Number Theory: Complete Summary

Jubair Ahammad Akter

May 6, 2025

Contents

1. Divisibility

Basic Divisibility Rules

- Rule for 2: Last digit is even
- Rule for 3: Sum of digits divisible by 3
- Rule for 4: Last 2 digits divisible by 4
- Rule for 5: Last digit is 0 or 5
- Rule for 6: Divisible by 2 and 3
- Rule for 7: Double the last digit and subtract it from the rest of the number, then check is the new number divisible by 7
- Rule for 9: Sum of digits divisible by 9
- Rule for 10: Last digit is 0
- Rule for 11: Alternating sum of digits divisible by 11

Theorems and Properties(all are integer here)

- **Division Algorithm:** $a = bq + r$, with $0 \leq r < |b|$. $(a \neq 0)$
- If $a \mid b$, then $a \neq 0$ and $|a| \leq |b|$.
- If $a \mid b$, then $a \mid c$, then $a \mid (b + c)$.
- if a is an integer $a \mid a$, $a \mid 0$. and $a \mid -a$.
- **Transitivity:** If $a \mid b$ and $b \mid c$, then $a \mid c$.
- **Bézout's Identity:** If $\gcd(a, b) = d$, then $ax + by = d$ for some integers x, y.
- **Prime Divisibility:** If $p \mid ab$ and p is prime, then $p \mid a$ or $p \mid b$.

2. Modular Arithmetic, Inverse, and Residue Classes

- $m \mid (a - b) \iff a \equiv b \pmod{m}$.
- Operations, if $a \equiv b \pmod{m}$ and a,b,c are all integer:
  - $a + c \equiv b + c \pmod{m}$
  - $a - c \equiv b - c \pmod{m}$
  - $ac \equiv bc \pmod{m}$
  - $a^c \equiv b^c \pmod{m}$

- if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ where a,b,c,d,m are all integer, then,

$$ac \equiv bd, \pmod{m}$$

- **Cancellation:** If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.
- **Modular Inverse:** $a^{-1} \pmod{m}$ exists if $\gcd(a, m) = 1$.
- **For prime p:** $a^{-1} \equiv a^{p-2} \pmod{p}$.
- **Chienese Reminder Theorem (CRT):** For coprime m_1, m_2, m_3, solve:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases}$$

Solution: The solution to the system can be found using the formula:

$$x \equiv \sum_{i=1}^{3} a_i \cdot M_i \cdot y_i \pmod{M}$$

where:

$$M = m_1 \cdot m_2 \cdot m_3$$

$$M_i = \frac{M}{m_i}, \quad y_i \text{ is the modular inverse of } M_i \mod m_i.$$

That is, y_i satisfies:

$$M_i \cdot y_i \equiv 1, \pmod{m_i}$$

This means y_i is the number such that when M_i is multiplied by y_i, the result is congruent to 1 (modulo m_i). The modular inverse y_i can be found using the Extended Euclidean Algorithm.

3. Fermat's, Euler's, and Wilson's Theorems

- **Totient Function:** Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ be the prime factorization of n. Then the Euler's Totient Function $\phi(n)$ is:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

This formula applies for n which has the prime factorization $p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$. The product runs over all distinct primes $p_1, p_2, \ldots, p_k$ dividing n.

- **Fermat's Little Theorem:** $a^{p-1} \equiv 1$, (mod p) or $a^p \equiv a$, (mod p), if p is prime.
- **Euler's Theorem:** $a^{\phi(n)} \equiv 1 \pmod{n}$, if $\gcd(a, n) = 1$.
- **Wilson's Theorem:** $(p-1)! \equiv -1 \pmod{p}$ or $(p-2)! \equiv 1 \pmod{p}$, if p is prime.

4. Primes, GCD, and LCM

- **Prime:** Divisible only by 1 and itself.
- **GCD:** Use Euclidean algorithm: $\gcd(a, b) = \gcd(b, a \mod b)$.
- **LCM:** $\text{lcm}(a, b) = \frac{a \cdot b}{\gcd(a,b)}$.
- The relation between GCD and LCM:

GCD and LCM Relationship

Let

$$a = dx, \quad b = dy$$

where $\gcd(x, y) = 1$. Then,

$$\gcd(a, b) = d$$

$$\text{lcm}(a, b) = dxy$$

$$\gcd(a, b) \times \text{LCM}(a, b) = d \times dxy = (dx) \times (dy) = a \times b$$

5. Number, Sum, and Product of Divisors

Let the prime factorization of n be:

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

- **Number of Prime Divisors:** k
- **Number of Divisors:**

$$\tau(n) = \prod_{i=1}^{k} (a_i + 1) = (a_1 + 1)(a_2 + 1) \dots (a_k + 1)$$

- **Sum of Divisors:**

$$\sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1} \right) \times \left(\frac{p_2^{a_2+1} - 1}{p_2 - 1} \right) \times \cdots \times \left(\frac{p_k^{a_k+1} - 1}{p_k - 1} \right)$$

- **Product of Divisors:** Product of Divisors $= n^{\frac{\tau(n)}{2}} = n^{\frac{\text{Number of Divisors of n}}{2}}$

Divisor Calculations for $n = 64800 = 2^5 \times 3^4 \times 5^2$

- **Number of Prime Divisors:** $k = 3$
- **Number of Divisors:**

$$\tau(64800) = (5+1)(4+1)(2+1) = 6 \times 5 \times 3 = 90$$

- **Sum of Divisors:**

$$\sigma(64800) = \left(\frac{2^{5+1}-1}{2-1}\right) \times \left(\frac{3^{4+1}-1}{3-1}\right) \times \left(\frac{5^{2+1}-1}{5-1}\right)$$

$$\sigma(64800) = 63 \times 121 \times 31 = 238713$$

- **Product of Divisors:**

$$\text{Product of Divisors} = 64800^{\frac{90}{2}} = 64800^{45}$$

Divisor Calculations for $n = 2500 = 2^2 \times 5^4$

- **Number of Prime Divisors:** $k = 2$
- **Number of Divisors:**

$$\tau(2500) = (2+1)(4+1) = 3 \times 5 = 15$$

- **Sum of Divisors:**

$$\sigma(2500) = \left(\frac{2^{2+1}-1}{2-1}\right) \times \left(\frac{5^{4+1}-1}{5-1}\right)$$

$$\sigma(2500) = 7 \times 781 = 5467$$

- **Product of Divisors:**

$$\text{Product of Divisors} = 2500^{\frac{15}{2}} = \left(2500^{\frac{1}{2}}\right)^{15} = 50^{15}$$

6. Number Systems

Decimal	Binary	Octal	Hexadecimal
0	0000	00	0
1	0001	01	1
2	0010	02	2
3	0011	03	3
4	0100	04	4
5	0101	05	5
6	0110	06	6
7	0111	07	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F
16	10000	20	10

Table 1: Number system conversions for decimal, binary, octal, and hexadecimal

- Decimal: Base 10
- Binary: Base 2 (e.g., $1011_2 = 11_{10}$)
- Octal: Base 8 (e.g., $17_8 = 15_{10}$)
- Hexadecimal: Base 16 (e.g., $1F_{16} = 31_{10}$)

Decimal 123 to Binary

Converting Decimal 123 to Binary:
1. Decimal 123 to Binary:

$$123 \div 2 = 61 \text{ remainder } 1$$

$$61 \div 2 = 30 \text{ remainder } 1$$

$$30 \div 2 = 15 \text{ remainder } 0$$

$$15 \div 2 = 7 \text{ remainder } 1$$

$$7 \div 2 = 3 \text{ remainder } 1$$

$$3 \div 2 = 1 \text{ remainder } 1$$

$$1 \div 2 = 0 \text{ remainder } 1$$

Reading the remainders from bottom to top, we get:

$$123_{\text{decimal}} = 1111011_{\text{binary}}$$

Decimal 123 to Hexadecimal

Converting Decimal 123 to Hexadecimal:
2. Decimal 123 to Hexadecimal:

$$123 \div 16 = 7 \text{ remainder } 11$$

Since the remainder is 11, which corresponds to **B** in hexadecimal:

$$123_{\text{decimal}} = 7B_{\text{hexadecimal}}$$

Hexadecimal '7B' to Decimal

Converting Hexadecimal '7B' to Decimal:
3. Hexadecimal $7B$ to Decimal: In hexadecimal, the place values are powers of 16. So, we have:

$$7 \times 16^1 + 11 \times 16^0 = 7 \times 16 + 11 = 112 + 11 = 123$$

Thus:

$$7B_{\text{hexadecimal}} = 123_{\text{decimal}}$$

7. Legendre's Theorem

The exponent of a prime p in $n!$:

$$e_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Legendre's Theorem: This theorem gives the exponent of a prime p in the prime factorization of $n!$.

The exponent $\alpha_p(n!)$ of a prime p in $n!$ is given by:

$$\alpha_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

where $\left\lfloor \frac{n}{p^k} \right\rfloor$ is the number of multiples of p^k less than or equal to n.

Example: Power of 2 in $10!$

To find the power of 2 in $10!$:

$$\alpha_2(10!) = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{4} \right\rfloor + \left\lfloor \frac{10}{8} \right\rfloor = 5 + 2 + 1 = 8$$

So, the power of 2 in $10!$ is 8.

8. Pythagorean Triples

If $a, b, c \in \mathbf{Z}^+$ and $a^2 + b^2 = c^2$, then (a, b, c) is called a Pythagorean triple.

(3,4,5)	(5,12,13)	(7,24,25)	(8,15,17)	(9,40,41)	(11,60,61)	(12,35,37)
(6,8,10)	(10,24,26)	(14,48,50)	(16,30,34)	(18,80,82)	(22,120,122)	(24,70,74)
(9,12,15)	(15,36,39)	(21,72,75)	(24,45,51)	(27,120,123)	(33,180,183)	(36,105,111)

Table 2: List of Primitive and Non-Primitive Pythagorean Triples

Eucledean technique:
The triples can be generated using the following formulas:

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

where $m > n > 0$

9. Floor and Ceiling Functions

Definition:

- The *floor function*, denoted $\lfloor x \rfloor$, is the greatest integer less than or equal to x.
- The *ceiling function*, denoted $\lceil x \rceil$, is the least integer greater than or equal to x.

Both functions are defined for any real number x.

Examples:

1. **For positive numbers:**
$$\lfloor 2.7 \rfloor = 2, \quad \lceil 2.7 \rceil = 3$$
2. **For negative numbers:**
$$\lfloor -2.7 \rfloor = -3, \quad \lceil -2.7 \rceil = -2$$
3. **For positive integers:**
$$\lfloor 5 \rfloor = 5, \quad \lceil 5 \rceil = 5$$
4. **For negative integers:**
$$\lfloor -5 \rfloor = -5, \quad \lceil -5 \rceil = -5$$

Fractional Part:
The fractional part of a number x, denoted $\{x\}$, is defined as:

$$x = \lfloor x \rfloor + \{x\}$$

This represents the "decimal" part of x, which is always between 0 and 1, i.e., $0 \leq \{x\} < 1$.

Example of Fractional Part

Example for positive number: For $x = 3.14$,

$$\lfloor 3.14 \rfloor = 3, \quad \{3.14\} = 3.14 - 3 = 0.14$$

Example for negative number: For $x = -2.75$,

$$\lfloor -2.75 \rfloor = -3, \quad \{-2.75\} = -2.75 - (-3) = 0.25$$

Theories and Properties:

- **Floor function properties:**
  - If x is an integer, then $\lfloor x \rfloor = x$.
  - $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.
  - $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$.
  - $\lfloor x \rfloor = x - \{x\}$, where $\{x\}$ is the fractional part of x.
- **Ceiling function properties:**
  - If x is an integer, then $\lceil x \rceil = x$.
  - $\lceil x \rceil - 1 < x \leq \lceil x \rceil$.
  - $\lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil$.
  - $\lceil x \rceil = x + (1 - \{x\})$, where $\{x\}$ is the fractional part of x and $x \notin \mathbb{Z}$.
- **Floor and Ceiling function relations:**
  - For any real number x:
  $$\lceil x \rceil = -\lfloor -x \rfloor$$
  - For any real number x:
  $$\lfloor x \rfloor + \lceil x \rceil = \lfloor x \rfloor + \lfloor x \rfloor + 1 \quad \text{if } x \notin \mathbb{Z}$$