$\mathbb{Z}_p$ and prime factorisations

Andres Buritica

April 23, 2022

1 The integers modulo a prime

Let p be a prime.

We define $\mathbb{Z}_p$ (the integers mod p) using an equivalence relation

$$a \equiv b \pmod{p} \iff p \mid b - a$$

over the integers.

This gives us p equivalence classes corresponding to the least residues mod p:

$$\{0, 1, 2, \ldots, p-1\}.$$

- Prove that addition, subtraction, multiplication and exponentiation are consistently defined: that is, if a, b, c, d are integers with $a \equiv b \pmod{p}$ and $c \equiv d \pmod{p}$ then

  $$a + c \equiv b + d \pmod{p}, \quad a - c \equiv b - d \pmod{p}, \quad ac \equiv bd \pmod{p}, \quad a^n \equiv b^n \pmod{p}.$$

- Prove that for any integer a with $p \nmid a$ there is an integer b with $0 \leq b < p$ such that $ab \equiv 1 \pmod{p}$. We call b the inverse of a in mod p, notated a^{-1}.

- We may define fractions in mod p as

  $$\frac{a}{b} \equiv ab^{-1} \pmod{p},$$

  assuming $p \nmid b$. Prove that addition, subtraction, multiplication and division by anything nonzero still work as expected.

- Prove that $(p-1)! \equiv -1 \pmod{p}$.

- Find the least residues of

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

  in mod p.

- Let $\mathbb{Z}_p^*$ be the set of nonzero residues mod p, and let a be an element of $\mathbb{Z}_p^*$. Prove that the function $f(x) = ax$ is a bijection from $\mathbb{Z}_p^*$ to $\mathbb{Z}_p^*$. Deduce that $p \mid a^{p-1} - 1$.

- Prove that if $a^m \equiv 1 \pmod{p}$ and $a^n \equiv 1 \pmod{p}$ then $a^{\gcd(m,n)} \equiv 1 \pmod{p}$.

2 Arithmetic functions

We define:

- The number of positive divisors function $d(n)$.
- The sum of positive divisors function $\sigma(n)$.
- The totient function $\varphi(n)$: the number of positive integers which are at most n and coprime to n.

A function $f : \mathbb{N} \to \mathbb{R}$ is called multiplicative if for any coprime positive integers a and b, we have

$$f(a)f(b) = f(ab).$$

It's called completely multiplicative if this equation holds for *any* positive integers a and b

- Prove that the values at the primes of a completely multiplicative function completely define the function (unless these values are all 0, in which case $f(1)$ can be 0 or 1).
- Prove that the values at prime powers of a multiplicative function completely define it (once again, unless these values are all 0).
- Prove that d and σ are multiplicative.
- Find formulae for $d(n), \sigma(n), \varphi(n)$ where $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

3 Problems

1. Prove that if there are two terms of an arithmetic progression which are coprime integers, then there is an infinite subset of that progression all of whose elements are coprime integers.
2. Let n be an even positive integer such that $\sigma(n) = 2n$. Prove that $n = 2^{p-1}(2^p - 1)$, where p is a prime.
3. Define the sequence $a_n = 2^n + 3^n + 6^n - 1,\ n \in \mathbb{N}$. Find all primes which do not divide a_n for any n.
4. For any positive integer n, prove that $\displaystyle\sum_{d|n} \varphi(d) = n$.
5. Let x and y be positive integers and let p be prime. Assume there are coprime positive integers m and n such that $x^m \equiv y^n \pmod{p}$. Prove that there is a unique positive integer z with $0 \leq z < p$ such that
$$x \equiv z^n \pmod{p}, \qquad y \equiv z^m \pmod{p}.$$
6. Let a and b be positive integers such that $a^n + n \mid b^n + n$ for all positive integers n. Prove that $a = b$.
7. Let n and k be positive integers such that $\varphi^k(n) = 1$ (that is, φ iterated k times). Prove that $n \leq 3^k$.

4 Homework

1. Prove that $\sigma(n) < n\sqrt{2d(n)}$ for all positive integers n.
2. Given a positive integer k, show that there exists a prime p such that one can choose distinct integers $a_1, a_2, \ldots, a_{k+3} \in \{1, 2, \ldots, p-1\}$ such that p divides $a_i a_{i+1} a_{i+2} a_{i+3} - i$ for all $i = 1, 2, \ldots, k$.
3. Find all completely multiplicative functions $f : \mathbb{N} \to \mathbb{R}$ such that for all $a, b \in \mathbb{N}$, at least two of $f(a), f(b), f(a+b)$ are equal.