# NUMBER THEORY AND CRYPTOGRAPHY

AMBRESH YADAV

*Date*: Mahindra University & IIIT Kancheepuram
April 30, 2026.

Contents

1. Euclidean Division Algorithm 3
1.1. Greatest Common Divisor 3
2. Congruence 6
3. Prime Numbers and Generalized Induction 10
4. Definition of a Ring: 15
5. Unit 20
6. Binomial Coefficients 36
7. RSA Encryption and Decryption 38
7.1. Key Generation: 38
7.2. Decryption: 38
7.3. Binomial Coefficients 40
8. Introduction to cryptography 44
8.1. ONE-WAY FUNCTIONS 54
8.2. CONSTRUCTING ONE-WAY FUNCTIONS 56

## 1. Euclidean Division Algorithm

**Theorem 1.1.** Let $a$ and $b$ be positive integers with $a < b$. If $a$ divides $b$, then the greatest common divisor of $a$ and $b$ is $a$. If $a$ does not divide $b$, then the Euclidean algorithm applied to $a$ and $b$ terminates after a finite number $n$ of steps. The output of the algorithm, $r_n$, is the greatest common divisor of $a$ and $b$.

*Proof.* Consider the case when $a$ does not divide $b$. We apply the Euclidean algorithm as follows:

$$\begin{aligned}
b &= aq_1 + r_1 \quad \text{with} \quad 0 \leq r_1 < a, \\
a &= r_1q_2 + r_2 \quad \text{with} \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2q_3 + r_3 \quad \text{with} \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n \quad \text{with} \quad 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_nq_{n+1} + 0.
\end{aligned}$$

At this point, $r_n$ is the greatest common divisor of $a$ and $b$. This conclusion follows from the fact that the Euclidean algorithm terminates when the remainder is zero, and the last non-zero remainder is $r_n$. Thus, we have:

$$\gcd(a, b) = r_n.$$

Since the sequence of remainders $\{r_i\}$ is strictly decreasing and bounded below by 0, the algorithm must terminate after a finite number of steps. Therefore, the greatest common divisor of $a$ and $b$ is $r_n$. □

### 1.1. Greatest Common Divisor.

**Exercise 1.1.** Use the Euclidean algorithm to calculate the greatest common divisior in the following cases.

(1) item gcd of 6 and 9
(2) gcd of 25 and 40

**Solution 1.1.** (1)

$$9 = 6 \cdot 1 + 3$$
$$r_1 = 3$$

,

$$6 = 3 \cdot 2 + 0$$
$$\text{Thus,} \quad \gcd(6, 9) = 3$$

(2)

$$40 = 25 \cdot 1 + 15$$

,

$$quadso \quad r_1 = 15,$$

$$25 = 15 \cdot 1 + 10$$

,

$$quadso \quad r_2 = 10,$$

$$15 = 10 \cdot 1 + 5$$

,

$$quadso \quad r_3 = 5$$

,

$$10 = 5 \cdot 2 + 0$$

.

$$quadThus, \quad \gcd(25, 40) = 5$$

**Theorem 1.2** (Bezout Theorem)**.** Let $a$ and $b$ be integers with greatest common divisor $d$. Then there exist integers $r$ and $s$ such that $d = ar + bs$

*Proof.* Let $a$ and $b$ be integers with greatest common divisor $d$. By the definition of the greatest common divisor, $d$ divides both $a$ and $b$, and any common divisor of $a$ and $b$ divides $d$.

By the Euclidean algorithm, there exist integers $x$ and $y$ such that $d = ax + by$. We will show that such integers $r$ and $s$ exist as well.

Consider the set $S = ax + by : x, y \in \mathbb{Z}$. Since $d = ax + by$ is an element of $S$, $S$ is non-empty. Let $r$ be the smallest positive integer in $S$. By the well-ordering principle, such an $r$ exists.

Now, let $s = \frac{d-ar}{b}$. We need to show that $s$ is an integer. Since $r$ is the smallest positive integer in $S$, $d - ar$ must be a multiple of $b$. Therefore, $\frac{d-ar}{b}$ is an integer.

Now, we will show that $d = ar + bs$.

$$d = ax + by$$

$$d = ar + (d - ar)/b * b$$

$$d = ar + (d - ar) = d$$

□

**Theorem 1.3.** Suppose that a and b are two relatively prime integers, and suppose that $c$ is an integer such that a divides the product $bc$. Then a divides $c$.

*Proof.* Since it is given that a and b is relatively prime integer therefore GCD(a,b)=1 we know from Bezout theorem if a and b is integer with GCD equal to d then there exist integer x and y such that

$$d = ax + by$$

as( d=1)

$$1 = ax + by$$

multiply by c both side

$$c = (ac)x + (bc)y$$

since a divides bc(given) and a divides ac therefore a will divides thier sum that is a divides c □

**Proposition 1.1.** Let $a$ and $b$ be relatively prime integers, and suppose that $c$ is an integer and n a positive integer such that a divides the product $b^{nc}$. Then a divides c.

*Proof.* □

**Theorem 1.4** (Descartes)**.** Suppose $a_0, a_1, \ldots, a_n$ an are integers, and suppose further that $r$ and $s$ are relatively prime integers such that the rational number$\frac{r}{s}$ is a solution to the equation

$$a_n x^n + a_{n_1} x^{n-1} + \cdots + a_1 x_1 + a_0 = 0$$

Then $s$ divides $a_n$ and $r$ divides $a_0$.

*Proof.* Since it is given that $\frac{r}{s}$ is solution of the given equation, so lets place this in the equation

$$a_n x^n + a_{n_1} x^{n-1} + \cdots + a_1 x_1 + a_0 = 0$$

now it will become

$$a_n r^n + a_{n1} r^{n1} s + \cdots + a_1 r s^{n1} + a_0 s^n = 0$$

now rewrite the RHS part

$$a_n r^n + a_{n1} r^{n1} + \cdots + a_0 s^{n1)} s = 0$$
$$a_n r^n = -(a_{n1} r^{n1} + \cdots + a_0 s^{n1})$$

now we can see that s divides $a_n r^n$ , from Proposition 1.1 we can conclude that s divides $a_n$ □

**Theorem 1.5** (Solution to Diophantine equation)**.** Let $a, b, c$ be integers. The equation $ax+by = c$ has integer solutions if and only if $gcd(a, b)$ divides.

**Problem 1.1.** Find a solution to the equation $4x + 18y = 32$

**Solution 1.2.** Applying the Euclidean algorithm, we see $2 = (18, 4) = 18+4\times(-4)$. Multiplying through by 16 gives $18(16) + 4(64) = 32$.

**Definition 1.1** (Quadratic Diophantine Equations - Pythagorean Triples)**.**

A solution

$$(x0, y0, z0)$$

to the diophantine equation $x^2 + y^{=}z^2$ is called a Pythagorean triple. A Pythagorean triple is primitive if $x0, y0, z0$ are pairwise relatively prime. Looking (mod 4), we see a primitve Pythagorean triple must have exactly one of $x$ and $y$ be even and the other odd.

**Theorem 1.6.** For integers $a, b$ and $e$, if $(a, b)$ divides $e$, then the equation $ax + by = e$ has an integer solution

*Proof.* Assume that $(a, b) = d$. We are assuming that d divides e, therefore $e = dt$
By Theorem 1.2 there are solutions $x = r$ and $y = s$ to the equation $ax + by = d$, that is, there are integers $r$ and $s$ such that $ar + bs = d$. Multiplying both sides of this last equation by $t$, we obtain

$$a(rt) + b(st) = dt = e. \tag{1}$$

Thus, the equation $ax + by = e$ has the solution $x = rt$ and $y = st$. □

**Problem 1.2.** For each of the following equations, decide whether it can be solved in integers. If so, find a solution.

(1) $6x + 9y = 2$;
(2) $6x + 9y = -33$;
(3) $25x + 40y = 345$;
(4) $14x + 85y = 3$;
(5) $66x + 561y = 22$.

**Solution 1.3.** 1. $6x + 9y = 2$

This equation can't be solved in integers because 2 is not a multiple of the greatest common divisor of 6 and 9, which is 3.

2. $6x + 9y = -33$

This equation can be solved in integers because $-33$ is a multiple of the greatest common divisor of 6 and 9, which is 3. We can divide both sides by 3 to get $2x+3y = -11$. One possible solution is $x = -5$ and $y = 5$.

3. $25x + 40y = 345$

This equation can be solved in integers because 345 is a multiple of the greatest common divisor of 25 and 40, which is 5. We can divide both sides by 5 to get $5x+8y = 69$. One possible solution is $x = 13$ and $y = -8$.

4. $14x + 85y = 3$

This equation can't be solved in integers because 3 is not a multiple of the greatest common divisor of 14 and 85, which is 1.

5. $66x + 561y = 22$

This equation can't be solved in integers because 22 is not a multiple of the greatest common divisor of 66 and 561, which is 3.

**Problem 1.3.** Suppose you have two hourglasses, the first measuring a time period of $a$ minutes and the second measuring a time period of $b$ minutes. How can you use them to measure a time period of $c$ minutes, where $a$, $b$, and $c$ are as follows?

(1) $a = 3$, $b = 7$, and $c = 8$;
(2) $a = 5$, $b = 7$, and $c = 11$;
(3) $a = 6$, $b = 11$, and $c = 13$.

**Solution 1.4.** (1) For $a = 3$, $b = 7$, and $c = 8$:

- Start both hourglasses together.
- When the first hourglass runs out (after 3 minutes), flip it immediately.
- When the second hourglass runs out (after 7 minutes), flip it immediately.
- When the first hourglass runs out again (after 6 minutes, since it has been flipped), stop the second hourglass.

At this point, the first hourglass has been running for 6 minutes and the second hourglass has been running for 1 minute, totaling 7 minutes. Since the first hourglass still has 2 minutes of sand left, we can use it to measure the remaining 1 minute needed to reach 8 minutes.

(2) For $a = 5$, $b = 7$, and $c = 11$: A similar approach can be used as in case 1, with the hourglasses running for 10 minutes, and then using the first hourglass for 1 minute to complete the measurement.

(3) For $a = 6$, $b = 11$, and $c = 13$:

A similar approach can be used as in the previous cases, with the hourglasses running for 12 minutes, and then using the first hourglass for 1 minute to complete the measurement.

## 2. Congruence

**Definition 2.1** (Congruence)**.** For a positive integer m and integers a and b, we follow Gauss and write a  b (mod m) to mean that a and b have the same remainder upon division by m. In words, the notation is read as a is congruent to b modulo m.

**Theorem 2.1.** Fix an integer m ¿ 1. Suppose a, b, and c are integers such that

$$a \equiv b \pmod{m}$$

and

$$b \equiv c \pmod{m}$$

Then

$$a \equiv c \pmod{m}$$

*Proof.* the congruence

$$a \equiv b \pmod{m}$$

implies that (a-b) is divisible by m similarly congruence

$$b \equiv c \pmod{m}$$

implies that (b-c) is divisible by m and we know that if a number divides two integer then it will also divides their sum ,hence m divides (a-b)+(b-c)

this implies

$$a \equiv c \pmod{m}$$

□

**Proposition 2.1.** Fix an integer m ¿ 1. Suppose a, b, e, and f are integers satisfying

$$a \equiv e \pmod{m}$$

and

$$b \equiv f \pmod{m}$$

. Then

$$(a+b) \equiv (e+f) \pmod{m}$$

. and

$$(ab) \equiv (ef) \pmod{m}$$

**Proposition 2.2.** Fix an integer m ¿ 1. Suppose a and b are integers satisfying

$$a \equiv b \pmod{m}$$

Then for every integer r, the congruence

$$(ra) \equiv (rb) \pmod{m}$$

holds.

**Theorem 2.2.** **Let a and m be positive integers with $m >$1. The congruence**

$$(ax) \equiv c \pmod{m}$$

**is solvable if and only if (a,m) = 1.**

- **Part 1: If** $\gcd(a,m) = 1$**, then** $ax \equiv 1 \pmod{m}$ **is solvable.**

  *Proof.* – By definition, $\gcd(a,m) = 1$ means that there exist integers $x$ and $y$ such that:

  $$ax + my = 1$$

  This is a direct result of Bézout's Identity.

  – Rearrange this equation as:

  $$ax + my = 1 \implies ax \equiv 1 \pmod{m}$$

  – This shows that there exists an integer $x$ (specifically the one from Bézout's Identity) such that $ax \equiv 1 \pmod{m}$.

  Thus, if $\gcd(a,m) = 1$, the congruence $ax \equiv 1 \pmod{m}$ has a solution. □

- **Part 2: If** $ax \equiv 1 \pmod{m}$ **is solvable, then** $\gcd(a,m) = 1$**.**

  *Proof.* – Suppose $ax \equiv 1 \pmod{m}$ has a solution. This means there exists an integer $x$ such that:

  $$ax \equiv 1 \pmod{m}$$

  In other words, there exists an integer $k$ such that:

  $$ax - 1 = km \implies ax - km = 1$$

– This equation can be rewritten as:

$$ax + m(-k) = 1$$

which shows that 1 can be expressed as a linear combination of $a$ and $m$.

– According to Bézout's Identity, if 1 can be written as a linear combination of $a$ and $m$, then the greatest common divisor of $a$ and $m$ must be 1:

$$\gcd(a, m) = 1$$

Thus, if $ax \equiv 1 \pmod{m}$ is solvable, then $\gcd(a, m) = 1$. □

Combining Part 1 and Part 2, we have shown that the congruence $ax \equiv 1 \pmod{m}$ is solvable if and only if $\gcd(a, m) = 1$. This completes the proof.

- For each of the congruences below, decide whether there is a solution. If there is one, find a solution using the Euclidean algorithm.

**Problem 2.1.** $8x \equiv 1 \pmod{6}$

**Solution 2.1.** (1) Find $\gcd(8, 6)$:

$$8 = 6 \cdot 1 + 2,$$
$$6 = 2 \cdot 3 + 0.$$

So, $\gcd(8, 6) = 2$.

(2) Since $\gcd(8, 6) = 2$ does not divide 1, there is no solution to $8x \equiv 1 \pmod{6}$.

**Problem 2.2.** $8x \equiv 4 \pmod{6}$

**Solution 2.2.** (1) Find $\gcd(8, 6)$:

$$8 = 6 \cdot 1 + 2,$$
$$6 = 2 \cdot 3 + 0.$$

So, $\gcd(8, 6) = 2$.

(2) Since $\gcd(8, 6) = 2$ divides 4, there is a solution. Simplify the congruence by dividing everything by $\gcd(8, 6) = 2$:

$$\frac{8}{2}x \equiv \frac{4}{2} \pmod{\frac{6}{2}} \implies 4x \equiv 2 \pmod{3}.$$

(3) Solve $4x \equiv 2 \pmod{3}$. Since $4 \equiv 1 \pmod{3}$, the equation becomes:

$$x \equiv 2 \pmod{3}.$$

(4) Thus, $x = 2$ is a solution to $8x \equiv 4 \pmod{6}$.

**Problem 2.3.** $15x \equiv 1 \pmod{21}$

**Solution 2.3.** (1) Find $\gcd(15, 21)$:

$$21 = 15 \cdot 1 + 6,$$
$$15 = 6 \cdot 2 + 3,$$
$$6 = 3 \cdot 2 + 0.$$

So, $\gcd(15, 21) = 3$.

(2) Since $\gcd(15, 21) = 3$ does not divide 1, there is no solution to $15x \equiv 1 \pmod{21}$.

**Problem 2.4.** $15x \equiv 6 \pmod{21}$

**Solution 2.4.** (1) Find $\gcd(15, 21)$:

$$21 = 15 \cdot 1 + 6,$$
$$15 = 6 \cdot 2 + 3,$$
$$6 = 3 \cdot 2 + 0.$$

So, $\gcd(15, 21) = 3$.

(2) Since $\gcd(15, 21) = 3$ divides 6, there is a solution. Simplify the congruence by dividing everything by $\gcd(15, 21) = 3$:

$$\frac{15}{3}x \equiv \frac{6}{3} \pmod{\frac{21}{3}} \implies 5x \equiv 2 \pmod 7.$$

(3) Solve $5x \equiv 2 \pmod 7$ using the Euclidean algorithm:

$$7 = 5 \cdot 1 + 2,$$
$$5 = 2 \cdot 2 + 1,$$
$$2 = 2 \cdot 1 + 0.$$

(4) Back-substitute to express 1 as a linear combination of 5 and 7:

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7.$$

Thus, $x \equiv 3 \pmod 7$ is a solution.

**Problem 2.5. Problem** Observe that $ra$ is $(a, m)$-accessible for every positive integer $r$. In particular, the integers $a, 2a, 3a, \ldots, (m-1)a$ are all $(a, m)$-accessible.

**Solution 2.5.** By definition, an integer $n$ is $(a, m)$-accessible if it can be expressed as a non-negative linear combination of $a$ and $m$, i.e., $n = xa + ym$ for some non-negative integers $x$ and $y$.

For any positive integer $r$, $ra$ can be written as:

$$ra = ra + 0 \cdot m$$

Here, $x = r$ and $y = 0$ are non-negative integers, showing that $ra$ is $(a, m)$-accessible.

In particular, for $r = 1, 2, \ldots, m-1$, the integers $a, 2a, 3a, \ldots, (m-1)a$ are all of the form $ra$, making them $(a, m)$-accessible.

**Problem 2.6. Problem** Deduce from this that $ra + sm$ is also $(a, m)$-accessible for every non-negative integer $s$.

**Solution 2.6.** Given $ra$ is $(a, m)$-accessible, let's consider $ra + sm$ for any non-negative integer $s$.

We can express $ra + sm$ as:

$$ra + sm = ra + sm$$

Here, $x = r$ and $y = s$ are non-negative integers, thus showing that $ra + sm$ is $(a, m)$-accessible.

**Problem 2.7. Problem** For an integer $r$ between 0 and $m - 1$, the congruence class $C(ra)$ consists of all the integers congruent to $ra$ modulo $m$. Observe that these are the integers of the form $\ldots, ra - 2m, ra - m, ra, ra + m, ra + 2m, ra + 3m, \ldots$. Deduce that all the integers in this congruence class that are greater than or equal to $ra$ are $(a, m)$-accessible.

**Solution 2.7.** Consider the congruence class $C(ra)$ which consists of all integers of the form $ra+km$, where $k$ is any integer. The integers $ra, ra+m, ra+2m, \ldots$ are all in this class and greater than or equal to $ra$.

From the previous results, we know that $ra$ is $(a,m)$-accessible. For any $k \geq 0$, $ra+km$ can be expressed as:

$$ra + km = ra + km$$

Here, $x = r$ and $y = k$ are non-negative integers. Therefore, all integers in the congruence class $C(ra)$ that are greater than or equal to $ra$ are $(a,m)$-accessible.

**Remark 2.1.** we know $ra + sm$ is $(a,m)$-accessible for non-negative $s$. Therefore, all integers of the form $ra + km$ where $k \geq 0$ (i.e., $k = 0, 1, 2, \ldots$) are $(a,m)$-accessible.

.

**Problem 2.8.**
Deduce that in the congruence class $C(ra)$, the largest integer that might fail to be $(a,m)$-accessible, assuming that it is positive, is $ra - m$.

**Solution 2.8.** From the congruence class $C(ra)$, the integers greater than or equal to $ra$ are $(a,m)$-accessible. The integer just below $ra$ in the congruence class is $ra - m$. Hence, $ra - m$ is the largest integer that might not be $(a,m)$-accessible if it is positive.

## 3. Prime Numbers and Generalized Induction

**Theorem 3.1.** Every integer $n \geq 2$ is divisible by a prime number.

**Proof by Induction:**

- Base Case: For $n = 2$
  - The integer 2 is a prime number.
  - Therefore, 2 is divisible by itself, a prime number.

  Induction Hypothesis:
  - Assume that for some integer $k \geq 2$, the statement is true.
  - That is, $k$ is divisible by a prime number.
- Induction Step:
  - We need to show that $k+1$ is also divisible by a prime number.
  - Case 1: $k+1$ is a prime number.
    - If $k+1$ is a prime number, then it is trivially divisible by itself, a prime number.
  - Case 2: $k+1$ is not a prime number.
    - If $k+1$ is not a prime number, it can be written as a product of two integers, say $a$ and $b$, where $1 < a \leq b < k+1$.
    - Since $1 < a < k+1$ and $1 < b < k+1$, both $a$ and $b$ are integers less than $k+1$.
    - According to the induction hypothesis, $a$ and $b$ must be divisible by some prime numbers.
    - Therefore, $k+1 = a \cdot b$ must also be divisible by a prime number, as at least one of the factors $a$ or $b$ must be divisible by a prime number.

Thus, by the principle of mathematical induction, we conclude that every integer $n \geq 2$ is divisible by a prime number.

**Theorem 3.2.** Every integer $n \geq 2$ is either a prime number or a product of a finite number of prime numbers.

*Proof.* **Proof by Induction:**

- **Base Case:** For $n = 2$
  - The integer 2 is a prime number.
  - Therefore, 2 satisfies the statement as it is a prime number.
- **Induction Hypothesis:**
  - Assume that for some integer $k \geq 2$, the statement is true.
  - That is, every integer $n$ such that $2 \leq n \leq k$ is either a prime number or can be expressed as a product of a finite number of prime numbers.
- **Induction Step:**
  - We need to show that $k+1$ is either a prime number or can be expressed as a product of a finite number of prime numbers.
  - **Case 1:** $k + 1$ is a prime number.
    - If $k + 1$ is a prime number, then it satisfies the statement trivially, as it is a prime number.
  - **Case 2:** $k + 1$ is not a prime number.
    - If $k + 1$ is not a prime number, it can be written as a product of two integers $a$ and $b$, where $2 \leq a \leq b < k + 1$.
    - Since $a$ and $b$ are both less than $k + 1$, by the induction hypothesis, both $a$ and $b$ are either prime numbers or products of a finite number of prime numbers.
    - Therefore, $k + 1 = a \cdot b$ must be a product of a finite number of prime numbers.

□

Thus, by the principle of mathematical induction, we conclude that every integer $n \geq 2$ is either a prime number or a product of a finite number of prime numbers.

**Theorem 3.3.** For each positive integer n, there are at least n distinct prime numbers.

*Proof.* We prove by induction on $n$ that for each positive integer $n$, there are at least $n$ distinct prime numbers.

Base Case: For $n = 1$:
The smallest prime number is 2. Thus, there is at least 1 prime number. Therefore, the statement holds for $n = 1$.

Inductive Step:
Assume that for some $k \geq 1$, there are at least $k$ distinct prime numbers. We need to show that there are at least $k + 1$ distinct prime numbers.
Let $p_1, p_2, \ldots, p_k$ be $k$ distinct prime numbers. Consider the product of these primes plus one:

$$P = p_1 p_2 \cdots p_k + 1$$

Now, $P$ is an integer greater than 1. According to the fundamental theorem of arithmetic, $P$ must be divisible by some prime number. Let this prime number be $q$.
Notice that $q$ cannot be any of the primes $p_1, p_2, \ldots, p_k$, because dividing $P$ by any of these primes leaves a remainder of 1:

$$P \equiv 1 \pmod{p_i} \quad \text{for each} \quad i = 1, 2, \ldots, k$$

Thus, $q$ must be a prime number distinct from $p_1, p_2, \ldots, p_k$. This means we have found a new prime number, distinct from the first $k$ primes.
Therefore, there are at least $k + 1$ distinct prime numbers.
By the principle of mathematical induction, the statement is true for all positive integers $n$.

□

**Theorem 3.4.** Suppose a prime number p divides the product bc of integers b and c. Then p divides b, or p divides c.

*Proof.*
- Statement: Suppose a prime number $p$ divides the product $bc$ of integers $b$ and $c$. Then $p$ divides $b$, or $p$ divides $c$.
- Proof: Given:
  - $p$ is a prime number.
  - $p \mid bc$, meaning $p$ divides the product $bc$.

  To Prove:
  - $p \mid b$ or $p \mid c$.

  Proof:
  - Assume $p \nmid b$. We need to show that $p \mid c$.
  - Since $p \nmid b$, $b$ and $p$ are coprime (i.e., $\gcd(b, p) = 1$).
  - By Bézout's Identity, there exist integers $x$ and $y$ such that:
$$bx + py = 1$$
  - Multiply both sides by $c$:
$$bcx + pcy = c$$
  - Since $p \mid bc$, we have $bc = kp$ for some integer $k$. Thus, $bcx = kpx$, so $p \mid bcx$.
  - Also, $p \mid pcy$ because $p \mid p$. Hence, $p \mid (bcx + pcy)$.
  - Therefore, $p \mid c$.

  Conclusion:
  - If $p \nmid b$, then $p \mid c$.
  - This proves that if $p \mid bc$, then $p \mid b$ or $p \mid c$.

**Theorem 3.5.** Suppose a and b are integers greater than 1 with prime factorizations
$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$
where $p_1, p_2, \ldots, p_r$ are distinct prime numbers, and $e_1, e_2, \ldots, e_r$ and $f_1, f_2, \ldots, f_r$ are non-negative integers.
numbers. Then a divides b if and only if for each index i the inequality $e_i \leq f_i$ holds.

Proof:

() If $a$ divides $b$, then $e_i \leq f_i$ for each $i$:
- Assume $a \mid b$. This means there exists an integer $k$ such that $b = ak$. We can write:
$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$
$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$
- Since $a \mid b$, we have:
$$p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} = \left(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\right) k$$
- Rewriting $k$ in terms of prime factors, say:
$$k = p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r}$$
- Substituting $k$ into the equation for $b$:
$$b = \left(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\right) \left(p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r}\right)$$
$$b = p_1^{e_1+g_1} p_2^{e_2+g_2} \cdots p_r^{e_r+g_r}$$

* By comparing exponents, we see that:

$$f_i = e_i + g_i$$

* Since $g_i$ are non-negative integers, it follows that $e_i \leq f_i$ for each $i$.

() If $e_i \leq f_i$ for each $i$, then $a$ divides $b$:

* Assume $e_i \leq f_i$ for each $i$. This means that for each $i$, we can write:

$$f_i = e_i + g_i$$

for some non-negative integers $g_i$.

* Let:

$$k = p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r}$$

* Then we can write:

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} = p_1^{e_1+g_1} p_2^{e_2+g_2} \cdots p_r^{e_r+g_r}$$

$$b = (p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) (p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r})$$

$$b = ak$$

* Therefore, $a \mid b$.

**Theorem 3.6.** Suppose a and b are integers greater than 1 with prime factorizations

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

where the exponents are nonnegative integers and $p_1, p_2, \ldots, p_r$ are distinct prime numbers. For each $i$ between 1 and $r$, let $h_i$ equal the larger of the two exponents $e_i$ and $f_i$. numbers. Then the least common multiple of a and b is given by the formula

$$[a, b] = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$$

*Proof.*
Proof: Let $(a, b)$ denote the least common multiple of $a$ and $b$.

- By definition, the least common multiple $[a, b]$ is the smallest positive integer that is divisible by both $a$ and $b$.
- The prime factorization of $a$ is given by

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

- The prime factorization of $b$ is given by

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}.$$

- For each prime $p_i$, the exponent in the prime factorization of $[a, b]$ must be the largest power of $p_i$ that appears in the factorizations of $a$ and $b$. Hence, we define

$$h_i = \max(e_i, f_i).$$

- Thus, the least common multiple of $a$ and $b$ can be written as

$$[a, b] = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r},$$

where $h_i = \max(e_i, f_i)$ for each $i = 1, 2, \ldots, r$.

Since $h_i \geq e_i$ and $h_i \geq f_i$ for each $i$, it follows that $[a, b]$ is divisible by both $a$ and $b$. Therefore, $[a, b]$ is the least common multiple of $a$ and $b$.

□

**Problem 3.1.** Let $a$ and $b$ be positive integers. Using the expressions for $\gcd(a,b)$ and $\text{lcm}(a,b)$ in terms of the prime factorizations of $a$ and $b$, prove that

$$ab = \gcd(a,b) \times \text{lcm}(a,b).$$

Conclude that

$$\text{lcm}(a,b) = \frac{ab}{\gcd(a,b)}.$$

**Solution 3.1.** * Let $a$ and $b$ have the following prime factorizations:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

where $p_1, p_2, \ldots, p_r$ are distinct prime numbers, and $e_i$, $f_i$ are nonnegative integers for $i = 1, 2, \ldots, r$.

* The greatest common divisor (GCD) of $a$ and $b$ is given by:

$$(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_r^{\min(e_r,f_r)}.$$

* The least common multiple (LCM) of $a$ and $b$ is given by:

$$[a,b] = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_r^{\max(e_r,f_r)}.$$

* To prove the relationship $ab = (a,b) \times [a,b]$:
  · Consider the product $ab$:

$$ab = (p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) \left(p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}\right).$$

  · Using properties of exponents, this can be written as:

$$ab = p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_r^{e_r+f_r}.$$

  · Consider the product $(a,b) \times [a,b]$:

$$(a,b) \times [a,b] = \left(p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_r^{\min(e_r,f_r)}\right) \left(p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_r^{\max(e_r,f_r)}\right).$$

  · Again, using properties of exponents, this can be written as:

$$(a,b) \times [a,b] = p_1^{\min(e_1,f_1)+\max(e_1,f_1)} p_2^{\min(e_2,f_2)+\max(e_2,f_2)} \cdots p_r^{\min(e_r,f_r)+\max(e_r,f_r)}.$$

  · Since $\min(e_i,f_i) + \max(e_i,f_i) = e_i + f_i$ for each $i$, we get:

$$(a,b) \times [a,b] = p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_r^{e_r+f_r}.$$

  · Therefore,

$$ab = (a,b) \times [a,b].$$

* Dividing both sides of the equation $ab = (a,b) \times [a,b]$ by $(a,b)$, we get:

$$[a,b] = \frac{ab}{(a,b)}.$$

– Definition of Min and Max:
  * $\min(e_i,f_i)$ is the smaller of $e_i$ and $f_i$.
  * $\max(e_i,f_i)$ is the larger of $e_i$ and $f_i$.
– **Case Analysis:**
  * Case 1: If $e_i \leq f_i$:
    · $\min(e_i,f_i) = e_i$
    · $\max(e_i,f_i) = f_i$
    · Therefore, $\min(e_i,f_i) + \max(e_i,f_i) = e_i + f_i$.

  - ∗ Case 2: If $e_i > f_i$:
    - · $\min(e_i, f_i) = f_i$
    - · $\max(e_i, f_i) = e_i$
    - · Therefore, $\min(e_i, f_i) + \max(e_i, f_i) = f_i + e_i = e_i + f_i$.
- In both cases, $\min(e_i, f_i) + \max(e_i, f_i)$ equals $e_i + f_i$. This equality always holds because one is always the minimum and the other is always the maximum, but their sum remains the same.

## 4. Definition of a Ring:

A *ring* $R$ is a set equipped with two binary operations, usually denoted as addition $(+)$ and multiplication $(\cdot)$, such that for all elements $a, b, c \in R$, the following properties hold:

- Additive Closure:
  $a + b$ is in $R$.
- Additive Associativity:
  $(a + b) + c = a + (b + c)$.
- Additive Identity:
  There exists an element $0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$.
- Additive Inverses:
  For each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
- Multiplicative Closure:
  $ab$ is in $R$.
- Multiplicative Associativity:
  $(ab)c = a(bc)$.
- Distributivity:
  $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

A ring may or may not have a multiplicative identity element.

**Definition of a Number Ring:**

Let $K$ be a number field, which is a finite extension of the rational numbers $\mathbb{Q}$. The *ring of integers* $\mathcal{O}_K$ of $K$ is defined as the set of all algebraic integers in $K$, which are roots of monic polynomials with integer coefficients.

- **Properties of $\mathcal{O}_K$:**
  - ∗ $\mathcal{O}_K$ is a ring.
  - ∗ $\mathcal{O}_K$ is a Dedekind domain, meaning it is a Noetherian, integrally closed domain, and every nonzero prime ideal in $\mathcal{O}_K$ is maximal.
  - ∗ Examples include $\mathbb{Z}$ (the ring of integers of $\mathbb{Q}$) and other rings of integers of number fields like $\mathbb{Z}[\sqrt{2}]$ for $\mathbb{Q}(\sqrt{2})$.

beginitemize

**Problem 4.1.** Suppose $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$ and its multiplicative inverse is $c + d\sqrt{2}$. Show that:

$$ac + 2bd = 1 \quad \text{and} \quad ad + bc = 0.$$

**Solution 4.1.**

- Let $a + b\sqrt{2}$ be a unit with inverse $c + d\sqrt{2}$.
- By definition of unit, $(a + b\sqrt{2})(c + d\sqrt{2}) = 1$.
- Expanding and equating real and irrational parts:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}.$$

- Equating real and irrational parts gives:

$$ac + 2bd = 1 \quad \text{and} \quad ad + bc = 0.$$

**Problem 4.2.** Using these equations, deduce that $a - b\sqrt{2}$ is also a unit in $\mathbb{Z}[\sqrt{2}]$, and its inverse is $c - d\sqrt{2}$.

**Solution 4.2.**
- From $ac + 2bd = 1$ and $ad + bc = 0$, we can deduce that $(a - b\sqrt{2})(c - d\sqrt{2}) = 1$.
- Thus, $a - b\sqrt{2}$ is a unit with inverse $c - d\sqrt{2}$.

**Problem 4.3.** Continuing with these numbers, show that $(a+b\sqrt{2})(a-b\sqrt{2})(c+d\sqrt{2})(c-d\sqrt{2}) = 1$ and deduce that $a^2 - 2b^2$ must equal 1 or -1.

**Solution 4.3.**
- From the previous deductions, we have:

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = 1 \quad \text{or} \quad a^2 - 2b^2 = -1.$$

- This follows directly from the multiplication of conjugates and using $ac + 2bd = 1$ and $ad + bc = 0$.

**Problem 4.4.** You have proved that if $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$, then $a^2 - 2b^2 = \pm 1$.

**Solution 4.4.**
- As deduced, if $a + b\sqrt{2}$ is a unit, then $a^2 - 2b^2 = \pm 1$.

**Problem 4.5.** Conversely, suppose $a$ and $b$ are integers satisfying either $a^2 - 2b^2 = 1$ or $a^2 - 2b^2 = -1$. Prove that $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. What is its multiplicative inverse?

**Solution 4.5.**
- If $a^2 - 2b^2 = 1$ or $a^2 - 2b^2 = -1$, then $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.
- The multiplicative inverse can be found as $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ or $-\frac{a}{a^2-2b^2} + \frac{b}{a^2-2b^2}\sqrt{2}$, depending on whether $a^2 - 2b^2 = 1$ or $a^2 - 2b^2 = -1$.

**Problem 4.6.** Conclude that the units in $\mathbb{Z}[\sqrt{2}]$ correspond to solutions to the Diophantine equations $x^2 - 2y^2 = 1$ and $x^2 - 2y^2 = -1$.

**Solution 4.6.**
Units in $\mathbb{Z}[\sqrt{2}]$ are precisely the solutions to $x^2 - 2y^2 = 1$ and $x^2 - 2y^2 = -1$.
These correspond to $a + b\sqrt{2}$ where $a^2 - 2b^2 = \pm 1$.

**Problem 4.7.** Observe that $(1, 1)$ is a solution to one of these equations, as is $(3, 2)$. Deduce that $\sqrt{2} + 1$ is a unit, with inverse $\sqrt{2} - 1$, and $3 + 2\sqrt{2}$ is a unit with inverse $3 - 2\sqrt{2}$.

**Solution 4.7.**
$(1, 1)$ and $(3, 2)$ are solutions to $x^2 - 2y^2 = 1$.
Thus, $\sqrt{2}+1$ and $3+2\sqrt{2}$ are units in $\mathbb{Z}[\sqrt{2}]$ with inverses $\sqrt{2}-1$ and $3-2\sqrt{2}$, respectively.
Observe that $3 + 2\sqrt{2}$ is just $(\sqrt{2} + 1)^2$, and the inverse of $3 + 2\sqrt{2}$ is $(\sqrt{2} - 1)^2$. More generally, show that $(\sqrt{2}+1)^n$ is a unit for every positive integer $n$ by describing its inverse. Observe that we get in this way infinitely many units in $\mathbb{Z}[\sqrt{2}]$.

**Problem 4.8.**

**Solution 4.8.**
$3 + 2\sqrt{2} = (\sqrt{2} + 1)^2$.
Its inverse is $(\sqrt{2} - 1)^2$.
More generally, $(\sqrt{2} + 1)^n$ is a unit in $\mathbb{Z}[\sqrt{2}]$ for every positive integer $n$.
Its inverse can be derived similarly using the properties of units.

**Definition 4.1. Definition of Norm**

For an element $\alpha = a + b\sqrt{d}$ in the quadratic field $\mathbb{Q}(\sqrt{d})$, where $a$ and $b$ are rational numbers (or integers if we are considering the ring of integers within $\mathbb{Q}(\sqrt{d})$), the *norm* of $\alpha$ is defined as:

$$N(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

where $\overline{\alpha} = a - b\sqrt{d}$ is the conjugate of $\alpha$.

**Problem 4.9.** Prove that if $a$ is an even integer and $b$ is an integer, the number $a + b\sqrt{2}$ cannot be a unit in $\mathbb{Z}[\sqrt{2}]$. (Is it possible for such a pair $(a, b)$ to satisfy the equation $x^2 - 2y^2 = \pm 1$?) Conclude that there are infinitely many numbers in $\mathbb{Z}[\sqrt{2}]$ that are not units.

**Solution 4.9.** Norm Calculation:

- The norm $N$ of an element $\alpha = a + b\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ is defined as:

$$N(\alpha) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

- An element $\alpha \in \mathbb{Z}[\sqrt{2}]$ is a unit if there exists another element $\beta \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha\beta = 1$. This implies that the norm of a unit must be $\pm 1$.

Proving $a + b\sqrt{2}$ is not a Unit:

- Suppose $a + b\sqrt{2}$ is a unit. Then there exists $c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

- This expands to:

$$ac + 2bd + (ad + bc)\sqrt{2} = 1$$

- For this equality to hold, both the rational and irrational parts must separately equate:

$$ac + 2bd = 1 \quad \text{and} \quad ad + bc = 0$$

Considering $a$ is Even:

- Let $a = 2k$, where $k$ is an integer.
- Substituting into the norm:

$$N(2k + b\sqrt{2}) = (2k)^2 - 2b^2 = 4k^2 - 2b^2$$

- To be a unit, $N(2k + b\sqrt{2})$ must equal $\pm 1$.
- However, $4k^2 - 2b^2$ cannot yield $\pm 1$ when $k$ and $b$ are integers,

Conclusion:

- Since $a + b\sqrt{2}$ with $a$ even cannot satisfy the conditions to be a unit, and there are infinitely many even integers $a$, it follows that there are infinitely many elements in $\mathbb{Z}[\sqrt{2}]$ that are not units.

Therefore, $a + b\sqrt{2}$ cannot be a unit in $\mathbb{Z}[\sqrt{2}]$ for any even integer $a$ and integer $b$.

**Pell Equation: Theory**

- Definition:
  - The Pell equation is a type of Diophantine equation of the form:

$$x^2 - Dy^2 = 1$$

or sometimes:

$$x^2 - Dy^2 = -1$$

where $D$ is a nonsquare positive integer (for the first form) or any integer (for the second form), and $x$ and $y$ are integers.

- **Name and Historical Context:**

    - The name "Pell equation" comes from the English mathematician John Pell, although historically it was known much earlier and was studied by Indian mathematicians.
  - **Solutions and Properties:**
    - **Fundamental Solution:** The Pell equation always has at least one solution $(x_1, y_1)$ in integers, known as the fundamental solution.
    - **Generating More Solutions:** If $(x_1, y_1)$ is a solution to $x^2 - Dy^2 = 1$, then all other solutions can be generated using powers of a specific fundamental solution.
    - Infinitely Many Solutions: The equation has infinitely many integer solutions if $D$ is not a perfect square and the fundamental solution exists.
  - Special Cases:
    - If $D = 1$, the equation reduces to $x^2 - y^2 = 1$, which has solutions like $(x, y) = (1, 0), (2, 1), (3, 2), \ldots$.
    - If $D = -1$, the equation becomes $x^2 + y^2 = 1$, which has solutions $(x, y) = (\pm 1, 0), (0, \pm 1)$.
  - Applications
  - Pell equations arise in various areas of mathematics and have connections to number theory, algebraic number theory, and cryptography. They are also related to continued fractions and provide solutions to problems such as finding integer solutions to certain quadratic forms.
  - Summary:
    - In summary, the Pell equation $x^2 - Dy^2 = 1$ or $x^2 - Dy^2 = -1$ is a fundamental type of Diophantine equation that has been studied extensively due to its rich mathematical properties and applications.

**Definition 4.2. Gaussian integer** :A Gaussian integer is a complex number of the form a+bi where both a and b are integers. We often denote the set of Gaussian integers by Z[i] .

**Problem 4.10.** Show that if $r$ is an even integer, then $r^2$ is divisible by 4, or equivalently, $r^2$ is congruent to 0 modulo 4.

**Solution 4.10.**
An even integer $r$ can be written as $r = 2k$ for some integer $k$.
Squaring $r$, we get $r^2 = (2k)^2 = 4k^2$.
Since $4k^2$ is clearly divisible by 4, we have $r^2 \equiv 0 \pmod 4$.

**Problem 4.11.** Show that if $r$ is an odd integer, then $r^2$ is congruent to 1 modulo 4.

**Solution 4.11.**
An odd integer $r$ can be written as $r = 2k + 1$ for some integer $k$.
Squaring $r$, we get $r^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
Since $4(k^2 + k)$ is divisible by 4, we have $r^2 \equiv 1 \pmod 4$.

**Problem 4.12.** Deduce that for every pair of integers $a$ and $b$, $a^2 + b^2$ is congruent to 0, 1, or 2 modulo 4 but never congruent to 3 modulo 4.

**Solution 4.12.**

From Problems 1 and 2, the possible values of $r^2$ modulo 4 are:
If $r$ is even: $r^2 \equiv 0 \pmod 4$
If $r$ is odd: $r^2 \equiv 1 \pmod 4$

- Consider all combinations of $a^2$ and $b^2$ modulo 4:
- $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 0 \pmod 4$: $a^2 + b^2 \equiv 0 + 0 = 0 \pmod 4$
- $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 1 \pmod 4$: $a^2 + b^2 \equiv 0 + 1 = 1 \pmod 4$
- $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 0 \pmod 4$: $a^2 + b^2 \equiv 1 + 0 = 1 \pmod 4$
- $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$: $a^2 + b^2 \equiv 1 + 1 = 2 \pmod 4$

- There is no combination where $a^2 + b^2$ is congruent to 3 modulo 4.

**Problem 4.13.** Conclude that $x^2 + y^2 = n$ has no integer solutions for $n \equiv 3 \pmod 4$.

**Solution 4.13.**
Given $n \equiv 3 \pmod 4$:
Suppose $x^2 + y^2 = n$.
From Problem 3, we know $x^2 + y^2$ can be 0, 1, or 2 modulo 4, but not 3.
Thus, it is impossible for $x^2 + y^2 \equiv 3 \pmod 4$.
Therefore, if $n \equiv 3 \pmod 4$, there are no integer solutions to the equation $x^2 + y^2 = n$.

**Example 4.1.** Consider $n = 7$. Since $7 \equiv 3 \pmod 4$, the equation $x^2 + y^2 = 7$ has no integer solutions.

**Solution 4.14.**
Check possible pairs:
$x = 0$ and $y = \pm\sqrt{7}$ (not integers)
$x = \pm 1$ and $y = \pm\sqrt{6}$ (not integers)
$x = \pm 2$ and $y = \pm\sqrt{3}$ (not integers)
$x = \pm 3$ and $y = \pm\sqrt{-2}$ (not real numbers)
$x = \pm\sqrt{7}$ and $y = 0$ (not integers)
Thus, there are no integer solutions to $x^2 + y^2 = 7$, confirming the result.

**Theorem 4.1** (Fermat's)**.** Suppose $p$ is an odd prime number.
(1) If $p \equiv 1 \pmod 4$, then the equation $x^2 + y^2 = p$ has an integer solution.
(2) If $p \equiv 3 \pmod 4$, then the equation $x^2 + y^2 = p$ has no solution in integers.

**Example 4.2.**
- Suppose $p = 5$.
  - Since $5 \equiv 1 \pmod 4$, the equation $x^2 + y^2 = 5$ has an integer solution. For example, $(x, y) = (2, 1)$ satisfies $2^2 + 1^2 = 4 + 1 = 5$.
- Suppose $p = 7$.
  - Since $7 \equiv 3 \pmod 4$, the equation $x^2 + y^2 = 7$ has no integer solutions. For any integers $x$ and $y$, $x^2 + y^2$ cannot equal 7. Checking all possible values of $x$ and $y$, none satisfy the equation.

**Problem 4.14.** Let us look further at factorization in the ring $\mathbb{Z}[i]$ of Gaussian integers.
(1) Prove that if a pair of integers $a$ and $b$ is a solution to the equation $x^2 + y^2 = n$, then $n$ factors in $\mathbb{Z}[i]$ as the product $(a + bi)(a - bi)$.
(2) Describe a nontrivial factorization of 2 in $\mathbb{Z}[i]$.

**Solution 4.15.** Factorization in $\mathbb{Z}[i]$:
(1) Let $z = x + yi \in \mathbb{Z}[i]$. Then $\overline{z} = x - yi$ is its conjugate in $\mathbb{Z}[i]$.

Consider

$$N(z) = z\overline{z} = (x + yi)(x - yi) = x^2 + y^2.$$

Given $x^2 + y^2 = n$, we have $N(z) = n$. Therefore,

$$n = z\overline{z}.$$

Thus, $n$ factors in $\mathbb{Z}[i]$ as $(x + yi)(x - yi)$, which is $(a + bi)(a - bi)$ where $a = x$ and $b = y$.

**Solution 4.16.** In $\mathbb{Z}[i]$, the ring of Gaussian integers, a nontrivial factorization of 2 can be expressed using the elements of $\mathbb{Z}[i]$. Gaussian integers are of the form $a + bi$, where $a$ and $b$ are integers, and $i$ is the imaginary unit with $i^2 = -1$.
To find a nontrivial factorization of 2, we use the fact that 2 can be expressed as the product of two Gaussian integers other than $2 \cdot 1$ or $-2 \cdot -1$. One such factorization is:

$$2 = (1 + i)(1 - i).$$

Here's how this factorization works:

- Calculate $(1 + i)(1 - i)$:

$$(1 + i)(1 - i) = 1 - i^2 = 1 - (-1) = 1 + 1 = 2.$$

- Therefore, 2 factors into $(1 + i)(1 - i)$ in $\mathbb{Z}[i]$.
- This factorization is nontrivial because both $1 + i$ and $1 - i$ are not units (the units in $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$).

## 5. Unit

**Definition 5.1. Unit** In number theory, a **unit** is an element of a ring that has a multiplicative inverse. Formally, in a ring $R$, an element $u \in R$ is called a unit if there exists an element $v \in R$ such that:

$$u \cdot v = v \cdot u = 1$$

where 1 is the multiplicative identity in the ring $R$. The element $v$ is called the multiplicative inverse of $u$. In other words, a unit is an element that can be "undone" by multiplication, meaning you can multiply it by another specific element to get 1.

**Definition 5.2. Modular arithmetic**
Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value, called the modulus. It's a fundamental concept in number theory with applications in computer science, cryptography, and many other fields

**Definition 5.3. Units in Modular Arithmetic Rings**
In the ring of integers modulo $n$, denoted $\mathbb{Z}/n\mathbb{Z}$, an element $a$ is called a unit if there exists another element $b$ in the same ring such that:

$$a \times b \equiv 1 \pmod{n}$$

Here, $b$ is referred to as the multiplicative inverse of $a$. This means that $a$ and $b$ multiply together to give 1 when considered modulo $n$.

**Problem 5.1.** Let us take a look at the rings $\mathbb{Z}_m$ for small $m$.
(1) Suppose $m = 2$.

(a) Write the multiplication table for $\mathbb{Z}_2$.

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

(b) Using the multiplication table, check that 1 is a multiplicative identity for $\mathbb{Z}_2$.
- $1 \cdot 0 = 0$
- $1 \cdot 1 = 1$

Therefore, 1 is the multiplicative identity in $\mathbb{Z}_2$.

(c) Which numbers in $\mathbb{Z}_2$ are units? What are their multiplicative inverses? Is $\mathbb{Z}_2$ a field?
- The units in $\mathbb{Z}_2$ are the elements that have multiplicative inverses.
- From the table, 1 is its own inverse ($1 \cdot 1 = 1$).
- So, the only unit in $\mathbb{Z}_2$ is 1, and 1's multiplicative inverse is itself.
- Since every non-zero element has a multiplicative inverse, $\mathbb{Z}_2$ is a field.

(2) Suppose $m = 3$.

(a) Write the multiplication table for $\mathbb{Z}_3$.

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

(b) Using the multiplication table, check that 1 is a multiplicative identity for $\mathbb{Z}_3$.
- $1 \cdot 0 = 0$
- $1 \cdot 1 = 1$
- $1 \cdot 2 = 2$

Therefore, 1 is the multiplicative identity in $\mathbb{Z}_3$.

(c) Which numbers in $\mathbb{Z}_3$ are units? What are their multiplicative inverses? Is $\mathbb{Z}_3$ a field?
- The multiplication table for $\mathbb{Z}_3$ is:

| * | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

**Checking 1 as the multiplicative identity:**

$$1 * 0 = 0$$

$$1 * 1 = 1$$

$$1 * 2 = 2$$

Therefore, 1 is the multiplicative identity in $\mathbb{Z}_3$.
Units in $\mathbb{Z}_3$ and their inverses:
1 is its own inverse ($1 * 1 = 1$).
2 is its own inverse ($2 * 2 = 4\ a \equiv 1 \mod 3$).
So, the units in $\mathbb{Z}_3$ are 1 and 2, with inverses 1 and 2 respectively.
Since every non-zero element (1 and 2) has a multiplicative inverse, $\mathbb{Z}_3$ is a field.

**When $\mathbb{Z}_n$ will be a field?**
In number theory, $\mathbb{Z}_n$ (also denoted as $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$) will form a field if and only if $n$ is a prime number.
Here's why $\mathbb{Z}_n$ is a field when $n$ is a prime number:

(1) Multiplicative Inverses: In $\mathbb{Z}_n$, every non-zero element $a$ has a unique multiplicative inverse $b$ such that $ab \equiv 1 \mod n$. This means for every $a \in \mathbb{Z}_n \setminus \{0\}$, there exists a $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \mod n$.

(2) No Zero Divisors: In $\mathbb{Z}_n$, if $ab \equiv 0 \mod n$, then either $a \equiv 0 \mod n$ or $b \equiv 0 \mod n$. This property ensures that $\mathbb{Z}_n$ has no zero divisors, which is a necessary condition for being a field.

(3) Commutativity, Associativity, and Distributivity: $\mathbb{Z}_n$ inherits these properties from $\mathbb{Z}$, ensuring that addition and multiplication are well-defined and satisfy the field axioms.

Therefore, $\mathbb{Z}_n$ forms a field if and only if $n$ is a prime number. For composite $n$ (non-prime), $\mathbb{Z}_n$ will not satisfy all the field properties, particularly the existence of multiplicative inverses for all non-zero elements.

**Problem 5.2.** For each of the following equations, find a solution or explain why there is no solution:
* **(1)** $3x = 7$ in $\mathbb{Z}_{11}$

**Solution 5.1.** For each of the following equations will check if there is solution or not if not will give reason why not
**Equation:** $3x \equiv 7 \pmod{11}$
The Extended Euclidean Algorithm helps find solutions to the equation $a \cdot x + m \cdot y = \gcd(a, m)$. Since 3 and 11 are coprime ($\gcd(3, 11) = 1$), there exists an integer $x$ such that:

$$3 \cdot x + 11 \cdot y = 1 - - > (1)$$

Apply the Extended Euclidean Algorithm:
* Step 1: Apply the Euclidean Algorithm to find the gcd:

$$11 = 3 \cdot 3 + 2,$$
$$3 = 2 \cdot 1 + 1,$$
$$2 = 1 \cdot 2 + 0.$$

The gcd is 1, as expected.
* Step 2: lets do inverse of that 1 as a combination of 3 and 11:

$$1 = 3 - 2 \cdot 1,$$
$$1 = 3 - (11 - 3 \cdot 3),$$
$$1 = 3 - 11 + 3 \cdot 3,$$
$$1 = 3 \cdot 4 - 11.$$

So, $1 = 3 \cdot 4 - 11$, on comparing with equation first we can see that $x = 4$.
* Verify the result:

$$3 \cdot 4 = 12 \equiv 1 \pmod{11}$$

Thus, the multiplicative inverse of 3 in $\mathbb{Z}_{11}$ is 4.
$3x \equiv 7 \pmod{11}$ multiply by inverse both sides here
then will get $4 * 3x \equiv 7 * 4 \pmod{11}$
$x \equiv 28 \pmod{11}$
**Reduce 28 modulo 11**

$$28 \equiv 28 - 2 \cdot 11$$

$$28 \equiv 28 - 22$$

$$28 \equiv 6 \pmod{11}$$

The solution to the equation is:

$$x \equiv 6 \pmod{11}$$

**Proposition 5.1.** Suppose a is a unit in a ring R, and e is an arbitrary element of R. Then the equation ax = e is solvable in R, with the solution

$$x = a^{-1}e$$

**Proposition 5.2.** Suppose a is a unit in a ring R, and suppose that b and c are also in R. If ab = ac, then b = c.

**Problem 5.3. Suppose u is a unit in a ring R**
( 1) Recall that units can be canceled: If $r$ and $s$ are elements of $R$ satisfying $ur = us$, then $r = s$. Observe that the logically equivalent contrapositive takes the following form: If $r$ and $s$ are elements of $R$ satisfying $r \neq s$, then $ur \neq us$.

**Solution 5.2.** First, recall the cancellation property of units in a ring $R$. If $u$ is a unit in $R$, it means $u$ has a multiplicative inverse $u^{-1}$ such that $uu^{-1} = u^{-1}u = 1$. The property states:
**Direct statement:** If $ur = us$, then $r = s$ for any $r, s \in R$.

**Contrapositive:** If $r \neq s$, then $ur \neq us$.

This is due to the fact that if $ur = us$, multiplying both sides by $u^{-1}$ yields $r = s$. Conversely, if $r \neq s$, then multiplying both sides of $ur = us$ by $u^{-1}$ would give

$$r = s$$

which will lead to contradiction as in question it is given that r $\neq s, so$
$ur \neq us$.

**Problem 5.4.** Suppose that $R$ has only finitely many elements, and that $r_1, \ldots, r_t$ is a complete list of them, with no repetitions. Deduce that $ur_1, \ldots, ur_t$ is also a complete list of the elements of $R$, with no repetitions.

**Solution 5.3.** Now, suppose $R$ is a finite ring with elements $r_1, r_2, \ldots, r_t$. Since $u$ is a unit, it should shuffle the elements of $R$ when multiplied:
**Claim:** The set $\{ur_1, ur_2, \ldots, ur_t\}$ is a complete list of the elements of $R$ with no repetitions.
**Proof:**
**Completeness:** Since $u$ is a unit, multiplying any element $r$ of $R$ by $u$ results in another element of $R$. Thus, $ur_i \in R$ for all $i$.
**No Repetitions:** Suppose $ur_i = ur_j$. Using the cancellation property of units, we get $r_i = r_j$. Since $r_1, r_2, \ldots, r_t$ are distinct, it follows that $ur_i$ are also distinct.

Therefore, $\{ur_1, ur_2, \ldots, ur_t\}$ is a complete list of the elements of $R$ with no repetitions, meaning multiplication by $u$ indeed shuffles the elements of $R$.

**Problem 5.5.** Give an example to show that, for a nonzero element $a$ in a ring $R$, the set $\{ar_1, ar_2, \ldots, ar_t\}$ may not be a complete list of elements of $R$. That is, some elements may be repeated in this list, and some may be omitted. You need only produce a single ring $R$ and a single nonzero element $a$ of $R$ in order to demonstrate this.

**Solution 5.4. Example Showing Non-Unit Element Does Not Shuffle Elements**
Consider the ring $R = \mathbb{Z}/6\mathbb{Z}$, which consists of integers modulo 6: $R = \{0, 1, 2, 3, 4, 5\}$.
Let $a = 2$, which is a nonzero element of $R$.
Now, calculate $ar_i$ for each $r_i \in R$:

$$\begin{aligned} 2 \times 0 &= 0, \\ 2 \times 1 &= 2, \\ 2 \times 2 &= 4, \\ 2 \times 3 &= 6 \equiv 0 \pmod 6, \\ 2 \times 4 &= 8 \equiv 2 \pmod 6, \\ 2 \times 5 &= 10 \equiv 4 \pmod 6. \end{aligned}$$

The results are $\{0, 2, 4, 0, 2, 4\}$. Notice that the elements $ar_i$ are not a complete list of all elements of $R$, which are $\{0, 1, 2, 3, 4, 5\}$. we can see that

* The element 1 from $R$ is missing in the set $\{0, 2, 4\}$.
* The elements $0, 2$, and $4$ appear multiple times hence it also violate non repeating criteria.

Therefore, multiplication by the arbitrary nonzero element $a = 2$ in the ring $R = \mathbb{Z}/6\mathbb{Z}$ does not shuffle all elements of $R$ into a complete list without repetitions. Instead, some elements are repeated, and some are not there in set . This example demonstrates that not all nonzero elements in a ring necessarily permute the elements of the ring when multiplied.

**Problem 5.6. Suppose m ¿ 1 is an integer and a is an integer relatively prime to m.**
1. Recall that since $(a, m) = 1$, it follows that $[a]$ is a unit in $\mathbb{Z}_m$.
Deduce that multiplication of all the elements of $\mathbb{Z}_m$ by $[a]$ produces a shuffle of $\mathbb{Z}_m$.

**Solution 5.5. Multiplication by a Unit in $\mathbb{Z}_m$:**
Since $(a, m) = 1$, we know that $a$ and $m$ are relatively prime, which implies that $a$ has a multiplicative inverse modulo $m$. In other words, there exists an integer $b$ such that:

$$ab \equiv 1 \pmod m$$

This means that $[a]$ is a unit in $\mathbb{Z}_m$. When we multiply all elements of $\mathbb{Z}_m$ (which are $[0], [1], [2], \ldots, [m-1]$) by $[a]$, we get:

$$[0] \cdot [a], [1] \cdot [a], [2] \cdot [a], \ldots, [m-1] \cdot [a]$$

Because $[a]$ is a unit, multiplication by $[a]$ is a bijection (a one-to-one and onto map) on $\mathbb{Z}_m$. This bijection means that multiplying by $[a]$ effectively permutes or "shuffles" the elements of $\mathbb{Z}_m$.

**Problem 5.7.** Conclude that the set [0], [a], [2a], [3a], . . . , [(m 1)a] is a complete list of the m elements of $Z_m$

**Solution 5.6.** Since the multiplication by $[a]$ permutes the elements of $\mathbb{Z}_m$, it follows that the set:

$$[0], [a], [2a], [3a], \ldots, [(m-1)a]$$

is a complete list of the $m$ elements of $\mathbb{Z}_m$. This set contains exactly $m$ elements, which correspond to all possible equivalence classes modulo $m$.

**Problem 5.8.** Reinterpret this, in terms of congruences, to say that every integer is congruent, modulo m, to exactly one of the integers 0, a, 2a, 3a, . . . , (m 1)a.

**Solution 5.7.** We can see the above result in terms of congruences. Specifically, for any integer $k$, there exists a unique integer $j$ in the range $0, 1, 2, \ldots, m-1$ such that:

$$k \equiv ja \pmod{m}$$

This means that every integer $k$ is congruent modulo $m$ to exactly one of the integers in the set:

$$0, a, 2a, 3a, \ldots, (m-1)a$$

**Problem 5.9.** Conclude that we have shown again that 0, a, 2a, 3a, . . . , (m 1)a is a complete set of distinct congruence class representatives modulo m. Thus, if (a,m) = 1, then multiplication by [a] shuffles congruence classes modulo m.

**Solution 5.8.** Consequently, the set:

$$0, a, 2a, 3a, \ldots, (m-1)a$$

is a complete set of distinct congruence class representatives modulo $m$. Each of these representatives is unique modulo $m$, and together they cover all possible congruence classes.
Thus, if $(a, m) = 1$, then multiplication by $[a]$ shuffles the congruence classes modulo $m$. This shows that multiplying by $[a]$ permutes the elements of $\mathbb{Z}_m$ such that each element in $\mathbb{Z}_m$ is represented uniquely in the form $ja \pmod{m}$ for $j \in \{0, 1, 2, \ldots, m-1\}$.

**Roots of Unity**
An $n$-th root of unity is any complex number $z$ such that:

$$z^n = 1$$

for some positive integer $n$.

* **Properties**
  **Existence**: There are exactly $n$ distinct $n$-th roots of unity. **Form**: The $n$-th roots of unity can be expressed in the form:

$$e^{2\pi ik/n}$$

  where $k = 0, 1, 2, \ldots, n-1$. These are complex numbers lying on the unit circle in the complex plane, equally spaced.

* **Cyclotomic Polynomial**
  The $n$-th roots of unity are the roots of the polynomial:
  $$x^n - 1 = 0$$
  This can be factored as:
  $$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$
  The polynomial $x^{n-1}+x^{n-2}+\cdots+x+1$ is called the $n$-th cyclotomic polynomial when $n$ is a prime number.
* **Primitive Roots of Unity**
  A primitive $n$-th root of unity is an $n$-th root of unity that generates all $n$-th roots of unity when raised to integer powers. Specifically, $\zeta$ is a primitive $n$-th root of unity if:
  $$\zeta^k \neq 1$$
  for $0 < k < n$.

**Problem 5.10. Verify the following statements**
1. The two numbers 1 and $-1$ are second roots of unity. They can be written as $\cos 0 + i \sin 0$ and $\cos \pi + i \sin \pi$.

2. The two complex numbers $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ are third roots of unity, as is 1. These three numbers can be written as $\cos \frac{2\pi k}{3} + i \sin \frac{2\pi k}{3}$ for $k$ equal to $0, 1$, and 2.

3. The four complex numbers $\pm 1$ and $\pm i$ are fourth roots of unity. These four numbers can be written as $\cos \frac{2\pi k}{4} + i \sin \frac{2\pi k}{4}$ for $k$ equal to $0, 1, 2$, and 3.

4. The two complex numbers $\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ are sixth roots of unity, as are $\pm 1$ and $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. These six numbers can be written as $\cos \frac{2\pi k}{6} + i \sin \frac{2\pi k}{6}$ for $k$ equal to $0, 1, 2, 3, 4$, and 5.

**Solution 5.9. Verification of Statements**
* **1. Second Roots of Unity**
  The second roots of unity are solutions to the equation:
  $$z^2 = 1$$
  The solutions are $z = 1$ and $z = -1$. These can be expressed using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$:
  · For $z = 1$:
  $$1 = e^{i \cdot 0} = \cos 0 + i \sin 0$$
  · For $z = -1$:
  $$-1 = e^{i\pi} = \cos \pi + i \sin \pi$$
  So, the statement is verified.
* **2. Third Roots of Unity**
  The third roots of unity are solutions to the equation:
  $$z^3 = 1$$
  The solutions are $z = 1$ and:
  $$z = e^{2\pi i/3} = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$$

$$z = e^{4\pi i/3} = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$$

We can check the explicit forms:

· For $z = e^{2\pi i/3}$:

$$\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

· For $z = e^{4\pi i/3}$:

$$\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

So, the statement is verified.

∗ **3. Fourth Roots of Unity**

The fourth roots of unity are solutions to the equation:

$$z^4 = 1$$

The solutions are:

$$z = e^{2\pi ik/4}$$

for $k = 0, 1, 2, 3$. Explicitly:

· For $k = 0$:

$$e^{2\pi i\cdot 0/4} = 1 = \cos 0 + i\sin 0$$

· For $k = 1$:

$$e^{2\pi i\cdot 1/4} = i = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$$

· For $k = 2$:

$$e^{2\pi i\cdot 2/4} = -1 = \cos\pi + i\sin\pi$$

· For $k = 3$:

$$e^{2\pi i\cdot 3/4} = -i = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}$$

So, the statement is verified.

∗ **4. Sixth Roots of Unity**

The sixth roots of unity are solutions to the equation:

$$z^6 = 1$$

The solutions are:

$$z = e^{2\pi ik/6}$$

for $k = 0, 1, 2, 3, 4, 5$. Explicitly:

· For $k = 0$:

$$e^{2\pi i\cdot 0/6} = 1 = \cos 0 + i\sin 0$$

· For $k = 1$:

$$e^{2\pi i\cdot 1/6} = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$$

· For $k = 2$:

$$e^{2\pi i\cdot 2/6} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$$

· For $k = 3$:

$$e^{2\pi i\cdot 3/6} = -1 = \cos\pi + i\sin\pi$$

· For $k = 4$:

$$e^{2\pi i \cdot 4/6} = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$$

· For $k = 5$:

$$e^{2\pi i \cdot 5/6} = \frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}$$

So, the statement is verified.

**Proposition 5.3.** Let $R$ be a ring with multiplicative identity 1.

(1) Suppose $u$ and $v$ are units in $R$. Then $uv$ is a unit too.
(2) More generally, if $u_1, \ldots, u_t$ are units in $R$, then the product $u_1 u_2 \cdots u_t$ is a unit.
(3) In particular, if $u$ is a unit and $t$ is a positive integer, then $u^t$ is a unit.
(4) Suppose $R$ has only finitely many units; say, $R$ has $t$ units. Then every unit $u$ in $R$ satisfies $u^n = 1$ for some integer $n$ less than or equal to $t$.

**Theorem 5.1.** Suppose $R$ is a ring with only finitely many units. Then there is a positive integer $e$ such that every unit $u$ in $R$ satisfies $u^e = 1$. In particular, for an integer $m > 1$, there is a positive integer $e$ such that every unit $u$ in $\mathbb{Z}_m$ satisfies $u^e = 1$. Equivalently, there is a positive integer $e$ such that every integer $a$ relatively prime to $m$ satisfies the congruence

$$a^e \equiv 1 \pmod{m}$$

*Proof.* **Ring with Finite Units:** Let $R$ be a ring with finitely many units. The set of units in $R$ forms a group under multiplication, denoted $R^*$.

**Finite Group of Units:** Since $R$ has finitely many units, $R^*$ is a finite group. Suppose $R^*$ has order $t$.

**Order of a Finite Group:** By Lagrange's theorem, the order of any element $u$ in $R^*$ divides the order of the group. Hence, for each unit $u$ in $R$, there exists an integer $d$ such that

$$d \mid t \quad \text{and} \quad u^d = 1.$$

**Exponent $e$:** Since $R^*$ is finite, let $e = t$. Then, for any unit $u$ in $R$,

$$u^e = u^t = 1,$$

since the order of any element divides the order of the group.
**Application to $\mathbb{Z}_m$:** For $R = \mathbb{Z}_m$, the ring of integers modulo $m$, the units are the integers that are relatively prime to $m$. The group of units in $\mathbb{Z}_m$ is denoted by $(\mathbb{Z}_m)^*$ and consists of all integers $a$ such that $\gcd(a, m) = 1$. Since $(\mathbb{Z}_m)^*$ is a finite group, there exists a positive integer $e$ such that for every unit $u$ in $\mathbb{Z}_m$,

$$u^e = 1.$$

**Equivalence for Relatively Prime Integers:** Every integer $a$ that is relatively prime to $m$ is a unit in $\mathbb{Z}_m$. Therefore, there exists a positive integer $e$ such that

$$a^e \equiv 1 \pmod{m}$$

for every integer $a$ that is relatively prime to $m$.
This completes the proof

□

**Definition 5.4. Characterization of Units in $\mathbf{z}_m$**

An element $[a]$ in $\mathbb{Z}_m$ is a unit if and only if $a$ is relatively prime to $m$, which means $\gcd(a, m) = 1$. This is because if $a$ and $m$ are relatively prime, the integer $a$ has a multiplicative inverse modulo $m$ according to the properties of the greatest common divisor and Bezout's identity.

**Example**

Let's consider $\mathbb{Z}_{12}$ with $m = 12$:
The elements of $\mathbb{Z}_{12}$ are $[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]$.
To find the units in $\mathbb{Z}_{12}$, we identify the elements that have a multiplicative inverse. These elements are those integers between 0 and 11 that are relatively prime to 12:

$$\begin{aligned}
\gcd(1, 12) = 1 &\implies 1 \text{ is a unit.} \\
\gcd(2, 12) = 2 &\implies 2 \text{ is not a unit.} \\
\gcd(3, 12) = 3 &\implies 3 \text{ is not a unit.} \\
\gcd(4, 12) = 4 &\implies 4 \text{ is not a unit.} \\
\gcd(5, 12) = 1 &\implies 5 \text{ is a unit.} \\
\gcd(6, 12) = 6 &\implies 6 \text{ is not a unit.} \\
\gcd(7, 12) = 1 &\implies 7 \text{ is a unit.} \\
\gcd(8, 12) = 4 &\implies 8 \text{ is not a unit.} \\
\gcd(9, 12) = 3 &\implies 9 \text{ is not a unit.} \\
\gcd(10, 12) = 2 &\implies 10 \text{ is not a unit.} \\
\gcd(11, 12) = 1 &\implies 11 \text{ is a unit.}
\end{aligned}$$

Thus, the units in $\mathbb{Z}_{12}$ are $[1], [5], [7]$, and $[11]$.

**Problem 5.11.** For each of the values of $m$ from 2 to 13, answer the following questions:

(1) What are the units in $\mathbb{Z}_m$?
(2) What is the order of each unit $u$ in $\mathbb{Z}_m$? In other words, for each unit $u$, what is the smallest positive integer $f$ such that $u^f \equiv 1 \pmod{m}$?
(3) What is the smallest integer $e$ such that every unit $u$ of $\mathbb{Z}_m$ satisfies $u^e \equiv 1 \pmod{m}$?
(4) Let $\phi(m)$ stand for the number of units in $\mathbb{Z}_m$. Does every unit $u$ in $\mathbb{Z}_m$ satisfy $u^{\phi(m)} \equiv 1 \pmod{m}$? In particular, for prime values of $m$ in the range from 2 to 13, does every unit $u$ in $\mathbb{Z}_m$ satisfy $u^{m-1} \equiv 1 \pmod{m}$?

**Solution 5.10.** $*$ **For $m = 2$:**
Units in $\mathbb{Z}_2$: [1] Order of each unit:[1] has order 1.

Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 1$. $\varphi(2) = 1$. Does every unit $u$ satisfy $u^{\varphi(2)} = 1$? Yes, since $u^1 = 1$.

∗ **For $m = 3$:**
(1) Units in $\mathbb{Z}_3$: $[1], [2]$
(2) Order of each unit:
  · $[1]$ has order 1.
  · $[2]$ has order 2.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 2$.
(4) $\varphi(3) = 2$. Does every unit $u$ satisfy $u^{\varphi(3)} = 1$? Yes, since $u^2 = 1$.

∗ **For $m = 4$:**
(1) Units in $\mathbb{Z}_4$: $[1], [3]$
(2) Order of each unit:
  · $[1]$ has order 1.
  · $[3]$ has order 2.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 2$.
(4) $\varphi(4) = 2$. Does every unit $u$ satisfy $u^{\varphi(4)} = 1$? Yes, since $u^2 = 1$.

∗ **For $m = 5$:**
(1) Units in $\mathbb{Z}_5$: $[1], [2], [3], [4]$
(2) Order of each unit:
  · $[1]$ has order 1.
  · $[2], [3], [4]$ each has order 4.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 4$.
(4) $\varphi(5) = 4$. Does every unit $u$ satisfy $u^{\varphi(5)} = 1$? Yes, since $u^4 = 1$.

∗ **For $m = 6$:**
(1) Units in $\mathbb{Z}_6$: $[1], [5]$
(2) Order of each unit:
  · $[1], [5]$ each has order 2.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 2$.
(4) $\varphi(6) = 2$. Does every unit $u$ satisfy $u^{\varphi(6)} = 1$? Yes, since $u^2 = 1$.

∗ **For $m = 7$:**
(1) Units in $\mathbb{Z}_7$: $[1], [2], [3], [4], [5], [6]$
(2) Order of each unit:
  · $[1]$ has order 1.
  · $[2], [3], [4], [5], [6]$ each has order 6.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 6$.
(4) $\varphi(7) = 6$. Does every unit $u$ satisfy $u^{\varphi(7)} = 1$? Yes, since $u^6 = 1$.

∗ **For $m = 8$:**
(1) Units in $\mathbb{Z}_8$: $[1], [3], [5], [7]$
(2) Order of each unit:
  · $[1], [3], [5], [7]$ each has order 2.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 2$.

(4) $\varphi(8) = 4$. Does every unit $u$ satisfy $u^{\varphi(8)} = 1$? Yes, since $u^2 = 1$.

∗ **For $m = 9$:**
(1) Units in $\mathbb{Z}_9$: $[1], [2], [4], [5], [7], [8]$
(2) Order of each unit:
· $[1], [2], [4], [5], [7], [8]$ each has order 6.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 6$.
(4) $\varphi(9) = 6$. Does every unit $u$ satisfy $u^{\varphi(9)} = 1$? Yes, since $u^6 = 1$.

∗ **For $m = 10$:**
(1) Units in $\mathbb{Z}_{10}$: $[1], [3], [7], [9]$
(2) Order of each unit:
· $[1], [3], [7], [9]$ each has order 4.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 4$.
(4) $\varphi(10) = 4$. Does every unit $u$ satisfy $u^{\varphi(10)} = 1$? Yes, since $u^4 = 1$.

∗ **For $m = 11$:**
(1) Units in $\mathbb{Z}_{11}$: $[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]$
(2) Order of each unit:
· $[1]$ has order 1.
· $[2], [3], [4], [5], [6], [7], [8], [9], [10]$ each has order 10.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 10$.
(4) $\varphi(11) = 10$. Does every unit $u$ satisfy $u^{\varphi(11)} = 1$? Yes, since $u^{10} = 1$.

∗ **For $m = 12$:**
(1) Units in $\mathbb{Z}_{12}$: $[1], [5], [7], [11]$
(2) Order of each unit:
· $[1], [5], [7], [11]$ each has order 2.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 2$.
(4) $\varphi(12) = 4$. Does every unit $u$ satisfy $u^{\varphi(12)} = 1$? Yes, since $u^2 = 1$.

∗ **For $m = 13$:**
(1) Units in $\mathbb{Z}_{13}$: $[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]$
(2) Order of each unit:
· $[1]$ has order 1.
· $[2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]$ each has order 12.
(3) Smallest $e$ such that $u^e = 1$ for every unit $u$: $e = 12$.
(4) $\varphi(13) = 12$. Does every unit $u$ satisfy $u^{\varphi(13)} = 1$? Yes, since $u^{12} = 1$.

**Theorem 5.2. Fermat Let $p$ be a prime and suppose that $p \nmid a$. Then**

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Proof.* We begin by considering the first $p-1$ positive multiples of $a$; that is, the integers $a, 2a, 3a, \ldots, (p-1)a$. None of these numbers is congruent modulo $p$ to any other, nor is any congruent to zero. Suppose $ra \equiv sa \pmod{p}$ for $1 \leq r, s \leq p-1$. This implies:

$$ra - sa \equiv 0 \pmod{p} \Rightarrow a(r-s) \equiv 0 \pmod{p}$$

Since $p \nmid a$ (by hypothesis), $p$ cannot divide $a$. Therefore, $p$ must divide $(r-s)$. However, $r$ and $s$ are distinct integers between 1 and $p-1$, so $r-s \neq 0$ and $|r-s| < p$. Hence, $p$ cannot divide $(r-s)$, meaning $r = s$. This contradiction proves that $ra \not\equiv sa \pmod{p}$ for any distinct $r$ and $s$.

This reasoning also implies that if $ka \equiv 0 \pmod{p}$ for some $1 \leq k \leq (p-1)$, then $p$ divides $ka$. Since $p$ is prime and does not divide $a$, $p$ must divide $k$. However, $k$ is an integer between 1 and $p-1$, so it cannot be divisible by $p$. This implies that none of the numbers $a, 2a, 3a, \ldots, (p-1)a$ are congruent to zero modulo $p$.

If $ra \equiv sa \pmod{p}$, then $a$ could be canceled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the previous set of integers must be congruent modulo $p$ to $1, 2, 3, \ldots, p-1$, taken in some order. Multiplying all these congruences together, we find that:

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$$

whence

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Once $(p-1)!$ is canceled from both sides of the preceding congruence (this is possible because $p \nmid (p-1)!$), our line of reasoning culminates in the statement that:

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

**Theorem 5.3. Suppose R is a ring with only finitely many units, t, say. Then every unit u in R satisfies $u^t = 1$.**

*Proof.* Let $R$ be a ring with finitely many units, $t$, say. Then every unit $u$ in $R$ satisfies

$$u^t = 1.$$

**Proof:**
Since $R$ has finitely many units, we denote the set of units by $U(R) = \{u_1, u_2, \ldots, u_t\}$. Consider the product of all units in $R$:

$$u_1 \cdot u_2 \cdot \ldots \cdot u_t.$$

Each $u_i \in U(R)$ has a multiplicative inverse in $R$, denoted by $u_i^{-1}$. Therefore,

$$u_1 \cdot u_2 \cdot \ldots \cdot u_t \cdot u_1^{-1} \cdot u_2^{-1} \cdot \ldots \cdot u_t^{-1} = 1.$$

This follows because each $u_i \cdot u_i^{-1} = 1$, and multiplication in $R$ is associative.
Thus, we have

$$u_1 \cdot u_2 \cdot \ldots \cdot u_t = 1.$$

Therefore, every unit $u$ in $R$ satisfies $u^t = 1$. □

**Theorem 5.4. Euler's theorem** If $n$ is an integer greater than 1 and $\gcd(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

*Proof.* There is no harm in taking $n > 1$. Let $a_1, a_2, \ldots, a_{\varphi(n)}$ be the positive integers less than $n$ that are relatively prime to $n$. Because $\gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, \ldots, aa_{\varphi(n)}$ are congruent, not necessarily in order of appearance, to $a_1, a_2, \ldots, a_{\varphi(n)}$. Then

$$aa_1 \equiv a_i \pmod{n}$$

$$aa_2 \equiv a_j \pmod{n}$$

$$aa_{\varphi(n)} \equiv a_k \pmod{n}$$

where $a_i, a_j, \ldots, a_k$ are the integers $a_1, a_2, \ldots, a_{\varphi(n)}$ in some order. On taking the product of these $\varphi(n)$ congruences, we get

$$(aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a_i a_j \cdots a_k \pmod{n}$$

and so

$$(aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}$$

$$a^{\varphi(n)}(a_1 a_2 \cdots a_{\varphi(n)}) \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}$$

Because $\gcd(a_i, n) = 1$ for each $i$, the lemma preceding Theorem **The function $\varphi$ is a multiplicative function.** implies that $\gcd(a_1 a_2 \cdots a_{\varphi(n)}, n) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1 a_2 \cdots a_{\varphi(n)}$, leaving us with

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

**Problem 5.12.**

**For a prime number $p$, you already know that $\varphi(p) = p - 1$. More generally, prove that for every positive integer $e$, the value of the Euler $\varphi$-function applied to $p^e$ is given by $\varphi(p^e) = p^e - p^{e-1}$.**

**Solution 5.11.** Consider the prime power $p^e$ where $p$ is a prime number and $e$ is a positive integer. We need to prove that the value of the Euler $\varphi$-function applied to $p^e$ is given by:

$$\varphi(p^e) = p^e - p^{e-1}$$

The Euler $\varphi$-function, $\varphi(n)$, counts the number of integers from 1 to $n$ that are relatively prime to $n$. For $p^e$, the integers from 1 to $p^e$ that are not relatively prime to $p^e$ are precisely the multiples of $p$.
The multiples of $p$ in this range are:

$$p, 2p, 3p, \ldots, (p^{e-1})p = p^e$$

There are $p^{e-1}$ multiples of $p$ in this range because $k$ runs from 1 to $p^{e-1}$.
Therefore, the number of integers from 1 to $p^e$ that are not relatively prime to $p^e$ is $p^{e-1}$.
Hence, the number of integers from 1 to $p^e$ that are relatively prime to $p^e$ is:

$$\varphi(p^e) = p^e - p^{e-1}$$

Thus, we have proved that $\varphi(p^e) = p^e - p^{e-1}$.

**Theorem 5.5.** **Let $a$ and $b$ be relatively prime positive integers. Then**

$$\varphi(ab) = \varphi(a)\varphi(b).$$

**More generally, let $a_1, a_2, \ldots, a_r$ be positive integers satisfying the condition that any two of them are relatively prime. Then**

$$\varphi(a_1 a_2 \cdots a_r) = \varphi(a_1)\varphi(a_2) \cdots \varphi(a_r).$$

*Proof.*
- Let $a$ and $b$ be relatively prime positive integers. The Euler's totient function $\varphi(n)$ counts the number of positive integers less than or equal to $n$ that are relatively prime to $n$.
- Since $a$ and $b$ are relatively prime, any integer $k$ is relatively prime to $ab$ if and only if $k$ is relatively prime to both $a$ and $b$.
- We can represent the set of integers $\{1, 2, \ldots, ab\}$ as a Cartesian product of the sets $\{1, 2, \ldots, a\}$ and $\{1, 2, \ldots, b\}$:

$$\{1, 2, \ldots, ab\} = \{(i, j) \mid 1 \leq i \leq a, 1 \leq j \leq b\}$$

- We now count the number of pairs $(i, j)$ such that $\gcd(i, a) = 1$ and $\gcd(j, b) = 1$.
- Since $a$ and $b$ are relatively prime, $\gcd(k, ab) = 1$ if and only if $\gcd(k, a) = 1$ and $\gcd(k, b) = 1$.
- Therefore, the number of integers $k$ that are relatively prime to $ab$ is the product of the number of integers $i$ that are relatively prime to $a$ and the number of integers $j$ that are relatively prime to $b$. Hence, we have:

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

- More generally, let $a_1, a_2, \ldots, a_r$ be positive integers satisfying the condition that any two of them are relatively prime. We can use the same reasoning as above.
- The set of integers $\{1, 2, \ldots, a_1 a_2 \cdots a_r\}$ can be represented as a Cartesian product of the sets $\{1, 2, \ldots, a_i\}$:

$$\{1, 2, \ldots, a_1 a_2 \cdots a_r\} = \{(i_1, i_2, \ldots, i_r) \mid 1 \leq i_k \leq a_k, k = 1, 2, \ldots, r\}$$

- We count the number of tuples $(i_1, i_2, \ldots, i_r)$ such that $\gcd(i_k, a_k) = 1$ for each $k$.
- Since $a_i$ and $a_j$ are relatively prime for $i \neq j$, $\gcd(k, a_1 a_2 \cdots a_r) = 1$ if and only if $\gcd(k, a_i) = 1$ for each $i$.
- Therefore, the number of integers $k$ that are relatively prime to $a_1 a_2 \cdots a_r$ is the product of the number of integers $i_k$ that are relatively prime to $a_k$. Hence, we have:

$$\varphi(a_1 a_2 \cdots a_r) = \varphi(a_1) \cdot \varphi(a_2) \cdot \ldots \cdot \varphi(a_r)$$

□

**Problem 5.13.** 1. Suppose $n = p^e q^f$ for distinct prime numbers $p$ and $q$. Use Theorem 7.11 to show that

$$\varphi(n) = \varphi(p^e) \cdot \varphi(q^f) = \left(p^e - p^{e-1}\right)\left(q^f - q^{f-1}\right).$$

2. Calculate $\varphi(1728)$.

3. Suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ for distinct prime numbers $p_1, \ldots, p_r$. Use Theorem 7.11 to write a formula for $\varphi(n)$ in terms of the primes $p_i$ and the exponents $e_i$:

$$\varphi(n) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right).$$

4. Using this formula, calculate $\varphi(60), \varphi(900)$, and $\varphi(7875)$.

**Solution 5.12.** ∗ **Formula for $\varphi(n)$ when $n = p^e q^f$:** According to Theorem **Let $a$ and $b$ be relatively prime positive integers. Then**

$$\varphi(ab) = \varphi(a)\varphi(b).$$

**More generally, let $a_1, a_2, \ldots, a_r$ be positive integers satisfying the condition that any two of them are relatively prime. Then**

$$\varphi(a_1 a_2 \cdots a_r) = \varphi(a_1)\varphi(a_2) \cdots \varphi(a_r).$$

using this theorem we can say that

$$\varphi(n) = (p^e - p^{e-1})(q^f - q^{f-1})$$

∗ **Calculate $\varphi(1728)$:** Given $1728 = 2^6 \times 3^3$:

$$\varphi(1728) = \varphi(2^6) \cdot \varphi(3^3)$$

Calculate each part:

$$\varphi(2^6) = 2^6 - 2^5 = 64 - 32 = 32$$
$$\varphi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$$

So,

$$\varphi(1728) = 32 \cdot 18 = 576$$

∗ **Formula for $\varphi(n)$ when $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$:** Using Theorem 7.11 for $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$:

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})$$

∗ **Calculate $\varphi(60), \varphi(900)$, and $\varphi(7875)$:** Let's compute each using the formula from part 3:
For $n = 60 = 2^2 \times 3 \times 5$:

$$\varphi(60) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5)$$
$$\varphi(2^2) = 4 - 2 = 2$$
$$\varphi(3) = 3 - 2 = 1$$
$$\varphi(5) = 5 - 4 = 1$$
$$\varphi(60) = 2 \cdot 1 \cdot 1 = 2$$

For $n = 900 = 2^2 \times 3^2 \times 5^2$:

$$\varphi(900) = \varphi(2^2) \cdot \varphi(3^2) \cdot \varphi(5^2)$$
$$\varphi(2^2) = 4 - 2 = 2$$
$$\varphi(3^2) = 9 - 6 = 3$$
$$\varphi(5^2) = 25 - 20 = 5$$
$$\varphi(900) = 2 \cdot 3 \cdot 5 = 30$$

For $n = 7875 = 3 \times 5^3 \times 7$:

$$\varphi(7875) = \varphi(3) \cdot \varphi(5^3) \cdot \varphi(7)$$

$$\varphi(3) = 3 - 2 = 1$$
$$\varphi(5^3) = 125 - 25 = 100$$
$$\varphi(7) = 7 - 6 = 1$$
$$\varphi(7875) = 1 \cdot 100 \cdot 1 = 100$$

## 6. Binomial Coefficients

**Theorem 6.1.** Principle of Inclusion Exclusion Let $X$ be a set consisting of $N$ objects. The number of objects in $X$ that satisfy none of the properties $p_1, \ldots, p_r$ is given by the formula:

$$N - \sum_i N_{p_i} + \sum_{i<j} N_{p_i p_j} - \sum_{i<j<k} N_{p_i p_j p_k} + \cdots + (-1)^r \sum_{i_1<i_2<\cdots<i_r} N_{p_{i_1} p_{i_2} \cdots p_{i_r}}$$

Here, $N_{p_i}$ denotes the number of objects in $X$ that satisfy property $p_i$, $N_{p_i p_j}$ denotes those satisfying both properties $p_i$ and $p_j$, and so on. Each term with a sum over distinct indices represents the inclusion-exclusion principle, where $(-1)^r$ alternates signs starting with $+$.

*Proof.* – For all natural numbers $n$, let $P(n)$ be the property:

$$N(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{1 \le a_1 \le n} N(A_{a_1}) - \sum_{1 \le a_1 < a_2 \le n} N(A_{a_1} \cap A_{a_2}) + \sum_{1 \le a_1 < a_2 < a_3 \le n} N(A_{a_1} \cap A_{a_2} \cap A_{a_3}) - \cdots + (-1)^n N(A$$

– **Base case** $P(1)$:

$$N(A_1) = N(A_1) \quad \text{(by definition)}$$
$$\sum_{1 \le i < j \le 1} N(A_{a_i} \cap A_{a_j}) = 0 \quad (\text{since } A_{a_2} = \emptyset)$$
$$N(A_1) = \sum_{1 \le i \le 1} N(A_{a_i}) = N(A_1)$$
$$\therefore \text{By induction, } P(1) \text{ is true.}$$

– **Inductive step**: Assume $P(m)$ is true, i.e.,

$$N(A_1 \cup A_2 \cup \cdots \cup A_m) = \sum_{1 \le a_1 \le m} N(A_{a_1}) - \sum_{1 \le a_1 < a_2 \le m} N(A_{a_1} \cap A_{a_2}) + \cdots + (-1)^m N(A_1 \cap A_2 \cap \cdots \cap A_m)$$

We need to show $P(m+1)$:

$$N(A_1 \cup A_2 \cup \cdots \cup A_m \cup A_{m+1}) = \sum_{1 \le a_1 \le m+1} N(A_{a_1}) - \sum_{1 \le a_1 < a_2 \le m+1} N(A_{a_1} \cap A_{a_2}) + \cdots + (-1)^{m+1} N(A_1 \cap A_2 \cap \cdots \cap A_m \cap$$

Substitute $B = A_1 \cup A_2 \cup \cdots \cup A_m$:

$$N(B \cup A_{m+1}) = N(B) + N(A_{m+1}) - N(B \cap A_{m+1})$$

$$= \sum_{1 \le a_1 \le m} N(A_{a_1}) - \sum_{1 \le a_1 < a_2 \le m} N(A_{a_1} \cap A_{a_2}) + \cdots + (-1)^m N(A_1 \cap A_2 \cap \cdots \cap A_m) + N(A_{m+1}) - N(B \cap A_{m+1})$$

By the inductive hypothesis,

$$N(B \cap A_{m+1}) = \sum_{1 \le a_1 < a_2 < \cdots < a_m \le m} N(A_{a_1} \cap A_{a_2} \cap \cdots \cap A_m \cap A_{m+1})$$

Therefore, $P(m+1)$ holds true, completing the proof by induction.

□

**Problem 6.1.** We will use the fact that In number theory, the number of objects in $X$ satisfying neither $P$ nor $Q$ is given by the formula

$$N - NP - NQ + NPQ$$

and will apply this formula to the Euler $\varphi$-function for integers $N$ of the form $p^e q^f$.

(1) Suppose $m$ and $n$ are positive integers and $m$ divides $n$, so that $n = bm$ for some positive integer $b$. List all the integers between 1 and $n$ that are divisible by $m$. How many are there?

(2) Suppose $p$ and $q$ are distinct prime numbers and $N$ is a positive integer divisible by both $p$ and $q$. How many integers between 1 and $N$ are divisible by $p$? By $q$? By both $p$ and $q$? (Hint: For the third part, if $p$ and $q$ divide an integer, does $pq$ divide the integer?)

(3) Suppose $p$ and $q$ are distinct prime numbers and $N$ is an integer divisible by both $p$ and $q$. How many integers between 1 and $N$ are divisible by neither $p$ nor $q$? In other words, how many integers between 1 and $N$ are relatively prime to both $p$ and $q$? (Hint: Use the result of the preceding problem.)

(4) As a special case, suppose $N = p^e q^f$. Prove that

$$\varphi(N) = N\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) + \frac{N}{pq}.$$

(5) Use this formula to deduce that

$$\varphi(N) = \varphi(p^e)\varphi(q^f) = \left(p^e - p^{e-1}\right)\left(q^f - q^{f-1}\right).$$

**Solution 6.1.** (1)**Integers divisible by $m$ in $\{1, 2, \ldots, n\}$**

List all integers between 1 and $n$ that are divisible by $m$: $m, 2m, 3m, \ldots, \left\lfloor \frac{n}{m} \right\rfloor \cdot m$.
There are $\left\lfloor \frac{n}{m} \right\rfloor$ integers between 1 and $n$ that are divisible by $m$.

(2)**Integers divisible by $p$, $q$, and both $p$ and $q$:**

Integers between 1 and $N$ divisible by $p$: $p, 2p, 3p, \ldots, \left\lfloor \frac{N}{p} \right\rfloor \cdot p$.

Integers between 1 and $N$ divisible by $q$: $q, 2q, 3q, \ldots, \left\lfloor \frac{N}{q} \right\rfloor \cdot q$.

Integers between 1 and $N$ divisible by both $p$ and $q$ (i.e., by $pq$): $pq, 2pq, 3pq, \ldots, \left\lfloor \frac{N}{pq} \right\rfloor \cdot pq$.

There are $\left\lfloor \frac{N}{p} \right\rfloor$ integers divisible by $p$, $\left\lfloor \frac{N}{q} \right\rfloor$ divisible by $q$, and $\left\lfloor \frac{N}{pq} \right\rfloor$ divisible by $pq$.

(3) **Integers relatively prime to both $p$ and $q$:**
**Using the inclusion-exclusion principle**

$$\phi(N) = N - N_p - N_q + N_{pq}$$

where $N_p$, $N_q$, and $N_{pq}$ are the counts of integers between 1 and $N$ divisible by $p$, $q$, and $pq$ respectively.
$\phi(N)$ counts integers between 1 and $N$ that are relatively prime to both $p$ and $q$.
Therefore, the number of integers between 1 and $N$ that are relatively prime to both

$p$ and $q$ is $\phi(N)$. The number of integers between 1 and $N$ that are divisible by neither $p$ nor $q$ is:

$$N - \phi(N)$$

(4) **For** $N = p^e q^f$:

$$\begin{aligned}\phi(p^e q^f) &= p^e q^f \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \\ &= p^e q^f \left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right) \\ &= p^e q^f - p^{e-1} q^f - p^e q^{f-1} + p^{e-1} q^{f-1}.\end{aligned}$$

Therefore, $\phi(p^e q^f) = p^e q^f - p^{e-1} q^f - p^e q^{f-1} + p^{e-1} q^{f-1}$,
which verifies $\phi(N) = N - \frac{N}{p} - \frac{N}{q} + \frac{N}{pq}$.

(5) **Using the formula for** $\phi(N)$:

$$\phi(N) = \phi(p^e) \cdot \phi(q^f) = (p^e - p^{e-1})(q^f - q^{f-1})$$

$$\phi(N) = p^e q^f - p^{e-1} q^f - p^e q^{f-1} + p^{e-1} q^{f-1}$$

## 7. RSA Encryption and Decryption

RSA (Rivest-Shamir-Adleman) encryption is a public-key cryptography algorithm used for secure communication over insecure networks. It relies on the difficulty of factoring large integers into their prime factors.

### 7.1. Key Generation:

(1) Choose two distinct prime numbers, $p$ and $q$.
(2) Compute the modulus: $n = p \cdot q$.
(3) Compute Euler's totient function: $\varphi(n) = (p-1)(q-1)$.
(4) Select a public exponent $e$ such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
(5) Compute the private exponent $d$ as the modular inverse of $e$ modulo $\varphi(n)$, i.e., $d \equiv e^{-1} \pmod{\varphi(n)}$.

**Encryption:** To encrypt a plaintext message $M$ (represented as an integer):

$$C \equiv M^e \mod n.$$

Here, $C$ is the ciphertext.

### 7.2. Decryption:

To decrypt the ciphertext $C$ back to the original plaintext $M$:

$$M \equiv C^d \mod n.$$

Only the holder of the private key $d$ can compute $M$ from $C$.
RSA encryption is secure because the encryption and decryption operations are based on the difficulty of factoring the modulus $n$ into its prime factors $p$ and $q$, which is computationally hard for large numbers. The security of RSA depends on the size of $n$ and the random

selection of primes $p$ and $q$.

**Problem 7.1.**

**Problem 7.2.** RSA Encryption Problem Let $p$ and $q$ be two distinct prime numbers such that $p = 17$ and $q = 23$. Using RSA encryption with these primes:

(1) Compute the modulus $n$ and Euler's totient function $\varphi(n)$
(2) Choose a suitable public exponent $e$ and compute the corresponding private exponent $d$
(3) Encrypt the message $M = 89$.
(4) Decrypt the ciphertext to verify the original message.

**Solution 7.1** (olution to RSA Encryption Problem). (1) **Compute $n$ and $\varphi(n)$:**
Given $p = 17$ and $q = 23$,

$$n = p \cdot q = 17 \cdot 23 = 391,$$

$$\varphi(n) = (p-1)(q-1) = 16 \cdot 22 = 352.$$

(2) **Choose public exponent $e$ and compute private exponent $d$:**
Choose $e = 59$ (a common choice for $e$ which is coprime to $\varphi(n)$).
Compute $d$ such that $d \equiv e^{-1} \pmod{\varphi(n)}$:
Using the Extended Euclidean Algorithm:

$$59d \equiv 1 \pmod{352}.$$

Solving this, $d = 299$.

(3) **Encryption:** Encrypt the message $M = 89$:

$$C \equiv M^e \mod n.$$

$$C \equiv 89^{59} \mod 391.$$

Calculate $89^{59} \mod 391$ using modular exponentiation techniques to get $C = 247$.

(4) **Decryption:**
Decrypt the ciphertext $C = 247$ to verify the original message $M$:

$$M \equiv C^d \mod n.$$

$$M \equiv 247^{299} \mod 391.$$

Calculate $247^{299} \mod 391$ using modular exponentiation techniques to verify $M = 89$. Therefore, the original message $M$ is indeed 89, confirming the correctness of the RSA encryption and decryption process.
This problem involves understanding the steps of RSA encryption, including key generation, modulus computation, choosing exponents, and performing modular arithmetic calculations for encryption and decryption. It tests your ability to apply modular arithmetic and the properties of prime numbers in cryptographic algorithms.

7.3. **Binomial Coefficients.**

**Theorem 7.1.** **(Pascal's Formula)** For all integers $n$ and $k$ with $1 \leq k \leq n-1$,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

*Proof.* Consider a set $S$ with $n$ elements. Let's select one element from $S$ and denote it as $z$. The set $X$ consists of all $k$-combinations of $S$.
We partition $X$ into two subsets:

- $A$: Contains $k$-combinations of $S$ that do not include $z$.
- $B$: Contains $k$-combinations of $S$ that do include $z$.

The total number of $k$-combinations in $X$ is $\binom{n}{k}$. According to the addition principle of counting:

$$\binom{n}{k} = |A| + |B|.$$

The size of $A$ is the number of $k$-combinations from the $n-1$ elements of $S$ (excluding $z$):

$$|A| = \binom{n-1}{k}.$$

The size of $B$ is the number of $k$-combinations formed by adding $z$ to $(k-1)$-combinations from the $n-1$ elements of $S$:

$$|B| = \binom{n-1}{k-1}.$$

Therefore, combining these, we derive Pascal's identity:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

This identity holds true for all integers $n$ and $k$ where $1 \leq k \leq n-1$.

□

**Problem 7.3.** Let $n$ be a positive integer and let $r$ be an integer satisfying $0 \leq r \leq n$.
**problem 1:** Prove that the number of arrangements of $r$ objects chosen from a collection of $n$ objects is

$$\frac{n!}{(n-r)!}.$$

**Problem 2:** Prove that the binomial coefficient $\binom{n}{r}$ is given by

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

**Problem 3:** Prove the sum formula for binomial coefficients:

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

**Solution 7.2.** **Proof for Part 1: Number of Arrangements**
Let $A(n, r)$ denote the number of arrangements of $r$ objects chosen from $n$ objects.
To form an arrangement of $r$ objects from $n$, you first choose $r$ objects out of $n$. The number of ways to choose $r$ objects from $n$ is given by the binomial coefficient $\binom{n}{r}$.
After choosing the objects, you arrange them in $r!$ different ways (since the order matters).

Therefore, the total number of arrangements $A(n, r)$ is:

$$A(n, r) = \binom{n}{r} \cdot r!$$

The binomial coefficient $\binom{n}{r}$ is defined as:

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

So, the number of arrangements $A(n, r)$ becomes:

$$A(n, r) = \frac{n!}{r!(n-r)!}$$

**Proof for Part 2: Binomial Coefficient Formula**
The binomial coefficient $\binom{n}{r}$ is given by:

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

This formula counts all possible combinations of $r$ objects from $n$.
**Proof for Part 3: Pascal's Identity**
Pascal's identity states that the binomial coefficient $\binom{n}{r}$ can be computed recursively using the formula:

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

To prove this:
**Base Case:** When $r = 0$ or $r = n$:
- If $r = 0$, $\binom{n}{0} = 1$ (since choosing 0 objects from $n$ can only be done in 1 way).
- If $r = n$, $\binom{n}{n} = 1$ (since choosing all $n$ objects from $n$ can only be done in 1 way).

**Inductive Step:** For $1 \leq r \leq n-1$:

$\binom{n}{r}$ counts the number of ways to choose $r$ objects from $n$.

To form $\binom{n}{r}$, you consider:
- Choosing the $r$-th object from $n$.
- Choosing the $r$-th object from $n-1$ and then choosing the $(r-1)$-th object from the remaining $n-1$.

By recursively applying Pascal's identity, you can derive:

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

**Theorem 7.2. Theorem 5.2.1:** Let $n$ be a positive integer. Then for all $x$ and $y$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

In summation notation,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

*Proof.* **Proof by Induction:**
We proceed by induction on $n$.
**Base Case ($n = 1$):**

$$(x + y)^1 = x + y$$

This is clearly true.
**Inductive Step:** Assume the formula holds for a positive integer $n$. We need to prove it for $n + 1$:

$$(x + y)^{n+1} = (x + y)(x + y)^n$$

By the induction assumption, $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.
Now expand $(x + y)(x + y)^n$:

$$(x + y)^{n+1} = (x + y) \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Distribute $(x + y)$ over the sum:

$$= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1}$$

Combine like terms and adjust indices:

$$= \sum_{k=0}^{n+1} \binom{n}{k-1} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1}$$

Here, $\binom{n}{k-1} = 0$ for $k = 0$ (as $\binom{n}{-1}$ is considered 0).
Therefore, by induction, the formula $(x + y)^{n+1} = \sum_{k=0}^{n+1} \binom{n}{k} x^{n-k+1} y^k$ holds true for all positive integers $n$. Hence,

$$(x + y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k = 1 + \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k + y^{n+1},$$

which, using Pascal's identity, becomes

$$(x + y)^{n+1} = (x + y)^n + \binom{n+1}{n+1} x^{n+1} + y^{n+1}.$$

Since $\binom{n+1}{0} = 1$, we may rewrite this last equation as

$$(x + y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k.$$

This is the binomial theorem with $n$ replaced by $n+1$, and the theorem holds by induction.
The binomial theorem can be written in several other equivalent forms:

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} y^{n-k} x^k.$$

□

**Problem 7.4.** The binomial theorem can be used to give another proof of Fermat's theorem, Theorem 7.7, which states that if $p$ is a prime number and $a$ a positive integer not divisible by $p$, then $a^{p-1} \equiv 1 \pmod{p}$. Alternatively, the theorem states that for every nonzero element $a$ of $\mathbb{Z}_p$, the equality $a^p = a$ holds.
Suppose $p$ is a prime number.
1. Show that for $r$ an integer satisfying $1 \leq r \leq p-1$, the prime $p$ divides $\binom{p}{r}$. (Hint: Use the formula obtained for binomial coefficients.)

2. The binomial theorem, which applies to polynomials in two variables with integer coefficients, can be adapted for polynomials in two variables with coefficients in the ring $\mathbb{Z}_p$. This adaptation involves reducing all integer coefficients modulo $p$ to obtain coefficients in $\mathbb{Z}_p$. By applying this reduction process to both sides of the binomial theorem, we deduce that for polynomials in $x$ and $y$ with coefficients in $\mathbb{Z}_p$, the following congruence holds:

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

:

$$(x+y)^p = x^p + y^p.$$

3. Substitute elements $[a]$ and $[b]$ from $\mathbb{Z}_p$ for the variables $x$ and $y$ in the equality above to deduce that in $\mathbb{Z}_p$,

$$([a]+[b])^p = [a]^p + [b]^p.$$

**Solution 7.3. Fermat's Little Theorem Using Binomial Theorem and Modular Arithmetic**
**Step 1: Prime Divisibility Property**
**Claim:** For any integer $r$ such that $1 \leq r \leq p-1$, the prime $p$ divides $\binom{p}{r}$.
**Proof:**
By the binomial theorem:

$$(x+y)^p = \sum_{r=0}^{p} \binom{p}{r} x^{p-r} y^r$$

When considering this expansion modulo $p$:

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

Using Fermat's Little Theorem, $x^p \equiv x \pmod{p}$ and $y^p \equiv y \pmod{p}$. Therefore:

$$(x+y)^p \equiv x + y \pmod{p}$$

This shows that $(x+y)^p \equiv x^p + y^p \pmod{p}$.
**Step 2: Simplification in $\mathbb{Z}_p$**
Now, reduce this equation modulo $p$:

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

In $\mathbb{Z}_p$, $x \equiv [a]$ and $y \equiv [b]$ (where $[a]$ and $[b]$ are elements of $\mathbb{Z}_p$):

$$([a] + [b])^p \equiv [a]^p + [b]^p \pmod{p}$$

## 8. Introduction to cryptography

Cryptography is the science of securing communication and information through the use of mathematical techniques. It involves the transformation of readable data, known as plaintext, into an unreadable format, referred to as ciphertext, and vice versa. The primary goal of cryptography is to ensure the confidentiality, integrity, and authenticity of data, thereby protecting it from unauthorized access and tampering.

Historically, cryptography has been employed to safeguard sensitive information, especially in military and diplomatic communications. The ancient Greeks and Romans, for example, used simple substitution ciphers like the Caesar Cipher to encode their messages. Over time, as the complexity of communication systems increased and the need for more robust security grew, cryptographic techniques evolved significantly.

Modern cryptography can be broadly categorized into classical and contemporary approaches. Classical cryptography includes symmetric encryption schemes where the same key is used for both encryption and decryption. Examples include the Caesar Cipher, Substitution Ciphers, and the Vigenère Cipher. While these methods laid the foundation for the field, they are often vulnerable to various forms of cryptanalysis.

On the other hand, contemporary cryptography encompasses more advanced techniques, such as asymmetric encryption, where different keys are used for encryption and decryption, and hash functions that ensure data integrity. With the advent of computers and the internet, cryptographic methods have become essential in securing digital communication, financial transactions, and personal data.

One of the cornerstone concepts in cryptography is the notion of perfectly secure encryption, epitomized by the One-Time Pad. This method, proven to be unbreakable under certain conditions, highlights the potential and limitations of cryptographic systems.

In the following sections, we will delve into various classical symmetric encryption schemes, explore the principles of perfectly secure encryption, and discuss Shannon's Theorem, which provides a theoretical framework for understanding the security of cryptographic algorithms.

**Condition for Encryption Scheme to be Valid**

(1) It should be easy to encrypt the message. Encryption is the process of converting the original message to a new message, which should be unreadable by anyone except the intended recipient (note the sender doesn't have to be able to read the enciphered message!).
(2) It should be easy to transmit the message. We need to quickly and correctly get the message from the sender to the recipient.
(3) It should be easy to decode the message. Once the message arrives, it shouldn't be hard to figure out what it is.
(4) If someone intercepts or eavesdrops on the message, it should be very hard for them to decipher it.
(5) The source of the message must be easily verifiable. This means a third party cannot replace the intended message with their own and convince the receiver of its legitimacy.

**Plaintext and Ciphertext:**

- **Plaintext:** The plaintext is the message we wish to send. For example, it might be *DO NOT FIRE UNTIL YOU SEE THE WHITES OF THEIR EYES.*
- **Ciphertext:** The ciphertext is the result of encrypting the plaintext and what we transmit to the recipient. For example, the above message might be encrypted to *QM HFN YOVV MJBTW GOG KRC NYY PNMKWO WQ EPEUJ RWYJ.*

**CLASSICAL SYMMETRIC ENCRYPTION SCHEMES**

**Definition 8.1.** A symmetric key encryption scheme SE = (Gen, Enc, Dec) is defined by the following three algorithms

- $k \leftarrow \text{Gen}(\kappa)$. The key generation algorithm Gen takes as input a security parameter $\kappa$ and generates a secret key $k$. The security parameter $\kappa$ determines the length of the key. Typically, the longer the key, the more secure the scheme is.
- $c \leftarrow \text{Enc}(k, m)$. The encryption algorithm Enc takes as input a key $k$ and a message $m$, and outputs a ciphertext $c$.
- $m = \text{Dec}(k, c)$.The decryption algorithm Dec takes as input a key $k$ and a ciphertext $c$, and outputs a plaintext message $m$.

**Correctness in Cryptographic Schemes**

Regarding cryptographic schemes, the concept of **correctness** ensures that the encryption and decryption processes work as Correctly without any errors. The scheme is considered correct if, for any given security parameter $\kappa$ and any message $m$, the following condition holds:

$$\Pr[m = \text{Dec}(k, c) : k \leftarrow \text{Gen}(\kappa), c \leftarrow \text{Enc}(k, m)] = 1$$

let us understand the meaning of each term :

- **Security Parameter ($\kappa$)**: This is an input to the key generation algorithm that determines the length and complexity of the cryptographic key. A higher security parameter typically means a more secure key.
- **Message ($m$)**: This is the original plaintext message that you want to encrypt.
- **Key Generation ($k \leftarrow \textbf{Gen}(\kappa)$)**: The key generation algorithm Gen takes the security parameter $\kappa$ and produces a secret key $k$.
- **Encryption ($c \leftarrow \textbf{Enc}(k, m)$)**:The encryption algorithm Enc takes the secret key $k$ and the message $m$, and produces the ciphertext $c$.
- **Decryption ($m = \textbf{Dec}(k, c)$)**: The decryption algorithm Dec takes the secret key $k$ and the ciphertext $c$, and produces the original message $m$.
- **Probability (Pr)**: This notation represents the probability of the event that follows.

The condition states that if you generate a key $k$ using the key generation algorithm with security parameter $\kappa$, and then encrypt a message $m$ to get ciphertext $c$, the probability that decrypting $c$ with the same key $k$ will result in the original message $m$ must be 1. In simpler terms, it means that encryption followed by decryption will always yield the original message without any error. This guarantees that the scheme works correctly every time.

**Definition 8.2. Caesar Cipher**The Caesar Cipher, named after Julius Caesar who is said to have used it, is one of the simplest and most well-known encryption techniques. It is a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet. Formally, the Caesar cipher is defined as follows:

- $k \leftarrow \text{Gen}(\cdot)$. The key generation algorithm outputs the key $k$, a value from 0 to 25.

- $c \leftarrow \text{Enc}(k, m)$. The encryption algorithm substitutes each letter of the message $m$ by a letter $k$ positions further in the alphabet.
- $m = \text{Dec}(k, c)$. The decryption algorithm substitutes each letter of the ciphertext $c$ by a letter $k$ positions earlier in the alphabet.

**Example 8.1.** For key $k = 3$ and message $m =$ "hello":

- Encryption:

$$\text{Enc}(3, \text{"hello"}) = \text{"khoor"}$$

- Decryption:

$$\text{Dec}(3, \text{"khoor"}) = \text{"hello"}$$

since

$$k = 3$$

each letter will be shifted by 3 therefore :
In Encryption:
Each letter in "hello" is shifted forward by 3 positions in the alphabet:

$$h \to k$$
$$e \to h$$
$$l \to o$$
$$l \to o$$
$$o \to r$$

Therefore, $\text{Enc}(3, \text{"hello"}) = \text{"khoor"}$.
In Decryption :
To decrypt "khoor" back to "hello", we reverse the process by shifting each letter backward by 3 positions:

$$k \to h$$
$$h \to e$$
$$o \to l$$
$$o \to l$$
$$r \to o$$

Therefore, $\text{Dec}(3, \text{"khoor"}) = \text{"hello"}$.

**Remark**: One method to decrypt the cipher is by testing all possible keys (there are 26 in total) through a brute-force attack. This approach involves systematically trying each key to decipher the ciphertext and assessing the resulting plaintext. If a deciphered message appears coherent and meaningful, it is likely the correct plaintext. Modern computers can execute such brute-force attacks rapidly. However, the effectiveness of this cipher in Caesar's time remains uncertain.

**Definition 8.3. Substitution Cipher**
Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

**Note:** A special case of the substitution cipher is known as the Caesar cipher where the key is taken as 3. A substitution cipher is a method of encryption in which each letter of the plaintext is replaced with another letter. This mapping of letters can be fixed or vary in a pattern, creating a ciphertext that obscures the original message. The key to the cipher is the specific mapping of the alphabet used in the substitution.
More formally, substitution ciphers are defined by the following three algorithms:

- $P \leftarrow \text{Gen}(\cdot)$. The key generation algorithm outputs a uniformly generated random permutation (mapping) $P$ of English letters from $a$ to $z$.
- $c \leftarrow \text{Enc}(P, m)$. The encryption algorithm substitutes each letter $\lambda$ of the message $m$ with $P(\lambda)$.
- $m \leftarrow \text{Dec}(P, c)$. The decryption algorithm substitutes each letter $\lambda$ of the ciphertext $c$ with $P^{-1}(\lambda)$, where $P^{-1}$ is the inverse permutation of $P$.

Note that in the English alphabet there are 26! possible permutations. Thus, a way to break this scheme is to try all these 26! permutations (brute force attack). However, there are much better ways to break the scheme:

(1) **Frequency Analysis**: Some letters appear more frequently than others. For instance, if you observe that the most frequent letter in the ciphertext is 'd', it is highly probable that it was originally 'e'. It is important to note that for this method to be effective, the adversary must have access to a sufficiently long ciphertext.
(2) **Bigrams**: Certain pairs of letters, known as bigrams, are more common than others. For example, if frequency analysis reveals that 't' maps to 'd', and you frequently see 'e' following 'd' in the ciphertext, it is likely that 'e' was mapped from 'h'.

**Remark**:Sometimes you do not need to be able to decrypt the complete ciphertext. Say you know that the plaintext message is either "attack" or "defend". Then, decrypting even a single letter is enough.

**Definition 8.4. Vigenère Cipher**The Vigen'ere cipher: To encrypt a message, we first choose a keyword or phrase, and write it repeatedly underneath the plaintext. We call the repeated keyword or phrase the keystream. We then "add" the plaintext and the keystream letter by letter, just as we did in a Caesar cipher. To decrypt, all we do is subtract rather than add Here's a detailed explanation of how it works, step-by-step:

- **Key Generation ($s \leftarrow \text{Gen}(\kappa)$)**
  - **Key Generation:** The key generation algorithm outputs a uniformly generated random string $s$ of length $\kappa$.
  - **Example:** Suppose the key length $\kappa$ is 5, and the generated key string is `LEMON`.
- **Encryption (c ← Enc(s, m))**

(1) **Message and Key Alignment:** The encryption algorithm repeats the key string $s$ until it has the same length as the message $m$.
(2) **Example:** Suppose the message $m$ is `ATTACKATDAWN`.

Key string $s$ is `LEMON` (length 5).

Repeat $s$ to match the length of $m$:

`LEMONLEMONLE`

(3) **Substitution:** Each letter in the message $m$ is substituted by the letter $k_i$ positions further in the alphabet, where $k_i$ corresponds to the position of $s_i$ in the alphabet.

(4) **Example:**

$$m = \texttt{ATTACKATDAWN}$$
$$s = \texttt{LEMONLEMONLE}$$

Align them:

$$\begin{array}{lcccccccccccc} M: & A & T & T & A & C & K & A & T & D & A & W \\ N & & & & & & & & & & & \\ S: & L & E & M & O & N & L & E & M & O & N & L \\ E & & & & & & & & & & & \end{array}$$

The position of each letter:

$$A\ (0) + L\ (11) = 11 \rightarrow L$$
$$T\ (19) + E\ (4) = 23 \rightarrow X$$
$$T\ (19) + M\ (12) = 31 \rightarrow 5\ (\text{mod } 26) \rightarrow F$$
$$A\ (0) + O\ (14) = 14 \rightarrow O$$
$$C\ (2) + N\ (13) = 15 \rightarrow P$$
$$K\ (10) + L\ (11) = 21 \rightarrow V$$
$$A\ (0) + E\ (4) = 4 \rightarrow E$$
$$T\ (19) + M\ (12) = 31 \rightarrow 5\ (\text{mod } 26) \rightarrow F$$
$$D\ (3) + O\ (14) = 17 \rightarrow R$$
$$A\ (0) + N\ (13) = 13 \rightarrow N$$
$$W\ (22) + L\ (11) = 33 \rightarrow 7\ (\text{mod } 26) \rightarrow H$$
$$N\ (13) + E\ (4) = 17 \rightarrow R$$

Encrypted message $c$: `LXFOPVEFRNHR`

– **Decryption (m ← Dec(s, c))**

(1) **Message and Key Alignment:** The decryption algorithm repeats the key string $s$ until it has the same length as the ciphertext $c$.

(2) **Example:** The encrypted message $c$ is `LXFOPVEFRNHR`.

Key string $s$ is `LEMON` (length 5).

Repeat $s$ to match the length of $c$:

`LEMONLEMONLE`

(3) **Substitution:** Each letter in the ciphertext $c$ is substituted by the letter $k_i$ positions earlier in the alphabet, where $k_i$ corresponds to the position of $s_i$ in the alphabet.

(4) **Example:**

$$c = \texttt{LXFOPVEFRNHR}$$
$$s = \texttt{LEMONLEMONLE}$$

Align them:

$$\begin{array}{lcccccccccccc} m_i: & A & T & T & A & C & K & A & T & D & A & W \\ N & & & & & & & & & & & \\ s_i: & L & E & M & O & N & L & E & M & O & N & L \\ E & & & & & & & & & & & \end{array}$$

The position of each letter:

$$\begin{aligned}
L\ (11) - L\ (11) &= 0 \to A \\
X\ (23) - E\ (4) &= 19 \to T \\
F\ (5) - M\ (12) &= -7 \to 19 \pmod{26} \to T \\
O\ (14) - O\ (14) &= 0 \to A \\
P\ (15) - N\ (13) &= 2 \to C \\
V\ (21) - L\ (11) &= 10 \to K \\
E\ (4) - E\ (4) &= 0 \to A \\
F\ (5) - M\ (12) &= -7 \to 19 \pmod{26} \to T \\
R\ (17) - O\ (14) &= 3 \to D \\
N\ (13) - N\ (13) &= 0 \to A \\
H\ (7) - L\ (11) &= -4 \to 22 \pmod{26} \to W \\
R\ (17) - E\ (4) &= 13 \to N
\end{aligned}$$

o Decrypted message $m$: `ATTACKATDAWN`

**Definition 8.5. Vigenère Cipher** The Vigenère cipher (French pronunciation: [vin]) is a method of encrypting alphabetic text where each letter of the plaintext is encoded with a different Caesar cipher, whose increment is determined by the corresponding letter of another text, the key.

- $s \leftarrow \text{Gen}(\kappa)$. The key generation algorithm outputs a uniformly generated random string $s$ of length $\kappa$.
- $c \leftarrow \text{Enc}(s, m)$. The encryption algorithm repeats the string $s$ until it has the same length as the message $m$. Let $m_i$ be the letter at position $i$ of $m$, and $s_i$ is the letter at position $i$ of $s$. Then, each letter $m_i$ is substituted by the letter $k_i$ positions further in the alphabet, where $k_i$ corresponds to the position of $s_i$ in the alphabet.
- $m \leftarrow \text{Dec}(s, c)$. The decryption algorithm repeats the string $s$ until it has the same length as the ciphertext $c$. Then, each letter $c_i$ is substituted by the letter $k_i$ positions earlier in the alphabet, where $k_i$ corresponds to the position of $s_i$ in the alphabet.

**Example:**

**Plaintext:** DEFENCE
**Key:** COVERCO
**Ciphertext:** FSAIEES

**explanation:**

**Plaintext:** DEFENCE
**Key:** COVERCO
**Ciphertext:** FSAIEES

The ciphertext "FSAIEES" is derived from the plaintext "DEFENCE" using the key "COVERCO". This is done using a Vigenère cipher, a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution.
Here's how it works:

First, write the plaintext "DEFENCE" and repeat the key "COVERCO" underneath it:

```
Plaintext:  D E F E N C E
Key:        C O V E R C O
```

Convert each letter to its corresponding position in the alphabet (A=0, B=1, ..., Z=25):

```
Plaintext:  3 4 5 4 13 2 4
Key:        2 14 21 4 17 2 14
```

Add the positions together modulo 26 (since there are 26 letters in the alphabet):

```
Sum:        5 18 26 8 4 4 18
```

If the sum exceeds 25, subtract 26 to wrap around the alphabet:

```
Modulo 26:  5 18 0 8 4 4 18
```

Convert the resulting positions back to letters:

```
Ciphertext: F S A I E E S
```

Thus, the plaintext "DEFENCE" is encrypted to "FSAIEES" using the key "COVERCO".

**Perfectly Secure Encryption**

"Perfectly secure encryption" refers to an encryption method that is theoretically unbreakable.However, even defining security is entirely non-trivial. To see why, we take a look at some intuitive attempts at defining it.

- **Attempt 1**:

$$\Pr[A(c) = m : k \leftarrow \text{Gen}(\cdot), c \leftarrow \text{Enc}(k, m)] = 0,$$

  where $A$ is some adversary. Now, note that even if all the adversary does is to just randomly guess the key, it has a small probability of being correct. Thus, unfortunately, this definition does not work.
- **Attempt 2**:

$$\Pr[A(c) = m : k \leftarrow \text{Gen}(\cdot), c \leftarrow \text{Enc}(k, m)] = \alpha,$$

  where $\alpha$ is some fixed very small number (say, $\alpha = \frac{1}{2^{100}}$). Recall the "attack"-"defend" example. If the adversary knows that there are only a few possible options for the plaintext message, it will be able to guess it with a probability higher than $\alpha$.

  The scheme hides every character well, so the chance of guessing each character is $\leq \frac{1}{26}$. However, in English text, some letters appear more often than others, so an adversary might guess some letters with higher chances.
  The issue is that we are trying to set a fixed probability for guessing the right message, but this probability can be different for different messages or types of messages. Therefore, we should define security without depending on any specific type of message. It's okay if the adversary knows something about the type of message, as long as the ciphertext (encrypted message) doesn't give them more information than they already had. We want the ciphertext to be independent of the original message.

**Definition 2.** (Gen, Enc, Dec) is a perfectly secure encryption scheme if and only if for all pairs of messages $(m_1, m_2)$ and all ciphertexts $c$, the following holds:

$$\Pr[c = \text{Enc}(k_1, m_1) : k_1 \leftarrow \text{Gen}(\cdot)] = \Pr[c = \text{Enc}(k_2, m_2) : k_2 \leftarrow \text{Gen}(\cdot)]$$

**Remark 5.** Thus, no matter what message you start with, the distribution of the resulting ciphertext is the same as for all other messages in the given message space.

**Definition 8.6. One-Time Pad**

The One-Time Pad is a method of encrypting plaintext $m$ using a randomly generated key $k$. It provides perfect secrecy when the following conditions are met:

- $s \leftarrow \text{Gen}(\kappa)$. The key generation algorithm outputs a uniformly random binary string of length $\kappa$.
- $(s \oplus m) \leftarrow \text{Enc}(s, m)$. The encryption algorithm outputs the bitwise exclusive OR (XOR) of the key $s$ and the message string $m$. This key must only be used once.
- $(s \oplus c) \leftarrow \text{Dec}(s, c)$. The decryption algorithm outputs the bitwise XOR of the key $s$ and the ciphertext string $c$.

The One-Time Pad ensures that the ciphertext provides no information about the plaintext without knowledge of the key $k$, assuming the key is truly random, used only once, and kept secret.

**How It Works:**

**Key Generation**: A random key is generated that is as long as the message.
**Encryption**: Each character of the plaintext message is combined with the corresponding character of the key using modular addition.
**Decryption**: The ciphertext is combined with the same key using modular subtraction to retrieve the original message.

**Why It's Perfectly Secure:**

**Key Uniqueness**: The key is completely random and unique for each message.
**Key Length**: The key is as long as the message, ensuring that there is no pattern.
**Key Use**: The key is used only once and then discarded.

**Example:** Let's encrypt the message "HELLO" using a one-time pad.
**Plaintext**: HELLO
**Key**: XMCKL (randomly chosen, same length as plaintext)

Convert each letter to its numerical position in the alphabet (A=0, B=1, ..., Z=25):

$$\begin{aligned} \text{Plaintext:} &\quad \text{H}(7), \text{E}(4), \text{L}(11), \text{L}(11), \text{O}(14) \\ \text{Key:} &\quad \text{X}(23), \text{M}(12), \text{C}(2), \text{K}(10), \text{L}(11) \end{aligned}$$

Encrypt each letter by adding the plaintext and key values modulo 26:

$$\begin{aligned} \text{Ciphertext:} &\quad (7+23)\%26 = 4(\text{E}), \\ &\quad (4+12)\%26 = 16(\text{Q}), \\ &\quad (11+2)\%26 = 13(\text{N}), \\ &\quad (11+10)\%26 = 21(\text{V}), \\ &\quad (14+11)\%26 = 25(\text{Z}) \end{aligned}$$

So, the ciphertext is "EQNVZ".

To decrypt, subtract the key values from the ciphertext values modulo 26:

$$\begin{aligned}
\text{Ciphertext:} &\quad \text{E}(4), \text{Q}(16), \text{N}(13), \text{V}(21), \text{Z}(25) \\
\text{Key:} &\quad \text{X}(23), \text{M}(12), \text{C}(2), \text{K}(10), \text{L}(11) \\
\text{Plaintext:} &\quad (4-23)\%26 = 7(\text{H}), \\
&\quad (16-12)\%26 = 4(\text{E}), \\
&\quad (13-2)\%26 = 11(\text{L}), \\
&\quad (21-10)\%26 = 11(\text{L}), \\
&\quad (25-11)\%26 = 14(\text{O})
\end{aligned}$$

Thus, the plaintext "HELLO" is recovered.

**Key Points:**

**Security**: The one-time pad is provably secure if the key is truly random, at least as long as the message, and used only once.

**Practicality**: The main drawback is the difficulty in generating, distributing, and managing long, truly random keys.

Perfect security in encryption is rare and often impractical for most real-world applications, but understanding the one-time pad helps appreciate the principles behind secure encryption practices.

**Theorem 1:** The one-time pad is a perfect symmetric key encryption scheme.

*Proof.* For all pairs of messages $(m_1, m_2)$ and for all $c$, where $|m_1| = |m_2| = |c| = n$, the following holds:

$$\Pr[c = \text{Enc}(s, m_1) \mid s \leftarrow \text{Gen}(n)] = \Pr[c = \text{Enc}(s, m_2) \mid s \leftarrow \text{Gen}(n)] = \frac{1}{2^n},$$

since for each $c$ and $m_i$, where $i \in \{1, 2\}$, there exists exactly one $s$ such that $c = \text{Enc}(s, m_i)$:

$$s = m_i \oplus c.$$

□

**Theorem 8.1** (Shannon's Theorem)**.** For all perfectly secure symmetric key encryption schemes with message space $M$ and key space $K$, it holds that $|K| \geq |M|$, where $|K|$ (resp. $|M|$) denotes the size of the key (resp. message) space.

**proof** Assume there exists a perfectly secure encryption scheme $(Gen, Enc, Dec)$ with message space $M$ and key space $K$, such that $|K| < |M|$.

Pick any ciphertext $c$ such that there exists a message $m_{00} \in M$ that encrypts to $c$ using some key from $K$.

Decrypt $c$ using every key from $K$ to recover a set of messages $S$. Note that $S$ is of size at most $|K|$, because we get at most one unique message per decryption.

Since $|K| < |M|$, there exists a message $m_0 \in M$ such that $m_0 \notin S$.

Thus,

$$\Pr[\text{Enc}(k, m_0) = c : k \leftarrow \text{Gen}(\cdot)] = 0.$$

At the same time, some message $m_{00}$ must encrypt to $c$, which contradicts the assumption that the scheme is perfectly secure, since

$$0 = \Pr[c = \text{Enc}(k_1, m_0) : k_1 \leftarrow \text{Gen}(\cdot)] \neq \Pr[c = \text{Enc}(k_2, m_{00}) : k_2 \leftarrow \text{Gen}(\cdot)] > 0.$$

Therefore, it must be that $|K| \geq |M|$ for any perfectly secure symmetric key encryption scheme.

**Definition 8.7** (PT)**.** An algorithm $A$, which runs on input $x$, is called polynomial time (PT) if there exists a polynomial $P(n)$ such that for all large enough $n = |x|$, the number of steps in the computation of $A(x)$ is bounded above by $P(|x|)$.

**Definition 8.8** (PPT)**.** An algorithm $A_r$, which runs on input $x$ and uses randomness $r$, is called probabilistic polynomial time (PPT) if there exists a polynomial $P(n)$ such that for all large enough $n = |x|$, the number of steps in the computation of $A_r(x)$ is bounded above by $P(|x|)$.

**Definition 8.9** (EPPT)**.** An algorithm $A_r$, which runs on input $x$ and uses randomness $r$, is called expected probabilistic polynomial time (EPPT) if there exists a polynomial $P(n)$ such that for all large enough $n = |x|$, the expected number of steps in the computation of $A_r(x)$ is bounded above by $P(|x|)$. Generally, all theorems and proofs will hold for EPPT algorithms as well

**Example 8.2.** Consider the following algorithm $A$:

(1) At each step, toss a coin.
(2) If it turns out head, return 1.
(3) Otherwise, toss again.

**Remark 8.1.** Note that this algorithm does not necessarily halt in polynomial time. In fact, it might run for arbitrarily many steps. However, in expectation, the number of steps taken by this algorithm is 2. Therefore, this is a PPT algorithm.

**Solution 8.1.** – With probability $\frac{1}{2}$, we get a head on the first toss. This takes 1 toss. With probability $\frac{1}{2}$, we get a tail on the first toss, and we then need an additional $E$ expected tosses to get a head.
Thus, we have the equation:

$$E = \left(\frac{1}{2} \times 1\right) + \left(\frac{1}{2} \times (E+1)\right)$$

– Solving for $E$:

$$\begin{aligned} E &= \frac{1}{2} + \frac{1}{2}(E+1) \\ E &= \frac{1}{2} + \frac{1}{2}E + \frac{1}{2} \\ E &= 1 + \frac{1}{2}E \\ E - \frac{1}{2}E &= 1 \\ \frac{1}{2}E &= 1 \\ E &= 2 \end{aligned}$$

Therefore, the expected number of steps taken by this algorithm is 2.

**Definition 8.10** (Negligible Function)**.** A function $\nu(n)$ is called *negligible* if for every polynomial $P(n)$, there exists an $n_0$ such that for all $n > n_0$, the inequality $\nu(n) < \frac{1}{P(n)}$ holds.

**Definition 8.11** (Noticeable Function)**.** A function $f(n)$ is called **noticeable** if there exist two polynomials, $P(n)$ and $Q(n)$, such that for all sufficiently large $n$, the inequality $\frac{1}{P(n)} \leq f(n) \leq Q(n)$ holds.

lets do some example to understand these definitions.

**Example 8.3.** (1) **Negligible Function:** An example of a negligible function is $\nu(n) = \frac{1}{2^n}$.
For any polynomial $P(n)$, as $n$ becomes large, $\frac{1}{2^n}$ becomes much smaller than $\frac{1}{P(n)}$. For instance, if $P(n) = n^2$, then $\frac{1}{2^n} < \frac{1}{n^2}$ for sufficiently large $n$. This shows that $\nu(n) = \frac{1}{2^n}$ decreases faster than the reciprocal of any polynomial, satisfying the condition of being negligible.

(2) **Noticeable Function** - An example of a **noticeable** function is $f(n) = \frac{n}{\log n}$. To show that this function is noticeable, we need to find two polynomials $P(n)$ and $Q(n)$ such that $\frac{1}{P(n)} \leq \frac{n}{\log n} \leq Q(n)$ for all sufficiently large $n$.

(3) **Lower Bound:** Consider $P(n) = \log^2 n$. Then $\frac{1}{P(n)} = \frac{1}{\log^2 n}$. For sufficiently large $n$, $\frac{1}{\log^2 n} \leq \frac{n}{\log n}$.
**Upper Bound:** Consider $Q(n) = n^2$. Then $Q(n) = n^2$. Clearly, $\frac{n}{\log n} \leq n^2$ for all sufficiently large $n$.
Thus, $\frac{1}{P(n)} \leq f(n) \leq Q(n)$ holds, making $f(n) = \frac{n}{\log n}$ a **noticeable** function.

The following facts about negligible and noticeable functions are easy to derive:

- $f(n) = \text{poly}_1(n) \cdot \text{poly}_2(n)$ is a polynomial.
- $f(n) = \text{notice}_1(n) \cdot \text{notice}_2(n)$ is noticeable.
- $f(n) = \text{notice}(n) \cdot \text{negl}(n)$ is negligible.
- $f(n) = \text{negl}_1(n) \cdot \text{negl}_2(n)$ is negligible.
- $f(n) = \text{notice}_1(n) + \text{notice}_2(n)$ is noticeable.
- $f(n) = \text{notice}(n) + \text{negl}(n)$ is noticeable.
- $f(n) = \text{negl}_1(n) + \text{negl}_2(n)$ is negligible.
- $f(n) = c \cdot \text{notice}(n)$ is noticeable for constant $c$.
- $f(n) = c \cdot \text{negl}(n)$ is negligible for constant $c$.

## 8.1. ONE-WAY FUNCTIONS.

**Definition 8.12** ( Strong One-way Functions)**.** A function $f : \{0,1\}^n \to \{0,1\}^m$ is a one-way function if the following conditions hold:

(1) $f$ runs in polynomial time. Equivalently, the computation of $f(x)$ is polynomial time for all $x$.
(2) For all probabilistic polynomial-time (PPT) adversaries $A$, there exists a negligible function $\text{negl}(n)$ such that for all large enough $n$, we have

$$\Pr[f(x) = f(x') : x \xleftarrow{\$} \{0,1\}^n, x' \xleftarrow{\$} A(f(x))] \leq \text{negl}(n),$$

where $x$ is uniformly sampled from $\{0,1\}^n$ and $x'$ is the output of $A$ given $f(x)$.

**Remark 8.2.** Here, $f(x)$ is called the image of $x$, and $x$ is called the preimage of $f(x)$. We can easily extend this definition to $f : D \to R$ for any domain $D$ and range $R$. Moreover,

we can either view the domain $D$ as a set from which the input is sampled randomly, or as a distribution.

There is an important subtlety to this definition: in the second condition, we require that the probability of any adversary finding any preimage is negligible. It might be tempting to change the second condition to:

$$\Pr[x = x' : x \xleftarrow{\$} \{0,1\}^n, x' \xleftarrow{\$} A(f(x))] \leq \text{negl}(n)$$

However, this modified definition is not very useful. To see that, consider the function $f$ such that $f(x) = 0$ for all $x$. Then $f$ is an OWF under this definition, but it is intuitively useless for cryptographic purposes. Therefore, we strengthen condition 2 to the above definition.

**Definition 8.13** (Weak one-way functions)**. (Weak OWF).** A function $f : \{0,1\}^n \to \{0,1\}^m$ is a weak one-way function if the following holds:

(1) $f$ runs in polynomial time. Equivalently, the computation of $f(x)$ is polynomial time for all $x$.
(2) For all PPT adversaries $A$, there exists a noticeable function notice$(n)$ such that for all large enough $n$, we have

$$\Pr[f(x) = f(x') : x \xleftarrow{\$} \{0,1\}^n, x' \xleftarrow{\$} A(f(x))] \leq 1 - \text{notice}(n).$$

Intuitively, a weak one-way function should be hard to invert on some noticeable fraction of inputs.

**Definition 8.14.** A function $f : D \to R$ is an injective one-way function if it satisfies the following conditions:

(1) $f$ is a one-way function, meaning it is easy to compute but hard to invert on average.
(2) $f$ is injective, meaning that for every pair of distinct elements $x_1, x_2 \in D$, we have $f(x_1) \neq f(x_2)$.

Injective one-way functions are also known as one-to-one one-way functions.

**Remark 8.3.** An injective function (also known as one-to-one function) is a function that maps distinct elements of its domain to distinct elements of its range

**Definition 8.15** (one-way permutation)**.** A function $f : D \to R$ is a *one-way permutation (OWP)* if $f$ is an injective one-way function and $f$ is a permutation (i.e., $D = R$).

Unfortunately, one-way functions only satisfy a weak sense of security. They only guarantee that the input to the function $f$ is not leaked entirely, but it is still possible that a substantial amount of information is leaked. In fact, the following statement is true:

**Proposition 8.1.** Given a one-way function $f : \{0,1\}^n \to \{0,1\}^n$, we can build another one-way function $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$, such that $g$ leaks half of its input.

*Proof.* **Proof.** Let $||$ denote concatenation. Consider the following definition of $g$: given input $x_1||x_2$, where $|x_1| = |x_2| = n$, output $f(x_1)||x_2$. It suffices for us to argue that $g$ is a one-way function.

Assume for the sake of contradiction that there is an adversary $A$ that inverts $g$ with a noticeable probability. We construct an adversary $B$ that inverts $f$ with noticeable probability. Consider the following algorithm:

(1) Given $f(x)$, construct $y = f(x)||t$, where $t$ is a random number from $\{0,1\}^n$.
(2) Run $A(y)$.
(3) If $A$ halts without failing, return the first $n$ bits of $A(y)$'s output.

(4) Otherwise, return FAIL.

Now it is easy to see that $B$ succeeds as long as $A$ succeeds. Since $A$ has a noticeable probability of success, $B$ has a noticeable probability of success, which implies $f$ is not a one-way function, leading to a contradiction. Therefore $g$ is a one-way function. □

**Theorem 8.2.** If P = NP, then one-way functions do not exist.

*Proof.* If P = NP, then one-way functions do not exist.
Sketch of the Proof: Assume for the sake of contradiction that there exists a one-way function $f : D \to R$. Then, since $f$ can be computed in polynomial time, inverting $f$ is in NP because, given a preimage, it takes polynomial time to check its validity. Assuming P = NP, finding a preimage for $f$ could be computed in polynomial time, which means $f$ is not a one-way function, leading to a contradiction.
Detailed Proof:
Assume that P = NP and that there exists a one-way function $f : D \to R$. By the definition of a one-way function, $f$ satisfies the following properties:

- $f$ is easy to compute: There exists a polynomial-time algorithm that, given any input $x \in D$, computes $f(x)$.
- $f$ is hard to invert: For every polynomial-time algorithm $A$ and every polynomial $p(n)$, the probability that $A$ outputs a preimage of $f(x)$ (i.e., some $x'$ such that $f(x') = f(x)$) is negligible for large $n$ when $x$ is chosen uniformly at random from $D$.

However, if P = NP, then any problem in NP can be solved in polynomial time. In particular, consider the following decision problem: Given $y \in R$ and $x' \in D$, does $f(x') = y$? This problem is in NP because, given $x'$ and $y$, we can check in polynomial time whether $f(x') = y$.
Now, if P = NP, then there exists a polynomial-time algorithm $B$ that solves this problem. That is, $B$ can find, for any given $y$, an $x'$ such that $f(x') = y$, provided such an $x'$ exists. This means that inverting $f$ can also be done in polynomial time, as we can use $B$ to find a preimage $x'$ of any given $y = f(x)$.
This conclusion contradicts the assumption that $f$ is a one-way function, as $f$ would no longer be hard to invert. Therefore, if P = NP, one-way functions cannot exist.

□

## 8.2. CONSTRUCTING ONE-WAY FUNCTIONS.

Assumption 1 (Factoring Assumption).
Define $P_n = \{p : p \text{ is prime and } p \leq 2^n\}$ as the set of all $n$-bit prime numbers. Then for all PPT algorithms $A$:

$$\Pr[A(N) = (p, q) : p \xleftarrow{\$} P_n, q \xleftarrow{\$} P_n, N = p \cdot q] \leq \text{negl}(n).$$

**Theorem 8.3.** (Chebyshev's Theorem). Let $p$ be an $n$-bit number chosen uniformly at random. Then $\Pr[p \text{ is prime}] \geq \frac{1}{2n}$.