

Putnam practice - Number theory

Division algorithm: For any integer a and positive integer b , we have $a = b \cdot q + r$ for some integers q (quotient) and $0 \leq r < b$ (remainder).

Bézout's identity: $\gcd(a, b) = ax + by$ for some integers x, y .

Congruence: $a \equiv b \pmod{m}$ if and only if $m \mid a - b$ (i.e., m divides $a - b$).

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$ and $a \cdot c \equiv b \cdot d \pmod{m}$.

$n^2 \equiv 0, 1 \pmod{3}$, $n^2 \equiv 0, 1 \pmod{4}$, $n^2 \equiv 0, 1, 4 \pmod{8}$.

Euclid's lemma: Suppose a prime p divides $a \cdot b$, then $p \mid a$ or $p \mid b$.

Fermat's little theorem: For any prime p and $\gcd(a, p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Chinese remainder theorem: Suppose $\gcd(m_1, m_2) = 1$. Then the solutions of $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ corresponds to $x \equiv a \pmod{m_1 m_2}$ for some unique a .

Questions:

1. For any polynomial $p(x)$ with integer coefficients and any two distinct integers a, b , prove that $a - b \mid p(a) - p(b)$.
2. Let $p(x)$ be a polynomial with integer coefficients and degree at least 1. Prove that $p(n)$ is a composite number for infinitely many integers n .
3. (2017) Let f be a polynomial with positive integer coefficients. Prove that if n is a positive integer, then $f(n)$ divides $f(f(n) + 1)$ if and only if $n = 1$.
4. (1969) Let n be a positive integer such that 24 divides $n + 1$. Prove that the sum of all the positive divisors of n is divisible by 24.
5. (2010) Prove that for each positive integer n , the number $10^{10^{10^n}} + 10^{10^n} + 10^n - 1$ is not prime.
6. (1972) For all integer $n > 1$, prove that n does not divide $2^n - 1$.
7. (1994) For any integer a , set $n_a = 101a - 100 \cdot 2^a$. Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.