Number Theory

Number Theory is concerned with the properties of integers.

Important concepts:

- $\text{lcm}(m, n)$ is the **least common multiple**.
- $\gcd(m, n)$ is the **greatest common divisor**. We say that m and n are **relatively prime** (or **coprime**) if $\gcd(m, n) = 1$.
- $n \equiv o \mod m$ implies $n - o$ is a multiple of m. $(m|n - o)$
- **Modular Arithmetic.** If you only care about the value of an expression modulo n, then you can do your calculations modulo n.

Example. What is the last digit of 2^{20}?

Solution. The answer is $2^{20} \mod 10$. To solve, find a pattern:
$2^0 \equiv 1$, $2^1 \equiv \mathbf{2}$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 6$, $2^5 \equiv \mathbf{2}$. (Cycle period 4)

Number Theory

Important theorems:

- The Fundamental Theorem of Arithmetic. Every positive integer can be written as the product of primes in exactly one way. Often "Unique factorization": Write $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$.

- Bézout's identity For integers a and b, there exist integers x and y satisfying $ax + by = gcd(a, b)$

Example. Find an integral solution to the equation $10x + 6y = 14$.

Solution. We know that a solution exists to $10x + 6y = 2$; find it and then multiply x and y by 7. (Try $x = 2$, $y = -3$)

- You may want to read up on the Chinese remainder theorem.

Number Theory

Important theorems:

- Fermat's little theorem For p prime, n integer. Then $n^p \equiv n \mod p$. (When n and p are relatively prime, $n^{p-1} \equiv 1 \mod p$)

Example. Show that for every prime p there is an integer n such that $2^n + 3^n + 6^n - 1$ is divisible by p.

Solution. Try it out for small p. $2^1 + 3^1 + 6^1 - 1$
We know $2^{p-1}, 3^{p-1}, 6^{p-1} \equiv 1 \mod p$.
Consider $3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \mod p$.
Therefore, $6 \cdot 2^{p-2} + 6 \cdot 3^{p-2} + 6 \cdot 6^{p-2} \equiv 6 \mod p$.
We conclude $2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 0 \mod p$

- Wilson's theorem For p prime, $p \mid \big((p-1)! + 1\big)$.