Modular Arithmetic 2

Andres Buritica Monroy

1 Inverses

Let a and n be positive integers such that $\gcd(a, n) = 1$.

- Prove that there exists a unique least residue $a^{-1} \pmod n$ such that $aa^{-1} \equiv 1 \pmod n$.
- Use this fact to give another proof that if $ax \equiv ay \pmod n$, then $x \equiv y \pmod n$.

The least residue a^{-1} such that $aa^{-1} \equiv 1 \pmod n$ is called the *inverse* of a mod n.

Let a, b, c, d, k, n be positive integers such that $\gcd(b, n) = \gcd(d, n) = 1$. Prove that

- $b^{-1}d^{-1} \equiv (bd)^{-1} \pmod n$
- $(b^k)^{-1} \equiv (b^{-1})^k \pmod n$
- $ab^{-1} + cd^{-1} \equiv (ad + bc)(bd)^{-1} \pmod n$

2 More Theorems

- (Wilson's Theorem) Prove that $(n-1)! \equiv -1 \pmod n$ if and only if n is prime.
- (GCD Trick) Prove that if $a^x \equiv 1 \pmod n$ and $a^y \equiv 1 \pmod n$ then $a^{\gcd(x,y)} \equiv 1 \pmod n$.
- (Chinese Remainder Theorem) Let $a_1, a_2, \ldots, a_k$ be pairwise coprime positive integers, and let $b_1, b_2, \ldots, b_k$ be integers. Prove that there is exactly one least residue x mod $a_1 a_2 \cdots a_k$ such that for each i,
$$b_i \equiv x \pmod{a_i}.$$
- (Euler's product formula) Prove that if $\gcd(a, b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$. Use this fact to find a formula for $\varphi(n)$ in terms of the prime factorisation of n.

3 Problems

1. Let $p = 3k - 1$ be a prime. Prove that
$$1^{-1} - 2^{-1} + 3^{-1} - 4^{-1} + \cdots + (2k-1)^{-1} \equiv 0 \pmod p.$$
2. Prove that for each positive integer n there exist n consecutive positive integers, none of which is a prime power.

3. Call a lattice point "visible" if the greatest common divisor of its coordinates is 1. Prove that there exists a 100×100 square on the board none of whose points are visible.

4. We are given a positive integer $s \geq 2$. For each positive integer k, we define its twist k' as follows: write k as $as + b$, where a, b are non-negative integers and $b < s$, then $k' = bs + a$. For the positive integer n, consider the infinite sequence $d_1, d_2, \ldots$ where $d_1 = n$ and d_{i+1} is the twist of d_i for each positive integer i. Prove that this sequence contains 1 if and only if the remainder when n is divided by $s^2 - 1$ is either 1 or s.

5. Let $p > 3$ be prime. Define $m = (4^p - 1)/3$. Prove that $2^{m-1} \equiv 1 \pmod{m}$.

6. Define a sequence by $a_1 = n$ and $a_{i+1} = \frac{a_i(a_i-1)}{2}$ for each $i \geq 1$. For which positive integers n are all values of a_i odd?

4 Homework

1. Compute the remainder when 2023^{2022} is divided by 2021.
2. We define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

   For each prime p and positive integer k, find the least residues of

$$\binom{p-1}{k} \quad \text{and} \quad \frac{1}{p}\binom{p}{k}$$

   in mod p.

3. Prove that if p is an odd prime that divides n^2+1 for some integer n, then $p \equiv 1 \pmod 4$.