Number Theory – group L2

Instructor: Dušan Djukić *Date: 27.2.2022.*

1. Suppose that a and b are integers such that $2^n a + b$ is a perfect square for every $n \in \mathbb{N}$. Prove that $a = 0$.

2. Does there exist an integer x such that $x^2 + 2$ is divisible by 3^{2022}?

> Recall *Wilson's theorem*
> If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

3. Is there a positive integer n such that $n! + 1$ is divisible by $n + 100$?

4. Find all triples of positive integers a, b, c such that $a \mid bc + 1$, $b \mid ac + 1$ and $c \mid ab + 1$.

> Recall *Euler's totient function*
> Given a positive integer n with the prime factorization $n = p_1^{r_1} \cdots p_k^{r_k}$, Euler's totient function $\varphi(n)$ counts the remainders modulo n (i.e. numbers among $0, 1, \dots, n-1$) that are coprime to n:
> $$\varphi(n) = p_1^{r_1-1}(p_1 - 1) \cdots p_k^{r_k-1}(p_k - 1) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

5. Prove that there is a positive integer n, not divisible by any of the numbers from 2 to 1000, such that the numbers $n^2 - 1$, $n^2 - 2, \dots, n^2 - 1000$ are all composite.

> Recall *multiplicative inverses*
> Given a positive integer n and an integer a coprime to n, an *inverse* of a modulo n is an integer $a^{-1} := b$ such that $ab \equiv 1 \pmod{n}$. It is unique modulo n.
>
> It can be found by Euclidean algorithm. Here is how. We take $n = \boxed{999}$ and $a = \boxed{128}$.
>
> *Step 1.*
> The Euclidean algorithm yields a decaying sequence of remainders.
> $$\begin{aligned} 999 - 7 \cdot 128 &= \boxed{103} \\ 128 - 1 \cdot 103 &= \boxed{25} \\ 103 - 4 \cdot 25 &= \boxed{3} \\ 25 - 8 \cdot 3 &= \boxed{1} \end{aligned}$$
>
> *Step 2.*
> Now we express 1 in terms of boxed remainders, repeatedly eliminating the smallest ones.
> $$\begin{aligned} 1 &= \boxed{25} - 8 \cdot \boxed{3} \\ &= 25 - 8(103 - 4 \cdot 25) = 33 \cdot \boxed{25} - 8 \cdot \boxed{103} \\ &= 33(128 - 103) - 8 \cdot 103 = 33 \cdot \boxed{128} - 41 \cdot \boxed{103} \\ &= 33 \cdot 128 - 41(999 - 7 \cdot 128) = 320 \cdot \boxed{128} - 41 \cdot \boxed{999}. \end{aligned}$$
>
> Thus $320 \cdot 128 \equiv 1 \pmod{999}$, which means that the inverse of 128 modulo 999 is 320.

6. Denote $m = 2^{100}$ and $n = 3^{100}$. Prove that there exist positive integers a, b, c, d such that $am - bn = cm - dn = ad - bc = 1$.

Number Theory – group L2

Instructor: Dušan Djukić *Date: 28.2.2022.*

7. Are there 20 positive integers $a_1, \ldots, a_{10}$, $b_1, \ldots, b_{10}$ with the following property: For every subset of indices $S \subseteq \{1, \ldots, 10\}$, the sum $\sum_{i \in S} a_i$ divides $12 + \sum_{i \in S} b_i$?

8. If $a, b, c, d, e, f, g, h, i$ are the numbers $1, 2, 3, 4, 5, 6, 7, 8, 9$ in some order, what is the minimum possible value of $\frac{abc-def}{ghi}$?

9. Denote by $S(n)$ the sum of decimal digits of number n. Prove that there are infinitely many positive integers k such that $S(2^k) > S(2^{k+1})$.

Number Theory – group L2

Instructor: Dušan Djukić *Date: 1.3.2022.*

10. Last k digits of some perfect square are equal and nonzero. At most how much can k be, and for which digit is it possible?

11. Is there a perfect square that ends with the digits (a) 987654321? (b) 987654329?

12. Is there a perfect square that *starts* with the digits 987654321?

13. Prove that there exists a multiple of 5^{100} whose all digits are odd.

14. Using each of the digits $1, 2, 3, \dots, 8, 9$ exactly once, we form nine nine-digit numbers, not necessarily distinct. Their sum ends in n zeroes. Find the maximum possible n.

15. Find all positive integers n with the property that the numbers $n, 2n, 3n, \dots, n^2$ all have the same sum of digits.

16. Prove that every positive integer $n > 1$ has a multiple less than n^4 whose decimal expansion contains at most four distinct digits.

17. Are there nonzero integers a, b, c, d such that $ac + bd = 16$ and $ad - bc = 1$?

Number Theory – group L2

Instructor: Dušan Djukić *Date: 2.3.2022.*

18. Define $p_1 = 2$ and, for $n \geqslant 2$, p_n is the largest prime factor of $p_1 p_2 \cdots p_{n-1} + 1$. Prove that no term p_n is equal to 5.
19. Find all triples of positive integers a, b, c such that $b^2 + 1$ and $c^2 + 1$ are both prime and $a^2 + 1 = (b^2 + 1)(c^2 + 1)$.
20. Find all primes p, q such that $p^3 - q^5 = (p + q)^2$.
21. Solve the equation $x^2 + 4 = y^5$ in integers.
22. Does the equation $x^4 + y^3 = z! + 7$ have infinitely many solutions in positive integers?
23. Let p and q be two primes with $p < q < 2p$. Prove that there exist two consecutive positive integers such that their largest prime divisors are p and q (in some order).
24. Given $a_0 = a$, define $a_{n+1} = 22a_n + 1$. Is it possible to choose a so that a_{2021} be divisible by 2021?
25. The sequence (a_n) is defined by $a_1 = 1$, $a_2 = 3$ and $a_{n+2} = (n + 3)a_{n+1} - (n + 2)a_n$. Find all values of n for which a_n is divisible by 11.

Linear recurrences

Sequences (x_n) defined by a recurrence relation of the form

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k}, \qquad (\spadesuit)$$

with the first k terms given, can be solved in closed form. Here is how.

We first check if there are exponential sequences of the form $x_n = \alpha^n$ that satisfy ($\spadesuit$). It turns out that the constant α must satisfy $P(x) = x^k - c_1 x^{k-1} - \cdots - c_{k-1}x - c_k = 0$. The polynomial $P(x)$ is called the *characteristic polynomial.*

So, let the zeros of $P(x)$ be $\alpha_1, \ldots, \alpha_\ell$. We allow multiple roots, so let r_i be the multiplicity of the zero α_i. Then the sequence $x_n = \alpha_i^n$ satisfies ($\spadesuit$). Moreover, even the sequence $x_n = n^k \alpha_i^n$ satisfies ($\spadesuit$), if $0 \leqslant k \leqslant r_i - 1$ is an integer. In general, every linear combination of the described sequences, and no others, satisfies ($\spadesuit$).

To sum up, a formula for x_n will have the form

$$x_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_\ell(n)\alpha_\ell^n,$$

where $P_i(x)$ are some polynomials of degree strictly less than r_i.

26. Find a_n in closed form if:
(a) $a_0 = 0$, $a_1 = 1$ and $a_n = 2a_{n-1} + a_{n-2}$ for $n \geqslant 2$;
(b) $a_0 = a_1 = 0$, $a_2 = 1$, $a_n = 3a_{n-2} - 2a_{n-3}$.

Number Theory – group L2

Instructor: Dušan Djukić *Date: 3.3.2022.*

27. Define $a_0 = 0$ and $a_{n+1} = 3a_n + \sqrt{8a_n^2 + 1}$. Prove that each term a_n is an integer.

28. The Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 2$.
(a) Find F_n in closed form.
(b) Prove that one of $5F_n^2 + 4$ and $5F_n^2 - 4$ is a perfect square.

29. Let $a_0 = 1$ and $a_{n+1} = \frac{1+a_n}{3+a_n}$. Find a_n in closed form.

30. A sequence (a_n) satisfies $a_{n+1} = a_n^3 + 103$ for all $n \in \mathbb{N}$. Prove that this sequence contains at most one perfect square.

31. Is there a positive integer greater than 10^{100}, having no zero digits, such that switching two of its digits yields a number with the same set of prime divisors?

32. If a prime p divides $x^2 + y^2$ for some integers x, y, but $p \nmid xy$, prove that $p \equiv 1 \pmod 4$ or $p = 2$.

33. If x, y are positive integers, prove that $4xy - x - y$ cannot be a perfect square.

34. If a prime p divides $x^2 + xy + y^2$ for some integer x, y, but $p \nmid xy$, prove that $p \equiv 1 \pmod 3$ or $p = 3$.

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

Solutions – group L2

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

1. Note that $3b = 4(2^n a + b) - (2^{n+2}a + b)$. But $b = 0$ does not work, and if $a \neq 0$, then we get infinitely many ways to write $3b$ as a difference of two squares, which is impossible. Thus we must have $a = 0$.

2. We prove by induction on n that there is x such that $3^n \mid x^2 + 2$.

   Base of induction is $n = 1$: then e.g. $x = 1$.

   Inductive step: Assuming there is x with $3^n \mid x^2 + 2$, we will find y with $3^{n+1} \mid y^2 + 2$. We set $y = x + 3^n k$. Then $y^2 + 2 = x^2 + 2 + 2x \cdot 3^n k + 3^{2n}k^2$ is divisible by 3^{n+1} if $2x \cdot k \equiv -\frac{x^2+2}{3^n} \pmod 3$, and such a k obviously exists.

3. We will find n such that $p = n + 100$ is a prime. Since $p \mid (p-1)! + 1$, we infer $p \mid (p-1)! - (p-100)! = (p-100)! \cdot [(p-1)(p-2)\cdots(p-99) - 1] \equiv -99! - 1$, so it is enough to take for p any prime divisor of $99! + 1$ (then clearly $p > 100$, so $n > 0$).

4. Each of the numbers a, b, c divides $ab+bc+ca+1$. The numbers a, b, c must be pairwise coprime, so $abc \mid ab+bc+ca+1$, i.e. $F = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc}$ is an integer. Let $a \leqslant b \leqslant c$.

   For $a \geqslant 3$ we have $F \leqslant \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{60} < 1$, so no solutions.

   If $a = 2$, then $b \geqslant 5$ leads to $F < 1$, and $b = 4$ is impossible, so $b = 3$ and $c \mid 2 \cdot 3 + 1$, i.e. $(a, b, c) = (2, 3, 7)$.

   If $a = 1$, then $b \mid c + 1$ and $c \mid b + 1$ and we get three more solutions: $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 3)$.

5. Take $n = 1000!m + 1$. Then $n^2 - k = m^2 \cdot 1000! - 2m \cdot 1000! - (k-1)$ is obviously composite for $k = 1, 3, 4, 5, \dots, 1000$. As for $n^2 - 2$, we can set m to make it divisible by e.g. $33^2 - 2 = 1087$ which is a prime, and it is enough to take m so that $1000!m \equiv 32 \pmod{1087}$.

   (Alternatively, instead of 1087, which is prime by chance, we could have taken any odd prime divisor of $1000!^2 - 2$.)

6. Taking a to be a multiplicative inverse of m modulo n we find a, b with $am - bn = 1$.

   Take $c = a + n$ and $d = b + m$. Then also $cm - dn = 1$. Moreover, $ad - bc = a(b+m) - b(a+n) = 1$.

7. If there are two disjoint sums $\sum_{i \in S} a_i$ and $\sum_{i \in T} a_i$ (i.e. with $S \cap T = \emptyset$) that are both divisible by 5, then 5 would also divide each of $12 + \sum_{i \in S} b_i$, $12 + \sum_{i \in T} b_i$ and $12 + \sum_{i \in S \cup T} b_i$. Subtracting these we would obtain $5 \mid 12$, a contradiction.

So, let us just prove that such disjoint sums exist. Among the 11 partial sums $s_k = a_1 + a_2 + \dots + a_k$ $(0 \leqslant k \leqslant 10)$ there are three s_i, s_j, s_k $(i < j < k)$ that give the same remainder upon division 5, but then $s_j - s_i$ and $s_k - s_j$ are disjoint sums divisible by 5, as desired.

8. If $abc - def \geqslant 2$, then the expression $D = \frac{abc-def}{ghi}$ cannot be less than $\frac{2}{7 \cdot 8 \cdot 9} = \frac{1}{252}$.

   On the other hand, if $abc = m$ and $def = m - 1$, then D will be smallest when m is smallest. Since $abc \cdot def \geqslant 6! = 720$, we must have $abc \geqslant 28$. For $28 \leqslant m \leqslant 35$ this is impossible, but for $m = 36$ we find $2 \cdot 3 \cdot 6 - 1 \cdot 5 \cdot 7 = 1$ and then $\frac{2 \cdot 3 \cdot 6 - 1 \cdot 5 \cdot 7}{4 \cdot 8 \cdot 9} = \frac{1}{288}$, which is the smallest possible value.

9. Assume to the contrary that $S(2^k) \leqslant S(2^{k+1})$ whenever k is big enough, say $k \geqslant m$. Since 2^k and hence $S(2^k)$ gives remainders $1, 2, 4, 8, 7, 5$ when $k \equiv 0, 1, 2, 3, 4, 5 \pmod 6$, it means that $S(2^{k+1}) - S(2^k) \equiv 1, 2, 4, 8, 7, 5 \pmod 6$, so $S(2^{k+6}) - S(2^k) \geqslant 27$ whenever $k \geqslant m$. This implies $S(2^{m+6t}) \geqslant 27t$ and consequently $2^{m+6t} > 10^{3t}$ for every t, but this is false already for $t = m$, a contradiction.

10. A square never ends with $2, 3, 7, 8$ (modulo 10), nor with $11, 55, 66, 99$ (modulo 4), so the only acceptable last digits are 4. A square can end with 444 ($38^2 = 1444$), but it cannot end with 4444, because $10000k + 4444 = 4(2500k + 1111)$ and $2500k + 1111$ is 3 modulo 4 and cannot be a square. Hence the largest k is 3.

11. In (a) we can take e.g. $111111111^2 = 12345678987654321$.

    In (b) note that $1^2, 3^2, 5^2, \dots, (\frac{10^9}{8} - 1)^2$ are all distinct modulo 10^9 and all are $1 \pmod 8$, so they take all the 9-digit endings that are $1 \pmod 8$, including 987654329.

    (Explicitly: $30168427^2 = 910133987654329$.)

12. Let $\sqrt{987654321}$ and $\sqrt{987654322}$ differ in k-th decimal. Then between $10^k\sqrt{987654321}$ and $10^k\sqrt{987654322}$ there is an integer m, and m^2 obviously starts with 987654321.

    (Explicitly: $3142696806^2 = 9876543214442601636$.)

13. We will inductively construct an n-digit number x_n with odd digits that is divisible by 5^n. Start with $x_1 = 5$. Given x_n, take $x_{n+1} = x_n + k \cdot 10^n$, where $k \in \{1, 3, 5, 7, 9\}$ is such that $\frac{x_{n+1}}{5^n} = \frac{x_n}{5^n} + 2^n k$ is divisible by 5.

14. The sum cannot end in 9 zeroes, because all numbers are divisible by 9 and $9 \cdot 987654321 < 9000000000$. On the other hand, $8 \cdot 987654321 + 198765432 = 8100000000$, so it can end in 8 zeroes.

15. Number 1 works, but 10^k does not if $k \geqslant 1$. On the other hand, $10^k - 1 = 99 \cdots 99$ works. Indeed, it suffices to check multiples not divisible by 10: then $\overline{a_{k-1} \dots a_1 a_0} \cdot \overline{99 \dots 99} = \overline{a_{k-1} \dots a_1 c_0 b_{k-1} \dots b_1 d_0}$, where $c_0 = a_0 - 1$, $b_i = 9 - a_i$ for $i \geqslant 1$ and $d_0 = 10 - b_0$. For instance, $135 \cdot 999 = 134\,865$.

    Assume that $10^k < n < 10^{k+1} - 1$ and consider $(10^k + 1)n$. Its last k digits coincide with those in n, and the number consisting of the first $k + 1$ digits is larger than n, so its sum of digits is greater than the first digits of n. Hence the sum of digits of $(10^k + 1)n$ is greater than the sum of digits of n. Therefore the answer is $n = 1$ or $n = 10^k - 1$.

16. Let $10^k \leqslant n < 10^{k+1}$. The statement is trivial if $k \leqslant 4$ (n itself works), so assume that $k \geqslant 5$. Consider all numbers with at most $4k$ digits consisting of digits 0 and 1 only. There are 2^{4k} such numbers and all are less than n^4. Since $2^{4k} > 10^{k+1} > n$, two of these numbers give the same remainder modulo n, so their difference is a multiple od n. Moreover, it is less than n^4 and has only digits $0, 1, 8, 9$.

17. Note that $(a^2+b^2)(c^2+d^2) = a^2c^2+b^2d^2+a^2d^2+b^2c^2 = (ac+bd)^2+(ad-bc)^2 = 257$ is prime, so either $a^2+b^2 = 1$ or $c^2+d^2 = 1$, which is impossible if all the numbers are nonzero.

18. Since $p_2 = 3$, the number $p_1 \cdots p_{n-1} + 1$ is not divisible by 2 or 3, so if $p_n = 5$, we must have $p_1 \cdots p_{n-1} + 1 = 5^k$ for some k. But then $p_1 \cdots p_{n-1} = 5^k - 1$ is divisible by 4, which is impossible.

19. If $b = c$, then $(b^2+1)^2 - a^2 = 1$, which is impossible. Let $b > c$ and denote $b^2+1 = p$. Note that then $a^2+1 < p^2$, so $b < a < p$. On the other hand, since $p \mid (a+b)(a-b) = c^2(b^2+1)$, we have $a \equiv \pm b \pmod{p}$, so we must have $a = p - b = b^2 - b + 1$. Direct computation yields $a^2+1 = (b^2+1)(b^2-2b+2)$, so $c = b-1$. But if b^2+1 is an odd prime, then b^2-2b+2 is even, so it must be 2. Thus $b = 2$, $c = 1$ and $a = 3$.

20. Since $p^3 \equiv p$ and $q^5 \equiv q \pmod{3}$, we have $p - q \equiv (p+q)^2 \pmod{3}$. If $3 \mid p - q$, then also $3 \mid p + q$, so $p = q = 3$, which is not a solution. Therefore $p - q \equiv (p+q)^2 \equiv 1 \pmod{3}$, but $p + q \equiv 1$ or 2, implying $3 \mid q$ and $3 \mid p$, respectively. For $p = 3$ we get no solutions, and for $q = 3$ we get the only solution $(p, q) = (7, 3)$.

21. Modulo 11, the possible remainders of x^2+4 modulo 11 are $2, 4, 5, 7, 8, 9$, whereas y^5 can give only remainders $0, 1, 10$. So the equation is incompatible modulo 11.

22. If $z \geqslant 13$, then the equation is incompatible modulo 13, because $x^4 \equiv 0, 1, 3, 9$, $y^3 \equiv 0, 1, 5, 8, 12$ and $x^4 + y^3 \not\equiv 7 \pmod{13}$. Therefore all solutions (if any exist) must have $z < 13$ and hence are only finitely many,

23. Since $-\frac{q-1}{2}, \dots, \frac{q-3}{2}, \frac{q-1}{2}$ form a complete residue system modulo q, there is an integer a with $a < \frac{q}{2} < p$ such that $ap \equiv 1 \pmod{q}$. Then the largest prime divisor of $|a|p \pm 1$ is q, while that of $|a|p$ is p.

24. Define $b_{2021} = 0$ and $b_{n-1} = 22^{-1}(b_n - 1) \pmod{2021}$. Clearly $a_0 \equiv b_0 \pmod{2021}$ works.

25. The first few terms modulo 11 are $1, 3, 9, 0, 10, 4, 6, 0, 1, 0, 0$. From this point on, all terms are divisible by 11. Thus the answer is $n = 4$, $n = 8$ and $n \geqslant 10$.

26. (a) The characteristic polynomial is $P(t) = t^2 - 2t - 1$ and its zeros are $1 + \sqrt{2}$ and $1 - \sqrt{2}$. It follows that $a_n = A(1+\sqrt{2})^n + B(1-\sqrt{2})^n$ for some constants A, B. Moreover, $a_0 = 0 = A + B$ and $a_1 = 1 = A(1+\sqrt{2}) + B(1-\sqrt{2})$ give $A = -B = \frac{1}{2\sqrt{2}}$, so $a_n = \frac{1}{2\sqrt{2}}[(1+\sqrt{2})^n - (1-\sqrt{2})^n]$.

    (b) The characteristic polynomial is $t^3 - 3t + 2$, with a double root $t = 1$ and a root $t = -2$. It follows that $a_n = (A + Bn) \cdot 1^n + C(-2)^n$. Plugging in $n = 0, 1, 2$ gives us a_0, a_1, a_2 yields $A = -\frac{1}{9}$, $B = \frac{1}{3}$, $C = \frac{1}{9}$, so $a_n = \frac{(-2)^n + 3n - 1}{9}$.

27. We have $(a_{n+1}-3a_n)^2 = 8a_n^2+1$, i.e. $a_{n+1}^2 - 6a_na_{n+1} + a_n^2 = 1$. Subtracting the analogous equation for $n-1$, which is $a_{n-1}^2 - 6a_na_{n-1} + a_n^2 = 1$, we obtain $a_{n+1}^2 - a_{n-1}^2 = 6a_n(a_{n+1}-a_{n-1})$. Canceling $a_{n+1}-a_{n-1}$ (which is obviously positive) yields $a_{n+1} = 6a_n - a_{n-1}$. All terms are integers by induction.

28. (a) The characteristic polynomial of F_n is t^2-t-1 with the zeros $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$, so $F_n = A\phi^n + B\bar{\phi}^n$. From $F_0 = 0$ and $F_1 = 1$ we find $A = -B = \frac{1}{\sqrt{5}}$, so $F_n = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}}$.

    (b) Using $\phi\bar{\phi} = -1$ we obtain $5F_n^2 = \phi^{2n} + \bar{\phi}^{2n} - 2(-1)^n$, so $5F_n^2 + 4(-1)^n = (\phi^n + \bar{\phi}^n)^2$. Finally, note that $L_n = \phi^n + \bar{\phi}^n$ is an integer, because $L_0 = 2$, $L_1 = 1$ and $L_{n+1} = L_n + L_{n-1}$.

29. Write $a_n = \frac{x_n}{y_n}$, assuming the initial values $x_0 = y_0 = 1$. Then $\frac{x_{n+1}}{y_{n+1}} = a_{n+1} = \frac{y_n + x_n}{3y_n + x_n}$, so we can define $x_{n+1} = x_n + y_n$ and $y_{n+1} = x_n + 3y_n$.

    We will eliminate y_n. The first relation gives $y_n = x_{n+1} - x_n$ and consequently $y_{n+1} = x_{n+2} - x_{n+1}$, so the second relation becomes $x_{n+2} - x_{n+1} = x_n + 3(x_{n+1} - x_n)$, i.e. $x_{n+2} - 4x_{n+1} + 2x_n = 0$. From here we obtain $x_n = A(2+\sqrt{2})^n + B(2-\sqrt{2})^n$, and from the initial values $x_0 = 1$ and $x_1 = 2$ we find $A = B = \frac{1}{2}$, so $x_n = \frac{1}{2}[(2+\sqrt{2})^n + (2-\sqrt{2})^n]$. For y_n we get $y_n = x_{n+1} - x_n = \frac{1}{2}[(1+\sqrt{2})(2+\sqrt{2})^n + (1-\sqrt{2})(2-\sqrt{2})^{n+1}]$.

30. We can assume w.l.o.g. that $a_0 = x^2$ is a square. Then $a_0 \equiv 0, 1 \pmod 4$, which implies $a_1 \equiv 3, 0 \pmod 4$ and $a_2 \equiv 2, 3 \pmod 4$. By induction it follows that $a_n \equiv 2, 3 \pmod 4$ for every $n \geqslant 2$, so a_n is not a square if $n \geqslant 2$.

    It remains to verify that $a_1 = x^6 + 103$ is not a square. If to the contrary $a_1 = y^2$, then $(y - x^3)(y + x^3) = 103$ is a prime, implying that $x^3 = 51$, a contradiction.

31. The answer is *yes*. Consider the number $x = \overline{144\dots443} = 13 \cdot \frac{10^k-1}{9}$. Switching the digits 1 and 3 yields number $y = 31 \cdot \frac{10^k-1}{9}$. The numbers x and y have the same set of prime divisors if $\frac{10^k-1}{9}$ is a multiple of $13 \cdot 31$, which by Euler's theorem happens whenever $\varphi(13 \cdot 31) = 360$ divides k.

32. Suppose that $p \equiv 3 \pmod 4$. Then $\frac{p-1}{2}$ is odd. Since $y^2 \equiv -x^2 \pmod p$, raising to $\frac{p-1}{2}$-th power gives us $1 \equiv y^{p-1} \equiv -x^{p-1} \equiv -1 \pmod p$, which is impossible.

33. If $4xy - x - y = z^2$, then $(4x-1)(4y-1) = 4z^2 + 1$, so $4x^2+1$ has at least one prime divisor of the form $4k-1$, which is impossible by the previous problem.

34. Suppose that $p = 3k+2$. Since $p \mid x^3 - y^3$, we have $y^{p-2} = y^{3k} \equiv x^{3k} = x^{p-2}$, and since also $y^{p-1} \equiv x^{p-1}$ by Fermat's theorem, we deduce that $y \equiv x$. But then $p \mid x^2 + xy + y^2 \equiv 3x^2 \pmod p$, so $p \mid 3$, which is a contradiction.

35. (a) Note that $p \mid q^3 + 1$, and since $p > q+1$, this means that $p \mid (-q)^2 - q + 1$. By the previous problem, this is possible only if $p = 3$ or $p \equiv 1 \pmod 3$. However, the former case would yield no solution, so we have $p \equiv 1 \pmod 3$, but then $3 \mid q^3 + q = q(q^2+1)$, so $3 \mid q$, i.e. $q = 3$. Solving the cubic yields $p = 7$.

(b) We will prove more. 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 $q \leqslant 5$. For $q = 2$ we get no solution, but for $q = 5$ we get another solution: $p = 14$.