Topics from Number Theory

1. Integer Division with Remainder
   If an integer n is divided by a non-zero integer m, there must be an integral quotient q and a remainder r, where $0 \leq |r| < m$. This operaton is called Integer Division with Remainder and denoted by

   $$n = mq + r.$$

2. Two intergers a and b are said to be congruent modulo m, denoted by $a \equiv b \pmod{m}$, if a and b have the same remainder when they are divided by a non-zero integer m.
   If the remainders are different, then a and b are said to be not congruent modulo m and denoted by $a \not\equiv b \pmod{m}$.

3. If $a \equiv b \pmod{m}$, then the following statements are true:
   (a) $a - b = p \cdot m$, where p is an integer.
   (b) $a - b \equiv 0 \pmod{m}$
   (c) $m|(a - b)$

4. Properties of Congruence
   (a) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$
   (b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$
   (c) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \cdot c \equiv b \cdot d \pmod{m}$
   (d) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$, for all natural numbers n.
   (e) If $a \cdot c \equiv b \cdot c \pmod{m}$, and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

5. Units Digit of Powers of Positive Integers a^n, $n \in \mathbb{N}$.
   (a) If the units digit of a is 0, 1, 5, or 6, the units digit of a^n is the same as the units digit of a.

(b) If the units digit of a is 4, the units digit of a^n alternates between 4 and 6.

(c) If the units digit of a is 9, the units digit of a^n alternates between 9 and 1.

(d) If the units digit of a is 2, the units digit of a^n is periodic with the sequence 2, 4, 8, and 6. The period is 4.

(e) If the units digit of a is 3, the units digit of a^n is periodic with the sequence 3, 9, 7, and 1. The period is 4.

(f) If the units digit of a is 7, the units digit of a^n is periodic with the sequence 7, 9, 3, and 1. The period is 4.

(g) If the units digit of a is 8, the units digit of a^n is periodic with the sequence 8, 4, 2, and 6. The period is 4.

6. Last Two Digits of Powers of Positive Integers a^n, $n \in \mathbb{N}$

(a) The last two digits of 5^n, $n \geq 2$ are 25.

(b) The last two digits of 6^n, $n \geq 2$ repeat in the sequence "36, 16, 96, 76, 56" with a period 5.

(c) The last two digits of 7^n, $n \geq 2$ repeat in the sequence "49, 43, 01, 07" with a period 4.

(d) The last two digits of 76^n are always 76.

7. Properties of Perfect Squares

(a) The units digit of a perfect square can only be among 0, 1, 4, 5, 6, or 9. The units digit of a perfect square cannot end in 2, 3, 7, or 8.

(b) If the prime factorization of a natural number n is $p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, then for n to be a perfect square, $m_1, m_2, \dots, m_k$ all have to be even and consequently, the number of positive divisors of n have to be odd.

(c) For a perfect square number ending in zeros, the number of tail zeros has to be even.

(d) $n^2 \equiv 0$ or $1 \pmod{2, 3, 4}$.

(e) $n^2 \equiv 0$, 1 or $4 \pmod 8$.

(f) An odd perfect square number having two or more digits must have an even tens digit.

(g) If the tens digit of a perfect square number n^2 is odd, then the units digit of n^2 must be 6.

8. Properties of Floor Function and Fractional Part of a Real Number

(a) For any real number x, the largest integer less than or equal to x, denoted by $\lfloor x \rfloor$, is called the integer part of x. The function $f(x) = \lfloor x \rfloor$ where $x \in \mathbb{R}$, is called the floor function of x.

(b) For any real number x, the value $x - \lfloor x \rfloor$, denoted by $\{x\}$, is called the fractional part of x.

(c) For $x \in \mathbb{R}$, $0 \leq \{x\} < 1$, and $\{x\} = 0$ if and only if x is an integer.

(d) For $x \in \mathbb{R}$, $x - 1 < \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

(e) For $n \in \mathbb{Z}$ and $x \in \mathbb{R}$, $\lfloor n + x \rfloor = n + \lfloor x \rfloor$.

(f) For $x \in \mathbb{R}$,

$$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor - 1 & \text{if x is not an integer} \\ -\lfloor x \rfloor & \text{if x is an integer.} \end{cases}$$

(g) $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor \geq \lfloor x + y \rfloor - 1$, where $x, y \in \mathbb{R}$.
In general, for $x_1, x_2, \ldots, x_n \in \mathbb{R}$,

$$\lfloor x_1 + x_2 + \cdots + x_n \rfloor \geq \lfloor x_1 \rfloor + \lfloor x_2 \rfloor + \cdots + \lfloor x_n \rfloor.$$

(h) $\lfloor xy \rfloor \geq \lfloor x \rfloor \cdot \lfloor y \rfloor$, where $x, y \geq 0$.
In general, for $x_1, x_2, \ldots, x_n \geq 0$,

$$\lfloor x_1 x_2 \ldots x_n \rfloor \geq \lfloor x_1 \rfloor \cdot \lfloor x_2 \rfloor \ldots \cdot \lfloor x_n \rfloor.$$

(i) $\lfloor \frac{x}{n} \rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$ for $n \in \mathbb{N}, x \in \mathbb{R}$.

(j) Hermite Identity
For any $x \in \mathbb{R}$,

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor .$$

(k) Legendre's Theorem
In the prime factorization of the product $n! = 1 \cdot 2 \ldots \cdot n$,the index of a prime factor p is given by

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$