$\mathbb{Z}_n$ and Diophantine equations

Andres Buritica Monroy

1 The integers modulo an integer

Let n be a positive integer.

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

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

over the integers.

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

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

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

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

- Prove that for any integer a with $\gcd(n, a) = 1$ there is an integer b with $0 \le b < n$ such that $ab \equiv 1 \pmod{n}$. We call b the inverse of a in mod n, notated a^{-1}.
- We may define fractions in mod n as

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

  assuming $\gcd(b, n) = 1$. Prove that addition, subtraction, and multiplication still work.
- Let's say you have integers a, b, c, n such that $ab \equiv ac \pmod{n}$. What can you say about $c - b$?
- Let $\mathbb{Z}_n^*$ be the set of nonzero residues mod n that 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 $n \mid a^{\varphi(n)} - 1$.
- Prove that if $a^x \equiv 1 \pmod{n}$ and $a^y \equiv 1 \pmod{n}$ then $a^{\gcd(x,y)} \equiv 1 \pmod{n}$.
- Let m and n be coprime positive integers. For any integers a and b, prove that there is a unique residue c mod mn such that $a \equiv c \pmod{m}$, $b \equiv c \pmod{n}$.
- Prove that φ is multiplicative.
- What is the product of the elements of $\mathbb{Z}_n^*$ mod n?

2 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 $\{7,9\}$.

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.

3 Diophantine equation tricks

- Factorising expressions
- Using mods to find contradictions or get conditions on the variables
- Choosing a prime that divides some number or expression
- Reducing expressions mod other expressions
- Quadratic discriminant trick: if a, b, c, n are positive integers such that $an^2 + bn + c = 0$ then $b^2 - 4ac$ is a perfect square.
- (for later lectures) Bounding arguments, descent, ν_p considerations

4 Problems

1. Find the minimum possible value of $m + n$, where m and n are distinct positive integers such that $1000 \mid 1978^m - 1978^n$.
2. Show that for any fixed integers n and a, the sequence $a, a^a, a^{a^a}, \ldots$ is eventually constant mod n.
3. An infinite arithmetic progression contains a perfect ath power and a perfect bth power. Prove that it contains a perfect $\mathrm{lcm}(a, b)$th power.
4. Prove that if a and b are positive integers, then $4ab - a - b$ is not a perfect square.
5. Let n be a positive integer, and let S be a set of n positive integers all at most n^2. Prove that there is a set T of n positive integers such that the set $\{s + t : s \in S, t \in T\}$ covers at least half of the residues mod n^2.
6. Let n and z be integers greater than 1 such that $\gcd(n, z) = 1$. Prove that there is some nonnegative integer $i < n$ such that $1 + z + z^2 + \cdots + z^i$ is divisible by n.
7. Find all positive integer solutions to $3^x + 4^y = 5^z$.
8. Let $n > 1$ be a positive integer and let p be a prime. Given that $n \mid p - 1$ and $p \mid n^3 - 1$, prove that $4p - 3$ is a perfect square.

5 Homework

1. Let $n > 1$ be an odd positive integer and let S be the set of integers x, with $1 \leq x \leq n$, such that both x and $x+1$ are coprime to n. Find the product of the elements of S mod n.

2. What is the smallest positive integer n for which there exist positive integers $x_1, x_2, \ldots, x_n$ such that
$$x_1^3 + x_2^3 + \cdots + x_n^3 = 2002^{2002}?$$

3. Find all integers x, y such that $(x^2 + y)(x + y^2) = (x - y)^3$.