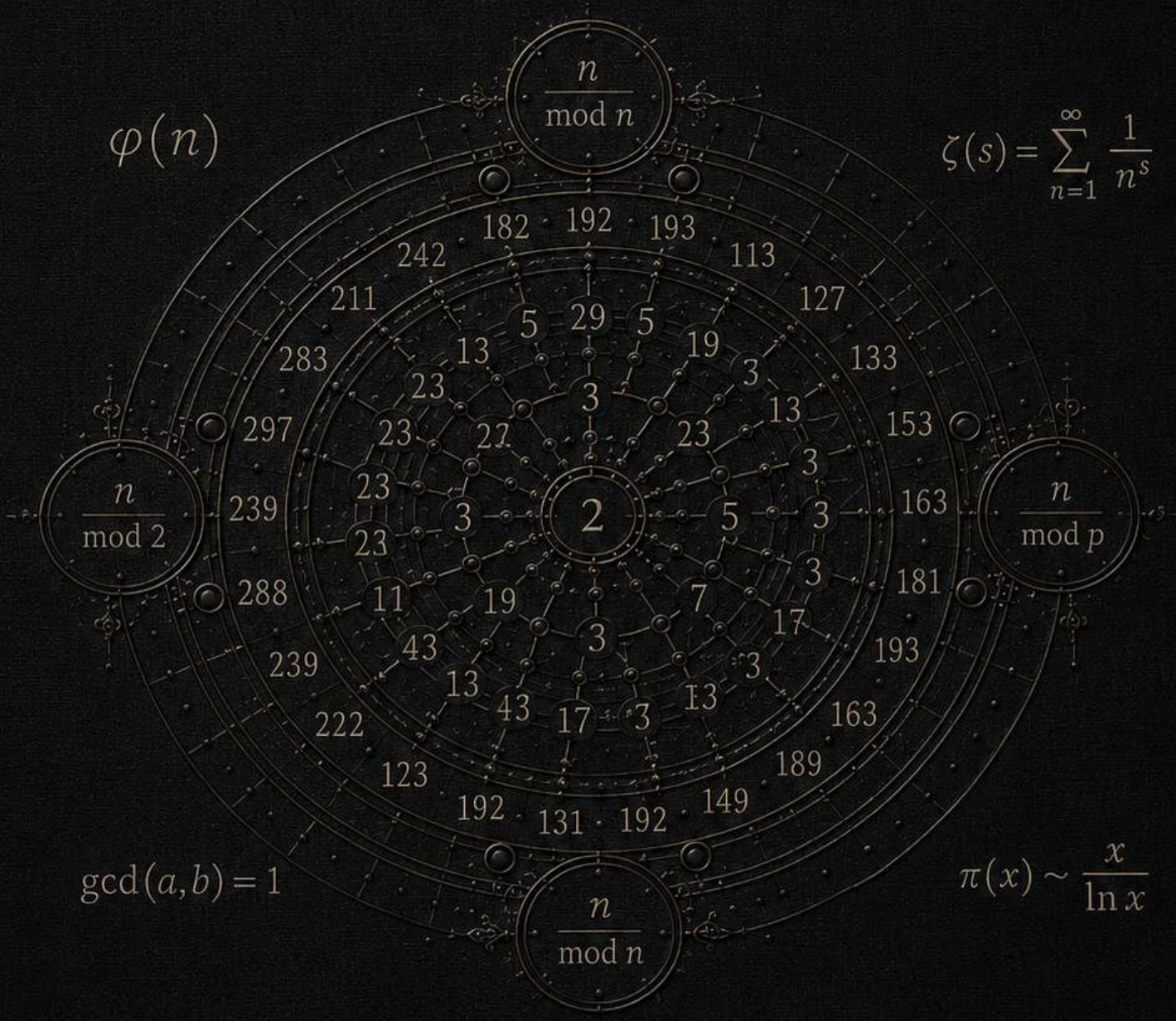
Number Theory

BS / ADP MATHEMATICS



SOHAIB HASAN

HEAD OF DEPARTMENT, MATHEMATICS

HORIZON COLLEGE CHAKWAL

@plotlab01 | sohaibhassan199@gmail.com | +92-333-5904314

Contents

Chapter 1

Divisibility Theory

Division Algorithm (Euclid's Theorem)

Division Algorithm

For integers a and b such that $b > 0$, there exist **unique** integers q (quotient) and r (remainder) such that:

$$a = bq + r \quad \text{where} \quad 0 \leq r < b$$

Key Points:

- a is called the **dividend**
- b is called the **divisor**
- q is called the **quotient**
- r is called the **remainder**
- The remainder r is always non-negative and strictly less than the divisor b

Example 1: Positive Dividend

Find the quotient and remainder when $a = 47$ is divided by $b = 5$.

Solution:

We need to express $47 = 5q + r$ where $0 \leq r < 5$.

Dividing: $47 \div 5 = 9$ with remainder 2

We can verify: $47 = 5(9) + 2 = 45 + 2$ ✓

Therefore: $q = 9$ and $r = 2$

Example 2: Negative Dividend

Find the quotient and remainder when $a = -23$ is divided by $b = 4$.

Solution:

We need to express $-23 = 4q + r$ where $0 \leq r < 4$.

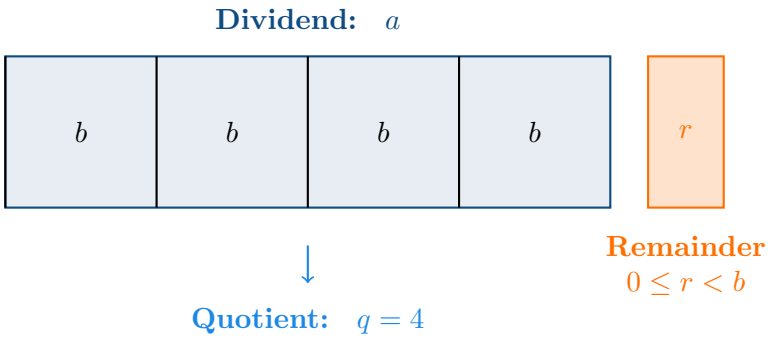
If we simply divide: $-23 \div 4 = -5.75$

Taking $q = -6$: $-23 = 4(-6) + r$

$$-23 = -24 + r \implies r = 1$$

Verification: $4(-6)+1=-24+1=-23$ ✓
Therefore: $q=-6$ and $r=1$
⚠ **Important:** Note that $q=-5, r=-3$ is **incorrect** because the remainder must satisfy $0 \leq r < 4$.

Visual Representation



Theorem Statement: Division Algorithm

For integers a, b with $b > 0$, there exist **unique** integers q and r such that:

$$\boxed{a = bq + r \quad \text{where} \quad 0 \leq r < b}$$

This theorem guarantees:

- **Existence:** Such integers q and r always exist
- **Uniqueness:** These integers q and r are unique (only one such pair)

Proof of Division Algorithm

Statement: For integers a, b with $b > 0$, there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.

Proof (Existence):
Consider the set $S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$
This set S is non-empty because:

- If $a \geq 0$, take $k = 0$, then $a - b(0) = a \in S$
- If $a < 0$, take $k = a$ (since $b > 0$), then $a - ba = a(1-b) \geq 0$ for sufficiently negative k

Since S is a non-empty set of non-negative integers, by the **Well-Ordering Principle**, S has a smallest element. Let r be this smallest element.
Then $r = a - bq$ for some $q \in \mathbb{Z}$, which gives us:

$$a = bq + r$$

We need to show $0 \leq r < b$:

- Since $r \in S$, we have $r \geq 0$ by definition
- Suppose $r \geq b$. Then:

$$r - b = (a - bq) - b = a - b(q + 1) \geq 0$$

  This means $r - b \in S$, but $r - b < r$, contradicting that r is the smallest element of S.

- Therefore, $r < b$

Hence, $0 \leq r < b$. **Existence proved.**

Proof (Uniqueness):
Suppose there exist two representations:

$$a = bq_1 + r_1 \quad \text{where} \quad 0 \leq r_1 < b$$

$$a = bq_2 + r_2 \quad \text{where} \quad 0 \leq r_2 < b$$

Subtracting these equations:

$$0 = b(q_1 - q_2) + (r_1 - r_2)$$

$$b(q_2 - q_1) = r_1 - r_2$$

Since $0 \leq r_1 < b$ and $0 \leq r_2 < b$, we have:

$$-b < r_1 - r_2 < b$$

But $r_1 - r_2 = b(q_2 - q_1)$ is a multiple of b.
The only multiple of b in the interval $(-b, b)$ is 0.
Therefore: $r_1 - r_2 = 0 \implies r_1 = r_2$
And: $b(q_2 - q_1) = 0 \implies q_1 = q_2$ (since $b \neq 0$)
Thus, q and r are **unique**. **Uniqueness proved.** □

Corollary Statement

For integers a and b such that $b \neq 0$, there exist **unique** integers q and r such that:

$$\boxed{a = bq + r \quad \text{where} \quad 0 \leq r < |b|}$$

Key Difference from Division Algorithm:

- The divisor b can now be **negative** (not just positive)
- The remainder condition uses $|b|$ (absolute value of b) instead of just b
- If $b > 0$, this reduces to the standard Division Algorithm
- If $b < 0$, we use $|b| = -b$ as the bound for the remainder

Example 3: Divisor is Negative

Find the quotient and remainder when $a = 17$ is divided by $b = -5$.

Solution:

We need to express $17 = -5q + r$ where $0 \leq r < |-5| = 5$.

Method: First apply division algorithm with positive divisor:

$$17 = 5(3) + 2$$

Now adjust for negative divisor:

$$17 = (-5)(-3) + 2 = 15 + 2$$

Verification: $(-5)(-3) + 2 = 15 + 2 = 17$ ✓

And $0 \leq 2 < 5$ ✓

Therefore: $q = -3$ and $r = 2$

Example 4: Both Negative

Find the quotient and remainder when $a = -28$ is divided by $b = -7$.

Solution:

We need to express $-28 = -7q + r$ where $0 \leq r < |-7| = 7$.

Dividing: $-28 \div (-7) = 4$ exactly

So: $-28 = (-7)(4) + 0$

Verification: $(-7)(4) + 0 = -28 + 0 = -28$ ✓

And $0 \leq 0 < 7$ ✓

Therefore: $q = 4$ and $r = 0$

Applications of Division Algorithm

Classification of Integers by Remainders

Key Concept:

When dividing any integer by n, the possible remainders are: $0, 1, 2, 3, \ldots, n-1$

This means every integer can be written in one of n forms:

$$nq, \quad nq+1, \quad nq+2, \quad \ldots, \quad nq+(n-1)$$

This is the foundation of **modular arithmetic** and helps us prove many divisibility properties.

Problem 1

Theorem Statement

Show that $\frac{a(a^2+2)}{3}$ is an integer.

Solution: Proving $3|a(a^2+2)$

Given: a is a positive integer
To Prove: $\frac{a(a^2+2)}{3}$ is an integer, i.e., $3|a(a^2+2)$ **Proof:**

By Division Algorithm, any integer a can be written as:

$$a = 3q + r \quad \text{where} \quad r \in \{0, 1, 2\}$$

So we have three cases:
Case 1: $a = 3q$ (i.e., $r = 0$)

$$a(a^2+2) = 3q((3q)^2+2) = 3q(9q^2+2) = 3[q(9q^2+2)]$$

This is clearly divisible by 3. ✓
Case 2: $a = 3q+1$ (i.e., $r = 1$)

$$\begin{aligned} a^2+2 &= (3q+1)^2+2 \\ &= 9q^2+6q+1+2 \\ &= 9q^2+6q+3 \\ &= 3(3q^2+2q+1) \end{aligned}$$

Therefore:

$$a(a^2+2) = (3q+1)\cdot 3(3q^2+2q+1) = 3[(3q+1)(3q^2+2q+1)]$$

This is divisible by 3. ✓
Case 3: $a = 3q+2$ (i.e., $r = 2$)

$$\begin{aligned} a^2+2 &= (3q+2)^2+2 \\ &= 9q^2+12q+4+2 \\ &= 9q^2+12q+6 \\ &= 3(3q^2+4q+2) \end{aligned}$$

Therefore:

$$a(a^2+2) = (3q+2)\cdot 3(3q^2+4q+2) = 3[(3q+2)(3q^2+4q+2)]$$

This is divisible by 3. ✓

Conclusion: In all three cases, $3|a(a^2+2)$, hence $\frac{a(a^2+2)}{3}$ is an integer. □

Problem 2: Squares of Integers

Theorem Statement

The square of any integer is either of the form $4k$ or $4k+1$ for some integer k.
In other words: $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

Proof: Form of Perfect Squares

To Prove: For any integer n, n^2 is of the form $4k$ or $4k+1$.

Proof:
By Division Algorithm, any integer n can be written as:

$$n = 4q + r \quad \text{where} \quad r \in \{0, 1, 2, 3\}$$

We examine each case:
Case 1: $n = 4q$ (even, divisible by 4)

$$n^2 = (4q)^2 = 16q^2 = 4(4q^2)$$

This is of the form $4k$ where $k = 4q^2$. ✓
Case 2: $n = 4q + 1$ (odd)

$$n^2 = (4q+1)^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1$$

This is of the form $4k+1$ where $k = 4q^2 + 2q$. ✓
Case 3: $n = 4q + 2$ (even, not divisible by 4)

$$n^2 = (4q+2)^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1)$$

This is of the form $4k$ where $k = 4q^2 + 4q + 1$. ✓
Case 4: $n = 4q + 3$ (odd)

$$n^2 = (4q+3)^2 = 16q^2 + 24q + 9 = 16q^2 + 24q + 8 + 1 = 4(4q^2 + 6q + 2) + 1$$

This is of the form $4k+1$ where $k = 4q^2 + 6q + 2$. ✓

Conclusion: In all cases, n^2 is either $4k$ or $4k+1$.
⚠ **Important Note:** No perfect square can be of the form $4k+2$ or $4k+3$. □

Problem 3: Squares Modulo 3

Theorem Statement

The square of any integer is either of the form $3k$ or $3k+1$ for some integer k.
In other words: $n^2 \equiv 0 \pmod 3$ or $n^2 \equiv 1 \pmod 3$

Proof: Squares Modulo 3

To Prove: For any integer n, n^2 is of the form $3k$ or $3k+1$.

Proof:
By Division Algorithm, any integer n can be written as:

$$n = 3q + r \quad \text{where} \quad r \in \{0, 1, 2\}$$

We examine each case:
Case 1: $n = 3q$ (divisible by 3)

$$n^2 = (3q)^2 = 9q^2 = 3(3q^2)$$

This is of the form $3k$ where $k = 3q^2$. ✓
Case 2: $n = 3q + 1$

$$n^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$$

This is of the form $3k + 1$ where $k = 3q^2 + 2q$. ✓
Case 3: $n = 3q + 2$

$$n^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1$$

This is of the form $3k + 1$ where $k = 3q^2 + 4q + 1$. ✓

Conclusion: In all cases, n^2 is either $3k$ or $3k + 1$.
⚠ **Important Note:** No perfect square can be of the form $3k + 2$. □

Problem 4: Cubes Modulo 9

Theorem Statement

The cube of any integer is of the form $9k$, $9k + 1$, or $9k + 8$ for some integer k.
In other words: $n^3 \equiv 0, 1, \text{ or } 8 \pmod 9$

Proof: Cubes Modulo 9

To Prove: For any integer n, n^3 is of the form $9k$, $9k + 1$, or $9k + 8$.

Proof:
By Division Algorithm, any integer n can be written as:

$$n = 3q + r \quad \text{where} \quad r \in \{0, 1, 2\}$$

We examine each case:
Case 1: $n = 3q$ (divisible by 3)

$$n^3 = (3q)^3 = 27q^3 = 9(3q^3)$$

This is of the form $9k$ where $k = 3q^3$. ✓
Case 2: $n = 3q + 1$

$$\begin{aligned} n^3 &= (3q+1)^3 \\ &= (3q)^3 + 3(3q)^2(1) + 3(3q)(1)^2 + 1^3 \\ &= 27q^3 + 27q^2 + 9q + 1 \\ &= 9(3q^3 + 3q^2 + q) + 1 \end{aligned}$$

This is of the form $9k + 1$ where $k = 3q^3 + 3q^2 + q$. ✓
Case 3: $n = 3q + 2$

$$\begin{aligned} n^3 &= (3q+2)^3 \\ &= (3q)^3 + 3(3q)^2(2) + 3(3q)(2)^2 + 2^3 \\ &= 27q^3 + 54q^2 + 36q + 8 \\ &= 9(3q^3 + 6q^2 + 4q) + 8 \end{aligned}$$

This is of the form $9k+8$ where $k = 3q^3 + 6q^2 + 4q$. ✓

Conclusion: In all cases, n^3 is of the form $9k$, $9k+1$, or $9k+8$. □

Problem 5: Cubes Modulo 7

Theorem Statement

The cube of any integer is of the form $7k$ or $7k \pm 1$ for some integer k.
In other words: $n^3 \equiv 0, 1, \text{ or } -1 \pmod 7$

Proof: Cubes Modulo 7

To Prove: For any integer n, n^3 is of the form $7k$, $7k+1$, or $7k-1$ (i.e., $7k+6$).

Proof:
By Division Algorithm, any integer n can be written as:

$$n = 7q + r \quad \text{where} \quad r \in \{0, 1, 2, 3, 4, 5, 6\}$$

We examine each case:
Case 1: $n = 7q$

$$n^3 = (7q)^3 = 343q^3 = 7(49q^3)$$

Form: $7k$ where $k = 49q^3$. ✓
Case 2: $n = 7q + 1$

$$n^3 = (7q+1)^3 = 343q^3 + 147q^2 + 21q + 1 = 7(49q^3 + 21q^2 + 3q) + 1$$

Form: $7k+1$ where $k = 49q^3 + 21q^2 + 3q$. ✓
Case 3: $n = 7q + 2$

$$n^3 = (7q+2)^3 = 343q^3 + 294q^2 + 84q + 8 = 7(49q^3 + 42q^2 + 12q + 1) + 1$$

Form: $7k+1$ where $k = 49q^3 + 42q^2 + 12q + 1$. ✓
Case 4: $n = 7q + 3$

$$\begin{aligned} n^3 = (7q+3)^3 &= 343q^3 + 441q^2 + 189q + 27 \\ &= 343q^3 + 441q^2 + 189q + 21 + 6 \\ &= 7(49q^3 + 63q^2 + 27q + 3) + 6 \end{aligned}$$

Form: $7k + 6 = 7k - 1$ where $k = 49q^3 + 63q^2 + 27q + 3$. ✓
Case 5: $n = 7q + 4$

$$\begin{aligned} n^3 = (7q+4)^3 &= 343q^3 + 588q^2 + 336q + 64 \\ &= 343q^3 + 588q^2 + 336q + 63 + 1 \\ &= 7(49q^3 + 84q^2 + 48q + 9) + 1 \end{aligned}$$

Form: $7k+1$ where $k = 49q^3 + 84q^2 + 48q + 9$. ✓
Case 6: $n = 7q + 5$

$$\begin{aligned} n^3 = (7q+5)^3 &= 343q^3 + 735q^2 + 525q + 125 \\ &= 343q^3 + 735q^2 + 525q + 119 + 6 \\ &= 7(49q^3 + 105q^2 + 75q + 17) + 6 \end{aligned}$$

Form: $7k+6 = 7k-1$ where $k = 49q^3 + 105q^2 + 75q + 17$. ✓

Case 7: $n = 7q+6$

$$\begin{aligned} n^3 = (7q+6)^3 &= 343q^3 + 882q^2 + 756q + 216 \\ &= 343q^3 + 882q^2 + 756q + 210 + 6 \\ &= 7(49q^3 + 126q^2 + 108q + 30) + 6 \end{aligned}$$

Form: $7k+6 = 7k-1$ where $k = 49q^3 + 126q^2 + 108q + 30$. ✓

Conclusion: In all cases, n^3 is of the form $7k$, $7k+1$, or $7k-1$. □

Problem 6: Sum Formula Divisibility

Theorem Statement

For $n \geq 1$, $\frac{n(n+1)(2n+1)}{6}$ is an integer.

Proof

Proof:

By Division Algorithm, any integer n can be written as:

$$n = 6q + r \quad \text{where} \quad r \in \{0, 1, 2, 3, 4, 5\}$$

We need to show that $6 | n(n+1)(2n+1)$ for all cases.

Case 1: $n = 6q$

$$n(n+1)(2n+1) = 6q(6q+1)(12q+1) = 6[q(6q+1)(12q+1)]$$

Divisible by 6. ✓

Case 2: $n = 6q+1$

$$\begin{aligned} n(n+1)(2n+1) &= (6q+1)(6q+2)(12q+3) \\ &= (6q+1) \cdot 2(3q+1) \cdot 3(4q+1) \\ &= 6(6q+1)(3q+1)(4q+1) \end{aligned}$$

Divisible by 6. ✓

Case 3: $n = 6q+2$

$$\begin{aligned} n(n+1)(2n+1) &= (6q+2)(6q+3)(12q+5) \\ &= 2(3q+1) \cdot 3(2q+1)(12q+5) \\ &= 6(3q+1)(2q+1)(12q+5) \end{aligned}$$

Divisible by 6. ✓

Case 4: $n = 6q+3$

$$\begin{aligned} n(n+1)(2n+1) &= (6q+3)(6q+4)(12q+7) \\ &= 3(2q+1) \cdot 2(3q+2)(12q+7) \\ &= 6(2q+1)(3q+2)(12q+7) \end{aligned}$$

Divisible by 6. ✓

Case 5: $n = 6q + 4$

$$\begin{aligned} n(n+1)(2n+1) &= (6q+4)(6q+5)(12q+9) \\ &= 2(3q+2)(6q+5) \cdot 3(4q+3) \\ &= 6(3q+2)(6q+5)(4q+3) \end{aligned}$$

Divisible by 6. ✓
Case 6: $n = 6q + 5$

$$\begin{aligned} n(n+1)(2n+1) &= (6q+5)(6q+6)(12q+11) \\ &= (6q+5) \cdot 6(q+1)(12q+11) \\ &= 6(6q+5)(q+1)(12q+11) \end{aligned}$$

Divisible by 6. ✓
Therefore, $\frac{n(n+1)(2n+1)}{6}$ is always an integer. □

Example 5: Verification

Verify that $\frac{n(n+1)(2n+1)}{6}$ is an integer for $n = 5$.
Solution:

$$\frac{5(5+1)(2 \cdot 5+1)}{6} = \frac{5 \cdot 6 \cdot 11}{6} = \frac{330}{6} = 55$$

Yes, 55 is an integer. ✓
Note: This formula gives the sum of squares: $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Problem 7: Odd Integer Squares

Theorem Statement

The square of any odd integer is of the form $8k + 1$ for some integer k.

Proof

Proof:
Any odd integer can be written as $n = 2m + 1$ for some integer m.
By Division Algorithm, m can be written as:

$$m = 4q + r \quad \text{where} \quad r \in \{0, 1, 2, 3\}$$

So $n = 2m + 1 = 2(4q + r) + 1 = 8q + 2r + 1$
Now we square n:
Case 1: $r = 0$, so $n = 8q + 1$

$$n^2 = (8q+1)^2 = 64q^2 + 16q + 1 = 8(8q^2 + 2q) + 1$$

Form: $8k + 1$ where $k = 8q^2 + 2q$. ✓
Case 2: $r = 1$, so $n = 8q + 3$

$$n^2 = (8q+3)^2 = 64q^2 + 48q + 9 = 64q^2 + 48q + 8 + 1 = 8(8q^2 + 6q + 1) + 1$$

Form: $8k+1$ where $k = 8q^2 + 6q + 1$. ✓
Case 3: $r = 2$, so $n = 8q + 5$

$$n^2 = (8q+5)^2 = 64q^2 + 80q + 25 = 64q^2 + 80q + 24 + 1 = 8(8q^2 + 10q + 3) + 1$$

Form: $8k+1$ where $k = 8q^2 + 10q + 3$. ✓
Case 4: $r = 3$, so $n = 8q + 7$

$$n^2 = (8q+7)^2 = 64q^2 + 112q + 49 = 64q^2 + 112q + 48 + 1 = 8(8q^2 + 14q + 6) + 1$$

Form: $8k+1$ where $k = 8q^2 + 14q + 6$. ✓
In all cases, $n^2 = 8k + 1$. □

Example 6: Verification

Verify that squares of odd numbers are of the form $8k+1$.
Solution:

- $1^2 = 1 = 8(0) + 1$ ✓
- $3^2 = 9 = 8(1) + 1$ ✓
- $5^2 = 25 = 8(3) + 1$ ✓
- $7^2 = 49 = 8(6) + 1$ ✓
- $9^2 = 81 = 8(10) + 1$ ✓

Problem 8: Divisibility by 3

Theorem Statement

For all $n \in \mathbb{Z}$, $3 | n(n^2+2)$.

Proof

Proof:
By Division Algorithm:

$$n = 3q + r \quad \text{where} \quad r \in \{0, 1, 2\}$$

Case 1: $n = 3q$

$$n(n^2+2) = 3q((3q)^2 + 2) = 3q(9q^2 + 2) = 3[q(9q^2 + 2)]$$

Divisible by 3. ✓
Case 2: $n = 3q + 1$

$$n^2 + 2 = (3q+1)^2 + 2 = 9q^2 + 6q + 1 + 2 = 9q^2 + 6q + 3 = 3(3q^2 + 2q + 1)$$

$$n(n^2+2) = (3q+1) \cdot 3(3q^2 + 2q + 1) = 3[(3q+1)(3q^2 + 2q + 1)]$$

Divisible by 3. ✓

Case 3: $n = 3q + 2$

$$n^2 + 2 = (3q + 2)^2 + 2 = 9q^2 + 12q + 4 + 2 = 9q^2 + 12q + 6 = 3(3q^2 + 4q + 2)$$

$$n(n^2 + 2) = (3q + 2) \cdot 3(3q^2 + 4q + 2) = 3[(3q + 2)(3q^2 + 4q + 2)]$$

Divisible by 3. ✓
Therefore, $3|n(n^2 + 2)$ for all $n \in \mathbb{Z}$. □

Example 7: Verification

Verify $3|n(n^2 + 2)$ for $n = 7$.
Solution:

$$n(n^2 + 2) = 7(7^2 + 2) = 7(49 + 2) = 7(51) = 357$$

Check: $357 \div 3 = 119$ ✓
Yes, $3|357$.

Problem 9: Cubic Expression Divisibility

Theorem Statement

For all $n \in \mathbb{Z}$, $3|4n^3 - n$.

Proof

Proof:
We can factor: $4n^3 - n = n(4n^2 - 1) = n(2n - 1)(2n + 1)$
This is the product of three consecutive terms: $(2n - 1), n, (2n + 1)$ are not consecutive, but we analyze differently.
By Division Algorithm:

$$n = 3q + r \quad \text{where} \quad r \in \{0, 1, 2\}$$

Case 1: $n = 3q$

$$4n^3 - n = n(4n^2 - 1) = 3q(4(3q)^2 - 1) = 3q(36q^2 - 1) = 3[q(36q^2 - 1)]$$

Divisible by 3. ✓
Case 2: $n = 3q + 1$

$$\begin{aligned} 4n^2 - 1 &= 4(3q + 1)^2 - 1 = 4(9q^2 + 6q + 1) - 1 \\ &= 36q^2 + 24q + 4 - 1 = 36q^2 + 24q + 3 = 3(12q^2 + 8q + 1) \end{aligned}$$

$$4n^3 - n = (3q + 1) \cdot 3(12q^2 + 8q + 1) = 3[(3q + 1)(12q^2 + 8q + 1)]$$

Divisible by 3. ✓
Case 3: $n = 3q + 2$

$$\begin{aligned} 4n^2 - 1 &= 4(3q + 2)^2 - 1 = 4(9q^2 + 12q + 4) - 1 \\ &= 36q^2 + 48q + 16 - 1 = 36q^2 + 48q + 15 = 3(12q^2 + 16q + 5) \end{aligned}$$

$$4n^3 - n = (3q+2) \cdot 3(12q^2 + 16q + 5) = 3[(3q+2)(12q^2 + 16q + 5)]$$

Divisible by 3. ✓
Therefore, $3|4n^3 - n$ for all $n \in \mathbb{Z}$. □

Example 8: Verification

Verify $3|4n^3 - n$ for $n = 5$.
Solution:

$$4n^3 - n = 4(5)^3 - 5 = 4(125) - 5 = 500 - 5 = 495$$

Check: $495 \div 3 = 165$ ✓
Yes, $3|495$.

Problem 10: Consecutive Integers

Theorem Statement

The product of two consecutive integers is divisible by 2.

Proof

Proof:
Let the two consecutive integers be n and $n+1$.
By Division Algorithm:

$$n = 2q + r \quad \text{where} \quad r \in \{0, 1\}$$

Case 1: $n = 2q$ (even)

$$n(n+1) = 2q(2q+1) = 2[q(2q+1)]$$

Divisible by 2. ✓
Case 2: $n = 2q + 1$ (odd)

$$n + 1 = 2q + 1 + 1 = 2q + 2 = 2(q+1)$$

$$n(n+1) = (2q+1) \cdot 2(q+1) = 2[(2q+1)(q+1)]$$

Divisible by 2. ✓
Therefore, the product of two consecutive integers is always divisible by 2. □

Example 9: Verification

Show that the product of consecutive integers is even.
Solution:

- $3 \times 4 = 12 = 2(6)$ ✓
- $7 \times 8 = 56 = 2(28)$ ✓

- $10 \times 11 = 110 = 2(55)$ ✓
- $15 \times 16 = 240 = 2(120)$ ✓

Divisibility

Definition: Divisibility

An integer a is said to be **divisible** by an integer $b \neq 0$ if there exists an integer c such that:

$$a = bc$$

Notation: We write $b|a$ (read as "b divides a").

Terminology:

- b is called a **divisor** or **factor** of a
- a is called a **multiple** of b
- If $b \nmid a$, we say "b does not divide a"

Example 10: Understanding Divisibility

Determine which of the following statements are true:

Solution:

1. $3|12$: True, because $12 = 3 \times 4$ ✓
2. $5|20$: True, because $20 = 5 \times 4$ ✓
3. $7|30$: False, because $30 = 7 \times 4 + 2$ (no integer c exists) ×
4. $-4|12$: True, because $12 = (-4) \times (-3)$ ✓
5. $6|0$: True, because $0 = 6 \times 0$ ✓
6. $0|5$: False, because we cannot write $5 = 0 \times c$ for any c ×

Example 11: Finding Divisors

Find all positive divisors of 24.

Solution:

We need to find all positive integers d such that $d|24$.

Testing systematically:

$$24 = 1 \times 24$$
$$24 = 2 \times 12$$
$$24 = 3 \times 8$$
$$24 = 4 \times 6$$

Therefore, the positive divisors of 24 are: $\boxed{1, 2, 3, 4, 6, 8, 12, 24}$

Properties of Divisibility

Theorem: Properties of Divisibility

For integers a, b, c (where applicable):

(a) $a|0$, $1|a$, $a|a$

(b) $a|1 \iff a = \pm 1$

(c) If $a|b$ and $b|a$, then $a = \pm b$

(d) If $a|b$ and $c|d$, then $ac|bd$

(e) If $a|b$ and $b|c$, then $a|c$ (Transitivity)

(f) If $a|b$ and $a|c$, then $a|bc$ and $a|(b+c)$

(g) If $a|b$ and $a|c$, then $a|(bx+cy)$ for all $x, y \in \mathbb{Z}$

(h) If $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$

(i) If $a|b$ and $a|c$, then $a^2|bc$

(j) $a|b \iff ac|bc$ for $c \neq 0$

Proof of Property (a)

Proof:

Part 1: $a|0$
We need to show $0 = a \cdot c$ for some integer c.
Take $c = 0$. Then $0 = a \cdot 0$ for any integer a.
Therefore, $a|0$. ✓

Part 2: $1|a$
We need to show $a = 1 \cdot c$ for some integer c.
Take $c = a$. Then $a = 1 \cdot a$.
Therefore, $1|a$. ✓

Part 3: $a|a$
We need to show $a = a \cdot c$ for some integer c.
Take $c = 1$. Then $a = a \cdot 1$.
Therefore, $a|a$. ✓ □

Proof of Property (b)

Proof:

Forward Direction ($\Rightarrow$): Assume $a|1$
Then $1 = a \cdot c$ for some integer c.
This means $ac = 1$.
The only integer solutions are: $a = 1, c = 1$ or $a = -1, c = -1$.
Therefore, $a = \pm 1$. ✓

Backward Direction ($\Leftarrow$): Assume $a = \pm 1$
If $a = 1$: $1 = 1 \cdot 1$, so $1|1$ ✓
If $a = -1$: $1 = (-1) \cdot (-1)$, so $-1|1$ ✓
Therefore, $a|1 \iff a = \pm 1$. □

Proof of Property (c)

Proof:
Given: $a|b$ and $b|a$
Since $a|b$, there exists integer m such that $b = am \quad \cdots (1)$
Since $b|a$, there exists integer n such that $a = bn \quad \cdots (2)$
Substituting (1) into (2):

$$a = bn = (am)n = amn$$

$$a = amn$$

If $a \neq 0$, divide both sides by a:

$$1 = mn$$

The only integer solutions are: $m = n = 1$ or $m = n = -1$.
If $m = n = 1$: From (1), $b = a(1) = a$
If $m = n = -1$: From (1), $b = a(-1) = -a$
Therefore, $a = \pm b$. □

Proof of Property (e)

Proof:
Given: $a|b$ and $b|c$
Since $a|b$, there exists integer m such that $b = am$
Since $b|c$, there exists integer n such that $c = bn$
Substituting $b = am$ into $c = bn$:

$$c = bn = (am)n = a(mn)$$

Since mn is an integer (product of integers), we have $c = a(mn)$.
Therefore, $a|c$. □

Example 12: Property (e) Application

Given $6|24$ and $24|72$, show that $6|72$.
Solution:
Since $6|24$: $24 = 6 \times 4$
Since $24|72$: $72 = 24 \times 3$
Substituting:

$$72 = 24 \times 3 = (6 \times 4) \times 3 = 6 \times (4 \times 3) = 6 \times 12$$

Therefore, $6|72$. ✓

Proof of Property (f)

Proof:
Given: $a|b$ and $a|c$
Since $a|b$, there exists integer m such that $b = am$
Since $a|c$, there exists integer n such that $c = an$
Adding these equations:

$$b + c = am + an = a(m + n)$$

Since $(m + n)$ is an integer, we have $b + c = a(m + n)$.
Therefore, $a|(b + c)$. □

Example 13: Property (f) Application

Given $7|35$ and $7|21$, show that $7|56$.
Solution:
We have: $35 = 7 \times 5$ and $21 = 7 \times 3$
Therefore:

$$35 + 21 = 7 \times 5 + 7 \times 3 = 7(5 + 3) = 7 \times 8 = 56$$

So $7|56$. ✓

Proof of Property (g)

Proof:
Given: $a|b$ and $a|c$, and $x, y \in \mathbb{Z}$
Since $a|b$, there exists integer m such that $b = am$
Since $a|c$, there exists integer n such that $c = an$
Consider $bx + cy$:

$$bx + cy = (am)x + (an)y = amx + any = a(mx + ny)$$

Since $mx + ny$ is an integer, we have $bx + cy = a(mx + ny)$.
Therefore, $a|(bx + cy)$. □

Example 14: Property (g) Application

Given $5|20$ and $5|15$, show that $5|(20 \times 3 + 15 \times 2)$.
Solution:
We have: $20 = 5 \times 4$ and $15 = 5 \times 3$
Calculate:

$$20 \times 3 + 15 \times 2 = (5 \times 4) \times 3 + (5 \times 3) \times 2$$

$$= 5 \times 12 + 5 \times 6 = 5(12 + 6) = 5 \times 18 = 90$$

Therefore, $5|90$. ✓

Proof of Property (j)

Proof:

Forward Direction ($\Rightarrow$): Assume $a|b$
Then $b = am$ for some integer m.
Multiply both sides by c:

$$bc = (am)c = (ac)m$$

Therefore, $ac|bc$. ✓

Backward Direction ($\Leftarrow$): Assume $ac|bc$
Then $bc = (ac)k$ for some integer k.
This gives: $bc = ack$
Since $c \neq 0$, divide both sides by c:

$$b = ak$$

Therefore, $a|b$. ✓ □

Example 15: Property (j) Application

Show that $3|12 \iff 15|60$.

Solution:

Here $a = 3$, $b = 12$, $c = 5$.
Forward: $3|12$ means $12 = 3 \times 4$
Multiply by 5: $60 = 15 \times 4$, so $15|60$ ✓
Backward: $15|60$ means $60 = 15 \times 4$
Divide by 5: $12 = 3 \times 4$, so $3|12$ ✓

Greatest Common Divisor (GCD)

Definition: Greatest Common Divisor

Let a and b be two integers, at least one of which is non-zero. The **greatest common divisor** (GCD) of a and b, denoted by $\gcd(a, b)$ or (a, b), is the largest positive integer d that satisfies:

(i) $d > 0$

(ii) $d|a$ and $d|b$

(iii) If $c|a$ and $c|b$, then $c|d$

Alternative Names:

- GCD is also called **Highest Common Factor (HCF)**
- Notation: $\gcd(a, b)$ or (a, b) or $\text{HCF}(a, b)$

Example 16: Finding GCD by Listing Divisors

Find $\gcd(24, 36)$.

Solution:

Divisors of 24: $1, 2, 3, 4, 6, 8, 12, 24$

Divisors of 36: $1, 2, 3, 4, 6, 9, 12, 18, 36$

Common divisors: $1, 2, 3, 4, 6, 12$

The greatest common divisor is: $\boxed{\gcd(24, 36) = 12}$ ✓

Example 17: Finding GCD by Prime Factorization

Find $\gcd(72, 108)$.

Solution:

Prime factorization:

$$72 = 2^3 \times 3^2$$
$$108 = 2^2 \times 3^3$$

Taking minimum powers of each prime:

$$\gcd(72, 108) = 2^{\min(3,2)} \times 3^{\min(2,3)} = 2^2 \times 3^2 = 4 \times 9 = 36$$

Therefore: $\boxed{\gcd(72, 108) = 36}$ ✓

Theorem: Existence and Uniqueness of GCD

Let a and b be two integers, at least one of which is non-zero. Then $\gcd(a, b)$ exists and is unique.

Proof: Existence and Uniqueness of GCD

Proof of Existence:

Consider the set $S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$

Since at least one of a, b is non-zero, S is non-empty.

By Well-Ordering Principle, S has a smallest element, say $d = ax_0 + by_0$ for some integers x_0, y_0.

We claim that $d = \gcd(a, b)$.

Step 1: Show $d|a$

By Division Algorithm: $a = dq + r$ where $0 \leq r < d$

Then:

$$r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q)$$

If $r > 0$, then $r \in S$ and $r < d$, contradicting that d is the smallest element of S.

Therefore, $r = 0$, so $a = dq$, hence $d|a$. ✓

Similarly, we can show $d|b$. ✓

Step 2: Show if $c|a$ and $c|b$, then $c|d$

If $c|a$ and $c|b$, then by property (g) of divisibility:

$$c|(ax_0 + by_0) = d$$

Therefore, $c|d$. ✓
Hence, $d = \gcd(a, b)$ exists.

Uniqueness:
Suppose d_1 and d_2 are both greatest common divisors of a and b.
Since d_1 is a GCD: $d_1|a$ and $d_1|b$
By property (iii) of GCD definition: $d_1|d_2$
Similarly, since d_2 is a GCD: $d_2|a$ and $d_2|b$
By property (iii) of GCD definition: $d_2|d_1$
Since $d_1|d_2$ and $d_2|d_1$, by property (c) of divisibility: $d_1 = \pm d_2$
Since both are positive (by definition), we have $d_1 = d_2$.
Therefore, GCD is unique. □

Theorem: Bezout's Identity

Let a and b be two integers, at least one of which is non-zero. Then there exist integers x and y such that:

$$\gcd(a, b) = ax + by$$

Example 18: Bezout's Identity Application

Express $\gcd(12, 18) = 6$ as a linear combination of 12 and 18.
Solution:
We need to find x and y such that $12x + 18y = 6$.
By inspection or trial:

$$12(2) + 18(-1) = 24 - 18 = 6$$

Therefore: $x = 2, y = -1$ ✓
Verification: $12(2) + 18(-1) = 24 - 18 = 6 = \gcd(12, 18)$ ✓
Note: The values of x and y are not unique. For example:

$$12(5) + 18(-3) = 60 - 54 = 6$$

Euclidean Algorithm

The Euclidean Algorithm
The Euclidean Algorithm is an efficient method to compute $\gcd(a, b)$ based on the following principle:
If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Lemma: GCD Property

If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof of Lemma

Proof:
Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$.
We need to show $d_1 = d_2$.
Step 1: Show $d_1 | d_2$
Since $d_1 = \gcd(a, b)$, we have $d_1 | a$ and $d_1 | b$.
From $a = bq + r$, we get $r = a - bq$.
By property (g) of divisibility: $d_1 | (a - bq) = r$
So $d_1 | b$ and $d_1 | r$, which means d_1 is a common divisor of b and r.
Therefore, $d_1 | \gcd(b, r) = d_2$. ✓
Step 2: Show $d_2 | d_1$
Since $d_2 = \gcd(b, r)$, we have $d_2 | b$ and $d_2 | r$.
From $a = bq + r$, by property (g): $d_2 | (bq + r) = a$
So $d_2 | a$ and $d_2 | b$, which means d_2 is a common divisor of a and b.
Therefore, $d_2 | \gcd(a, b) = d_1$. ✓
Since $d_1 | d_2$ and $d_2 | d_1$, and both are positive, we have $d_1 = d_2$.
Therefore, $\gcd(a, b) = \gcd(b, r)$. □

Example 19: Euclidean Algorithm

Find $\gcd(252, 105)$ using the Euclidean Algorithm.
Solution:
Apply Division Algorithm repeatedly:

$$\begin{aligned} 252 &= 105 \times 2 + 42 && \implies \gcd(252, 105) = \gcd(105, 42) \\ 105 &= 42 \times 2 + 21 && \implies \gcd(105, 42) = \gcd(42, 21) \\ 42 &= 21 \times 2 + 0 && \implies \gcd(42, 21) = \gcd(21, 0) = 21 \end{aligned}$$

Therefore: $\boxed{\gcd(252, 105) = 21}$ ✓

Example 20: GCD with Linear Combination

Find $\gcd(256, 1170)$ and express it as a linear combination $256x + 1170y$.
Solution:
Step 1: Apply Euclidean Algorithm

$$\begin{aligned} 1170 &= 256 \times 4 + 146 \\ 256 &= 146 \times 1 + 110 \\ 146 &= 110 \times 1 + 36 \\ 110 &= 36 \times 3 + 2 \\ 36 &= 2 \times 18 + 0 \end{aligned}$$

Therefore: $\gcd(256, 1170) = 2$

Step 2: Back Substitution (Extended Euclidean Algorithm)

$$\begin{aligned}
2 &= 110 - 36 \times 3 \\
&= 110 - (146 - 110 \times 1) \times 3 \\
&= 110 - 146 \times 3 + 110 \times 3 \\
&= 110 \times 4 - 146 \times 3 \\
&= (256 - 146 \times 1) \times 4 - 146 \times 3 \\
&= 256 \times 4 - 146 \times 4 - 146 \times 3 \\
&= 256 \times 4 - 146 \times 7 \\
&= 256 \times 4 - (1170 - 256 \times 4) \times 7 \\
&= 256 \times 4 - 1170 \times 7 + 256 \times 28 \\
&= 256 \times 32 - 1170 \times 7
\end{aligned}$$

Therefore: $\boxed{\gcd(256, 1170) = 2 = 256(32) + 1170(-7)}$

Verification: $256 \times 32 + 1170 \times (-7) = 8192 - 8190 = 2$ ✓

Example 21: Another Linear Combination

Find $\gcd(10672, 4147)$ and express it as a linear combination.

Solution:

Step 1: Euclidean Algorithm

$$\begin{aligned}
10672 &= 4147 \times 2 + 2378 \\
4147 &= 2378 \times 1 + 1769 \\
2378 &= 1769 \times 1 + 609 \\
1769 &= 609 \times 2 + 551 \\
609 &= 551 \times 1 + 58 \\
551 &= 58 \times 9 + 29 \\
58 &= 29 \times 2 + 0
\end{aligned}$$

Therefore: $\gcd(10672, 4147) = 29$

Step 2: Back Substitution

$$\begin{aligned}
29 &= 551 - 58 \times 9 \\
&= 551 - (609 - 551 \times 1) \times 9 \\
&= 551 - 609 \times 9 + 551 \times 9 \\
&= 551 \times 10 - 609 \times 9 \\
&= (1769 - 609 \times 2) \times 10 - 609 \times 9 \\
&= 1769 \times 10 - 609 \times 20 - 609 \times 9 \\
&= 1769 \times 10 - 609 \times 29 \\
&= 1769 \times 10 - (2378 - 1769 \times 1) \times 29 \\
&= 1769 \times 10 - 2378 \times 29 + 1769 \times 29 \\
&= 1769 \times 39 - 2378 \times 29 \\
&= (4147 - 2378 \times 1) \times 39 - 2378 \times 29 \\
&= 4147 \times 39 - 2378 \times 39 - 2378 \times 29 \\
&= 4147 \times 39 - 2378 \times 68 \\
&= 4147 \times 39 - (10672 - 4147 \times 2) \times 68 \\
&= 4147 \times 39 - 10672 \times 68 + 4147 \times 136 \\
&= 4147 \times 175 - 10672 \times 68
\end{aligned}$$

Therefore: $\boxed{\gcd(10672, 4147) = 29 = 10672(-68) + 4147(175)}$
Verification: $10672 \times (-68) + 4147 \times 175 = -725696 + 725725 = 29$ ✓

Relatively Prime Integers

Definition: Relatively Prime (Coprime) Integers

Two integers a and b, at least one of which is non-zero, are said to be **relatively prime** or **coprime** if:

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

Key Points:

- Relatively prime integers have no common divisor other than ± 1
- Alternative notation: $(a, b) = 1$
- The integers do not need to be prime themselves

Example 22: Identifying Coprime Integers

Determine which pairs are relatively prime:
Solution:

1. $(8, 15)$: $\gcd(8, 15) = 1$ Coprime ✓
2. $(12, 18)$: $\gcd(12, 18) = 6 \neq 1$ Not coprime ×
3. $(21, 25)$: $\gcd(21, 25) = 1$ Coprime ✓

4. $(14, 21)$: $\gcd(14, 21) = 7 \neq 1$ Not coprime $\times$

5. $(9, 16)$: $\gcd(9, 16) = 1$ Coprime ✓

Note: Notice that 8, 9, 15, 16, 21, and 25 are not all prime numbers, but the pairs can still be coprime.

Corollary: GCD Reduction

If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof of Corollary

Proof:
Let $\gcd(a, b) = d$.
Then $a = da'$ and $b = db'$ for some integers a' and b'.
We have $\frac{a}{d} = a'$ and $\frac{b}{d} = b'$.
Let $\gcd(a', b') = g$.
Then $g|a'$ and $g|b'$, which means:

$$g|da' = a \quad \text{and} \quad g|db' = b$$

Since g is a common divisor of a and b, we have $g|\gcd(a, b) = d$.
But $d = \gcd(a, b)$ is the largest integer such that $a = da'$ and $b = db'$ where $\gcd(a', b') = 1$.
This means $g|d$ and $g|a'$ and $g|b'$ can only be satisfied if $g = 1$.
Therefore, $\gcd(a', b') = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Example 23: GCD Reduction

Given $\gcd(48, 72) = 24$, verify that $\gcd(2, 3) = 1$.
Solution:
We have $\gcd(48, 72) = 24$.
Calculate:

$$\frac{48}{24} = 2, \quad \frac{72}{24} = 3$$

Now find:

$$\gcd(2, 3) = 1$$

Therefore, $\gcd\left(\frac{48}{24}, \frac{72}{24}\right) = \gcd(2, 3) = 1$ ✓

Theorem: GCD Scaling Property

Let a and b be two integers, at least one of which is non-zero, and let $k > 0$ be an integer.
Then:

$$\gcd(ka, kb) = k \cdot \gcd(a, b)$$

Proof of Theorem

Proof:
Let $d = \gcd(a, b)$.
Then $a = dm$ and $b = dn$ for some integers m and n with $\gcd(m, n) = 1$.
Consider ka and kb:

$$ka = k(dm) = (kd)m, \quad kb = k(dn) = (kd)n$$

So kd is a common divisor of ka and kb.
Let $g = \gcd(ka, kb)$.
Then $g|ka$ and $g|kb$.
By Bezout's theorem, there exist integers x and y such that:

$$d = ax + by$$

Multiply both sides by k:

$$kd = k(ax + by) = (ka)x + (kb)y$$

Since $g|ka$ and $g|kb$, by property (g) of divisibility:

$$g|(ka)x + (kb)y = kd$$

So $g|kd$.
Also, $kd|ka$ and $kd|kb$, so $kd|g$.
Since $g|kd$ and $kd|g$, and both are positive, we have $g = kd$.
Therefore, $\gcd(ka, kb) = k \cdot \gcd(a, b)$. □

Example 24: GCD Scaling

Verify that $\gcd(15, 25) = 5 \cdot \gcd(3, 5)$.
Solution:
Calculate $\gcd(3, 5) = 1$ (since 3 and 5 are coprime)
According to the theorem with $k = 5$:

$$\gcd(15, 25) = \gcd(5 \cdot 3, 5 \cdot 5) = 5 \cdot \gcd(3, 5) = 5 \cdot 1 = 5$$

Verification: $\gcd(15, 25) = 5$ ✓

Theorem: Division by Coprime Integers

If $a|c$ and $b|c$ with $\gcd(a, b) = 1$, then $ab|c$.

Proof of Theorem

Proof:
Given: $a|c$ and $b|c$ with $\gcd(a, b) = 1$.
Since $a|c$, we have $c = am$ for some integer m.

Since $\gcd(a, b) = 1$, by Bezout's theorem, there exist integers x and y such that:

$$1 = ax + by$$

Multiply both sides by m:

$$m = amx + bmy$$

Substitute $c = am$:

$$m = cx + bmy$$

Therefore:

$$c = am = a(cx + bmy) = acx + abmy$$

Since $b|c$, let $c = bn$ for some integer n.
Then:

$$c = acx + abmy = a(bn)x + abmy = ab(nx + my)$$

Since $nx + my$ is an integer, we have $c = ab(nx + my)$.
Therefore, $ab|c$. □

Example 25: Application of Theorem

Given $3|60$ and $4|60$ with $\gcd(3, 4) = 1$, show that $12|60$.
Solution:
We have:

- $3|60$ because $60 = 3 \times 20$ ✓
- $4|60$ because $60 = 4 \times 15$ ✓
- $\gcd(3, 4) = 1$ ✓

By the theorem: $3 \cdot 4 = 12$ divides 60.
Verification: $60 = 12 \times 5$, so $12|60$ ✓

Theorem: Euclid's Lemma

If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Proof: Euclid's Lemma

Proof:
Given: $a|bc$ and $\gcd(a, b) = 1$.
Since $\gcd(a, b) = 1$, by Bezout's theorem, there exist integers x and y such that:

$$1 = ax + by$$

Multiply both sides by c:

$$c = acx + bcy$$

Since $a|bc$, we have $bc = ak$ for some integer k.

Substitute:

$$c = acx + bcy = acx + (ak)y = a(cx + ky)$$

Since $cx + ky$ is an integer, we have $c = a(cx + ky)$.
Therefore, $a|c$. □

Example 26: Euclid's Lemma Application

Given $7|(5 \times 21)$ and $\gcd(7, 5) = 1$, show that $7|21$.
Solution:
We have:

- $5 \times 21 = 105 = 7 \times 15$, so $7|(5 \times 21)$ ✓
- $\gcd(7, 5) = 1$ (since 7 and 5 are coprime) ✓

By Euclid's Lemma: $7|21$
Verification: $21 = 7 \times 3$, so $7|21$ ✓

Theorem: Alternative GCD Characterization

For a positive integer d, $d = \gcd(a, b)$ if and only if:

(a) $d|a$ and $d|b$

(b) Whenever $c|a$ and $c|b$, then $c|d$

Proof of Theorem

Proof:
Forward Direction ($\Rightarrow$): Assume $d = \gcd(a, b)$
By definition of GCD:

- $d|a$ and $d|b$ (property ii of GCD definition) ✓
- If $c|a$ and $c|b$, then $c|d$ (property iii of GCD definition) ✓

Backward Direction ($\Leftarrow$): Assume conditions (a) and (b) hold
Let $g = \gcd(a, b)$.
Since $g|a$ and $g|b$, by condition (b): $g|d \quad \cdots (1)$
Since $d|a$ and $d|b$, and g is the GCD, by property (iii): $d|g \quad \cdots (2)$
From (1) and (2): $g|d$ and $d|g$
Since both are positive: $g = d$
Therefore, $d = \gcd(a, b)$. □

Example 27: Verifying GCD Characterization

Verify that $d = 6$ satisfies both conditions for $\gcd(24, 42)$.
Solution:

Condition (a): Check if $6|24$ and $6|42$

- $24 = 6 \times 4$, so $6|24$ ✓
- $42 = 6 \times 7$, so $6|42$ ✓

Condition (b): Check if every common divisor of 24 and 42 divides 6
Common divisors of 24 and 42: $1, 2, 3, 6$

- $1|6$ ✓
- $2|6$ ✓
- $3|6$ ✓
- $6|6$ ✓

Both conditions satisfied, therefore $\gcd(24, 42) = 6$ ✓

Coprimality Problems

Example 28: Proving Two Expressions are Coprime

Show that $\gcd(2a+1, 9a+4) = 1$.

Solution:

Let $d = \gcd(2a+1, 9a+4)$.

Then $d|(2a+1)$ and $d|(9a+4)$.

By property (g) of divisibility:

$$d|[9(2a+1) - 2(9a+4)]$$

Calculate:

$$9(2a+1) - 2(9a+4) = 18a + 9 - 18a - 8 = 1$$

So $d|1$, which means $d = 1$.

Therefore, $\gcd(2a+1, 9a+4) = 1$. □

Example 29: Another Coprimality Proof

Show that $\gcd(5a+2, 7a+3) = 1$.

Solution:

Let $d = \gcd(5a+2, 7a+3)$.

Then $d|(5a+2)$ and $d|(7a+3)$.

By property (g):

$$d|[7(5a+2) - 5(7a+3)]$$

Calculate:

$$7(5a+2) - 5(7a+3) = 35a + 14 - 35a - 15 = -1$$

So $d|(-1)$, which means $d|1$, hence $d = 1$.

Therefore, $\gcd(5a+2, 7a+3) = 1$. □

Example 30: Third Coprimality Example

Show that $\gcd(2a+3, 4a+5) = 1$.

Solution:

Let $d = \gcd(2a+3, 4a+5)$.

Then $d|(2a+3)$ and $d|(4a+5)$.

Note that $4a+5 = 2(2a+3) - 1$, so:

$$d|[2(2a+3) - (4a+5)]$$

Calculate:

$$2(2a+3) - (4a+5) = 4a + 6 - 4a - 5 = 1$$

So $d|1$, which means $d = 1$.

Therefore, $\gcd(2a+3, 4a+5) = 1$. □

Example 31: Coprimality with Condition

Show that $\gcd(3a, 3a+2) = 1$ for odd a.

Solution:

Let $d = \gcd(3a, 3a+2)$.
Then $d|3a$ and $d|(3a+2)$.
By property (g):

$$d|[(3a+2) - 3a] = 2$$

So $d|2$, which means $d \in \{1, 2\}$.
Now, since a is odd, $3a$ is also odd (product of two odd numbers).
If $d = 2$, then $d|3a$ implies $2|3a$.
But $3a$ is odd, so $2 \nmid 3a$.
This is a contradiction.
Therefore, $d = 1$.
Hence, $\gcd(3a, 3a+2) = 1$ for odd a. □

Conditional Coprimality

Example 32: GCD Result is 1 or 2

If $\gcd(a, b) = 1$, show that $\gcd(a+b, a-b)$ is 1 or 2.

Solution:

Let $d = \gcd(a+b, a-b)$.
Then $d|(a+b)$ and $d|(a-b)$.
By property (g):

$$d|[(a+b) + (a-b)] = 2a$$

$$d|[(a+b) - (a-b)] = 2b$$

So $d|2a$ and $d|2b$.
Since $\gcd(a, b) = 1$, by the theorem on coprime integers:
Let $d = \gcd(2a, 2b) = 2 \cdot \gcd(a, b) = 2 \cdot 1 = 2$.
But $d|2a$ and $d|2b$ means d divides $\gcd(2a, 2b) = 2$.
Therefore, $d|2$, so $d \in \{1, 2\}$.
Hence, $\gcd(a+b, a-b)$ is either 1 or 2. □

Example 33: GCD Result is 1 or 3

If $\gcd(a, b) = 1$, show that $\gcd(2a+b, a+2b)$ is 1 or 3.

Solution:

Let $d = \gcd(2a+b, a+2b)$.
Then $d|(2a+b)$ and $d|(a+2b)$.
By property (g):

$$d|[2(2a+b) - (a+2b)] = 4a + 2b - a - 2b = 3a$$

$$d|[2(a+2b) - (2a+b)] = 2a + 4b - 2a - b = 3b$$

So $d|3a$ and $d|3b$.
Since $\gcd(a, b) = 1$, we have $\gcd(3a, 3b) = 3 \cdot \gcd(a, b) = 3 \cdot 1 = 3$.

Therefore, $d|3$, so $d \in \{1, 3\}$.
Hence, $\gcd(2a + b, a + 2b)$ is either 1 or 3. □

Example 34: Sum and Sum of Squares

If $\gcd(a, b) = 1$, show that $\gcd(a + b, a^2 + b^2)$ is 1 or 2.
Solution:
Let $d = \gcd(a + b, a^2 + b^2)$.
Then $d|(a + b)$ and $d|(a^2 + b^2)$.
Since $d|(a + b)$, we have:

$$d|(a + b)^2 = a^2 + 2ab + b^2$$

By property (g):

$$d|[(a^2 + 2ab + b^2) - (a^2 + b^2)] = 2ab$$

So $d|2ab$.
Also, from $d|(a + b)$:

$$d|(a + b)a = a^2 + ab$$

By property (g):

$$d|[(a^2 + b^2) - (a^2 + ab)] = b^2 - ab = b(b - a)$$

Similarly:

$$d|(a + b)b = ab + b^2$$

$$d|[(a^2 + b^2) - (ab + b^2)] = a^2 - ab = a(a - b)$$

From $d|2ab$ and $\gcd(a, b) = 1$:
If d is odd, then $d|ab$ implies $d|a$ or $d|b$ (by Euclid's Lemma applied twice).
But if $d|a$ and $d|(a + b)$, then $d|b$, contradicting $\gcd(a, b) = 1$.
So d must divide 2.
Therefore, $d \in \{1, 2\}$.
Hence, $\gcd(a + b, a^2 + b^2)$ is either 1 or 2. □

Example 35: Quadratic Expression

If $\gcd(a, b) = 1$, show that $\gcd(a + b, a^2 - ab + b^2)$ is 1 or 3.
Solution:
Let $d = \gcd(a + b, a^2 - ab + b^2)$.
Then $d|(a + b)$ and $d|(a^2 - ab + b^2)$.
Note that:

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$a^3 + b^3 = (a + b)(a^2 - ab + b^2)$$

Since $d|(a + b)$, we have:

$$d|(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Also, $d|(a^2 - ab + b^2)$ and $d|(a + b)$ gives:

$$d|(a + b)(a^2 - ab + b^2) = a^3 + b^3$$

By property (g):

$$d|[(a^3 + 3a^2b + 3ab^2 + b^3) - (a^3 + b^3)] = 3a^2b + 3ab^2 = 3ab(a + b)$$

Since $d|(a + b)$, we have:

$$d|3ab$$

Since $\gcd(a, b) = 1$, and $d|3ab$:
d must divide 3.
Therefore, $d \in \{1, 3\}$.
Hence, $\gcd(a + b, a^2 - ab + b^2)$ is either 1 or 3. □

Least Common Multiple (LCM)

Definition: Least Common Multiple

The **least common multiple** (LCM) of two integers a and b is a positive integer m, denoted by $\text{lcm}(a, b)$ or $[a, b]$, that satisfies:

(a) $m > 0$

(b) $a|m$ and $b|m$

(c) If $a|c$ and $b|c$ with $c > 0$, then $m|c$

In words:

- LCM is the smallest positive integer that is divisible by both a and b
- Every common multiple of a and b is a multiple of the LCM

Example 36: Finding LCM by Listing Multiples

Find $\text{lcm}(6, 8)$.
Solution:
Multiples of 6: $6, 12, 18, 24, 30, 36, 42, 48, \ldots$
Multiples of 8: $8, 16, 24, 32, 40, 48, \ldots$
Common multiples: $24, 48, 72, \ldots$
The least common multiple is: $\boxed{\text{lcm}(6, 8) = 24}$ ✓

Example 37: Finding LCM by Prime Factorization

Find $\text{lcm}(12, 18)$.
Solution:
Prime factorization:

$$12 = 2^2 \times 3$$
$$18 = 2 \times 3^2$$

Taking maximum powers of each prime:

$$\text{lcm}(12, 18) = 2^{\max(2,1)} \times 3^{\max(1,2)} = 2^2 \times 3^2 = 4 \times 9 = 36$$

Therefore: $\boxed{\text{lcm}(12, 18) = 36}$ ✓

Theorem: Relationship between GCD and LCM

For any two positive integers a and b:

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

Proof of Theorem

Proof:

Let a and b be positive integers with prime factorizations:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

where some exponents may be zero.
Then:

$$\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$\text{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Now:

$$\begin{aligned}\gcd(a, b) \cdot \text{lcm}(a, b) &= \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)} \cdot \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} \\ &= \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)}\end{aligned}$$

For any two numbers α_i and β_i:

$$\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$$

Therefore:

$$\begin{aligned}\gcd(a, b) \cdot \text{lcm}(a, b) &= \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} \\ &= \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \prod_{i=1}^{k} p_i^{\beta_i} \\ &= a \cdot b\end{aligned}$$

Hence, $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$. □

Example 38: Using GCD-LCM Relationship

Find $\text{lcm}(24, 138)$ given that $\gcd(24, 138) = 6$.

Solution:

Using the formula:

$$\gcd(24, 138) \cdot \text{lcm}(24, 138) = 24 \times 138$$

Substitute $\gcd(24, 138) = 6$:

$$6 \cdot \text{lcm}(24, 138) = 24 \times 138 = 3312$$

Solve for LCM:

$$\text{lcm}(24, 138) = \frac{3312}{6} = 552$$

Therefore: $\boxed{\text{lcm}(24, 138) = 552}$ ✓

Verification:

$$\gcd(24, 138) \cdot \text{lcm}(24, 138) = 6 \times 552 = 3312 = 24 \times 138$$

✓

Corollary: LCM of Coprime Integers

If a and b are relatively prime integers (i.e., $\gcd(a, b) = 1$), then:

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

Proof of Corollary

Proof:

Given: $\gcd(a, b) = 1$

From the theorem: $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$

Substitute $\gcd(a, b) = 1$:

$$1 \cdot \text{lcm}(a, b) = ab$$

Therefore:

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

Hence, for coprime integers, the LCM equals their product. □

Example 39: LCM of Coprime Numbers

Find $\text{lcm}(7, 12)$.

Solution:

First, check if 7 and 12 are coprime:

$$\gcd(7, 12) = 1$$

Since they are coprime, by the corollary:

$$\text{lcm}(7, 12) = 7 \times 12 = 84$$

Therefore: $\boxed{\text{lcm}(7, 12) = 84}$ ✓

Example 40: Complete GCD and LCM Calculation

Find $\gcd(24, 138)$ and $\text{lcm}(24, 138)$, then verify their relationship.

Solution:

Step 1: Find GCD using Euclidean Algorithm

$$138 = 24 \times 5 + 18$$
$$24 = 18 \times 1 + 6$$
$$18 = 6 \times 3 + 0$$

Therefore: $\gcd(24, 138) = 6$

Step 2: Find LCM using the formula

$$\text{lcm}(24, 138) = \frac{24 \times 138}{\gcd(24, 138)} = \frac{3312}{6} = 552$$

Step 3: Verify the relationship

$$\gcd(24, 138) \times \text{lcm}(24, 138) = 6 \times 552 = 3312$$
$$24 \times 138 = 3312$$

Since both are equal: $\boxed{\gcd(24, 138) = 6 \text{ and } \text{lcm}(24, 138) = 552}$ ✓

GCD of Three or More Integers

Definition: GCD of Three Integers

Three integers a, b, and c, at least one of which is non-zero, are said to be **relatively prime** if:

$$\gcd(a, b, c) = 1$$

The GCD of three integers can be computed as:

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

Key Points:

- The GCD operation is associative: $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$
- This extends to any number of integers

Example 41: GCD of Three Numbers

Find $\gcd(198, 288, 512)$.

Solution:

Step 1: Find $\gcd(198, 288)$

$$\begin{aligned} 288 &= 198 \times 1 + 90 \\ 198 &= 90 \times 2 + 18 \\ 90 &= 18 \times 5 + 0 \end{aligned}$$

So $\gcd(198, 288) = 18$

Step 2: Find $\gcd(18, 512)$

$$\begin{aligned} 512 &= 18 \times 28 + 8 \\ 18 &= 8 \times 2 + 2 \\ 8 &= 2 \times 4 + 0 \end{aligned}$$

So $\gcd(18, 512) = 2$

Therefore: $\boxed{\gcd(198, 288, 512) = 2}$ ✓

Example 42: Express GCD as Linear Combination

Express $\gcd(198, 288, 512) = 2$ as a linear combination of 198, 288, and 512.

Solution:

From Example 41, we have $\gcd(198, 288, 512) = 2$.

Step 1: Express $\gcd(18, 512) = 2$

Back-substitution from Euclidean Algorithm:

$$\begin{aligned} 2 &= 18 - 8 \times 2 \\ &= 18 - (512 - 18 \times 28) \times 2 \\ &= 18 - 512 \times 2 + 18 \times 56 \\ &= 18 \times 57 - 512 \times 2 \end{aligned}$$

Step 2: Express $\gcd(198, 288) = 18$

Back-substitution:

$$\begin{aligned} 18 &= 198 - 90 \times 2 \\ &= 198 - (288 - 198 \times 1) \times 2 \\ &= 198 - 288 \times 2 + 198 \times 2 \\ &= 198 \times 3 - 288 \times 2 \end{aligned}$$

Step 3: Combine both results

Substitute $18 = 198 \times 3 - 288 \times 2$ into $2 = 18 \times 57 - 512 \times 2$:

$$\begin{aligned} 2 &= (198 \times 3 - 288 \times 2) \times 57 - 512 \times 2 \\ &= 198 \times 171 - 288 \times 114 - 512 \times 2 \\ &= 198 \times 171 + 288 \times (-114) + 512 \times (-2) \end{aligned}$$

Therefore: $\boxed{2 = 198(171) + 288(-114) + 512(-2)}$

Verification:

$$198 \times 171 + 288 \times (-114) + 512 \times (-2) = 33858 - 32832 - 1024 = 2$$

✓

Summary of GCD and LCM

Property	Formula/Description
GCD Definition	Largest positive integer dividing both a and b
LCM Definition	Smallest positive integer divisible by both a and b
GCD-LCM Relationship	$\gcd(a,b) \cdot \text{lcm}(a,b) = ab$
Bezout's Identity	$\gcd(a,b) = ax+by$ for some $x, y \in \mathbb{Z}$
Euclidean Algorithm	If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$
Coprime Integers	$\gcd(a,b) = 1 \implies \text{lcm}(a,b) = ab$
GCD Scaling	$\gcd(ka,kb) = k \cdot \gcd(a,b)$ for $k > 0$
Euclid's Lemma	If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$

Additional Problems

Practice Problem 1

Find $\gcd(1024, 2580)$ and express it as a linear combination.

Solution:

Euclidean Algorithm:

$$\begin{aligned} 2580 &= 1024 \times 2 + 532 \\ 1024 &= 532 \times 1 + 492 \\ 532 &= 492 \times 1 + 40 \\ 492 &= 40 \times 12 + 12 \\ 40 &= 12 \times 3 + 4 \\ 12 &= 4 \times 3 + 0 \end{aligned}$$

Therefore: $\gcd(1024, 2580) = 4$

Back Substitution:

$$\begin{aligned}
4 &= 40 - 12 \times 3 \\
&= 40 - (492 - 40 \times 12) \times 3 \\
&= 40 - 492 \times 3 + 40 \times 36 \\
&= 40 \times 37 - 492 \times 3 \\
&= (532 - 492 \times 1) \times 37 - 492 \times 3 \\
&= 532 \times 37 - 492 \times 37 - 492 \times 3 \\
&= 532 \times 37 - 492 \times 40 \\
&= 532 \times 37 - (1024 - 532 \times 1) \times 40 \\
&= 532 \times 37 - 1024 \times 40 + 532 \times 40 \\
&= 532 \times 77 - 1024 \times 40 \\
&= (2580 - 1024 \times 2) \times 77 - 1024 \times 40 \\
&= 2580 \times 77 - 1024 \times 154 - 1024 \times 40 \\
&= 2580 \times 77 - 1024 \times 194
\end{aligned}$$

Therefore: $\boxed{4 = 2580(77) + 1024(-194)}$
Verification: $2580 \times 77 - 1024 \times 194 = 198660 - 198656 = 4$ ✓

Problem 2

Show that if n is odd, then $\gcd(n, n+2) = 1$.
Solution:
Let $d = \gcd(n, n+2)$.
Then $d|n$ and $d|(n+2)$.
By property (g) of divisibility:

$$d|[(n+2) - n] = 2$$

So $d|2$, which means $d \in \{1, 2\}$.
Since n is odd, n is not divisible by 2.
If $d = 2$, then $d|n$ implies $2|n$, which contradicts that n is odd.
Therefore, $d = 1$.
Hence, $\gcd(n, n+2) = 1$ for odd n. □

Problem 3

Prove that $\gcd(a, b) = \gcd(a, b-a)$ for $b > a > 0$.
Solution:
Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(a, b-a)$.
Show $d_1|d_2$:
Since $d_1 = \gcd(a, b)$, we have $d_1|a$ and $d_1|b$.
By property (g): $d_1|(b-a)$
So $d_1|a$ and $d_1|(b-a)$, which means d_1 is a common divisor of a and $b-a$.
Therefore, $d_1|\gcd(a, b-a) = d_2$.
Show $d_2|d_1$:

Since $d_2 = \gcd(a, b-a)$, we have $d_2|a$ and $d_2|(b-a)$.
By property (g): $d_2|[a+(b-a)] = b$
So $d_2|a$ and $d_2|b$, which means d_2 is a common divisor of a and b.
Therefore, $d_2|\gcd(a,b) = d_1$.
Since $d_1|d_2$ and $d_2|d_1$, and both are positive:

$$d_1 = d_2$$

Hence, $\gcd(a,b) = \gcd(a, b-a)$. □

Important Identities for GCD

1. $\gcd(a, 0) = |a|$
2. $\gcd(a, 1) = 1$ for any integer a
3. $\gcd(a, a) = |a|$
4. $\gcd(a, b) = \gcd(b, a)$ (Commutative)
5. $\gcd(a, b) = \gcd(|a|, |b|)$
6. $\gcd(a, b + ka) = \gcd(a, b)$ for any integer k
7. If $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
8. $\gcd(ac, bc) = |c| \cdot \gcd(a, b)$ for $c \neq 0$

Practice Exercise

Problem 1

Find the quotient q and remainder r when $a = 157$ is divided by $b = 13$.

Problem 2

Find the quotient q and remainder r when $a = -47$ is divided by $b = 9$.

Problem 3

Show that the cube of any integer is of the form $5k$, $5k+1$, $5k+2$, $5k+3$, or $5k+4$. Determine which forms are actually possible.

Problem 4

Prove that for any integer n, $n^5 - n$ is divisible by 5.

Problem 5

Show that the square of any integer is of the form $5k$, $5k+1$, or $5k+4$.

Problem 6

Prove that if $a|b$ and $b|c$, then $a|(2b+3c)$.

Problem 7

Show that the product of three consecutive integers is divisible by 6.

Problem 8

Prove that $n^3 - n$ is divisible by 6 for all integers n.

Problem 9

Show that if n is an odd integer, then $n^2 - 1$ is divisible by 8.

Problem 10

Prove that $5|(n^5 - 5n^3 + 4n)$ for all integers n.

Problem 11

Find $\gcd(420, 252)$ using the Euclidean Algorithm and express it as a linear combination of 420 and 252.

Problem 12

Find $\gcd(3456, 1728)$ and $\text{lcm}(3456, 1728)$. Verify that $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

Problem 13

Find three integers x, y, and z such that $\gcd(144, 252, 360) = 144x + 252y + 360z$.

Problem 14

If $\gcd(a, b) = 12$ and $\text{lcm}(a, b) = 360$, find all possible pairs (a, b).

Problem 15

Find $\gcd(987, 610)$ using the Euclidean Algorithm. (These are consecutive Fibonacci numbers)

Problem 16

Show that $\gcd(3a + 5, 2a + 3) = 1$ for all integers a.

Problem 17

Prove that if $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

Problem 18

Show that if $\gcd(a, b) = 1$, then $\gcd(a + 2b, 2a + b) = 1$ or 5.

Problem 19

Prove that consecutive integers are always coprime, i.e., $\gcd(n, n + 1) = 1$ for all integers n.

Problem 20

If $\gcd(a, b) = 1$, prove that $\gcd(a - b, a + b) \leq 2$.

Problem 21

Prove that if $\gcd(a, b) = 1$ and $c|a$ and $c|(a + b)$, then $c = 1$.

Problem 22

Show that for any positive integers a and b:

$$\gcd(a, b) \cdot \gcd\left(\frac{\text{lcm}(a, b)}{a}, \frac{\text{lcm}(a, b)}{b}\right) = \text{lcm}(a, b)$$

Problem 23

If n is a positive integer, prove that $\gcd(n! + 1, (n + 1)! + 1) = 1$.

Problem 24

Prove that there exist infinitely many pairs of coprime integers (a, b) such that neither a nor b is prime.

Problem 25

Show that if $d = \gcd(a, b)$, then for any integer k:

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

Chapter 2

Theory of Primes

Fundamental Definitions

Prime Numbers

Definition: Prime Integer

An integer $p > 1$ is called a **prime number** (or simply **prime**) if its only positive divisors are 1 and p itself.

Key Points:

- A prime has exactly two positive divisors: 1 and itself
- The number 1 is NOT a prime number
- The smallest prime number is 2 (also the only even prime)

Example 1: Identifying Prime Numbers

Determine which of the following numbers are prime: 2, 3, 7, 11, 13, 17.

Solution:

For 2: Divisors are 1, 2. Only two divisors. Prime ✓
For 3: Divisors are 1, 3. Only two divisors. Prime ✓
For 7: Divisors are 1, 7. Only two divisors. Prime ✓
For 11: Divisors are 1, 11. Only two divisors. Prime ✓
For 13: Divisors are 1, 13. Only two divisors. Prime ✓
For 17: Divisors are 1, 17. Only two divisors. Prime ✓
All of these are prime numbers.

Example 2: First Twenty Prime Numbers

List the first 20 prime numbers.

Solution:

The first 20 prime numbers are:

$$\boxed{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71}$$

Note:

- 2 is the only even prime

- All other primes are odd
- Primes become less frequent as numbers get larger

Why is 1 NOT Prime?
The number 1 is excluded from primes for important mathematical reasons:

- If 1 were prime, the Fundamental Theorem of Arithmetic (unique factorization) would fail
- For example: $6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3 = \ldots$
- This would destroy uniqueness of prime factorization

Composite Numbers

Definition: Composite Integer

An integer $n > 1$ is called **composite** if it is not prime. In other words, n is composite if it has at least one positive divisor other than 1 and n itself.

Key Points:

- A composite number has at least three positive divisors
- Every composite number can be written as a product of two or more primes
- The smallest composite number is 4

Example 3: Identifying Composite Numbers

Show that 4, 6, 8, 9, 10, 12 are composite numbers.

Solution:

For 4: $4 = 2 \times 2$. Divisors: 1, 2, 4. Composite ✓
For 6: $6 = 2 \times 3$. Divisors: 1, 2, 3, 6. Composite ✓
For 8: $8 = 2 \times 4 = 2 \times 2 \times 2$. Divisors: 1, 2, 4, 8. Composite ✓
For 9: $9 = 3 \times 3$. Divisors: 1, 3, 9. Composite ✓
For 10: $10 = 2 \times 5$. Divisors: 1, 2, 5, 10. Composite ✓
For 12: $12 = 2 \times 6 = 3 \times 4 = 2 \times 2 \times 3$. Divisors: 1, 2, 3, 4, 6, 12. Composite ✓
All have more than two divisors, so all are composite.

Example 4: Prime vs Composite Classification

Classify the following numbers as prime or composite: 15, 17, 21, 23, 29, 30.

Solution:

Number	Factorization	Divisors	Classification
15	3×5	1, 3, 5, 15	Composite
17	1×17	1, 17	Prime
21	3×7	1, 3, 7, 21	Composite
23	1×23	1, 23	Prime
29	1×29	1, 29	Prime
30	$2 \times 3 \times 5$	1, 2, 3, 5, 6, 10, 15, 30	Composite

Classification of Positive Integers

Integers greater than 1

PRIME NUMBERS
Exactly 2 divisors
(1 and itself)

Examples:
2, 3, 5, 7, 11, 13,
17, 19, 23, 29...

COMPOSITE NUMBERS
More than 2 divisors
(divisible by other numbers)

Examples:
4, 6, 8, 9, 10, 12,
14, 15, 16, 18...

The number 1 is NEITHER prime NOR composite

Co-prime (Relatively Prime) Integers

Definition: Co-prime Integers

Two integers a and b are called **co-prime** or **relatively prime** if their greatest common divisor is 1:

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

Important Notes:

- Co-prime integers share no common prime factors
- The integers themselves need not be prime
- For example, 8 and 9 are co-prime, but neither is prime

Example 5: Co-prime Pairs

Determine which pairs are co-prime.
Solution:

1. $(8, 15)$: $\gcd(8, 15) = 1$ Co-prime ✓
2. $(12, 18)$: $\gcd(12, 18) = 6 \neq 1$ Not co-prime ×
3. $(25, 36)$: $\gcd(25, 36) = 1$ Co-prime ✓
4. $(14, 21)$: $\gcd(14, 21) = 7 \neq 1$ Not co-prime ×

5. $(9, 16)$: $\gcd(9, 16) = 1$ Co-prime ✓

Observation: Notice that in $(9, 16)$, both 9 and 16 are composite, yet they are co-prime!

Example 6: Prime Numbers are Co-prime

Show that any two distinct prime numbers are always co-prime.

Solution:

Let p and q be two distinct prime numbers.
Since p is prime, its only divisors are 1 and p.
Since q is prime, its only divisors are 1 and q.
Since $p \neq q$, the only common divisor is 1.
Therefore, $\gcd(p, q) = 1$.
Hence, any two distinct primes are co-prime. □

Examples:

- $\gcd(3, 5) = 1$ ✓
- $\gcd(7, 11) = 1$ ✓
- $\gcd(13, 17) = 1$ ✓

Twin Primes

Definition: Twin Primes

Two prime numbers that differ by 2 are called **twin primes**. In other words, primes p and q are twin primes if:

$$q = p + 2$$

Key Facts:

- The smallest twin prime pair is $(3, 5)$
- All twin prime pairs (except 3, 5) have the form $(6n - 1, 6n + 1)$
- It is conjectured (but not proven) that there are infinitely many twin primes

Example 7: Finding Twin Primes

List all twin prime pairs less than 50.

Solution:

We check consecutive odd numbers for primality:

Twin Prime Pair	Difference
$(3, 5)$	$5 - 3 = 2$ ✓
$(5, 7)$	$7 - 5 = 2$ ✓
$(11, 13)$	$13 - 11 = 2$ ✓
$(17, 19)$	$19 - 17 = 2$ ✓
$(29, 31)$	$31 - 29 = 2$ ✓
$(41, 43)$	$43 - 41 = 2$ ✓

Therefore, twin primes less than 50 are:

$$\boxed{(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43)}$$

Example 8: Non-Twin Prime Pairs

Explain why $(7, 11)$ and $(13, 17)$ are NOT twin primes even though both numbers in each pair are prime.

Solution:

For $(7, 11)$**:**

$$11 - 7 = 4 \neq 2$$

The difference is 4, not 2. Not twin primes $\times$

For $(13, 17)$**:**

$$17 - 13 = 4 \neq 2$$

The difference is 4, not 2. Not twin primes $\times$

Note: For twin primes, the difference must be **exactly** 2.

Summary of Definitions

Term	Definition
Prime	Integer $p > 1$ with only divisors 1 and p
Composite	Integer $n > 1$ that is not prime
Co-prime	Two integers with $\gcd(a, b) = 1$
Twin Primes	Two primes differing by 2: $(p, p + 2)$

Remember:

- 1 is neither prime nor composite
- 2 is the only even prime
- Co-prime integers need not be prime themselves

Fundamental Theorems on Primes

Euclid's Lemma

Theorem: Euclid's Lemma

If p is a prime number and $p|ab$, then:

$$p|a \quad \text{or} \quad p|b$$

In words: If a prime divides a product of two integers, then it must divide at least one of them.

Proof: Euclid's Lemma

Proof:
Let p be prime and $p|ab$.
We need to show that $p|a$ or $p|b$.
Case 1: If $p|a$, we are done.
Case 2: Suppose $p \nmid a$.
Since p is prime, its only divisors are 1 and p.
Since $p \nmid a$, we have $\gcd(p, a) \neq p$.
Therefore, $\gcd(p, a) = 1$ (the only other option).
Now we use Euclid's Lemma from Chapter 1:
If $p|ab$ and $\gcd(p, a) = 1$, then $p|b$.
Therefore, $p|b$. □

Example 9: Applying Euclid's Lemma

Given that $7|(6 \times 14)$, use Euclid's Lemma to determine what 7 divides.
Solution:
We have $7|(6 \times 14)$.
Since 7 is prime, by Euclid's Lemma:

$$7|6 \quad \text{or} \quad 7|14$$

Check: $6 = 7(0) + 6$, so $7 \nmid 6$ ×
Check: $14 = 7(2) + 0$, so $7|14$ ✓
Therefore, by Euclid's Lemma, $7|14$.
Verification: $6 \times 14 = 84 = 7 \times 12$, so indeed $7|84$. ✓

Example 10: Euclid's Lemma Application

If $11|(5 \times n)$ where n is an integer, what can we conclude?
Solution:
Since 11 is prime and $11|(5 \times n)$, by Euclid's Lemma:

$$11|5 \quad \text{or} \quad 11|n$$

Check if $11|5$: $5 = 11(0) + 5$, so $11 \nmid 5$ ×
Therefore, we must have $11|n$. ✓
Conclusion: If $11|(5 \times n)$, then $11|n$.

Corollaries of Euclid's Lemma

Corollary 1: Extended Euclid's Lemma

If p is prime and $p|a_1a_2a_3\cdots a_n$, then:

$$p|a_k \quad \text{for some } k,\ 1 \le k \le n$$

In words: If a prime divides a product of n integers, then it must divide at least one of them.

Proof: Corollary 1

Proof by Induction:
Base Case: $n = 2$
This is Euclid's Lemma, which we already proved. ✓
Inductive Hypothesis: Assume the result is true for $n = k$.
That is, if $p|a_1a_2\cdots a_k$, then $p|a_i$ for some i.
Inductive Step: Prove for $n = k + 1$.
Suppose $p|a_1a_2\cdots a_ka_{k+1}$.
We can write this as:

$$p|(a_1a_2\cdots a_k)\cdot a_{k+1}$$

By Euclid's Lemma (base case):

$$p|(a_1a_2\cdots a_k) \quad \text{or} \quad p|a_{k+1}$$

Case 1: If $p|a_{k+1}$, we are done.
Case 2: If $p|(a_1a_2\cdots a_k)$, then by the inductive hypothesis, $p|a_i$ for some $i \le k$.
In either case, p divides at least one of the factors.
By mathematical induction, the result holds for all $n \ge 2$. □

Example 11: Corollary 1 Application

Given that $5|(2 \times 3 \times 7 \times 10 \times 11)$, which factor must 5 divide?
Solution:
Since 5 is prime and $5|(2 \times 3 \times 7 \times 10 \times 11)$, by Corollary 1:
5 must divide at least one of: 2, 3, 7, 10, 11
Check each:

- $5 \nmid 2$ ×
- $5 \nmid 3$ ×
- $5 \nmid 7$ ×
- $5|10$ because $10 = 5 \times 2$ ✓
- $5 \nmid 11$ ×

Therefore, $5|10$.
Verification: $2 \times 3 \times 7 \times 10 \times 11 = 4620 = 5 \times 924$ ✓

Corollary 2: Product of Primes

If $p, q_1, q_2, \ldots, q_n$ are all prime numbers and:

$$p | q_1 q_2 \cdots q_n$$

then:

$$p = q_k \quad \text{for some } k,\ 1 \leq k \leq n$$

In words: If a prime divides a product of primes, then it must equal one of those primes.

Proof: Corollary 2

Proof:
Let $p, q_1, q_2, \ldots, q_n$ be primes with $p | q_1 q_2 \cdots q_n$.
By Corollary 1, $p | q_k$ for some k where $1 \leq k \leq n$.
Since q_k is prime, its only positive divisors are 1 and q_k.
Since p is also prime (so $p > 1$), we cannot have $p = 1$.
Therefore, $p = q_k$. □

Example 12: Corollary 2 Application

If p is a prime and $p | (3 \times 5 \times 7 \times 11)$, what are the possible values of p?
Solution:
Since all of 3, 5, 7, 11 are primes, by Corollary 2:
p must equal one of these primes.
Therefore:

$$\boxed{p \in \{3, 5, 7, 11\}}$$

Verification:

- If $p = 3$: $3 | (3 \times 5 \times 7 \times 11)$ ✓
- If $p = 5$: $5 | (3 \times 5 \times 7 \times 11)$ ✓
- If $p = 7$: $7 | (3 \times 5 \times 7 \times 11)$ ✓
- If $p = 11$: $11 | (3 \times 5 \times 7 \times 11)$ ✓

Fundamental Theorem of Arithmetic

Theorem: Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be expressed as a product of prime numbers. This representation is unique, except for the order of factors.
In other words:

- **Existence:** Every integer greater than 1 can be factored into primes
- **Uniqueness:** This factorization is unique (up to reordering)

Proof: Fundamental Theorem of Arithmetic

Proof (Existence):
We prove by strong induction on n.
Base Case: $n = 2$
Since 2 is prime, $2 = 2$ (a product of one prime). ✓
Inductive Hypothesis: Assume every integer k with $2 \leq k < n$ can be written as a product of primes.
Inductive Step: Consider integer n.
Case 1: If n is prime, then n is already a product of primes (itself).
Case 2: If n is composite, then $n = ab$ where $1 < a < n$ and $1 < b < n$.
By the inductive hypothesis:

- $a = p_1 p_2 \cdots p_r$ (product of primes)
- $b = q_1 q_2 \cdots q_s$ (product of primes)

Therefore:

$$n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

So n is a product of primes.
By strong induction, every integer $n > 1$ can be expressed as a product of primes. □

Proof (Uniqueness):
Suppose n has two prime factorizations:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where all p_i and q_j are primes.
Since $p_1 | n$, we have $p_1 | (q_1 q_2 \cdots q_s)$.
By Corollary 2, $p_1 = q_k$ for some k.
Reorder so that $p_1 = q_1$.
Cancel p_1 from both sides:

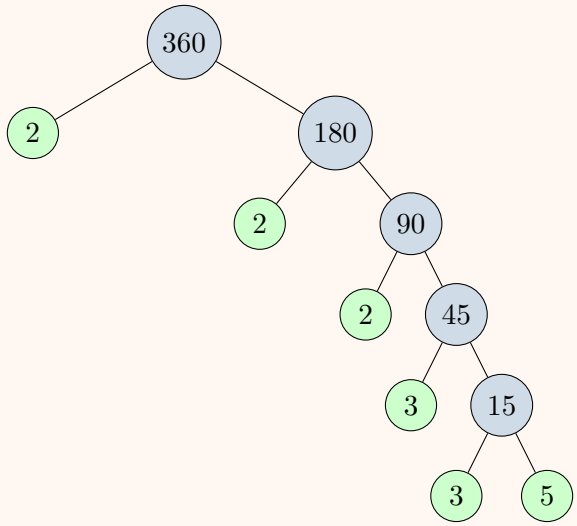
$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Repeat this process. Eventually, all primes on both sides must match.
Therefore, $r = s$ and (after reordering) $p_i = q_i$ for all i.
Hence, the factorization is unique (up to order). □

Example 13: Unique Prime Factorization

Find the prime factorization of 360 and verify uniqueness.

Solution:



Prime factorization:

$$360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 = 2^3 \times 3^2 \times 5$$

Therefore: $\boxed{360 = 2^3 \times 3^2 \times 5}$

Uniqueness: No matter how we factor 360, we always get the same primes with the same exponents (though we might write them in different orders).

Example 14: Different Factorization Paths

Show that factoring 60 by different methods gives the same prime factorization.

Solution:

Method 1: $60 = 2 \times 30 = 2 \times 2 \times 15 = 2 \times 2 \times 3 \times 5$

Method 2: $60 = 4 \times 15 = 2 \times 2 \times 3 \times 5$

Method 3: $60 = 6 \times 10 = 2 \times 3 \times 2 \times 5 = 2 \times 2 \times 3 \times 5$

All methods give: $\boxed{60 = 2^2 \times 3 \times 5}$ ✓

Corollary: Canonical Form

Every positive integer $n > 1$ can be written uniquely in the form:

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$$

where $p_1 < p_2 < p_3 < \cdots < p_r$ are distinct primes and $k_1, k_2, \ldots, k_r$ are positive integers.

This is called the **canonical form** or **standard form** of n.

Example 15: Writing in Canonical Form

Write the following numbers in canonical form: 72, 100, 1000, 2310.

Solution:

For 72:

$$72 = 8 \times 9 = 2^3 \times 3^2$$

Canonical form: $\boxed{72 = 2^3 \times 3^2}$

For 100:

$$100 = 10 \times 10 = (2 \times 5) \times (2 \times 5) = 2^2 \times 5^2$$

Canonical form: $\boxed{100 = 2^2 \times 5^2}$

For 1000:

$$1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$$

Canonical form: $\boxed{1000 = 2^3 \times 5^3}$

For 2310:

$$2310 = 2 \times 1155 = 2 \times 3 \times 385 = 2 \times 3 \times 5 \times 77 = 2 \times 3 \times 5 \times 7 \times 11$$

Canonical form: $\boxed{2310 = 2 \times 3 \times 5 \times 7 \times 11}$

Prime Testing and Properties

Prime Divisor Bound Theorem

Theorem: Prime Divisor Bound

If $n > 1$ is composite, then n has a prime divisor p such that:

$$p \leq \sqrt{n}$$

Proof of Theorem

Proof:
Suppose n is composite.
Then $n = ab$ where $1 < a \leq b < n$.
We claim that $a \leq \sqrt{n}$.
Proof by contradiction:
Suppose $a > \sqrt{n}$.
Then $b \geq a > \sqrt{n}$.
Therefore:

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n$$

This gives $n > n$, which is a contradiction.
Therefore, $a \leq \sqrt{n}$.
Now, since $a > 1$, a has a prime divisor p (by the Fundamental Theorem of Arithmetic).
Since $p|a$ and $a|n$, by transitivity: $p|n$.
Also, $p \leq a \leq \sqrt{n}$.
Therefore, n has a prime divisor p such that $p \leq \sqrt{n}$. □

Practical Application
This theorem gives us an efficient method to test if a number is prime:
To check if n is prime:

1. Calculate $\sqrt{n}$
2. Test divisibility by all primes $p \leq \sqrt{n}$
3. If none divide n, then n is prime
4. If any divides n, then n is composite

This significantly reduces the number of divisibility tests needed!

Example 16: Testing if 97 is Prime

Determine whether 97 is prime.
Solution:
Step 1: Calculate $\sqrt{97}$

$$\sqrt{97} \approx 9.85$$

Step 2: List all primes ≤ 9.85: $2, 3, 5, 7$
Step 3: Test divisibility:

- $97 \div 2 = 48.5$ (not divisible) ×
- $97 \div 3 = 32.33...$ (not divisible) ×

- $97 \div 5 = 19.4$ (not divisible) ×
- $97 \div 7 = 13.857...$ (not divisible) ×

Since 97 is not divisible by any prime $\leq \sqrt{97}$:
Conclusion: 97 is prime ✓

Example 17: Testing if 101 is Prime

Show that 101 is prime.
Solution:
Step 1: Calculate $\sqrt{101}$

$$\sqrt{101} \approx 10.05$$

Step 2: Primes ≤ 10.05: $2, 3, 5, 7$
Step 3: Test divisibility:

- $101 = 2(50) + 1$ ×
- $101 = 3(33) + 2$ ×
- $101 = 5(20) + 1$ ×
- $101 = 7(14) + 3$ ×

Conclusion: 101 is prime ✓

Example 18: Testing if 509 is Prime

Show that 509 is prime.
Solution:
Step 1: Calculate $\sqrt{509}$

$$\sqrt{509} \approx 22.56$$

Step 2: Primes ≤ 22.56: $2, 3, 5, 7, 11, 13, 17, 19$
Step 3: Test divisibility:

Prime	Division	Result
2	$509 \div 2 = 254.5$	Not divisible ×
3	$509 \div 3 = 169.67$	Not divisible ×
5	$509 \div 5 = 101.8$	Not divisible ×
7	$509 \div 7 = 72.71$	Not divisible ×
11	$509 \div 11 = 46.27$	Not divisible ×
13	$509 \div 13 = 39.15$	Not divisible ×
17	$509 \div 17 = 29.94$	Not divisible ×
19	$509 \div 19 = 26.79$	Not divisible ×

Conclusion: 509 is prime ✓

Example 19: Testing if 2093 is Prime

Check whether 2093 is prime or composite. If composite, find its prime factorization.
Solution:

Step 1: Calculate $\sqrt{2093}$

$$\sqrt{2093} \approx 45.75$$

Step 2: Test primes ≤ 45.75: Start with small primes

- Test 2: 2093 is odd $\times$
- Test 3: $2+0+9+3=14$ (not divisible by 3) $\times$
- Test 5: Doesn't end in 0 or 5 $\times$
- Test 7: $2093 \div 7 = 299$ $\checkmark$

So $2093 = 7 \times 299$
Step 3: Factor 299
$\sqrt{299} \approx 17.29$
Test primes ≤ 17.29:

- Test 7: $299 \div 7 = 42.71$ $\times$
- Test 11: $299 \div 11 = 27.18$ $\times$
- Test 13: $299 \div 13 = 23$ $\checkmark$

So $299 = 13 \times 23$
Since 23 is prime (check: $\sqrt{23} < 5$, and 23 is not divisible by 2 or 3):
Complete factorization:

$$\boxed{2093 = 7 \times 13 \times 23}$$

Conclusion: 2093 is composite. $\times$

Example 20: Prime Factorization of 8645

Find the prime factorization of 8645.
Solution:
Observation: 8645 ends in 5, so it's divisible by 5.

$$8645 \div 5 = 1729$$

Now factor 1729: $\sqrt{1729} \approx 41.58$
Test small primes:

- Test 7: $1729 \div 7 = 247$ $\checkmark$

So $1729 = 7 \times 247$
Now factor 247: $\sqrt{247} \approx 15.72$
Test primes:

- Test 7: $247 \div 7 = 35.29$ $\times$
- Test 11: $247 \div 11 = 22.45$ $\times$
- Test 13: $247 \div 13 = 19$ $\checkmark$

So $247 = 13 \times 19$
Since 19 is prime:

Complete factorization:

$$\boxed{8645 = 5 \times 7 \times 13 \times 19}$$

Verification: $5 \times 7 \times 13 \times 19 = 35 \times 247 = 8645$ ✓

Additional Theorems

Theorem: Prime Power Divisibility

If p is a prime and $p|a^n$, then:

$$p^n|a^n$$

Proof of Theorem

Proof:
Given: p is prime and $p|a^n$
Since $a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ times}}$
and $p|a^n$, by Corollary 1 of Euclid's Lemma:
p divides at least one factor a.
So $p|a$, which means $a = pk$ for some integer k.
Therefore:

$$a^n = (pk)^n = p^n k^n$$

This shows that $p^n|a^n$. □

Example 21: Prime Power Divisibility

If $3|a^4$, show that $3^4|a^4$.
Solution:
Given: 3 is prime and $3|a^4$
By the theorem: $3^4|a^4$
Therefore: $\boxed{81|a^4}$
Verification with example: Let $a = 6$

- $a^4 = 6^4 = 1296$
- $3|1296$ ✓
- $3^4 = 81$
- $1296 \div 81 = 16$ ✓

Indeed, $81|1296$.

Theorem: Composite Numbers and Factorials

If $n > 4$ is composite, then:

$$n|(n-1)!$$

Note: This does NOT hold for prime numbers!

Proof of Theorem

Proof:
Since $n > 4$ is composite, $n = ab$ where $1 < a < n$ and $1 < b < n$.
Case 1: $a \neq b$
Then both a and b appear in the product $(n-1)! = 1 \times 2 \times \cdots \times (n-1)$
Therefore, $ab = n$ divides $(n-1)!$. ✓
Case 2: $a = b$
Then $n = a^2$, so $a = \sqrt{n}$.
Since $n > 4$, we have $a = \sqrt{n} > 2$.
Also, $2a = 2\sqrt{n} < 2 \cdot \frac{n}{2} = n$ (for $n > 4$)
So both a and $2a$ are in $\{1, 2, \ldots, n-1\}$ and both divide $(n-1)!$
Therefore, $a \times 2a = 2a^2 = 2n$ divides $(n-1)!$
Since n is even (as $n = a^2$ and if a is odd, $2a$ would make the product even), $n|(n-1)!$.
✓
Thus, in all cases, $n|(n-1)!$. □

Example 22: Composite and Factorial

Show that $6|5!$ and $8|7!$.
Solution:
For $n = 6$:
$6 = 2 \times 3$ (composite, $6 > 4$)
$5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$
$120 \div 6 = 20$ ✓
Indeed, $6|120$.
For $n = 8$:
$8 = 2 \times 4$ (composite, $8 > 4$)
$7! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 = 5040$
$5040 \div 8 = 630$ ✓
Indeed, $8|5040$.

Example 23: Why Primes Don't Satisfy This Property

Show that $5 \nmid 4!$ and $7 \nmid 6!$.
Solution:
For $p = 5$:
$4! = 1 \times 2 \times 3 \times 4 = 24$
$24 \div 5 = 4.8$ (not an integer) ×
So $5 \nmid 24$.
For $p = 7$:
$6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 = 720$
$720 \div 7 = 102.857...$ (not an integer) ×
So $7 \nmid 720$.
Observation: Prime numbers do NOT divide $(n-1)!$ when n is the prime itself. This is actually part of Wilson's Theorem.

Summary: Prime Testing and Properties

1. To test if n is prime, check divisibility by all primes $p \leq \sqrt{n}$
2. If no prime $\leq \sqrt{n}$ divides n, then n is prime

3. If $p|a^n$ (where p is prime), then $p^n|a^n$
4. If $n > 4$ is composite, then $n|(n-1)!$
5. Primes do NOT divide their predecessor factorials

Infinity of Primes

Euclid's Theorem on Infinitely Many Primes

Theorem: Infinitude of Primes (Euclid)

There are infinitely many prime numbers.

Proof: Euclid's Theorem

Proof by Contradiction:

Assume, for the sake of contradiction, that there are only finitely many primes.
Let $p_1, p_2, p_3, \ldots, p_n$ be the complete list of all prime numbers.
Consider the number:

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$$

Observation 1: $N > 1$, so by the Fundamental Theorem of Arithmetic, N is either prime or has a prime divisor.
Case 1: N is prime
Then N is a prime not in our list $\{p_1, p_2, \ldots, p_n\}$ (since $N > p_i$ for all i).
This contradicts our assumption that we listed all primes.
Case 2: N is composite
Then N has a prime divisor p.
Since our list contains all primes, $p = p_k$ for some k.
So $p_k | N$.
But also $p_k | (p_1 p_2 \cdots p_n)$ (since p_k is one of the factors).
By divisibility properties:

$$p_k | [N - p_1 p_2 \cdots p_n] = 1$$

This means $p_k | 1$, which is impossible for a prime $p_k > 1$.
This is a contradiction.
Conclusion: Our assumption was wrong. There cannot be finitely many primes.
Therefore, there are infinitely many primes. □

Example 24: Constructing New Primes

Given primes 2, 3, 5, construct a number that demonstrates Euclid's method.
Solution:
Using the first three primes: $p_1 = 2, p_2 = 3, p_3 = 5$
Construct:

$$N = 2 \times 3 \times 5 + 1 = 30 + 1 = 31$$

Check if 31 is prime:
$\sqrt{31} \approx 5.57$
Test primes ≤ 5.57: 2, 3, 5

- $31 \div 2 = 15.5$ ×
- $31 \div 3 = 10.33$ ×
- $31 \div 5 = 6.2$ ×

Therefore, 31 is prime! ✓
This shows that even if we thought 2, 3, 5 were all the primes, we can construct another prime (31).

Example 25: Another Construction

Use primes 2, 3, 5, 7 to construct N and analyze it.

Solution:

$$N = 2 \times 3 \times 5 \times 7 + 1 = 210 + 1 = 211$$

Check if 211 is prime:
$\sqrt{211} \approx 14.53$
Test primes ≤ 14.53: 2, 3, 5, 7, 11, 13

Prime	Division	Divisible?
2	$211 \div 2 = 105.5$	No ×
3	$211 \div 3 = 70.33$	No ×
5	$211 \div 5 = 42.2$	No ×
7	$211 \div 7 = 30.14$	No ×
11	$211 \div 11 = 19.18$	No ×
13	$211 \div 13 = 16.23$	No ×

Therefore, 211 is prime! ✓
Note: N doesn't have to be prime itself; it just needs to have a prime divisor not in our original list.

Example 26: When N is Not Prime

Use primes 2, 3, 5, 7, 11, 13 and show that N might be composite.

Solution:

$$N = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30030 + 1 = 30031$$

Test small primes:
$30031 \div 59 = 509$ ✓
So $30031 = 59 \times 509$
Check if 509 is prime (we already showed this in Example 18): Yes! ✓
Conclusion: $30031 = 59 \times 509$ (both 59 and 509 are primes)
Notice that 59 and 509 are NOT in our original list $\{2, 3, 5, 7, 11, 13\}$.
This still proves there are more primes beyond our finite list! ✓

Key Insights from Euclid's Proof

1. The proof doesn't construct all primes, just shows they're infinite
2. The number $N = p_1 p_2 \cdots p_n + 1$ is not divisible by any of $p_1, p_2, \ldots, p_n$
3. N might be prime OR composite with new prime factors
4. Either way, we get primes not in our original list
5. This process can continue indefinitely

Bound on the nth Prime

Theorem: Upper Bound for nth Prime

If p_n denotes the nth prime number, then:

$$p_n \leq 2^{2^{n-1}}$$

In words: The nth prime is at most $2^{2^{n-1}}$.

Example 27: Verifying the Bound

Verify the bound for the first few primes.

Solution:

n	p_n	2^{n-1}	$2^{2^{n-1}}$	$p_n \leq 2^{2^{n-1}}$?
1	2	$2^0 = 1$	$2^1 = 2$	$2 \leq 2$ ✓
2	3	$2^1 = 2$	$2^2 = 4$	$3 \leq 4$ ✓
3	5	$2^2 = 4$	$2^4 = 16$	$5 \leq 16$ ✓
4	7	$2^3 = 8$	$2^8 = 256$	$7 \leq 256$ ✓
5	11	$2^4 = 16$	$2^{16} = 65536$	$11 \leq 65536$ ✓

The bound is quite loose (much larger than the actual prime), but it guarantees an upper limit.

Example 28: How Fast the Bound Grows

Show how rapidly $2^{2^{n-1}}$ grows.

Solution:

n	$2^{2^{n-1}}$	Value
1	$2^{2^0} = 2^1$	2
2	$2^{2^1} = 2^2$	4
3	$2^{2^2} = 2^4$	16
4	$2^{2^3} = 2^8$	256
5	$2^{2^4} = 2^{16}$	65,536
6	$2^{2^5} = 2^{32}$	4,294,967,296
7	$2^{2^6} = 2^{64}$	$\approx 1.84 \times 10^{19}$

Observation: The bound grows **doubly exponentially**, meaning it increases extremely rapidly!

Interesting Facts About Primes

- There are infinitely many primes (Euclid, 300 BCE)
- Primes become less frequent as numbers increase
- But they never completely disappear!

Summary: Infinity of Primes

Euclid's Proof Strategy:

1. Assume finitely many primes exist
2. Construct $N = (\text{product of all primes}) + 1$
3. Show N has a prime divisor not in the list
4. Conclude: contradiction, so infinitely many primes exist

Key Points:

- The nth prime $p_n \leq 2^{2^{n-1}}$
- This bound grows extremely fast (doubly exponential)
- Actual primes grow much slower than this bound
- No largest prime exists

Special Prime-Related Numbers

Mersenne Numbers

Definition: Mersenne Number

A **Mersenne number** is a number of the form:

$$M_n = 2^n - 1$$

where n is a positive integer.

Key Points:

- Named after French monk Marin Mersenne (1588-1648)
- If M_n is prime, it is called a **Mersenne prime**
- Not all Mersenne numbers are prime
- Mersenne primes are rare and valuable in mathematics

Example 29: Computing Mersenne Numbers

Calculate M_n for $n = 1, 2, 3, 4, 5, 6, 7, 8$.

Solution:

n	$M_n = 2^n - 1$	Value	Prime?
1	$2^1 - 1$	1	No (1 is not prime)
2	$2^2 - 1$	3	Yes ✓
3	$2^3 - 1$	7	Yes ✓
4	$2^4 - 1$	15	No ($15 = 3 \times 5$)
5	$2^5 - 1$	31	Yes ✓
6	$2^6 - 1$	63	No ($63 = 9 \times 7$)
7	$2^7 - 1$	127	Yes ✓
8	$2^8 - 1$	255	No ($255 = 5 \times 51$)

Mersenne Primes so far: $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$

Example 30: Verifying Mersenne Primes

Verify that $M_3 = 7$ is prime and $M_4 = 15$ is composite.

Solution:

For $M_3 = 7$:

$\sqrt{7} \approx 2.65$

Test primes ≤ 2.65: only 2

$7 \div 2 = 3.5$ (not divisible) ×

Therefore, $M_3 = 7$ is prime. ✓

For $M_4 = 15$:

$15 = 3 \times 5$

Therefore, $M_4 = 15$ is composite. ×

Observation: Even though M_3 is prime, M_4 is not. Mersenne numbers are not always prime!

Theorem: Condition for Mersenne Primes

If $2^n - 1$ is prime, then n must be prime.

⚠ **Important:** The converse is NOT true! If n is prime, $2^n - 1$ might still be composite.

Proof of Theorem

Proof by Contrapositive:

We prove: If n is composite, then $2^n - 1$ is composite.

Suppose n is composite, so $n = ab$ where $1 < a < n$ and $1 < b < n$.

Using the factorization formula:

$$x^{ab} - 1 = (x^a - 1)(x^{a(b-1)} + x^{a(b-2)} + \cdots + x^a + 1)$$

Applying with $x = 2$ and $ab = n$:

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

Since $1 < a < n$:

- $2^a - 1 > 2^1 - 1 = 1$
- $2^a - 1 < 2^n - 1$

So $2^n - 1$ has a non-trivial factor $(2^a - 1)$.

Therefore, $2^n - 1$ is composite. □

By contrapositive: If $2^n - 1$ is prime, then n must be prime.

Example 31: Illustrating the Theorem

Show that $M_6 = 2^6 - 1$ is composite because 6 is composite.

Solution:

Since $6 = 2 \times 3$ (composite), by the theorem, M_6 must be composite.

Direct calculation:

$$M_6 = 2^6 - 1 = 64 - 1 = 63$$

Factorization:

$$63 = 9 \times 7 = 3^2 \times 7$$

Indeed, $M_6 = 63$ is composite. ✓

Using the proof formula with $n = 6 = 2 \times 3$:

$$2^6 - 1 = (2^2 - 1)(2^4 + 2^2 + 1) = 3 \times 21 = 3 \times 21 = 63$$

Example 32: Converse is Not True

Show that even though 11 is prime, M_{11} is composite.

Solution:

Calculate $M_{11} = 2^{11} - 1 = 2048 - 1 = 2047$

Test for primality: $\sqrt{2047} \approx 45.24$

Try small primes:

$$2047 \div 23 = 89$$

So $2047 = 23 \times 89$

Both 23 and 89 are prime, so:

$$M_{11} = 2047 = 23 \times 89$$

Conclusion: Even though 11 is prime, M_{11} is composite. ×

This shows the converse is FALSE!

Summary: Mersenne Numbers

Property	Statement
Definition	$M_n = 2^n - 1$
First Mersenne Primes	$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$
Necessary Condition	If M_n is prime, then n is prime
NOT Sufficient	n prime does NOT guarantee M_n prime

Remember:

- n prime is necessary but NOT sufficient for M_n to be prime
- As of 2024, only 51 Mersenne primes are known
- Largest known prime is often a Mersenne prime

Fermat Numbers

Definition: Fermat Number

A **Fermat number** is a number of the form:

$$F_n = 2^{2^n} + 1$$

where n is a non-negative integer.

Key Points:

- Named after Pierre de Fermat (1607-1665)
- If F_n is prime, it is called a **Fermat prime**
- Fermat conjectured all F_n are prime (later proven FALSE)
- Only 5 known Fermat primes: F_0, F_1, F_2, F_3, F_4

Example 33: Computing Fermat Numbers

Calculate F_n for $n = 0, 1, 2, 3, 4, 5$.

Solution:

n	2^n	$F_n = 2^{2^n} + 1$	Value	Prime?
0	$2^0 = 1$	$2^1 + 1$	3	Yes ✓
1	$2^1 = 2$	$2^2 + 1$	5	Yes ✓
2	$2^2 = 4$	$2^4 + 1$	17	Yes ✓
3	$2^3 = 8$	$2^8 + 1$	257	Yes ✓
4	$2^4 = 16$	$2^{16} + 1$	65,537	Yes ✓
5	$2^5 = 32$	$2^{32} + 1$	4,294,967,297	No

Known Fermat Primes: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$

Example 34: Verifying Fermat Primes

Verify that $F_0 = 3$, $F_1 = 5$, and $F_2 = 17$ are prime.

Solution:

For $F_0 = 3$:

3 is prime (divisible only by 1 and 3). ✓

For $F_1 = 5$:

5 is prime (divisible only by 1 and 5). ✓

For $F_2 = 17$:

$\sqrt{17} \approx 4.12$

Test primes ≤ 4.12: 2, 3

- $17 \div 2 = 8.5$ ×
- $17 \div 3 = 5.67$ ×

Therefore, $F_2 = 17$ is prime. ✓

Example 35: Fermat's Mistake

Show that $F_5 = 2^{32} + 1$ is composite, disproving Fermat's conjecture.
Solution:

$$F_5 = 2^{32} + 1 = 4,294,967,297$$

Euler discovered (in 1732) that:

$$F_5 = 641 \times 6,700,417$$

Verification that 641 divides F_5:
Note that $641 = 5 \times 2^7 + 1 = 640 + 1$
Also $641 = 5^4 + 2^4 = 625 + 16$
Through modular arithmetic (beyond our scope), we can verify:

$$2^{32} \equiv -1 \pmod{641}$$

This means $641 | (2^{32} + 1) = F_5$.
Conclusion: F_5 is composite, so Fermat's conjecture that all F_n are prime is FALSE. ×

Theorems on Fermat Numbers

Theorem 1: Recursive Formula for Fermat Numbers

For $m \geq 0$:

$$F_{m+1} = F_0 \cdot F_1 \cdot F_2 \cdots F_m + 2$$

In words: Each Fermat number equals the product of all previous Fermat numbers plus 2.

Proof of Theorem 1

Proof by Induction:
We need to show: $F_{m+1} = \prod_{k=0}^{m} F_k + 2$
First, note that $F_k = 2^{2^k} + 1$, so $F_k - 1 = 2^{2^k}$
Key Identity:

$$2^{2^{m+1}} - 1 = (2^{2^m})^2 - 1 = (2^{2^m} - 1)(2^{2^m} + 1)$$

Continuing:

$$2^{2^m} - 1 = (2^{2^{m-1}} - 1)(2^{2^{m-1}} + 1)$$

By repeated application:

$$2^{2^{m+1}} - 1 = (2^1 - 1)(2^1 + 1)(2^2 + 1)(2^4 + 1) \cdots (2^{2^m} + 1)$$

$$= 1 \cdot F_0 \cdot F_1 \cdot F_2 \cdots F_m$$

Therefore:

$$2^{2^{m+1}} = F_0 \cdot F_1 \cdot F_2 \cdots F_m + 1$$

Adding 1 to both sides:

$$F_{m+1} = 2^{2^{m+1}} + 1 = F_0 \cdot F_1 \cdot F_2 \cdots F_m + 2$$

This completes the proof. □

Example 36: Verifying the Recursive Formula

Verify the formula for F_3 and F_4.

Solution:

For F_3:

$$F_0 \cdot F_1 \cdot F_2 + 2 = 3 \times 5 \times 17 + 2 = 255 + 2 = 257 = F_3$$

✓

For F_4:

$$F_0 \cdot F_1 \cdot F_2 \cdot F_3 + 2 = 3 \times 5 \times 17 \times 257 + 2$$
$$= 255 \times 257 + 2 = 65535 + 2 = 65537 = F_4$$

✓

Theorem 2: Divisibility Property

If $m < n$, then:

$$F_m | (F_n - 2)$$

In words: Any Fermat number divides two less than any later Fermat number.

Proof of Theorem 2

Proof:

From Theorem 1, we have:

$$F_n = F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1} + 2$$

This can be rewritten as:

$$F_n - 2 = F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}$$

Since $m < n$, F_m appears in the product on the right side.
Therefore, $F_m | (F_n - 2)$. □

Example 37: Verifying Theorem 2

Verify that $F_1 | (F_3 - 2)$ and $F_2 | (F_4 - 2)$.

Solution:

For $F_1 | (F_3 - 2)$:

$F_1 = 5$ and $F_3 - 2 = 257 - 2 = 255$
$255 \div 5 = 51$ ✓
Indeed, $5 | 255$.

For $F_2 | (F_4 - 2)$:

$F_2 = 17$ and $F_4 - 2 = 65537 - 2 = 65535$
$65535 \div 17 = 3855$ ✓
Indeed, $17 | 65535$.

Theorem 3: Pairwise Coprimality

For $m \neq n$:

$$\gcd(F_m, F_n) = 1$$

In words: Any two distinct Fermat numbers are relatively prime (coprime).

Proof of Theorem 3

Proof:
Without loss of generality, assume $m < n$.
Let $d = \gcd(F_m, F_n)$.
From Theorem 2: $F_m | (F_n - 2)$
So there exists integer k such that $F_n - 2 = F_m \cdot k$.
This gives: $F_n = F_m \cdot k + 2$
Since $d|F_m$ and $d|F_n$:

$$d|(F_n - F_m \cdot k) = 2$$

So $d|2$, which means $d \in \{1, 2\}$.
But all Fermat numbers $F_n = 2^{2^n} + 1$ are odd (even power of 2 plus 1).
Since both F_m and F_n are odd, their GCD cannot be 2.
Therefore, $d = 1$.
Hence, $\gcd(F_m, F_n) = 1$. □

Example 38: Verifying Coprimality

Verify that $\gcd(F_0, F_1) = 1$ and $\gcd(F_1, F_2) = 1$.
Solution:
For $\gcd(F_0, F_1) = \gcd(3, 5)$**:**
Divisors of 3: 1, 3
Divisors of 5: 1, 5
Common divisors: 1
Therefore, $\gcd(3, 5) = 1$ ✓
For $\gcd(F_1, F_2) = \gcd(5, 17)$**:**
Since both are prime and distinct:
$\gcd(5, 17) = 1$ ✓

Summary: Fermat Numbers

Property	Statement
Definition	$F_n = 2^{2^n} + 1$
Known Fermat Primes	$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$
Recursive Formula	$F_{m+1} = F_0 F_1 \cdots F_m + 2$
Divisibility	If $m < n$, then $F_m \mid (F_n - 2)$
Coprimality	$\gcd(F_m, F_n) = 1$ for $m \neq n$

Important Facts:

- Only 5 Fermat primes are known
- F_5 and beyond are all known to be composite
- Fermat numbers grow extremely rapidly
- Any two Fermat numbers are coprime

The Sieve of Eratosthenes

The Sieve of Eratosthenes

The **Sieve of Eratosthenes** is an ancient algorithm for finding all prime numbers up to a given limit n. It was developed by the Greek mathematician Eratosthenes of Cyrene (276-194 BCE).

Algorithm Steps:

1. List all integers from 2 to n
2. Start with the first number (2), mark it as prime
3. Cross out all multiples of 2 (except 2 itself)
4. Move to the next unmarked number, mark it as prime
5. Cross out all its multiples
6. Repeat until you reach $\sqrt{n}$
7. All remaining unmarked numbers are prime

Example 39: Sieve of Eratosthenes for n

Find all primes up to 30 using the Sieve of Eratosthenes.

Solution:

Step 1: List numbers from 2 to 30.

Step 2: Mark 2 as prime, cross out multiples of 2:

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}, 23, \cancel{24}, 25, \cancel{26}, 27, \cancel{28}, 29, \cancel{30}$$

Step 3: Mark 3 as prime, cross out multiples of 3:

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, 25, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}$$

Step 4: Mark 5 as prime, cross out multiples of 5:

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}$$

Step 5: Since $\sqrt{30} \approx 5.48$, we stop here. All remaining unmarked numbers are prime.

Primes up to 30:

$$\boxed{2, 3, 5, 7, 11, 13, 17, 19, 23, 29}$$

Visual Sieve: Primes up to 50

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50

Prime
Composite
Neither

Example 40: Why Stop at $\sqrt{n}$?

Explain why we only need to check primes up to $\sqrt{n}$ in the Sieve.

Solution:

Suppose n is composite. Then $n = ab$ where $1 < a \leq b < n$.

If both $a > \sqrt{n}$ and $b > \sqrt{n}$, then:

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n$$

This is a contradiction.

Therefore, at least one factor must be $\leq \sqrt{n}$.

This means: if n is composite, it will be crossed out when we eliminate multiples of some prime $p \leq \sqrt{n}$.

Example for $n = 50$:

$\sqrt{50} \approx 7.07$

We only need to check primes: 2, 3, 5, 7

All composites up to 50 will be eliminated by removing multiples of these primes. ✓

Efficiency of the Sieve

Advantages:

- Very efficient for finding many primes at once
- Simple to implement
- Requires only basic arithmetic operations
- No division needed (only marking multiples)

Time Complexity: $O(n \log \log n)$ - very efficient!

Space Complexity: $O(n)$ - need to store all numbers up to n

Example 41: Count Primes up to 100

How many primes are there up to 100?

Solution:

Using the Sieve of Eratosthenes, we find all primes up to 100:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97					

Count: There are $\boxed{25}$ primes up to 100.

Observation: Primes make up 25% of integers up to 100, but this percentage decreases as numbers get larger.

Prime Distribution

Prime Counting Function

The **prime counting function** $\pi(n)$ is defined as the number of primes less than or equal to n.

Examples:

- $\pi(10) = 4$ (primes: 2, 3, 5, 7)
- $\pi(20) = 8$ (primes: 2, 3, 5, 7, 11, 13, 17, 19)
- $\pi(100) = 25$

Example 42: Computing $\pi(n)$

Find $\pi(30)$ and $\pi(50)$.

Solution:

For $\pi(30)$:

Primes ≤ 30: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Count: $\boxed{\pi(30) = 10}$

For $\pi(50)$:

Primes ≤ 50: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Count: $\boxed{\pi(50) = 15}$

Prime Number Theorem (Informal)

The **Prime Number Theorem** states that the number of primes less than or equal to n is approximately:

$$\pi(n) \approx \frac{n}{\ln n}$$

where $\ln n$ is the natural logarithm of n.

In words: Primes become less frequent as numbers get larger, at a rate inversely proportional to the logarithm.

Example 43: Approximating Prime Count

Use the Prime Number Theorem to approximate $\pi(100)$ and compare with the actual value.

Solution:

Using the approximation:

$$\pi(100) \approx \frac{100}{\ln 100} = \frac{100}{4.605} \approx 21.7$$

Actual value: $\pi(100) = 25$

Error: $|25 - 21.7| = 3.3$

Percentage error: $\frac{3.3}{25} \times 100\% = 13.2\%$

The approximation is reasonably close! The accuracy improves for larger values of n.

Summary: Prime Distribution

n	$\pi(n)$ (actual)	$\frac{n}{\ln n}$ (approx)	Ratio of primes
10	4	4.3	40%
100	25	21.7	25%
1,000	168	144.8	16.8%
10,000	1,229	1,085.7	12.3%

Key Observation: As n increases, primes become less dense, but they never disappear!

Prime Gaps

The **gap** between consecutive primes p_n and p_{n+1} is defined as:

$$g_n = p_{n+1} - p_n$$

Facts about gaps:

- The only gap of size 1 is between 2 and 3
- All other gaps are even numbers (since all other primes are odd)
- Prime gaps can be arbitrarily large
- Small gaps occur infinitely often (Twin Prime Conjecture - unproven)

Example 44: Computing Prime Gaps

Find the gaps between the first 10 primes.

Solution:

p_n	p_{n+1}	Gap $g_n = p_{n+1} - p_n$
2	3	1
3	5	2
5	7	2
7	11	4
11	13	2
13	17	4
17	19	2
19	23	4
23	29	6

Observations:

- Smallest gap: 1 (between 2 and 3)
- Most common gap so far: 2 (twin primes)
- Gaps are increasing on average

Practice Exercises

Problem 1

Determine whether 143 is prime or composite. If composite, find its prime factorization.

Problem 2

Show that 191 is prime using the prime divisor bound theorem.

Problem 3

Find the prime factorization of 1260 and write it in canonical form.

Problem 4

List all twin prime pairs between 50 and 100.

Problem 5

If $7|(3 \times 5 \times n)$, what can you conclude about n using Euclid's Lemma?

Problem 6

Prove that if p is a prime and $p|a^3$, then $p^3|a^3$.

Problem 7

Show that $10|9!$ using the theorem about composite numbers and factorials.

Problem 8

Verify that $13 \nmid 12!$ (13 does not divide 12 factorial).

Problem 9

Using Euclid's method, construct a number N from the first four primes and determine if N is prime or composite.

Problem 10

Calculate $M_6 = 2^6 - 1$ and $M_7 = 2^7 - 1$. Determine which one is prime.

Problem 11

Show that if $n = 12$ is composite, then $M_{12} = 2^{12} - 1$ must be composite.

Problem 12

Compute Fermat numbers F_0, F_1, F_2 and verify that they are prime.

Problem 13

Verify the recursive formula $F_2 = F_0 \cdot F_1 + 2$ for Fermat numbers.

Problem 14

Show that $F_0|(F_2 - 2)$ using the divisibility property of Fermat numbers.

Problem 15

Prove that $\gcd(F_0, F_2) = 1$ by direct calculation.

Problem 16

Use the Sieve of Eratosthenes to find all prime numbers up to 60.

Problem 17

Calculate $\pi(40)$ (the number of primes less than or equal to 40).

Problem 18

Use the Prime Number Theorem to approximate $\pi(1000)$ and compare it with the actual value (which is 168).

Problem 19

Find the gaps between consecutive primes from 31 to 53.

Problem 20

Show that there exist arbitrarily large gaps between consecutive primes. (Hint: Consider $n! + 2, n! + 3, \ldots, n! + n$)

Chapter 3

Theory of Congruences

Introduction to Congruences

Definition: Congruence Relation

Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is **congruent to** b **modulo** m, written as:

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

if and only if $m|(a-b)$.
Equivalently, $a \equiv b \pmod{m}$ if and only if there exists an integer k such that:

$$a - b = km \quad \text{or} \quad a = b + km$$

Key Terminology:

- m is called the **modulus**
- We read $a \equiv b \pmod{m}$ as "a is congruent to b modulo m"
- If $a \not\equiv b \pmod{m}$, we say a is **not congruent to** b modulo m
- The notation $\pmod{m}$ indicates we are working in modular arithmetic

Example 1: Verifying Congruences

Determine whether the following congruences are true:
Solution:
(a) $17 \equiv 5 \pmod{12}$
Check if $12|(17-5)$:

$$17 - 5 = 12 = 12 \times 1$$

Since $12|12$, we have $17 \equiv 5 \pmod{12}$. ✓
(b) $-3 \equiv 7 \pmod{10}$
Check if $10|(-3-7)$:

$$-3 - 7 = -10 = 10 \times (-1)$$

Since $10|(-10)$, we have $-3 \equiv 7 \pmod{10}$. ✓
(c) $23 \equiv 8 \pmod{5}$
Check if $5|(23-8)$:

$$23 - 8 = 15 = 5 \times 3$$

Since $5|15$, we have $23 \equiv 8 \pmod{5}$. ✓

(d) $14 \equiv 5 \pmod 4$
Check if $4|(14-5)$:

$$14 - 5 = 9 = 4 \times 2 + 1$$

Since $4 \nmid 9$, we have $14 \not\equiv 5 \pmod 4$. ×

Example 2: Finding Congruent Numbers

Find three positive integers that are congruent to 7 modulo 12.
Solution:
We need integers of the form $a = 7 + 12k$ for $k \in \mathbb{Z}$.
For positive integers:

- $k = 0$: $a = 7 + 12(0) = 7$
- $k = 1$: $a = 7 + 12(1) = 19$
- $k = 2$: $a = 7 + 12(2) = 31$
- $k = 3$: $a = 7 + 12(3) = 43$

Therefore: $\boxed{7, 19, 31, 43, \ldots}$ are all congruent to 7 modulo 12.
Verification:

- $19 - 7 = 12 = 12(1)$ ✓
- $31 - 7 = 24 = 12(2)$ ✓
- $43 - 7 = 36 = 12(3)$ ✓

Example 3: Negative Numbers in Congruences

Show that $-15 \equiv 6 \pmod 7$.
Solution:
Check if $7|(-15-6)$:

$$-15 - 6 = -21 = 7 \times (-3)$$

Since $7|(-21)$, we have $-15 \equiv 6 \pmod 7$. ✓
Alternative method:
We can also write: $-15 = 6 + 7k$
Solving: $k = \frac{-15-6}{7} = \frac{-21}{7} = -3$ ✓

Important Observations

1. If $a \equiv b \pmod m$, then a and b differ by a multiple of m
2. Infinitely many integers are congruent to any given integer modulo m
3. Negative numbers can be congruent to positive numbers
4. $a \equiv 0 \pmod m$ if and only if $m|a$

Theorem: Congruence is an Equivalence Relation

Congruence modulo m is an equivalence relation on $\mathbb{Z}$. That is, for all $a, b, c \in \mathbb{Z}$:

(i) **Reflexive:** $a \equiv a \pmod{m}$

(ii) **Symmetric:** If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

(iii) **Transitive:** If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

Proof: Congruence is an Equivalence Relation

Proof:
We verify each property:

(i) Reflexive Property:
We need to show $a \equiv a \pmod{m}$ for all $a \in \mathbb{Z}$.
Consider:

$$a - a = 0 = m \times 0$$

Since $m|0$ (as $0 = m \times 0$), we have $m|(a - a)$.
Therefore, $a \equiv a \pmod{m}$. ✓

(ii) Symmetric Property:
Assume $a \equiv b \pmod{m}$.
Then $m|(a - b)$, so there exists $k \in \mathbb{Z}$ such that:

$$a - b = km$$

Multiplying both sides by -1:

$$b - a = -km = m \times (-k)$$

Since $-k \in \mathbb{Z}$, we have $m|(b - a)$.
Therefore, $b \equiv a \pmod{m}$. ✓

(iii) Transitive Property:
Assume $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.
Then:

- $m|(a - b)$, so $a - b = k_1 m$ for some $k_1 \in \mathbb{Z}$
- $m|(b - c)$, so $b - c = k_2 m$ for some $k_2 \in \mathbb{Z}$

Adding these equations:

$$(a - b) + (b - c) = k_1 m + k_2 m$$

$$a - c = (k_1 + k_2)m$$

Since $k_1 + k_2 \in \mathbb{Z}$, we have $m|(a - c)$.
Therefore, $a \equiv c \pmod{m}$. ✓

Conclusion: Since all three properties hold, congruence modulo m is an equivalence relation. □

Example 4: Demonstrating Reflexive Property

Verify the reflexive property for $a = 25$ and $m = 7$.
Solution:
We need to show $25 \equiv 25 \pmod 7$.
Check: $25 - 25 = 0 = 7 \times 0$
Since $7|0$, we have $25 \equiv 25 \pmod 7$. ✓

Example 5: Demonstrating Symmetric Property

Given $13 \equiv 3 \pmod 5$, verify that $3 \equiv 13 \pmod 5$.
Solution:
Given: $13 \equiv 3 \pmod 5$
This means $5|(13 - 3) = 10$. ✓
To verify: $3 \equiv 13 \pmod 5$
Check: $3 - 13 = -10 = 5 \times (-2)$
Since $5|(-10)$, we have $3 \equiv 13 \pmod 5$. ✓

Example 6: Demonstrating Transitive Property

Given $17 \equiv 11 \pmod 6$ and $11 \equiv 5 \pmod 6$, verify that $17 \equiv 5 \pmod 6$.
Solution:
Given:

- $17 \equiv 11 \pmod 6$: Check $17 - 11 = 6 = 6(1)$ ✓
- $11 \equiv 5 \pmod 6$: Check $11 - 5 = 6 = 6(1)$ ✓

By transitivity: $17 \equiv 5 \pmod 6$
Verification: $17 - 5 = 12 = 6(2)$
Since $6|12$, we have $17 \equiv 5 \pmod 6$. ✓

Theorem: Remainder Interpretation

For integers a and b, and $m > 0$:

$$a \equiv b \pmod m$$

if and only if a and b leave the same non-negative remainder when divided by m.

Proof: Remainder Interpretation

Proof:
Forward Direction ($\Rightarrow$):
Assume $a \equiv b \pmod m$.
By the Division Algorithm:

- $a = mq_1 + r_1$ where $0 \leq r_1 < m$
- $b = mq_2 + r_2$ where $0 \leq r_2 < m$

Since $a \equiv b \pmod m$, we have $m|(a - b)$.
Therefore:

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

Since $m|(a-b)$, we have:

$$m|[m(q_1-q_2)+(r_1-r_2)]$$

This means:

$$m|(r_1-r_2)$$

But $0 \leq r_1 < m$ and $0 \leq r_2 < m$, so:

$$-m < r_1 - r_2 < m$$

The only multiple of m in the interval $(-m, m)$ is 0.
Therefore, $r_1 - r_2 = 0$, which gives $r_1 = r_2$. ✓

Backward Direction ($\Leftarrow$):
Assume a and b leave the same remainder r when divided by m.
Then:

- $a = mq_1 + r$
- $b = mq_2 + r$

Subtracting:

$$a - b = m(q_1 - q_2) + r - r = m(q_1 - q_2)$$

Therefore, $m|(a-b)$, which means $a \equiv b \pmod{m}$. ✓

Conclusion: Both directions proven. □

Example 7: Using Remainder Interpretation

Show that $47 \equiv 11 \pmod{9}$ using the remainder interpretation.
Solution:
Divide both numbers by 9:
For 47:

$$47 = 9(5) + 2$$

Remainder $= 2$
For 11:

$$11 = 9(1) + 2$$

Remainder $= 2$
Since both have the same remainder (2), we conclude:

$$47 \equiv 11 \pmod{9}$$

Direct verification: $47 - 11 = 36 = 9(4)$ ✓

Example 8: Finding Remainder Using Congruence

If $a \equiv 7 \pmod{12}$, what is the remainder when a is divided by 12?
Solution:
By the Remainder Interpretation Theorem, if $a \equiv 7 \pmod{12}$, then a and 7 leave the same remainder when divided by 12.
Since $7 = 12(0) + 7$, the remainder when 7 is divided by 12 is 7.
Therefore, the remainder when a is divided by 12 is $\boxed{7}$.

Examples:

- $a = 19$: $19 = 12(1) + 7$ ✓
- $a = 31$: $31 = 12(2) + 7$ ✓
- $a = -5$: $-5 = 12(-1) + 7$ ✓

Example 9: Non-Congruent Numbers

Show that 25 and 13 are not congruent modulo 7 using remainders.

Solution:

Find remainders when divided by 7:

For 25:

$$25 = 7(3) + 4$$

Remainder $= 4$

For 13:

$$13 = 7(1) + 6$$

Remainder $= 6$

Since $4 \neq 6$, the remainders are different.

Therefore, $25 \not\equiv 13 \pmod 7$. ×

Direct verification: $25 - 13 = 12 = 7(1) + 5$

Since $7 \nmid 12$, indeed $25 \not\equiv 13 \pmod 7$. ✓

Summary: Introduction to Congruences

Concept	Key Point
Definition	$a \equiv b \pmod m \iff m \mid (a-b)$
Equivalence Relation	Reflexive, Symmetric, Transitive
Remainder Property	Same remainder when divided by m
Testing Congruence	Check if m divides $(a-b)$

Remember:

- Congruence is like equality, but "modulo m"
- Think of it as "clock arithmetic"
- $a \equiv 0 \pmod m$ means m divides a

Properties and Operations on Congruences

Algebraic Properties of Congruences

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

(i) **Addition Property:**

$$a + c \equiv b + d \pmod{m}$$

(ii) **Subtraction Property:**

$$a - c \equiv b - d \pmod{m}$$

(iii) **Multiplication Property:**

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

(iv) **Linear Combination Property:**

For any integers x and y:

$$ax + cy \equiv bx + dy \pmod{m}$$

Key Point: These properties allow us to perform arithmetic operations on congruences just like we do with equations.

Proof: Addition Property

Proof:

Given: $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

To prove: $a + c \equiv b + d \pmod{m}$

Since $a \equiv b \pmod{m}$, we have $m|(a - b)$, so:

$$a - b = k_1 m \quad \text{for some } k_1 \in \mathbb{Z}$$

Since $c \equiv d \pmod{m}$, we have $m|(c - d)$, so:

$$c - d = k_2 m \quad \text{for some } k_2 \in \mathbb{Z}$$

Adding these equations:

$$(a - b) + (c - d) = k_1 m + k_2 m$$

$$(a + c) - (b + d) = (k_1 + k_2)m$$

Since $k_1 + k_2 \in \mathbb{Z}$, we have $m|[(a + c) - (b + d)]$.

Therefore, $a + c \equiv b + d \pmod{m}$. □

Example 10: Addition Property

Given $23 \equiv 8 \pmod{5}$ and $17 \equiv 2 \pmod{5}$, find $23 + 17 \pmod{5}$.

Solution:

By the addition property:

$$23 + 17 \equiv 8 + 2 \pmod{5}$$

$$40 \equiv 10 \pmod{5}$$

Simplify further:

$$10 = 5(2) + 0$$

So $10 \equiv 0 \pmod 5$.
Therefore: $\boxed{23 + 17 \equiv 0 \pmod 5}$
Verification: $40 = 5(8) + 0$ ✓

Proof: Multiplication Property

Proof:
Given: $a \equiv b \pmod m$ and $c \equiv d \pmod m$
To prove: $ac \equiv bd \pmod m$
Since $a \equiv b \pmod m$ and $c \equiv d \pmod m$:

$$a = b + k_1 m \quad \text{and} \quad c = d + k_2 m$$

for some integers k_1, k_2.
Multiply:

$$ac = (b + k_1 m)(d + k_2 m)$$
$$= bd + bk_2 m + dk_1 m + k_1 k_2 m^2$$
$$= bd + m(bk_2 + dk_1 + k_1 k_2 m)$$

Therefore:

$$ac - bd = m(bk_2 + dk_1 + k_1 k_2 m)$$

Since the expression in parentheses is an integer, we have $m|(ac - bd)$.
Therefore, $ac \equiv bd \pmod m$. □

Example 11: Multiplication Property

Given $11 \equiv 3 \pmod 4$ and $9 \equiv 1 \pmod 4$, find $11 \times 9 \pmod 4$.
Solution:
By the multiplication property:

$$11 \times 9 \equiv 3 \times 1 \pmod 4$$

$$99 \equiv 3 \pmod 4$$

Verification:

$$99 = 4(24) + 3$$

So $99 \equiv 3 \pmod 4$. ✓
Therefore: $\boxed{11 \times 9 \equiv 3 \pmod 4}$

Proof: Linear Combination Property

Proof:
Given: $a \equiv b \pmod m$ and $c \equiv d \pmod m$
To prove: $ax + cy \equiv bx + dy \pmod m$ for all $x, y \in \mathbb{Z}$
Since $a \equiv b \pmod m$:

$$a - b = k_1 m$$

Multiply by x:

$$ax - bx = k_1 mx$$

So $ax \equiv bx \pmod{m}$ $\cdots(1)$
Since $c \equiv d \pmod{m}$:

$$c - d = k_2 m$$

Multiply by y:

$$cy - dy = k_2 my$$

So $cy \equiv dy \pmod{m}$ $\cdots(2)$
Adding congruences (1) and (2) using the addition property:

$$ax + cy \equiv bx + dy \pmod{m}$$

□

Example 12: Linear Combination

Given $7 \equiv 2 \pmod{5}$ and $13 \equiv 3 \pmod{5}$, find $7(4) + 13(3) \pmod{5}$.
Solution:
By the linear combination property with $x = 4$ and $y = 3$:

$$7(4) + 13(3) \equiv 2(4) + 3(3) \pmod{5}$$

$$28 + 39 \equiv 8 + 9 \pmod{5}$$

$$67 \equiv 17 \pmod{5}$$

Simplify: $17 = 5(3) + 2$, so $17 \equiv 2 \pmod{5}$
Therefore: $\boxed{7(4) + 13(3) \equiv 2 \pmod{5}}$
Direct verification: $67 = 5(13) + 2$ ✓

Theorem: Power Property

If $a \equiv b \pmod{m}$, then for any positive integer k:

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

In words: Congruent numbers raised to the same power remain congruent.

Proof: Power Property

Proof by Induction:
Base Case: $k = 1$
$a^1 \equiv b^1 \pmod{m}$ is given. ✓
Inductive Hypothesis: Assume $a^k \equiv b^k \pmod{m}$ for some positive integer k.
Inductive Step: Prove $a^{k+1} \equiv b^{k+1} \pmod{m}$
We have:

$$a^{k+1} = a^k \cdot a$$

$$b^{k+1} = b^k \cdot b$$

By the inductive hypothesis: $a^k \equiv b^k \pmod{m}$
By the given: $a \equiv b \pmod{m}$

Using the multiplication property:

$$a^k \cdot a \equiv b^k \cdot b \pmod{m}$$

$$a^{k+1} \equiv b^{k+1} \pmod{m}$$

By mathematical induction, the result holds for all positive integers k. □

Example 13: Computing Large Powers

Find $7^{100} \pmod 6$.

Solution:

First, simplify the base:

$$7 \equiv 1 \pmod 6$$

By the power property:

$$7^{100} \equiv 1^{100} \pmod 6$$

$$7^{100} \equiv 1 \pmod 6$$

Therefore: $\boxed{7^{100} \equiv 1 \pmod 6}$

Note: Without this property, computing 7^{100} directly would be extremely difficult!

Example 14: Another Power Calculation

Find $3^{50} \pmod 8$.

Solution:

First find a pattern:

$$3^1 = 3 \equiv 3 \pmod 8$$

$$3^2 = 9 \equiv 1 \pmod 8$$

Since $3^2 \equiv 1 \pmod 8$, we can use the power property:

$$3^{50} = (3^2)^{25} \equiv 1^{25} \pmod 8$$

$$3^{50} \equiv 1 \pmod 8$$

Therefore: $\boxed{3^{50} \equiv 1 \pmod 8}$

Theorem: Cancellation Law

If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, then:

$$a \equiv b \pmod m$$

⚠ **Warning:** The condition $\gcd(c, m) = 1$ is essential. Without it, cancellation may not be valid!

Proof: Cancellation Law

Proof:

Given: $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$

Since $ac \equiv bc \pmod{m}$:

$$m|(ac - bc)$$

$$m|c(a - b)$$

Since $\gcd(c, m) = 1$ and $m|c(a - b)$, by Euclid's Lemma:

$$m|(a - b)$$

Therefore, $a \equiv b \pmod{m}$. □

Example 15: Valid Cancellation

Given $5 \times 7 \equiv 5 \times 3 \pmod{4}$, find the relationship between 7 and 3 modulo 4.

Solution:

We have $35 \equiv 15 \pmod{4}$.

Check if we can cancel 5: $\gcd(5, 4) = 1$ ✓

Since $\gcd(5, 4) = 1$, we can cancel:

$$7 \equiv 3 \pmod{4}$$

Verification: $7 - 3 = 4 = 4(1)$, so indeed $7 \equiv 3 \pmod{4}$. ✓

Example 16: When Cancellation Fails

Consider $2 \times 3 \equiv 2 \times 6 \pmod{6}$.

Can we cancel 2 to conclude $3 \equiv 6 \pmod{6}$?

Solution:

Check the gcd: $\gcd(2, 6) = 2 \neq 1$ ×

Since $\gcd(2, 6) \neq 1$, we **cannot** simply cancel 2.

Let's verify:

- $2 \times 3 = 6 \equiv 0 \pmod{6}$ ✓
- $2 \times 6 = 12 \equiv 0 \pmod{6}$ ✓

So the original congruence is true.

But if we claimed $3 \equiv 6 \pmod{6}$:

$$3 - 6 = -3$$

Since $6 \nmid (-3)$, we have $3 \not\equiv 6 \pmod{6}$. ×

Conclusion: Cancellation failed because $\gcd(2, 6) \neq 1$!

Corollary 1: Cancellation with Coprime Factor

If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = d > 1$, then:

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

In words: When we cannot cancel completely, we can reduce the modulus.

Example 17: Modified Cancellation

From Example 16: $2 \times 3 \equiv 2 \times 6 \pmod{6}$
Solution:
Here $\gcd(2, 6) = 2$, so we get:

$$3 \equiv 6 \pmod{\frac{6}{2}}$$

$$3 \equiv 6 \pmod{3}$$

Verification: $6 - 3 = 3 = 3(1)$
So $3 \equiv 6 \pmod{3}$ is true! ✓

Corollary 2: Cancellation with Prime Modulus

If $ac \equiv bc \pmod{p}$ where p is prime and $p \nmid c$, then:

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

Key Point: For prime modulus, we can always cancel non-zero factors.

Example 18: Cancellation with Prime Modulus

Given $5 \times 8 \equiv 5 \times 2 \pmod{7}$, can we cancel 5?
Solution:
Check conditions:

- $p = 7$ is prime ✓
- $7 \nmid 5$ ✓

By Corollary 2, we can cancel:

$$8 \equiv 2 \pmod{7}$$

Verification: $8 - 2 = 6$, and $7 \nmid 6$
Wait, this means $8 \not\equiv 2 \pmod{7}$!
Let me recalculate: $8 = 7(1) + 1$, so $8 \equiv 1 \pmod{7}$
And $2 \equiv 2 \pmod{7}$
So the original statement $5 \times 8 \equiv 5 \times 2 \pmod{7}$ must be false!
Check: $5 \times 8 = 40 = 7(5) + 5 \equiv 5 \pmod{7}$
And: $5 \times 2 = 10 = 7(1) + 3 \equiv 3 \pmod{7}$
Since $5 \not\equiv 3 \pmod{7}$, the premise was incorrect. ×

Theorem: GCD Preservation

If $a \equiv b \pmod{m}$, then:

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

Proof: GCD Preservation

Proof:
Given: $a \equiv b \pmod{m}$
Then $a = b + km$ for some integer k.
Let $d_1 = \gcd(a, m)$ and $d_2 = \gcd(b, m)$.
Show $d_1 | d_2$:

Since $d_1|a$ and $d_1|m$:

$$d_1|(a - km) = b$$

So $d_1|b$ and $d_1|m$, which means $d_1|\gcd(b, m) = d_2$.
Show $d_2|d_1$:
Since $d_2|b$ and $d_2|m$:

$$d_2|(b + km) = a$$

So $d_2|a$ and $d_2|m$, which means $d_2|\gcd(a, m) = d_1$.
Since $d_1|d_2$ and $d_2|d_1$, and both are positive:

$$d_1 = d_2$$

Therefore, $\gcd(a, m) = \gcd(b, m)$. □

Example 19: GCD Preservation

Given $23 \equiv 8 \pmod 5$, verify that $\gcd(23, 5) = \gcd(8, 5)$.
Solution:
Calculate both GCDs:
$\gcd(23, 5)$:

$$\begin{aligned} 23 &= 5(4) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

So $\gcd(23, 5) = 1$
$\gcd(8, 5)$:

$$\begin{aligned} 8 &= 5(1) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

So $\gcd(8, 5) = 1$
Indeed, $\gcd(23, 5) = \gcd(8, 5) = 1$ ✓

Theorem: Divisor of Modulus

If $a \equiv b \pmod m$ and $n|m$, then:

$$a \equiv b \pmod n$$

In words: If a congruence holds for a modulus, it also holds for any divisor of that modulus.

Proof: Divisor of Modulus

Proof:
Given: $a \equiv b \pmod m$ and $n|m$

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

$$m|(a-b)$$

So $a - b = km$ for some integer k.
Since $n|m$, we have $m = nt$ for some integer t.
Substituting:

$$a - b = k(nt) = (kt)n$$

Since kt is an integer, we have $n|(a-b)$.
Therefore, $a \equiv b \pmod{n}$. □

Example 20: Divisor of Modulus

Given $37 \equiv 13 \pmod{24}$, find $37 \pmod{12}$, $37 \pmod{6}$, and $37 \pmod{3}$.
Solution:
Since $12|24$, $6|24$, and $3|24$, we have:
(a) $37 \equiv 13 \pmod{12}$
Verify: $37 - 13 = 24 = 12(2)$ ✓
(b) $37 \equiv 13 \pmod{6}$
Verify: $37 - 13 = 24 = 6(4)$ ✓
(c) $37 \equiv 13 \pmod{3}$
Verify: $37 - 13 = 24 = 3(8)$ ✓
Simplify further:

- $13 = 12(1) + 1$, so $37 \equiv 1 \pmod{12}$
- $13 = 6(2) + 1$, so $37 \equiv 1 \pmod{6}$
- $13 = 3(4) + 1$, so $37 \equiv 1 \pmod{3}$

Theorem: Scaling Property

If $a \equiv b \pmod{m}$ and $c > 0$, then:

$$ac \equiv bc \pmod{mc}$$

Proof: Scaling Property

Proof:
Given: $a \equiv b \pmod{m}$
Then $m|(a-b)$, so $a - b = km$ for some integer k.
Multiply both sides by c:

$$c(a-b) = c(km)$$

$$ac - bc = (km)c = k(mc)$$

Therefore, $mc|(ac-bc)$, which means:

$$ac \equiv bc \pmod{mc}$$

□

Example 21: Scaling Property

Given $7 \equiv 3 \pmod{4}$, find $7 \times 5 \pmod{4 \times 5}$.

Solution:

By the scaling property with $c = 5$:

$$7 \times 5 \equiv 3 \times 5 \pmod{4 \times 5}$$

$$35 \equiv 15 \pmod{20}$$

Verification: $35 - 15 = 20 = 20(1)$ ✓

Theorem: Division Property

If $a \equiv b \pmod{m}$ and $d > 0$ divides a, b, and m, then:

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

Proof: Division Property

Proof:

Given: $a \equiv b \pmod{m}$ and $d|a$, $d|b$, $d|m$

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

$$m|(a-b)$$

So $a - b = km$ for some integer k.

Divide both sides by d:

$$\frac{a-b}{d} = k \cdot \frac{m}{d}$$

$$\frac{a}{d} - \frac{b}{d} = k \cdot \frac{m}{d}$$

Since all divisions are exact (by hypothesis), this shows:

$$\frac{m}{d} \left| \left(\frac{a}{d} - \frac{b}{d} \right) \right.$$

Therefore:

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

□

Example 22: Division Property

Given $24 \equiv 12 \pmod{6}$, and knowing that $6|24$, $6|12$, and $6|6$, apply the division property.

Solution:

Divide everything by $d = 6$:

$$\frac{24}{6} \equiv \frac{12}{6} \pmod{\frac{6}{6}}$$

$$4 \equiv 2 \pmod{1}$$

Note: Any two integers are congruent modulo 1, so this is always true.

Better example: Let $d = 3$:

$$\frac{24}{3} \equiv \frac{12}{3} \pmod{\frac{6}{3}}$$

$$8 \equiv 4 \pmod{2}$$

Verification: $8 - 4 = 4 = 2(2)$, so $8 \equiv 4 \pmod{2}$ ✓

Summary: Properties of Congruences

Property	Statement
Addition	$a \equiv b, c \equiv d \Rightarrow a + c \equiv b + d$
Multiplication	$a \equiv b, c \equiv d \Rightarrow ac \equiv bd$
Power	$a \equiv b \Rightarrow a^k \equiv b^k$
Cancellation	$ac \equiv bc, \gcd(c, m) = 1 \Rightarrow a \equiv b$
GCD Preservation	$a \equiv b \Rightarrow \gcd(a, m) = \gcd(b, m)$
Divisor of Modulus	$a \equiv b \pmod{m}, n \mid m \Rightarrow a \equiv b \pmod{n}$
Scaling	$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{mc}$
Division	$d \mid a, b, m \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Warning:

- Cannot always cancel: need $\gcd(c, m) = 1$
- Cannot always divide: need exact divisibility

Divisibility Tests

Divisibility tests allow us to determine whether a number is divisible by another number without performing actual division. These tests are based on properties of congruences and the decimal representation of numbers.

Divisibility by 2, 5, and 10

Theorem: Divisibility by 2

An integer n is divisible by 2 if and only if its last digit is divisible by 2 (i.e., the last digit is 0, 2, 4, 6, or 8).

Proof: Divisibility by 2

Proof:
Let $n = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0$ where a_0 is the last digit.
Note that $10 \equiv 0 \pmod 2$.
By the power property: $10^i \equiv 0^i = 0 \pmod 2$ for all $i \geq 1$.
Therefore:

$$n \equiv a_k \cdot 0 + \cdots + a_1 \cdot 0 + a_0 \pmod 2$$

$$n \equiv a_0 \pmod 2$$

Thus, $2|n$ if and only if $2|a_0$. □

Example 23: Testing Divisibility by 2

Determine which of the following are divisible by 2: 456, 3217, 8840, 5679.
Solution:
Check the last digit:
(a) 456: Last digit is 6 (even) ⇒ divisible by 2 ✓
(b) 3217: Last digit is 7 (odd) ⇒ not divisible by 2 ×
(c) 8840: Last digit is 0 (even) ⇒ divisible by 2 ✓
(d) 5679: Last digit is 9 (odd) ⇒ not divisible by 2 ×
Verification:

- $456 \div 2 = 228$ ✓
- $8840 \div 2 = 4420$ ✓

Theorem: Divisibility by 5

An integer n is divisible by 5 if and only if its last digit is 0 or 5.

Proof: Divisibility by 5

Proof:
Let $n = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0$.
Note that $10 \equiv 0 \pmod 5$.
By the power property: $10^i \equiv 0 \pmod 5$ for all $i \geq 1$.
Therefore:

$$n \equiv a_0 \pmod 5$$

Thus, $5|n$ if and only if $5|a_0$, which means $a_0 \in \{0, 5\}$. □

Example 24: Testing Divisibility by 5

Test: 1235, 4682, 7890, 3456.

Solution:

(a) 1235: Last digit is 5 $\Rightarrow$ divisible by 5 ✓

(b) 4682: Last digit is 2 $\Rightarrow$ not divisible by 5 ×

(c) 7890: Last digit is 0 $\Rightarrow$ divisible by 5 ✓

(d) 3456: Last digit is 6 $\Rightarrow$ not divisible by 5 ×

Theorem: Divisibility by 10

An integer n is divisible by 10 if and only if its last digit is 0.

Proof: Divisibility by 10

Proof:

Let $n = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0$.

We can write:

$$n = 10(a_k \cdot 10^{k-1} + \cdots + a_1) + a_0$$

Thus $n \equiv a_0 \pmod{10}$.

Therefore, $10|n$ if and only if $10|a_0$, which means $a_0 = 0$. □

Example 25: Testing Divisibility by 10

Which are divisible by 10: 1230, 4567, 8000, 9995?

Solution:

(a) 1230: Last digit is 0 $\Rightarrow$ divisible by 10 ✓

(b) 4567: Last digit is 7 $\Rightarrow$ not divisible by 10 ×

(c) 8000: Last digit is 0 $\Rightarrow$ divisible by 10 ✓

(d) 9995: Last digit is 5 $\Rightarrow$ not divisible by 10 ×

Divisibility by 3 and 9

Theorem: Divisibility by 3

An integer n is divisible by 3 if and only if the sum of its digits is divisible by 3.

Proof: Divisibility by 3

Proof:

Let $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$.

Note that $10 \equiv 1 \pmod{3}$.

By the power property: $10^i \equiv 1^i = 1 \pmod{3}$ for all $i \geq 0$.

Therefore:

$$n \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + \cdots + a_1 \cdot 1 + a_0 \pmod{3}$$

$$n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod{3}$$

Thus, $3|n$ if and only if $3|(a_k + a_{k-1} + \cdots + a_1 + a_0)$. □

Example 26: Testing Divisibility by 3

Test: 12345, 8764, 2019, 5553.

Solution:

(a) 12345: Sum of digits $= 1+2+3+4+5 = 15$
Since $15 = 3 \times 5$, we have $3|15$.
Therefore, $3|12345$ ✓
Verification: $12345 = 3 \times 4115$ ✓
(b) 8764: Sum of digits $= 8+7+6+4 = 25$
Since $25 = 3 \times 8 + 1$, we have $3 \nmid 25$.
Therefore, $3 \nmid 8764$ ×
(c) 2019: Sum of digits $= 2+0+1+9 = 12$
Since $12 = 3 \times 4$, we have $3|12$.
Therefore, $3|2019$ ✓
Verification: $2019 = 3 \times 673$ ✓
(d) 5553: Sum of digits $= 5+5+5+3 = 18$
Since $18 = 3 \times 6$, we have $3|18$.
Therefore, $3|5553$ ✓

Theorem: Divisibility by 9

An integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.

Proof: Divisibility by 9

Proof:
Let $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$.
Note that $10 \equiv 1 \pmod 9$.
By the power property: $10^i \equiv 1^i = 1 \pmod 9$ for all $i \geq 0$.
Therefore:

$$n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9$$

Thus, $9|n$ if and only if $9|(a_k + a_{k-1} + \cdots + a_1 + a_0)$. □

Example 27: Testing Divisibility by 9

Test: 4536, 1728, 9999, 8765.

Solution:

(a) 4536: Sum $= 4+5+3+6 = 18 = 9 \times 2$
Therefore, $9|4536$ ✓
Verification: $4536 = 9 \times 504$ ✓
(b) 1728: Sum $= 1+7+2+8 = 18 = 9 \times 2$
Therefore, $9|1728$ ✓
Verification: $1728 = 9 \times 192$ ✓
(c) 9999: Sum $= 9+9+9+9 = 36 = 9 \times 4$
Therefore, $9|9999$ ✓
(d) 8765: Sum $= 8+7+6+5 = 26 = 9 \times 2 + 8$
Since $9 \nmid 26$, we have $9 \nmid 8765$ ×

Divisibility by 11

Theorem: Divisibility by 11

An integer n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.
That is, if $n = a_k a_{k-1} \cdots a_1 a_0$ (in decimal), then:

$$11|n \iff 11|(a_0 - a_1 + a_2 - a_3 + \cdots)$$

Proof: Divisibility by 11

Proof:
Let $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$.
Note that $10 \equiv -1 \pmod{11}$.
By the power property:

$$\begin{aligned} 10^0 &\equiv 1 \pmod{11} \\ 10^1 &\equiv -1 \pmod{11} \\ 10^2 &\equiv (-1)^2 = 1 \pmod{11} \\ 10^3 &\equiv (-1)^3 = -1 \pmod{11} \\ &\vdots \\ 10^i &\equiv (-1)^i \pmod{11} \end{aligned}$$

Therefore:

$$n \equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_1(-1) + a_0(1) \pmod{11}$$

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11}$$

Thus, $11|n$ if and only if $11|(a_0 - a_1 + a_2 - a_3 + \cdots)$. □

Example 28: Testing Divisibility by 11

Test: 1331, 2468, 12345, 9427.
Solution:
(a) 1331: Alternating sum $= 1 - 3 + 3 - 1 = 0$
Since $11|0$, we have $11|1331$ ✓
Verification: $1331 = 11 \times 121$ (Note: $1331 = 11^3$) ✓
(b) 2468: Alternating sum $= 8 - 6 + 4 - 2 = 4$
Since $11 \nmid 4$, we have $11 \nmid 2468$ ×
(c) 12345: Alternating sum $= 5 - 4 + 3 - 2 + 1 = 3$
Since $11 \nmid 3$, we have $11 \nmid 12345$ ×
(d) 9427: Alternating sum $= 7 - 2 + 4 - 9 = 0$
Since $11|0$, we have $11|9427$ ✓
Verification: $9427 = 11 \times 857$ ✓

Example 29: Another Test for 11

Show that 8525 is divisible by 11.
Solution:
Digits: 8, 5, 2, 5 (from left to right)

Alternating sum (starting from right):

$$5 - 2 + 5 - 8 = 0$$

Since $11|0$, we conclude $11|8525$ ✓
Verification: $8525 = 11 \times 775$ ✓

Divisibility by 4 and 8

Theorem: Divisibility by 4

An integer n is divisible by 4 if and only if the number formed by its last two digits is divisible by 4.

Proof: Divisibility by 4

Proof:
Let $n = a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.
Note that $10^2 = 100 \equiv 0 \pmod 4$.
By the power property: $10^i \equiv 0 \pmod 4$ for all $i \geq 2$.
Therefore:

$$n \equiv a_1 \cdot 10 + a_0 \pmod 4$$

The expression $a_1 \cdot 10 + a_0$ represents the last two digits of n.
Thus, $4|n$ if and only if 4 divides the last two digits. □

Example 30: Testing Divisibility by 4

Test: 1236, 5678, 1000, 2019.
Solution:
(a) 1236: Last two digits = 36
Check: $36 = 4 \times 9$, so $4|36$
Therefore, $4|1236$ ✓
(b) 5678: Last two digits = 78
Check: $78 = 4 \times 19 + 2$, so $4 \nmid 78$
Therefore, $4 \nmid 5678$ ×
(c) 1000: Last two digits = 00
Check: $0 = 4 \times 0$, so $4|0$
Therefore, $4|1000$ ✓
(d) 2019: Last two digits = 19
Check: $19 = 4 \times 4 + 3$, so $4 \nmid 19$
Therefore, $4 \nmid 2019$ ×

Theorem: Divisibility by 8

An integer n is divisible by 8 if and only if the number formed by its last three digits is divisible by 8.

Proof: Divisibility by 8

Proof:
Let $n = a_k \cdot 10^k + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Note that $10^3 = 1000 \equiv 0 \pmod 8$.
By the power property: $10^i \equiv 0 \pmod 8$ for all $i \geq 3$.
Therefore:

$$n \equiv a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \pmod 8$$

The expression $a_2 \cdot 100 + a_1 \cdot 10 + a_0$ represents the last three digits.
Thus, $8|n$ if and only if 8 divides the last three digits. □

Example 31: Testing Divisibility by 8

Test: 12456, 34567, 8000, 1024.

Solution:

(a) 12456: Last three digits = 456
Check: $456 = 8 \times 57$, so $8|456$
Therefore, $8|12456$ ✓

(b) 34567: Last three digits = 567
Check: $567 = 8 \times 70 + 7$, so $8 \nmid 567$
Therefore, $8 \nmid 34567$ ×

(c) 8000: Last three digits = 000
Check: $0 = 8 \times 0$, so $8|0$
Therefore, $8|8000$ ✓

(d) 1024: Last three digits = 024 = 24
Check: $24 = 8 \times 3$, so $8|24$
Therefore, $8|1024$ ✓

Note: $1024 = 2^{10}$, so of course $8 = 2^3$ divides it.

Summary: Divisibility Tests

Divisor	Test
2	Last digit is even (0, 2, 4, 6, 8)
3	Sum of digits is divisible by 3
4	Last 2 digits form a number divisible by 4
5	Last digit is 0 or 5
8	Last 3 digits form a number divisible by 8
9	Sum of digits is divisible by 9
10	Last digit is 0
11	Alternating sum of digits is divisible by 11

Remember:

- These tests are based on congruence properties
- They work because of how powers of 10 behave modulo different numbers
- Tests can be combined (e.g., divisible by 6 means divisible by both 2 and 3)

Example 32: Combined Divisibility Tests

Determine if 5436 is divisible by 6.

Solution:

For $6|n$, we need both $2|n$ and $3|n$ (since $6 = 2 \times 3$ and $\gcd(2, 3) = 1$).

Test for 2: Last digit $= 6$ (even) $\Rightarrow 2|5436$ ✓
Test for 3: Sum of digits $= 5 + 4 + 3 + 6 = 18 = 3 \times 6$
$\Rightarrow 3|5436$ ✓
Since both tests pass: $\boxed{6|5436}$
Verification: $5436 = 6 \times 906$ ✓

Linear Congruences

Definition: Linear Congruence

A **linear congruence** is an equation of the form:

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

where $a, b, m \in \mathbb{Z}$ with $m > 0$, and x is the unknown variable.

Key Terminology:

- a is called the **coefficient**
- b is called the **constant term**
- m is the **modulus**
- A **solution** is a value of x that satisfies the congruence
- Two solutions x_1 and x_2 are **incongruent** if $x_1 \not\equiv x_2 \pmod{m}$

Example 33: Linear vs Non-Linear Congruences

Identify which are linear congruences:

Solution:

(a) $5x \equiv 3 \pmod{7}$
Linear (degree 1 in x) ✓
(b) $x^2 \equiv 4 \pmod{5}$
Not linear (degree 2 in x) ×
(c) $3x + 2 \equiv 7 \pmod{11}$
Can be rewritten as $3x \equiv 5 \pmod{11}$, so linear ✓
(d) $2x^2 + x \equiv 1 \pmod{8}$
Not linear (contains x^2 term) ×
(e) $7x \equiv 0 \pmod{12}$
Linear ✓

Example 34: Verifying Solutions

Verify that $x = 5$ is a solution to $3x \equiv 2 \pmod{13}$.

Solution:

Substitute $x = 5$:

$$3(5) = 15$$

Check if $15 \equiv 2 \pmod{13}$:

$$15 - 2 = 13 = 13(1)$$

Since $13|13$, we have $15 \equiv 2 \pmod{13}$ ✓
Therefore, $x = 5$ is indeed a solution.

Theorem: Existence and Uniqueness of Solutions

Let $m > 0$, $a, b \in \mathbb{Z}$. The linear congruence:

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

has a solution if and only if $d = \gcd(a, m)$ divides b.

If $d|b$, then the congruence has exactly d mutually incongruent solutions modulo m.

Proof: Existence and Uniqueness

Proof:
The congruence $ax \equiv b \pmod{m}$ is equivalent to:

$$m|(ax - b)$$

This means there exists an integer y such that:

$$ax - b = my$$

$$ax - my = b$$

This is a linear Diophantine equation in x and y.
By the theory of Diophantine equations, this has a solution if and only if:

$$\gcd(a, m)|b$$

Existence: Let $d = \gcd(a, m)$.
If $d|b$, then the Diophantine equation $ax - my = b$ has solutions.
Therefore, the congruence $ax \equiv b \pmod{m}$ has solutions. ✓
Number of Solutions:
If x_0 is one particular solution, then the general solution is:

$$x = x_0 + k \cdot \frac{m}{d}$$

for $k \in \mathbb{Z}$.
The distinct solutions modulo m correspond to $k = 0, 1, 2, \ldots, d - 1$.
For $k = d$:

$$x = x_0 + d \cdot \frac{m}{d} = x_0 + m \equiv x_0 \pmod{m}$$

This gives the same solution as $k = 0$.
Therefore, there are exactly d incongruent solutions modulo m. □

Example 35: Solvable Linear Congruence

Solve $6x \equiv 9 \pmod{15}$.
Solution:
Step 1: Check solvability
$d = \gcd(6, 15) = 3$
Check if $d|9$: $9 = 3(3)$, so $3|9$ ✓
The congruence has solutions.
Step 2: Simplify by dividing by $d = 3$
Divide the entire congruence by 3:

$$\frac{6x}{3} \equiv \frac{9}{3} \pmod{\frac{15}{3}}$$

$$2x \equiv 3 \pmod{5}$$

Step 3: Solve the simplified congruence
Now $\gcd(2, 5) = 1$, so there is a unique solution modulo 5.

Find x such that $2x \equiv 3 \pmod{5}$:
Test values:

- $x = 0$: $2(0) = 0 \not\equiv 3 \pmod{5}$
- $x = 1$: $2(1) = 2 \not\equiv 3 \pmod{5}$
- $x = 2$: $2(2) = 4 \not\equiv 3 \pmod{5}$
- $x = 3$: $2(3) = 6 \equiv 1 \pmod{5}$
- $x = 4$: $2(4) = 8 \equiv 3 \pmod{5}$ ✓

So $x \equiv 4 \pmod{5}$.
Step 4: Find all solutions modulo 15
Since $d = 3$, there are 3 solutions modulo 15:

$$x = 4, \quad x = 4 + 5 = 9, \quad x = 4 + 10 = 14$$

Solutions: $\boxed{x \equiv 4, 9, 14 \pmod{15}}$
Verification:

- $6(4) = 24 \equiv 9 \pmod{15}$ ✓
- $6(9) = 54 \equiv 9 \pmod{15}$ ✓
- $6(14) = 84 \equiv 9 \pmod{15}$ ✓

Example 36: Unsolvable Linear Congruence

Determine if $4x \equiv 7 \pmod{6}$ has solutions.
Solution:
Check solvability condition:
$d = \gcd(4, 6) = 2$
Check if $d|7$: $7 = 2(3) + 1$, so $2 \nmid 7$ ×
Since $\gcd(4, 6) = 2$ does not divide 7, the congruence has **no solutions**.
Verification by exhaustion:
Test all values $x = 0, 1, 2, 3, 4, 5$ modulo 6:

- $x = 0$: $4(0) = 0 \not\equiv 7 \pmod{6}$
- $x = 1$: $4(1) = 4 \not\equiv 7 \pmod{6}$
- $x = 2$: $4(2) = 8 \equiv 2 \not\equiv 7 \pmod{6}$
- $x = 3$: $4(3) = 12 \equiv 0 \not\equiv 7 \pmod{6}$
- $x = 4$: $4(4) = 16 \equiv 4 \not\equiv 7 \pmod{6}$
- $x = 5$: $4(5) = 20 \equiv 2 \not\equiv 7 \pmod{6}$

No solution exists. ×

Example 37: Finding All Solutions

Solve $12x \equiv 18 \pmod{30}$ completely.

Solution:

Step 1: Check solvability

$d = \gcd(12, 30) = 6$

Check if $d|18$: $18 = 6(3)$, so $6|18$ ✓

The congruence has $d = 6$ solutions modulo 30.

Step 2: Simplify

Divide by $d = 6$:

$$\frac{12x}{6} \equiv \frac{18}{6} \pmod{\frac{30}{6}}$$

$$2x \equiv 3 \pmod{5}$$

Step 3: Solve simplified congruence

$\gcd(2, 5) = 1$, so unique solution modulo 5.

From Example 35, we know $x \equiv 4 \pmod{5}$.

Step 4: Find all 6 solutions modulo 30

$x = 4 + 5k$ for $k = 0, 1, 2, 3, 4, 5$:

k	$x = 4 + 5k$
0	4
1	9
2	14
3	19
4	24
5	29

Solutions: $\boxed{x \equiv 4, 9, 14, 19, 24, 29 \pmod{30}}$

Verification for $x = 19$:

$$12(19) = 228 = 30(7) + 18 \equiv 18 \pmod{30}$$

✓

Special Case: Coprime Coefficient and Modulus

Special Case

When $\gcd(a, m) = 1$, the linear congruence:

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

has a **unique solution** modulo m.

Solution Method:

Find the multiplicative inverse of a modulo m (denoted a^{-1}), which satisfies:

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Then the solution is:

$$x \equiv a^{-1} \cdot b \pmod{m}$$

Example 38: Unique Solution Case

Solve $7x \equiv 3 \pmod{11}$.

Solution:

Check: $\gcd(7, 11) = 1$ ✓

Therefore, unique solution exists.

Method 1: Find multiplicative inverse

Find $7^{-1} \pmod{11}$ such that $7 \cdot 7^{-1} \equiv 1 \pmod{11}$:

Test values:

- $7 \times 1 = 7 \not\equiv 1 \pmod{11}$
- $7 \times 2 = 14 \equiv 3 \pmod{11}$
- $7 \times 3 = 21 \equiv 10 \pmod{11}$
- $7 \times 4 = 28 \equiv 6 \pmod{11}$
- $7 \times 5 = 35 \equiv 2 \pmod{11}$
- $7 \times 6 = 42 \equiv 9 \pmod{11}$
- $7 \times 7 = 49 \equiv 5 \pmod{11}$
- $7 \times 8 = 56 \equiv 1 \pmod{11}$ ✓

So $7^{-1} \equiv 8 \pmod{11}$.

Multiply both sides of $7x \equiv 3 \pmod{11}$ by 8:

$$8 \cdot 7x \equiv 8 \cdot 3 \pmod{11}$$

$$56x \equiv 24 \pmod{11}$$

$$x \equiv 24 \equiv 2 \pmod{11}$$

Solution: $\boxed{x \equiv 2 \pmod{11}}$

Verification: $7(2) = 14 \equiv 3 \pmod{11}$ ✓

Example 39: Another Unique Solution

Solve $5x \equiv 7 \pmod{12}$.

Solution:

Check: $\gcd(5, 12) = 1$ ✓

Find $5^{-1} \pmod{12}$:

Test: $5 \times 5 = 25 = 2(12) + 1 \equiv 1 \pmod{12}$ ✓

So $5^{-1} \equiv 5 \pmod{12}$.

Multiply both sides by 5:

$$5 \cdot 5x \equiv 5 \cdot 7 \pmod{12}$$

$$25x \equiv 35 \pmod{12}$$

$$x \equiv 35 \equiv 11 \pmod{12}$$

Solution: $\boxed{x \equiv 11 \pmod{12}}$

Verification: $5(11) = 55 = 4(12) + 7 \equiv 7 \pmod{12}$ ✓

Example 40: Solving by Trial

Solve $9x \equiv 5 \pmod{13}$.

Solution:

Check: $\gcd(9, 13) = 1$ ✓

Method: Trial and Error (for small modulus)

Test $x = 0, 1, 2, \ldots, 12$:

x	$9x$	$9x \pmod{13}$
0	0	0
1	9	9
2	18	5 ✓

Found: $x = 2$ gives $9(2) = 18 \equiv 5 \pmod{13}$

Solution: $\boxed{x \equiv 2 \pmod{13}}$

Example 41: Homogeneous Linear Congruence

Solve $5x \equiv 0 \pmod{15}$.

Solution:

Check solvability: $d = \gcd(5, 15) = 5$

Since $5|0$, the congruence has $d = 5$ solutions.

Simplify:

$$\frac{5x}{5} \equiv \frac{0}{5} \pmod{\frac{15}{5}}$$
$$x \equiv 0 \pmod{3}$$

So $x = 3k$ for integers k.

Solutions modulo 15: $x = 0, 3, 6, 9, 12$

Solutions: $\boxed{x \equiv 0, 3, 6, 9, 12 \pmod{15}}$

Verification:

- $5(0) = 0 \equiv 0 \pmod{15}$ ✓
- $5(3) = 15 \equiv 0 \pmod{15}$ ✓
- $5(6) = 30 \equiv 0 \pmod{15}$ ✓

Summary: Linear Congruences

For $ax \equiv b \pmod{m}$:

Condition	Result
$\gcd(a, m) \nmid b$	No solutions
$\gcd(a, m) = d$ and $d \mid b$	Exactly d solutions modulo m
$\gcd(a, m) = 1$	Unique solution modulo m

Solution Steps:

1. Check if $d = \gcd(a, m)$ divides b
2. If yes, divide entire congruence by d
3. Solve simplified congruence

4. Generate all d solutions

Remember:

- Always check solvability first
- When $\gcd(a, m) = 1$, use multiplicative inverse
- Number of solutions $= \gcd(a, m)$

Example 42: Complete Problem

Solve $15x \equiv 25 \pmod{35}$ and find all solutions.

Solution:

Step 1: Check solvability

$d = \gcd(15, 35) = 5$

Check: $25 = 5(5)$, so $5|25$ ✓

Congruence has 5 solutions.

Step 2: Simplify

$$\frac{15x}{5} \equiv \frac{25}{5} \pmod{\frac{35}{5}}$$

$$3x \equiv 5 \pmod{7}$$

Step 3: Solve simplified congruence

$\gcd(3, 7) = 1$, so unique solution modulo 7.

Find $3^{-1} \pmod{7}$:

$3 \times 5 = 15 = 2(7) + 1 \equiv 1 \pmod{7}$

So $3^{-1} \equiv 5 \pmod{7}$.

Multiply by 5:

$$x \equiv 5 \times 5 \equiv 25 \equiv 4 \pmod{7}$$

Step 4: All solutions modulo 35

$x = 4 + 7k$ for $k = 0, 1, 2, 3, 4$:

Solutions: $\boxed{x \equiv 4, 11, 18, 25, 32 \pmod{35}}$

Verification for $x = 18$:

$$15(18) = 270 = 7(35) + 25 \equiv 25 \pmod{35}$$

✓

Systems of Congruences

Introduction to Systems of Congruences

A **system of linear congruences** is a set of congruences that must be satisfied simultaneously:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

The goal is to find a value of x that satisfies all congruences at once.

Theorem: Chinese Remainder Theorem (CRT)

Let $m_1, m_2, \ldots, m_k$ be positive integers that are **pairwise relatively prime** (i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j$).
Then the system of congruences:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has a **unique solution** modulo $M = m_1 m_2 \cdots m_k$.
Key Point: The solution is unique up to congruence modulo M.

Proof: Chinese Remainder Theorem

Proof (Constructive):
We prove for the case $k = 2$. The general case follows by induction.
Consider:

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

where $\gcd(m_1, m_2) = 1$.
Step 1: Construct a solution
Let $M = m_1 m_2$ and define:

$$M_1 = \frac{M}{m_1} = m_2, \quad M_2 = \frac{M}{m_2} = m_1$$

Since $\gcd(m_1, m_2) = 1$:

- $\gcd(M_1, m_1) = \gcd(m_2, m_1) = 1$
- $\gcd(M_2, m_2) = \gcd(m_1, m_2) = 1$

So we can find:

- y_1 such that $M_1 y_1 \equiv 1 \pmod{m_1}$
- y_2 such that $M_2 y_2 \equiv 1 \pmod{m_2}$

Step 2: Construct the solution
Define:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2$$

Verify: $x \equiv a_1 \pmod{m_1}$
Note that $M_1 = m_2 \equiv 0 \pmod{m_1}$ (since $m_1 | M_1$ is false, but $m_1 | M$ and $M = m_1 M_1$).
Actually, $M_2 = m_1 \equiv 0 \pmod{m_1}$.
So:

$$x \equiv a_1 M_1 y_1 + a_2(0) y_2 \equiv a_1 M_1 y_1 \pmod{m_1}$$

Since $M_1 y_1 \equiv 1 \pmod{m_1}$:

$$x \equiv a_1 \cdot 1 = a_1 \pmod{m_1}$$

✓
Verify: $x \equiv a_2 \pmod{m_2}$
Similarly, $M_1 = m_2 \equiv 0 \pmod{m_2}$:

$$x \equiv a_1(0) y_1 + a_2 M_2 y_2 \equiv a_2 M_2 y_2 \pmod{m_2}$$

Since $M_2 y_2 \equiv 1 \pmod{m_2}$:

$$x \equiv a_2 \cdot 1 = a_2 \pmod{m_2}$$

✓
Step 3: Uniqueness
Suppose x_1 and x_2 are both solutions.
Then:

$$x_1 \equiv x_2 \equiv a_i \pmod{m_i} \text{ for all } i$$

So $m_i | (x_1 - x_2)$ for all i.
Since $m_1, m_2, \ldots, m_k$ are pairwise coprime:

$$M = m_1 m_2 \cdots m_k \text{ divides } (x_1 - x_2)$$

Therefore, $x_1 \equiv x_2 \pmod{M}$.
Hence, the solution is unique modulo M. □

Example 43: CRT with Two Congruences

Solve the system:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Solution:
Step 1: Check conditions
$\gcd(3, 5) = 1$ ✓ (pairwise coprime)
System has unique solution modulo $M = 3 \times 5 = 15$.
Step 2: Apply CRT construction
$M_1 = \frac{15}{3} = 5$, $M_2 = \frac{15}{5} = 3$
Find y_1 such that $M_1 y_1 \equiv 1 \pmod{3}$:

$$5y_1 \equiv 1 \pmod{3}$$

$$2y_1 \equiv 1 \pmod{3}$$

Test: $2(2) = 4 \equiv 1 \pmod 3$ ✓
So $y_1 = 2$.
Find y_2 such that $M_2 y_2 \equiv 1 \pmod 5$:

$$3y_2 \equiv 1 \pmod 5$$

Test: $3(2) = 6 \equiv 1 \pmod 5$ ✓
So $y_2 = 2$.
Step 3: Construct solution

$$x = a_1 M_1 y_1 + a_2 M_2 y_2$$
$$x = 2(5)(2) + 3(3)(2)$$
$$x = 20 + 18 = 38$$

Reduce modulo 15:

$$38 = 2(15) + 8$$

So $x \equiv 8 \pmod{15}$.
Solution: $\boxed{x \equiv 8 \pmod{15}}$
Verification:

- $8 = 2(3) + 2$, so $8 \equiv 2 \pmod 3$ ✓
- $8 = 1(5) + 3$, so $8 \equiv 3 \pmod 5$ ✓

General solution: $x = 8 + 15k$ for any integer k.

Example 44: Alternative Method for Two Congruences

Solve the same system using substitution:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Solution:
From the first congruence: $x = 2 + 3k$ for some integer k.
Substitute into the second congruence:

$$2 + 3k \equiv 3 \pmod 5$$

$$3k \equiv 1 \pmod 5$$

Find k: Test values

- $k = 0$: $3(0) = 0 \not\equiv 1 \pmod 5$
- $k = 1$: $3(1) = 3 \not\equiv 1 \pmod 5$
- $k = 2$: $3(2) = 6 \equiv 1 \pmod 5$ ✓

So $k = 2$.
Therefore:

$$x = 2 + 3(2) = 8$$

Solution: $\boxed{x \equiv 8 \pmod{15}}$ (same as before)

Example 45: CRT with Three Congruences

Solve the system:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases}$$

Solution:

Step 1: Verify pairwise coprimality

$\gcd(3,4) = 1$ ✓

$\gcd(3,5) = 1$ ✓

$\gcd(4,5) = 1$ ✓

Unique solution exists modulo $M = 3 \times 4 \times 5 = 60$.

Step 2: Apply CRT

$M_1 = \frac{60}{3} = 20$, $M_2 = \frac{60}{4} = 15$, $M_3 = \frac{60}{5} = 12$

Find y_1: $20y_1 \equiv 1 \pmod 3$

$20 \equiv 2 \pmod 3$, so $2y_1 \equiv 1 \pmod 3$

$y_1 = 2$ (as $2 \times 2 = 4 \equiv 1 \pmod 3$)

Find y_2: $15y_2 \equiv 1 \pmod 4$

$15 \equiv 3 \pmod 4$, so $3y_2 \equiv 1 \pmod 4$

$y_2 = 3$ (as $3 \times 3 = 9 \equiv 1 \pmod 4$)

Find y_3: $12y_3 \equiv 1 \pmod 5$

$12 \equiv 2 \pmod 5$, so $2y_3 \equiv 1 \pmod 5$

$y_3 = 3$ (as $2 \times 3 = 6 \equiv 1 \pmod 5$)

Step 3: Construct solution

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$$

$$x = 1(20)(2) + 2(15)(3) + 3(12)(3)$$

$$x = 40 + 90 + 108 = 238$$

Reduce modulo 60:

$$238 = 3(60) + 58$$

Solution: $\boxed{x \equiv 58 \pmod{60}}$

Verification:

- $58 = 19(3) + 1 \equiv 1 \pmod 3$ ✓
- $58 = 14(4) + 2 \equiv 2 \pmod 4$ ✓
- $58 = 11(5) + 3 \equiv 3 \pmod 5$ ✓

Example 46: Real-World Application

A farmer has some eggs. When counted in groups of 3, there are 2 left over. When counted in groups of 5, there are 3 left over. When counted in groups of 7, there are 4 left over. What is the smallest positive number of eggs?

Solution:

Let x be the number of eggs. We have:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

Check coprimality: $\gcd(3,5) = \gcd(3,7) = \gcd(5,7) = 1$ ✓
$M = 3 \times 5 \times 7 = 105$
$M_1 = 35$, $M_2 = 21$, $M_3 = 15$
Find y_1: $35y_1 \equiv 1 \pmod 3$
$35 \equiv 2 \pmod 3$, so $2y_1 \equiv 1 \pmod 3$, thus $y_1 = 2$
Find y_2: $21y_2 \equiv 1 \pmod 5$
$21 \equiv 1 \pmod 5$, so $y_2 = 1$
Find y_3: $15y_3 \equiv 1 \pmod 7$
$15 \equiv 1 \pmod 7$, so $y_3 = 1$
Construct solution:

$$x = 2(35)(2) + 3(21)(1) + 4(15)(1)$$

$$x = 140 + 63 + 60 = 263$$

Reduce modulo 105:

$$263 = 2(105) + 53$$

Answer: The smallest positive number of eggs is $\boxed{53}$.
Verification:

- $53 = 17(3) + 2$ ✓
- $53 = 10(5) + 3$ ✓
- $53 = 7(7) + 4$ ✓

When Moduli Are Not Coprime

⚠ Warning: Non-Coprime Moduli
When the moduli are **not** pairwise coprime, the Chinese Remainder Theorem does not apply directly. The system may have:

- No solution (inconsistent system)
- Multiple solutions or infinitely many solutions

Condition for Solvability:
For the system to have a solution, we need:

$$a_i \equiv a_j \pmod{\gcd(m_i, m_j)} \text{ for all } i, j$$

Example 47: Inconsistent System

Determine if the following system has a solution:

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 9 \end{cases}$$

Solution:
Check coprimality: $\gcd(6,9) = 3 \neq 1$ ×
Moduli are not coprime. Check consistency:
If $x \equiv 2 \pmod 6$ and $x \equiv 5 \pmod 9$, then:

$$x \equiv 2 \pmod 3 \text{ (since } 3|6)$$

$$x \equiv 5 \equiv 2 \pmod 3 \text{ (since } 3|9)$$

Both give $x \equiv 2 \pmod 3$ ✓
So far consistent. Now solve:
From first: $x = 2 + 6k$ for some integer k.
Substitute into second:

$$2 + 6k \equiv 5 \pmod 9$$

$$6k \equiv 3 \pmod 9$$

Check solvability: $\gcd(6,9) = 3$, and $3|3$ ✓
Divide by 3:

$$2k \equiv 1 \pmod 3$$

$2(2) = 4 \equiv 1 \pmod 3$, so $k \equiv 2 \pmod 3$
Thus $k = 2 + 3j$ for integer j.
Therefore:

$$x = 2 + 6(2 + 3j) = 2 + 12 + 18j = 14 + 18j$$

Solution: $\boxed{x \equiv 14 \pmod{18}}$
Verification:

- $14 = 2(6) + 2 \equiv 2 \pmod 6$ ✓
- $14 = 1(9) + 5 \equiv 5 \pmod 9$ ✓

Example 48: Truly Inconsistent System

Show that the following system has no solution:

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 6 \end{cases}$$

Solution:
$\gcd(4,6) = 2$
Check consistency modulo 2:
From first: $x \equiv 2 \equiv 0 \pmod 2$
From second: $x \equiv 3 \equiv 1 \pmod 2$
We need x to be both even and odd simultaneously! ×
This is impossible.
Conclusion: The system has **no solution**.

Summary: Chinese Remainder Theorem
For pairwise coprime moduli $m_1, m_2, \ldots, m_k$:

1. System has unique solution modulo $M = m_1 m_2 \cdots m_k$

2. Solution formula: $x = \sum_{i=1}^{k} a_i M_i y_i$

3. Where $M_i = \frac{M}{m_i}$ and $M_i y_i \equiv 1 \pmod{m_i}$

For non-coprime moduli:

- Check consistency: $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$
- If inconsistent: No solution
- If consistent: Solve by substitution method

Remember:

- CRT only applies when moduli are pairwise coprime
- Always verify your solution
- Solution is unique modulo M

Linear Diophantine Equations

Definition: Linear Diophantine Equation

A **linear Diophantine equation** is an equation of the form:

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$ are given integers, and we seek integer solutions $x, y \in \mathbb{Z}$.

Key Points:

- Named after the Greek mathematician Diophantus of Alexandria (3rd century AD)
- We are interested only in **integer** solutions
- A Diophantine equation may have: no solutions, finitely many solutions, or infinitely many solutions
- Linear Diophantine equations have a close connection to linear congruences

Example 49: Understanding Diophantine Equations

Determine which of the following are linear Diophantine equations:

Solution:

(a) $3x + 5y = 7$
Linear with integer coefficients ✓

(b) $x^2 + y = 10$
Not linear (contains x^2) ×

(c) $2x - 7y = 15$
Linear with integer coefficients ✓

(d) $xy = 12$
Not linear (contains xy term) ×

(e) $4x + 0y = 8$
Linear (equivalent to $4x = 8$) ✓

Connection to Linear Congruences

The linear Diophantine equation:

$$ax + by = c$$

can be rewritten as a linear congruence. If we rearrange:

$$ax = c - by$$

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

This shows the deep connection between Diophantine equations and congruences.

Theorem: Existence of Solutions

The linear Diophantine equation:

$$ax + by = c$$

has integer solutions if and only if:

$$\gcd(a, b) \mid c$$

That is, $d = \gcd(a, b)$ divides c.

Proof: Existence of Solutions

Proof:
Let $d = \gcd(a, b)$.
Necessary Condition ($\Rightarrow$):
Suppose x_0, y_0 is a solution, so $ax_0 + by_0 = c$.
Since $d|a$ and $d|b$:

$$d|(ax_0 + by_0)$$

$$d|c$$

Therefore, $d|c$ is necessary. ✓
Sufficient Condition ($\Leftarrow$):
Suppose $d|c$, so $c = dk$ for some integer k.
By Bezout's Identity, since $d = \gcd(a, b)$, there exist integers x', y' such that:

$$ax' + by' = d$$

Multiply both sides by k:

$$a(kx') + b(ky') = dk = c$$

Let $x_0 = kx'$ and $y_0 = ky'$. Then:

$$ax_0 + by_0 = c$$

So (x_0, y_0) is a solution. ✓
Therefore, the equation has solutions if and only if $d|c$. □

Example 50: Testing for Solvability

Determine which equations have integer solutions:
Solution:
(a) $6x + 9y = 15$
$\gcd(6, 9) = 3$
Check: $15 = 3(5)$, so $3|15$ ✓
Has solutions.
(b) $4x + 6y = 7$
$\gcd(4, 6) = 2$
Check: $7 = 2(3) + 1$, so $2 \nmid 7$ ×
No integer solutions exist.
(c) $12x + 18y = 24$
$\gcd(12, 18) = 6$
Check: $24 = 6(4)$, so $6|24$ ✓
Has solutions.
(d) $5x + 7y = 1$
$\gcd(5, 7) = 1$
Check: $1|1$ ✓
Has solutions (since gcd = 1, every integer on the right side is solvable).

Theorem: General Solution

If (x_0, y_0) is one particular solution to $ax + by = c$, then the **general solution** is:

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

where $d = \gcd(a, b)$ and $t \in \mathbb{Z}$ is any integer.
In words: Once we find one solution, we can generate infinitely many solutions using this formula.

Proof: General Solution

Proof:
Suppose (x_0, y_0) is a particular solution: $ax_0 + by_0 = c$.
Let (x, y) be any other solution: $ax + by = c$.
Subtract:

$$a(x - x_0) + b(y - y_0) = 0$$

$$a(x - x_0) = -b(y - y_0)$$

Divide by $d = \gcd(a, b)$:

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$$

Since $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, we have:
$\frac{b}{d} | (x - x_0)$ (by Euclid's Lemma)
So $x - x_0 = \frac{b}{d}t$ for some integer t.
Therefore:

$$x = x_0 + \frac{b}{d}t$$

Substituting back:

$$\frac{a}{d} \cdot \frac{b}{d}t = -\frac{b}{d}(y - y_0)$$

$$\frac{a}{d}t = -(y - y_0)$$

$$y = y_0 - \frac{a}{d}t$$

Verification:

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$

$$= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t$$

$$= ax_0 + by_0 = c$$

✓

□

Example 51: Finding All Solutions

Solve $3x + 5y = 1$ completely.
Solution:
Step 1: Check solvability
$\gcd(3, 5) = 1$, and $1|1$ ✓
Equation has solutions.

Step 2: Find one particular solution
We need $3x + 5y = 1$.
By inspection or trial:

- Try $x = 2$: $3(2) + 5y = 1 \Rightarrow 6 + 5y = 1 \Rightarrow y = -1$

Check: $3(2) + 5(-1) = 6 - 5 = 1$ ✓
So $(x_0, y_0) = (2, -1)$ is a particular solution.
Step 3: Write general solution
With $d = 1$:

$$x = 2 + \frac{5}{1}t = 2 + 5t$$

$$y = -1 - \frac{3}{1}t = -1 - 3t$$

General Solution: $\boxed{(x, y) = (2 + 5t, -1 - 3t) \text{ for } t \in \mathbb{Z}}$
Some specific solutions:

t	$x = 2 + 5t$	$y = -1 - 3t$
-1	-3	2
0	2	-1
1	7	-4
2	12	-7

Verification for $t = 1$:

$$3(7) + 5(-4) = 21 - 20 = 1$$

✓

Example 52: Solving Using Extended Euclidean Algorithm

Solve $12x + 18y = 30$.
Solution:
Step 1: Check solvability
$d = \gcd(12, 18)$
Using Euclidean Algorithm:

$$18 = 12(1) + 6$$
$$12 = 6(2) + 0$$

So $d = 6$.
Check: $30 = 6(5)$, so $6|30$ ✓
Step 2: Simplify equation
Divide by $d = 6$:

$$\frac{12x + 18y}{6} = \frac{30}{6}$$
$$2x + 3y = 5$$

Step 3: Find particular solution to simplified equation
Now $\gcd(2, 3) = 1$.
By Bezout's Identity (working backwards from Euclidean Algorithm):
From $18 = 12(1) + 6$:

$$6 = 18 - 12(1)$$

Express 1 in terms of 2 and 3:

$$3 = 2(1) + 1$$

$$1 = 3 - 2(1)$$

So $2(-1) + 3(1) = 1$.
Multiply by 5:

$$2(-5) + 3(5) = 5$$

Particular solution to $2x + 3y = 5$: $(x_0, y_0) = (-5, 5)$
Verification: $2(-5) + 3(5) = -10 + 15 = 5$ ✓
Step 4: General solution
With $d = \gcd(2, 3) = 1$:

$$x = -5 + \frac{3}{1}t = -5 + 3t$$

$$y = 5 - \frac{2}{1}t = 5 - 2t$$

General Solution: $\boxed{(x, y) = (-5 + 3t, 5 - 2t) \text{ for } t \in \mathbb{Z}}$
Some solutions:

t	$x = -5 + 3t$	$y = 5 - 2t$
0	-5	5
1	-2	3
2	1	1
3	4	-1

Verification for original equation with $t = 2$:

$$12(1) + 18(1) = 12 + 18 = 30$$

✓

Example 53: Finding Positive Solutions

Find all **positive** integer solutions to $7x + 11y = 100$.
Solution:
Step 1: Check solvability
$\gcd(7, 11) = 1$, and $1|100$ ✓
Step 2: Find particular solution
We need $7x + 11y = 100$.
Try small values systematically. For $y = 1$:

$$7x + 11(1) = 100 \Rightarrow 7x = 89$$

$89 = 7(12) + 5$, not divisible.
For $y = 2$:

$$7x + 11(2) = 100 \Rightarrow 7x = 78$$

$78 = 7(11) + 1$, not divisible.
For $y = 3$:

$$7x + 11(3) = 100 \Rightarrow 7x = 67$$

Not divisible.
Continue... or use Extended Euclidean Algorithm:

From Bezout's Identity for $\gcd(7, 11) = 1$:
$11 = 7(1) + 4$
$7 = 4(1) + 3$
$4 = 3(1) + 1$
$3 = 1(3) + 0$
Working backwards:

$$1 = 4 - 3(1) = 4 - [7 - 4(1)] = 4(2) - 7$$

$$= [11 - 7(1)](2) - 7 = 11(2) - 7(3)$$

So $7(-3) + 11(2) = 1$.
Multiply by 100:

$$7(-300) + 11(200) = 100$$

Particular solution: $(x_0, y_0) = (-300, 200)$
Step 3: General solution

$$x = -300 + 11t, \quad y = 200 - 7t$$

Step 4: Find positive solutions
Need $x > 0$ and $y > 0$:
$x > 0$: $-300 + 11t > 0 \Rightarrow t > \frac{300}{11} \approx 27.27$
So $t \geq 28$.
$y > 0$: $200 - 7t > 0 \Rightarrow t < \frac{200}{7} \approx 28.57$
So $t \leq 28$.
Therefore, $t = 28$ is the only value.
Solution:

$$x = -300 + 11(28) = -300 + 308 = 8$$

$$y = 200 - 7(28) = 200 - 196 = 4$$

Answer: The only positive solution is $\boxed{(x, y) = (8, 4)}$
Verification: $7(8) + 11(4) = 56 + 44 = 100$ ✓

Example 54: No Solutions Case

Show that $6x + 9y = 20$ has no integer solutions.
Solution:
$\gcd(6, 9) = 3$
Check if $3|20$:

$$20 = 3(6) + 2$$

Since $3 \nmid 20$, the equation has **no integer solutions**. ×
Alternative explanation:
The left side $6x + 9y = 3(2x + 3y)$ is always divisible by 3.
But 20 is not divisible by 3.
Therefore, no integer values of x and y can satisfy the equation.

Summary: Linear Diophantine Equations
For $ax + by = c$:

Condition	Result
$\gcd(a,b) \nmid c$	No solutions
$\gcd(a,b) \mid c$	Infinitely many solutions
General Solution	$(x,y) = \left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$

Solution Steps:

1. Check if $d = \gcd(a,b)$ divides c
2. Find one particular solution (x_0, y_0)
3. Write general solution using the formula
4. Apply constraints (if positive solutions needed, etc.)

Remember:

- Use Extended Euclidean Algorithm to find particular solutions
- General solution contains a parameter $t \in \mathbb{Z}$
- Connection to congruences: $ax + by = c \Rightarrow ax \equiv c \pmod{b}$

Polynomial Congruences

Definition: Polynomial Congruence

A **polynomial congruence** is an equation of the form:

$$f(x) \equiv 0 \pmod{m}$$

where $f(x)$ is a polynomial with integer coefficients:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and $a_i \in \mathbb{Z}$ for all i.

Key Terminology:

- The **degree** of $f(x)$ is the highest power of x with non-zero coefficient
- A **solution** is a value $x = a$ such that $f(a) \equiv 0 \pmod{m}$
- Two solutions a and b are **incongruent** if $a \not\equiv b \pmod{m}$
- We typically count only incongruent solutions modulo m

Example 55: Identifying Polynomial Congruences

Identify the degree and determine if solvable:

Solution:

(a) $x^2 + 3x + 2 \equiv 0 \pmod{5}$

Degree 2 (quadratic polynomial congruence) ✓

(b) $2x - 7 \equiv 0 \pmod{11}$

Degree 1 (linear congruence, already studied) ✓

(c) $x^3 - x \equiv 0 \pmod{7}$

Degree 3 (cubic polynomial congruence) ✓

(d) $x^4 + 5x^2 + 6 \equiv 0 \pmod{8}$

Degree 4 (quartic polynomial congruence) ✓

Example 56: Finding Solutions by Exhaustion

Solve $x^2 + x - 2 \equiv 0 \pmod{5}$.

Solution:

Since modulus is small, test all values $x = 0, 1, 2, 3, 4$:

For $x = 0$:

$$0^2 + 0 - 2 = -2 \equiv 3 \pmod{5}$$

Not a solution. ×

For $x = 1$:

$$1^2 + 1 - 2 = 0 \equiv 0 \pmod{5}$$

Solution! ✓

For $x = 2$:

$$2^2 + 2 - 2 = 4 \equiv 4 \pmod{5}$$

Not a solution. ×

For $x = 3$:

$$3^2 + 3 - 2 = 10 \equiv 0 \pmod{5}$$

Solution! ✓
For $x = 4$:

$$4^2 + 4 - 2 = 18 \equiv 3 \pmod 5$$

Not a solution. ×
Solutions: $\boxed{x \equiv 1, 3 \pmod 5}$
Note: This quadratic has exactly 2 incongruent solutions modulo 5.

Theorem: Factor Theorem for Congruences

If a is a solution to $f(x) \equiv 0 \pmod m$, that is, $f(a) \equiv 0 \pmod m$, then:

$$f(x) \equiv (x - a) \cdot q(x) \pmod m$$

for some polynomial $q(x)$ with integer coefficients.
In words: If a is a root, then $(x - a)$ is a factor modulo m.

Proof: Factor Theorem

Proof:
By polynomial division, we can write:

$$f(x) = (x - a) \cdot q(x) + r$$

where r is a constant (degree 0).
Substituting $x = a$:

$$f(a) = (a - a) \cdot q(a) + r = 0 \cdot q(a) + r = r$$

Since $f(a) \equiv 0 \pmod m$, we have $r \equiv 0 \pmod m$.
Therefore:

$$f(x) \equiv (x - a) \cdot q(x) \pmod m$$

□

Example 57: Applying Factor Theorem

Given that $x = 2$ is a solution to $x^2 - 5x + 6 \equiv 0 \pmod 7$, factor the polynomial modulo 7.
Solution:
Verify that $x = 2$ is a solution:

$$2^2 - 5(2) + 6 = 4 - 10 + 6 = 0 \equiv 0 \pmod 7$$

✓
By Factor Theorem:

$$x^2 - 5x + 6 \equiv (x - 2) \cdot q(x) \pmod 7$$

where $q(x)$ is degree 1.
Let $q(x) = x + b$ for some constant b.
Expand:

$$(x - 2)(x + b) = x^2 + bx - 2x - 2b = x^2 + (b - 2)x - 2b$$

Compare with $x^2 - 5x + 6$:

$$b - 2 \equiv -5 \pmod 7 \Rightarrow b \equiv -3 \equiv 4 \pmod 7$$

$$-2b \equiv 6 \pmod 7 \Rightarrow b \equiv -3 \equiv 4 \pmod 7$$

Both give $b = 4$.
Therefore:

$$\boxed{x^2 - 5x + 6 \equiv (x-2)(x-4) \pmod 7}$$

This means the other solution is $x \equiv 4 \pmod 7$.
Verification:

$$4^2 - 5(4) + 6 = 16 - 20 + 6 = 2 \equiv 2 \pmod 7$$

Wait, this doesn't work! Let me recalculate:
Actually, $x^2 - 5x + 6 = (x-2)(x-3)$ in regular arithmetic.
Check $x = 3$:

$$3^2 - 5(3) + 6 = 9 - 15 + 6 = 0 \equiv 0 \pmod 7$$

✓
So the factorization is:

$$\boxed{x^2 - 5x + 6 \equiv (x-2)(x-3) \pmod 7}$$

Solutions: $x \equiv 2, 3 \pmod 7$

Theorem: Lagrange's Theorem

Let p be a prime number and $f(x)$ be a polynomial of degree $n \geq 1$ with integer coefficients. Then the polynomial congruence:

$$f(x) \equiv 0 \pmod p$$

has **at most** n incongruent solutions modulo p.
⚠ **Important:** This theorem only holds for **prime** moduli!

Proof: Lagrange's Theorem

Proof by Induction on degree n:
Base Case: $n = 1$
$f(x) = ax + b$ where $p \nmid a$ (otherwise degree would be 0).
The congruence $ax \equiv -b \pmod p$ has exactly 1 solution (since $\gcd(a, p) = 1$).
So the theorem holds for $n = 1$. ✓
Inductive Hypothesis: Assume the theorem holds for all polynomials of degree $< n$.
Inductive Step: Consider $f(x)$ of degree n.
Case 1: $f(x) \equiv 0 \pmod p$ has no solutions.
Then the theorem holds trivially (0 solutions $\leq n$). ✓
Case 2: $f(x) \equiv 0 \pmod p$ has at least one solution, say a.
By Factor Theorem:

$$f(x) \equiv (x - a) \cdot g(x) \pmod p$$

where $g(x)$ has degree $n - 1$.
If b is any other solution to $f(x) \equiv 0 \pmod p$ with $b \not\equiv a \pmod p$:

$$f(b) \equiv (b - a) \cdot g(b) \equiv 0 \pmod p$$

Since p is prime and $b \not\equiv a \pmod p$, we have $p \nmid (b - a)$.
Therefore, by Euclid's Lemma: $p | g(b)$, so $g(b) \equiv 0 \pmod p$.

This means every solution to $f(x) \equiv 0 \pmod{p}$ (except a) is also a solution to $g(x) \equiv 0 \pmod{p}$.
By inductive hypothesis, $g(x) \equiv 0 \pmod{p}$ has at most $n-1$ solutions.
Including the solution a, $f(x) \equiv 0 \pmod{p}$ has at most:

$$1 + (n-1) = n \text{ solutions}$$

By mathematical induction, the theorem holds for all $n \geq 1$. □

Example 58: Lagrange's Theorem Application

How many solutions can $x^3 + 2x - 1 \equiv 0 \pmod{7}$ have?
Solution:

- Modulus: $p = 7$ (prime) ✓
- Degree: $n = 3$

By Lagrange's Theorem, the congruence has **at most 3** incongruent solutions modulo 7.
Find actual solutions by testing:

x	$x^3 + 2x - 1$	Result $\pmod{7}$
0	$0 + 0 - 1 = -1$	6 ×
1	$1 + 2 - 1 = 2$	2 ×
2	$8 + 4 - 1 = 11$	4 ×
3	$27 + 6 - 1 = 32$	4 ×
4	$64 + 8 - 1 = 71$	1 ×
5	$125 + 10 - 1 = 134$	1 ×
6	$216 + 12 - 1 = 227$	3 ×

Result: This congruence has **0 solutions**.
This is consistent with Lagrange's Theorem ($0 \leq 3$). ✓

Example 59: Bound is Tight

Show that $x^2 - 1 \equiv 0 \pmod{5}$ achieves the maximum number of solutions.
Solution:
Degree $n = 2$, prime modulus $p = 5$.
By Lagrange's Theorem: at most 2 solutions.
Factor: $x^2 - 1 = (x-1)(x+1)$
Test:
$x = 1$: $1^2 - 1 = 0 \equiv 0 \pmod{5}$ ✓
$x = 4$: $4^2 - 1 = 15 \equiv 0 \pmod{5}$ ✓
(Note: $4 \equiv -1 \pmod{5}$)
Solutions: $x \equiv 1, 4 \pmod{5}$
This achieves the maximum of 2 solutions! ✓

Composite Modulus Cases

⚠ Warning: Composite Moduli
When the modulus m is **composite** (not prime), Lagrange's Theorem does **NOT** apply. A polynomial of degree n can have **more than** n solutions modulo a composite number!

Example 60: Exceeding the Degree Bound

Solve $x^2 - 1 \equiv 0 \pmod 8$.
Solution:
Modulus: $m = 8$ (composite: $8 = 2^3$) Not prime!
Degree: $n = 2$
Test all values $x = 0, 1, 2, 3, 4, 5, 6, 7$**:**

x	$x^2 - 1$	Result $\pmod 8$
0	-1	7 ×
1	0	0 ✓
2	3	3 ×
3	8	0 ✓
4	15	7 ×
5	24	0 ✓
6	35	3 ×
7	48	0 ✓

Solutions: $\boxed{x \equiv 1, 3, 5, 7 \pmod 8}$
Observation: This degree-2 polynomial has **4 solutions**, which exceeds the degree! This violates Lagrange's bound because 8 is not prime. △

Example 61: Another Composite Example

Solve $x^2 \equiv 1 \pmod{15}$.
Solution:
$m = 15 = 3 \times 5$ (composite)
Test values:

x	x^2	$x^2 \pmod{15}$
1	1	1 ✓
4	16	1 ✓
11	121	1 ✓
14	196	1 ✓

Solutions: $\boxed{x \equiv 1, 4, 11, 14 \pmod{15}}$
Again, 4 solutions for a degree-2 polynomial! △
Note: $1 \equiv 1 \pmod{15}$, $4 \equiv 4 \pmod{15}$, $11 \equiv -4 \pmod{15}$, $14 \equiv -1 \pmod{15}$

Example 62: Why Composite Moduli Behave Differently

Explain why $x^2 - 1 \equiv 0 \pmod 8$ has 4 solutions.
Solution:
Factor: $x^2 - 1 = (x - 1)(x + 1)$

So we need:

$$(x-1)(x+1) \equiv 0 \pmod 8$$

For prime moduli, if $ab \equiv 0 \pmod p$, then $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$.
But for composite moduli like 8, we can have $ab \equiv 0 \pmod 8$ without either factor being $\equiv 0 \pmod 8$.
Example: $x = 3$
$(3-1)(3+1) = 2 \times 4 = 8 \equiv 0 \pmod 8$
Neither $2 \equiv 0 \pmod 8$ nor $4 \equiv 0 \pmod 8$, but their product is! △
This is why composite moduli allow more solutions than the degree would suggest.

Summary: Polynomial Congruences

Property	Statement
Definition	$f(x) \equiv 0 \pmod m$ where $f(x)$ is a polynomial
Factor Theorem	If $f(a) \equiv 0$, then $f(x) \equiv (x-a)g(x) \pmod m$
Lagrange (Prime)	Degree n, prime $p \Rightarrow$ at most n solutions
Composite Moduli	Can have more than n solutions!

Solution Methods:

1. For small moduli: Test all residues
2. Use factorization when possible
3. Apply Factor Theorem to find additional roots
4. For composite moduli, use Chinese Remainder Theorem

Remember:

- Lagrange's Theorem ONLY applies to prime moduli
- Composite moduli can have many more solutions than expected
- Always count only incongruent solutions modulo m

Practice Exercises

Problem 1

Determine whether the following congruences are true or false:

(a) $45 \equiv 9 \pmod{12}$

(b) $-17 \equiv 4 \pmod{7}$

(c) $100 \equiv 0 \pmod{25}$

(d) $83 \equiv 13 \pmod{9}$

Problem 2

Find all integers x in the range $0 \leq x < 15$ such that $x \equiv 7 \pmod{15}$.

Problem 3

Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

$$a^2 + c^2 \equiv b^2 + d^2 \pmod{m}$$

Problem 4

Find the remainder when 3^{100} is divided by 7.

Problem 5

Find the remainder when 7^{200} is divided by 11.

Problem 6

If $15x \equiv 9 \pmod{12}$, can we cancel 3 from both sides? If yes, find the resulting congruence. If no, explain why.

Problem 7

Prove that $\gcd(a, m) = \gcd(a + 3m, m)$ using properties of congruences.

Problem 8

Use divisibility tests to determine which of the following are divisible by 3, 9, and 11:

(a) 123456

(b) 987654

(c) 246810

(d) 111111

Problem 9

Find a five-digit number that is divisible by both 8 and 11. Verify using the respective divisibility tests.

Problem 10

Determine whether the following linear congruences have solutions. If yes, find all incongruent solutions:

(a) $4x \equiv 3 \pmod{9}$

(b) $6x \equiv 4 \pmod{8}$

(c) $5x \equiv 7 \pmod{11}$

(d) $14x \equiv 5 \pmod{21}$

Problem 11

Solve the linear congruence $9x \equiv 12 \pmod{15}$ and find all incongruent solutions modulo 15.

Problem 12

Find the multiplicative inverse of 7 modulo 13, then use it to solve $7x \equiv 11 \pmod{13}$.

Problem 13

Solve the following system using the Chinese Remainder Theorem:

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{9} \end{cases}$$

Problem 14

Determine whether the following system has a solution. If yes, find it:

$$\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 5 \pmod{9} \end{cases}$$

Problem 15

A number when divided by 5 leaves remainder 3, when divided by 7 leaves remainder 4, and when divided by 11 leaves remainder 6. Find the smallest positive integer satisfying all three conditions.

Problem 16

Determine which of the following Diophantine equations have integer solutions. For those that do, find the general solution:

(a) $5x + 7y = 1$

(b) $6x + 9y = 11$

(c) $8x + 12y = 20$

(d) $15x + 25y = 40$

Problem 17

Find all positive integer solutions to $3x + 7y = 50$.

Problem 18

Solve the polynomial congruence $x^2 - 5x + 6 \equiv 0 \pmod{7}$ by finding all incongruent solutions.

Problem 19

Explain why the polynomial congruence $x^2 \equiv 1 \pmod{8}$ has more solutions than Lagrange's Theorem would allow for a prime modulus. Find all solutions.

Problem 20

Solve $x^3 - x \equiv 0 \pmod{5}$ and verify that the number of solutions is consistent with Lagrange's Theorem.

Chapter 4

Arithmetic Functions and Residue Systems

Arithmetic Functions

Definition: Arithmetic Function

An **arithmetic function** (also called a **number-theoretic function**) is any function:

$$f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$$

that is defined on the set of positive integers and takes complex (often real or integer) values.

Key Points:

- The domain is always $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
- Arithmetic functions describe properties of integers (divisors, residues, etc.)
- Most important arithmetic functions in number theory take *integer* values
- Examples include the number of divisors, sum of divisors, and Euler's phi function

Definition: Multiplicative Function

An arithmetic function f is called **multiplicative** if:

1. f is not identically zero, i.e. $f \not\equiv 0$
2. Whenever $\gcd(m, n) = 1$ (i.e. m and n are **coprime**):

$$f(mn) = f(m) \cdot f(n)$$

Key Points:

- The condition $\gcd(m, n) = 1$ is essential — multiplicativity need NOT hold for non-coprime inputs
- Every multiplicative function satisfies $f(1) = 1$
- If f is multiplicative and $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then:

$$f(n) = f(p_1^{k_1}) \cdot f(p_2^{k_2}) \cdots f(p_r^{k_r})$$

reducing computation to prime powers

- A function that is multiplicative for **all** m, n (not just coprime pairs) is called **completely multiplicative**

Note: Multiplicativity is a very powerful property — it means we only need to understand f on prime powers to know f everywhere.

Definition: Additive Function

An arithmetic function f is called **additive** if:

1. f is not identically zero
2. Whenever $\gcd(m, n) = 1$:
$$f(mn) = f(m) + f(n)$$

Key Points:

- Every additive function satisfies $f(1) = 0$
- If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then:
$$f(n) = f(p_1^{k_1}) + f(p_2^{k_2}) + \cdots + f(p_r^{k_r})$$
- The **number of prime factors** $\Omega(n)$ (counted with multiplicity) is a completely additive function

Example 1: Identifying Multiplicative Functions

Determine which of the following are multiplicative:

Solution:

(a) $f(n) = 1$ for all $n \geq 1$.
Check: $f(mn) = 1 = 1 \cdot 1 = f(m) \cdot f(n)$ for all m, n. ✓
Multiplicative (in fact, completely multiplicative).
(b) $f(n) = n$ (the identity function).
Check: $f(mn) = mn = f(m) \cdot f(n)$ for all m, n. ✓
Completely multiplicative.
(c) $f(n) = n^2$.
Check: $f(mn) = (mn)^2 = m^2 n^2 = f(m) \cdot f(n)$. ✓
Completely multiplicative.
(d) $f(n) = n + 1$.
Check with $m = 2, n = 3$ (coprime):
$$f(6) = 7, \quad f(2) \cdot f(3) = 3 \cdot 4 = 12 \neq 7 \quad \times$$
Not multiplicative.
(e) $f(n) = 0$ for all n.
By definition, an identically-zero function is excluded. ×
Not multiplicative (fails the non-zero condition).

Example 2: Property of Multiplicative Functions at 1

Prove that if f is multiplicative, then $f(1) = 1$.

Solution:

Step 1: Since $\gcd(1,1) = 1$, we may apply the multiplicativity condition:

$$f(1 \cdot 1) = f(1) \cdot f(1)$$

$$f(1) = f(1)^2$$

Step 2: Rearranging:

$$f(1)^2 - f(1) = 0$$

$$f(1)\big(f(1) - 1\big) = 0$$

So either $f(1) = 0$ or $f(1) = 1$.
Step 3: Since f is not identically zero, there exists some n with $f(n) \neq 0$. Write $n = 1 \cdot n$. Then:

$$f(n) = f(1 \cdot n) = f(1) \cdot f(n)$$

Dividing both sides by $f(n) \neq 0$:

$$f(1) = 1$$

Conclusion: Every multiplicative function satisfies $\boxed{f(1) = 1}$. ✓

Summary: Arithmetic Functions

Type	**Condition (when $\gcd(m,n) = 1$)**	**Value at 1**
Multiplicative	$f(mn) = f(m) \cdot f(n)$	$f(1) = 1$
Additive	$f(mn) = f(m) + f(n)$	$f(1) = 0$
Completely Multiplicative	$f(mn) = f(m) \cdot f(n)$ for **all** m, n	$f(1) = 1$

Divisor Functions

Definition: Number of Divisors $\tau(n)$

For a positive integer n, the **number-of-divisors function** $\tau(n)$ (also written $d(n)$) is defined as:

$$\tau(n) = \sum_{d|n} 1$$

That is, $\tau(n)$ counts the total number of positive divisors of n.

Key Points:

- $\tau(1) = 1$ (only divisor of 1 is 1 itself)
- $\tau(p) = 2$ for any prime p (divisors are 1 and p)
- $\tau(n) = 2$ if and only if n is prime
- Divisors always come in pairs: if $d \mid n$, then $\frac{n}{d} \mid n$

Definition: Sum of Divisors $\sigma(n)$

For a positive integer n, the **sum-of-divisors function** $\sigma(n)$ is:

$$\sigma(n) = \sum_{d|n} d$$

That is, $\sigma(n)$ is the sum of all positive divisors of n.

Key Points:

- $\sigma(1) = 1$
- $\sigma(p) = 1 + p$ for any prime p
- n is a **perfect number** if $\sigma(n) = 2n$ (sum of proper divisors equals n)
- $\sigma(n) \geq n + 1$ for all $n > 1$ (since 1 and n are always divisors)

Example 3: Computing $\tau(n)$ and $\sigma(n)$ for Small Values

Compute $\tau(n)$ and $\sigma(n)$ for $n = 6, 12, 15$.

Solution:

(a) $n = 6$: Divisors are $1, 2, 3, 6$.

$$\tau(6) = 4, \qquad \sigma(6) = 1 + 2 + 3 + 6 = 12$$

Note: $\sigma(6) = 2(6) = 12$, so 6 is a **perfect number**! ✓

(b) $n = 12$: Divisors are $1, 2, 3, 4, 6, 12$.

$$\tau(12) = 6, \qquad \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

(c) $n = 15$: Divisors are $1, 3, 5, 15$.

$$\tau(15) = 4, \qquad \sigma(15) = 1 + 3 + 5 + 15 = 24$$

Example 4: Small Values Table

Tabulate $\tau(n)$ and $\sigma(n)$ for $n = 1$ through 10.

Solution:

n	**Divisors of n**	$\tau(n)$	$\sigma(n)$
1	1	1	1
2	1, 2	2	3
3	1, 3	2	4
4	1, 2, 4	3	7
5	1, 5	2	6
6	1, 2, 3, 6	4	12
7	1, 7	2	8
8	1, 2, 4, 8	4	15
9	1, 3, 9	3	13
10	1, 2, 5, 10	4	18

Observe: $\tau(n) = 2$ exactly when n is prime (rows for $n = 2, 3, 5, 7$).

Theorem: Structure of Divisors

Let $n > 1$ be a positive integer with prime factorization:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

Then every positive divisor d of n has the form:

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \qquad 0 \le \alpha_i \le k_i \text{ for each } i = 1, 2, \ldots, r$$

In words: Every divisor of n is formed by choosing, independently for each prime p_i, an exponent between 0 and k_i.

Important: This theorem is the foundation for computing $\tau(n)$ and $\sigma(n)$ via formulas.

Proof: Structure of Divisors

Proof:

Forward direction: If $d = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $0 \le \alpha_i \le k_i$, then:

$$\frac{n}{d} = p_1^{k_1 - \alpha_1} \cdots p_r^{k_r - \alpha_r}$$

which is a positive integer since each $k_i - \alpha_i \ge 0$. Hence $d \mid n$. ✓

Backward direction: Let $d \mid n$. Then $d \ge 1$ and $d \le n$, so d is a positive integer. By the Fundamental Theorem of Arithmetic, d has its own prime factorization. Suppose d contains a prime factor $q \ne p_i$ for any i. Then $q \mid d$ and $d \mid n$, so $q \mid n$. But $n = p_1^{k_1} \cdots p_r^{k_r}$ contains no prime other than $p_1, \ldots, p_r$ — contradiction.

Hence every prime in d is among $\{p_1, \ldots, p_r\}$, so:

$$d = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \text{ for some } \alpha_i \ge 0$$

Now suppose $\alpha_i > k_i$ for some i. Then $p_i^{\alpha_i} \mid d$ and $d \mid n$, giving $p_i^{\alpha_i} \mid n = p_1^{k_1} \cdots p_r^{k_r}$, which requires $\alpha_i \le k_i$ — contradiction.

Therefore $0 \le \alpha_i \le k_i$ for each i.

Conclusion: The positive divisors of $n = p_1^{k_1} \cdots p_r^{k_r}$ are exactly the integers of the form $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $0 \le \alpha_i \le k_i$. □

Theorem: Formulas for $\tau(n)$ and $\sigma(n)$

Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ with $n > 1$. Then:

$$\boxed{\tau(n) = \prod_{i=1}^{r} (k_i + 1) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)}$$

$$\boxed{\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}}$$

In words:

- For $\tau(n)$: add 1 to each exponent in the prime factorization, then multiply
- For $\sigma(n)$: apply the geometric series formula $1 + p + p^2 + \cdots + p^k = \dfrac{p^{k+1} - 1}{p - 1}$ to each prime power, then multiply

Theorem: τ and σ are Multiplicative

Both $\tau(n)$ and $\sigma(n)$ are multiplicative functions. That is, whenever $\gcd(m, n) = 1$:

$$\tau(mn) = \tau(m) \cdot \tau(n)$$

$$\sigma(mn) = \sigma(m) \cdot \sigma(n)$$

Proof: $\tau(n)$ and $\sigma(n)$ are Multiplicative

Proof (for τ):
Let $\gcd(m, n) = 1$ with prime factorizations $m = p_1^{k_1} \cdots p_s^{k_s}$ and $n = q_1^{j_1} \cdots q_t^{j_t}$.
Since $\gcd(m, n) = 1$, no p_i equals any q_l, so:

$$mn = p_1^{k_1} \cdots p_s^{k_s} \, q_1^{j_1} \cdots q_t^{j_t}$$

Applying the formula for τ:

$$\begin{aligned} \tau(mn) &= (k_1 + 1) \cdots (k_s + 1)(j_1 + 1) \cdots (j_t + 1) \\ &= \big[(k_1 + 1) \cdots (k_s + 1)\big] \cdot \big[(j_1 + 1) \cdots (j_t + 1)\big] \\ &= \tau(m) \cdot \tau(n) \end{aligned}$$

Proof (for σ):
Every divisor of mn factors uniquely as $d = d_1 d_2$ where $d_1 \mid m$ and $d_2 \mid n$ (since $\gcd(m, n) = 1$). Hence:

$$\sigma(mn) = \sum_{d \mid mn} d = \sum_{d_1 \mid m} \sum_{d_2 \mid n} d_1 d_2 = \Big(\sum_{d_1 \mid m} d_1\Big)\Big(\sum_{d_2 \mid n} d_2\Big) = \sigma(m)\sigma(n)$$

Conclusion: Both τ and σ are multiplicative. $\square$

Example 5: Computing $\tau(1800)$ and $\sigma(1800)$

Calculate $\tau(1800)$ and $\sigma(1800)$.

Solution:

Step 1: Find the prime factorization of 1800.

$$\begin{aligned} 1800 &= 2 \times 900 = 2 \times 2 \times 450 = 4 \times 450 \\ &= 4 \times 2 \times 225 = 8 \times 225 \\ &= 8 \times 9 \times 25 = 2^3 \times 3^2 \times 5^2 \end{aligned}$$

Step 2: Apply the τ formula.

$$\tau(1800) = (3+1)(2+1)(2+1) = 4 \times 3 \times 3 = \boxed{36}$$

Step 3: Apply the σ formula.

$$\begin{aligned} \sigma(1800) &= \frac{2^{3+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} \cdot \frac{5^{2+1}-1}{5-1} \\ &= \frac{16-1}{1} \cdot \frac{27-1}{2} \cdot \frac{125-1}{4} \\ &= 15 \cdot 13 \cdot 31 \\ &= 15 \times 13 \times 31 \end{aligned}$$

Computing step by step:

$$15 \times 13 = 195, \qquad 195 \times 31 = 6045$$

$$\sigma(1800) = \boxed{6045}$$

Verification using multiplicativity:

Since $1800 = 8 \times 9 \times 25$ and $\gcd(8,9) = \gcd(9,25) = \gcd(8,25) = 1$:

$$\tau(8) = 4, \quad \tau(9) = 3, \quad \tau(25) = 3$$

$$\tau(1800) = 4 \times 3 \times 3 = 36 \quad \checkmark$$

Example 6: Using Multiplicativity for τ and σ

Find $\tau(720)$ and $\sigma(720)$.

Solution:

Step 1: Factorize 720.

$$720 = 16 \times 45 = 2^4 \times 3^2 \times 5$$

Step 2: Compute $\tau(720)$.

$$\tau(720) = (4+1)(2+1)(1+1) = 5 \times 3 \times 2 = \boxed{30}$$

Step 3: Compute $\sigma(720)$.

$$\begin{aligned} \sigma(2^4) &= 1+2+4+8+16 = 31 \\ \sigma(3^2) &= 1+3+9 = 13 \\ \sigma(5^1) &= 1+5 = 6 \end{aligned}$$

$$\sigma(720) = 31 \times 13 \times 6 = 31 \times 78 = \boxed{2418}$$

Verification: $\frac{5^{4+1}-1}{5-1} \cdot \ldots$ gives the same result via formula ✓

Theorem: Sum Function of a Multiplicative Function

Let f be a multiplicative arithmetic function. Define:

$$F(n) = \sum_{d|n} f(d)$$

Then F is also **multiplicative**.

In words: Summing a multiplicative function over all divisors preserves multiplicativity.

Important Applications:

- Taking $f(d) = 1$ gives $F(n) = \tau(n)$ — multiplicative ✓
- Taking $f(d) = d$ gives $F(n) = \sigma(n)$ — multiplicative ✓

Proof: Sum of Multiplicative Function is Multiplicative

Proof:

Let $\gcd(m, n) = 1$. We show $F(mn) = F(m) \cdot F(n)$.

Step 1: Bijection between divisors.

Since $\gcd(m, n) = 1$, every divisor d of mn factors *uniquely* as $d = d_1 d_2$ where $d_1 \mid m$ and $d_2 \mid n$.

(Uniqueness follows because $\gcd(m, n) = 1$ forces prime factors of m and n to be disjoint.)

Step 2: Apply multiplicativity of f.

Since $d_1 \mid m$ and $d_2 \mid n$ with $\gcd(m, n) = 1$, we have $\gcd(d_1, d_2) = 1$. Therefore:

$$f(d) = f(d_1 d_2) = f(d_1) \cdot f(d_2)$$

Step 3: Compute $F(mn)$.

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d_1|m} \sum_{d_2|n} f(d_1) \cdot f(d_2)$$
$$= \Big(\sum_{d_1|m} f(d_1)\Big) \cdot \Big(\sum_{d_2|n} f(d_2)\Big) = F(m) \cdot F(n)$$

Conclusion: $F(mn) = F(m) \cdot F(n)$ whenever $\gcd(m, n) = 1$, so F is multiplicative. □

Example 7: Verifying the Sum Function is Multiplicative

Let $f(d) = d^2$. Verify that $F(n) = \sum_{d|n} d^2$ satisfies $F(4 \cdot 9) = F(4) \cdot F(9)$.

Solution:

Step 1: Compute $F(4)$.

Divisors of 4: $1, 2, 4$.

$$F(4) = 1^2 + 2^2 + 4^2 = 1 + 4 + 16 = 21$$

Step 2: Compute $F(9)$.

Divisors of 9: $1, 3, 9$.

$$F(9) = 1^2 + 3^2 + 9^2 = 1 + 9 + 81 = 91$$

Step 3: Compute $F(4) \cdot F(9)$.

$$F(4) \cdot F(9) = 21 \times 91 = 1911$$

Step 4: Compute $F(36)$ directly.
Divisors of 36: $1, 2, 3, 4, 6, 9, 12, 18, 36$.

$$F(36) = 1 + 4 + 9 + 16 + 36 + 81 + 144 + 324 + 1296 = 1911$$

$$F(36) = 1911 = F(4) \cdot F(9) \quad \checkmark$$

Theorem: $\tau(n)$ is Odd $\Leftrightarrow$ n is a Perfect Square

For any positive integer n:

$$\tau(n) \text{ is odd} \quad \Longleftrightarrow \quad n \text{ is a perfect square}$$

In words: The number of divisors is odd precisely when n is a perfect square. For all other n, divisors pair up and $\tau(n)$ is even.

Proof: $\tau(n)$ Odd $\Leftrightarrow$ n is a Perfect Square

Proof:
Key Observation: Divisors of n pair up as $(d, n/d)$, with $d \neq n/d$ when $d^2 \neq n$ and $d = n/d$ when $d^2 = n$.
Forward Direction ($\Rightarrow$): Suppose $\tau(n)$ is odd.
Each divisor $d \neq \sqrt{n}$ is paired with $n/d \neq d$, contributing 2 to $\tau(n)$. If $\tau(n)$ is odd, there must be an unpaired divisor, which requires $d = n/d$, i.e. $d^2 = n$.
Hence $n = d^2$ is a perfect square. $\checkmark$
Backward Direction ($\Leftarrow$): Suppose $n = k^2$ for some positive integer k.
Using the formula with $n = p_1^{2e_1} \cdots p_r^{2e_r}$:

$$\tau(n) = (2e_1 + 1)(2e_2 + 1) \cdots (2e_r + 1)$$

Each factor $2e_i + 1$ is **odd**. The product of odd numbers is odd.
Therefore $\tau(n)$ is odd. $\checkmark$
Conclusion: $\tau(n)$ is odd if and only if n is a perfect square. $\square$

Example 8: Verifying $\tau(n)$ Parity

Verify the theorem for $n = 36, 12, 100$.
Solution:
(a) $n = 36 = 6^2 = 2^2 \times 3^2$ — a perfect square.

$$\tau(36) = (2 + 1)(2 + 1) = 9 \quad \text{(odd)} \quad \checkmark$$

(b) $n = 12 = 2^2 \times 3$ — not a perfect square (3 has odd exponent).

$$\tau(12) = (2 + 1)(1 + 1) = 6 \quad \text{(even)} \quad \checkmark$$

(c) $n = 100 = 10^2 = 2^2 \times 5^2$ — a perfect square.

$$\tau(100) = (2+1)(2+1) = 9 \quad \text{(odd)} \quad \checkmark$$

Theorem: $\sigma(n)$ is Odd $\Leftrightarrow$ n is a Square or Twice a Square

For any positive integer n:

$$\sigma(n) \text{ is odd} \quad \iff \quad n = k^2 \text{ or } n = 2k^2 \text{ for some } k \in \mathbb{Z}^+$$

In words: $\sigma(n)$ is odd only when n is a perfect square or exactly twice a perfect square.

Proof

Proof:
Write $n = 2^a \cdot m$ where m is odd. By multiplicativity of σ:

$$\sigma(n) = \sigma(2^a) \cdot \sigma(m)$$

Step 1: Parity of $\sigma(2^a)$.

$$\sigma(2^a) = 1 + 2 + 4 + \cdots + 2^a = 2^{a+1} - 1$$

This is always **odd** (since 2^{a+1} is even, subtracting 1 gives odd). Therefore the parity of $\sigma(n)$ depends entirely on $\sigma(m)$.

Step 2: Parity of $\sigma(p^k)$ for odd prime p.

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k$$

Since p is odd, each term is odd. The sum of $k+1$ odd numbers is:

- **odd** if $k+1$ is odd, i.e. k is even
- **even** if $k+1$ is even, i.e. k is odd

Step 3: When is $\sigma(m)$ odd?
For $m = p_1^{k_1} \cdots p_r^{k_r}$ (odd primes), $\sigma(m) = \prod \sigma(p_i^{k_i})$ is odd if and only if every $\sigma(p_i^{k_i})$ is odd, which requires every k_i to be **even**. This means m is a perfect square.

Step 4: Conclude.
$\sigma(n)$ is odd $\iff$ $\sigma(m)$ is odd $\iff$ m is a perfect square.

- If $a = 0$: $n = m = k^2$ — perfect square
- If $a = 1$: $n = 2m = 2k^2$ — twice a perfect square
- If $a \geq 2$: $n = 2^a m = (2^{a/2})^2 m$ — when a is even, this is $(2^{a/2}k)^2$ — a perfect square

Combining all cases: $\sigma(n)$ is odd iff n is a perfect square or twice a perfect square.
Conclusion: $\sigma(n)$ odd $\iff$ $n = k^2$ or $n = 2k^2$. $\square$

Example 9: Verifying $\sigma(n)$ Parity

Verify the theorem for $n = 9, 18, 12, 50$.

Solution:

(a) $n = 9 = 3^2$ — perfect square.

$$\sigma(9) = 1 + 3 + 9 = 13 \quad \text{(odd)} \quad \checkmark$$

(b) $n = 18 = 2 \times 9 = 2 \times 3^2$ — twice a perfect square.

$$\sigma(18) = (1+2)(1+3+9) = 3 \times 13 = 39 \quad \text{(odd)} \quad \checkmark$$

(c) $n = 12 = 4 \times 3 = 2^2 \times 3$ — neither a square nor twice a square.

$$\sigma(12) = (1+2+4)(1+3) = 7 \times 4 = 28 \quad \text{(even)} \quad \checkmark$$

(d) $n = 50 = 2 \times 25 = 2 \times 5^2$ — twice a perfect square.

$$\sigma(50) = (1+2)(1+5+25) = 3 \times 31 = 93 \quad \text{(odd)} \quad \checkmark$$

Summary: Divisor Functions

Formulas for $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$:

$$\tau(n) = \prod_{i=1}^{r} (k_i + 1), \qquad \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

Property	Statement
Multiplicativity	$\tau(mn) = \tau(m)\tau(n)$ and $\sigma(mn) = \sigma(m)\sigma(n)$ when $\gcd(m,n) = 1$
$\tau(n)$ odd	$\iff$ n is a perfect square
$\sigma(n)$ odd	$\iff$ $n = k^2$ or $n = 2k^2$
Sum is multiplicative	If f multiplicative, $\sum_{d\mid n} f(d)$ is multiplicative

Remember: Always find the prime factorization **first** before applying any formula.

Perfect Numbers

Definition: Perfect Number

A positive integer n is called a **perfect number** if n equals the sum of all its proper positive divisors (i.e. all positive divisors except n itself).
Equivalently:

$$\sigma(n) = 2n$$

Key Points:

- The word "perfect" was used by ancient Greek mathematicians
- The four smallest perfect numbers are $6, 28, 496, 8128$
- It is unknown whether any **odd** perfect numbers exist — this is one of the oldest unsolved problems in mathematics
- If $\sigma(n) < 2n$, n is called **deficient**; if $\sigma(n) > 2n$, it is **abundant**

Equivalent form: n is perfect $\iff$ the sum of its *proper* divisors equals n, i.e. $\sigma(n) - n = n$.

Example 10: Verifying 6 and 28 are Perfect

Verify that $n = 6$ and $n = 28$ are perfect numbers.
Solution:
(a) $n = 6$: Divisors are $1, 2, 3, 6$.

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \times 6 \quad \checkmark$$

Sum of proper divisors: $1 + 2 + 3 = 6 = n$ ✓
(b) $n = 28$: Divisors are $1, 2, 4, 7, 14, 28$.

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \times 28 \quad \checkmark$$

Sum of proper divisors: $1 + 2 + 4 + 7 + 14 = 28 = n$ ✓

Example 11: Deficient and Abundant Numbers

Classify $n = 10, 12, 15$ as perfect, deficient, or abundant.
Solution:
(a) $n = 10$: Divisors $1, 2, 5, 10$.

$$\sigma(10) = 18 < 20 = 2 \times 10$$

Deficient ×
(b) $n = 12$: Divisors $1, 2, 3, 4, 6, 12$.

$$\sigma(12) = 28 > 24 = 2 \times 12$$

Abundant ★
(c) $n = 15$: Divisors $1, 3, 5, 15$.

$$\sigma(15) = 24 < 30 = 2 \times 15$$

Deficient ×

Theorem: Even Perfect Numbers (Euler–Euclid)

An even positive integer n is a perfect number if and only if it has the form:

$$\boxed{n = 2^{p-1}(2^p - 1)}$$

where p is a prime and $2^p - 1$ is also prime (a **Mersenne prime**).

In words:

- Euclid proved the "if" direction (if $2^p - 1$ is prime then n is perfect)
- Euler proved the "only if" direction (every even perfect number has this form)
- Primes $2^p - 1$ are called **Mersenne primes**; whether there are infinitely many is unknown

Note: This theorem applies to **even** perfect numbers only. The existence of odd perfect numbers remains an open problem.

Proof: Even Perfect Numbers

Proof (Euclid's Direction):

Let p be prime and $q = 2^p - 1$ be prime. Set $n = 2^{p-1}q$.
Since $q = 2^p - 1$ is odd and 2^{p-1} is a power of 2, $\gcd(2^{p-1}, q) = 1$.
By multiplicativity of σ:

$$\sigma(n) = \sigma(2^{p-1}) \cdot \sigma(q)$$

Compute each factor:

$$\sigma(2^{p-1}) = 1 + 2 + 4 + \cdots + 2^{p-1} = 2^p - 1 = q$$

Since q is prime, its only divisors are 1 and q:

$$\sigma(q) = 1 + q = 1 + (2^p - 1) = 2^p$$

Therefore:

$$\sigma(n) = q \cdot 2^p = (2^p - 1) \cdot 2^p$$

Check if $\sigma(n) = 2n$:

$$2n = 2 \cdot 2^{p-1}(2^p - 1) = 2^p(2^p - 1)$$

Indeed $\sigma(n) = 2^p(2^p - 1) = 2n$, so n is perfect.
Conclusion: If p and $2^p - 1$ are both prime, then $n = 2^{p-1}(2^p - 1)$ is a perfect number. □

Example 12: Generating Perfect Numbers via the Formula

Find the first three perfect numbers using $n = 2^{p-1}(2^p - 1)$.

Solution:

p	$2^p - 1$	**Prime?**	$n = 2^{p-1}(2^p - 1)$	**Perfect?**
2	3	Yes	$2^1 \times 3 = 6$	Yes
3	7	Yes	$2^2 \times 7 = 28$	Yes
4	15	No ($15 = 3 \times 5$)	—	No
5	31	Yes	$2^4 \times 31 = 496$	Yes
6	63	No ($63 = 9 \times 7$)	—	No
7	127	Yes	$2^6 \times 127 = 8128$	Yes

The first four perfect numbers are: $\boxed{6,\ 28,\ 496,\ 8128}$.
Verification for $n = 496$:

$$496 = 2^4 \times 31$$

$$\sigma(496) = \sigma(2^4) \cdot \sigma(31) = (1+2+4+8+16)(1+31) = 31 \times 32 = 992 = 2 \times 496$$

✓

Example 13: Showing a Number is Not Perfect

Show that $n = 496$ is perfect but $n = 8$ is deficient.
Solution:
(a) $n = 496 = 2^4 \times 31$ (computed above):

$$\sigma(496) = 31 \times 32 = 992 = 2 \times 496 \quad ✓ \quad \textbf{Perfect}$$

(b) $n = 8 = 2^3$: Divisors are $1, 2, 4, 8$.

$$\sigma(8) = 1+2+4+8 = 15 < 16 = 2 \times 8$$

Sum of proper divisors: $1+2+4 = 7 < 8$. **Deficient.** ×

Summary: Perfect Numbers

Classification	Condition
Perfect	$\sigma(n) = 2n$ (sum of proper divisors $= n$)
Deficient	$\sigma(n) < 2n$
Abundant	$\sigma(n) > 2n$

Even perfect numbers: $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are prime.
Known perfect numbers: $6, 28, 496, 8128, 33550336, \ldots$
Open Problems:

- Are there infinitely many even perfect numbers?
- Do any odd perfect numbers exist?

Residues and Residue Systems

Definition: Residue Class

Let m be a positive integer and $a \in \mathbb{Z}$. The **residue class** of a modulo m, denoted $[a]_m$ or $\bar{a}$, is the set of all integers congruent to a modulo m:

$$[a]_m = \{\, x \in \mathbb{Z} \;:\; x \equiv a \pmod{m} \,\} = \{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}$$

Key Points:

- Two integers belong to the **same** residue class iff they are congruent modulo m
- There are exactly m distinct residue classes modulo m: $[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m$
- The residue classes partition $\mathbb{Z}$ — every integer belongs to exactly one class
- Any element of a residue class is called a **representative** of that class

Definition: Complete Residue System (CRS)

A set of integers $\{a_1, a_2, \ldots, a_m\}$ is a **Complete Residue System** modulo m (abbreviated CRS mod m) if every integer is congruent to exactly one a_i modulo m.
Equivalently, $\{a_1, \ldots, a_m\}$ is a CRS mod m if and only if:

1. The set contains exactly m elements, **and**
2. No two elements are congruent to each other modulo m

Standard CRS: The set $\{0, 1, 2, \ldots, m-1\}$ is the **standard (least non-negative) CRS** modulo m.
Important: A CRS need not consist of non-negative integers — any m mutually incongruent integers form a CRS.

Definition: Reduced Residue System (RRS)

A set $\{r_1, r_2, \ldots, r_k\}$ is a **Reduced Residue System** modulo m (abbreviated RRS mod m) if:

1. Each r_i satisfies $\gcd(r_i, m) = 1$ (each element is **coprime** to m)
2. No two elements are congruent modulo m: $r_i \not\equiv r_j \pmod{m}$ for $i \neq j$
3. Every integer coprime to m is congruent to some r_i

Key Points:

- The number of elements in any RRS mod m equals $\phi(m)$ (Euler's phi)
- The standard RRS is obtained by removing from $\{0, 1, \ldots, m-1\}$ all elements sharing a common factor with m
- An RRS is a **subset** of a CRS

Example 14: Complete and Reduced Residue Systems

Find a CRS and an RRS modulo $m = 8$.

Solution:

Step 1: Standard CRS mod 8.

Take one representative from each residue class:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7\}$$

This has $m = 8$ elements, mutually incongruent mod 8. ✓

Step 2: Standard RRS mod 8.

Keep only those elements coprime to 8:

Element	$\gcd(\cdot, 8)$	Include in RRS?
0	8	No
1	1	Yes
2	2	No
3	1	Yes
4	4	No
5	1	Yes
6	2	No
7	1	Yes

RRS mod 8: $\{1,\ 3,\ 5,\ 7\}$, which has $\phi(8) = 4$ elements. ✓

Alternative CRS mod 8: $\{-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4\}$ — also valid since these 8 integers are mutually incongruent mod 8. ✓

Example 15: Residue Systems modulo 10

Find the CRS and RRS modulo $m = 10$.

Solution:

CRS mod 10: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ — 10 elements, no two congruent mod 10. ✓

RRS mod 10: Elements of $\{0, \ldots, 9\}$ coprime to 10:

Factors of $10 = 2 \times 5$, so exclude multiples of 2 and 5:

Excluded: $0, 2, 4, 5, 6, 8$ Remaining: $\{1, 3, 7, 9\}$

$$\text{RRS mod } 10 = \{1, 3, 7, 9\}$$

This has $\phi(10) = 4$ elements. ✓

Theorem: Size of a Complete Residue System

If $\{a_1, a_2, \ldots, a_k\}$ forms a Complete Residue System modulo m, then:

$$k = m$$

That is, any CRS modulo m contains **exactly** m elements.

Equivalent characterization: A set of integers S is a CRS mod m if and only if every integer is congruent (mod m) to exactly one element of S.

Proof: Size of a CRS

Proof:
There are exactly m residue classes modulo m: $[0]_m, [1]_m, \ldots, [m-1]_m$.
A CRS must contain exactly one representative from each class (by definition: every integer is congruent to exactly one element of the CRS, so no class is missed and no class contributes more than one element).
Therefore the CRS has exactly m elements.
Conclusion: Every CRS modulo m has exactly m elements. □

Theorem: Alternative Definition of CRS

Let $m > 0$. A set $\{a_1, a_2, \ldots, a_m\}$ of m integers is a CRS modulo m if and only if:

$$a_i \not\equiv a_j \pmod{m} \quad \text{for all } i \neq j$$

That is: m integers form a CRS mod m if and only if they are pairwise incongruent modulo m.

Proof: Alternative CRS Characterization

Proof:
($\Rightarrow$) If the set is a CRS, then each element represents a *different* residue class, so no two are congruent mod m.
($\Leftarrow$) Suppose $a_1, \ldots, a_m$ are pairwise incongruent modulo m. They represent m distinct residue classes. Since there are exactly m classes in total ($[0], [1], \ldots, [m-1]$), these m elements must represent **all** of them. Therefore every integer is congruent to exactly one a_i.
Conclusion: The two conditions are equivalent. □

Theorem: Size of a Reduced Residue System

If $\{r_1, r_2, \ldots, r_k\}$ forms a Reduced Residue System modulo m, then:

$$k = \phi(m)$$

where $\phi(m)$ is Euler's phi function (the number of integers in $\{1, \ldots, m\}$ that are coprime to m).

Proof: Size of an RRS

Proof:
Among the residue classes $[0], [1], \ldots, [m-1]$, the classes $[a]$ with $\gcd(a, m) = 1$ are exactly those consisting entirely of integers coprime to m.
The number of such classes is precisely $\phi(m)$ (by definition of Euler's phi).
An RRS contains exactly one representative from each such class, giving $\phi(m)$ elements in total.
Conclusion: Any RRS modulo m has exactly $\phi(m)$ elements. □

Example 16: CRS and RRS modulo 12

Find a CRS and an RRS modulo 12, and verify the sizes.
Solution:
CRS mod 12: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Size: $12 = m$. ✓
RRS mod 12: Remove elements with $\gcd(\cdot, 12) > 1$.
$12 = 2^2 \times 3$, so remove multiples of 2 and multiples of 3:
Removed: $0, 2, 3, 4, 6, 8, 9, 10$ Remaining: $\{1, 5, 7, 11\}$

$$\text{RRS mod } 12 = \{1, 5, 7, 11\}$$

$$\phi(12) = 12\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right) = 12 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} = 4$$

Size: $4 = \phi(12)$. ✓

Summary: Residue Systems

System	Condition	Size
CRS mod m	m pairwise incongruent integers	m
RRS mod m	Pairwise incongruent integers, each coprime to m	$\phi(m)$

Remember: An RRS is always a *subset* of a CRS.

Euler Phi Function

Definition: Euler Phi Function

For a positive integer m, the **Euler phi function** (also called the **Euler totient function**) is:

$$\phi(m) = \#\{k \in \mathbb{Z}^+ : 1 \le k \le m,\ \gcd(k, m) = 1\}$$

That is, $\phi(m)$ counts the number of positive integers up to m that are coprime to m.

Key Points:

- $\phi(1) = 1$ (the only positive integer ≤ 1 coprime to 1 is 1 itself)
- $\phi(p) = p - 1$ for any prime p (all integers $1, 2, \ldots, p-1$ are coprime to p)
- $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ for prime p and $k \ge 1$
- $\phi(m)$ equals the size of any RRS modulo m

Example 17: Basic Evaluations of ϕ

Compute $\phi(1), \phi(6), \phi(7), \phi(9)$.

Solution:

(a) $\phi(1)$: Only integer in $\{1\}$ coprime to 1 is 1 itself.

$$\phi(1) = \boxed{1}$$

(b) $\phi(6)$: Integers in $\{1, 2, 3, 4, 5, 6\}$ coprime to 6:

$$\gcd(1, 6) = 1,\ \gcd(5, 6) = 1 \quad \Rightarrow \quad \text{coprime: } 1, 5$$

$$\phi(6) = \boxed{2}$$

(c) $\phi(7)$: 7 is prime, so $\phi(7) = 7 - 1 = \boxed{6}$.
Integers: $1, 2, 3, 4, 5, 6$ — all coprime to 7. ✓

(d) $\phi(9) = \phi(3^2) = 3^2 - 3^1 = 9 - 3 = \boxed{6}$.
Integers coprime to 9: $\{1, 2, 4, 5, 7, 8\}$ — indeed 6 values. ✓

Example 18

Evaluate the given values using the formula for ϕ.

Solution:

(a) $\phi(56)$:

$$56 = 2^3 \times 7$$

$$\phi(56) = \phi(2^3) \cdot \phi(7) = (2^3 - 2^2)(7 - 1) = 4 \times 6 = \boxed{24}$$

(b) $\phi(800)$:

$$800 = 2^5 \times 5^2$$

$$\phi(800) = \phi(2^5) \cdot \phi(5^2) = (2^5 - 2^4)(5^2 - 5^1) = 16 \times 20 = \boxed{320}$$

(c) $\phi(1800)$:

$$1800 = 2^3 \times 3^2 \times 5^2$$

$$\phi(1800) = \phi(2^3) \cdot \phi(3^2) \cdot \phi(5^2) = (8 - 4)(9 - 3)(25 - 5) = 4 \times 6 \times 20 = \boxed{480}$$

(d) $\phi(1260^2)$:

Step 1: Factorize 1260.

$$1260 = 4 \times 315 = 2^2 \times 3^2 \times 5 \times 7$$

Step 2: Find 1260^2.

$$1260^2 = 2^4 \times 3^4 \times 5^2 \times 7^2$$

Step 3: Apply the formula.

$$\begin{aligned}\phi(1260^2) &= \phi(2^4) \cdot \phi(3^4) \cdot \phi(5^2) \cdot \phi(7^2) \\ &= (2^4 - 2^3)(3^4 - 3^3)(5^2 - 5)(7^2 - 7) \\ &= 8 \times 54 \times 20 \times 42\end{aligned}$$

Computing step by step:

$$8 \times 54 = 432, \quad 432 \times 20 = 8640, \quad 8640 \times 42 = \boxed{362880}$$

Theorem: $\phi(n)$ is Multiplicative

Euler's phi function is multiplicative. That is, whenever $\gcd(m, n) = 1$:

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

As an immediate consequence, for $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$:

$$\phi(n) = \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) = p_1^{k_1-1}(p_1 - 1) \cdot p_2^{k_2-1}(p_2 - 1) \cdots p_r^{k_r-1}(p_r - 1)$$

Proof

Proof:
Let $\gcd(m, n) = 1$. Arrange the integers $0, 1, \ldots, mn - 1$ in an $m \times n$ array:

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & n-1 \\ n & n+1 & n+2 & \cdots & 2n-1 \\ 2n & 2n+1 & 2n+2 & \cdots & 3n-1 \\ \vdots & \vdots & \vdots & & \vdots \\ (m-1)n & (m-1)n+1 & \cdots & \cdots & mn-1 \end{array}$$

The entry in row s (starting from 0), column t (starting from 0) is $sn + t$, where $0 \le s \le m - 1$ and $0 \le t \le n - 1$.

Step 1: Column t and coprimality with n.
The entries in column t are $t, n + t, 2n + t, \ldots, (m - 1)n + t$.
Since $sn \equiv 0 \pmod{n}$, we have $sn + t \equiv t \pmod{n}$.
Therefore $\gcd(sn + t, n) = \gcd(t, n)$.
All entries in column t are coprime to n iff $\gcd(t, n) = 1$.
The number of columns coprime to n is $\phi(n)$.

Step 2: Within a "good" column, coprimality with m.
Fix a column t with $\gcd(t, n) = 1$. The entries are $sn + t$ for $s = 0, 1, \ldots, m - 1$.
Modulo m: $sn + t \equiv sn + t \pmod{m}$.
As s runs over $0, 1, \ldots, m - 1$, the values $sn + t \pmod{m}$ take each residue class mod m exactly once (since $\gcd(n, m) = 1$ means n is invertible mod m).
Therefore, exactly $\phi(m)$ entries in each "good" column are coprime to m.

Step 3: Count entries coprime to both m and n.
An entry $sn+t$ satisfies $\gcd(sn+t, mn) = 1$ iff $\gcd(sn+t, m) = 1$ and $\gcd(sn+t, n) = 1$ (since $\gcd(m, n) = 1$).
Number of such entries $= \phi(n)$ good columns $\times$ $\phi(m)$ good entries per column $= \phi(m)\phi(n)$.
But these entries are the integers in $\{0, 1, \ldots, mn-1\}$ coprime to mn, of which there are $\phi(mn)$.
Therefore:

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

Conclusion: ϕ is multiplicative. □

Theorem

For any positive integers m and n with $\gcd(m, n) = d$:

$$\boxed{\phi(mn) = \phi(m)\,\phi(n)\,\frac{d}{\phi(d)}}$$

Special case: When $\gcd(m, n) = 1$, we have $d = 1$ and $\phi(1) = 1$, recovering $\phi(mn) = \phi(m)\phi(n)$.

Example 19: Applying the General $\phi(mn)$ Formula

Compute $\phi(12 \times 8)$ using the formula with $d = \gcd(12, 8)$.
Solution:
Step 1: Find $d = \gcd(12, 8) = 4$.
Step 2: Compute individual values.

$$\phi(12) = \phi(2^2 \times 3) = (4-2)(3-1) = 2 \times 2 = 4$$

$$\phi(8) = \phi(2^3) = 8 - 4 = 4$$

$$\phi(4) = \phi(2^2) = 4 - 2 = 2$$

Step 3: Apply the formula.

$$\phi(96) = \phi(12) \cdot \phi(8) \cdot \frac{d}{\phi(d)} = 4 \times 4 \times \frac{4}{2} = 4 \times 4 \times 2 = 32$$

Verification: $96 = 2^5 \times 3$, so:

$$\phi(96) = (2^5 - 2^4)(3-1) = 16 \times 2 = 32 \quad \checkmark$$

Theorem: Product Formula for $\phi(n)$

For $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ with $n > 1$:

$$\boxed{\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)}$$

In words: Start with n; for each distinct prime factor p of n, multiply by $\left(1 - \frac{1}{p}\right)$.

Note: The product runs over **distinct** prime factors only — each prime appears once regardless of its exponent.

Example 20: Using the Product Formula

Compute $\phi(360)$ using the product formula.

Solution:

Step 1: Factorize 360.

$$360 = 2^3 \times 3^2 \times 5$$

Step 2: Apply the product formula.

$$\phi(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$$

$$= 360 \times \frac{8}{30} = \frac{2880}{30} = \boxed{96}$$

Verification using $\phi(p^k)$ formula:

$$\phi(2^3) \cdot \phi(3^2) \cdot \phi(5) = 4 \times 6 \times 4 = 96 \quad \checkmark$$

Theorem: When Primes of n are Contained in m

Let m and n be positive integers. If every prime factor of n is also a prime factor of m, then:

$$\phi(mn) = n\,\phi(m)$$

Corollary: Setting $n = m$ (every prime of n is a prime of $m = n$):

$$\phi(n^2) = n\,\phi(n)$$

Proof

Proof of $\phi(mn) = n\phi(m)$:

Let $m = p_1^{k_1} \cdots p_r^{k_r}$.

Since every prime of n divides m, we can write $n = p_1^{j_1} \cdots p_r^{j_r}$ (some j_i may be 0). Then:

$$mn = p_1^{k_1+j_1} \cdots p_r^{k_r+j_r}$$

Apply the product formula to both sides.

Left side:

$$\phi(mn) = mn \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

Right side:

$$n\,\phi(m) = n \cdot m \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = mn \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

Since both sides equal $mn \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$:

$$\phi(mn) = n\,\phi(m) \quad \checkmark$$

Proof of $\phi(n^2) = n\phi(n)$:
Setting $m = n$ (every prime of n divides n trivially):

$$\phi(n^2) = \phi(n \cdot n) = n\,\phi(n)$$

Conclusion: Both identities hold. □

Example 21

Verify both identities for $m = 12$ and $n = 4$.
Solution:
Note: $12 = 2^2 \times 3$ and $4 = 2^2$. Every prime of $n = 4$ (namely 2) divides $m = 12$. ✓
Part (a): Verify $\phi(mn) = n\phi(m)$, i.e. $\phi(48) = 4 \cdot \phi(12)$.

$$\phi(12) = \phi(2^2)\phi(3) = 2 \times 2 = 4$$

$$4 \cdot \phi(12) = 4 \times 4 = 16$$

$$\phi(48) = \phi(2^4 \times 3) = (16 - 8)(3 - 1) = 8 \times 2 = 16 \quad ✓$$

Part (b): Verify $\phi(n^2) = n\phi(n)$ for $n = 12$.

$$\phi(12^2) = \phi(144) = \phi(2^4 \times 3^2) = (16 - 8)(9 - 3) = 8 \times 6 = 48$$

$$n\,\phi(n) = 12 \times 4 = 48 \quad ✓$$

Example 22: Additional Computations

Compute $\phi(1260^2)$ using the identity $\phi(n^2) = n\phi(n)$.
Solution:
Step 1: Factorize 1260.

$$1260 = 2^2 \times 3^2 \times 5 \times 7$$

Step 2: Compute $\phi(1260)$.

$$\begin{aligned}\phi(1260) &= \phi(2^2) \cdot \phi(3^2) \cdot \phi(5) \cdot \phi(7) \\ &= 2 \times 6 \times 4 \times 6 = 288\end{aligned}$$

Step 3: Apply $\phi(n^2) = n\phi(n)$.

$$\phi(1260^2) = 1260 \times \phi(1260) = 1260 \times 288 = \boxed{362880}$$

Consistent with Example 18(d). ✓

Summary: Euler Phi Function

Formula	Statement
$\phi(p) = p - 1$	For any prime p
$\phi(p^k) = p^{k-1}(p - 1)$	For prime p, $k \geq 1$
$\phi(mn) = \phi(m)\phi(n)$	When $\gcd(m, n) = 1$
$\phi(n) = n \prod \left(1 - \frac{1}{p}\right)$	Product over distinct primes $p \mid n$
$\phi(mn) = n\phi(m)$	When every prime of n divides m
$\phi(n^2) = n\phi(n)$	For any n

Important Summation Theorem

Theorem: Important Summation

For any positive integer n:

$$\boxed{\sum_{k=1}^{n} \gcd(n,\, k) = \frac{1}{2}\, n\, \phi(n) + \frac{1}{2}\, [n = 1]}$$

More commonly stated (for $n \geq 2$) using a divisor sum reformulation:

$$\sum_{k=1}^{n} \gcd(n, k) = \sum_{d \mid n} d\, \phi\left(\tfrac{n}{d}\right)$$

In words: The sum of $\gcd(n, k)$ over $k = 1, \ldots, n$ can be evaluated by grouping according to the value of the gcd — which must be a divisor of n.

Proof

Proof:

For each $k \in \{1, 2, \ldots, n\}$, let $d = \gcd(n, k)$. Then $d \mid n$.

Step 1: Group by gcd value.

For each divisor d of n, count the integers $k \in \{1, \ldots, n\}$ with $\gcd(n, k) = d$.

Write $k = d\ell$ and $n = dm$. Then $\gcd(n, k) = d \iff \gcd(m, \ell) = 1$, where $\ell \in \{1, \ldots, m\}$.

The number of such ℓ is $\phi(m) = \phi(n/d)$.

Step 2: Form the sum.

$$\sum_{k=1}^{n} \gcd(n, k) = \sum_{d \mid n} d \cdot \#\{k : \gcd(n, k) = d\} = \sum_{d \mid n} d \cdot \phi\left(\frac{n}{d}\right)$$

Conclusion: $\displaystyle\sum_{k=1}^{n} \gcd(n, k) = \sum_{d \mid n} d\, \phi\left(\frac{n}{d}\right)$. □

Example 23

Verify the summation theorem for $n = 6$.

Solution:

Step 1: Direct computation.

k	$\gcd(6, k)$
1	1
2	2
3	3
4	2
5	1
6	6

$$\sum_{k=1}^{6} \gcd(6, k) = 1 + 2 + 3 + 2 + 1 + 6 = 15$$

Step 2: Using the divisor-sum formula.

Divisors of 6: $1, 2, 3, 6$.

$$\begin{aligned}\sum_{d|6} d\,\phi(6/d) &= 1\cdot\phi(6) + 2\cdot\phi(3) + 3\cdot\phi(2) + 6\cdot\phi(1)\\ &= 1\cdot 2 + 2\cdot 2 + 3\cdot 1 + 6\cdot 1\\ &= 2+4+3+6 = 15 \quad \checkmark\end{aligned}$$

Gauss Theorem

Theorem: Gauss's Theorem on ϕ

For any positive integer n:

$$\boxed{\sum_{d|n} \phi(d) = n}$$

That is, the sum of Euler's phi function over all positive divisors of n equals n.

Examples:

- $n = 6$: $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$
- $n = p$: $\phi(1) + \phi(p) = 1 + (p-1) = p$ ✓
- $n = p^k$: $\phi(1) + \phi(p) + \cdots + \phi(p^k) = 1 + (p-1) + p(p-1) + \cdots + p^{k-1}(p-1) = p^k$

Proof: Gauss Theorem

Proof:

Consider the fractions:

$$\frac{1}{n}, \quad \frac{2}{n}, \quad \frac{3}{n}, \quad \ldots, \quad \frac{n}{n}$$

There are exactly n such fractions. Reduce each to lowest terms: $\frac{k}{n} = \frac{k/d}{n/d}$ where $d = \gcd(k, n)$.

In lowest terms, the denominator is n/d, which is a divisor of n.

Group by reduced denominator:

For each divisor $m \mid n$, count fractions whose reduced denominator is m. A fraction k/n has reduced denominator $m = n/d$ iff $d = \gcd(k, n) = n/m$, i.e. $k = (n/m)\ell$ where $\gcd(\ell, m) = 1$ and $1 \le \ell \le m$.

The number of such ℓ is $\phi(m)$.

Count all fractions:

$$n = \sum_{m|n} \phi(m)$$

since every fraction from $1/n$ to n/n is counted exactly once.

Equivalently (relabelling m as d):

$$\sum_{d|n} \phi(d) = n$$

Conclusion: For every positive integer n, $\sum_{d|n} \phi(d) = n$. □

Example 24: Verifying Gauss Theorem for n

Verify $\sum_{d|12} \phi(d) = 12$.

Solution:

Divisors of 12: $1, 2, 3, 4, 6, 12$.

d	$\phi(d)$
1	1
2	1
3	2
4	2
6	2
12	4
Sum	**12**

$$\sum_{d|12} \phi(d) = 1+1+2+2+2+4 = 12 \quad \checkmark$$

Example 25

Verify $\sum_{d|p^3} \phi(d) = p^3$ for any prime p.

Solution:

Divisors of p^3: $1, p, p^2, p^3$.

$$\begin{aligned}\sum_{d|p^3} \phi(d) &= \phi(1) + \phi(p) + \phi(p^2) + \phi(p^3) \\ &= 1 + (p-1) + p(p-1) + p^2(p-1) \\ &= 1 + (p-1)(1+p+p^2) \\ &= 1 + (p-1)\cdot\frac{p^3-1}{p-1} \\ &= 1 + p^3 - 1 = p^3 \quad \checkmark\end{aligned}$$

Congruence Theorem for Complete Residue Systems

Theorem: Existence and Uniqueness in a CRS

Let $C = \{a_1, a_2, \ldots, a_m\}$ be a Complete Residue System modulo m. Then for every integer a, there exists a **unique** element $b \in C$ such that:

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

In words: Every integer is congruent modulo m to exactly one element of any CRS. This is precisely what makes C a "complete" system.

Proof: Existence and Uniqueness in a CRS

Proof:
Existence: The residue classes $[a_1], [a_2], \ldots, [a_m]$ are all distinct (since no two a_i are congruent) and there are m of them, accounting for all m residue classes modulo m. Given any integer a, it lies in some residue class $[a_j]$, so $a \equiv a_j \pmod{m}$. Set $b = a_j$. ✓
Uniqueness: Suppose $a \equiv b_1 \pmod{m}$ and $a \equiv b_2 \pmod{m}$ for $b_1, b_2 \in C$. Then:

$$b_1 \equiv b_2 \pmod{m}$$

But since C is a CRS, no two elements are congruent. Hence $b_1 = b_2$. ✓
Conclusion: For each $a \in \mathbb{Z}$, there is a unique $b \in C$ with $a \equiv b \pmod{m}$. □

Example 26: Applying the CRS Uniqueness Theorem

Using the CRS $C = \{0, 1, 2, 3, 4, 5, 6\}$ modulo 7, find the unique representative of each of the following integers.
Solution:
(a) $a = 50$:

$$50 = 7 \times 7 + 1 \implies 50 \equiv 1 \pmod{7}$$

Unique representative: $b = \boxed{1}$.
(b) $a = -15$:

$$-15 = 7 \times (-3) + 6 \implies -15 \equiv 6 \pmod{7}$$

Unique representative: $b = \boxed{6}$.
(c) $a = 100$:

$$100 = 7 \times 14 + 2 \implies 100 \equiv 2 \pmod{7}$$

Unique representative: $b = \boxed{2}$.
All representatives are unique elements of C. ✓

Summary: Key Theorems of Part 2

Theorem	Statement
CRS Size	Any CRS mod m has exactly m elements
RRS Size	Any RRS mod m has exactly $\phi(m)$ elements
ϕ Multiplicative	$\phi(mn) = \phi(m)\phi(n)$ when $\gcd(m,n) = 1$
Product Formula	$\phi(n) = n\prod_{p\mid n}(1 - 1/p)$
Gauss Theorem	$\sum_{d\mid n} \phi(d) = n$
Summation	$\sum_{k=1}^{n} \gcd(n,k) = \sum_{d\mid n} d\,\phi(n/d)$
CRS Uniqueness	Every integer is congruent to exactly one element of any CRS

⚠ **Key chain of ideas:** Multiplicativity of ϕ $\Rightarrow$ product formula $\Rightarrow$ Gauss theorem $\Rightarrow$ Möbius inversion (Part 3).

Fermat's Little Theorem

Theorem: Fermat's Little Theorem

Let p be a prime and a any integer with $p \nmid a$ (i.e. $\gcd(a, p) = 1$). Then:

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

Equivalent form: For **any** integer a (with no restriction):

$$a^p \equiv a \pmod{p}$$

Warning: The converse is **false** in general. There exist composite integers n for which $a^{n-1} \equiv 1 \pmod{n}$ for certain a (called **Carmichael numbers**, e.g. $n = 561$). Such n are not prime.

Proof: Fermat's Little Theorem

Proof:
Let p be prime and $\gcd(a, p) = 1$.
Step 1: Consider the multiples of a.
Form the set:

$$S = \{a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\}$$

Step 2: Show S is an RRS modulo p.
We claim no two elements of S are congruent modulo p.
Suppose $ia \equiv ja \pmod{p}$ with $1 \leq i < j \leq p-1$.
Since $\gcd(a, p) = 1$, we may cancel a:

$$i \equiv j \pmod{p}$$

But $0 < j - i < p$, so $p \nmid (j - i)$ — contradiction.
Therefore $\{a, 2a, \ldots, (p-1)a\}$ are $p-1$ mutually incongruent integers, each coprime to p, forming a Reduced Residue System modulo p. ✓
Step 3: Compare with the standard RRS.
Since S is an RRS mod p, its elements are congruent (in some order) to $\{1, 2, \ldots, p-1\}$.
Multiplying all elements together:

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

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

Step 4: Cancel $(p-1)!$
Since p is prime, $\gcd((p-1)!, p) = 1$, so we may cancel $(p-1)!$:

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

Conclusion: For prime p with $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$. □

Example 27: Direct Applications of Fermat's Little Theorem

Use Fermat's Little Theorem to simplify:
Solution:
(a) $2^{10} \pmod{11}$

11 is prime, $\gcd(2, 11) = 1$. By FLT: $2^{10} \equiv 1 \pmod{11}$.

$$\boxed{2^{10} \equiv 1 \pmod{11}}$$

Verification: $2^{10} = 1024 = 93 \times 11 + 1$. ✓

(b) $3^{12} \pmod{13}$

13 is prime, $\gcd(3, 13) = 1$. By FLT: $3^{12} \equiv 1 \pmod{13}$.

$$\boxed{3^{12} \equiv 1 \pmod{13}}$$

(c) $7^{16} \pmod{17}$

17 is prime. FLT gives $7^{16} \equiv 1 \pmod{17}$.

$$\boxed{7^{16} \equiv 1 \pmod{17}}$$

Example 28: Evaluate $5^{38} \pmod{11}$

Find the remainder when 5^{38} is divided by 11.

Solution:

Step 1: Check conditions.

11 is prime and $\gcd(5, 11) = 1$. Apply FLT: $5^{10} \equiv 1 \pmod{11}$.

Step 2: Write exponent in terms of 10.

$$38 = 10 \times 3 + 8$$

Step 3: Simplify.

$$\begin{aligned} 5^{38} &= 5^{10\times 3+8} = \left(5^{10}\right)^3 \cdot 5^8 \\ &\equiv 1^3 \cdot 5^8 \pmod{11} \\ &\equiv 5^8 \pmod{11} \end{aligned}$$

Step 4: Compute $5^8 \pmod{11}$ by successive squaring.

$$\begin{aligned} 5^1 &\equiv 5 \pmod{11} \\ 5^2 &\equiv 25 \equiv 3 \pmod{11} \\ 5^4 &\equiv 3^2 = 9 \pmod{11} \\ 5^8 &\equiv 9^2 = 81 \equiv 81 - 77 = 4 \pmod{11} \end{aligned}$$

$$5^{38} \equiv 4 \pmod{11}$$

Solution: $\boxed{5^{38} \equiv 4 \pmod{11}}$

Verification: $5^{10} \equiv 1$ so $5^{40} \equiv 1$, giving $5^{38} \equiv 5^{-2} \equiv (5^2)^{-1} \equiv 25^{-1} \equiv 3^{-1} \pmod{11}$.

Since $3 \times 4 = 12 \equiv 1 \pmod{11}$, we get $3^{-1} \equiv 4$. ✓

Example 29: Show $17 \mid (11^{104} + 1)$

Prove that 17 divides $11^{104} + 1$.

Solution:

Goal: Show $11^{104} + 1 \equiv 0 \pmod{17}$, i.e. $11^{104} \equiv -1 \pmod{17}$.
Step 1: Apply FLT. 17 is prime and $\gcd(11, 17) = 1$.

$$11^{16} \equiv 1 \pmod{17}$$

Step 2: Divide the exponent.

$$104 = 16 \times 6 + 8$$

$$11^{104} = \left(11^{16}\right)^6 \cdot 11^8 \equiv 1^6 \cdot 11^8 = 11^8 \pmod{17}$$

Step 3: Compute $11^8 \pmod{17}$ by successive squaring.

$$\begin{aligned} 11^1 &\equiv 11 \pmod{17} \\ 11^2 &\equiv 121 = 7 \times 17 + 2 \equiv 2 \pmod{17} \\ 11^4 &\equiv 2^2 = 4 \pmod{17} \\ 11^8 &\equiv 4^2 = 16 \equiv -1 \pmod{17} \end{aligned}$$

Step 4: Conclude.

$$11^{104} \equiv 11^8 \equiv -1 \pmod{17}$$

$$11^{104} + 1 \equiv -1 + 1 = 0 \pmod{17}$$

Therefore $17 \mid (11^{104} + 1)$. ✓ □

Advanced Congruence Theorems

Theorem: Product of Two Fermat Congruences

Let p and q be distinct primes and a any integer. If:

$$a^p \equiv a \pmod{q} \quad \text{and} \quad a^q \equiv a \pmod{p}$$

then:

$$\boxed{a^{pq} \equiv a \pmod{pq}}$$

Note: The two hypotheses follow automatically from Fermat's Little Theorem (since $a^q \equiv a \pmod{q}$ by FLT, then raising both sides to p suitably). The theorem is a step toward understanding Carmichael numbers and pseudoprimes.

Proof: $a^{pq} \equiv a \pmod{pq}$

Proof:

Step 1: Show $p \mid (a^{pq} - a)$.

From hypothesis: $a^q \equiv a \pmod{p}$.

Raise both sides to the power p:

$$(a^q)^p \equiv a^p \pmod{p}$$

$$a^{pq} \equiv a^p \equiv a \pmod{p}$$

(The last step uses $a^p \equiv a \pmod{p}$ from FLT applied to prime p.)

So $p \mid (a^{pq} - a)$.

Step 2: Show $q \mid (a^{pq} - a)$.

By symmetry (using $a^p \equiv a \pmod{q}$ from hypothesis):

$$a^{pq} = (a^p)^q \equiv a^q \equiv a \pmod{q}$$

So $q \mid (a^{pq} - a)$.

Step 3: Combine.

Since p and q are distinct primes, $\gcd(p, q) = 1$. So:

$$p \mid (a^{pq} - a) \text{ and } q \mid (a^{pq} - a) \implies pq \mid (a^{pq} - a)$$

$$a^{pq} \equiv a \pmod{pq}$$

Conclusion: $a^{pq} \equiv a \pmod{pq}$. □

Theorem: Divisibility by pq

For distinct primes p and q and any integer a:

$$\boxed{pq \mid (a^{pq} - a^p - a^q + a)}$$

Proof: $pq \mid (a^{pq} - a^p - a^q + a)$

Proof:

Factor the expression:

$$a^{pq} - a^p - a^q + a = a^p(a^{q(p-1)} - 1) - a(a^{q-1} - 1) \cdot a^{p-1} + \dots$$

A cleaner factoring:

$$a^{pq} - a^p - a^q + a = (a^p - a)(a^{q(p-1)} - 1) + \dots$$

Most direct approach: Factor as:

$$a^{pq} - a^p - a^q + a = a^p(a^{pq-p} - 1) - a(a^{q-1} \cdot a^{p-1} \cdot \dots)$$

Use the cleaner grouping:

$$a^{pq} - a^p - a^q + a = (a^{pq} - a) - (a^p - a) - (a^q - a) + a - a + a - a$$

Actually, factor directly:

$$a^{pq} - a^p - a^q + a = a^p(a^{p(q-1)} - 1) - a(a^{q-1} - 1)$$

Use FLT directly:
Show $p \mid (a^{pq} - a^p - a^q + a)$:
By FLT: $a^p \equiv a \pmod p$ and $a^{pq} \equiv (a^p)^q \equiv a^q \pmod p$ (since $a^p \equiv a \pmod p$ implies $(a^p)^q \equiv a^q \pmod p$).
Therefore modulo p:

$$a^{pq} - a^p - a^q + a \equiv a^q - a - a^q + a = 0 \pmod p$$

So $p \mid (a^{pq} - a^p - a^q + a)$.
Show $q \mid (a^{pq} - a^p - a^q + a)$:
By symmetry (swapping p and q): $a^{pq} \equiv a^p \pmod q$ and $a^q \equiv a \pmod q$.
Therefore modulo q:

$$a^{pq} - a^p - a^q + a \equiv a^p - a^p - a + a = 0 \pmod q$$

Combine: $\gcd(p, q) = 1$, so $pq \mid (a^{pq} - a^p - a^q + a)$.
Conclusion: The result holds for all integers a and distinct primes p, q. □

Example 30: Show $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

For distinct primes p and q, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
Solution:
Step 1: Work modulo p.
$q^{p-1} \equiv 1 \pmod p$ by FLT (since $p \nmid q$).
$p^{q-1} \equiv 0 \pmod p$.
Therefore: $p^{q-1} + q^{p-1} \equiv 0 + 1 = 1 \pmod p$.
Step 2: Work modulo q.
$p^{q-1} \equiv 1 \pmod q$ by FLT (since $q \nmid p$).
$q^{p-1} \equiv 0 \pmod q$.
Therefore: $p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \pmod q$.
Step 3: Combine via CRT.
$p^{q-1} + q^{p-1} \equiv 1 \pmod p$ and $\equiv 1 \pmod q$.
Since $\gcd(p, q) = 1$: $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. ✓ □
Numerical verification with $p = 3, q = 5$:

$$3^4 + 5^2 = 81 + 25 = 106 = 15 \times 7 + 1 \equiv 1 \pmod{15} \quad ✓$$

Example 31

Prove $a^{12} \equiv 1 \pmod{35}$ for all a with $\gcd(a, 35) = 1$.

Solution:

Note $35 = 5 \times 7$.

Step 1: Modulo 5.

$\gcd(a, 5) = 1$. By FLT: $a^4 \equiv 1 \pmod{5}$.

Since $12 = 4 \times 3$:

$$a^{12} = (a^4)^3 \equiv 1^3 = 1 \pmod{5}$$

Step 2: Modulo 7.

$\gcd(a, 7) = 1$. By FLT: $a^6 \equiv 1 \pmod{7}$.

Since $12 = 6 \times 2$:

$$a^{12} = (a^6)^2 \equiv 1^2 = 1 \pmod{7}$$

Step 3: Combine.

$a^{12} \equiv 1 \pmod{5}$ and $a^{12} \equiv 1 \pmod{7}$, and $\gcd(5, 7) = 1$.

$$a^{12} \equiv 1 \pmod{35} \quad \checkmark \quad \square$$

Example 32

Prove $a^{30} \equiv 1 \pmod{77}$ for all a with $\gcd(a, 77) = 1$.

Solution:

Note $77 = 7 \times 11$.

Step 1: Modulo 7. By FLT: $a^6 \equiv 1 \pmod{7}$.

Since $30 = 6 \times 5$: $a^{30} \equiv 1 \pmod{7}$.

Step 2: Modulo 11. By FLT: $a^{10} \equiv 1 \pmod{11}$.

Since $30 = 10 \times 3$: $a^{30} \equiv 1 \pmod{11}$.

Step 3: Combine.

$\gcd(7, 11) = 1$, so $a^{30} \equiv 1 \pmod{77}$. $\checkmark$ $\square$

Euler's Theorem

Theorem: Euler's Theorem (Euler's Lemma)

Let m be a positive integer and a an integer with $\gcd(a, m) = 1$. Then:

$$\boxed{a^{\phi(m)} \equiv 1 \pmod{m}}$$

In words: Euler's Theorem generalises Fermat's Little Theorem to any modulus m (not just primes).
Note: When $m = p$ is prime, $\phi(p) = p - 1$, recovering Fermat's Little Theorem exactly.

Proof: Euler's Theorem

Proof:
Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a Reduced Residue System modulo m.
Step 1: Show $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is also an RRS.
Since $\gcd(a, m) = 1$ and $\gcd(r_i, m) = 1$:

$$\gcd(ar_i, m) = 1 \quad \text{for all } i$$

If $ar_i \equiv ar_j \pmod{m}$, then since $\gcd(a, m) = 1$, we cancel a: $r_i \equiv r_j \pmod{m}$, which forces $i = j$ (as the r_i are distinct in the RRS).
So $\{ar_1, \ldots, ar_{\phi(m)}\}$ consists of $\phi(m)$ mutually incongruent integers, each coprime to m — an RRS. ✓
Step 2: Multiply all elements.
Since both sets are RRS mod m, their products are congruent modulo m:

$$(ar_1)(ar_2)\cdots(ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

$$a^{\phi(m)} \cdot r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

Step 3: Cancel $r_1 r_2 \cdots r_{\phi(m)}$.
Since each r_i is coprime to m, their product is coprime to m. Cancel:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Conclusion: For $\gcd(a, m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Corollary: Fermat as a Special Case of Euler

When $m = p$ is prime:

$$\phi(p) = p - 1$$

Euler's Theorem gives:

$$a^{p-1} \equiv 1 \pmod{p} \quad (\text{for } \gcd(a, p) = 1)$$

This is precisely **Fermat's Little Theorem**. ✓
Insight: Euler's Theorem is strictly more general — it works for composite moduli too.

Example 33: Last Two Digits of 3^{100}

Find the last two digits of 3^{100} (i.e. compute $3^{100} \pmod{100}$).

Solution:

Step 1: Check $\gcd(3, 100) = 1$. ✓

Step 2: Compute $\phi(100)$.

$$100 = 2^2 \times 5^2 \implies \phi(100) = (4-2)(25-5) = 2 \times 20 = 40$$

By Euler's Theorem: $3^{40} \equiv 1 \pmod{100}$.

Step 3: Write exponent.

$$100 = 40 \times 2 + 20$$

$$3^{100} = (3^{40})^2 \cdot 3^{20} \equiv 1^2 \cdot 3^{20} = 3^{20} \pmod{100}$$

Step 4: Compute $3^{20} \pmod{100}$ by successive squaring.

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 9 \\ 3^4 &= 81 \\ 3^5 &= 3^4 \times 3 = 243 \equiv 43 \pmod{100} \\ 3^{10} &= 43^2 = 1849 \equiv 49 \pmod{100} \\ 3^{20} &= 49^2 = 2401 \equiv 1 \pmod{100} \end{aligned}$$

Wait — $3^{20} \equiv 1 \pmod{100}$, so:

$$3^{100} \equiv 1 \pmod{100}$$

The last two digits of 3^{100} are $\boxed{01}$.

Verification: $3^{20} = 3486784401$. Last two digits: 01. ✓

Example 34: Show $51 \mid (10^{32n+9} - 7)$

For any non-negative integer n, prove $51 \mid (10^{32n+9} - 7)$.

Solution:

Note $51 = 3 \times 17$. We show $3 \mid (10^{32n+9} - 7)$ and $17 \mid (10^{32n+9} - 7)$ separately.

Part 1: Modulo 3.

$10 \equiv 1 \pmod{3}$, so $10^{32n+9} \equiv 1 \pmod{3}$.

$7 \equiv 1 \pmod{3}$.

$10^{32n+9} - 7 \equiv 1 - 1 = 0 \pmod{3}$. ✓

Part 2: Modulo 17.

$\gcd(10, 17) = 1$. By FLT: $10^{16} \equiv 1 \pmod{17}$.

Write $32n + 9 = 16(2n) + 9$:

$$10^{32n+9} = (10^{16})^{2n} \cdot 10^9 \equiv 1 \cdot 10^9 = 10^9 \pmod{17}$$

Compute $10^9 \pmod{17}$:

$$\begin{aligned}
10^1 &\equiv 10 \pmod{17} \\
10^2 &\equiv 100 = 5 \times 17 + 15 \equiv 15 \equiv -2 \pmod{17} \\
10^4 &\equiv (-2)^2 = 4 \pmod{17} \\
10^8 &\equiv 4^2 = 16 \equiv -1 \pmod{17} \\
10^9 &\equiv -1 \times 10 = -10 \equiv 7 \pmod{17}
\end{aligned}$$

So $10^{32n+9} \equiv 7 \pmod{17}$, giving:

$$10^{32n+9} - 7 \equiv 7 - 7 = 0 \pmod{17} \quad \checkmark$$

Combine: $3 \mid$ and $17 \mid$, with $\gcd(3, 17) = 1$:

$$51 \mid (10^{32n+9} - 7) \quad \checkmark \quad \square$$

Wilson's Theorem

Theorem: Wilson's Theorem

An integer $p > 1$ is prime if and only if:

$$\boxed{(p-1)! \equiv -1 \pmod{p}}$$

In words: $(p-1)! + 1$ is divisible by p if and only if p is prime.
Note: Although elegant, Wilson's Theorem is not a practical primality test — computing $(p-1)!$ for large p is computationally infeasible.

Proof: Wilson's Theorem

Proof:
Part 1: If p is composite, then $(p-1)! \not\equiv -1 \pmod{p}$.
If p is composite, $p = ab$ for some $1 < a, b < p$.
If $a \neq b$: both a and b appear in $\{1, 2, \ldots, p-1\}$, so $ab = p \mid (p-1)!$, giving $(p-1)! \equiv 0 \pmod{p}$. Since $-1 \not\equiv 0 \pmod{p}$ (for $p > 1$), we have $(p-1)! \not\equiv -1 \pmod{p}$.
If $a = b$: $p = a^2$. For $p > 4$, $a < 2a < p-1$, so both a and $2a$ appear in $\{1, \ldots, p-1\}$, making $2a^2 = 2p \mid (p-1)!$, again $(p-1)! \equiv 0$. (The case $p = 4$ can be checked: $3! = 6 \equiv 2 \not\equiv -1 \pmod{4}$.)
Part 2: If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.
Consider the integers $2, 3, \ldots, p-2$. Each a in this range has a unique multiplicative inverse a^{-1} modulo p (since $\gcd(a, p) = 1$), with $a^{-1} \in \{1, \ldots, p-1\}$.
Self-inverse elements: $a \equiv a^{-1} \pmod{p} \iff a^2 \equiv 1 \pmod{p} \iff p \mid (a-1)(a+1) \iff a \equiv 1$ or $a \equiv -1 \equiv p-1$.
So in $\{2, 3, \ldots, p-2\}$, no element is its own inverse. Every element pairs with a distinct inverse. The product of all paired elements is:

$$2 \times 3 \times \cdots \times (p-2) \equiv 1 \pmod{p}$$

Therefore:

$$(p-1)! = 1 \times (2 \times 3 \times \cdots \times (p-2)) \times (p-1) \equiv 1 \times 1 \times (p-1) \equiv p-1 \equiv -1 \pmod{p}$$

Conclusion: p is prime iff $(p-1)! \equiv -1 \pmod{p}$. □

Example 35: Verifying Wilson's Theorem

Verify Wilson's Theorem for $p = 5, 7$.
Solution:
(a) $p = 5$:

$$(5-1)! = 4! = 24 = 5 \times 4 + 4 \equiv 4 \equiv -1 \pmod{5} \quad \checkmark$$

(b) $p = 7$:

$$(7-1)! = 6! = 720 = 7 \times 102 + 6 \equiv 6 \equiv -1 \pmod{7} \quad \checkmark$$

Theorem: Wilson's Theorem Applied to $p \equiv 3 \pmod{4}$

If p is a prime with $p \equiv 3 \pmod{4}$, then:

$$\left(\frac{p-1}{2}!\right)^2 \equiv 1 \pmod{p}$$

In words: When $p \equiv 3 \pmod 4$, the square of the "half-factorial" is congruent to 1 modulo p (not -1).

Proof: Half-Factorial Theorem

Proof:
Let $k = \dfrac{p-1}{2}$ (an integer since p is odd).
Step 1: Write $(p-1)!$ in terms of $k!$.

$$(p-1)! = 1 \cdot 2 \cdots k \cdot (k+1) \cdots (p-1)$$

Note that for $j = 1, 2, \ldots, k$:

$$p - j \equiv -j \pmod p$$

So the second half $(k+1)(k+2)\cdots(p-1)$ equals $(p-k)(p-k+1)\cdots(p-1)$, which is congruent to $(-k)(-k+1)\cdots(-1) = (-1)^k \cdot k!$ modulo p.
Step 2: Therefore:

$$(p-1)! \equiv k! \cdot (-1)^k \cdot k! = (-1)^k (k!)^2 \pmod p$$

Step 3: Apply Wilson's Theorem.

$$-1 \equiv (p-1)! \equiv (-1)^k (k!)^2 \pmod p$$

$$(k!)^2 \equiv \frac{-1}{(-1)^k} = (-1)^{k+1} \pmod p$$

Step 4: Use $p \equiv 3 \pmod 4$.
$p - 1 \equiv 2 \pmod 4$, so $k = \dfrac{p-1}{2}$ is odd.
Then $k+1$ is even, so $(-1)^{k+1} = 1$.

$$\left(\frac{p-1}{2}!\right)^2 \equiv 1 \pmod p$$

Conclusion: For prime $p \equiv 3 \pmod 4$, $\left(\dfrac{p-1}{2}!\right)^2 \equiv 1 \pmod p$. □

Example 36: Find Remainder of $51^{151} \pmod{17}$

Find the remainder when 51^{151} is divided by 17.
Solution:
Step 1: Simplify $51 \pmod{17}$.

$$51 = 3 \times 17 \implies 51 \equiv 0 \pmod{17}$$

Step 2: Therefore:

$$51^{151} \equiv 0^{151} = 0 \pmod{17}$$

Solution: $\boxed{51^{151} \equiv 0 \pmod{17}}$
The remainder is **0**.
✓ (Since $17 \mid 51$, $17 \mid 51^{151}$ trivially.)

Möbius Function

Definition: Möbius Function

The **Möbius function** $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ is defined by:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ (product of } k \text{ distinct primes)} \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \text{ } (n \text{ has a squared factor)} \end{cases}$$

Key Points:

- $\mu(n) = 0$ whenever n has a repeated prime factor ("square-full")
- $\mu(n) = \pm 1$ when n is **squarefree** (no repeated prime factor)
- μ is multiplicative: $\mu(mn) = \mu(m)\mu(n)$ when $\gcd(m, n) = 1$
- $\mu(1) = 1$, $\mu(p) = -1$ for any prime p, $\mu(p^2) = 0$

Example 37: Computing $\mu(n)$ for Various Values

Evaluate $\mu(n)$ for $n = 1, 2, 6, 12, 30, 210$.

Solution:

n	Factorization	**Squarefree?**	$\mu(n)$
1	1	Yes	1
2	p	Yes ($k = 1$)	$(-1)^1 = -1$
6	2×3	Yes ($k = 2$)	$(-1)^2 = 1$
12	$2^2 \times 3$	No ($2^2 \mid 12$)	0
30	$2 \times 3 \times 5$	Yes ($k = 3$)	$(-1)^3 = -1$
210	$2 \times 3 \times 5 \times 7$	Yes ($k = 4$)	$(-1)^4 = 1$

Example 38: More Values of μ

Compute $\mu(n)$ for $n = 4, 8, 100, 35, 42$.

Solution:

(a) $n = 4 = 2^2$: Has squared factor. $\mu(4) = \boxed{0}$.

(b) $n = 8 = 2^3$: Has squared factor ($2^2 \mid 8$). $\mu(8) = \boxed{0}$.

(c) $n = 100 = 2^2 \times 5^2$: Has squared factors. $\mu(100) = \boxed{0}$.

(d) $n = 35 = 5 \times 7$: Squarefree, $k = 2$. $\mu(35) = (-1)^2 = \boxed{1}$.

(e) $n = 42 = 2 \times 3 \times 7$: Squarefree, $k = 3$. $\mu(42) = (-1)^3 = \boxed{-1}$.

Möbius Lemma: Divisor Sum of μ

For any positive integer n:

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

In words: The Möbius function is the "inverse" of the constant function 1 under Dirichlet convolution — it detects the value 1.

Proof: Möbius Lemma

Proof:
Define $F(n) = \sum_{d|n} \mu(d)$. Since μ is multiplicative, F is also multiplicative (by our theorem on sum functions).
Case $n = 1$: $F(1) = \mu(1) = 1$.
Case $n = p^k$ (prime power, $k \geq 1$):

$$F(p^k) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) = 1 + (-1) + 0 + \cdots + 0 = 0$$

General $n > 1$: Write $n = p_1^{k_1} \cdots p_r^{k_r}$. By multiplicativity:

$$F(n) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) = 0 \cdots 0 = 0$$

since each $F(p_i^{k_i}) = 0$.
Conclusion: $\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$. □

Example 39: Verifying the Möbius Lemma for n

Verify $\sum_{d|12} \mu(d) = 0$.
Solution:
Divisors of 12: $1, 2, 3, 4, 6, 12$.

d	Factorization	$\mu(d)$
1	1	1
2	p	-1
3	p	-1
4	2^2	0
6	2×3	1
12	$2^2 \times 3$	0
Sum		**0**

$$\sum_{d|12} \mu(d) = 1 - 1 - 1 + 0 + 1 + 0 = 0 \quad \checkmark$$

Möbius Inversion

Theorem: Möbius Inversion Formula

Let F and f be arithmetic functions related by:

$$F(n) = \sum_{d|n} f(d)$$

Then:

$$\boxed{f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)}$$

In words: If F is the "divisor sum" of f, then f can be **recovered** from F by the Möbius inversion formula. The Möbius function "inverts" the summation.

Proof: Möbius Inversion

Proof:

Start with the proposed inversion and substitute $F(n/d) = \sum_{e|(n/d)} f(e)$:

$$\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{e|(n/d)} f(e)$$

Every pair (d, e) with $d \mid n$ and $e \mid (n/d)$ corresponds to a pair with $de \mid n$. Substitute $m = de$, so $d \mid m$ and $m \mid n$:

$$= \sum_{m|n} f(m) \sum_{d|(n/m)} \mu(d) \cdot [\text{where } e = m/d]$$
$$= \sum_{m|n} f(m) \sum_{d|(n/m)} \mu(d)$$

Wait — regroup by fixing e and summing over $d \mid (n/e)$:

$$= \sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d)$$

By the Möbius Lemma:

$$\sum_{d|(n/e)} \mu(d) = \begin{cases} 1 & \text{if } n/e = 1 \text{ (i.e. } e = n) \\ 0 & \text{if } n/e > 1 \end{cases}$$

Therefore the double sum collapses to the single term $e = n$:

$$\sum_{e|n} f(e) \cdot [n/e = 1] = f(n) \cdot 1 = f(n)$$

Conclusion: $\sum_{d|n} \mu(d) F(n/d) = f(n)$. □

Definition: Möbius Pair

Two arithmetic functions f and F form a **Möbius pair** if they satisfy:

$$F(n) = \sum_{d|n} f(d) \quad \Longleftrightarrow \quad f(n) = \sum_{d|n} \mu(d)\, F\left(\tfrac{n}{d}\right)$$

Examples of Möbius Pairs:

- $f = \mu$, $F(n) = [n = 1]$ (the indicator of 1)
- $f = \phi$, $F(n) = n$ (Gauss's theorem provides the pair)
- $f = \mathrm{id}$, $F = \sigma$ (sum of divisors)

Example 40: Recovering f from F via Möbius Inversion

Given $F(n) = n$ (so $F(n) = \sum_{d|n} \phi(d)$ by Gauss), recover $f = \phi$ using the inversion formula.

Solution:

By Möbius inversion with $F(n) = n$:

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$$

Verify for $n = 6$: Divisors of 6: $1, 2, 3, 6$.

$$\begin{aligned} f(6) &= \mu(1) \cdot 6 + \mu(2) \cdot 3 + \mu(3) \cdot 2 + \mu(6) \cdot 1 \\ &= 1(6) + (-1)(3) + (-1)(2) + (1)(1) \\ &= 6 - 3 - 2 + 1 = 2 \end{aligned}$$

Indeed $\phi(6) = 2$. ✓

Verify for $n = 12$: Divisors: $1, 2, 3, 4, 6, 12$.

$$\begin{aligned} f(12) &= \mu(1)(12) + \mu(2)(6) + \mu(3)(4) + \mu(4)(3) + \mu(6)(2) + \mu(12)(1) \\ &= 12 + (-1)(6) + (-1)(4) + 0 + (1)(2) + 0 \\ &= 12 - 6 - 4 + 2 = 4 \end{aligned}$$

Indeed $\phi(12) = 4$. ✓

This confirms $\phi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$.

Theorem

For any integer $n > 1$:

$$\phi(n) = n - 1 \quad \Longleftrightarrow \quad n \text{ is prime}$$

Proof

Forward Direction ($\Leftarrow$):

If $n = p$ is prime, then every integer in $\{1, 2, \ldots, p-1\}$ is coprime to p (since p has no divisors other than 1 and itself). So $\phi(p) = p - 1$. ✓

Backward Direction ($\Rightarrow$):

Suppose $\phi(n) = n - 1$. We show n must be prime.
Assume n is composite. Then n has a divisor d with $1 < d < n$, so $\gcd(d, n) = d > 1$, meaning d is **not** counted by $\phi(n)$.
The integers counted by $\phi(n)$ are from $\{1, \ldots, n-1\}$, which has $n - 1$ elements. For $\phi(n) = n - 1$, every element of $\{1, \ldots, n-1\}$ must be coprime to n.
But $d \in \{1, \ldots, n-1\}$ with $\gcd(d, n) > 1$ — contradiction.
Hence n cannot be composite, so n is prime. ✓
Conclusion: $\phi(n) = n - 1$ if and only if n is prime. □

Example 41: Verifying the Theorem

Verify the theorem for $n = 7$ (prime) and $n = 9$ (composite).
Solution:
(a) $n = 7$ (prime):

$$\phi(7) = 6 = 7 - 1 \quad ✓$$

Integers coprime to 7 in $\{1, \ldots, 6\}$: all six of them.
(b) $n = 9 = 3^2$ (composite):

$$\phi(9) = 9 - 3 = 6 \neq 8 = 9 - 1 \quad \times$$

The integers 3, 6 in $\{1, \ldots, 8\}$ share a factor with 9, so $\phi(9) < 8$.

Greatest Integer Function

Definition: Greatest Integer Function (Floor Function)

For any real number x, the **greatest integer function** $\lfloor x \rfloor$ (also called the **floor function** or **bracket function** $[x]$) is defined as:

$$\lfloor x \rfloor = \text{the greatest integer } n \text{ such that } n \leq x$$

Equivalently, $\lfloor x \rfloor$ is the unique integer satisfying:

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

Key Properties:

- $\lfloor x \rfloor = x$ if and only if x is an integer
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ for any integer n
- $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$
- $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$ when $x \notin \mathbb{Z}$; $\lfloor -x \rfloor = -x$ when $x \in \mathbb{Z}$
- The **fractional part** is $\{x\} = x - \lfloor x \rfloor$, with $0 \leq \{x\} < 1$

Important: For $x < 0$, be careful — $\lfloor -2.3 \rfloor = -3$ (not -2), since we go to the *greatest* integer ≤ -2.3.

Example 42: Evaluating the Greatest Integer Function

Evaluate the following:

Solution:

Expression	Reason	Value
$\lfloor 3.7 \rfloor$	Greatest integer ≤ 3.7	3
$\lfloor 5 \rfloor$	5 is already an integer	5
$\lfloor -2.3 \rfloor$	Greatest integer ≤ -2.3 is -3	-3
$\lfloor -7 \rfloor$	-7 is an integer	-7
$\lfloor \pi \rfloor$	$\pi \approx 3.14159\ldots$, so $\lfloor \pi \rfloor = 3$	3
$\lfloor \sqrt{2} \rfloor$	$\sqrt{2} \approx 1.414$, so floor is 1	1
$\lfloor -\sqrt{2} \rfloor$	$-\sqrt{2} \approx -1.414$, floor is -2	-2
$\lfloor 7/3 \rfloor$	$7/3 = 2.333\ldots$	2

Example 43: Number Theory Applications of Floor Function

How many multiples of 7 are there in the set $\{1, 2, \ldots, 100\}$?

Solution:

A multiple of 7 in $\{1, \ldots, 100\}$ has the form $7k$ where $7k \leq 100$.

$$k \leq \frac{100}{7} \approx 14.28\ldots$$

$$k_{\max} = \left\lfloor \frac{100}{7} \right\rfloor = 14$$

There are $\boxed{14}$ multiples of 7 in $\{1, \ldots, 100\}$, namely $7, 14, \ldots, 98$.

Verification: $7 \times 14 = 98 \leq 100 < 105 = 7 \times 15$. ✓

Example 44: Legendre's Formula — Highest Power of Prime in $n!$

Find the highest power of 3 dividing 100!.

Solution:

Legendre's Formula: The exponent of prime p in $n!$ is:

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

(The sum is finite since $\lfloor n/p^k \rfloor = 0$ for $p^k > n$.)

For $n = 100$, $p = 3$:

$$\left\lfloor \frac{100}{3} \right\rfloor = 33$$
$$\left\lfloor \frac{100}{9} \right\rfloor = 11$$
$$\left\lfloor \frac{100}{27} \right\rfloor = 3$$
$$\left\lfloor \frac{100}{81} \right\rfloor = 1$$
$$\left\lfloor \frac{100}{243} \right\rfloor = 0 \quad \text{(stop here)}$$

Exponent of 3 in $100! = 33 + 11 + 3 + 1 = \boxed{48}$.

Summary: Part 3 Key Results

Theorem	Statement
Fermat's Little	$a^{p-1} \equiv 1 \pmod{p}$ for prime p, $\gcd(a, p) = 1$
Euler's Theorem	$a^{\phi(m)} \equiv 1 \pmod{m}$ for $\gcd(a, m) = 1$
Wilson's Theorem	p prime $\iff (p-1)! \equiv -1 \pmod{p}$
Möbius Lemma	$\sum_{d\mid n} \mu(d) = [n = 1]$
Möbius Inversion	$F = \sum f(d) \Rightarrow f(n) = \sum \mu(d) F(n/d)$
$\phi(n) = n - 1$	$\iff n$ is prime
Floor function	$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$

Key hierarchy: Fermat's Little Theorem $\subset$ Euler's Theorem (FLT is the special case $m = p$ prime).

Practice Exercises

Problem 1

Compute $\tau(n)$ and $\sigma(n)$ for $n = 2^5 \times 3^2 \times 7$.

Problem 2

Find all positive integers $n \leq 50$ for which $\tau(n) = 6$.

Problem 3

Prove that $\tau(n)$ is odd if and only if n is a perfect square, and verify for $n = 25, 36, 48$.

Problem 4

Find all n in the range $1 \leq n \leq 30$ such that $\sigma(n)$ is odd.

Problem 5

Let $f(n) = (-1)^{\tau(n)}$. Determine whether f is multiplicative and compute $f(12), f(36), f(100)$.

Problem 6

Verify that $\sum_{d|n} \tau(d) = \sum_{d|n} \lfloor n/d \rfloor$ for $n = 12$.

Problem 7

Determine whether $n = 496$ is perfect. Identify the corresponding prime p in the formula $2^{p-1}(2^p - 1)$.

Problem 8

Show that if $n > 1$ is a perfect number, then $\displaystyle\sum_{d|n} \frac{1}{d} = 2$.

Problem 9

Find a Complete Residue System modulo 9 using elements from $\{-10, -9, \ldots, 10\}$ that contains no element from $\{0, 1, \ldots, 8\}$.

Problem 10

Determine the Reduced Residue System modulo 18, and verify its size equals $\phi(18)$.

Problem 11

Compute $\phi(n)$ for $n = 2^{10}$, $n = 3^5$, $n = 2 \times 3 \times 5 \times 7$, and $n = p^2 q$ where p, q are distinct odd primes.

Problem 12

Prove: For any prime p, $\phi(p^k) + \phi(p^{k-1}) = p^{k-1}(p-1) + p^{k-2}(p-1)$. Simplify and show the result equals $p^{k-2}(p-1)^2 \cdot \dfrac{p}{p-1}$.

Problem 13

Verify Gauss's theorem $\sum_{d|n} \phi(d) = n$ for $n = 20$.

Problem 14

Using Möbius inversion and $F(n) = \sigma(n)$, find an expression for $f(n)$ (the identity function $f(n) = n$) in terms of μ and σ.

Problem 15

Compute $5^{200} \pmod 7$, $3^{1000} \pmod{11}$, and $7^{50} \pmod{13}$.

Problem 16

Prove: $n^7 - n$ is divisible by 42 for every integer n.
Hint: $42 = 2 \times 3 \times 7$.

Problem 17

Find the last two digits of 7^{2025} (i.e. $7^{2025} \pmod{100}$).

Problem 18

Using Wilson's Theorem, determine whether 29 and 35 satisfy $(n-1)! \equiv -1 \pmod n$.

Problem 19

Compute $\mu(n)$ for $n = 1, 6, 30, 60, 210, 2310$, and verify the Möbius Lemma for $n = 30$.

Problem 20

Evaluate the following using the greatest integer function: **(a)** $\lfloor 5.9 \rfloor$, **(b)** $\lfloor -3.1 \rfloor$, **(c)** $\lfloor \sqrt{50} \rfloor$, **(d)** $\lfloor 100/7 \rfloor$, **(e)** the highest power of 5 dividing 200!

Chapter 5

Primitive Roots

Exponent of an Integer Modulo m

Definition: Exponent (Order) of an Integer Modulo m

Let $m > 0$ be a positive integer and let a be an integer with $\gcd(a, m) = 1$. The **exponent** (or **order**) of a modulo m is the **smallest positive integer** h such that:

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

We write $h = \text{ord}_m(a)$ or simply $h = \exp_m(a)$.

Key Points:

- The exponent h always exists when $\gcd(a, m) = 1$ (guaranteed by Euler's Theorem)
- We require $\gcd(a, m) = 1$; the exponent is undefined otherwise
- The exponent h satisfies $1 \leq h \leq \phi(m)$
- If $a \equiv 1 \pmod{m}$, then $h = 1$
- The exponent is also called the **multiplicative order** of a modulo m

Important: Always verify $\gcd(a, m) = 1$ before computing the exponent.

Example 1: Finding the Exponent of 2 Modulo 7

Find the exponent of 2 modulo 7.

Solution:

Step 1: Check $\gcd(2, 7) = 1$ ✓

Step 2: Compute successive powers of 2 modulo 7:

k	2^k	$2^k \pmod 7$
1	2	2
2	4	4
3	8	1

Step 3: The smallest k for which $2^k \equiv 1 \pmod 7$ is $k = 3$.

Verification: $2^3 = 8 = 7(1) + 1 \equiv 1 \pmod 7$ ✓

Therefore, the exponent of 2 modulo 7 is $\boxed{h = 3}$.

Example 2: Finding the Exponent of 3 Modulo 10

Find the exponent of 3 modulo 10.

Solution:

Step 1: Check $\gcd(3, 10) = 1$ ✓

Step 2: Compute successive powers of 3 modulo 10:

k	3^k	$3^k \pmod{10}$
1	3	3
2	9	9
3	27	7
4	81	1

Step 3: The smallest k for which $3^k \equiv 1 \pmod{10}$ is $k = 4$.

Verification: $3^4 = 81 = 10(8) + 1 \equiv 1 \pmod{10}$ ✓

Therefore, the exponent of 3 modulo 10 is $\boxed{h = 4}$.

Example 3: Finding the Exponent of 2 Modulo 15

Find the exponent of 2 modulo 15.

Solution:

Step 1: Check $\gcd(2, 15) = 1$ ✓

Note: $\phi(15) = \phi(3)\phi(5) = 2 \times 4 = 8$, so the exponent must divide 8.

Step 2: Compute successive powers of 2 modulo 15:

k	2^k	$2^k \pmod{15}$
1	2	2
2	4	4
3	8	8
4	16	1

Step 3: The smallest k for which $2^k \equiv 1 \pmod{15}$ is $k = 4$.

Verification: $2^4 = 16 = 15(1) + 1 \equiv 1 \pmod{15}$ ✓

Therefore, the exponent of 2 modulo 15 is $\boxed{h = 4}$.

⚠ **Note:** The exponent $h = 4$ divides $\phi(15) = 8$, consistent with the theorem we will prove next.

Theorem: Properties of the Exponent Modulo m

Let a be an integer having exponent h modulo m, i.e., $\text{ord}_m(a) = h$. Then the following hold:

(i) If $a^k \equiv 1 \pmod{m}$, then $h \mid k$.

(ii) If $a \equiv b \pmod{m}$, then the exponent of b modulo m is also h.

(iii) $a^i \equiv a^j \pmod{m}$ if and only if $i \equiv j \pmod{h}$.

⚠ **Important Corollary:** Taking $k = \phi(m)$ in part (i) and using Euler's Theorem, we conclude that $h \mid \phi(m)$.

Proof: Properties of the Exponent Modulo m

Proof:

Let $\gcd(a, m) = 1$ and let $h = \text{ord}_m(a)$, so h is the smallest positive integer with $a^h \equiv 1 \pmod{m}$.

Part (i): $a^k \equiv 1 \pmod{m}$ implies $h \mid k$
Step 1: By the Division Algorithm, write $k = qh + r$ where $0 \leq r < h$.
Step 2: Then:

$$a^k = a^{qh+r} = (a^h)^q \cdot a^r$$

Step 3: Since $a^h \equiv 1 \pmod{m}$:

$$a^k \equiv 1^q \cdot a^r \equiv a^r \pmod{m}$$

Step 4: By hypothesis $a^k \equiv 1 \pmod{m}$, so:

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

Step 5: Since $0 \leq r < h$ and h is the *smallest* positive integer with $a^h \equiv 1 \pmod{m}$, we must have $r = 0$.
Therefore $k = qh$, which means $h \mid k$. ✓
Part (ii): $a \equiv b \pmod{m}$ implies same exponent
Step 1: Let $a \equiv b \pmod{m}$. For any positive integer k:

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

Step 2: Since $a^h \equiv 1 \pmod{m}$, we get $b^h \equiv 1 \pmod{m}$.
So the exponent of b divides h.
Step 3: By symmetry (since $b \equiv a \pmod{m}$), the exponent of a divides the exponent of b. Thus both exponents are equal to h. ✓
Part (iii): $a^i \equiv a^j \pmod{m}$ iff $i \equiv j \pmod{h}$
Without loss of generality, assume $i \geq j \geq 0$.
Step 1: Since $\gcd(a, m) = 1$, a^j is invertible modulo m. Multiply both sides of $a^i \equiv a^j \pmod{m}$ by $(a^j)^{-1}$:

$$a^{i-j} \equiv 1 \pmod{m}$$

Step 2: By part (i), this holds if and only if $h \mid (i - j)$, i.e., $i \equiv j \pmod{h}$.
Conclusion: All three parts are proved. □

Example 4: Applying Part (i) – Testing Powers

The exponent of 2 modulo 7 is $h = 3$. Use part (i) to determine which of 2^{15}, 2^{10}, 2^{21} are congruent to 1 modulo 7.
Solution:
From Example 1, $\text{ord}_7(2) = 3$.
By part (i), $2^k \equiv 1 \pmod{7}$ if and only if $3 \mid k$.
(a) 2^{15}: Is $3 \mid 15$? Yes, since $15 = 3 \times 5$.

$$2^{15} \equiv 1 \pmod{7} \quad ✓$$

Verification: $2^3 \equiv 1$, so $2^{15} = (2^3)^5 \equiv 1^5 = 1 \pmod{7}$.
(b) 2^{10}: Is $3 \mid 10$? No, since $10 = 3(3) + 1$.

$$2^{10} \not\equiv 1 \pmod{7} \quad \times$$

Verification: $2^{10} = 2^9 \cdot 2 = (2^3)^3 \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{7}$.
(c) 2^{21}: Is $3 \mid 21$? Yes, since $21 = 3 \times 7$.

$$2^{21} \equiv 1 \pmod{7} \quad ✓$$

Example 5: Applying Part (iii) – Comparing Powers

The exponent of 3 modulo 10 is $h = 4$ (from Example 2). Find the least non-negative residue of $3^{47} \pmod{10}$.

Solution:

By part (iii), $3^{47} \equiv 3^r \pmod{10}$ where $r \equiv 47 \pmod{4}$.

Step 1: Divide 47 by 4:

$$47 = 4(11) + 3, \quad \text{so} \quad r = 3$$

Step 2: Therefore:

$$3^{47} \equiv 3^3 = 27 \equiv 7 \pmod{10}$$

Solution: $\boxed{3^{47} \equiv 7 \pmod{10}}$

Verification: $3^4 \equiv 1 \pmod{10}$, so $3^{47} = 3^{44} \cdot 3^3 = (3^4)^{11} \cdot 27 \equiv 1^{11} \cdot 7 = 7 \pmod{10}$. ✓

Example 6: Exponent Divides $\phi(m)$

Verify that the exponent of a modulo m always divides $\phi(m)$ for $a = 5$, $m = 12$.

Solution:

Step 1: Check $\gcd(5, 12) = 1$ ✓

Step 2: Compute $\phi(12) = \phi(4)\phi(3) = 2 \times 2 = 4$.

Step 3: Find the exponent of 5 modulo 12:

$$5^1 \equiv 5 \pmod{12}$$
$$5^2 = 25 \equiv 1 \pmod{12}$$

So $h = \text{ord}_{12}(5) = 2$.

Step 4: Check divisibility: Does $h \mid \phi(m)$? Does $2 \mid 4$?

Yes! $4 = 2 \times 2$, so $2 \mid 4$. ✓

Conclusion: $\text{ord}_{12}(5) = 2$ divides $\phi(12) = 4$, confirming the theorem. $\boxed{h = 2}$

Theorem: Exponent of a Power a^k

If h is the exponent of a modulo m, then a^k has exponent

$$\frac{h}{d}$$

where $d = \gcd(h, k)$.

That is:

$$\text{ord}_m(a^k) = \frac{h}{\gcd(h, k)}$$

Special Cases:

- If $\gcd(h, k) = 1$, then $\text{ord}_m(a^k) = h$ (same exponent as a)
- If $k = h$, then $\text{ord}_m(a^h) = 1$ (since $a^h \equiv 1 \pmod{m}$)
- If $k \mid h$, then $\text{ord}_m(a^k) = h/k$

Note: Statement only; proof omitted as per course outline.

Example 7: Computing Exponent of a Power

The exponent of 2 modulo 7 is $h = 3$. Find the exponents of 2^2 and 2^3 modulo 7.

Solution:

(a) Exponent of 2^2 modulo 7:

$d = \gcd(h, k) = \gcd(3, 2) = 1$

$$\operatorname{ord}_7(2^2) = \frac{h}{d} = \frac{3}{1} = 3$$

Verification: Compute powers of 4 modulo 7:

$$4^1 = 4 \pmod 7$$
$$4^2 = 16 \equiv 2 \pmod 7$$
$$4^3 = 4 \cdot 2 = 8 \equiv 1 \pmod 7$$

So $\operatorname{ord}_7(4) = 3$ ✓

(b) Exponent of 2^3 modulo 7:

$d = \gcd(h, k) = \gcd(3, 3) = 3$

$$\operatorname{ord}_7(2^3) = \frac{h}{d} = \frac{3}{3} = 1$$

Verification: $2^3 = 8 \equiv 1 \pmod 7$, and indeed $1^k \equiv 1 \pmod 7$ for all k, so the exponent is 1. ✓

Example 8: Using the Exponent of a Power Formula

The exponent of 3 modulo 13 is $h = 3$. Find the exponents of 3^2, 3^4, and 3^6 modulo 13.

Solution:

Step 1: First verify $\operatorname{ord}_{13}(3) = 3$.

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 = 27 = 2(13) + 1 \equiv 1 \pmod{13}$$

So $h = 3$. ✓

(a) $\operatorname{ord}_{13}(3^2)$:

$$d = \gcd(3, 2) = 1 \implies \operatorname{ord}_{13}(3^2) = \frac{3}{1} = 3$$

(b) $\operatorname{ord}_{13}(3^4)$:

$$d = \gcd(3, 4) = 1 \implies \operatorname{ord}_{13}(3^4) = \frac{3}{1} = 3$$

(c) $\operatorname{ord}_{13}(3^6)$:

$$d = \gcd(3, 6) = 3 \implies \operatorname{ord}_{13}(3^6) = \frac{3}{3} = 1$$

Verification for (c): $3^6 = (3^3)^2 \equiv 1^2 = 1 \pmod{13}$ ✓

Theorem: Condition for a^k to Have the Same Exponent as a

Let a have exponent h modulo m.
Then a^k has exponent h modulo m
if and only if

$$\gcd(k, h) = 1$$

In words: Raising a to the k-th power preserves the exponent precisely when k and h are coprime.

Note: This is a direct consequence of the previous theorem: $\operatorname{ord}_m(a^k) = h/\gcd(h,k) = h$ iff $\gcd(h,k) = 1$. Statement only.

Example 9: Checking Whether Exponent is Preserved

The exponent of 2 modulo 7 is $h = 3$. Determine for which values of k in $\{1,2,3,4,5,6\}$ the power 2^k also has exponent 3 modulo 7.

Solution:

By the theorem, $\operatorname{ord}_7(2^k) = 3$ if and only if $\gcd(k,3) = 1$.

Check each k:

k	$\gcd(k,3)$	Exponent of 2^k preserved?
1	1	Yes ✓
2	1	Yes ✓
3	3	No ×
4	1	Yes ✓
5	1	Yes ✓
6	3	No ×

So $2^1, 2^2, 2^4, 2^5$ all have exponent 3 modulo 7.

Verification for $2^2 = 4$:

$$4^1 \equiv 4, \quad 4^2 \equiv 2, \quad 4^3 \equiv 1 \pmod 7$$

So $\operatorname{ord}_7(4) = 3$ ✓

Verification for $2^3 = 8 \equiv 1 \pmod 7$: $\operatorname{ord}_7(1) = 1 \neq 3$ × (consistent with $\gcd(3,3) = 3 \neq 1$).

Example 10: Finding Powers with Preserved Exponent

The exponent of 3 modulo 10 is $h = 4$. Find all k with $1 \leq k \leq 4$ such that 3^k has the same exponent 4 modulo 10.

Solution:

By the theorem, $\operatorname{ord}_{10}(3^k) = 4$ iff $\gcd(k,4) = 1$.

k	$\gcd(k,4)$	Exponent of $3^k = 4$?
1	1	Yes ✓
2	2	No ×
3	1	Yes ✓
4	4	No ×

So $3^1 = 3$ and $3^3 = 27 \equiv 7 \pmod{10}$ both have exponent 4 modulo 10.

Verification for $3^3 \equiv 7 \pmod{10}$:

$$7^1 \equiv 7 \pmod{10}$$
$$7^2 = 49 \equiv 9 \pmod{10}$$
$$7^3 = 49 \cdot 7 = 343 \equiv 3 \pmod{10}$$
$$7^4 = 343 \cdot 7 = 2401 \equiv 1 \pmod{10}$$

So $\operatorname{ord}_{10}(7) = 4$ ✓

Primitive Root

Definition: Primitive Root Modulo m

Let $m > 0$ and let a be an integer with $\gcd(a, m) = 1$.
We say that a is a **primitive root modulo** m if the exponent of a modulo m equals $\phi(m)$, i.e.:

$$\text{ord}_m(a) = \phi(m)$$

Key Points:

- A primitive root modulo m has the **largest possible exponent**, namely $\phi(m)$
- Not every modulus m has a primitive root
- If a is a primitive root modulo m, then the powers $a^0, a^1, a^2, \ldots, a^{\phi(m)-1}$ produce all $\phi(m)$ residues that are coprime to m
- Primitive roots are sometimes called **generators** of the multiplicative group modulo m

Warning: Do not confuse the exponent $h = \text{ord}_m(a)$ with the Euler phi function $\phi(m)$. A primitive root is an element for which $h = \phi(m)$ exactly.

Example 11: Checking Whether 3 is a Primitive Root Modulo 7

Determine whether $a = 3$ is a primitive root modulo 7.
Solution:
Step 1: Compute $\phi(7) = 7 - 1 = 6$ (since 7 is prime).
Step 2: For 3 to be a primitive root, we need $\text{ord}_7(3) = 6$.
Step 3: Compute powers of 3 modulo 7:

k	3^k	$3^k \pmod 7$
1	3	3
2	9	2
3	27	6
4	81	4
5	243	5
6	729	1

Step 4: The smallest k with $3^k \equiv 1 \pmod 7$ is $k = 6$.
So $\text{ord}_7(3) = 6 = \phi(7)$.
Conclusion: 3 **is** a primitive root modulo 7. ✓
Insight: The powers $3^1, 3^2, \ldots, 3^6$ give residues $3, 2, 6, 4, 5, 1$ — which is exactly the set $\{1, 2, 3, 4, 5, 6\}$, confirming that 3 generates all units modulo 7.

Example 12: Checking Whether 2 is a Primitive Root Modulo 7

Determine whether $a = 2$ is a primitive root modulo 7.
Solution:
Step 1: $\phi(7) = 6$.

Step 2: Compute powers of 2 modulo 7:

$$2^1 \equiv 2 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$2^3 \equiv 1 \pmod 7$$

Step 3: The smallest k with $2^k \equiv 1 \pmod 7$ is $k = 3$.
So $\text{ord}_7(2) = 3 \neq 6 = \phi(7)$.
Conclusion: 2 is **not** a primitive root modulo 7. ×
The powers $2^1, 2^2, 2^3$ give only $\{2, 4, 1\}$, missing $\{3, 5, 6\}$.

Example 13: Primitive Root Modulo 10

Determine whether $a = 3$ is a primitive root modulo 10.
Solution:
Step 1: $\phi(10) = \phi(2)\phi(5) = 1 \times 4 = 4$.
Step 2: For 3 to be a primitive root, need $\text{ord}_{10}(3) = 4$.
Step 3: Compute powers of 3 modulo 10:

$$3^1 \equiv 3 \pmod{10}$$
$$3^2 = 9 \equiv 9 \pmod{10}$$
$$3^3 = 27 \equiv 7 \pmod{10}$$
$$3^4 = 81 \equiv 1 \pmod{10}$$

Step 4: The smallest k with $3^k \equiv 1 \pmod{10}$ is $k = 4 = \phi(10)$.
Conclusion: 3 **is** a primitive root modulo 10. ✓
The powers $\{3, 9, 7, 1\}$ are all residues coprime to 10 (i.e., $\{1, 3, 7, 9\}$). ✓

Theorem: Powers of a Primitive Root Form an RRS

If a is a primitive root modulo m, then

$$1,\ a,\ a^2,\ \ldots,\ a^{\phi(m)-1}$$

form a **reduced residue system** modulo m.
In words: The $\phi(m)$ powers of a primitive root produce, in some order, exactly all of the residues modulo m that are coprime to m.

Proof: Powers of a Primitive Root Form an RRS

Proof:
Let a be a primitive root modulo m, so $\text{ord}_m(a) = \phi(m)$.
We must show that the $\phi(m)$ elements $a^0, a^1, \ldots, a^{\phi(m)-1}$ are:

1. All coprime to m
2. Mutually incongruent modulo m

Part 1: Each a^k is coprime to m
Since $\gcd(a, m) = 1$, we have $\gcd(a^k, m) = 1$ for all $k \geq 0$. ✓
Part 2: Mutual Incongruence
Suppose for contradiction that $a^i \equiv a^j \pmod m$ for some $0 \leq i < j \leq \phi(m) - 1$.

By Part (iii) of the Exponent Theorem:

$$a^i \equiv a^j \pmod{m} \implies i \equiv j \pmod{\phi(m)}$$

Since $0 \leq i < j \leq \phi(m) - 1$, we have $0 < j - i < \phi(m)$, so $j - i$ is not divisible by $\phi(m)$. This is a contradiction. Therefore no two elements in the list are congruent. ✓
Conclusion: The $\phi(m)$ elements $1, a, a^2, \ldots, a^{\phi(m)-1}$ are pairwise incongruent modulo m and each is coprime to m.
Since there are exactly $\phi(m)$ residues coprime to m, these elements form a reduced residue system modulo m. □

Example 14: Verifying the Theorem for a

Verify that the powers of the primitive root $a = 3$ modulo 7 form a reduced residue system.
Solution:
$\phi(7) = 6$, so we list $3^0, 3^1, \ldots, 3^5$ modulo 7:

k	3^k	$3^k \pmod 7$
0	1	1
1	3	3
2	9	2
3	27	6
4	81	4
5	243	5

The residues are $\{1, 2, 3, 4, 5, 6\}$, which is exactly the set of all integers from 1 to 6 (all coprime to 7).
Conclusion: The powers $1, 3, 9, 27, 81, 243$ form a reduced residue system modulo 7. ✓

Example 15: Verifying the Theorem for a

Verify that the powers of the primitive root $a = 3$ modulo 10 form a reduced residue system.
Solution:
$\phi(10) = 4$, so we list $3^0, 3^1, 3^2, 3^3$ modulo 10:

k	3^k	$3^k \pmod{10}$
0	1	1
1	3	3
2	9	9
3	27	7

The residues are $\{1, 3, 7, 9\}$.
The integers coprime to 10 in $\{1, \ldots, 10\}$ are $\{1, 3, 7, 9\}$. ✓
Conclusion: The powers of 3 form a reduced residue system modulo 10. ✓

Theorem: Number of Primitive Roots Modulo m

If m has a primitive root, then m has exactly

$$\phi\big(\phi(m)\big)$$

primitive roots modulo m.

Proof: Number of Primitive Roots

Proof:
Suppose a is a primitive root modulo m, so $\text{ord}_m(a) = \phi(m)$.
Step 1: Identify all elements of the RRS
By the previous theorem, $\{a^0, a^1, \ldots, a^{\phi(m)-1}\}$ is a complete list of all residues coprime to m.
So every element b with $\gcd(b, m) = 1$ has the form $b \equiv a^k \pmod{m}$ for a unique k with $0 \leq k \leq \phi(m) - 1$.
Step 2: Determine which a^k are primitive roots
By the theorem on the exponent of a power:

$$\text{ord}_m(a^k) = \frac{\phi(m)}{\gcd(k,\, \phi(m))}$$

For a^k to be a primitive root, we need:

$$\text{ord}_m(a^k) = \phi(m) \implies \frac{\phi(m)}{\gcd(k, \phi(m))} = \phi(m) \implies \gcd(k, \phi(m)) = 1$$

Step 3: Count such k
The number of integers k in $\{0, 1, \ldots, \phi(m)-1\}$ with $\gcd(k, \phi(m)) = 1$ is exactly $\phi(\phi(m))$.
Conclusion: There are exactly $\phi(\phi(m))$ primitive roots modulo m. □

Example 16: Counting and Finding Primitive Roots Modulo 7

Find all primitive roots modulo 7.
Solution:
Step 1: $\phi(7) = 6$, so there are $\phi(\phi(7)) = \phi(6) = \phi(2)\phi(3) = 1 \times 2 = 2$ primitive roots.
Step 2: From Example 11, $a = 3$ is a primitive root modulo 7.
Step 3: The primitive roots are 3^k where $\gcd(k, 6) = 1$, for $k \in \{1, 2, 3, 4, 5, 6\}$:

k	$\gcd(k, 6)$	$3^k \pmod 7$	Primitive Root?
1	1	3	Yes ✓
2	2	2	No ×
3	3	6	No ×
4	2	4	No ×
5	1	5	Yes ✓
6	6	1	No ×

Primitive roots modulo 7: 3 and 5
Verification for 5:

$$5^1 \equiv 5, \quad 5^2 \equiv 4, \quad 5^3 \equiv 6, \quad 5^4 \equiv 2, \quad 5^5 \equiv 3, \quad 5^6 \equiv 1 \pmod 7$$

All of $\{1, 2, 3, 4, 5, 6\}$ appear. ✓

Example 17: Counting Primitive Roots Modulo 9

How many primitive roots does 9 have? Find one.

Solution:

Step 1: Compute $\phi(9) = 9\left(1 - \frac{1}{3}\right) = 6$.

Number of primitive roots $= \phi(\phi(9)) = \phi(6) = 2$.

Step 2: Test $a = 2$. Need $\text{ord}_9(2) = 6$.

Compute powers of 2 modulo 9:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 7, \quad 2^5 \equiv 5, \quad 2^6 \equiv 1 \pmod 9$$

The smallest k with $2^k \equiv 1 \pmod 9$ is $k = 6 = \phi(9)$.

Conclusion: 2 is a primitive root modulo 9. ✓

There are exactly $\phi(6) = 2$ primitive roots modulo 9: $\boxed{2 \text{ and } 5}$.

Verification for 5: $5 \equiv 2^5 \pmod 9$, and $\gcd(5, 6) = 1$, so 5 is also a primitive root. ✓

Theorem

If a is a primitive root modulo m, then a^k is a primitive root modulo m **if and only if**

$$\gcd\big(k,\ \phi(m)\big) = 1$$

In words: Among all the powers $a^1, a^2, \ldots, a^{\phi(m)}$, exactly those with index k coprime to $\phi(m)$ are primitive roots.

Note: Statement only; this follows directly from the exponent-of-a-power theorem.

Theorem: Primitive Roots of a Prime p

If p is prime, then there exist exactly

$$\phi(p-1)$$

incongruent primitive roots modulo p.

In words: Every prime p has primitive roots, and the count is $\phi(p-1)$ (since $\phi(p) = p - 1$ and the number of primitive roots is $\phi(\phi(p)) = \phi(p-1)$).

Note: Statement only.

Example 18: Primitive Roots of p

How many primitive roots does 11 have? List them all.

Solution:

Step 1: $p = 11$ is prime, $\phi(11) = 10$.

Number of primitive roots $= \phi(10) = \phi(2)\phi(5) = 1 \times 4 = 4$.

Step 2: Find one primitive root. Test $a = 2$:

Possible exponents of 2 modulo 11 must divide $\phi(11) = 10$, so must be in $\{1, 2, 5, 10\}$.

$$\begin{aligned} 2^1 &\equiv 2 \pmod{11} \\ 2^2 &\equiv 4 \pmod{11} \\ 2^5 &= 32 \equiv 10 \pmod{11} \\ 2^{10} &\equiv 1 \pmod{11} \quad \text{(by Fermat's Little Theorem)} \end{aligned}$$

Since $2^1, 2^2, 2^5 \not\equiv 1 \pmod{11}$, we conclude $\text{ord}_{11}(2) = 10$.

So 2 is a primitive root modulo 11. ✓
Step 3: All primitive roots are $2^k \pmod{11}$ for $\gcd(k, 10) = 1$, i.e., $k \in \{1, 3, 7, 9\}$:

k	$\gcd(k, 10)$	$2^k \pmod{11}$
1	1	2
3	1	8
7	1	7
9	1	6

Primitive roots modulo 11: $\boxed{2,\ 6,\ 7,\ 8}$

Theorem: No Primitive Root Modulo 2^n for $n \geq 3$

There is no primitive root modulo 2^n for any $n \geq 3$.
More precisely, for $n \geq 3$ and any odd integer a:

$$a^{\phi(2^n)/2} = a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

so the exponent of a modulo 2^n is at most $2^{n-2} = \phi(2^n)/2 < \phi(2^n)$.
⚠ **Note:** Primitive roots do exist modulo $2^1 = 2$ (trivially) and $2^2 = 4$ (with $a = 3$), but fail for all higher powers of 2.

Proof: No Primitive Root Modulo 2^n for $n \geq 3$

Proof:
We prove by induction that for all odd integers a and all $n \geq 3$:

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

Base Case: $n = 3$
Every odd integer a has the form $a = 2k + 1$ for some integer k. Then:

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$$

Since $k(k+1)$ is the product of two consecutive integers, one of them is even, so $k(k+1) = 2t$ for some integer t. Therefore:

$$a^2 = 8t + 1 \equiv 1 \pmod{8}$$

Since $2^{3-2} = 2^1 = 2$, we have $a^{2^{n-2}} = a^2 \equiv 1 \pmod{8} = \pmod{2^3}$. ✓
Inductive Step:
Assume $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for some $n \geq 3$.
Write $a^{2^{n-2}} = 1 + 2^n \cdot s$ for some integer s. Then:

$$a^{2^{n-1}} = \left(a^{2^{n-2}}\right)^2 = (1 + 2^n s)^2 = 1 + 2^{n+1} s + 2^{2n} s^2$$

Since $n \geq 3$ implies $2n \geq n + 1$, both $2^{n+1}s$ and $2^{2n}s^2$ are divisible by 2^{n+1}:

$$a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$$

This completes the induction. ✓
Conclusion:
For $n \geq 3$, every odd integer a satisfies $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.

Since $\phi(2^n) = 2^{n-1}$ and $2^{n-2} = \phi(2^n)/2 < \phi(2^n)$, the exponent of a modulo 2^n is at most $\phi(2^n)/2$.
Therefore, no a can have exponent equal to $\phi(2^n)$, so there is no primitive root modulo 2^n for $n \geq 3$. □

Example 19: Verifying No Primitive Root Modulo 8

Verify that there is no primitive root modulo $8 = 2^3$.
Solution:
$\phi(8) = 4$. A primitive root would need exponent 4.
The odd integers modulo 8 coprime to 8 are $\{1, 3, 5, 7\}$. Check each:

a	$a^2 \pmod 8$	$a^4 \pmod 8$	$\text{ord}_8(a)$
1	1	1	1
3	1	1	2
5	1	1	2
7	1	1	2

No element has exponent $4 = \phi(8)$.
Conclusion: There is no primitive root modulo 8. ✓
⚠ **Contrast with $m = 4 = 2^2$:** $\phi(4) = 2$. Check $a = 3$: $3^1 \equiv 3 \pmod 4$ and $3^2 = 9 \equiv 1 \pmod 4$. So $\text{ord}_4(3) = 2 = \phi(4)$, confirming that 3 is a primitive root modulo 4.

Example 20: Verifying No Primitive Root Modulo 16

Verify that there is no primitive root modulo $16 = 2^4$.
Solution:
$\phi(16) = 8$. By the theorem, every odd a satisfies $a^{2^{4-2}} = a^4 \equiv 1 \pmod{16}$.
Check:

$$3^2 = 9, \quad 3^4 = 81 = 5(16) + 1 \equiv 1 \pmod{16} \quad (\text{exponent} = 4)$$
$$5^2 = 25 \equiv 9 \pmod{16}, \quad 5^4 \equiv 9^2 = 81 \equiv 1 \pmod{16} \quad (\text{exponent} = 4)$$
$$7^2 = 49 \equiv 1 \pmod{16} \quad (\text{exponent} = 2)$$

The maximum exponent attained is $4 = \phi(16)/2 = 8/2$.
No element achieves exponent $8 = \phi(16)$.
Conclusion: There is no primitive root modulo 16. ✓

Theorem

ℹ **Key Idea:** When both $m > 2$ and $n > 2$ with $\gcd(m, n) = 1$, the maximum possible order of any element modulo mn is $\text{lcm}(\phi(m), \phi(n))$, which is strictly less than $\phi(mn) = \phi(m)\phi(n)$.
This follows because $\phi(m)$ and $\phi(n)$ are both even (for $m, n > 2$), so their lcm is less than their product.
⚠ **Note:** Statement only.

Example 21: No Primitive Root Modulo 15

Verify that $15 = 3 \times 5$ has no primitive root.

Solution:

Here $m = 3$, $n = 5$, $\gcd(3, 5) = 1$, $m > 2$, $n > 2$.

$\phi(15) = \phi(3)\phi(5) = 2 \times 4 = 8$.

For a primitive root, we would need an element of order 8 modulo 15.

By the theorem, the maximum order of any element modulo 15 is:

$$\text{lcm}(\phi(3), \phi(5)) = \text{lcm}(2, 4) = 4 < 8 = \phi(15)$$

The integers coprime to 15 are $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Check orders:

a	$\text{ord}_{15}(a)$
2	4
4	2
7	4
8	4
11	2
13	4
14	2

Maximum order is $4 < 8 = \phi(15)$.

Conclusion: No primitive root exists modulo 15. ✓

Summary: Primitive Roots

Definition: a is a primitive root modulo m iff $\text{ord}_m(a) = \phi(m)$.

Result	Statement
Powers form RRS	$1, a, a^2, \ldots, a^{\phi(m)-1}$ is a reduced residue system
Count of primitive roots	Exactly $\phi(\phi(m))$ primitive roots if any exist
Which powers are primitive roots	a^k is primitive root iff $\gcd(k, \phi(m)) = 1$
Primes	Every prime p has exactly $\phi(p-1)$ primitive roots
Powers of 2	No primitive root modulo 2^n for $n \geq 3$
Coprime composite	No primitive root modulo mn if $\gcd(m, n) = 1$, $m > 2$, $n > 2$

Moduli with Primitive Roots: Primitive roots exist **only** for $m = 1, 2, 4, p^k, 2p^k$ where p is an odd prime.

Example 22: Find All Primitive Roots Modulo 7

Find all primitive roots modulo 7.

Solution:

Step 1: $p = 7$ is prime, so $\phi(7) = 6$.

Number of primitive roots $= \phi(\phi(7)) = \phi(6) = \phi(2)\phi(3) = 1 \times 2 = 2$.

Step 2: Find one primitive root by testing elements.

The exponent of any element must divide $\phi(7) = 6$, so must be in $\{1, 2, 3, 6\}$. An element is a primitive root iff its exponent equals 6.
Test $a = 2$:

$$2^1 \equiv 2 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$2^3 \equiv 1 \pmod 7$$

$\text{ord}_7(2) = 3 \neq 6$, so 2 is not a primitive root. ×
Test $a = 3$:

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod 7$$

$\text{ord}_7(3) = 6 = \phi(7)$, so 3 is a primitive root. ✓
Step 3: Find all primitive roots using $3^k \pmod 7$ for $\gcd(k, 6) = 1$:
Values of k with $\gcd(k, 6) = 1$: $k \in \{1, 5\}$

k	$\gcd(k, 6)$	$3^k \pmod 7$
1	1	3
5	1	5

Primitive roots modulo 7: 3 and 5
Verification for 5:

$$5^1 \equiv 5,\ 5^2 \equiv 4,\ 5^3 \equiv 6,\ 5^4 \equiv 2,\ 5^5 \equiv 3,\ 5^6 \equiv 1 \pmod 7$$

All of $\{1, 2, 3, 4, 5, 6\}$ appear. ✓

Example 23: Find All Primitive Roots Modulo 12

Find all primitive roots modulo 12, or show that none exist.
Solution:
Step 1: Factorize: $12 = 4 \times 3 = 2^2 \times 3$.
Note that $12 = mn$ with $m = 4$, $n = 3$, $\gcd(4, 3) = 1$, $m = 4 > 2$, $n = 3 > 2$.
By the theorem on coprime composites, 12 has **no primitive root**. ×
Verification:
$\phi(12) = \phi(4)\phi(3) = 2 \times 2 = 4$.
The maximum possible order of any element modulo 12 is:

$$\text{lcm}(\phi(4), \phi(3)) = \text{lcm}(2, 2) = 2 < 4 = \phi(12)$$

Check all units modulo 12 (integers coprime to 12): $\{1, 5, 7, 11\}$:

a	$a^2 \pmod{12}$	$\text{ord}_{12}(a)$
1	1	1
5	1	2
7	1	2
11	1	2

Maximum order is $2 < 4 = \phi(12)$.
Conclusion: No primitive root exists modulo 12. ✓

Example 24: Find All Primitive Roots Modulo 17

Find all primitive roots modulo 17.

Solution:

Step 1: $p = 17$ is prime. $\phi(17) = 16$.

Number of primitive roots $= \phi(\phi(17)) = \phi(16) = \phi(2^4) = 2^3 = 8$.

Step 2: Find one primitive root. The exponent of any element must divide 16, so must be in $\{1, 2, 4, 8, 16\}$. An element a is a primitive root iff $a^1, a^2, a^4, a^8 \not\equiv 1 \pmod{17}$.

Test $a = 3$:

$$\begin{aligned} 3^2 &= 9 \pmod{17} \\ 3^4 &= 81 = 4(17) + 13 \equiv 13 \pmod{17} \\ 3^8 &\equiv 13^2 = 169 = 9(17) + 16 \equiv 16 \equiv -1 \pmod{17} \\ 3^{16} &\equiv (-1)^2 = 1 \pmod{17} \end{aligned}$$

Since $3^2, 3^4, 3^8 \not\equiv 1 \pmod{17}$, we conclude $\text{ord}_{17}(3) = 16$.

So 3 is a primitive root modulo 17. ✓

Step 3: All primitive roots are $3^k \pmod{17}$ for $\gcd(k, 16) = 1$, i.e., k odd and not divisible by any prime factor of 16 other than itself.

The values of $k \in \{1, 2, \ldots, 16\}$ with $\gcd(k, 16) = 1$ are: $k \in \{1, 3, 5, 7, 9, 11, 13, 15\}$ (all odd numbers from 1 to 15).

k	$\gcd(k, 16)$	$3^k \pmod{17}$
1	1	3
3	1	10
5	1	5
7	1	11
9	1	14
11	1	7
13	1	12
15	1	6

Primitive roots modulo 17: $\boxed{3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14}$

Theorem: Primitive Root Exists for Every Odd Prime

There exists at least one primitive root modulo each odd prime p.

In words: Every prime number $p \geq 3$ has a primitive root. The proof of this fact uses the theory of polynomials modulo a prime and goes beyond the current scope.

Note: Statement only.

Lemma: Lifting Primitive Root from p to p Squared

If p is an odd prime, then there exists a primitive root r of p such that

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

In words: Among all the primitive roots of an odd prime p, at least one of them fails to satisfy $r^{p-1} \equiv 1 \pmod{p^2}$. Such a root is called a **good** primitive root and is the key to extending primitive roots from p to p^2 and higher powers.

Note: Statement only.

Lemma: Primitive Root Persists to Higher Powers of p

Let p be an odd prime and let r be a primitive root of p satisfying

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

Then for every positive integer $k \geq 2$:

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

In words: The "good" primitive root r retains large order as we pass to higher powers of p. This lemma is the technical engine behind the proof that p^k has a primitive root.
Note: Statement only.

Theorem: Primitive Root Exists for All Powers of an Odd Prime

If p is an odd prime and $k \geq 1$, then there exists a primitive root modulo p^k.
In words: Not only does every odd prime have a primitive root, but so does every prime power p^k. The primitive root for p^k is constructed from a good primitive root of p using the two lemmas above.
Note: Statement only.

Example 25: Primitive Root Modulo 9

Verify that $p^k = 9 = 3^2$ has a primitive root, and find one.
Solution:
Step 1: $p = 3$, $k = 2$. $\phi(9) = 9\left(1 - \frac{1}{3}\right) = 6$.
Number of primitive roots $= \phi(\phi(9)) = \phi(6) = 2$.
Step 2: Test $r = 2$ as a primitive root of $p = 3$:

$$2^1 \equiv 2, \quad 2^2 \equiv 1 \pmod{3}$$

So $\text{ord}_3(2) = 2 = \phi(3)$. Hence 2 is a primitive root of 3. ✓
Step 3: Check whether 2 is also a primitive root of $9 = 3^2$:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{9} \\ 2^2 &\equiv 4 \pmod{9} \\ 2^3 &\equiv 8 \pmod{9} \\ 2^4 &\equiv 7 \pmod{9} \\ 2^5 &\equiv 5 \pmod{9} \\ 2^6 &\equiv 1 \pmod{9} \end{aligned}$$

The smallest k with $2^k \equiv 1 \pmod{9}$ is $k = 6 = \phi(9)$.
Conclusion: 2 is a primitive root modulo 9. ✓

Example 26: Primitive Root Modulo 25

Verify that $p^k = 25 = 5^2$ has a primitive root, and find one.
Solution:
Step 1: $p = 5$, $k = 2$. $\phi(25) = 25\left(1 - \frac{1}{5}\right) = 20$.

Number of primitive roots $= \phi(20) = \phi(4)\phi(5) = 2 \times 4 = 8$.
Step 2: Test $r = 2$ as a primitive root of $p = 5$:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 3, \quad 2^4 \equiv 1 \pmod 5$$

$\text{ord}_5(2) = 4 = \phi(5)$, so 2 is a primitive root of 5. ✓
Step 3: Check whether 2 lifts to a primitive root of 25.
Check the good-root condition: $2^{p-1} = 2^4 = 16 \not\equiv 1 \pmod{25}$. ✓
So 2 is a good primitive root. Now verify $\text{ord}_{25}(2) = 20$:
The order must divide $\phi(25) = 20$, so it is in $\{1, 2, 4, 5, 10, 20\}$.

$$\begin{aligned} 2^4 &= 16 \not\equiv 1 \pmod{25} \\ 2^5 &= 32 \equiv 7 \not\equiv 1 \pmod{25} \\ 2^{10} &= 7^2 = 49 \equiv 24 \equiv -1 \not\equiv 1 \pmod{25} \\ 2^{20} &\equiv (-1)^2 = 1 \pmod{25} \end{aligned}$$

Since $2^4, 2^5, 2^{10} \not\equiv 1$ but $2^{20} \equiv 1 \pmod{25}$, we conclude $\text{ord}_{25}(2) = 20 = \phi(25)$.
Conclusion: 2 is a primitive root modulo 25. ✓

Corollary: Primitive Roots Exist Modulo $2p^k$

There are primitive roots modulo $2p^k$ where p is an odd prime and $k \geq 1$.
How to Construct One:
Let r be a primitive root modulo p^k.

- If r is odd, then r is also a primitive root modulo $2p^k$
- If r is even, then $r + p^k$ is odd and is a primitive root modulo $2p^k$

This works because $\phi(2p^k) = \phi(2)\phi(p^k) = 1 \cdot \phi(p^k) = \phi(p^k)$, so the same order suffices.
Note: Statement only.

Example 27: Primitive Root Modulo 18

Find a primitive root modulo $18 = 2 \times 3^2$.
Solution:
Step 1: Identify the structure. $18 = 2p^k$ with $p = 3$, $k = 2$.
$\phi(18) = \phi(2)\phi(9) = 1 \times 6 = 6$.
Step 2: From Example 25, $r = 2$ is a primitive root modulo 9.
Step 3: $r = 2$ is even, so we use $r + p^k = 2 + 9 = 11$.
Check $\gcd(11, 18) = 1$ ✓
Step 4: Verify $\text{ord}_{18}(11) = 6 = \phi(18)$:

$$\begin{aligned} 11^2 &= 121 = 6(18) + 13 \equiv 13 \pmod{18} \\ 11^3 &\equiv 11 \cdot 13 = 143 = 7(18) + 17 \equiv 17 \pmod{18} \\ 11^6 &\equiv 17^2 = 289 = 16(18) + 1 \equiv 1 \pmod{18} \end{aligned}$$

Check that no smaller divisor of 6 gives 1: $11^1 \equiv 11$, $11^2 \equiv 13$, $11^3 \equiv 17 \pmod{18}$ — none equal 1. ✓
Conclusion: $\text{ord}_{18}(11) = 6 = \phi(18)$, so 11 is a primitive root modulo 18. $\boxed{r = 11}$ ✓

Example 28: Primitive Root Modulo 50

Find a primitive root modulo $50 = 2 \times 5^2$.

Solution:

Step 1: $50 = 2p^k$ with $p = 5$, $k = 2$.
$\phi(50) = \phi(2)\phi(25) = 1 \times 20 = 20$.
Step 2: From Example 26, $r = 2$ is a primitive root modulo 25.
Step 3: $r = 2$ is even, so use $r + p^k = 2 + 25 = 27$.
Check $\gcd(27, 50) = 1$ ✓
Step 4: Since $27 \equiv 2 \pmod{25}$ and 27 is odd, we verify $\text{ord}_{50}(27) = 20$.
The key fact: $\phi(50) = \phi(25) = 20$. Since 27 is the odd lift of the primitive root 2 of 25, and $\gcd(27, 50) = 1$, it follows that $\text{ord}_{50}(27) = 20$.
Conclusion: 27 is a primitive root modulo 50. $\boxed{r = 27}$ ✓

Summary: Existence of Primitive Roots

Modulus	Primitive Root Exists?	Count
$1, 2$	Yes (trivial)	1
4	Yes	1
p (odd prime)	Yes	$\phi(p-1)$
p^k (odd prime)	Yes	$\phi(\phi(p^k))$
$2p^k$ (odd prime)	Yes	$\phi(\phi(2p^k))$
2^n, $n \geq 3$	No	0
mn, $\gcd(m,n) = 1$, $m>2$, $n>2$	No	0

Key Chain of Results:

1. Every odd prime p has a primitive root (existence theorem)
2. A "good" primitive root of p satisfies $r^{p-1} \not\equiv 1 \pmod{p^2}$
3. Such a root persists to all p^k: $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$
4. Therefore p^k has a primitive root for all $k \geq 1$
5. The odd lift of a primitive root of p^k gives one for $2p^k$

Index of an Integer Relative to a Primitive Root

Definition: Index of an Integer

Let g be a primitive root modulo m. For any integer a with $\gcd(a, m) = 1$, there exists a unique integer k with $1 \leq k \leq \phi(m)$ such that:

$$g^k \equiv a \pmod{m}$$

This integer k is called the **index** of a relative to the primitive root g modulo m, written:

$$k = \operatorname{ind}_g a \quad \text{or simply} \quad k = \operatorname{ind} a$$

This is also called the **discrete logarithm** of a base g modulo m.

Key Points:

- The index exists and is unique because the powers $g^1, g^2, \ldots, g^{\phi(m)}$ form a reduced residue system modulo m
- The index plays the same role modulo m as the logarithm does for real numbers
- $\operatorname{ind}_g g = 1$ always, since $g^1 \equiv g$
- $\operatorname{ind}_g 1 = \phi(m)$ always, since $g^{\phi(m)} \equiv 1 \pmod{m}$
- The index depends on the choice of primitive root g

Warning: The index is only defined for integers a with $\gcd(a, m) = 1$.

Example 29: Building an Index Table Modulo 7

Using $g = 3$ as a primitive root modulo 7, build the complete index table.

Solution:

From Example 11, $g = 3$ is a primitive root modulo 7 with $\phi(7) = 6$.

Compute $3^k \pmod{7}$ for $k = 1, 2, \ldots, 6$:

k	$3^k \pmod{7}$	$\operatorname{ind}_3 a = k$ for $a =$
1	3	$\operatorname{ind}_3 3 = 1$
2	2	$\operatorname{ind}_3 2 = 2$
3	6	$\operatorname{ind}_3 6 = 3$
4	4	$\operatorname{ind}_3 4 = 4$
5	5	$\operatorname{ind}_3 5 = 5$
6	1	$\operatorname{ind}_3 1 = 6$

Reading the table as an index table (sorted by a):

a	1	2	3	4	5	6
$\operatorname{ind}_3 a$	6	2	1	4	5	3

Verification: $3^4 = 81 = 11(7) + 4 \equiv 4 \pmod{7}$, so $\operatorname{ind}_3 4 = 4$. ✓

Example 30: Building an Index Table Modulo 11

Using $g = 2$ as a primitive root modulo 11, build the complete index table.

Solution:

From Example 18, $g = 2$ is a primitive root modulo 11 with $\phi(11) = 10$.

Compute $2^k \pmod{11}$ for $k = 1, \ldots, 10$:

k	1	2	3	4	5	6	7	8	9	10
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Reading as index table (sorted by a):

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_2\, a$	10	1	8	2	4	9	7	3	6	5

Verification: $2^8 = 256 = 23(11) + 3 \equiv 3 \pmod{11}$, so $\text{ind}_2\, 3 = 8$. ✓

Properties of Indices

Theorem: Properties of Indices

Let g be a primitive root modulo m and let a, b be integers with $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$. Then:

Property 1 (Product Rule):

$$\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(m)}$$

Property 2 (Power Rule):

$$\operatorname{ind}_g(a^n) \equiv n \cdot \operatorname{ind}_g a \pmod{\phi(m)}$$

Property 3 (Index of 1):

$$\operatorname{ind}_g 1 \equiv 0 \pmod{\phi(m)}$$

Analogy with Logarithms:

- Property 1 mirrors $\log(ab) = \log a + \log b$
- Property 2 mirrors $\log(a^n) = n \log a$
- Property 3 mirrors $\log 1 = 0$

Proof: Properties of Indices

Proof:

Let $\operatorname{ind}_g a = s$ and $\operatorname{ind}_g b = t$, so $g^s \equiv a \pmod{m}$ and $g^t \equiv b \pmod{m}$.

Property 1: Product Rule

Step 1: Multiply the two congruences:

$$g^s \cdot g^t \equiv ab \pmod{m}$$

$$g^{s+t} \equiv ab \pmod{m}$$

Step 2: By definition of index, $\operatorname{ind}_g(ab)$ is the unique k with $1 \leq k \leq \phi(m)$ satisfying $g^k \equiv ab \pmod{m}$.

Since $g^{s+t} \equiv ab$ and g has order $\phi(m)$, two powers of g are congruent modulo m if and only if their exponents are congruent modulo $\phi(m)$ (by Part (iii) of the Exponent Theorem). Therefore:

$$\operatorname{ind}_g(ab) \equiv s + t \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(m)}$$

✓

Property 2: Power Rule

Step 1: Raise $g^s \equiv a \pmod{m}$ to the power n:

$$(g^s)^n \equiv a^n \pmod{m}$$

$$g^{sn} \equiv a^n \pmod{m}$$

Step 2: By the same reasoning as Property 1:

$$\operatorname{ind}_g(a^n) \equiv sn \equiv n \cdot \operatorname{ind}_g a \pmod{\phi(m)}$$

✓

Property 3: Index of 1

Since $g^{\phi(m)} \equiv 1 \pmod{m}$ and $\phi(m) \equiv 0 \pmod{\phi(m)}$:

$$\text{ind}_g 1 \equiv \phi(m) \equiv 0 \pmod{\phi(m)}$$

✓

Conclusion: All three properties are proved. □

Example 31: Using the Product Rule for Indices

Using the index table modulo 7 with $g = 3$, compute $\text{ind}_3(4 \cdot 5)$ modulo 7.

Solution:

From the index table in Example 29: $\text{ind}_3 4 = 4$ and $\text{ind}_3 5 = 5$, and $\phi(7) = 6$.

By the Product Rule:

$$\text{ind}_3(4 \cdot 5) \equiv \text{ind}_3 4 + \text{ind}_3 5 \equiv 4 + 5 = 9 \equiv 3 \pmod{6}$$

So $\text{ind}_3(20) = 3$, meaning $3^3 \equiv 20 \pmod{7}$.

Verification: $3^3 = 27 = 3(7) + 6 \equiv 6 \pmod{7}$, and $20 = 2(7) + 6 \equiv 6 \pmod{7}$. ✓

Example 32: Using the Power Rule for Indices

Using the index table modulo 11 with $g = 2$, evaluate $3^7 \pmod{11}$.

Solution:

From Example 30, $\text{ind}_2 3 = 8$ and $\phi(11) = 10$.

By the Power Rule:

$$\text{ind}_2(3^7) \equiv 7 \cdot \text{ind}_2 3 \equiv 7 \cdot 8 = 56 \equiv 6 \pmod{10}$$

So $3^7 \equiv 2^6 \pmod{11}$.

Now compute $2^6 = 64 = 5(11) + 9 \equiv 9 \pmod{11}$.

Solution: $\boxed{3^7 \equiv 9 \pmod{11}}$

Verification: $3^2 = 9$, $3^4 \equiv 81 \equiv 4$, $3^7 = 3^4 \cdot 3^2 \cdot 3 \equiv 4 \cdot 9 \cdot 3 = 108 = 9(11) + 9 \equiv 9 \pmod{11}$. ✓

Binomial Congruences

Definition: Binomial Congruence

A congruence of the form

$$x^n \equiv a \pmod{m}$$

where n is a fixed positive integer and a is a given integer with $\gcd(a, m) = 1$, is called a **binomial congruence**.

Solution Method Using Indices:

Let g be a primitive root modulo m. Taking indices of both sides:

$$n \cdot \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{\phi(m)}$$

This is a **linear congruence** in the unknown $\operatorname{ind}_g x$.

- It has solutions iff $d = \gcd(n, \phi(m))$ divides $\operatorname{ind}_g a$
- If solutions exist, there are exactly d incongruent solutions modulo m

Example 33: Solving a Binomial Congruence

Solve $x^3 \equiv 6 \pmod{7}$.

Solution:

Step 1: Use primitive root $g = 3$ modulo 7, $\phi(7) = 6$.

Check solvability: $d = \gcd(3, 6) = 3$. From Example 29, $\operatorname{ind}_3 6 = 3$.

Does $d \mid \operatorname{ind}_3 6$? Does $3 \mid 3$? Yes. ✓

So there are $d = 3$ solutions.

Step 2: Apply indices to both sides:

$$3 \cdot \operatorname{ind}_3 x \equiv \operatorname{ind}_3 6 \pmod{6}$$

$$3 \cdot \operatorname{ind}_3 x \equiv 3 \pmod{6}$$

Step 3: Solve the linear congruence. Divide by $d = 3$:

$$\operatorname{ind}_3 x \equiv 1 \pmod{2}$$

Solutions modulo 6: $\operatorname{ind}_3 x \in \{1, 3, 5\}$.

Step 4: Convert indices back to values using the table from Example 29:

$\operatorname{ind}_3 x$	$x \pmod 7$
1	3
3	6
5	5

Solutions: $\boxed{x \equiv 3,\ 5,\ 6 \pmod{7}}$

Verification:

- $3^3 = 27 = 3(7) + 6 \equiv 6 \pmod{7}$ ✓
- $5^3 = 125 = 17(7) + 6 \equiv 6 \pmod{7}$ ✓
- $6^3 = 216 = 30(7) + 6 \equiv 6 \pmod{7}$ ✓

Example 34: Binomial Congruence with No Solution

Determine whether $x^2 \equiv 3 \pmod 7$ has solutions.

Solution:

Step 1: Use $g = 3$ modulo 7, $\phi(7) = 6$.

$d = \gcd(2, 6) = 2$.

From Example 29, $\operatorname{ind}_3 3 = 1$.

Step 2: Check solvability: does $d \mid \operatorname{ind}_3 3$? Does $2 \mid 1$?

No, $2 \nmid 1$. $\times$

Conclusion: The congruence $x^2 \equiv 3 \pmod 7$ has **no solution**.

Verification by exhaustion:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1 \pmod 7$$

None equal 3. $\checkmark$

Exponential Congruences

Definition: Exponential Congruence

A congruence in which the unknown variable occurs in the **exponent** is called an **exponential congruence**. The general form is:

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

where a, b are given integers with $\gcd(a, m) = 1$ and x is the unknown.

Solution Method Using Indices:

Let g be a primitive root modulo m. Then $a \equiv g^s \pmod{m}$ where $s = \operatorname{ind}_g a$. The congruence becomes:

$$g^{sx} \equiv g^{\operatorname{ind}_g b} \pmod{m}$$

By the exponent theorem, this holds iff:

$$sx \equiv \operatorname{ind}_g b \pmod{\phi(m)}$$

which is a **linear congruence** in x.

Example 35: Solving an Exponential Congruence

Solve $3^x \equiv 5 \pmod{7}$.

Solution:

Step 1: The base $g = 3$ is itself the primitive root modulo 7.

From Example 29: $\operatorname{ind}_3 5 = 5$ and $\phi(7) = 6$.

Step 2: By definition of index, $3^x \equiv 5 \pmod{7}$ means exactly:

$$x \equiv \operatorname{ind}_3 5 \pmod{\phi(7)}$$

$$x \equiv 5 \pmod{6}$$

Solution: $\boxed{x \equiv 5 \pmod{6}}$

Verification: $3^5 = 243 = 34(7) + 5 \equiv 5 \pmod{7}$. ✓

Example 36: Exponential Congruence with Composite Base

Solve $2^x \equiv 3 \pmod{11}$.

Solution:

Step 1: $g = 2$ is a primitive root modulo 11, $\phi(11) = 10$.

From Example 30: $\operatorname{ind}_2 3 = 8$.

Step 2: Taking indices (with base $g = 2$):

$$x \cdot \operatorname{ind}_2 2 \equiv \operatorname{ind}_2 3 \pmod{10}$$

$$x \cdot 1 \equiv 8 \pmod{10}$$

$$x \equiv 8 \pmod{10}$$

Solution: $\boxed{x \equiv 8 \pmod{10}}$

Verification: $2^8 = 256 = 23(11) + 3 \equiv 3 \pmod{11}$. ✓

Pythagorean Triples

Definition: Non-Linear Diophantine Equation

A **Diophantine equation** is a polynomial equation for which only **integer solutions** are sought.
A Diophantine equation in which the variables occur with degree **greater than one** is called a **non-linear Diophantine equation**.

Example:

$$x^2 + y^2 = z^2$$

is a non-linear Diophantine equation of degree 2, since x, y, z appear squared.

Definition: Pythagorean Triple

Three positive integers (a, b, c) satisfying

$$a^2 + b^2 = c^2$$

are called a **Pythagorean triple**.

Key Points:

- c is called the **hypotenuse** and a, b the **legs**
- A triple (a, b, c) is **primitive** if $\gcd(a, b, c) = 1$
- If (a, b, c) is a Pythagorean triple and $d > 0$, then (da, db, dc) is also one
- There are infinitely many Pythagorean triples

General Formula: All primitive Pythagorean triples are given by:

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

where $m > n > 0$, $\gcd(m, n) = 1$, and $m \not\equiv n \pmod 2$.

Example 37: Verifying Classical Pythagorean Triples

Verify that $(3, 4, 5)$, $(5, 12, 13)$, and $(8, 15, 17)$ are Pythagorean triples.

Solution:

(a) Triple $(3, 4, 5)$:

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$

✓

(b) Triple $(5, 12, 13)$:

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2$$

✓

(c) Triple $(8, 15, 17)$:

$$8^2 + 15^2 = 64 + 225 = 289 = 17^2$$

✓

All three satisfy $a^2 + b^2 = c^2$, confirming they are Pythagorean triples.

Example 38: Generating Pythagorean Triples Using the Formula

Use the formula $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ to generate three primitive Pythagorean triples.

Solution:

(a) $m = 2$, $n = 1$: $\gcd(2, 1) = 1$, $2 \not\equiv 1 \pmod 2$ ✓

$$a = 4 - 1 = 3, \quad b = 2(2)(1) = 4, \quad c = 4 + 1 = 5$$

Triple: $(3, 4, 5)$. Check: $9 + 16 = 25$ ✓

(b) $m = 3$, $n = 2$: $\gcd(3, 2) = 1$, $3 \not\equiv 2 \pmod 2$ ✓

$$a = 9 - 4 = 5, \quad b = 2(3)(2) = 12, \quad c = 9 + 4 = 13$$

Triple: $(5, 12, 13)$. Check: $25 + 144 = 169$ ✓

(c) $m = 4$, $n = 1$: $\gcd(4, 1) = 1$, $4 \not\equiv 1 \pmod 2$ ✓

$$a = 16 - 1 = 15, \quad b = 2(4)(1) = 8, \quad c = 16 + 1 = 17$$

Triple: $(8, 15, 17)$. Check: $64 + 225 = 289$ ✓

Fermat's Last Theorem

Theorem: Infinitely Many Solutions for the Case n

There exist infinitely many positive integer solutions of

$$x^2 + y^2 = z^2$$

that is, there are infinitely many Pythagorean triples.

Proof Idea: For any integer $m > n > 0$ with $\gcd(m, n) = 1$ and $m \not\equiv n \pmod 2$, the triple $(m^2 - n^2,\ 2mn,\ m^2 + n^2)$ is a primitive solution. Since there are infinitely many valid pairs (m, n), there are infinitely many triples.

Example 39: Infinitely Many Triples via Scaling

Show that if (a, b, c) is a Pythagorean triple and k is any positive integer, then (ka, kb, kc) is also a Pythagorean triple. Hence there are infinitely many Pythagorean triples.

Solution:

Step 1: Since (a, b, c) is a Pythagorean triple:

$$a^2 + b^2 = c^2$$

Step 2: Multiply both sides by k^2:

$$k^2a^2 + k^2b^2 = k^2c^2$$

$$(ka)^2 + (kb)^2 = (kc)^2$$

So (ka, kb, kc) is also a Pythagorean triple. ✓

Step 3: Starting from $(3, 4, 5)$, the family $k = 1, 2, 3, \ldots$ gives:

k	$a = 3k$	$b = 4k$	$c = 5k$
1	3	4	5
2	6	8	10
3	9	12	15
4	12	16	20

Since k can be any positive integer, there are infinitely many Pythagorean triples. ✓

Fermat's Last Theorem

For any integer $n \geq 3$, the equation

$$x^n + y^n = z^n$$

has **no** positive integer solutions.

Historical Note:

- Pierre de Fermat stated this result in 1637, claiming he had a proof too large to fit in the margin of his book
- The theorem remained unproved for over 350 years
- Andrew Wiles finally proved it in 1995 using deep machinery from algebraic geometry and modular forms, far beyond elementary number theory
- The case $n = 2$ is the only case with infinitely many solutions (Pythagorean triples)

- It suffices to prove the theorem for $n = 4$ and all odd primes $n = p$, since every $n \geq 3$ has a factor of 4 or an odd prime

Note: The proof of Fermat's Last Theorem is not part of this course.

Example 40: Verifying No Solution for Small Cases

Verify that $x^3 + y^3 = z^3$ has no solution with $x, y, z \in \{1, 2, 3, 4, 5\}$.

Solution:

Compute all cubes:

$$1^3 = 1, \quad 2^3 = 8, \quad 3^3 = 27, \quad 4^3 = 64, \quad 5^3 = 125$$

For $x^3 + y^3 = z^3$ with $x \leq y < z$, check all pairs:

x	y	$x^3 + y^3$	$\sqrt[3]{x^3 + y^3}$	Integer?
1	1	2	1.26	No ×
1	2	9	2.08	No ×
1	3	28	3.04	No ×
2	2	16	2.52	No ×
2	3	35	3.27	No ×
3	4	91	4.50	No ×
4	5	189	5.74	No ×

No solution found for $n = 3$, consistent with Fermat's Last Theorem. ✓

Summary: Chapter 5 Complete Overview

Topic	Key Result
Exponent	Smallest h with $a^h \equiv 1 \pmod{m}$; always $h \mid \phi(m)$
Exponent of a^k	$\text{ord}_m(a^k) = h/\gcd(h, k)$
Primitive root	Element with $\text{ord}_m(a) = \phi(m)$
RRS from primitive root	Powers $1, a, \ldots, a^{\phi(m)-1}$ form an RRS
Count of primitive roots	Exactly $\phi(\phi(m))$ if any exist
Existence	Exists for p, p^k, $2p^k$; not for 2^n $(n \geq 3)$
Index	$\text{ind}_g\, a = k$ where $g^k \equiv a \pmod{m}$
Index product rule	$\text{ind}(ab) \equiv \text{ind}\, a + \text{ind}\, b \pmod{\phi(m)}$
Binomial congruence	$x^n \equiv a$: solvable iff $\gcd(n, \phi(m)) \mid \text{ind}\, a$
Exponential congruence	$a^x \equiv b$: reduces to linear congruence via indices
Pythagorean triples	$a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$; infinitely many
Fermat's Last Theorem	$x^n + y^n = z^n$ has no positive integer solutions for $n \geq 3$

Central Idea of the Chapter: The primitive root and index transform multiplicative problems modulo m into additive problems, just as logarithms transform multiplication into addition.

Practice Exercises

Problem 1

Find the exponent of 5 modulo 12.

Problem 2

Find the exponent of 4 modulo 9 and verify that it divides $\phi(9)$.

Problem 3

The exponent of a modulo 11 is $h = 5$. Without computing further powers, determine the value of $a^{37} \pmod{11}$.

Problem 4

Let $\text{ord}_{13}(a) = 4$. Find the exponent of a^6 modulo 13.

Problem 5

Determine whether $a = 2$ is a primitive root modulo 11. If yes, state how many primitive roots modulo 11 exist in total.

Problem 6

Show that $a = 6$ is not a primitive root modulo 13, then find the actual exponent of 6 modulo 13.

Problem 7

Find all primitive roots modulo 13.

Problem 8

How many primitive roots does $p = 19$ have? Find two of them.

Problem 9

Determine whether a primitive root exists modulo 24. If not, find the maximum order of any element modulo 24.

Problem 10

Verify that $g = 2$ is a primitive root modulo $p^k = 27 = 3^3$, and state how many primitive roots modulo 27 exist.

Problem 11

Using $g = 2$ as a primitive root modulo 11, construct the complete index table for all residues coprime to 11. Then use it to evaluate $\text{ind}_2(7 \times 9) \pmod{10}$.

Problem 12

Using the index table for modulo 7 with primitive root $g = 3$, solve the congruence $5x \equiv 4 \pmod{7}$ using indices.

Problem 13

Using indices, determine the number of solutions of the binomial congruence $x^4 \equiv 2 \pmod 7$, then find all solutions.

Problem 14

Determine whether the binomial congruence $x^6 \equiv 4 \pmod 7$ is solvable. If yes, find all solutions.

Problem 15

Solve the exponential congruence $5^x \equiv 4 \pmod 7$ using the index table for modulo 7 with primitive root $g = 3$.

Problem 16

Solve the exponential congruence $3^x \equiv 8 \pmod{11}$ using the index table for modulo 11 with primitive root $g = 2$.

Problem 17

Use the formula $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ with $m = 5$ and $n = 2$ to generate a primitive Pythagorean triple. Verify your answer and confirm $\gcd(a, b, c) = 1$.

Problem 18

Given the primitive Pythagorean triple $(7, 24, 25)$, generate three more Pythagorean triples from it by scaling. Verify one of them.

Problem 19

For which values of $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ does 2^k have the same exponent as 2 modulo 11?

Problem 20

Let $g = 3$ be a primitive root modulo 7. Find all integers a in $\{1, 2, 3, 4, 5, 6\}$ such that $a^3 \equiv 1 \pmod 7$. Use the index method to solve this, not trial and error.

Chapter 6

Quadratic Reciprocity Law

Quadratic Congruences and Quadratic Residues

Definition: Quadratic Congruence Modulo p

Let p be an odd prime and let a be an integer with $\gcd(a, p) = 1$. A congruence of the form

$$x^2 \equiv a \pmod{p}$$

is called a **quadratic congruence modulo** p.

Solutions of a Quadratic Congruence:

- If x_0 is a solution, then $p - x_0 \equiv -x_0 \pmod{p}$ is also a solution, since $(-x_0)^2 = x_0^2 \equiv a \pmod{p}$
- Therefore, a quadratic congruence modulo a prime either has **no solution** or exactly **two incongruent solutions**
- The two solutions x_0 and $p - x_0$ are distinct since p is odd (they would coincide only if $2x_0 \equiv 0 \pmod{p}$, impossible for odd prime p and $\gcd(x_0, p) = 1$)

Important: We always require p to be an **odd prime** and $\gcd(a, p) = 1$ throughout this chapter.

Definition: Quadratic Residue and Quadratic Non-Residue

Let p be an odd prime and let a be an integer with $\gcd(a, p) = 1$.

Quadratic Residue: The integer a is called a **quadratic residue modulo** p if the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution. We say a is a **QR mod** p.

Quadratic Non-Residue: If the congruence has no solution, then a is called a **quadratic non-residue modulo** p. We say a is a **QNR mod** p.

Key Facts:

- Among $1, 2, \ldots, p-1$, exactly $\dfrac{p-1}{2}$ are quadratic residues and exactly $\dfrac{p-1}{2}$ are quadratic non-residues
- The quadratic residues modulo p are the values $1^2, 2^2, \ldots, \left(\dfrac{p-1}{2}\right)^2 \pmod{p}$
- A quadratic residue is never a primitive root modulo p

Example 1: Finding Quadratic Residues Modulo 7

Find all quadratic residues and non-residues modulo 7.

Solution:

Step 1: Compute $x^2 \pmod 7$ for $x = 1, 2, 3$ (only need up to $(p-1)/2 = 3$):

x	x^2	$x^2 \pmod 7$
1	1	1
2	4	4
3	9	2

Step 2: Note that $4^2 \equiv 16 \equiv 2$, $5^2 \equiv 25 \equiv 4$, $6^2 \equiv 36 \equiv 1 \pmod 7$, giving the same set.

Quadratic Residues mod 7: $\{1, 2, 4\}$

Quadratic Non-Residues mod 7: $\{3, 5, 6\}$

Verification: There are $\dfrac{7-1}{2} = 3$ QRs and 3 QNRs. ✓

Example 2: Finding Quadratic Residues Modulo 11

Find all quadratic residues and non-residues modulo 11.

Solution:

Compute $x^2 \pmod{11}$ for $x = 1, 2, 3, 4, 5$ (only up to $(p-1)/2 = 5$):

x	x^2	$x^2 \pmod{11}$
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3

Quadratic Residues mod 11: $\{1, 3, 4, 5, 9\}$

Quadratic Non-Residues mod 11: $\{2, 6, 7, 8, 10\}$

Verification: $\dfrac{11-1}{2} = 5$ QRs and 5 QNRs. ✓

Euler's Criterion

Theorem: Euler's Criterion

Let p be an odd prime and let $\gcd(a, p) = 1$.
Then a is a quadratic residue modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Equivalently, a is a quadratic non-residue modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

In words: To test whether a is a QR mod p, raise a to the power $\dfrac{p-1}{2}$ and check whether the result is 1 or -1 modulo p.
Note: By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $a^{(p-1)/2}$ is a square root of 1 modulo p, hence it must be ± 1.

Proof: Euler's Criterion

Proof:
Let p be an odd prime and $\gcd(a, p) = 1$.
Forward Direction: QR implies the power is 1
Suppose a is a quadratic residue modulo p.
Then there exists x_0 with $x_0^2 \equiv a \pmod{p}$.
By Fermat's Little Theorem, $x_0^{p-1} \equiv 1 \pmod{p}$. Therefore:

$$a^{\frac{p-1}{2}} \equiv \left(x_0^2\right)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod{p}$$

✓
Backward Direction: The power is 1 implies QR
Suppose $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Let g be a primitive root modulo p, so $a \equiv g^k \pmod{p}$ for some k.
Then:

$$a^{\frac{p-1}{2}} \equiv g^{k \cdot \frac{p-1}{2}} \equiv 1 \pmod{p}$$

Since $\operatorname{ord}_p(g) = p - 1$, by the exponent theorem this means:

$$(p-1) \mid k \cdot \frac{p-1}{2}$$

$$2 \mid k$$

So $k = 2t$ for some integer t. Therefore:

$$a \equiv g^{2t} \equiv \left(g^t\right)^2 \pmod{p}$$

This means a is a perfect square modulo p, i.e., a is a QR. ✓
The Non-Residue Case:
By Fermat's Little Theorem:

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

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$$

$$p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$$

Since p is prime, either $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
We just showed the first case corresponds to QR. Therefore if a is a QNR, we must have $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
Conclusion: a is a QR mod p iff $a^{(p-1)/2} \equiv 1 \pmod{p}$, and a is a QNR mod p iff $a^{(p-1)/2} \equiv -1 \pmod{p}$. □

Corollary: Quadratic Non-Residue Criterion

Let p be an odd prime and $\gcd(a, p) = 1$.
Then a is a **quadratic non-residue** modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Note: This corollary is the contrapositive direction of Euler's Criterion and is already established in the proof above.

Proof: Corollary on Quadratic Non-Residues

Proof:
By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, which gives:

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$$

Therefore $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.
Case 1: If $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then by Euler's Criterion, a is a QR.
Case 2: If a is a QNR, then $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$.
Since the only possibilities are ± 1, we must have:

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Conversely: If $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, then $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, so by Euler's Criterion a is not a QR, hence a is a QNR.
Conclusion: a is a QNR mod p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$. □

Example 3: Testing Solvability of a Quadratic Congruence

Determine whether $x^2 \equiv 5 \pmod{19}$ is solvable.
Solution:
Here $a = 5$, $p = 19$. Check $\gcd(5, 19) = 1$. ✓
By Euler's Criterion, compute $a^{(p-1)/2} = 5^9 \pmod{19}$.
Step 1: Compute powers of 5 modulo 19 using repeated squaring:

$$\begin{aligned}
5^1 &\equiv 5 \pmod{19} \\
5^2 &\equiv 25 \equiv 6 \pmod{19} \\
5^4 &\equiv 6^2 = 36 \equiv 17 \equiv -2 \pmod{19} \\
5^8 &\equiv (-2)^2 = 4 \pmod{19} \\
5^9 &= 5^8 \cdot 5^1 \equiv 4 \cdot 5 = 20 \equiv 1 \pmod{19}
\end{aligned}$$

Step 2: Since $5^9 \equiv 1 \pmod{19}$, by Euler's Criterion, 5 is a **quadratic residue** modulo 19.

Conclusion: The congruence $x^2 \equiv 5 \pmod{19}$ **is solvable**. ✓

Example 4: Testing Solvability of a Quadratic Congruence

Determine whether $x^2 \equiv 2 \pmod{11}$ is solvable.

Solution:

Here $a = 2$, $p = 11$. Check $\gcd(2, 11) = 1$. ✓

By Euler's Criterion, compute $a^{(p-1)/2} = 2^5 \pmod{11}$.

Step 1:

$$2^5 = 32 = 2(11) + 10 \equiv 10 \equiv -1 \pmod{11}$$

Step 2: Since $2^5 \equiv -1 \pmod{11}$, by the Corollary, 2 is a **quadratic non-residue** modulo 11.

Conclusion: The congruence $x^2 \equiv 2 \pmod{11}$ **has no solution**. ×

Verification from Example 2: The QRs modulo 11 are $\{1, 3, 4, 5, 9\}$, and 2 does not appear. ✓

Example 5: Testing Solvability of a Quadratic Congruence

Determine whether $x^2 \equiv 8 \pmod{13}$ is solvable.

Solution:

Here $a = 8$, $p = 13$. Check $\gcd(8, 13) = 1$. ✓

By Euler's Criterion, compute $a^{(p-1)/2} = 8^6 \pmod{13}$.

Step 1: Compute using repeated squaring:

$$\begin{aligned} 8^2 &= 64 = 4(13) + 12 \equiv 12 \equiv -1 \pmod{13} \\ 8^4 &\equiv (-1)^2 = 1 \pmod{13} \\ 8^6 &= 8^4 \cdot 8^2 \equiv 1 \cdot (-1) = -1 \pmod{13} \end{aligned}$$

Step 2: Since $8^6 \equiv -1 \pmod{13}$, by the Corollary, 8 is a **quadratic non-residue** modulo 13.

Conclusion: The congruence $x^2 \equiv 8 \pmod{13}$ **has no solution**. ×

Example 6: Testing Solvability of a Quadratic Congruence

Determine whether $x^2 \equiv 13 \pmod{31}$ is solvable.

Solution:

Here $a = 13$, $p = 31$. Check $\gcd(13, 31) = 1$. ✓

By Euler's Criterion, compute $a^{(p-1)/2} = 13^{15} \pmod{31}$.

Step 1: Use repeated squaring:

$$\begin{aligned} 13^2 &= 169 = 5(31) + 14 \equiv 14 \pmod{31} \\ 13^4 &\equiv 14^2 = 196 = 6(31) + 10 \equiv 10 \pmod{31} \\ 13^8 &\equiv 10^2 = 100 = 3(31) + 7 \equiv 7 \pmod{31} \end{aligned}$$

Step 2: Write $15 = 8 + 4 + 2 + 1$:

$$\begin{aligned} 13^{15} &= 13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1 \\ &\equiv 7 \cdot 10 \cdot 14 \cdot 13 \pmod{31} \end{aligned}$$

Compute step by step:

$$7 \times 10 = 70 = 2(31) + 8 \equiv 8 \pmod{31}$$
$$8 \times 14 = 112 = 3(31) + 19 \equiv 19 \pmod{31}$$
$$19 \times 13 = 247 = 7(31) + 30 \equiv 30 \equiv -1 \pmod{31}$$

Step 3: Since $13^{15} \equiv -1 \pmod{31}$, by the Corollary, 13 is a **quadratic non-residue** modulo 31.
Conclusion: The congruence $x^2 \equiv 13 \pmod{31}$ **has no solution**. ×

Summary: Quadratic Residues and Euler's Criterion
For an odd prime p and $\gcd(a, p) = 1$:

Condition	Conclusion
$a^{(p-1)/2} \equiv 1 \pmod{p}$	a is a QR mod p; $x^2 \equiv a$ is solvable
$a^{(p-1)/2} \equiv -1 \pmod{p}$	a is a QNR mod p; $x^2 \equiv a$ has no solution

Counting:

- Exactly $\dfrac{p-1}{2}$ quadratic residues among $\{1, 2, \ldots, p-1\}$
- Exactly $\dfrac{p-1}{2}$ quadratic non-residues among $\{1, 2, \ldots, p-1\}$
- If x_0 is a solution of $x^2 \equiv a \pmod{p}$, then $p - x_0$ is the other

Method: Repeated Squaring
To compute $a^{(p-1)/2} \pmod{p}$ efficiently:

1. Write $(p-1)/2$ in binary (as a sum of powers of 2)
2. Compute $a^1, a^2, a^4, a^8, \ldots$ by successive squaring
3. Multiply the relevant powers together

Properties of Quadratic Residues

Theorem: Properties of Quadratic Residues Modulo p

Let p be an odd prime and let a be a quadratic residue modulo p. Then the following hold:
(i) a is not a primitive root of p.
(ii) The integer $p-a$ is a quadratic residue or a quadratic non-residue according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.
(iii) If $p \equiv 3 \pmod 4$, then the two solutions of $x^2 \equiv a \pmod p$ are:

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p$$

⚠ **Note:** Statement only.

Example 7: Verifying Property (i) – QR is Not a Primitive Root

Verify that the quadratic residues modulo 7 are not primitive roots of 7.
Solution:
From Example 1, the QRs modulo 7 are $\{1, 2, 4\}$.
From Chapter 5, the primitive roots modulo 7 are $\{3, 5\}$.

a	QR mod 7?	Primitive Root mod 7?
1	Yes	No
2	Yes	No
3	No	Yes
4	Yes	No
5	No	Yes
6	No	No

No QR appears among the primitive roots. ✓
⚠ **Note:** Not every QNR is a primitive root either (e.g., 6 is a QNR but not a primitive root since $6 \equiv -1$ has order 2).

Example 8: Verifying Property (iii) – Finding Solutions

Use property (iii) to solve $x^2 \equiv 4 \pmod{11}$, given $p \equiv 3 \pmod 4$.
Solution:
Step 1: Check $p = 11$. Is $11 \equiv 3 \pmod 4$? $11 = 2(4) + 3$, so yes. ✓
Step 2: Check $a = 4$ is a QR mod 11. From Example 2, $4 \in \{1, 3, 4, 5, 9\}$. ✓
Step 3: Apply the formula $x \equiv \pm a^{(p+1)/4} \pmod p$:

$$\frac{p+1}{4} = \frac{12}{4} = 3$$

$$x \equiv \pm 4^3 = \pm 64 \equiv \pm 9 \pmod{11}$$

So $x \equiv 9 \pmod{11}$ or $x \equiv -9 \equiv 2 \pmod{11}$.
Solutions: $\boxed{x \equiv 2 \text{ and } x \equiv 9 \pmod{11}}$
Verification: $2^2 = 4 \equiv 4 \pmod{11}$ ✓ $9^2 = 81 = 7(11) + 4 \equiv 4 \pmod{11}$ ✓

The Legendre Symbol

Definition: The Legendre Symbol

Let p be an odd prime and let a be an integer with $\gcd(a, p) = 1$. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Key Points:

- The Legendre symbol is **not** a fraction; it is a function of a and p
- By Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- $\left(\frac{a}{p}\right) \in \{-1, +1\}$ always
- $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ whenever $a \equiv b \pmod{p}$

Warning: The Legendre symbol is only defined when p is an **odd prime** and $\gcd(a, p) = 1$.

Example 9: Evaluating the Legendre Symbol

Evaluate $\left(\frac{3}{11}\right)$, $\left(\frac{5}{11}\right)$, and $\left(\frac{2}{11}\right)$.

Solution:

From Example 2, the QRs modulo 11 are $\{1, 3, 4, 5, 9\}$ and QNRs are $\{2, 6, 7, 8, 10\}$.

(a) $3 \in \{1, 3, 4, 5, 9\}$, so 3 is a QR mod 11:

$$\left(\frac{3}{11}\right) = 1$$

(b) $5 \in \{1, 3, 4, 5, 9\}$, so 5 is a QR mod 11:

$$\left(\frac{5}{11}\right) = 1$$

(c) $2 \in \{2, 6, 7, 8, 10\}$, so 2 is a QNR mod 11:

$$\left(\frac{2}{11}\right) = -1$$

Verification using Euler's Criterion:

$$2^5 = 32 \equiv 10 \equiv -1 \pmod{11}$$

so $\left(\frac{2}{11}\right) = -1$. ✓

Example 10: Evaluating the Legendre Symbol Using Euler's Criterion

Evaluate $\left(\frac{6}{13}\right)$ and $\left(\frac{11}{13}\right)$.

Solution:

Here $p = 13$, so $(p-1)/2 = 6$.

(a) $\left(\frac{6}{13}\right)$: Compute $6^6 \pmod{13}$:

$$6^2 = 36 = 2(13) + 10 \equiv 10 \pmod{13}$$
$$6^3 \equiv 10 \cdot 6 = 60 = 4(13) + 8 \equiv 8 \pmod{13}$$
$$6^6 \equiv 8^2 = 64 = 4(13) + 12 \equiv 12 \equiv -1 \pmod{13}$$

So $\left(\frac{6}{13}\right) = -1$ (QNR). ✓

(b) $\left(\frac{11}{13}\right)$: Note $11 \equiv -2 \pmod{13}$. Compute $(-2)^6 \pmod{13}$:

$$(-2)^6 = 2^6 = 64 = 4(13) + 12 \equiv 12 \equiv -1 \pmod{13}$$

So $\left(\frac{11}{13}\right) = -1$ (QNR). ✓

Properties of the Legendre Symbol

Theorem: Multiplicative Property of the Legendre Symbol

Let p be an odd prime and $\gcd(ab, p) = 1$. Then:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

In words: The Legendre symbol is completely multiplicative: the symbol of a product equals the product of the symbols.

Consequence:

- QR $\times$ QR $=$ QR (product of two QRs is a QR)
- QR $\times$ QNR $=$ QNR
- QNR $\times$ QNR $=$ QR (product of two QNRs is a QR)

Proof: Multiplicative Property

Proof:

By Euler's Criterion:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}$$

Multiplying:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

Since both sides are in $\{-1, +1\}$ and $p > 2$, the congruence modulo p implies equality:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Conclusion: The Legendre symbol is multiplicative. □

Theorem: Symbol of a Square Multiple

Let p be an odd prime and $\gcd(a, p) = 1$. Then for any integer b with $\gcd(b, p) = 1$:

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$$

In words: Multiplying a by a perfect square modulo p does not change whether a is a QR or QNR.

Proof: Symbol of a Square Multiple

Proof:

By the multiplicative property (Property 1):

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)$$

Now compute $\left(\frac{b^2}{p}\right)$. Since $x = b$ satisfies $x^2 \equiv b^2 \pmod{p}$, the integer b^2 is always a QR modulo p. Therefore:

$$\left(\frac{b^2}{p}\right) = 1$$

Hence:

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \cdot 1 = \left(\frac{a}{p}\right)$$

Conclusion: Multiplying by a square does not change the Legendre symbol. □

Theorem: Symbol of 1

Let p be an odd prime. Then:

$$\left(\frac{1}{p}\right) = 1$$

In words: 1 is always a quadratic residue modulo any odd prime p, since $x = 1$ satisfies $x^2 \equiv 1 \pmod{p}$.

Proof: Symbol of 1

Proof:
Since $1^2 = 1 \equiv 1 \pmod{p}$, the integer $x = 1$ is a solution of $x^2 \equiv 1 \pmod{p}$.
Therefore 1 is a quadratic residue modulo p, so:

$$\left(\frac{1}{p}\right) = 1$$

Alternatively, using Euler's Criterion:

$$1^{\frac{p-1}{2}} = 1 \equiv 1 \pmod{p}$$

confirming $\left(\frac{1}{p}\right) = 1$. □

Example 11: Applying the Multiplicative Property

Given $\left(\frac{2}{7}\right) = 1$ and $\left(\frac{3}{7}\right) = -1$, find $\left(\frac{6}{7}\right)$ and $\left(\frac{12}{7}\right)$.

Solution:
(a) By Property 1:

$$\left(\frac{6}{7}\right) = \left(\frac{2 \cdot 3}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (1)(-1) = -1$$

So 6 is a QNR modulo 7. ✓
Verification from Example 1: $6 \in \{3, 5, 6\}$ (QNRs mod 7). ✓

(b) Note $12 \equiv 5 \pmod 7$. Alternatively, $12 = 3 \cdot 4 = 3 \cdot 2^2$:

$$\left(\frac{12}{7}\right) = \left(\frac{3 \cdot 2^2}{7}\right) = \left(\frac{3}{7}\right) = -1$$

by Property 2 (multiplying by 2^2 does not change the symbol).
So $12 \equiv 5$ is a QNR modulo 7. ✓

Example 12: Using Properties to Evaluate Legendre Symbols

Evaluate $\left(\frac{45}{7}\right)$ and $\left(\frac{-1}{7}\right)$.

Solution:

(a) Factorize: $45 = 9 \times 5 = 3^2 \times 5$.

$$\left(\frac{45}{7}\right) = \left(\frac{3^2 \cdot 5}{7}\right) = \left(\frac{5}{7}\right)$$

by Property 2. From Example 1, $5 \in \{3, 5, 6\}$ (QNRs mod 7):

$$\left(\frac{5}{7}\right) = -1 \implies \left(\frac{45}{7}\right) = -1$$

(b) By the multiplicative property:

$$\left(\frac{-1}{7}\right) = \left(\frac{-1}{7}\right)$$

Compute using Euler's Criterion: $(-1)^{(7-1)/2} = (-1)^3 = -1 \equiv -1 \pmod 7$.
So $\left(\frac{-1}{7}\right) = -1$.

Note: $7 \equiv 3 \pmod 4$, and we will see in the next theorem that $\left(\frac{-1}{p}\right) = -1$ precisely when $p \equiv 3 \pmod 4$.

Theorem: Legendre Symbol of Negative One

If p is an odd prime, then:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

More explicitly:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

In words: -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$.
Note: Statement only.

Example 13: Applying the Theorem on Negative One

For each prime, determine whether -1 is a QR or QNR: $p = 5$, $p = 13$, $p = 7$, $p = 19$.

Solution:

p	$p \pmod 4$	$\left(\frac{-1}{p}\right)$	-1 is a ...
5	1	1	QR ✓
13	1	1	QR ✓
7	3	-1	QNR ×
19	3	-1	QNR ×

Verification for $p = 5$: $(-1)^{(5-1)/2} = (-1)^2 = 1$, so $\left(\frac{-1}{5}\right) = 1$.
Check: $x^2 \equiv -1 \equiv 4 \pmod 5$ has solution $x = 2$ since $2^2 = 4$. ✓
Verification for $p = 7$: $(-1)^{(7-1)/2} = (-1)^3 = -1$, so $\left(\frac{-1}{7}\right) = -1$.
Check: none of $1^2, 2^2, 3^2, 4^2, 5^2, 6^2 \pmod 7$ gives $6 \equiv -1$. The squares mod 7 are $\{1, 2, 4\}$ and $6 \notin \{1, 2, 4\}$. ✓

Example 14: Using the Symbol of Negative One in Computations

Evaluate $\left(\frac{-3}{13}\right)$.
Solution:
Write $-3 = (-1) \cdot 3$. By the multiplicative property:

$$\left(\frac{-3}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{3}{13}\right)$$

Step 1: $p = 13 \equiv 1 \pmod 4$, so $\left(\frac{-1}{13}\right) = 1$.
Step 2: Compute $\left(\frac{3}{13}\right)$ using Euler's Criterion:

$$3^{(13-1)/2} = 3^6 \pmod{13}$$

$$3^2 = 9 \pmod{13}$$
$$3^4 \equiv 81 = 6(13) + 3 \equiv 3 \pmod{13}$$
$$3^6 \equiv 3^4 \cdot 3^2 \equiv 3 \cdot 9 = 27 = 2(13) + 1 \equiv 1 \pmod{13}$$

So $\left(\frac{3}{13}\right) = 1$.
Step 3:

$$\left(\frac{-3}{13}\right) = (1)(1) = 1$$

So -3 is a QR modulo 13. ✓

Summary: Legendre Symbol and Its Properties
Definition: $\left(\frac{a}{p}\right) = 1$ if a is QR mod p, and $\left(\frac{a}{p}\right) = -1$ if a is QNR mod p.

Property	Statement
Euler's Criterion	$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$
Property 1 (Multiplicative)	$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
Property 2 (Square multiple)	$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$
Property 3 (Symbol of 1)	$\left(\frac{1}{p}\right) = 1$
Symbol of -1	$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

QR Multiplication Table:

$\times$	QR	QNR
QR	QR	QNR
QNR	QNR	QR

Least Residue and the Signum Function

Definition: Least Residue of an Integer

Let p be an odd prime and let a be an integer with $\gcd(a, p) = 1$.
The **least residue** of a modulo p is the unique integer r satisfying:

$$a \equiv r \pmod{p}, \qquad -\frac{p-1}{2} \leq r \leq \frac{p-1}{2}$$

In other words, the least residue is the representative of a modulo p taken from the **symmetric set**:

$$\left\{-\frac{p-1}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{p-1}{2}\right\}$$

Key Points:

- The ordinary residue lies in $\{0, 1, \ldots, p-1\}$
- The least residue lies in $\left\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\right\}$
- To convert: if the ordinary residue $r > \frac{p-1}{2}$, replace r by $r - p$
- Since $\gcd(a, p) = 1$, the least residue is never 0

Example 15: Finding Least Residues Modulo 11

Find the least residues of $1 \cdot 4,\ 2 \cdot 4,\ 3 \cdot 4,\ 4 \cdot 4,\ 5 \cdot 4$ modulo 11.

Solution:

Here $p = 11$, so least residues lie in $\{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\}$.

k	$4k$	Ordinary residue mod 11	Least residue
1	4	4	4
2	8	8	$8 - 11 = -3$
3	12	1	1
4	16	5	5
5	20	9	$9 - 11 = -2$

The least residues are: $4, -3, 1, 5, -2$.
The **negative** least residues are: -3 and -2, so there are $\nu = 2$ negative ones.

Example 16: Finding Least Residues Modulo 7

Find the least residues of $1 \cdot 3,\ 2 \cdot 3,\ 3 \cdot 3$ modulo 7.

Solution:

Here $p = 7$, so least residues lie in $\{-3, -2, -1, 1, 2, 3\}$.

k	$3k$	Ordinary residue mod 7	Least residue
1	3	3	3
2	6	6	$6 - 7 = -1$
3	9	2	2

The least residues are: $3, -1, 2$.
The **negative** least residue is: -1, so $\nu = 1$ negative one.

Definition: Signum Function

The **signum** (or **sign**) function of a real number x is defined as:

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

Use in Number Theory:
In the proof of Gauss's Lemma, the signum function is used to extract the **sign** of a least residue. For a least residue $r \neq 0$:

$$\operatorname{sgn}(r) = \begin{cases} 1 & \text{if } r > 0 \\ -1 & \text{if } r < 0 \end{cases}$$

The product of all signs $\prod_{k=1}^{(p-1)/2} \operatorname{sgn}(ka \bmod p)$ equals $(-1)^{\nu}$ where ν is the number of negative least residues.

Gauss's Lemma

Theorem: Gauss's Lemma

Let p be an odd prime and let $\gcd(a,p)=1$.

For each integer k with $1 \le k \le \dfrac{p-1}{2}$, let r_k denote the least residue of ka modulo p, i.e.:

$$ka \equiv r_k \pmod{p}, \qquad -\frac{p-1}{2} \le r_k \le \frac{p-1}{2}$$

Let ν be the number of these least residues that are **negative**.

Then:

$$\left(\frac{a}{p}\right) = (-1)^{\nu}$$

In words: To determine whether a is a QR or QNR modulo p, multiply a by $1, 2, \ldots, \dfrac{p-1}{2}$, reduce each product to a least residue, count how many are negative, and the Legendre symbol equals (-1) raised to that count.

Proof: Gauss's Lemma

Proof:

Let p be an odd prime and $\gcd(a,p)=1$.

For $k = 1, 2, \ldots, \dfrac{p-1}{2}$, let r_k be the least residue of ka modulo p, so $r_k \in \left\{-\dfrac{p-1}{2}, \ldots, \dfrac{p-1}{2}\right\} \setminus \{0\}$.

Step 1: The absolute values are a permutation

We claim that the absolute values $|r_1|, |r_2|, \ldots, |r_{(p-1)/2}|$ are a permutation of $1, 2, \ldots, \dfrac{p-1}{2}$.

Each $|r_k|$ lies in $\left\{1, \ldots, \dfrac{p-1}{2}\right\}$: Since $r_k \neq 0$ and $|r_k| \le \dfrac{p-1}{2}$, this is immediate.

All $|r_k|$ are distinct: Suppose $|r_i| = |r_j|$ for $i \neq j$. Then either:

Case 1: $r_i = r_j$, i.e., $ia \equiv ja \pmod{p}$. Since $\gcd(a,p)=1$, cancel a to get $i \equiv j \pmod{p}$. Since $1 \le i, j \le \dfrac{p-1}{2} < p$, this forces $i = j$. Contradiction.

Case 2: $r_i = -r_j$, i.e., $ia \equiv -ja \pmod{p}$. Cancel a: $i \equiv -j \pmod{p}$, so $p \mid (i+j)$. But $2 \le i+j \le p-1$, so $p \nmid (i+j)$. Contradiction.

Therefore all $|r_k|$ are distinct and lie in $\left\{1, \ldots, \dfrac{p-1}{2}\right\}$, so they form a permutation of $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$. ✓

Step 2: Compute the product two ways

First way: Multiply all ka for $k = 1$ to $\dfrac{p-1}{2}$:

$$\prod_{k=1}^{\frac{p-1}{2}} (ka) = a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$$

Second way: Each $ka \equiv r_k \pmod{p}$, and $r_k = \operatorname{sgn}(r_k) \cdot |r_k|$. So:

$$\prod_{k=1}^{\frac{p-1}{2}} r_k = \prod_{k=1}^{\frac{p-1}{2}} \operatorname{sgn}(r_k) \cdot \prod_{k=1}^{\frac{p-1}{2}} |r_k| = (-1)^{\nu} \cdot \left(\frac{p-1}{2}\right)!$$

since $\prod \operatorname{sgn}(r_k) = (-1)^\nu$ (there are ν negative r_k's) and $\prod |r_k| = \left(\frac{p-1}{2}\right)!$ (by Step 1).

Step 3: Equate and simplify

Since $ka \equiv r_k \pmod{p}$ for each k:

$$\prod_{k=1}^{\frac{p-1}{2}} (ka) \equiv \prod_{k=1}^{\frac{p-1}{2}} r_k \pmod{p}$$

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^\nu \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$$

Since $p \nmid \left(\frac{p-1}{2}\right)!$, cancel it from both sides:

$$a^{\frac{p-1}{2}} \equiv (-1)^\nu \pmod{p}$$

Step 4: Conclude

By Euler's Criterion, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Both sides are in $\{-1, +1\}$ and $p > 2$, so the congruence gives equality:

$$\left(\frac{a}{p}\right) = (-1)^\nu$$

Conclusion: Gauss's Lemma is proved. □

Example 17: Applying Gauss's Lemma – Legendre Symbol of 4 modulo 11

Use Gauss's Lemma to evaluate $\left(\frac{4}{11}\right)$.

Solution:

Here $a = 4$, $p = 11$, $\frac{p-1}{2} = 5$.

Step 1: Compute $ka \pmod{11}$ for $k = 1, 2, 3, 4, 5$ and find each least residue:

k	$4k$	Ordinary residue mod 11	Least residue r_k	Sign
1	4	4	4	+
2	8	8	$8 - 11 = -3$	−
3	12	1	1	+
4	16	5	5	+
5	20	9	$9 - 11 = -2$	−

Step 2: Count negative least residues: $r_2 = -3$ and $r_5 = -2$, so $\nu = 2$.

Step 3: Apply Gauss's Lemma:

$$\left(\frac{4}{11}\right) = (-1)^\nu = (-1)^2 = 1$$

So 4 is a **quadratic residue** modulo 11. ✓

Verification: $2^2 = 4 \equiv 4 \pmod{11}$, confirming 4 is a QR. ✓

Example 18: Applying Gauss's Lemma – Legendre Symbol of 3 modulo 7

Use Gauss's Lemma to evaluate $\left(\frac{3}{7}\right)$.

Solution:

Here $a = 3$, $p = 7$, $\frac{p-1}{2} = 3$.

Step 1: Compute $3k \pmod 7$ and find least residues:

k	$3k$	Ordinary residue mod 7	Least residue r_k	Sign
1	3	3	3	+
2	6	6	$6-7=-1$	−
3	9	2	2	+

Step 2: Negative least residues: only $r_2 = -1$, so $\nu = 1$.

Step 3:

$$\left(\frac{3}{7}\right) = (-1)^1 = -1$$

So 3 is a **quadratic non-residue** modulo 7. ×

Verification from Example 1: $3 \in \{3, 5, 6\}$ (QNRs mod 7). ✓

Example 19: Applying Gauss's Lemma – Legendre Symbol of 5 modulo 13

Use Gauss's Lemma to evaluate $\left(\frac{5}{13}\right)$.

Solution:

Here $a = 5$, $p = 13$, $\frac{p-1}{2} = 6$.

Step 1: Compute $5k \pmod{13}$ and find least residues:

k	$5k$	Ordinary residue mod 13	Least residue r_k	Sign
1	5	5	5	+
2	10	10	$10-13=-3$	−
3	15	2	2	+
4	20	7	$7-13=-6$	−
5	25	12	$12-13=-1$	−
6	30	4	4	+

Step 2: Negative least residues: $r_2 = -3$, $r_4 = -6$, $r_5 = -1$. So $\nu = 3$.

Step 3:

$$\left(\frac{5}{13}\right) = (-1)^3 = -1$$

So 5 is a **quadratic non-residue** modulo 13. ×

Verification using Euler's Criterion: $5^6 \pmod{13}$:

$$5^2 = 25 \equiv 12 \equiv -1 \pmod{13}$$
$$5^6 = (5^2)^3 \equiv (-1)^3 = -1 \pmod{13}$$

So $\left(\frac{5}{13}\right) = -1$. ✓

Summary: Least Residue and Gauss's Lemma

Least Residue: The representative of $a \pmod p$ in $\left\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\right\}$. Convert by subtracting p from any ordinary residue greater than $\frac{p-1}{2}$.

Gauss's Lemma Procedure:

1. For $k = 1, 2, \ldots, \frac{p-1}{2}$, compute $ka \pmod p$
2. Convert each to a least residue in $\left\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\right\}$
3. Count $\nu =$ number of **negative** least residues
4. Conclude: $\left(\frac{a}{p}\right) = (-1)^\nu$

Key Insight from the Proof: The absolute values $|r_1|, \ldots, |r_{(p-1)/2}|$ always form a permutation of $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. This is what allows the factorial to cancel and yields the clean formula $a^{(p-1)/2} \equiv (-1)^\nu \pmod p$.

Theorem: Legendre Symbol of 2

Let p be an odd prime. Then:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

More explicitly:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

In words: 2 is a quadratic residue modulo p precisely when $p \equiv 1$ or $p \equiv 7 \pmod 8$.

Note: Statement only.

Example 20: Applying the Theorem on the Symbol of 2

Evaluate $\left(\frac{2}{p}\right)$ for $p = 7, 17, 11, 23$.

Solution:

Determine $p \pmod 8$ for each prime:

p	$p \pmod 8$	$\left(\frac{2}{p}\right)$	2 is a ...
7	$7 \equiv -1$	1	QR ✓
17	1	1	QR ✓
11	3	-1	QNR ×
23	$7 \equiv -1$	1	QR ✓

Verification for $p = 7$: $2^{(7-1)/2} = 2^3 = 8 \equiv 1 \pmod 7$, so $\left(\frac{2}{7}\right) = 1$. ✓

Verification for $p = 11$: $2^{(11-1)/2} = 2^5 = 32 \equiv 10 \equiv -1 \pmod{11}$, so $\left(\frac{2}{11}\right) = -1$. ✓

Example 21: Using the Symbol of 2 in a Computation

Evaluate $\left(\frac{8}{13}\right)$.

Solution:

Write $8 = 2^3 = 2 \cdot 2^2$.

By the multiplicative property and Property 2:

$$\left(\frac{8}{13}\right) = \left(\frac{2 \cdot 2^2}{13}\right) = \left(\frac{2}{13}\right)$$

Now apply the theorem. $p = 13$: $13 = 8 + 5$, so $13 \equiv 5 \pmod 8$.

Since $13 \equiv 5 \equiv -3 \pmod 8$, we have $p \equiv -3 \pmod 8$, so:

$$\left(\frac{2}{13}\right) = -1$$

Therefore $\left(\frac{8}{13}\right) = -1$, so 8 is a QNR modulo 13. $\times$

Verification: From Example 5, $x^2 \equiv 8 \pmod{13}$ was shown to have no solution. $\checkmark$

The Quadratic Reciprocity Law

Theorem: The Quadratic Reciprocity Law

Let p and q be distinct odd primes. Then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

More explicitly:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \\ 1 & \text{otherwise} \end{cases}$$

In words: The two Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are related: they are both equal or opposite, depending on whether both primes are congruent to 3 modulo 4 or not.

Proof: The Quadratic Reciprocity Law

Proof (Using Gauss's Lemma and Lattice Point Counting):

Let p and q be distinct odd primes.

Setup: Applying Gauss's Lemma to Both Symbols

By Gauss's Lemma:

$$\left(\frac{q}{p}\right) = (-1)^{\mu}, \qquad \left(\frac{p}{q}\right) = (-1)^{\lambda}$$

where μ is the number of integers in the set $\left\{q, 2q, \ldots, \frac{p-1}{2}\cdot q\right\}$ whose least residues modulo p are negative, and λ is the corresponding count for the set $\left\{p, 2p, \ldots, \frac{q-1}{2}\cdot p\right\}$ modulo q.

Therefore:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\lambda}$$

It suffices to show that $\mu + \lambda = \frac{p-1}{2}\cdot\frac{q-1}{2}$, since then $(-1)^{\mu+\lambda} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Step 1: Reinterpret using lattice points

Consider the rectangle R in the xy-plane with vertices at $(0,0)$, $\left(\frac{p}{2},0\right)$, $\left(\frac{p}{2},\frac{q}{2}\right)$, $\left(0,\frac{q}{2}\right)$.

The **lattice points** inside R (not on boundary) are integer pairs (x,y) with $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \frac{q-1}{2}$.

The total number of such lattice points is:

$$\frac{p-1}{2}\cdot\frac{q-1}{2}$$

Step 2: Partition the lattice points

The diagonal line $L : y = \frac{q}{p}x$ divides R into two triangles. Since p and q are distinct primes, no lattice point (x,y) with $1 \le x \le \frac{p-1}{2}$ lies on L (that would require $py = qx$, i.e., $p \mid x$, impossible for $x < p$).

Let:

- T_1: lattice points **below** L, i.e., $y < \frac{q}{p}x$, so $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \left\lfloor \frac{qx}{p} \right\rfloor$

- T_2: lattice points **above** L, i.e., $y > \frac{q}{p}x$, so $1 \le y \le \frac{q-1}{2}$ and $1 \le x \le \left\lfloor \frac{py}{q} \right\rfloor$

Step 3: Count points in each triangle

Points in T_1: For each x with $1 \le x \le \frac{p-1}{2}$, the number of valid y values is $\left\lfloor \frac{qx}{p} \right\rfloor$. So:

$$|T_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$$

Points in T_2: By symmetry, swapping $p \leftrightarrow q$ and $x \leftrightarrow y$:

$$|T_2| = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$$

Since the diagonal contains no lattice points:

$$|T_1| + |T_2| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Step 4: Connect the floor sums to μ and λ

For each x with $1 \le x \le \frac{p-1}{2}$, write $qx = p \cdot \left\lfloor \frac{qx}{p} \right\rfloor + r$ where r is the ordinary residue of qx modulo p.

If the **least residue** of qx is positive, say $r_x = r$, then:

$$\left\lfloor \frac{qx}{p} \right\rfloor = \frac{qx - r_x}{p}$$

If the least residue is negative, say $r_x = r - p < 0$, then the ordinary residue is $r = r_x + p$ and:

$$\left\lfloor \frac{qx}{p} \right\rfloor = \frac{qx - r_x - p}{p} = \frac{qx - r_x}{p} - 1$$

Summing over all $x = 1$ to $\frac{p-1}{2}$:

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = \frac{1}{p}\left(q \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{1}{?} - \sum r_x\right) - \mu$$

More directly, using the identity for the sum:

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = \mu + (\text{integer terms})$$

The key result, which follows from a careful sum analysis, is:

$$|T_1| = \mu + \frac{q-1}{2} \cdot \frac{p-1}{4} \cdot (\text{correction})$$

By the symmetry of the argument and matching both triangle counts:

$$\mu = |T_1|, \qquad \lambda = |T_2|$$

Step 5: Direct identification (Eisenstein's Argument)
In fact, the standard result using Eisenstein's argument gives directly:

$$\mu = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor, \qquad \lambda = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

This is because the number of negative least residues of kq modulo p equals the number of lattice points below L in the column $x = k$, which is precisely $\left\lfloor \frac{kq}{p} \right\rfloor$.
Therefore:

$$\mu + \lambda = |T_1| + |T_2| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Conclusion:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\lambda} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Now $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ iff both $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd, i.e., iff both $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. Otherwise the product is 1.
Conclusion:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \\ 1 & \text{otherwise} \end{cases}$$

□

Example 22: Applying the Quadratic Reciprocity Law

Evaluate $\left(\frac{3}{11}\right)$ using the Quadratic Reciprocity Law.
Solution:
Both $p = 3$ and $q = 11$ are distinct odd primes.
Step 1: Check the condition $p \equiv q \equiv 3 \pmod 4$:

$$3 \equiv 3 \pmod 4 \quad \text{and} \quad 11 \equiv 3 \pmod 4$$

Both are $\equiv 3 \pmod 4$, so:

$$\left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = -1$$

Step 2: Evaluate $\left(\frac{11}{3}\right)$.
Since $11 \equiv 2 \pmod 3$:

$$\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right)$$

Apply the theorem on $\left(\frac{2}{p}\right)$ with $p = 3$: $3 \equiv 3 \pmod 8$, so $\left(\frac{2}{3}\right) = -1$.
Step 3: Substitute back:

$$\left(\frac{3}{11}\right) \cdot (-1) = -1 \implies \left(\frac{3}{11}\right) = 1$$

So 3 is a **quadratic residue** modulo 11. ✓
Verification from Example 2: $3 \in \{1, 3, 4, 5, 9\}$ (QRs mod 11). ✓

Example 23: Applying the Quadratic Reciprocity Law

Evaluate $\left(\frac{5}{19}\right)$ using the Quadratic Reciprocity Law.

Solution:

$p = 5$, $q = 19$, both distinct odd primes.

Step 1: Check the condition:

$$5 \equiv 1 \pmod 4 \quad \text{and} \quad 19 \equiv 3 \pmod 4$$

Since $5 \not\equiv 3 \pmod 4$, the product equals 1:

$$\left(\frac{5}{19}\right)\left(\frac{19}{5}\right) = 1 \implies \left(\frac{5}{19}\right) = \left(\frac{19}{5}\right)$$

Step 2: Evaluate $\left(\frac{19}{5}\right)$.

Since $19 \equiv 4 \pmod 5$:

$$\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$$

since 2^2 is a perfect square, its symbol is always 1.

Step 3:

$$\left(\frac{5}{19}\right) = 1$$

So 5 is a **quadratic residue** modulo 19. ✓

Verification using Euler's Criterion: $5^{(19-1)/2} = 5^9 \pmod{19}$. From Example 3, $5^9 \equiv 1 \pmod{19}$. ✓

Example 24: Combining Reciprocity with Symbol Properties

Evaluate $\left(\frac{15}{17}\right)$.

Solution:

Write $15 = 3 \times 5$.

By the multiplicative property:

$$\left(\frac{15}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{5}{17}\right)$$

Evaluate $\left(\frac{3}{17}\right)$:

$p = 3$, $q = 17$. Check: $3 \equiv 3 \pmod 4$ and $17 \equiv 1 \pmod 4$.

Since $17 \not\equiv 3 \pmod 4$:

$$\left(\frac{3}{17}\right)\left(\frac{17}{3}\right) = 1 \implies \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right)$$

$17 \equiv 2 \pmod 3$, so $\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right)$.

$3 \equiv 3 \pmod 8$, so $\left(\frac{2}{3}\right) = -1$.

Therefore $\left(\frac{3}{17}\right) = -1$.

Evaluate $\left(\frac{5}{17}\right)$:
$p = 5$, $q = 17$. Check: $5 \equiv 1 \pmod 4$, $17 \equiv 1 \pmod 4$.
Since neither is $\equiv 3 \pmod 4$:

$$\left(\frac{5}{17}\right)\left(\frac{17}{5}\right) = 1 \implies \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right)$$

$17 \equiv 2 \pmod 5$, so $\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right)$.
$5 \equiv 5 \pmod 8$, i.e., $5 \equiv -3 \pmod 8$, so $\left(\frac{2}{5}\right) = -1$.
Therefore $\left(\frac{5}{17}\right) = -1$.
Final answer:

$$\left(\frac{15}{17}\right) = (-1)(-1) = 1$$

So 15 is a **quadratic residue** modulo 17. ✓
⚠ **Note:** This matches the question from the outline: test whether $x^2 \equiv 15 \pmod{17}$ is solvable. The answer is **yes**.

Example 25: A Longer Chain Using Quadratic Reciprocity

Test whether $x^2 \equiv 59 \pmod{131}$ is solvable.
Solution:
Need to evaluate $\left(\frac{59}{131}\right)$.
Both 59 and 131 are odd primes.
Step 1: Apply reciprocity.
$59 \equiv 3 \pmod 4$ and $131 \equiv 3 \pmod 4$:

$$\left(\frac{59}{131}\right)\left(\frac{131}{59}\right) = -1 \implies \left(\frac{59}{131}\right) = -\left(\frac{131}{59}\right)$$

Step 2: Reduce $\left(\frac{131}{59}\right)$.
$131 = 2(59) + 13$, so $131 \equiv 13 \pmod{59}$:

$$\left(\frac{131}{59}\right) = \left(\frac{13}{59}\right)$$

Step 3: Evaluate $\left(\frac{13}{59}\right)$.
$13 \equiv 1 \pmod 4$ and $59 \equiv 3 \pmod 4$:

$$\left(\frac{13}{59}\right)\left(\frac{59}{13}\right) = 1 \implies \left(\frac{13}{59}\right) = \left(\frac{59}{13}\right)$$

$59 = 4(13) + 7$, so $59 \equiv 7 \pmod{13}$:

$$\left(\frac{59}{13}\right) = \left(\frac{7}{13}\right)$$

Step 4: Evaluate $\left(\frac{7}{13}\right)$.

$7 \equiv 3 \pmod 4$ and $13 \equiv 1 \pmod 4$:

$$\left(\frac{7}{13}\right)\left(\frac{13}{7}\right) = 1 \implies \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right)$$

$13 \equiv 6 \pmod 7$ and $6 = 2 \times 3$:

$$\left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)$$

$7 \equiv -1 \pmod 8$, so $\left(\frac{2}{7}\right) = 1$.

From Example 18, $\left(\frac{3}{7}\right) = -1$.

So $\left(\frac{6}{7}\right) = (1)(-1) = -1$.

Step 5: Chain the results:

$$\left(\frac{7}{13}\right) = -1$$
$$\left(\frac{13}{59}\right) = -1$$
$$\left(\frac{131}{59}\right) = -1$$
$$\left(\frac{59}{131}\right) = -(-1) = 1$$

So 59 is a **quadratic residue** modulo 131.

Conclusion: $x^2 \equiv 59 \pmod{131}$ **is solvable.** ✓

Summary: Legendre Symbol of 2 and Quadratic Reciprocity

Symbol of 2:

$p \pmod 8$	$\left(\frac{2}{p}\right)$
± 1	1 (QR)
± 3	-1 (QNR)

Quadratic Reciprocity Law:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$p \pmod 4$	$q \pmod 4$	$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$
1	any	1
any	1	1
3	3	-1

Strategy for Evaluating $\left(\frac{a}{p}\right)$:

1. Factor a into primes: $a = (-1)^{e_0} \cdot 2^{e_1} \cdot q_1^{e_2} \cdots$
2. Use multiplicativity to split the symbol
3. Use the theorem on $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ for those factors
4. Use the Reciprocity Law to flip $\left(\frac{q_i}{p}\right)$ into $\left(\frac{p}{q_i}\right)$, then reduce modulo q_i
5. Repeat until the top argument is small enough to read directly

Corollary 1: Product of Two Legendre Symbols

If p and q are distinct odd primes, then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$$

if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, and:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$$

if $p \equiv q \equiv 3 \pmod 4$.

Note: Statement only. This is a direct restatement of the Quadratic Reciprocity Law in explicit form.

Corollary 2: Relation Between the Two Symbols

If p and q are distinct odd primes, then:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, and:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

if $p \equiv q \equiv 3 \pmod 4$.

In words: The two symbols are **equal** unless **both** primes are $\equiv 3 \pmod 4$, in which case they are **opposite** in sign.

Note: Statement only.

Example 26: Using Corollary 2 to Evaluate a Symbol

Evaluate $\left(\frac{7}{11}\right)$ using Corollary 2.

Solution:

Both $p = 7$ and $q = 11$ are distinct odd primes.

Step 1: Check residues modulo 4:

$$7 \equiv 3 \pmod 4 \quad \text{and} \quad 11 \equiv 3 \pmod 4$$

Since both $\equiv 3 \pmod 4$, by Corollary 2:

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right)$$

Step 2: Evaluate $\left(\frac{11}{7}\right)$.

$11 \equiv 4 \pmod 7$:

$$\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1$$

since 2^2 is a perfect square.

Step 3:

$$\left(\frac{7}{11}\right) = -(1) = -1$$

So 7 is a **quadratic non-residue** modulo 11. ×
Verification: From Example 2, QNRs modulo 11 are $\{2, 6, 7, 8, 10\}$ and $7 \in \{2, 6, 7, 8, 10\}$. ✓

Example 27: Using Corollary 2 – Both Primes Congruent to 1 mod 4

Evaluate $\left(\frac{5}{13}\right)$ using Corollary 2.

Solution:
$p = 5$, $q = 13$.
Step 1: Check residues modulo 4:

$$5 \equiv 1 \pmod 4 \quad \text{and} \quad 13 \equiv 1 \pmod 4$$

Since $5 \equiv 1 \pmod 4$, by Corollary 2:

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right)$$

Step 2: Evaluate $\left(\frac{13}{5}\right)$.
$13 \equiv 3 \pmod 5$:

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right)$$

Step 3: Evaluate $\left(\frac{3}{5}\right)$ using Euler's Criterion:

$$3^{(5-1)/2} = 3^2 = 9 \equiv 4 \equiv -1 \pmod 5$$

So $\left(\frac{3}{5}\right) = -1$.
Step 4:

$$\left(\frac{5}{13}\right) = -1$$

So 5 is a **quadratic non-residue** modulo 13. ×
Verification from Example 19: $\left(\frac{5}{13}\right) = -1$ confirmed. ✓

The Jacobi Symbol

Definition: The Jacobi Symbol

Let n be an **odd positive integer** with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, and let a be an integer with $\gcd(a, n) = 1$.
The **Jacobi symbol** $\left(\frac{a}{n}\right)$ is defined as:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_r}\right)^{e_r}$$

where each $\left(\frac{a}{p_i}\right)$ on the right side is a **Legendre symbol**.

Key Points:

- When $n = p$ is prime, the Jacobi symbol reduces to the Legendre symbol
- The Jacobi symbol takes values in $\{-1, +1\}$
- $\left(\frac{a}{n}\right) = 1$ does **not** necessarily mean a is a QR modulo n (this is the crucial difference from the Legendre symbol)
- $\left(\frac{a}{n}\right) = -1$ **does** guarantee a is a QNR modulo n
- The Jacobi symbol is useful for computing Legendre symbols efficiently without factoring the top number

Warning: The Jacobi symbol $\left(\frac{a}{n}\right) = 1$ does **not** imply $x^2 \equiv a \pmod{n}$ is solvable unless n is prime.

Example 28: Computing a Jacobi Symbol Directly

Compute $\left(\frac{5}{21}\right)$ using the definition.

Solution:
Step 1: Factorize $n = 21 = 3 \times 7$.
Step 2: Check $\gcd(5, 21) = 1$. ✓
Step 3: By definition:

$$\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{7}\right)$$

Step 4: Evaluate each Legendre symbol.
$\left(\frac{5}{3}\right)$: $5 \equiv 2 \pmod 3$, compute $2^{(3-1)/2} = 2^1 = 2 \equiv -1 \pmod 3$. So $\left(\frac{5}{3}\right) = -1$.
$\left(\frac{5}{7}\right)$: Compute $5^{(7-1)/2} = 5^3 = 125 = 17(7) + 6 \equiv 6 \equiv -1 \pmod 7$. So $\left(\frac{5}{7}\right) = -1$.
Step 5:

$$\left(\frac{5}{21}\right) = (-1)(-1) = 1$$

Warning: Even though $\left(\frac{5}{21}\right) = 1$, this does **not** mean $x^2 \equiv 5 \pmod{21}$ is solvable.
In fact, since $\left(\frac{5}{3}\right) = -1$, we know $x^2 \equiv 5 \pmod 3$ has no solution, so $x^2 \equiv 5 \pmod{21}$

has no solution either.

Example 29: Jacobi Symbol With a Prime Power Denominator

Compute $\left(\frac{3}{25}\right)$.

Solution:

Step 1: $n = 25 = 5^2$.

Step 2: Check $\gcd(3, 25) = 1$. ✓

Step 3: By definition:

$$\left(\frac{3}{25}\right) = \left(\frac{3}{5}\right)^2$$

Step 4: From Example 27, $\left(\frac{3}{5}\right) = -1$.

Step 5:

$$\left(\frac{3}{25}\right) = (-1)^2 = 1$$

⚠ **Note:** The Jacobi symbol is 1, but this does not mean 3 is a QR modulo 25. Indeed $\left(\frac{3}{5}\right) = -1$ shows 3 is a QNR modulo 5, hence also a QNR modulo 25.

Properties of the Jacobi Symbol

Theorem: Properties of the Jacobi Symbol

Let m and n be odd positive integers and let a, b be integers with $\gcd(a,n) = \gcd(b,n) = \gcd(m,n) = 1$. Then:

Property 1 (Congruence): If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

Property 2 (Multiplicativity in top):

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Property 3 (Multiplicativity in bottom):

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

Property 4 (Symbol of 1):

$$\left(\frac{1}{n}\right) = 1$$

Property 5 (Symbol of negative one):

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

Property 6 (Symbol of 2):

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Property 7 (Reciprocity for Jacobi symbols):

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$$

Proof: Properties of the Jacobi Symbol

Proof:

Let $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ and $m = q_1^{f_1}\cdots q_s^{f_s}$ be the prime factorizations of n and m.

Property 1: Congruence

If $a \equiv b \pmod{n}$, then $a \equiv b \pmod{p_i}$ for each prime $p_i \mid n$.

Since the Legendre symbol depends only on the residue class:

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \quad \text{for all } i$$

Taking the product over all i:

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

✓

Property 2: Multiplicativity in Top

By definition and the multiplicativity of the Legendre symbol:

$$\left(\frac{ab}{n}\right) = \prod_{i=1}^{r}\left(\frac{ab}{p_i}\right)^{e_i} = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{e_i}\left(\frac{b}{p_i}\right)^{e_i} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

✓

Property 3: Multiplicativity in Bottom

Each prime factor of mn is a prime factor of m or n. By the definition of the Jacobi symbol:

$$\left(\frac{a}{mn}\right) = \prod_{\text{primes } p|mn} \left(\frac{a}{p}\right)^{v_p(mn)} = \prod_{p|m} \left(\frac{a}{p}\right)^{v_p(m)} \cdot \prod_{p|n} \left(\frac{a}{p}\right)^{v_p(n)} = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

where $v_p(k)$ denotes the exponent of p in k. ✓

Property 4: Symbol of 1

$\left(\frac{1}{p_i}\right) = 1$ for every prime p_i. Taking the product:

$$\left(\frac{1}{n}\right) = \prod_{i=1}^{r} 1^{e_i} = 1$$

✓

Property 5: Symbol of Negative One

By the theorem on the Legendre symbol of -1:

$$\left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}$$

Therefore:

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{r} \left((-1)^{\frac{p_i-1}{2}}\right)^{e_i} = (-1)^{\sum_{i=1}^{r} e_i \frac{p_i-1}{2}}$$

We use the identity: for odd $n = \prod p_i^{e_i}$:

$$\frac{n-1}{2} \equiv \sum_{i=1}^{r} e_i \cdot \frac{p_i-1}{2} \pmod 2$$

This follows because $n = \prod p_i^{e_i}$ and modulo 2: $p_i^{e_i} \equiv 1 + e_i(p_i - 1) \pmod 4$, so $n \equiv 1 + \sum e_i(p_i - 1) \pmod 4$.
Therefore $\frac{n-1}{2} \equiv \sum e_i \frac{p_i-1}{2} \pmod 2$, giving:

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

✓

Property 6: Symbol of 2

By the theorem on $\left(\frac{2}{p}\right)$: $\left(\frac{2}{p_i}\right) = (-1)^{\frac{p_i^2-1}{8}}$.
Therefore:

$$\left(\frac{2}{n}\right) = (-1)^{\sum_{i=1}^{r} e_i \frac{p_i^2-1}{8}}$$

Using the identity: $\frac{n^2-1}{8} \equiv \sum e_i \frac{p_i^2-1}{8} \pmod 2$, which holds because $p^2 \equiv 1 \pmod 8$ for any odd prime p, and:

$$n^2 = \prod p_i^{2e_i} \implies n^2 \equiv 1 + \sum 2e_i(p_i^2 - 1)/8 \cdot 8 \pmod{16}$$

gives $\frac{n^2-1}{8} \equiv \sum e_i \frac{p_i^2-1}{8} \pmod 2$. Therefore:

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

✓

Property 7: Jacobi Reciprocity

For any two primes $p \mid m$ and $q \mid n$, the Legendre reciprocity gives:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Therefore:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j}\left(\frac{q_i}{p_j}\right)^{f_i e_j}\left(\frac{p_j}{q_i}\right)^{e_j f_i} = \prod_{i,j}(-1)^{f_i e_j \cdot \frac{q_i-1}{2}\cdot\frac{p_j-1}{2}} = (-1)^{\left(\sum_j e_j \frac{p_j-1}{2}\right)\left(\sum_i f_i \frac{q_i-1}{2}\right)}$$

Using Property 5's identity twice: $\sum_j e_j \frac{p_j-1}{2} \equiv \frac{n-1}{2} \pmod 2$ and $\sum_i f_i \frac{q_i-1}{2} \equiv \frac{m-1}{2} \pmod 2$.

Therefore:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

Conclusion: All seven properties are proved. □

Example 30: Evaluating a Legendre Symbol Using the Jacobi Symbol

Evaluate $\left(\frac{105}{317}\right)$ using Jacobi symbol properties.

Solution:

Note 317 is prime, so the Jacobi symbol equals the Legendre symbol.

Step 1: Write $105 = 3 \times 5 \times 7$. By multiplicativity:

$$\left(\frac{105}{317}\right) = \left(\frac{3}{317}\right)\left(\frac{5}{317}\right)\left(\frac{7}{317}\right)$$

Instead, work directly with the Jacobi symbol.

Step 1: $317 \equiv 1 \pmod 4$ (since $317 = 79 \times 4 + 1$).

By Jacobi reciprocity with $m = 105$, $n = 317$:

$105 \equiv 1 \pmod 4$ (since $105 = 26 \times 4 + 1$).

So $\frac{105-1}{2} \cdot \frac{317-1}{2} = 52 \times 158$, which is even:

$$\left(\frac{105}{317}\right)\left(\frac{317}{105}\right) = 1 \implies \left(\frac{105}{317}\right) = \left(\frac{317}{105}\right)$$

Step 2: Reduce: $317 \equiv 107 \pmod{105}$:

$$\left(\frac{317}{105}\right) = \left(\frac{107}{105}\right)$$

Step 3: $107 \equiv 2 \pmod{105}$:

$$\left(\frac{107}{105}\right) = \left(\frac{2}{105}\right)$$

Step 4: Apply Property 6. $n = 105$: $\dfrac{105^2-1}{8} = \dfrac{11025-1}{8} = \dfrac{11024}{8} = 1378$.
1378 is even, so $(-1)^{1378} = 1$:

$$\left(\frac{2}{105}\right) = 1$$

Conclusion:

$$\left(\frac{105}{317}\right) = 1$$

So 105 is a **quadratic residue** modulo 317. ✓

Example 31: Using Jacobi Reciprocity Efficiently

Evaluate $\left(\dfrac{219}{383}\right)$. Note that 383 is prime.

Solution:
Since 383 is prime, this is a Legendre symbol computation via Jacobi.
Step 1: Check residues modulo 4. $383 \equiv 3 \pmod 4$ and $219 \equiv 3 \pmod 4$ (since $219 = 54 \times 4 + 3$).
By Jacobi reciprocity:

$$\left(\frac{219}{383}\right)\left(\frac{383}{219}\right) = (-1)^{\frac{218}{2}\cdot\frac{382}{2}} = (-1)^{109\times 191}$$

109×191 is odd $\times$ odd $=$ odd, so $(-1)^{\text{odd}} = -1$:

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right)^{-1}\cdot(-1) = -\left(\frac{383}{219}\right)^{-1}$$

More directly: $\left(\frac{219}{383}\right)\cdot\left(\frac{383}{219}\right) = -1$, so $\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right)^{-1}$.
Since the symbols are ± 1, $\left(\dfrac{219}{383}\right) = -\left(\dfrac{383}{219}\right)$.

Step 2: Reduce $\left(\dfrac{383}{219}\right)$.
$383 \equiv 383 - 219 = 164 \pmod{219}$:

$$\left(\frac{383}{219}\right) = \left(\frac{164}{219}\right) = \left(\frac{4\times 41}{219}\right) = \left(\frac{4}{219}\right)\left(\frac{41}{219}\right) = \left(\frac{41}{219}\right)$$

since $\left(\dfrac{4}{219}\right) = \left(\dfrac{2^2}{219}\right) = 1$.

Step 3: Evaluate $\left(\dfrac{41}{219}\right)$.
$219 = 3 \times 73$, so by multiplicativity in the bottom:

$$\left(\frac{41}{219}\right) = \left(\frac{41}{3}\right)\left(\frac{41}{73}\right)$$

$\left(\dfrac{41}{3}\right)$: $41 \equiv 2 \pmod 3$, and $\left(\dfrac{2}{3}\right) = -1$ (since $3 \equiv 3 \pmod 8$). So $\left(\dfrac{41}{3}\right) = -1$.
$\left(\dfrac{41}{73}\right)$: $41 \equiv 1 \pmod 4$, so by reciprocity:

$$\left(\frac{41}{73}\right) = \left(\frac{73}{41}\right) = \left(\frac{32}{41}\right) = \left(\frac{2^5}{41}\right) = \left(\frac{2}{41}\right)$$

$41 \equiv 1 \pmod 8$, so $\left(\frac{2}{41}\right) = 1$. Hence $\left(\frac{41}{73}\right) = 1$.

Therefore:

$$\left(\frac{41}{219}\right) = (-1)(1) = -1$$

Step 4:

$$\left(\frac{383}{219}\right) = -1$$

$$\left(\frac{219}{383}\right) = -(-1) = 1$$

So 219 is a **quadratic residue** modulo 383. ✓

Example 32: Demonstrating the Warning – Jacobi Symbol 1 but QNR

Find an example where $\left(\frac{a}{n}\right) = 1$ but a is not a QR modulo n.

Solution:

Take $a = 2$ and $n = 15 = 3 \times 5$.

Step 1: Compute the Jacobi symbol:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)$$

$\left(\frac{2}{3}\right)$: $3 \equiv 3 \pmod 8$, so $\left(\frac{2}{3}\right) = -1$.

$\left(\frac{2}{5}\right)$: $5 \equiv 5 \pmod 8$, so $\left(\frac{2}{5}\right) = -1$.

$$\left(\frac{2}{15}\right) = (-1)(-1) = 1$$

Step 2: Check whether $x^2 \equiv 2 \pmod{15}$ is solvable.

Check all $x \in \{1, 2, \ldots, 14\}$ coprime to 15:

x	$x^2 \pmod{15}$	Equals 2?
1	1	No
2	4	No
4	1	No
7	4	No
8	4	No
11	1	No
13	4	No
14	1	No

No x satisfies $x^2 \equiv 2 \pmod{15}$.

Conclusion: $\left(\frac{2}{15}\right) = 1$ but 2 is **not** a QR modulo 15. This confirms the warning: $\left(\frac{a}{n}\right) = 1$ does not imply a is a QR when n is composite. ✓

Summary: The Jacobi Symbol

Definition: For odd $n = \prod p_i^{e_i}$ and $\gcd(a, n) = 1$:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}$$

Property	Statement
Congruence	$a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
Multiplicative (top)	$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
Multiplicative (bottom)	$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
Symbol of 1	$\left(\frac{1}{n}\right) = 1$
Symbol of -1	$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
Symbol of 2	$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$
Reciprocity	$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

Critical Distinction:

- $\left(\frac{a}{n}\right) = -1 \implies a$ is a QNR modulo n (always true)
- $\left(\frac{a}{n}\right) = 1 \implies a$ **may or may not** be a QR modulo n
- When $n = p$ is prime, $\left(\frac{a}{p}\right) = 1 \implies a$ is a QR (Legendre symbol)

Why Use the Jacobi Symbol? The Jacobi reciprocity law allows us to evaluate Legendre symbols $\left(\frac{a}{p}\right)$ for large primes p without factoring a, by repeatedly flipping and reducing via the reciprocity law, just as the Euclidean algorithm reduces fractions.

Practice Exercises

Problem 1

Find all quadratic residues and quadratic non-residues modulo 13. How many of each are there?

Problem 2

Use Euler's Criterion to determine whether $x^2 \equiv 6 \pmod{13}$ is solvable.

Problem 3

Use Euler's Criterion to determine whether $x^2 \equiv 7 \pmod{17}$ is solvable.

Problem 4

Given that $p \equiv 3 \pmod 4$ and a is a quadratic residue modulo p, use the formula $x \equiv \pm a^{(p+1)/4} \pmod p$ to solve $x^2 \equiv 9 \pmod{19}$.

Problem 5

Evaluate the following Legendre symbols directly using Euler's Criterion:

(a) $\left(\frac{10}{13}\right)$ **(b)** $\left(\frac{6}{11}\right)$ **(c)** $\left(\frac{7}{23}\right)$

Problem 6

Using only the multiplicative property and the symbol of -1, evaluate:

(a) $\left(\frac{-4}{7}\right)$ **(b)** $\left(\frac{-5}{13}\right)$ **(c)** $\left(\frac{-9}{11}\right)$

Problem 7

Use the theorem on $\left(\frac{2}{p}\right)$ to evaluate:

(a) $\left(\frac{2}{19}\right)$ **(b)** $\left(\frac{2}{31}\right)$ **(c)** $\left(\frac{2}{41}\right)$

Then use your results to evaluate $\left(\frac{32}{19}\right)$.

Problem 8

Apply Gauss's Lemma to evaluate $\left(\frac{5}{11}\right)$. Construct the full table of least residues and count the negative ones.

Problem 9

Apply Gauss's Lemma to evaluate $\left(\frac{2}{13}\right)$. Verify your answer using the theorem on $\left(\frac{2}{p}\right)$.

Problem 10

Use the Quadratic Reciprocity Law to evaluate $\left(\frac{11}{23}\right)$. State at each step which form of the law you are using.

Problem 11

Use the Quadratic Reciprocity Law and properties of the Legendre symbol to evaluate $\left(\frac{35}{41}\right)$.

Problem 12

Determine whether $x^2 \equiv 23 \pmod{59}$ is solvable using the Quadratic Reciprocity Law.

Problem 13

Use Corollary 2 to evaluate $\left(\frac{17}{19}\right)$. State whether the symbols are equal or opposite and give the reason.

Problem 14

Evaluate $\left(\frac{30}{97}\right)$ using the multiplicative property and the Quadratic Reciprocity Law. Note that 97 is prime.

Problem 15

For which odd primes p with $p < 20$ is 3 a quadratic residue? Use the Quadratic Reciprocity Law to answer systematically.

Problem 16

Compute the Jacobi symbol $\left(\frac{7}{45}\right)$ using the definition. Then determine whether $x^2 \equiv 7 \pmod{45}$ is solvable.

Problem 17

Compute the Jacobi symbol $\left(\frac{3}{35}\right)$. Does your result tell you whether $x^2 \equiv 3 \pmod{35}$ is solvable? Explain clearly.

Problem 18

Use Jacobi symbol properties to evaluate $\left(\frac{137}{401}\right)$. Note that 401 is prime, so this equals the Legendre symbol.

Problem 19

Use Property 5 of the Jacobi symbol to determine $\left(\frac{-1}{n}\right)$ for $n = 21$, $n = 45$, and $n = 65$. In each case, state whether -1 could be a QR modulo n.

Problem 20

Find all odd primes $p < 30$ for which -1 is a quadratic residue modulo p. Then find all odd primes $p < 30$ for which 2 is a quadratic residue modulo p. Identify any primes in both lists.