Session 1

Intro to Modular Arithmetic

You may have encountered “clock arithmetic” in grade school, where after you get to 12, the next number is 1.

This leads to odd-looking equations such as
$6 + 9 = 3$ and $2 - 3 = 11$.

These look strange, but they are true using clock arithmetic, since for example 11 o’clock is 3 h before 2 o’clock. So what we are really doing is first computing $2 - 3 = -1$ and then adding 12 to the answer.

Similarly, 9 h after 6 o’clock is 3 o’clock, since $6 + 9 - 12 = 3$.

> 💡 The theory of congruences is a powerful method in number theory that is
> based on the simple idea of clock arithmetic.

Definition. Let $m \geq 1$ be an integer.

We say that the integers a and b are congruent modulo m if their difference $a - b$ is divisible by m.

We write:

$a \equiv b \pmod{m}$

to indicate that a and b are congruent modulo m. The number m is called the modulus

Proposition. Let $m \geq 1$ be an integer.
(a) If $a1 \equiv a2 \pmod{m}$ and $b1 \equiv b2 \pmod{m}$, then
$a1 \pm b1 \equiv a2 \pm b2 \pmod{m}$ and $a1 \cdot b1 \equiv a2 \cdot b2 \pmod{m}$.
(b) Let a be an integer. Then
$a \cdot b \equiv 1 \pmod{m}$ for some integer b if and only if $\gcd(a, m)=1$

Further, if a · b1 ≡ a · b2 ≡ 1 (mod m), then b1 ≡ b2 (mod m). We call b the (multiplicative) inverse of a modulo m

Fermat Little Theorem (FLM):

let p be a prime number, a be a positive integer

then $a^p \cong a \mod p$

Example:

a = 2 , p = 7

$2^7 \mod 7 = 2$

Another form of FLM:

let p be a prime number, a be a positive integer

then $a^{p-1} \cong 1 \mod p$

Euler's Totient Function:

$\phi(n) =$
$\text{the number of positive integers smaller than n and relatively prime to n}$

We have 3 cases

1. n is prime: phi(n) = n - 1
2. n is a product of 2 primes (p and q): phi(n) = (p-1)(q-1)
3. n is a squared prime: phi(n) = p*(p-1)

There's a 4th case but you look it up ;)

Euler's Theorem:

let p and q be distinct primes and n = p*q

and a is relatively prime to n, then

$a^{\phi(n)} = 1 \mod n$ which is similar to
$a^{(p-1)\times(q-1)} \mod n$

The Chinese Remainder Theorem

Suppose we wish to solve

x=2(mod5)

x=3(mod7)

for x. If we have a solution y, then y+35 is also a solution. So we only need to look for solutions modulo 35. By brute force, we find the only solution is x=17(mod35).

For any system of equations like this, the Chinese Remainder Theorem tells us there is always a unique solution up to a certain modulus, and describes how to find the solution efficiently.

> Given pairwise coprime positive integers n1,n2,...,nk and arbitrary integers a1,a2,...,ak the system of simultaneous congruences
>
> x≡a1(mod$n$1)
>
> x≡a2(mod$n$2)
>
> x≡ak(modnk)
>
> has a solution, and the solution is unique modulo N=n1n2…nk.

The following is a general construction to find a solution to a system of congruences using the Chinese remainder theorem:

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.
2. For each $i = 1, 2, \ldots, k$, compute

$$y_i = \frac{N}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$

3. For each $i = 1, 2, \ldots, k$, compute $z_i \equiv y_i^{-1} \mod n_i$ using Euclid's extended algorithm (z_i exists since $n_1, n_2, \ldots, n_k$ are pairwise coprime).
4. The integer $x = \sum_{i=1}^{k} a_i y_i z_i$ is a solution to the system of congruences, and $x \mod N$ is the unique solution modulo N.