Modular Arithmetic

1 Residue classes

Given an integer $n \geq 2$, we say that $a \in \mathbb{Z}$ is congruent to $b \in \mathbb{Z}$ modulo n if n divides $a - b$ — equivalently, if $a = b + kn$ for some $k \in \mathbb{Z}$, or if a and b have the same remainder in the division by n. In this case, we write $a \equiv b \pmod{n}$. Note that $\equiv$ is an equivalence relation on $\mathbb{Z}$ (reflexive: $a \equiv a \pmod{n}$; symmetric: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$; transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$). Therefore, we can partition $\mathbb{Z}$ into the equivalence classes, called residue classes,

$$[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\} = \{a + kn, k \in \mathbb{Z}\}.$$

Each residue class has a unique representative in $\{0, 1, \ldots, n-1\}$ — the remainder of any element of the class in the division by n — and is often identified to this representative. Hence, the set $\mathbb{Z}_n$ of residue classes modulo n is identified to $\{0, 1, \ldots, n-1\}$. Defining an addition and a multiplication on $\mathbb{Z}_n$ by $[a]_n + [b]_n = [a+b]_n$ and $[a]_n \cdot [b]_n = [a \cdot b]_n$, it can be seen that $(\mathbb{Z}_n, +)$ is a group. With $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n : \exists\, b \in \mathbb{Z}_n : [a]_n \cdot [b]_n = [1]_n\}$ denoting the set of units (i.e., invertible elements) of $\mathbb{Z}_n$, it can be seen that $(\mathbb{Z}_n^*, \cdot)$ is also a group.

2 Euler theorem

Note that (the representative) of $a \in \mathbb{Z}$ is a unit of $\mathbb{Z}_n$ if and only if there exist $b \in \mathbb{Z}$ and $k \in \mathbb{Z}$ such that $ab + kn = 1$. By Bézout lemma, this means that $a \in \mathbb{Z}_n^*$ if and only if a and n are coprime. One consequence is that, if p is prime, then every nonzero element in $\mathbb{Z}_p$ is invertible — this makes $\mathbb{Z}_p$ a field, where usual calculation rules apply, for instance $ab \equiv 0 \pmod{n}$ implies $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$. Another consequence is that

$$\operatorname{card}(\mathbb{Z}_n^*) = \operatorname{card}\{a \in [1 : n-1] \text{ such that } a \text{ and } n \text{ are coprime}\} = \phi(n),$$

where ϕ is Euler totient function. Thus, applying Lagrange theorem to the multiplicative group $\mathbb{Z}_n^*$ yields Euler theorem, that is

$$a^{\phi(n)} \equiv 1 \pmod{n} \qquad \text{whenever } \gcd(a, n) = 1.$$

When n is a prime number p, this becomes Fermat little theorem, that is

$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{whenever } a \text{ is not a multiple of } p.$$

Euler theorem provides a way to compute the powers modulo n of an integer a coprime with n, i.e., $a^m \equiv a^{m \bmod \phi(n)} \pmod{n}$.

3 Chinese remainder theorem

Given integers $n_1, n_2, \ldots, n_k \geq 2$ that are pairwise coprime, the chinese remainder theorem says that the system of congruence

$$\begin{aligned} x &\equiv r_1 \pmod{n_1}, \\ x &\equiv r_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv r_k \pmod{n_k}, \end{aligned}$$

has a unique solution modulo $N := n_1 n_2 \cdots n_k$. For the uniqueness, notice that, if x and x' are two solutions, then $n_1 | x - x'$, $n_2 | x - x'$, ..., $n_k | x - x'$, so $n_1 n_2 \cdots n_k | x - x'$ (because $n_1, n_2, \ldots, n_k$ are coprime), i.e., $x \equiv x' \pmod{N}$. For the existence, set $N_i := N/n_i$ and notice that N_i and n_i are coprime. Thus, we can consider the inverse m_i of N_i in $\mathbb{Z}_{n_i}$. It is now readily verified that $x := m_1 N_1 r_1 + m_2 N_2 r_2 + \cdots + m_k N_k r_k$ is a solution of the system of congruence. Stated differently, the theorem says that the map

$$x \in \mathbb{Z}_{n_1 n_2 \cdots n_k} \mapsto (x \bmod n_1, x \bmod n_2, \ldots, x \bmod n_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_k}$$

is bijective when $n_1, n_2, \ldots, n_k$ are pairwise coprime.

We can now justify that Euler totient function is multiplicative, i.e., that $\phi(nm) = \phi(n)\phi(m)$ when n and m are coprime. Indeed, for $x \in \mathbb{Z}$, the fundamental theorem of arithmetic reveals

$$[\gcd(x, nm) = 1] \Leftrightarrow [\gcd(x, n) = 1,\ \gcd(x, m) = 1] \Leftrightarrow [\gcd(x \bmod n, n) = 1,\ \gcd(x \bmod m, m) = 1],$$

so that $x \in \mathbb{Z}_{nm}^* \mapsto (x \bmod n, x \bmod m) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ is also a bijective map. The equality between the cardinalities of $\mathbb{Z}_{nm}^*$ and of $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ gives the desired result.

4 Exercises

Ex.1: Verify that $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n^*, \cdot)$ are groups.

Ex.2: We define a function f on positive integers by $f(1) = 3$ and $f(n+1) = 3f(n)$. What are the last two digits of $f(2012)$?

Ex.3: For any integer $n > 1$, prove that n does not divides $2^n - 1$.

Ex.4: What is the lowest degree monic polynomial which vanishes identically on the integers $\pmod{p}$ when p is prime? Same question $\pmod{100}$?

Ex.5: How many perfect squares are there $\pmod{2^n}$?