, c, all greater than 2022, that satisfy $a^3 + 2b^3 + 4c^3 = 6abc + 1$?
6. Are there positive integers a, b, c, all greater than 10^{10}, such that abc is divisible by each of the numbers $a + 2022$, $b + 2022$, $c + 2022$?
7. Positive integers a, b, c, d and n are such that $a + c < n$ and $\frac{a}{b} + \frac{c}{d} < 1$. Prove that $\frac{a}{b} + \frac{c}{d} < 1 - \frac{1}{n^3}$.
8. Find all real numbers α with the following property: There exist a real number $r > \alpha$ and an irrational number x such that both $x^2 - rx$ and $x^3 - rx$ are rational numbers.

Number Theory – level L4

Instructor: Dušan Djukić *Date: 4.6.2022.*

If $p > 2$ is a prime, then among $1, 2, \dots, p-1$ there are exactly $\frac{p-1}{2}$ quadratic residues and as many quadratic non-residues. *Legendre's symbol* is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p; \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p; \\ 0 & \text{if } p \mid a. \end{cases}$$

The congruence $x^2 \equiv a \pmod{p}$ has exactly $\left(\frac{a}{p}\right) + 1$ solutions modulo p.

- If $p > 2$ is a prime, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$. *(Euler's criterion)*

Consequently, -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod{4}$ or $p = 2$.

Also by Euler's criterion, Legendre's symbol is multiplicative: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Let $p \nmid a$ $(p > 2)$. Knowing Euler's criterion, we can write $a^{\frac{p-1}{2}}$ as $\frac{a \cdot 2a \cdots (\frac{p-1}{2}a)}{1 \cdot 2 \cdots \frac{p-1}{2}}$. To reduce this modulo p, we note that for each $k = 1, \dots, \frac{p-1}{2}$ there is a (unique) r_k such that $ka \equiv r_k \pmod{p}$ with $|r_k| \leqslant \frac{p-1}{2}$. Observe that $|r_1|, \dots, |r_{\frac{p-1}{2}}|$ is a permutation of $1, 2, \dots, \frac{p-1}{2}$, so writing $e_k = \operatorname{sgn} r_k = \pm 1$ we obtain

$$\left(\frac{a}{p}\right) \equiv \frac{r_1 r_2 \cdots r_{\frac{p-1}{2}}}{1 \cdot 2 \cdots \frac{p-1}{2}} = e_1 e_2 \cdots e_{\frac{p-1}{2}}.$$

Now show that $e_k = -1$ if and only if $[\frac{2ka}{p}] = 2[\frac{ka}{p}] + 1$, i.e. $e_k = (-1)^{[2ka/p]}$. The above equality thus becomes:

- If $p > 2$ and $p \nmid a$, then $\left(\frac{a}{p}\right) = (-1)^S$, where $S = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{2ka}{p}\right]$. *(Gauss' Lemma)*

Deduce from here:

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, so 2 is a quadratic residue mod $p > 2$ if and only if $p \equiv \pm 1 \pmod{8}$.

Now apply the Gauss lemma to $a = \frac{p+q}{2}$ to obtain

$$\left(\frac{q}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}}(-1)^{S_1} = (-1)^{S_1}, \quad \text{where} \quad S_1 = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor.$$

Also $\left(\frac{p}{q}\right) = (-1)^{S_2}$. Guess what is S_2?

Think graphically: which lattice points do S_1 and S_2 count? So why is $S_1 + S_2 = \frac{p-1}{2} \cdot \frac{q-1}{2}$?

Our conclusion:

- If $p, q > 2$ are distinct primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. *(Quadratic reciprocity law)*

There is an extension of the Legendre symbol to composite odd moduli, called the *Jacobi symbol.* Given an odd integer $n = p_1 p_2 \dots p_k$, where the p_i are odd primes (not necessarily distinct), the Jacobi symbol is defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

These inherit most relations from the Legendre symbols: $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$. An exception is that $\left(\frac{a}{n}\right) = 1$ does not imply that a is a quadratic residue modulo n.

9. Given a prime number p, prove that there exists x with $p \mid x^2 - x + 3$ if and only if there exists y with $p \mid y^2 - y + 25$.
10. Let $p = 4k + 3$ be a prime. Is $3k + 2$ a quadratic residue modulo p?
11. Let $p = 4k - 1$ be a prime. If congruence $x^2 \equiv a \pmod{p}$ has solutions, prove that these solutions are $x = \pm a^k$.
12. Prove that for every prime $p > 2$ there exists a quadratic non-residue $a < \sqrt{p} + 1$ modulo p.
13. Evaluate $[\frac{1}{101}] + [\frac{2}{101}] + [\frac{4}{101}] + \cdots + [\frac{2^{99}}{101}]$.
14. Prove that every prime p has a multiple of the form $x^2 + y^2 + 1$.
15. (a) Prove that every prime divisor of $n^4 - n^2 + 1$ is of the form $12k + 1$.

    (b) Prove that every prime divisor of $n^8 - n^4 + 1$ is of the form $24k + 1$.
16. Prove that $x^2 + 1$ is not divisible by $y^2 - 5$ for any x, y $(y > 2)$.
17. Prove that (a) $4xy - x - y$, (b) $4xyz - x - y$ cannot be a perfect square if x, y, z are positive integers.
18. Find all positive integers n such that the set $\{n, n+1, \dots, n+101\}$ can be partitioned into several subsets with equal products of elements.

Number Theory – level L4

Instructor: Dušan Djukić *Date: 6.6.2022.*

19. Let $P(x) = x^3+14x^2-2x+1$. Prove that there exists n such that $P(P(\dots P(x)\dots)) \equiv x \pmod{101}$ (P applied n times) for every x.

20. Prove that number $N = 2^{2^n} + 1$ is prime if and only if $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

21. Prove that the sum of all quadratic non-residues modulo a prime p is a multiple of p.

22. Let p be a prime. For a positive integer n denote $s_n = 1^n + 2^n + \cdots + (p-1)^n$. Prove that $s_n \equiv 0 \pmod{p}$ if $p-1 \nmid n$, but $s_n \equiv -1 \pmod{p}$ if $p-1 \mid n$.

The previous problem could be elegantly solved using a *primitive root* - that is, an integer g whose order modulo p equals $p-1$: thus $1, g, g^2, \dots, g^{p-2}$ form a permutation of $1, 2, \dots, p-1$ modulo p. So it is time to prove that a primitive root modulo a prime p always exists. The key statement, which we prove by induction on n ($n \mid p-1$), is that the number of residues of order exactly n modulo p equals $\varphi(n)$.

First of all, $x^n - 1 \equiv 0 \pmod{p}$ has at most n solutions mod p, but $\frac{x^{p-1}-1}{x^n-1} \equiv 0 \pmod{p}$ has at most $p-1-n$ solutions. Hence "at most" is in fact "exactly" in both cases. Thus there are exactly n residues of order *dividing* n. By the inductive hypothesis, for every $d < n$, $d \mid n$, there are $\varphi(d)$ residues of order d. Thus, by the following lemma, the number of residues of order *exactly* n equals $n - \sum_{d|n, d<n} \varphi(d) = \varphi(n)$, which finishes the induction:

Lemma. $\sum_{d|n} \varphi(d) = n$.

Proof. $\varphi(d)$ counts numbers $x \in \{1, 2, \dots, n\}$ with $\gcd(x, n) = \frac{n}{d}$. Thus $\sum_{d|n} \varphi(d)$ counts each elements from this set exactly once. $\square$

23. Let p is an odd prime and let a, b, c be integers with $p \nmid b^2 - ac$. Prove that $\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p}\right) = -\left(\frac{a}{p}\right)$.

24. If p is a prime and $p \nmid a$, prove that the congruence $x^2 + y^2 = a$ has exactly $p - \left(\frac{-1}{p}\right)$ solutions (x, y) modulo p.

25. If a is an integer, prove that the congruence $x^2 + y^2 + z^2 \equiv 2axyz \pmod{p}$ has exactly $\left(p + \frac{3}{2}(-1)^{p'}\right)^2 - \frac{5}{4}$ solutions (x, y, z), where $p' = \frac{p-1}{2}$.

26. Prove that there are no positive integers a, b, c for which $a^2 + b^2 + c^2$ is divisible by $3(ab + bc + ca)$.

27. Find all positive integers x for which $x^3 + 2x + 1$ is a power of 2.

Number Theory – level L4

Instructor: Dušan Djukić *Date: 7.6.2022.*

28. Suppose that m and n are positive integers such that $\varphi(5^m - 1) = 5^n - 1$. Prove that $\gcd(m, n) > 1$.

29. Given a positive integer n, prove that there are at most two pairs of positive integers (a, b) such that $a + b$ is a power of 2 and $a^2 + b = n$.

30. Find all pairs of positive integers x, y that satisfy the equation $3^x - 8^y = 2xy + 1$.

31. Find all n for which there is a permutation $(a_1, a_2, \ldots, a_n)$ of $1, 2, \ldots, n$ with the property that both $(a_1 + 1, \ldots, a_n + n)$ and $(a_1 - 1, \ldots, a_n - n)$ are also permutations of $1, 2, \ldots, n$ modulo n.

32. We say that n cells in an $n \times n$ table are *scattered* if no two are in the same row or column. Is it possible to write the numbers $1, 2, \ldots, n^2$ in an $n \times n$ table so that all scattered sets of cells have the same product of elements modulo $n^2 + 1$ if (a) $n = 8$, and if (b) $n = 10$?

Number Theory – level L4

Instructor: Dušan Djukić *Date: 9.6.2022.*

33. Prove that 2^{n^2+n-5} divides $\varphi(2^{2^n}-1)$ for all positive integers n.

34. Find all positive integers n such that $\tau(n)$ divides $2^{\sigma(n)}-1$.
    As usual, $\tau(n)$ is the number of divisors and $\sigma(n)$ the sum of divisors of n.

35. Find all pairs of positive rational numbers x, y satisfying $yx^y = y+1$.

36. Define $a_1 = 2021^{2021}$, and for $k \geqslant 2$, let a_k be the remainder when $a_{k-1} - a_{k-2} + a_{k-3} - \cdots$ is divided by k. Find the 2021^{2022}-th term of the sequence (a_n).

Solutions: Number Theory – level L4

Instructor: Dušan Djukić

1. Fix x. We observe that, whenever $a^2 > x$, the numbers $f(x+1) + (a^2 - x - 1)f(1)$ and $f(x) + (a^2 - x)f(1)$ are squares, since so is $x + 1 + 1 + \cdots + 1$. But these two squares differ by the fixed quantity $f(x+1) - f(x) - f(1)$, so if a is too big, this can only happen if this quantity is 0. Therefore $f(x+1) = f(x) + f(1)$, implying that $f(x) = cx$ for some constant $c \in \mathbb{N}$.

2. If x is odd, then $2 \mid x^2+1$ and $8 \mid x^2-1$. so $16 \mid x^4-1$. Also, if x is even, then $16 \mid x^4$. Thus every fourth power gives the remainder 0 or 1 modulo 16. In particular, if $16n$ is a sum of 15 fourth powers, then all these fourth powers are even, so n is also a sum of 15 fourth powers.

   But number 31 cannot be written as a sum of 15 fourth powers. Thus neither can the numbers $31 \cdot 16$, $31 \cdot 16^2$, etc.

3. The number $ab + bc + ca$ is divisible by each of a, b, c, so $a \mid bc$. Similarly, $b \mid ca$ and $c \mid ab$. Thus each of ab, bc, ca itself is a multiple of $L = \operatorname{lcm}(a, b, c)$, but their sum is $4L$. Thus these three multiples are $L, L, 2L$ in some order. This leads us to a, b, c being $k, 2k, 2k$ for some k and consequently that $k = 1$.

4. Every composite n works: if $n = ab$, $a, b \geqslant 2$, then $a+b+1+\cdots+1 = a\cdot b\cdot 1\cdot\cdots\cdot 1 = n$.

   On the other hand, by AM-GM, $n = a_1 + \cdots + a_k \geqslant k\sqrt[k]{a_1 \cdots a_k} = kn^{1/k}$, so $n \geqslant k^{\frac{k}{k-1}}$. This rules out $n = 2, 3$, but also $n = 5$, as then $k \geqslant 3$.

   The primes $n = p \geqslant 11$ work with the k-tuple $(\frac{p}{2}, \frac{1}{2}, 4, 1, \cdots, 1)$. Also, $n = 7$ works with the triple $(\frac{7}{6}, \frac{4}{3}, \frac{9}{2})$.

5. Recall that $x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z)$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ is the primitive (complex) cubic root of 1. Applying this factorization for a, $b\sqrt[3]{2}$, $c\sqrt[3]{4}$ yields $a^3 + 2b^3 + 4c^3 - 6abc = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{4})(a + b\omega^2\sqrt[3]{2} + c\omega\sqrt[3]{4})$.

   The smallest solution of the original equation in $\mathbb{N}$ is $(a, b, c) = (1, 1, 1)$; thus $(1 + \sqrt[3]{2} + \sqrt[3]{4})(1 + \omega\sqrt[3]{2} + \omega^2\sqrt[3]{4})(1 + \omega^2\sqrt[3]{2} + \omega\sqrt[3]{4}) = 1$. Now raise this to the n-th power: we have $(1 + \sqrt[3]{2} + \sqrt[3]{4})^n = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ for some positive integers a, b, c. But since algebra does not distinguish between the real and complex roots, we also have $(1+\omega\sqrt[3]{2}+\omega^2\sqrt[3]{4})^n = a+b\omega\sqrt[3]{2}+c\omega^2\sqrt[3]{4}$ and $(1+\omega^2\sqrt[3]{2}+\omega\sqrt[3]{4})^n = a+b\omega^2\sqrt[3]{2}+c\omega\sqrt[3]{4}$. Multiplying these three equalities gives us $a^3 + 2b^3 + 4c^3 - 6abc = 1$ for every n. Choosing n big leads to an arbitrarily big solution (a, b, c).

6. Why not e.g. $(a, b, c) = (an, an, a(n^2 - 1))$, where $a = 2022$.

7. Since $c \leqslant n-2$, we have $\frac{c}{d} \leqslant \frac{c}{c+1} \leqslant \frac{n-2}{n-1}$. Thus, if $\frac{a}{b} \leqslant \frac{1}{n}$, we have $\frac{a}{b} + \frac{c}{d} \leqslant \frac{n-2}{n-1} + \frac{1}{n}$ $= 1 - \frac{1}{n^2-n} < 1 - \frac{1}{n^3}$. Case $\frac{c}{d} \leqslant \frac{1}{n}$ is analogous.

   Now suppose that $\frac{a}{b}, \frac{c}{d} > \frac{1}{n}$ and $\frac{a}{b} + \frac{c}{d} > 1 - \frac{n-1}{n}$. Then $\frac{a}{b} \cdot \frac{c}{d} > \frac{1}{n} \cdot \frac{n-2}{n} = \frac{n-2}{n^2}$, so $bd < ac \cdot \frac{b}{a} \cdot \frac{d}{c} < \frac{1}{4}(a+c)^2 \cdot \frac{n^2}{n-2} \leqslant \frac{n^2(n-1)^2}{4(n-2)} < n^3$. Therefore $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \leqslant 1 - \frac{1}{bd} < 1 - \frac{1}{n^3}$.

8. Denote $x^2 - rx = a$. Then $b = x^3 - rx = x(rx+a) - rx = rx^2 + (a-r)x = (r^2 - r + a)x + ra$, so $b - ra = (r^2 - r + a)x$. Since $b - ra, r^2 - r + a \in \mathbb{Q}$ and $x \notin \mathbb{Q}$, it follows that $r^2 - r + a = x^2 - rx + (r^2 - r) = 0$. This quadratic in x has an irrational solution x if and only if its discriminant $D = r(4-3r)$ is not a rational square, so $0 < r < \frac{4}{3}$. On the other hand, $r = \frac{4}{3} - \frac{1}{3^n}$ works for $n > 1$, so the answer is all $\alpha < \frac{4}{3}$.

9. For $p = 2, 3, 11$ this is easy, so let p be some other prime. The two conditions reduce to $p \mid (2x-1)^2 + 11$ and $p \mid (2y-1)^2 + 99$, so x and y exist if and only if -11 and -99 are quadratic residues modulo p, respectively. Since $99 = 3^2 \cdot 11$, these are simultaneously quadratic residues, and therefore the statement.

10. We have $\left(\frac{3k+2}{4k+3}\right) = \left(\frac{12k+8}{4k+3}\right) = \left(\frac{-1}{4k+3}\right) = -1$, so the answer is No.

11. For $x = \pm a^k$ we have $x^2 = a^{2k} = a \cdot a^{\frac{p-1}{2}} = a\left(\frac{a}{p}\right) = a$ by Euler criterion, since a is a quadratic residue.

12. Let a be the smallest positive quadratic non-residue modulo p. Choose the smallest k such that $ka > p$. Then $0 < ka - p < a$, so it is a q.residue and hence so is k. Therefore $k \geqslant a$, but $k < \frac{a^2}{p} + 1$, which implies the statement.

13. Since 2 is a quadratic non-residue modulo $101 \equiv 5 \pmod 8$, we have $101 \mid 2^{50} + 1$ and hence $101 \mid 2^i + 2^{50+i}$ for $i = 0, 1, \dots, 49$. Therefore $\lfloor \frac{2^i}{101} \rfloor + \lfloor \frac{2^{50+i}}{101} \rfloor = \frac{2^i + 2^{50+i}}{101} - 1$. Summing up over $i = 0, \dots, 49$ gives the result $\frac{2^{100}-1}{101} - 50$.

14. The sets $X = \{x^2 \pmod p\}$ and $Y = \{-1 - y^2 \pmod p\}$ each have $\frac{p+1}{2}$ elements (we count zero as well), so they must overlap for some x and y: then $p \mid x^2 + y^2 + 1$.

15. (a) Note that $n^4 - n^2 + 1 = (n^2-1)^2 + n^2 = (n^2+1)^2 - 3n^2$, so both -1 and 3 are quadratic residues modulo p ($p \mid n^4 - n^2 + 1$). This implies $p \equiv 1 \pmod{12}$.

    (b) By part a, if $p \mid n^8 - n^4 + 1$, then $p \equiv 1 \pmod{12}$. Moreover, $n^8 - n^4 + 1 = (n^4 + n^2 + 1)^2 - 2(n^3 - n)^2$, so 2 is also a quadratic residue modulo p...

16. If y is even, then $y^2 - 5 \equiv 3 \pmod 4$, but $x^2 + 1$ has no such divisors. On the other hand, if y is odd, then $4 \mid y^2 - 5$, but $4 \nmid x^2 + 1$.

17. Let us do (b). If $4xzy - x - y = t^2$, then $(4xz-1)(4yz-1) = 4zt^2 + 1$, so $(\frac{-z}{4xz-1}) = 1$. But if z is odd, then $(\frac{-z}{4xz-1}) = -(-1)^{\frac{z-1}{2}}(\frac{4xz-1}{z}) = (-1)^{\frac{z+1}{2}}(\frac{-1}{-z}) = -1$. Therefore $z = 2^k u$ must be even, but then $(\frac{-z}{4xz-1}) = (\frac{-2^k u}{4xz-1}) = (\frac{2}{2^{k+2}xu-1})^k(\frac{-u}{2^{k+2}xu-1}) = 1^k \cdot (-1) = -1$ by the "z odd" case.

18. There are either one or two multiples of 101 among $n, \dots, n+101$, so there can be only two subsets. On the other hand, the numbers $n, \dots, n+101$ cannot include a multiple of 103, so they are $1, 2, \dots, 102$ modulo 103, but their product is $-1 \pmod{103}$ by Wilson's theorem and is a quadratic non-residue modulo 103, a contradiction.

19. The problem is equivalent to proving that $P(0), P(1), \dots, P(100)$ are distinct modulo 101, that is, that $101 \nmid \frac{P(x)-P(y)}{x-y}$ if $101 \nmid x-y$. Suppose that $101 \mid \frac{P(x)-P(y)}{x-y} = (x^2+xy+y^2)+14(x+y)-2$ with $x \not\equiv y \pmod{101}$. Multiplying by 4 and completing squares we find that $101 \mid (2x+y+14)^2+3(y-29)^2$. However, $\left(\frac{-3}{101}\right) = -1$, so 101 must divide both $2x+y+14$ and $y-29$, but this in turn implies $x \equiv y \equiv 29 \pmod{101}$, a contradiction.

20. We know that $N \equiv 5 \pmod{12}$, so if n is prime, then 3 is its quadratic non-residue and hence $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.
On the other hand, if $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$, then the order of 3 modulo every prime divisor p of N is $N-1 = 2^{2^n}$, which implies that $N-1 \mid p-1$ and hence $p = N$.

21. The sum of quadratic non-residues is congruent to $\sum_{i=1}^{p-1} i - \sum_{j=1}^{\frac{p-1}{2}} j^2 = \frac{p(p-1)}{2} - \frac{p(p^2-1)}{24}$, which is divisible by p.

22. Here is a general method of computing sums of this type. We have $p^{n+1} = \sum_{x=0}^{p-1} \left((x+1)^{n+1} - x^{n+1}\right) = \sum_{x=0}^{p-1} \left(\binom{n+1}{1}x^n + \binom{n+1}{2}x^{n-1} + \dots + \binom{n+1}{n}x + 1\right) = \binom{n+1}{1}s_n + \binom{n+1}{2}s_{n-1} + \dots + \binom{n+1}{n}s_1 + p$. In this way, we easily obtain by induction that $p \mid s_n$ for $n = 1, 2, \dots, p-2$. Furthermore, $s_{p-1} \equiv -1$ and $s_m \equiv s_n \pmod{p}$ whenever $m \equiv n \pmod{p-1}$, and the proof is complete.

Now there is another, easier proof that uses primitive roots: since $1, 2, \dots, p-1$ are a permutation of $1, g, g^2, \dots, g^{p-2}$, where g is a primitive root modulo p, we have $s_n \equiv 1 + g^n + g^{2n} + \dots + g^{(p-2)n} = \frac{g^{(p-1)n}-1}{g^n-1} \equiv 0 \pmod{p}$ if $p-1 \nmid n$.

23. By the Euler criterion, the sum in the problem is congruent to $\sum_{x=0}^{p-1}(ax^2+bx+c)^{\frac{p-1}{2}} = \sum_{x=0}^{p-1}\left[a^{\frac{p-1}{2}}x^{p-1} + A_{p-2}x^{p-2} + \dots + A_1x + A_0\right] = a^{\frac{p-1}{2}}s_{p-1} + A_{p-2}s_{p-2} + \dots + A_1s_1 + pA_0 \equiv -a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. But make sure it is not $(p-1)\left(\frac{a}{p}\right)$!

24. For every fixed $x = 0, 1, \dots, p-1$, there are $1 + \left(\frac{a-x^2}{p}\right)$ possible values of $y \pmod{p}$. The total number of solutions is $p + \sum_{x=0}^{p-1}\left(\frac{a-x^2}{p}\right) = p - \left(\frac{-1}{p}\right)$.

25. The congruence can be rewritten as $(z-axy)^2 \equiv a^2x^2y^2 - x^2 - y^2$, so for given x, y it has $1 + \left(\frac{a^2x^2y^2-x^2-y^2}{p}\right)$ solutions. Next, if only x is fixed, we have $p + \sum_y \left(\frac{(a^2x^2-1)y^2-x^2}{p}\right)$ solutions. By the previous problem, this equals $p - \left(\frac{a^2x^2-1}{p}\right)$ if $ax \not\equiv \{-1, 0, 1\} \pmod{p}$, but $p + p\left(\frac{-1}{p}\right)$ if $ax \equiv \pm 1$ and $p + (p-1)\left(\frac{-1}{p}\right)$ if $x \equiv 0 \pmod{p}$.

Thus the total number of solutions is $p^2 - \sum_x \left(\frac{a^2x^2-1}{p}\right) + 3p\left(\frac{-1}{p}\right) = p^2 + 1 + 3p(-1)^{p'}$.

26. We can assume that $\gcd(a, b, c) = 1$. If $a^2+b^2+c^2 = 3n(ab+bc+ca)$, then $(a+b+c)^2 = (3n+2)(ab+bc+ca)$. There is a prime divisor $p \equiv 2 \pmod{3}$ of $3n+2$ with $v_p(3n+2)$

odd. Then p must divide both $a+b+c$ and $ab+bc+ca \equiv ab-(a+b)^2 = -(a^2+ab+b^2)$, but this is impossible unless $p \mid a, b, c$.

27. Clearly, x is odd. Since $3 \mid x^3+2x$ for all x, it follows that n is even. Now $(x+1)(x^2-x+3) = 2^n+2$ is a square-plus-two, so all of its odd prime divisors are 1 or 3 modulo 8. Thus $x^2-x+3 \equiv 1$ or $3 \pmod 8$, which implies $x \equiv 1$ or 3 modulo 8, but then x^3+2x+1 is resp. 4 or 2 modulo 8. Therefore $n \leqslant 2$, and only $(x, n) = (1, 2)$ is a solution.

28. We first note that $5^m - 1$ cannot be a power of 2 unless $m = 1$. Indeed, if $8 \mid 5^m - 1$, then $2 \mid m$ and hence $24 \mid 5^m - 1$.

    Let $5^m - 1 = 2^a p_1^{b_1} \cdots p_k^{b_k}$ where the p_i are distinct primes. Then $5^n - 1 = 2^{a-1} p_1^{b_1-1} \cdots p_k^{b_k-1}(p_1-1)\cdots(p_k-1)$ is also divisible by 2^a.

    Suppose that $\gcd(m, n) = 1$. Then $\gcd(5^m-1, 5^n-1) = 4$, so each $b_i = 1$ and $a = 2$. This implies that m is odd, so $5^m - 1 = 5*^2 - 1$. It follows that 5 is a quadratic residue modulo each p_i, so $p_i \equiv \pm 1 \pmod 5$. Moreover, no $p_i - 1$ is divisible by 5, so each $p_i \equiv -1 \pmod 5$. Now $-1 \equiv 5^m - 1 \equiv (-1)^{k+1}$ and $-1 \equiv -3^{k+1} \pmod 5$, implying the contradictory conditions $2 \mid k$ and $4 \mid k+1$.

29. Let $a+b = 2^k$, $c+d = 2^l$ and $a^2+b = c^2+d = n$, where $l > k$. Subtracting yields $2^k(2^{l-k}-1) = 2^l - 2^k = c-a+d-b = c-a+a^2-c^2 = (a-c)(a+c-1)$. But is a and c are of the same parity, then $a+c-1$ is odd and hence $2^k \mid a-c$, which is impossible because $0 < a-c < a+b = 2^k$. We conclude that there is at most one pair (a, b) with a odd and at most one with a even.

30. If $2 \mid y$, then modulo 4 we find that also $2 \mid x$, so $2xy+1 = 3^x - 8^y$ is a difference of squares and hence $3^{x/2} + 8^{y/2} \leqslant 2xy+1 \leqslant x^2+y^2+1$, which leaves us only with small cases to test. The only solution will be $(x, y) = (4, 2)$.

    If y is odd, then modulo 3 we find $3 \mid xy$. If $3 \mid x$, then the LHS is a difference of cubes, which we deal with as in the first case. Finally, if $3 \nmid x$, then $v_3(y) = k > 0$, then $v_3(3^x - 2xy) = k+2$, but $v_3(2xy) = k$, so $x = k$ and hence $3^x - 8^y < 0$, a contradiction.

31. If both $(a_i + i \mid 1 \leqslant i \leqslant n)$ and $(a_i - i \mid 1 \leqslant i \leqslant n)$ are complete residue systems modulo n, we have $n(n+1) = \sum_{i=1}^n (a_i+i) \equiv \sum_{j=1}^n j = \frac{n(n+1)}{2} \pmod n$, so n is odd. Moreover, $\frac{n(n+1)(2n+1)}{3} = \sum_{j=1}^n 2j^2 \equiv \sum_{i=1}^n [(a_i+i)^2 + (a_i-i)^2] = \sum_{i=1}^n (2a_i^2 + 2i^2) = \frac{2n(n+1)(2n+1)}{3} \pmod n$, so $3 \mid (n+1)(2n+1)$, i.e. $3 \nmid n$. Thus $n = 6k \pm 1$.

    On the other hand, if $n = 6k \pm 1$, then $a_i = 2i \pmod n$ satisfies the conditions.

32. (a) If $n = 8$, then $n^2+1 = 65 = 5 \cdot 13$. The board can be partitioned into 8 scattered sets. One of these scattered sets contains a multiple of 13, one does not, so their products cannot be equal modulo 65.

    (b) If $n = 10$, then $n^2+1 = 101$ is prime and has a primitive root g. Then we can arrange $g^0, g^1, g^2, \ldots, g^{99}$ in the board in this order and easily show that the condition is fulfilled.

33. We use induction. For $n \leqslant 3$ the statement holds, so assume it for $n-1$ ($n \geqslant 4$). Then $\varphi(2^{2^n}-1) = \varphi(2^{2^{n-1}}-1)\varphi(2^{2^{n-1}}+1)$. By the inductive hypothesis, $\varphi(2^{2^{n-1}}-1)$ is divisible by 2^{n^2-n+5}. On the other hand, note that $2^{2^{n-1}}+1$ cannot be a prime power: indeed, if $2^{2^{n-1}}+1 = p^k$ with $k \geqslant 2$, then k must be odd and, by the LTE, $v_2(p-1) = v_2(p^k-1) = 2^{n-1}$, which is impossible. Therefore $2^{2^{n-1}}+1$ is either a prime of has at least two distinct prime factors that are both $\equiv 1 \pmod{2^n}$ (this follows by checking the order of 2). In either case, $\varphi(2^{2^{n-1}}+1)$ is divisible by 2^{2n}, which gives us the inductive step.

34. Let $n = \prod_i p_i^{r_i+1}$ and let p be the smallest prime divisor of $\tau(n) = \prod(r_i+1)$. Suppose that $p \mid 2^{\sigma(n)}-1$. The order of 2 modulo p divides $\gcd(p-1, \sigma(n))$, so there is a prime $q < p$ dividing $\sigma(n) = \prod_i \frac{p_i^{r_i+1}-1}{p_i-1}$. Hence $q \mid \frac{p_i^{r_i+1}-1}{p_i-1}$ for some i, so the order of p_i modulo q divides r_i+1. Since $\gcd(r_i+1, q-1) = 1$ by the assumption, it follows that this order is 1, i.e. $q \mid p_i - 1$, and hence $q \mid \frac{p_i^{r_i+1}-1}{p_i-1} \equiv r_i + 1 \pmod{q}$. This is again impossible, as $\gcd(r_i+1, q) \mid \gcd(\tau(n), q) = 1$. Therefore the only solution is $n = 1$.

35. Let $y = \frac{m}{n}$, where $\gcd(m,n) = 1$. Since $x^y = \frac{m+n}{m}$ is also an m-th power of a rational number and $m, m+n$ are coprime, it follows that both $m, m+n$ are m-th powers. But $2^m > m$, so m can be an m-th power only for $m = 1$. Then $(x,y) = ((n+1)^n, \frac{1}{n})$, where $n \in \mathbb{N}$.

36. We observe that $a_k \in \{0, 1, \ldots, k-1\}$ is the number such that $a_1 - a_2 + a_3 - \cdots + (-1)^k a_{k-1} = kb_k$ for some integer b_k. If k is even and $b_k > 0$, then b_k does not increase; if k is odd and $b_k > 0$, then b_k decreases at least by 1; if $b_k = 0$, then all consequent terms a_i and b_i ($i > k$) are zero. Thus b_k reaches zero before its 2021^{2022}-th term, so all the a_i after it are zero, and $a_{2021^{2022}} = 0$.