Lemma: If a, b, c are positive integers and $a^b \equiv 1 \pmod p$, $a^c \equiv 1 \pmod p$ then $a^{\gcd(b,c)} \equiv 1 \pmod p$.

Problem 1: Let n be an odd integer. Prove that n does not divide 3^n+1.

Idea: recall the classic problem

Let n be an integer with $n \geq 2$, show that $n \nmid 2^n - 1$.

Proof: on the board.

Problem 2: Let p be an odd prime, and let q and r be primes such that $p \mid q^r+1$. Prove that either $2r \mid p-1$ or $p \mid q^2-1$

$$q^r \equiv -1 \pmod p \Rightarrow q^{2r} \equiv 1 \pmod p$$

$$q^{p-1} \equiv 1 \pmod p$$

$$\Rightarrow q^{\gcd(p-1, 2r)} \equiv 1 \pmod p$$

① $\gcd(p-1, 2r) = 2$

$q^2 \equiv 1 \pmod p$

② $\gcd(-,-) = 2r$

$2r \mid p-1$

Example 2.5.9. *Let a and b be relatively prime integers. Prove that any odd divisor of $a^{2^n} + b^{2^n}$ is of the form $2^{n+1}m + 1$.*

Hint: consider an odd prime p divisor for $a^{2^n}+b^{2^n}$ and prove it's on the form $2^{n+1}m+1$.

$$p \mid a^{2^n}+b^{2^n} \Rightarrow a^{2^n} \equiv -b^{2^n} \pmod p$$

$$\Rightarrow a^{2^{n+1}} \equiv b^{2^{n+1}} \pmod p$$

$$\Rightarrow (\underbrace{a b^{-1}}_{c})^{2^n} \equiv -1 \pmod p$$

$$c^{2^n} \equiv -1 \pmod p$$

$$c^{\gcd(p-1,\,2^{n+1})} \equiv 1 \pmod p \Leftarrow \begin{cases} c^{2^{n+1}} \equiv 1 \pmod p \\ c^{p-1} \equiv 1 \pmod p \end{cases}$$

Example 2.5.10 (Bulgaria 1996). *Find all pairs of prime p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.*

Example 2.5.11 (USA TST 2003). *Find all ordered prime triples (p, q, r) such that $p \mid q^r + 1$, $q \mid r^p + 1$, and $r \mid p^q + 1$.*

Theorem 3.3.1. *For p being an odd prime relatively prime to integers a and b with $p \mid a - b$ then*

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers (x, p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

Example 3.3.4 (Bulgaria). *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

Determine all the pairs (p, n) of a prime number p and a positive integer n for which $\dfrac{n^p + 1}{p^n + 1}$ is an integer.

(APMO 2012)

N1. Find all pairs (k, n) of positive integers for which $7^k - 3^n$ divides $k^4 + n^2$.

(Austria)

(IMO 2007)

Example 2.5.10 (Bulgaria 1996). *Find all pairs of prime p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.*

Assume that $q > p$: $p \mid 5^p - 2^p$ or $p \mid 5^q - 2^q$

<u>Case 1</u>: $p \mid \underbrace{5^p - 2^p}_{5-2} \Rightarrow p \mid 3$ from Fermat's

<u>Case 2</u>: $p \mid 5^q - 2^q \Rightarrow 5^q \equiv 2^q \pmod{p}$

$$\Rightarrow (5 \cdot 2^{-1})^q \equiv 1 \pmod{p}$$

$$(5\, 2^{-1})^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow (5 \cdot 2^{-1})^{\gcd(q, p-1) = 1} \equiv 1$$

$$5 \equiv 2 \pmod{p} \Rightarrow p = 3$$

$\Rightarrow \boxed{p = 3}$ $\quad \cancel{3}q \mid (5^3 - 2^3)(5^q - 2^q)$

mod $q \Rightarrow 117 \times 3 \equiv 0 \pmod{q}$

$$\Rightarrow q \times 13 \times 3 \equiv 0 \pmod{q}$$

$$\Rightarrow q = 13 \text{ or } 3$$

$$(p, q) = (13, 3), (3, 13), (3, 3)$$

Example 2.5.11 (USA TST 2003). *Find all ordered prime triples (p, q, r) such that $p \mid q^r + 1$, $q \mid r^p + 1$, and $r \mid p^q + 1$.*

Assume that $p, q, r \neq 2$.

$$q^r \equiv -1 \pmod p$$

$$q^{2r} \equiv +1 \pmod p, \quad q^{p-1} \equiv 1 \pmod p$$

$\{2, 2r\} \ni \underline{\mathrm{ord}_p(q)} \mid \gcd(2r, p-1) = 2, \underline{2r}$

$\{2, 2p\} \ni \mathrm{ord}_q(r) \mid 2, 2p$

$\{2, 2q\} \ni \mathrm{ord}_r(p) \mid 2, 2q$

$$\mathrm{ord}_p(q) \mid p-1 \Rightarrow 2 \text{ or } \boxed{2r \mid p-1}$$

$$2 \text{ or } 2p \mid q-1$$

$$2 \text{ or } \boxed{2q \mid r-1}$$

$$\mathrm{ord}_p(q) = 2 \Rightarrow q^2 \equiv 1 \pmod p$$

$$p \mid q+1 \text{ or } \boxed{2r \mid p-1}$$

$q < r+1 \leftarrow \boxed{q \mid r+1}$ or $2p \mid q-1$

$\boxed{r \mid p+1}$ or $\boxed{2q \mid r-1}$

① ②

Case ①

$$\left.\begin{array}{l} r \mid p+1 \\ q \mid r+1 \\ 2r \mid p-1 \end{array}\right\} \quad r \mid 2 \Rightarrow r = 2 \times$$

Case ②

$$\left.\begin{array}{l} 2q \mid r-1 \\ q \mid r+1 \\ 2r \mid p-1 \end{array}\right\} \quad q \mid 2 \Rightarrow q = 2 \times$$

Example 2.5.11 (USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

$(2,2,2) \longrightarrow \times$

$(p,2,2) \longrightarrow \quad p \mid 2^2+1 \Rightarrow p=5$

$2 \mid 5^2+1$

$2 \mid 2^p+1 \Longrightarrow \times$

$(p,q,2) \longrightarrow \quad p \mid q^2+1$

$q \mid 2^p+1 \Longrightarrow \text{ord}_q 2 \mid 2p,\ q-1 \Rightarrow \text{ord}=2, 2p$

$\cancel{2 \mid p^q+1}$

Case 1 $\quad \text{ord}_q 2 = 2 \qquad 2^2 \equiv 1 \pmod q$

$\Rightarrow p \mid q^2+1$

$q \mid 2^2-1 = 3 \Rightarrow q=3$

$\Rightarrow \quad p \mid q^2+1 \Rightarrow p=5$

$(2,3,5)$

Case 2 $\quad \text{ord} = 2p$

$2^{2p} \equiv 1 \pmod q$

$2p \mid q-1 \Longrightarrow p \mid q^2-1$

$\boxed{p \mid q^2+1}$

$p \mid 2$

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers (x, p) such that p is prime, $x \le 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

If x is even $\Rightarrow 2 \mid (p-1)^x+1 \Rightarrow p=2 \Rightarrow x=2$

$\Rightarrow$ x is odd

Let q be the smallest prime $q \mid x$

$$\Rightarrow q^{p-1} \mid (p-1)^x+1$$

$$(p-1)^x \equiv -1 \pmod{q}$$

$$\operatorname{ord}_q p-1 \mid \gcd(2x, q-1) = 2$$

because q is the smallest divisor for x

$$\Rightarrow \operatorname{ord}_q p-1 = 2 \Rightarrow (p-1)^2 \equiv 1 \pmod{q}$$

$$\Rightarrow q \mid \boxed{(p-2)}\, p$$

$$p \equiv 2 \pmod{q} \Rightarrow p-1 \equiv 1 \pmod{q}$$

$$\Rightarrow p = q$$

$$p^{p-1} \mid (p-1)^x + 1$$

$$v_p((p-1)^x+1) = v_p((p-1)+1) + v_p(x)$$

$$p-1 \le 1 + v_p(x) \Rightarrow v_p(x) \ge p-2$$

$$\Rightarrow x \ge p^{p-2}$$

$$\Rightarrow 2p \ge p^{p-2}$$

$$\Rightarrow 2 \ge p^{p-3} \Rightarrow \boxed{p \le 3}$$

$$\Rightarrow (3,3), (2,2), (1,p)$$

Example 3.3.4 (Bulgaria). *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

$$n = \underline{\underline{p_1}}^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}, \quad 3^n - 2^n = q^\alpha$$

$$q^\alpha = 3^n - 2^n = \left(3^{\frac{n}{p_1}}\right)^{p_1} - \left(2^{\frac{n}{p_1}}\right)^{p_1} = \left(3^{\frac{n}{p_1}} - 2^{\frac{n}{p_1}}\right)\left(\text{———}\right)$$

$$\Rightarrow \boxed{3^{n/p_1} - 2^{n/p_1} = q^\beta}, \quad 3^n - 2^n = q^\alpha$$

$$\alpha > \beta$$

$$\underbrace{v_q(3^n - 2^n)}_{\alpha} = v_q\left(3^{\frac{n}{p_1}} - 2^{\frac{n}{p_1}}\right) + \underline{v_q(p_1)}$$

$$\alpha = \beta + v_q(p_1)$$

$$\Rightarrow p_1 = q$$

$$n = p^x, \quad 3^{p^x} - 2^{p^x} = p^\alpha$$

ord 3.2

Determine all the pairs (p, n) of a prime number p and a positive integer n for which $\dfrac{n^p+1}{p^n+1}$ is an integer.

(APMO 2012)

Assume that $p>3$. Take a prime q s.t. $q^\alpha \mid p+1$

$\Rightarrow q^\alpha \mid n^p+1 \Rightarrow \mathrm{ord}_{q^\alpha}(n) = d_q \mid 2p, (q-1)q^{\alpha-1}$

$\Rightarrow d_q = 2$ or $2p$

but $d_q \mid q-1$ and $q \leq p+1$

$\Rightarrow d_q = 2$

$\Rightarrow q^\alpha \mid n^2-1 \Rightarrow q^\alpha \mid n+1$

$\Rightarrow \boxed{p+1 \mid n+1} \Rightarrow p \leq n$

However $n^p > p^n \Rightarrow \Leftarrow !!$

$\Rightarrow p \geq n \Rightarrow p = n$

$p=2 \Rightarrow 2^n+1 \mid n^2+1 \Rightarrow 2^n \leq n^2$

$\Rightarrow n = 2, 4$

$p=3 \Rightarrow 3^n+1 \mid n^3+1 \Rightarrow 3^n \leq n^3$

$\Rightarrow n=3$

$$\underline{n} \mid m^{p(n-1)} - 1 = (m^{n-1}-1)(\text{———}), \quad m,n>1$$

$$\gcd(m^{n-1}-1, n) = 1$$

Let q be a prime $q \mid n$

$$m^{p(n-1)} \equiv 1 \pmod{q} \longrightarrow d \mid p(n-1)$$

$$m^{q-1} \equiv 1 \pmod{q} \longrightarrow \boxed{d \mid q-1}$$

$$m^{n-1} \not\equiv 1 \pmod{q} \longrightarrow d \nmid n-1$$

Let $d = \operatorname{ord}_q m$

$$p(n-1) = d\, m_0, \quad m \in \mathbb{Z}$$

$$\underline{(n-1)} = \frac{d\, m_0}{p} \Longrightarrow \frac{m_0}{p} \notin \mathbb{Z}$$

$$\Longrightarrow p \mid m_0$$

$$v_p(p(n-1)) = v_p(d)$$

$$\underline{v_p}(n-1)+1 = v_p(d)$$

$$d \mid q-1 \Rightarrow v_p(d) \leq v_p(q-1)$$

$$\Rightarrow v_p(n-1)+1 \leq v_p(q-1)$$

$$n = \underline{q_1}^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$$

$$\Longrightarrow v_p(n-1)+1 \leq v_p(q_i-1)$$

$$p^{\alpha} \| n-1 \Longrightarrow \alpha+1 \leq v_p(q_i-1)$$

$$\Longrightarrow p^{\alpha+1} \mid q_i - 1 \quad \forall\, q_i$$

$$\Longrightarrow q_i \equiv 1 \pmod{p^{\alpha+1}} \quad \forall\, q_i$$

$$n \equiv 1$$

Example 1.4.3. *(1998 IMO) Determine all pairs (x, y) of positive integers such that $x^2y + x + y$ is divisible by $xy^2 + y + 7$.*

Example 1.4.4. *(1992 IMO) Find all integers a, b, c with $1 < a < b < c$ such that*

$$(a-1)(b-1)(c-1)$$

divides $abc - 1$.

Example 1.4.2 (APMO 2002). *Find all pairs of positive integers a, b such that*

$$\frac{a^2+b}{b^2-a} \text{ and } \frac{b^2+a}{a^2-b}$$

are both integers.

Example 1.4.5 (Iran 2005). *Let $n, p > 1$ be positive integers and p be prime. Given that $n \mid p-1$ and $p \mid n^3 - 1$, prove that $4p - 3$ is a perfect square.*

Example 1.4.6 (David M. Bloom). *Let p be a prime with $p > 5$, and let $S = \{p - n^2 | n \in \mathbb{N}, n^2 < p\}$. Prove that S contains two elements a and b such that $a|b$ and $1 < a < b$.*

Example 3.4 (Math Prize Olympiad 2010)

Prove that for every positive integer n, there exists integers a and b such that $4a^2 + 9b^2 - 1$ is divisible by n.

- Let $P \in \mathbb{Z}[x]$ and for any integer n either $P(n) = 5$ or $P(n) = 2022$. Prove that either all $P(n) = 5$ or $P(n) = 2022$

Problem 4.1 (IMO 1989). Prove that for every positive integer n, there exists n consecutive positive integers such that none of them is a power of a prime.

Problem 4.2. Let n be a positive integer. Determine, in terms of n, the number of $x \in \{1, 2, \ldots, n\}$ for which $x^2 \equiv x \pmod{n}$.

Problem 4.3 (IMO 2009/1). Let n be a positive integer and let $a_1, a_2, a_3, \ldots, a_k$ (here $k \geq 2$) be distinct integers in the set $\{1, 2, \ldots, n\}$ such that n divides $a_i(a_{i+1} - 1)$ for $i = 1, 2, \ldots, k-1$. Prove that n does not divide $a_k(a_1 - 1)$.

Problem 4.4 (APMO 2009/4). Prove that for any positive integer k, there exists an arithmetic progression

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \ldots, \quad \frac{a_k}{b_k}$$

of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \ldots, k$, and moreover the $2k$ numbers $a_1, \ldots, a_k, b_1, \ldots, b_k$ are pairwise distinct.

Example 1.4.2 (APMO 2002). *Find all pairs of positive integers a, b such that*

$$\frac{a^2+b}{b^2-a} \text{ and } \frac{b^2+a}{a^2-b}$$

are both integers.

Assume that $a \geq b$.

$b^2-a \mid a^2+b \Rightarrow b^2-a \leq a^2+b \Rightarrow b(b-1) \leq a(a+1) \Rightarrow b-1 \leq a$

$a^2-b \mid b^2+a \Rightarrow a^2-b \leq b^2+a \Rightarrow a^2-a \leq b^2+b$

$a(a-1) \leq b(b+1) \Rightarrow a-1 \leq b$

$\Rightarrow a-1 \leq b \leq a$

Case 1 : $b=a$

$a^2-a \mid a^2+a \Rightarrow a-1 \mid a+1 \Rightarrow a-1 \mid 2$

$a^2-a \mid a^2+a$

$\Rightarrow a-1 \in \{2,1\}$

$a \in \{3,2\}$

$(a,b) = (2,2), (3,3)$

Case 2 : $a = b+1$

$b^2-(b+1) \mid (b+1)^2+b \Rightarrow b^2-b-1 \mid b^2+3b+1$

$(b+1)^2-b \mid b^2+b+1 \Rightarrow b^2+b+1 \mid b^2+b+1$ ✓

$b^2-b-1 \mid b^2+3b+1$

$\Rightarrow b^2-b-1 \mid 3b+1-(-b-1) = 4b+2$

$\Rightarrow b^2-b-1 \mid$

Example 1.4.5 (Iran 2005). *Let $n, p > 1$ be positive integers and p be prime. Given that $n \mid p-1$ and $p \mid n^3 - 1$, prove that $4p-3$ is a perfect square.*

$n^3 \equiv 1 \pmod{p} \Rightarrow p \mid (n-1)(n^2+n+1)$

but $n \mid p-1 \Rightarrow \begin{cases} p \geq n+1 \Rightarrow p \nmid n-1 \\ \text{and } p = nk+1 \end{cases}$

$\Rightarrow p \mid n^2+n+1$ $\qquad \underbrace{n+1, 2n}_{n}\underbrace{+1, 3n}_{n}+1$

$\Rightarrow nk+1 \mid n^2+n+1$

$\Rightarrow nk+1 \mid n^2+n+1 - (nk+1)$, $\gcd(nk+1, n) = 1$

$\Rightarrow nk+1 \mid n-k+1$

but $|n-k+1| \leq n+1$ or $k+1 \leq nk+1$

$\Rightarrow n-k+1 = 0 \Rightarrow n = k-1$

$p = n(n+1)+1$

$p = n^2+n+1 \Rightarrow 4p-3 = 4n^2+4n+1 = (2n+1)^2$

Example 1.4.6 (David M. Bloom). *Let p be a prime with $p > 5$, and let $S = \{p - n^2 | n \in \mathbb{N}, n^2 < p\}$. Prove that S contains two elements a and b such that $a|b$ and $1 < a < b$.*

We want n, m such that $p - n^2 \mid p - m^2$, $n^2 < p$, $m^2 < p$

$\iff p - n^2 \mid n^2 - m^2$

$\iff p - n^2 \mid (n-m)(n+m)$

$p - n^2 = n + m \Rightarrow \boxed{m = p - n^2 - n}$

Assume that $k^2 < p < (k+1)^2$

let $n = k \Rightarrow p - n^2 = p - k^2$

<u>Case 1</u> $p = k^2 + 1 \longrightarrow$ later

<u>Case 2</u> $p - k^2 = a > 1$

$a \mid k^2 - m^2$, $p = a + k^2$

$k^2 \equiv m^2 \pmod a$

$$m = \underbrace{p - k^2}_{a-k} - \underbrace{k}_{k-a} = a - k$$

$\boxed{k - a}$

- If $m = a - k > 0$:

$p - m^2 = (a + k^2) - (a - k)^2$

$= a + k^2 - k^2 + 2ak - a^2$

$p - m^2 = a - a^2 + 2ak = a(2k + 1 - a)$

$2k + 1 > a \iff 2k + 1 > p - k^2$

$\iff (k+1)^2 > p$ ✓

- If $a-k<0$, let $m=k-a$

$$p-m^2=(a+k^2)-(k-a)^2$$
$$=a(2k+1-a)>1 \qquad \square$$

<u>Case 1</u> $p=k^2+1 \Rightarrow k$ is even

$n=(k-1)$

$$p-(k-1)^2=(k^2+1)-(k-1)^2$$
$$=2k$$
$$p-1^2=k^2$$

$$\Rightarrow \quad p-(k-1)^2 \mid p-1 \qquad \blacksquare$$

Theorem 2.2.1 (Chinese Remainder Theorem). *The system of linear congruences*

$$\begin{cases} x \equiv a_1 \pmod{b_1}, \\ x \equiv a_2 \pmod{b_2}, \\ \cdots \\ x \equiv a_n \pmod{b_n}, \end{cases} \longrightarrow x \equiv r_{12} \pmod{b_1 b_2}$$

where $b_1, b_2, \cdots, b_n$ are pairwise relatively prime (aka $\gcd(b_i, b_j) = 1$ iff $i \neq j$) has one distinct solution for x modulo $b_1 b_2 \cdots b_n$.

For $n=2$:

$$\begin{cases} x \equiv a_1 \pmod{b_1} \Rightarrow x = b_1 k + a_1 \\ x \equiv a_2 \pmod{b_2} \end{cases}$$

$$b_1 k + a_1 \equiv a_2 \pmod{b_2}$$

$$b_1 k \equiv a_2 - a_1 \pmod{b_2}$$

$$k \equiv (a_2 - a_1)(b_1^{-1}) \pmod{b_2}$$

since $\gcd(b_1, b_2) = 1$

$$x \equiv r_1, r_2 \pmod{b_1 b_2}$$

$$\longrightarrow \quad r_1 \equiv a_1 \pmod{b_1}, \quad r_1 \equiv a_2 \pmod{b_2}$$

$$r_2 \equiv a_1 \pmod{b_1}, \quad r_2 \equiv a_2 \pmod{b_2}$$

$$b_1 \mid r_1 - r_2 \qquad b_2 \mid r_1 - r_2$$

$$\Rightarrow b_1 b_2 \mid r_1 - r_2$$

$$\Rightarrow r_1 \equiv r_2 \pmod{b_1 b_2}$$

1 2 3 4 5 1 2 3 4 5

1 2 3 4 5 6 7 8 9 10 11

1 2 3 4 5 6 7 8 9 10 .... 33 (mod 55)

$\pmod n$

If $\exists\ b \in \mathbb{N}$ s.t. $ab \equiv 1 \pmod n$

then $b = a^{-1} \pmod n$

if n is odd, then $2^{-1} = \frac{n+1}{2} \pmod n$

$$2 \times \frac{n+1}{2} = n+1 \equiv 1 \pmod n$$

$$2x \equiv 3 \pmod{19}$$

$x = 2^{-1} \cdot 3 \pmod{19}$
$= 10 \times 3$
$\equiv 30$

$(\overset{2^{-1}}{10}) \cdot 2x \equiv 10 \cdot 3 \pmod{19}$
$20x \equiv 30 \pmod{19}$
$x \equiv 11 \pmod{19}$

if $ax \equiv c \pmod n$

$x \equiv a^{-1} c \pmod n$ if a^{-1} exists

if $\underline{ab} \equiv \underline{1} \pmod n \Rightarrow n \mid ab - 1 \Rightarrow \gcd(a,n) = 1$

$d \mid -1$

if $\gcd(a,n) = 1$

$\{0 \cdot a, 1a, 2a, 3a, \dots, (n-1)a\} = \{0, 1, 2, \dots, n-1\} \pmod n$

if $ia \equiv ja \pmod n$

$\Rightarrow \underline{n} \mid ia - ja = (i-j)\underline{a}$

$\Rightarrow n \mid i-j \Rightarrow n \leq |i-j| \leq n-1$

$\Rightarrow \Leftarrow \Rightarrow i = j$

Example 3.4 (Math Prize Olympiad 2010)

Prove that for every positive integer n, there exists integers a and b such that $4a^2 + 9b^2 - 1$ is divisible by n.

Assume that $n = 2^k m$ where m is odd, $k \geq 0$

Note that $4(2^{-1})^2 + 9(0)^2 - 1 \equiv 0 \pmod{m}$

$4(0)^2 + 9(3^{-1})^2 - 1 \equiv 0 \pmod{2^k}$

$$\begin{cases} a \equiv 2^{-1} \pmod{m} \\ a \equiv 0 \pmod{2^k} \end{cases} \qquad \begin{cases} b \equiv 0 \pmod{m} \\ b \equiv 3^{-1} \pmod{2^k} \end{cases}$$

From CRT, $\exists$ such a, b.

$$\begin{matrix} m \mid 4a^2 + 9b^2 - 1 \\ 2^k \mid 4a^2 + 9b^2 - 1 \end{matrix} \implies \underbrace{2^k m}_{n} \mid 4a^2 + 9b^2 - 1$$

- Let $P \in \mathbb{Z}[x]$ and for any integer n either $P(n) = 5$ or $P(n) = 2022$. Prove that either all $P(n) = 5$ or $P(n) = 2022$

$$a-b \mid P(a) - P(b) \quad \forall\, a, b \in \mathbb{Z}$$

$$P(x+n) \equiv P(x) \pmod{n}$$

$P(x_0) = 2022$

$$P(x+2022k) \equiv P(x) \pmod{2022}$$

$$P(2022k + x_0) \equiv P(x_0) \equiv 0 \pmod{2022}$$

$$\Rightarrow \quad P(2022k + x_0) = 2022$$

$$P(5k + y_0) = 5 \quad \text{if } P(y_0) = 5$$

From CRT, $\exists\ x \in \mathbb{Z}$

$$x \equiv x_0 \pmod{2022}$$

$$x \equiv y_0 \pmod{5}$$

Problem 4.1 (IMO 1989). Prove that for every positive integer n, there exists n consecutive positive integers such that none of them is a power of a prime.

Problem 4.2. Let n be a positive integer. Determine, in terms of n, the number of $x \in \{1, 2, \ldots, n\}$ for which $x^2 \equiv x \pmod{n}$.

Example 3.1 (USAMO 2008/1)

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

(AoPS). *Show that for $c \in \mathbb{Z}$ and a prime p, the congruence $x^x \equiv c \pmod{p}$ has a solution.*

(ISL 2005 N6). *Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.*

Problem 4.3 (IMO 2009/1). Let n be a positive integer and let $a_1, a_2, a_3, \ldots, a_k$ (here $k \geq 2$) be distinct integers in the set $\{1, 2, \ldots, n\}$ such that n divides $a_i(a_{i+1} - 1)$ for $i = 1, 2, \ldots, k-1$. Prove that n does not divide $a_k(a_1 - 1)$.

1. (Poland 2003) A polynomial f with integer coefficients has the property that $\gcd(f(a), f(b)) = 1$ for some integers $a \neq b$. Prove that there is an infinite set of integers S such that $\gcd(f(m), f(n)) = 1$ whenever m, n are distinct elements of S.

2. Prove that for all positive integers k and n there exists a set S of n consecutive positive integers such that each $x \in S$ has at least k distinct prime divisors that do not divide any other element of S.

3. A lattice point is called visible if its coordinates are relatively prime integers. Prove that for any positive integer k there is a lattice point whose distance from each visible lattice point is greater than k.

4. a) Prove that for all $n \geq 1$ there is a positive integer a such that $a, 2a, \ldots, na$ are all perfect powers.

   b) (Balkan 2000) Prove that for all $n \geq 1$ there is a set A of n positive integers such that for all $1 \leq k \leq n$ and all $x_1, x_2, \ldots, x_k \in A$ the number $\frac{x_1 + x_2 + \ldots + x_k}{k}$ is a perfect power.