Modular arithmetic

Andres Buritica

August 20, 2022

1 Residue Classes

Let n be a nonzero integer. For integers a and b, we say that

$$a \equiv b \pmod{n} \iff n \mid b - a.$$

Notice that for fixed values of a and n, infinitely many values of b satisfy $a \equiv b \pmod{n}$.

- Prove that $a \equiv a \pmod{n}$.
- Prove that if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
- Prove that if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

We may divide the integers into n sets (the *residue classes mod* n), such that two integers are in the same residue class if and only if they are congruent mod n. The sets are as follows:

$$\begin{aligned}
[0]_n &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\} \\
[1]_n &= \{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, \ldots\} \\
[2]_n &= \{\ldots, 2-2n, 2-n, 2, 2+n, 2+2n, \ldots\} \\
&\vdots \\
[n-1]_n &= \{\ldots, -1-n, -1, n-1, 2n-1, 3n-1, \ldots\}
\end{aligned}$$

The numbers $0, 1, \ldots, n-1$ are called the *least residues mod* n. The set of least residues mod n is called the *integers mod* n, denoted $\mathbb{Z}_n$.

- Find the least residue of -1 mod 2022.

2 Operations

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

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

Therefore, it makes sense to define addition, subtraction and multiplication in $\mathbb{Z}_n$. For each of these operations (we use $\circ$ to denote any of them), we let $a \circ b$ in $\mathbb{Z}_n$ be the least residue of $a \circ b$ in $\mathbb{Z}$.

- What are $3 + 2$ and 3×2 in $\mathbb{Z}_4$?

Assume that for some integer a there is a least residue b such that $ab \equiv 1 \pmod{n}$. We call b the *inverse* of a mod n.

We define $\frac{c}{a} \equiv cb \pmod{n}$, for each positive integer c.

- Prove that if c has an inverse mod n, and $cx \equiv cy \pmod{n}$, then $x \equiv y \pmod{n}$.
- Prove that each integer has at most one inverse mod n.
- Prove that if b and d both have inverses mod n, then so does bd.
- Prove that

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{n}, \qquad \frac{a}{b} - \frac{c}{d} \equiv \frac{ad-bc}{bd} \pmod{n},$$
$$\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod{n}, \qquad \frac{a}{b} \div \frac{c}{d} \equiv \frac{ad}{bc} \pmod{n}$$

  assuming all of the denominators have inverses.

3 The integers modulo a prime

Let p be a prime.

- Let a be an integer. Prove that a has an inverse mod p if and only if $p \nmid a$.
- Prove that $(p-1)! \equiv -1 \pmod{p}$.
- 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 $p \mid a^{p-1} - 1$.

4 The integers modulo an integer

Let n be an integer.

- Let a be an integer. Prove that a has an inverse mod n if and only if $\gcd(n, a) = 1$.
- Say $ax \equiv ay \pmod{n}$, but $\gcd(n, a) \neq 1$. What can we say about x and y?
- Let $\mathbb{Z}_n^*$ be the set of least residues mod n which are coprime to n, and let a be an element of $\mathbb{Z}_n^*$.
  - Prove that the function $f(x) = ax$ is a bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*$.
  - Deduce that $n \mid a^{\varphi(n)} - 1$.

5 Chinese Remainder Theorem

- Let a and b be coprime positive integers, and let c and d be integers. Prove that there is exactly one least residue x mod ab such that
$$c \equiv x \pmod{a}, \qquad d \equiv x \pmod{b}.$$
- Let $a_1, a_2, \ldots, a_k$ be coprime positive integers, and let $b_1, b_2, \ldots, b_k$ be integers. Prove that there is exactly one least residue x mod $a_1 a_2 \cdots a_n$ such that for each i,
$$b_i \equiv x \pmod{a_i}.$$
- Recall that $\varphi(n)$ is the number of positive integers which are at most n and coprime to n. Prove that φ is multiplicative.

6 Choosing good mods

Prove that:

- Squares are 0, 1 or 4 mod each of {5,8}, and 0 or 1 mod 3.
- Cubes are 0, 1 or -1 mod each of {7,9}.

Often a problem will be solved by considering it under an appropriate mod. In general, for nth powers, try looking mod m where $\varphi(m)$ is a small multiple of n.

Also, of course, try choosing a mod which divides a bunch of terms.

- Find all positive integers a, b such that
$$a^4 + b^4 = 10a^2b^2 - 2022.$$

However, remember that if you find a single solution to an equation, then that solution is still a solution in every mod so you won't be able to find a contradiction.

- Find all positive integers a, b such that
$$a^4 + b^4 = 97.$$

7 Problems

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. 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. Find all primes p such that $29^p + 1$ is a multiple of p.
4. 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.
5. Let $p = 3k - 1$ be a prime. Prove that
$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2k-2} + \frac{1}{2k-1} \equiv 0 \pmod{p}.$$
6. Find all positive integers n such that $2^n + 7^n$ is a perfect square.
7. Show that for any fixed integers n and a, the sequence $a, a^a, a^{a^a}, \ldots$ is eventually constant mod n.
8. Prove that for each positive integer n there exist n consecutive positive integers, none of which is a prime power.
9. Prove that every positive integer has at least as many divisors which are 1 (mod 4) as divisors which are 3 (mod 4).
10. Let d be a positive integer. Prove that at least one of $2d-1,\ 5d-1,\ 13d-1$ is not a perfect square.
11. Find all pairs of positive integers x, y such that $x! + 5 = y^3$.
12. Prove that if m and n are matural numbers, then $3^m + 3^n + 1$ is not a perfect square.
13. Find all primes p and q such that $p + q = (p - q)^3$.
14. Find all pairs of positive integers x, y such that $1 + 2^x + 2^{2x+1} = y^2$.
15. Find all integers a, b such that
$$a^3 + (a+1)^3 + \cdots + (a+6)^3 = b^4 + 1.$$
16. Find all positive integers a for which $1! + 2! + \cdots + a!$ is a perfect cube.
17. What is the least residue mod n of the product of the elements of $\mathbb{Z}_n^*$?