Congruences

www.artofproblemsolving.com/community/c3591

by Peter, ZetaX, pohoatza, Yimin Ge, Hawk Tiger, maxal

1 Let p be an odd prime and let Z_p denote (the field of) integers modulo p. How many elements are in the set

$$\{x^2 : x \in Z_p\} \cap \{y^2+1 : y \in Z_p\}?$$

---

2 Suppose that p is an odd prime. Prove that

$$\sum_{j=0}^{p} \binom{p}{j}\binom{p+j}{j} \equiv 2^p + 1 \pmod{p^2}.$$

---

3 Show that

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^3}$$

for all prime numbers p with $p \ge 5$.

---

4 Let n be a positive integer. Prove that n is prime if and only if

$$\binom{n-1}{k} \equiv (-1)^k \pmod{n}$$

for all $k \in \{0, 1, \cdots, n-1\}$.

---

5 Prove that for $n \ge 2$,

$$\underbrace{2^{2^{\cdots^{2}}}}_{n \text{ terms}} \equiv \underbrace{2^{2^{\cdots^{2}}}}_{n-1 \text{ terms}} \pmod{n}.$$

---

6 Show that, for any fixed integer $n \ge 1$, the sequence

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \cdots \pmod{n}$$

is eventually constant.

---

7 Somebody incorrectly remembered Fermat's little theorem as saying that the congruence $a^{n+1} \equiv a \pmod{n}$ holds for all a if n is prime. Describe the set of integers n for which this property is in fact true.

---

8 Characterize the set of positive integers n such that, for all integers a, the sequence a, a^2, a^3, $\cdots$ is periodic modulo n.

---

9 Show that there exists a composite number n such that $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$.

---

10 Let p be a prime number of the form $4k+1$. Suppose that $2p+1$ is prime. Show that there is no $k \in \mathbb{N}$ with $k < 2p$ and $2^k \equiv 1 \pmod{2p+1}$.

---

11 During a break, n children at school sit in a circle around their teacher to play a game. The teacher walks clockwise close to the children and hands out candies to some of them according to the following rule. He selects one child and gives him a candy, then he skips the next child and gives a candy to the next one, then he skips 2 and gives a candy to the next one, then he skips 3, and so on. Determine the values of n for which eventually, perhaps after many rounds, all children will have at least one candy each.

---

12 Suppose that $m > 2$, and let P be the product of the positive integers less than m that are relatively prime to m. Show that $P \equiv -1 \pmod{m}$ if $m = 4$, p^n, or $2p^n$, where p is an odd prime, and $P \equiv 1 \pmod{m}$ otherwise.

---

13 Let Γ consist of all polynomials in x with integer coefficients. For f and g in Γ and m a positive integer, let $f \equiv g \pmod{m}$ mean that every coefficient of $f-g$ is an integral multiple of m. Let n and p be positive integers with p prime. Given that f, g, h, r and s are in Γ with $rf + sg \equiv 1 \pmod{p}$ and $fg \equiv h \pmod{p}$, prove that there exist F and G in Γ with $F \equiv f \pmod{p}$, $G \equiv g \pmod{p}$, and $FG \equiv h \pmod{p^n}$.

---

14 Determine the number of integers $n \geq 2$ for which the congruence

$$x^{25} \equiv x \pmod{n}$$

is true for all integers x.

---

15 Let $n_1, \cdots, n_k$ and a be positive integers which satify the following conditions:- for any $i \neq j$, $(n_i, n_j) = 1$, - for any i, $a^{n_i} \equiv 1 \pmod{n_i}$, - for any i, n_i does not divide $a-1$. Show that there exist at least $2^{k+1} - 2$ integers $x > 1$ with $a^x \equiv 1 \pmod{x}$.

---

16 Determine all positive integers $n \geq 2$ that satisfy the following condition; For all integers a, b relatively prime to n,

$$a \equiv b \pmod{n} \Longleftrightarrow ab \equiv 1 \pmod{n}.$$

---

17 Determine all positive integers n such that $xy+1 \equiv 0 \pmod{n}$ implies that $x+y \equiv 0 \pmod{n}$.

---

18 Let p be a prime number. Determine the maximal degree of a polynomial $T(x)$ whose coefficients belong to $\{0, 1, \cdots, p-1\}$, whose degree is less than p, and which satisfies

$$T(n) = T(m) \pmod{p} \Longrightarrow n = m \pmod{p}$$

for all integers n, m.

---

19 Let $a_1, \cdots, a_k$ and $m_1, \cdots, m_k$ be integers with $2 \le m_1$ and $2m_i \le m_{i+1}$ for $1 \le i \le k-1$. Show that there are infinitely many integers x which do not satisfy any of congruences

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \cdots, x \equiv a_k \pmod{m_k}.$$

---

20 Show that 1994 divides $10^{900} - 2^{1000}$.

---

21 Determine the last three digits of

$$2003^{2002^{2001}}.$$

---

22 Prove that $1980^{1981^{1982}} + 1982^{1981^{1980}}$ is divisible by 1981^{1981}.

---

23 Let p be an odd prime of the form $p = 4n+1$. - Show that n is a quadratic residue $\pmod{p}$. - Calculate the value $n^n \pmod{p}$.
