Let us get into…

- Number Theory

Introduction to Number Theory

- Number theory is about **integers** and their properties.

- We will start with the basic principles of

  - divisibility,
  - greatest common divisors,
  - least common multiples, and
  - modular arithmetic

- and look at some relevant algorithms.

Division

- If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c so that $b = ac$.

- When a divides b we say that a is a **factor** of b and that b is a **multiple** of a.

- The notation **a | b** means that a divides b.

- We write **a X b** when a does not divide b
- (see book for correct symbol).

Divisibility Theorems

- For integers a, b, and c it is true that

- if a | b and a | c, then a | (b + c)
  - **Example:** 3 | 6 and 3 | 9, so 3 | 15.

- if a | b, then a | bc for all integers c
  - **Example:** 5 | 10, so 5 | 20, 5 | 30, 5 | 40, …

- if a | b and b | c, then a | c
  - **Example:** 4 | 8 and 8 | 24, so 4 | 24.

Primes

- A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p.

- A positive integer that is greater than 1 and is not prime is called composite.

- The fundamental theorem of arithmetic:

- Every positive integer can be written **uniquely** as the **product of primes**, where the prime factors are written in order of increasing size.

Primes

- Examples:

15 = $3 \cdot 5$

48 = $2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

17 = 17

100 = $2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

512 = $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9$

515 = $5 \cdot 103$

28 = $2 \cdot 2 \cdot 7$

The Division Algorithm

- Let **a** be an integer and **d** a positive integer.
- Then there are unique integers **q** and **r**, with **$0 \leq r < d$**, such that **$a = dq + r$**.

- In the above equation,
  - **d** is called the divisor,
  - **a** is called the dividend,
  - **q** is called the quotient, and
  - **r** is called the remainder.

The Division Algorithm

- **Example:**

- When we divide 17 by 5, we have

- $17 = 5 \cdot 3 + 2$.

- 17 is the dividend,
- 5 is the divisor,
- 3 is called the quotient, and
- 2 is called the remainder.

The Division Algorithm

- **Another example:**
- What happens when we divide -11 by 3 ?
- Note that the remainder cannot be negative.
- $-11 = 3 \cdot (-4) + 1$.

- -11 is the dividend,
- 3 is the divisor,
- -4 is called the quotient, and
- 1 is called the remainder.

Greatest Common Divisors

- Let a and b be integers, not both zero.
- The largest integer d such that d | a and d | b is called the **greatest common divisor** of a and b.
- The greatest common divisor of a and b is denoted by gcd(a, b).
- **Example 1:** What is gcd(48, 72) ?
- The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.
- **Example 2:** What is gcd(19, 72) ?
- The only positive common divisor of 19 and 72 is 1, so gcd(19, 72) = 1.

Greatest Common Divisors

- **Using prime factorizations:**

- $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
- where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$

- $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$

- **Example:**

$a = 60 = 2^2 3^1 5^1$

$b = 54 = 2^1 3^3 5^0$

$\gcd(a, b) = 2^1 3^1 5^0 = 6$

Relatively Prime Integers

- **Definition:**

- Two integers a and b are **relatively prime** if gcd(a, b) = 1.

- **Examples:**

- Are 15 and 28 relatively prime?
- Yes, gcd(15, 28) = 1.
- Are 55 and 28 relatively prime?
- Yes, gcd(55, 28) = 1.
- Are 35 and 28 relatively prime?
- No, gcd(35, 28) = 7.

Relatively Prime Integers

- **Definition:**

- The integers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- **Examples:**

- Are 15, 17, and 27 pairwise relatively prime?
- No, because gcd(15, 27) = 3.

- Are 15, 17, and 28 pairwise relatively prime?
- Yes, because gcd(15, 17) = 1, gcd(15, 28) = 1 and gcd(17, 28) = 1.

Least Common Multiples

- **Definition:**

- The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

- We denote the least common multiple of a and b by lcm(a, b).

- **Examples:**

lcm(3, 7) = 21

lcm(4, 6) = 12

lcm(5, 10) = 10

Least Common Multiples

- **Using prime factorizations:**

- $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
- where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$

- $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$

- **Example:**

$a = 60 = 2^2 3^1 5^1$

$b = 54 = 2^1 3^3 5^0$

$\text{lcm}(a, b) = 2^2 3^3 5^1 = 4 \cdot 27 \cdot 5 = 540$

GCD and LCM

a = 60 = 2^2 3^1 5^1

b = 54 = 2^1 3^3 5^0

gcd(a, b) = 2^1 3^1 5^0 = 6

lcm(a, b) = 2^2 3^3 5^1 = 540

Theorem: a□b = gcd(a,b)□lcm(a,b)

Modular Arithmetic

- Let a be an integer and m be a positive integer. We denote by **a mod m** the remainder when a is divided by m.

- **Examples:**

9 mod 4 = 1

9 mod 3 = 0

9 mod 10 = 9

-13 mod 4 = 3

Congruences

- Let a and b be integers and m be a positive integer. We say that **a is congruent to b modulo m** if m divides a – b.

- We use the notation **$a \equiv b \pmod{m}$** to indicate that a is congruent to b modulo m.

- In other words:
$a \equiv b \pmod{m}$ if and only if **a mod m = b mod m**.

Congruences

- **Examples:**
- Is it true that $46 \equiv 68 \pmod{11}$?
- Yes, because $11 \mid (46 - 68)$.
- Is it true that $46 \equiv 68 \pmod{22}$?
- Yes, because $22 \mid (46 - 68)$.
- For which integers z is it true that $z \equiv 12 \pmod{10}$?
- It is true for any $z \in \{\ldots, -28, -18, -8, 2, 12, 22, 32, \ldots\}$
- **Theorem:** Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

The Euclidean Algorithm

- The **Euclidean Algorithm** finds the **greatest common divisor** of two integers a and b.
- For example, if we want to find gcd(287, 91), we **divide** 287 by 91:
- $287 = 91 \cdot 3 + 14$
- We know that for integers a, b and c, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
- Therefore, any divisor of 287 and 91 must also be a divisor of $287 - 91 \cdot 3 = 14$.
- Consequently, gcd(287, 91) = gcd(14, 91).

The Euclidean Algorithm

- In the next step, we divide 91 by 14:
- $91 = 14 \cdot 6 + 7$
- This means that gcd(14, 91) = gcd(14, 7).
- So we divide 14 by 7:
- $14 = 7 \cdot 2 + 0$
- We find that $7 \mid 14$, and thus gcd(14, 7) = 7.
- **Therefore, gcd(287, 91) = 7.**

Representations of Integers

- Let b be a positive integer greater than 1.
Then if n is a positive integer, it can be expressed **uniquely** in the form:

- $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$,

- where k is a nonnegative integer,
- $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b,
- and $a_k \neq 0$.

- **Example for b=10:**

- $859 = 8 \cdot 10^2 + 5 \cdot 10^1 + 9 \cdot 10^0$

Fermat's Little Theorem

Theorem: If p is prime & k not a multiple of p

$$1 \equiv k^{p-1} \pmod{p}$$

For example, when p=5, k=4, we have $k^{p-1} \bmod p = 4^4 \bmod 5 = 1$