1 | Modular Arithmetic

For a positive integer m and integers a, b we say that a, b are congruent modulo m if they have the same remainder upon division by m. Equivalently, a, b are congruent modulo m if $a - b$ is a multiple of m. This is denoted as $a \equiv b \pmod{m}$.

Example: $2 \equiv 26 \pmod{8}$

Addition, subtraction, and multiplication are defined in modular arithmetic. For $a \equiv 2 \pmod{8}$ and $a \equiv 5 \pmod{8}$:

- $a + b \equiv 7 \pmod{8}$
- $a - b \equiv 5 \pmod{8}$
- $ab \equiv 2 \pmod{8}$

Exponentiation and division are a bit more complex. <div class="admonition" style="–admonition-color: 173, 173, 173;"><div class="admonition-title"><div class="admonition-title-content"><div class="admonition-title-icon"><i class="fas fa-quote-left" aria-hidden="true"></i></div><div class="admonition-title-markdown">Fermat 's Little Theorem</div></div></div><div class="admonition-content-holder"><div class="admonition-content"> Let p be a prime.

1. If a is an integer, then $a^p \equiv a \pmod{p}$.
2. If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} = 1 \pmod{p}$

Proof:

- Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$. None of these are divisible by p.
- Furthermore, we can claim no two are congruent mod p.
  - Suppose the contrary: that $ra = sa \pmod{p}$.
  - Then $(r - s)a = 0 \pmod{p}$, but neither factor is a multiple of p (as established earlier), and therefore this is impossible.
- Thus $a, 2a, 3a, \ldots, p-1 \pmod{p} = 1, 2, 3, \ldots, p-1 \pmod{p}$ in some scrambled order.)
  - $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$
  - $(a^{p-1} - 1)(p-1)! \equiv 0 \pmod{p}$
  - Therefore, $\boxed{a^{p-1} \equiv 1 \pmod{p}}$

</div></div></div>

2 | Totient functions

Let n be a positive integer. The totient of n, denoted $\phi(n)$ (or $\Phi(n)$), is the number of positive integers $a \leq n$ such that a and n are relatively prime (share no common factors other than 1).

Suppose the prime factorization of n is $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where each p_i is a distinct prime and each $e_i \geq 1$. Then, $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}) = (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \cdots (p_r^{e_r} - p_r^{e_r - 1})$.

2.1 | Euler's Totient Theorem

If $\text{gcd}(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

3 | Primitive Roots

If p is prime, then these is some integer g, depending on p, such that $g, g^2, g^3, \ldots, g^{p-1}$ are all distinct modulo p. Such an integer g is known as a primitive root.

4 | Euclidean Algorithm

$\text{gcd}(a, b) = \text{gcd}(a, b - a)$ If d is any factor of a, b, say $a = kd$ and $b = ld$, then $b - a = (l - k)d$.

$$\begin{aligned}\text{gcd}(301, 161) &= \text{gcd}(161, 140)\\ &= \text{gcd}(140, 21)\\ &= \text{gcd}(21, 14)\\ &= \text{gcd}(14, 7)\\ &= \text{gcd}(7, 0)\\ &= 7\end{aligned}$$

<div class="admonition" style="–admonition-color: 173, 173, 173;"><div class="admonition-title"><div class="admonition-title-content"><div class="admonition-title-icon"><i class="fas fa-quote-left" aria-hidden="true"></i></div><div class="admonition-title-markdown">Bézout 's Lemma</div></div></div><div class="admonition-content-holder"><div class="admonition-content"> If a, b are integers, then $\text{gcd}(a, b)$ is the smallest positive integer d such that there exist integers x, y with $ax + by = d$.

</div></div></div>

5 | Diffie-Hellman Key Exchange

Alice and Bob select a prime p and a primitive root $g \pmod{p}$. Alice picks a random number a, and Bob a random number b.

Alice computes $A = g^a \bmod p$ and sends it to Bob. Bob computes $B = g^b \bmod p$ and sends it to Alice.

Alice computes $k_1 = B^a \bmod p$ and Bob computes $k_2 = A^b \bmod p$. $k_1 = k_2$, so this is a shared piece of information between Alice and Bob.

<div class="admonition" style="–admonition-color: 173, 173, 173;"><div class="admonition-title"><div class="admonition-title-content"><div class="admonition-title-icon"><i class="fas fa-quote-left" aria-hidden="true"></i></div><div class="admonition-title-markdown">Discrete Logarithm Problem</div></div></div><div class="admonition-content-holder"><div class="admonition-content"> Given a prime p, a primitive root g, and a nonzero residue class $x \pmod{p}$, find a number a s.t. $g^a = x \pmod{p}$.

</div></div></div>