Introduction to Number Theory and Algorithms

Christian J. Rudder

August 2024

Contents

This page is left intentionally blank.

— 1 —

Congruences

1.1 Equivalence Relations

Definition 1.1: Equivalence Relation

An **equivalence relation** on set S is a relation $\sim$ which satisfies:

1. **Reflexivity:** For all $a \in S$, $a \sim a$.
2. **Symmetry:** For all $a, b \in S$, if $a \sim b$, then $b \sim a$.
3. **Transitivity:** For all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

With $a \sim a$ reading, "a is related to a."

Definition 1.2: Equivalence Class

For $\sim$ equivalence relation on set S. For each $a \in S$, the **equivalence class** of a is the set

$$[a] = \{x \in S \mid x \sim a\}.$$

Note: For $x \in [a]$, x is a **representative** of the equivalence class $[a]$ (**??**).

Theorem 1.1: Equivalence Class Uniqueness

For $\sim$ equivalence relation on set S, for all $a, b \in S$:

(i) $a \in [a]$.

(ii) $a \in [b] \implies [a] = [b]$.

Proof 1.1: Equivalence Class Uniqueness

For $a, b \in S$:

(i) Since $\sim$ is reflexive, $a \sim a$.

(ii) Suppose $a \in [b]$. Then $a \sim b$. Then for $x \in S$,

$$\begin{aligned} x \in [a] &\implies x \sim a \text{ (Definition of } [a] \text{ (1.2))} \\ &\implies x \sim b \text{ (Transitivity, } x \sim a \wedge a \sim b) \\ &\implies x \in [b] \text{ (Definition of } [b] \text{ (1.2))} \end{aligned}$$

Thus $[a] \subseteq [b]$. Similarly, $[b] \subseteq [a]$. Therefore $[a] = [b]$.

■

1.2 Modular Congruences

Continuing with the notion of residues in, we introduce the concept of modular congruences (**??**).

Definition 2.1: Modular Congruence

For $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, a is **congruent** to b modulo n if $n \mid (a - b)$, denoted as

$$a \equiv b \pmod{n}.$$

If $n \nmid (a - b)$, then $a \not\equiv b \pmod{n}$.

I.e., a and b have the same remainder when divided by n.

Note: $a \equiv b \pmod{n}$: **a** and **b** are **dividends** of **n** our **divisor**, which relate by **remainder**.

Theorem 2.1: Modular Congruence Properties

For all $a, b, c \in \mathbb{Z}$, and some positive integer n:

(i) $a \equiv a \pmod{n}$;

(ii) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$;

(iii) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

Proof 2.1: Modular Congruence Properties

For all $a, b, c \in \mathbb{Z}$, and some positive integer n:

(i) $a \equiv a \pmod{n}$ so $n \mid (a - a)$, which holds.

(ii) $a \equiv b \pmod{n}$ so n divides $(a - b)$ and $-(a - b) = (b - a)$, then $b \equiv a \pmod{n}$.

(iii) $a \equiv b \pmod{n}$ so $n \mid (a - b)$, and $b \equiv c \pmod{n}$ is $n \mid (b - c)$. Therefore,

$$\begin{aligned} & n \mid (a-b) \quad \text{and} \quad n \mid (b-c) \\ \implies & n \mid [(a-b)+(b-c)] \\ \implies & n \mid (a-c) \\ \implies & a \equiv c \pmod{n}. \end{aligned}$$

■

Theorem 2.2: Modular Arithmetic

Let $a, a', b, b', n \in \mathbb{Z}$ with $n > 0$. If

$$a \equiv a' \pmod{n} \quad \text{and} \quad b \equiv b' \pmod{n},$$

then

$$a + b \equiv a' + b' \pmod{n} \quad \text{and} \quad a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Proof 2.2: Modular Arithmatic

Addition: For $a, a', b, b', n \in \mathbb{Z}$,

- So $a \equiv a' \pmod{n}$ then $n \mid (a - a')$ means $a - a' = nx$ for some $x \in \mathbb{Z}$.
- Similarly, $b \equiv b' \pmod{n}$ then $b - b' = ny$ for some $y \in \mathbb{Z}$.
- Adding both equations, $(a - a') + (b - b') = (nx + ny)$ so $(a + b) - (a + b') = n(x + y)$.
- Therefore, $a + b \equiv a' + b' \pmod{n}$, as $n \mid (a + b) - (a' + b')$.

Multiplication: Continuing,

- If we multiply both equations, $(a - a')(b - b') = (nx)(ny)$ so $(ab) - (a'b') = n(xy)$.
- Therefore, $ab \equiv a'b' \pmod{n}$, as $n \mid (ab) - (a'b')$.

■

Theorem 2.3: Least Residue

Let $a, n \in \mathbb{Z}$ with $n > 0$. There exists unique $z \in \mathbb{Z}$ such that:

(i) $0 \leq z < n$,

(ii) $a \equiv z \pmod{n}$.

(iii) z is the **least residue** of a modulo n.

Particularly, for all $x \in \mathbb{Z}$, $z \in [x, x + n)$.

I.e., the least non-negative remainder r, which could be thought of as $r := a \bmod n$.

Note: The period $[x, x + n)$, contains possible remainders, a call back to the Division Alg. (**??**).

Proof 2.3: Least Residue

For some $a, q, n, r \in \mathbb{Z}$,
The Division Algorithm grantees existence, for $a = qn + r : 0 \leq r < n$ (**??**). Residues mod $n > 0$ are non-empty. Thus by the Well-Ordering Principle, there's a least element. ■

Example: Working to find the **set of solutions z** for $a \equiv z \pmod{n}$, i.e., find z that satisfies,

$$\begin{aligned} 3z + 4 &\equiv 6 \pmod{7} \text{ (Given)} \\ 3z &\equiv 2 \pmod{7} \text{ (Subtracting 4 from both sides)} \end{aligned}$$

We can't necessarily divide, but we can shift residue by some favorable factor.

$$\begin{aligned} 3z \cdot 5 &\equiv 2 \cdot 5 \pmod{7} \text{ (Multiply 5 to both sides)} \\ 1 \cdot z &\equiv 10 \pmod{7} \text{ (Since } 15 \equiv 1 \pmod{7}\text{)} \end{aligned}$$

Finding solution $z \equiv 10 \pmod{7}$, which we can reduce to $z \equiv 3 \pmod{7}$, as $3 \equiv 10 \pmod{7}$.
We say "integers z has solutions" as $z \in [3]_7 = \{3 + 7k : k \in \mathbb{Z}\}$ possible solutions.

Note: $[3]_7$ reads as *"the residue class 3 modulo 7."* Mentioned in (1.2).

1.3 Solving Linear Congruences

Theorem 3.1: Modular Multiplicative Identities

Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$.

(i) For every $b \in \mathbb{Z}$, the congruence $az \equiv b \pmod{n}$ has a solution $z \in \mathbb{Z}$ if and only if $d \mid b$.

(ii) For every $z \in \mathbb{Z}$, we have $az \equiv 0 \pmod{n}$ if and only if $z \equiv 0 \pmod{n/d}$.

(iii) For all $z, z' \in \mathbb{Z}$, we have $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n/d}$.

Proof 3.1: Linear Congruence Identities

Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$.

(i)

$$\begin{aligned}
& az \equiv b \pmod{n} \quad \text{for some } z \in \mathbb{Z} \\
\iff & az - b = ny \quad \text{for some } z, y \in \mathbb{Z} \quad \text{(Def. of congruence (2.1))} \\
\iff & az - ny = b \quad \text{for some } z, y \in \mathbb{Z} \\
\iff & d \mid b \quad \text{(By Bezout's Identity (??)).}
\end{aligned}$$

(ii) Above is Bezout's Identity as a and n form a linear combination of b.-

$$\begin{aligned}
n \mid az \iff & n/d \mid (a/d)z \text{ (Props. of Divisibility (??))} \\
\iff & n/d \mid z. \text{ (Cancellation of GCD: } \gcd(a/d, n/d) = 1 \text{ (??))}
\end{aligned}$$

(iii)

$$\begin{aligned}
& az \equiv az' \pmod{n} \\
\iff & a(z - z') \equiv 0 \pmod{n} \\
\iff & z - z' \equiv 0 \pmod{n/d} \quad \text{(By Part (ii))} \\
\iff & z \equiv z' \pmod{n/d}.
\end{aligned}$$

■

For emphasis, as we saw above:

Definition 3.1: GCD Reduction

For $a, n \in \mathbb{Z}$, $d := \gcd(a, n)$, then $\gcd(a/d, n/d) = 1$.

Note: "→" (Maps to), "↦" (Defines the action of how a single element maps to another), "image" (the set of all outputs), and "pre-images" (the set of all inputs).

A corollary to the above theorem (3.1):

Theorem 3.2: Modular Multiplicative Map

Let $a, n \in \mathbb{Z}$ with $n > 0$, and residue classes $I_n := \{0, \dots, n-1\}$. Then $(a \mod n) \in I_n$. Notably, for $z \in \mathbb{Z}$, $(az \mod n)$ is also in I_n.

I.e., $(az \mod n)$ is some re-ordering of the residue class $(a \mod n)$. Defining function, τ_a:

$$\tau_a : I_n \to I_n : z \mapsto az \bmod n. \tag{3.2.1}$$

The length of the image of τ_a is the number of distinct factors of n relative to a, i.e., n/d. Let the image of τ_a be:

$$E := \{az \mod n : z \in I_n\} = \{i \cdot d \mod n : i = 0, \dots, n/d - 1\}. \tag{3.2.2}$$

The length of the pre-images of τ_a is the number of z solutions to $az \equiv b \pmod n$, i.e., d. Let the pre-images of τ_a be:

$$P := \{z \in I_n : az \equiv b \pmod n\}. \tag{3.2.3}$$

It follows that τ_a is a bijection (one-to-one and onto) if and only if $\gcd(a, n) = 1$. Then, the length of the image is n, and each pre-image has length 1.

Example: for $a = 1, 2, 3, 4, 5, 6$ and $n = 15$,

z	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2z \mod 15$	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
$3z \mod 15$	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
$4z \mod 15$	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
$5z \mod 15$	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
$6z \mod 15$	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9

- **Row:2** We see 2 and 15 are coprime, hence n images, $\{0, \dots, n-1\}$.
- **Row:3** We see 3 and 15. Taking out common factors, 15/3, we get 5 distinct images.
- **Row:4** We see 4 and 15 are coprime, hence n images, $\{0, \dots, n-1\}$.
- **Row:5** We see 5 and 15. Taking out common factors, 15/5, we get 3 distinct images.
- **Row:6** We see 6 and 15. Taking out common factors, 15/3, we get 5 distinct images.

Another corollary to the above theorem (3.1):

Theorem 3.3: Modular Congruence Cancellation

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(c, n) = 1$. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Example: We'll demonstrate different representations of members residue class $[2]_5$:

$$\begin{aligned} 8 &\equiv 13 \pmod{5} && \text{(i)} \\ 2 \cdot 4 &\equiv 3 \cdot 5 \pmod{5} && \text{(ii)} \\ 2 \cdot 4 &\equiv (-3) \cdot 4 \pmod{5} && \text{(iii)} \\ 2 &\equiv -3 \pmod{5} && \text{(iv)} \end{aligned}$$

Indeed $2 \equiv -3 \pmod{5}$, as $2 + 3 \equiv 3 - 3 \pmod{5}$. To show this, observe:

a	0	1	2	3	4	5	6	7	8	9	10	11	12
$a \mod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2
	0	-4	-3	-2	-1	0	-4	-3	-2	-1	0	-4	-3

Think of **negative numbers** as traveling backwards within the residue class.

Definition 3.2: Modular Iverses

Let $a, n \in \mathbb{Z}$ with $n > 0$. If $az \equiv 1 \pmod{n}$, then z is the **modular inverse** of a **modulo** n and unique.

Denoted: $a^{-1} \pmod{n}$.

If inverse z modulo n exists, it is unique, as if there were another inverse z', then $z' \equiv z \pmod{n}$.

Restating (3.1) under coprime conditions:

Theorem 3.4: Coprime Modular Multiplicative Identities

Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $\gcd(a, n) = 1$.

(i) The congruence $az \equiv 1 \pmod{n}$ has a solution $z \in \mathbb{Z}$, the modular inverse.

(ii) If $az \equiv 0 \pmod{n}$, then $z \equiv 0 \pmod{n}$ (i.e., z must be a multiple of n).

(iii) If $az \equiv az' \pmod{n}$, then $z \equiv z' \pmod{n}$ (i.e., a cancels out, as long as $\gcd(a, n) = 1$).

Try to find inverses from the above table. Take an a and find solution z to $az \equiv 1 \pmod{5}$.

The Chinese Remainder Theorem

Note: $\mathbb{Z}^+$ denotes the set of positive integers, and $\{x_i\}_{i=1}^k$ is short for $\{x_1, ..., x_k\}$.

Theorem 3.5: Chinese Remainder Theorem (CRT)

Let $\{n_i\}_{i=1}^k \in \mathbb{Z}^+$ all be coprime to each other and let $\{a_i\}_{i=1}^k$ be arbitrary integers. Then there is a solution $a \in \mathbb{Z}$ to the system of congruences:

$$\begin{aligned} a &\equiv a_1 \pmod{n_1} \\ a &\equiv a_2 \pmod{n_2} \\ &\vdots \\ a &\equiv a_k \pmod{n_k} \end{aligned}$$

Moreover, if a and b are solutions to the system, then $a \equiv b \pmod{\prod_{i=1}^k n_i}$.

Proof 3.2: Solving a System of Congruences (Part 1)

Let $\{n_i\}_{i=1}^k \in \mathbb{Z}^+$ all be pairwise coprime, and let $\{a_i\}_{i=1}^k$ be arbitrary integers,

Existence: (i) Construct a partial solution for each congruence. (ii) Each partial solution must not interfere with other congruences. (iii) Combine partial solutions:

We define indexes $i, j = 1, ..., k$ representing any two $e_1, ..., e_k$ integers such that:

$$e_j \equiv \begin{cases} 1 \pmod{n_i} & \text{if } j = i, \text{ (target congruence)} \\ 0 \pmod{n_i} & \text{if } j \neq i \text{ (non-interfering).} \end{cases}$$

I.e., e_j has multiplicative identity to it's own system, and additive identity to all other systems by being some multiple. This allows us to construct:

$$\begin{aligned} e_1 \cdot a_1 &\equiv 1 \cdot a_1 \pmod{n_1} \\ e_2 \cdot a_2 &\equiv 1 \cdot a_2 \pmod{n_2} \\ &\vdots \\ e_k \cdot a_k &\equiv 1 \cdot a_k \pmod{n_k} \end{aligned}$$

Using additive identity, we close partial-solutions to $a = \sum_{i=1}^k e_i a_i$, the whole solution. ■

Proof 3.3: Solving a System of Congruences (Part 2)

To construct such $e_1, ..., e_k$, let $n := \prod_{i=1}^{k} n_i$ (the product of all moduli) and $n_i^* := n/n_i$. Then, n_i and n_i^* are coprime, meaning they have solution $n_i^* z \equiv 1 \pmod{n_i}$ for some $z \in \mathbb{Z}$.

Then $z = (n_i^*)^{-1}$, we can now define $e_i := n_i^* z$ for each $i = 1, ..., k$. Therefore, $e_i \equiv 1 \pmod{n_i}$. Since n contains shared factors, and we take n_i at congruence i, $e_i \equiv 0 \pmod{n_j}$ for $i \neq j$.

Thus, we can now construct the solution $a = \sum_{i=1}^{k} e_i a_i$.

■

Proof 3.4: Uniqueness of Solutions (Part 3)

If a and a' both satisfy the system of congruences

$$a \equiv a_i \pmod{n_i} \quad \text{and} \quad a' \equiv a_i \pmod{n_i} \quad \text{for } i = 1, \ldots, k$$

Then they must be congruent, i.e., $a \equiv a' \pmod{\prod_{i=1}^{k} n_i}$.

■

Note: **Uniqueness refers to $\mathbb{Z}_\mathbf{n}$** (residue classes modulo n), not just a. So there may be multiple solutions, but they congruent to each other under a unique modulus n

Example: We'll find solution a to the system of congruences:

$$\begin{aligned} a &\equiv 3 \pmod{5} \\ a &\equiv 5 \pmod{7} \\ a &\equiv 2 \pmod{11} \end{aligned}$$

Observe that $(3 \bmod 5) = \{3, 8, 13, 18, 23, 28, 33, ...\}$, and $(5 \bmod 7) = \{5, 12, 19, 26, 33, ...\}$. Sets describing $3 + 5k$ and $5 + 7k$ respectively. We see, $3 \equiv 33 \pmod{5}$, and $5 \equiv 33 \pmod{7}$.

Obtaining $e_1 = 7$, as $3 + 5(7) \implies 3(7) \equiv 1 \pmod{5}$, and $5 + 7(7) \implies 5(7) \equiv 0 \pmod{7}$.
We can take $n = 5 \cdot 7 = 35$ to construct a new system:

$$\begin{aligned} a &\equiv 33 \pmod{35} = 33 + 35k = \{33, 68, ...\} \\ a &\equiv 2 \pmod{11} = 2 + 11k = \{2, 13, 24, 35, 46, 57, 68, ...\} \end{aligned}$$

We see that $33 \equiv 68 \pmod{35}$, and $2 \equiv 68 \pmod{11}$. Thus, $a = 68$:

$$\begin{aligned} 68 &\equiv 3 \pmod{5} \\ 68 &\equiv 5 \pmod{7} \\ 68 &\equiv 2 \pmod{11} \end{aligned}$$

We can design a general algorithm based off this example to solve such systems.

Chinese Remainder Theorem Algorithm

Function 3.1: CRT Algorithm - `crt()`

Computes $a \in \mathbb{Z}$ satisfying a given system of congruences:

Input: Positive integers $\{n_i\}_{i=1}^k$ and integers $\{a_i\}_{i=1}^k$
Output: An integer a satisfying the system of congruences

Function $crt(\{n_i\}_{i=1}^k, \{a_i\}_{i=1}^k)$**:**

```
    a ← a_1;
    N ← n_1;
    for i ← 2 to k do
        while a mod n_i ≠ a_i do
            a ← a + N;
        end
        N ← N × n_i;
    end
return a
```

We compute just like the example above:

1. First take a_1 and n_1 as our initial solution and modulus.
2. Then iterate starting with a_2 and n_2 to find solution $a \bmod (n_i) = a_i$.
3. If a is not congruent to a_i, we increment a by N until it is.
4. Then update N to the new product, and move to the next congruence.

1.4 Residue Classes

We've spoken before about residue classes in (**??**), but we'll go into more detail here.

Theorem 4.1: Residue Intervals

Remainders modular $n \in \mathbb{Z} : n > 1$, denoted $\mathbb{Z}_n$, is the interval $[0, (n-1)]$. As we pass $n-1$, we loop back to 0. Yielding a general interval of $[x, x+(n-1)]$ for $x \in \mathbb{Z}$.

Adding and multiplying residues shifts to some other position in the interval.

- **Addition:** $[(a+b) \bmod n] := [a] + [b] = [a+b] = [c] \iff a+b \equiv c \pmod n$
- **Multiplication:** $[(a \cdot b) \bmod n] := [a] \cdot [b] = [a \cdot b] = [c] \iff a \cdot b \equiv c \pmod n$

If n is odd, then our interval is $[-(n-1)/2, (n-1)/2]$. If even, then $[-n/2, n/2-1]$.

Example: Consider tables $\mathbb{Z}_5$ and $\mathbb{Z}_6$:

a	0	1	2	3	4	5	6	7	8	9	10	11	12
$a \mod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2
	0	-4	-3	-2	-1	0	-4	-3	-2	-1	0	-4	-3

Since 5 is odd, our interval is $[-(4)/2, (4)/2] = [-2, 2]$, which could be seen as the interval $a \in [3, 7]$.

a	0	1	2	3	4	5	6	7	8	9	10	11	12
$a \mod 6$	0	1	2	3	4	5	0	1	2	3	4	5	0
	0	-5	-4	-3	-2	-1	0	-5	-4	-3	-2	-1	0

Since 6 is even, our interval is $[-6/2, 6/2-1] = [-3, 2]$, which could be seen as the interval $a \in [3, 8]$. This interval is no different than $[0, 5]$ or $[0, 6]$, this shifting of the interval captures $[x, x + (n-1)]$.

Note: We'll use α: "alpha"; β: "beta"; and such as variables when discussing residue classes.

Theorem 4.2: Residue Class Operations

Let $\alpha \in \mathbb{Z}_n$ be residue classes. Then:

- **Additive Identity:** $\alpha + [0] = \alpha$; **Additive Inverse:** $\alpha + (-\alpha) = [0]$.
- **Multiplicative Identity:** $\alpha \cdot [1] = \alpha$; **Multiplicative Inverse:** $\alpha \cdot \alpha^{-1} = [1]$.

Moreover, **Residue classes form a ring** (**??**), including distributive properties.

Theorem 4.3: Inverse Residue Classes

For $n \in \mathbb{Z} : n > 1$,
let $Z_n^* := \{\alpha \in \mathbb{Z}_n \mid \gcd(\alpha, n) = 1\}$, i.e., Z_n^* contains elements in $\mathbb{Z}_n$ where α^{-1} exists.

- If n is prime, then $Z_n^* = \mathbb{Z}_n \setminus \{[0]\}$, i.e., Z_n^* contains all elements in $\mathbb{Z}_n$ except $[0]$.
- If n is composite, then $Z_n^* \subsetneq \mathbb{Z}_n \setminus \{[0]\}$.

Note: The symbol $\subsetneq$ denotes a proper subset. If $A \subsetneq B$, then A is a subset of B but not equal to B.

Proof 4.1: Residue Class Inverses

Primes: The congruence $\alpha z \equiv 1 \pmod{n}$ has a solution z for all $\alpha \in \mathbb{Z}_n$ if $gcd(\alpha, n) = 1$ (3.4).

Composites: $Z_n^* \subsetneq \mathbb{Z}_n \setminus \{[0]\}$. If $d := gcd(\alpha, n) \mid n$, and $1 < d < n$, then $d \neq 0$ and $\alpha \notin Z_n^*$ (3.1). We say $d < n$, otherwise $n \equiv 0 \pmod{n}$ where $d = n$.

■

Theorem 4.4: Inverse Operations

Let $\alpha, \beta, \gamma \in \mathbb{Z}_n$ be residue classes. Then:

- **Inverse of Inverse:** $(\alpha^{-1})^{-1} = \alpha$
- **Product of Inverse:** $(\alpha \cdot \beta)^{-1} = \alpha^{-1} \cdot \beta^{-1}$
- **Inverse Division:** $\alpha/\beta = \alpha \cdot \beta^{-1}$
- **Cancellation Law:** $\alpha\beta = \alpha\gamma \implies \beta = \gamma \iff \alpha \in Z_n^*$.

Theorem 4.5: Residue Powers Identities

Powers work similarly to integers. For $\alpha, \beta \in \mathbb{Z}_n$ and $k, l \in \mathbb{Z}$:

- **Zero Power:** $\alpha^0 = [1]$
- **General Powers:** $\alpha^1 = \alpha$ and $\alpha^2 = \alpha \cdot \alpha$ and so on.
- **Inverse Power:** Inverse α^k is $(\alpha^{-1})^k$.
- **Power of a Power:** $(\alpha^l)^k = \alpha^{lk} = (\alpha^k)^l$.
- **Product of Powers:** $\alpha^k \cdot \alpha^l = \alpha^{k+l}$.
- **Quotient of Powers:** $\alpha^k/\alpha^l = \alpha^{k-l}$.
- **Power of a Product:** $(\alpha\beta)^k = \alpha^k \cdot \beta^k$.

These identities also hold for $\alpha, \beta \in \mathbb{Z}_n^*$.

We may now generalize the Chinese Remainder Theorem (3.5) under residue classes.

Theorem 4.6: Chinese Remainder Map

Let $\{n_i\}_{i=1}^k \in \mathbb{Z}^+$ all be pairwise coprime, and $n := \prod_{i=1}^k n_i$. We define the map:

$$\begin{aligned} \theta : \mathbb{Z}_n &\to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [a]_n &\mapsto ([a]_{n_1}, \ldots, [a]_{n_k}) \end{aligned}$$

For $\mathbb{Z}_n$ (Residue classes modulo n), we can visualize:

$$\theta([a]_n) = \begin{cases} [a]_{n_1} & \text{mod } n_1 \\ [a]_{n_2} & \text{mod } n_2 \\ \vdots & \vdots \\ [a]_{n_k} & \text{mod } n_k \end{cases}$$

Where $[a]_n$ can be thought of as our a solution in the system of congruences:

$$\begin{aligned} a &\equiv a_1 \pmod{n_1} \\ a &\equiv a_2 \pmod{n_2} \\ &\vdots \\ a &\equiv a_k \pmod{n_k}, \end{aligned}$$

extending the Chinese Remainder Theorem to classes produced by a mod n, not just a.

(i) θ is unambiguous, i.e., any $[a]_n \in \mathbb{Z}_n$ has a unique image in $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

(ii) θ forms a ring isomorphism, meaning:

  (a) θ is a bijection (one-to-one and onto), i.e., there's an inverse map θ^{-1}, which is the process of finding a from $[a]_n$ (The Chinese Remainder Theorem).

  (b) θ preserves addition and multiplication, since residues form a ring. Thus, operating on residue classes only affects the inputs to the map (4.2).

Tip: The Chinese Remainder Map (θ) generates a system of congruences, while the Chinese Remainder Theorem solves them (θ^{-1}).

Euler's Phi Function

Tip: Leonhard Euler (1707–1783), pronounced as "oiler," was a Swiss mathematician born in Basel. He worked in St. Petersburg and Berlin, shaping calculus and number theory.

Also known as the **Euler Totient Function**:

Definition 4.1: Euler's Phi Function

For all $n \in \mathbb{Z}^+$, we define Euler's Phi Function as:

$$\varphi(n) := |\mathbb{Z}_n^*|$$

The number of inverses modulo n. Numbers coprime to n are in $\mathbb{Z}_n^*$.
Therefore, for primes p, $\varphi(p) = p - 1$.

Theorem 4.7: Chinese Remainder's Phi Function

Let $n := \prod_{i=1}^{k} n_i$ be the product of pairwise coprime integers. Then:

$$\varphi(n) = \prod_{i=1}^{k} \varphi(n_i) = \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_k)$$

The number of inverses in $\mathbb{Z}_n^*$ is the product of the number of inverses in $\mathbb{Z}_{n_i}^*$.

Proof 4.2: Chinese Remainder's Phi Function

Consider the Chinese Remainder Map $\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Since θ is isomorphic, it has a one-to-one correspondence. If we restrict our input to $\mathbb{Z}_n^*$, then the output will be in $\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. Hence, $|\mathbb{Z}_n^*| = |\mathbb{Z}_{n_1}^*| \times |\mathbb{Z}_{n_2}^*| \times \cdots \times |\mathbb{Z}_{n_k}^*| = \prod_{i=1}^{k} |\mathbb{Z}_{n_i}^*| = \prod_{i=1}^{k} \varphi(n_i)$. ■

Theorem 4.8: Euler's Phi of a Raised Prime

Let p be a prime and $e \in \mathbb{Z}^+$. Then:

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

Proof 4.3: Euler's Phi of a Raised Prime

$\varphi(n)$ counts residue classes in $\mathbb{Z}_n$ that are coprime to n. $\mathbb{Z}_n$ represent integers $[0, n-1]$.

Examining $\mathbb{Z}_{p^e}$, to obtain coprimes, we omit members sharing common factors to p^e, i.e., multiples p, which p^e gives us e of.

Since the last factor reaches p^e, we ignore it, as it's beyond $p^e - 1$. Leaving us p^{e-1} multiples. Therefore, $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

■

As implied by Theorem 4.7, we can generalize this to the prime factorization of n.

Theorem 4.9: Phi of Prime Factorization

Let $n := \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of n. $\{p_i^{e_i}\}$ are pairwise coprime. Then:

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1)$$

Expanding the product,

$$\varphi(n) = p_1^{e_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot p_k^{e_k} \cdot \left(1 - \frac{1}{p_k}\right)$$

Which gives us:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

as n represents $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

1.5 Euler's Theorem & Fermat's Little Theorem

We know residues repeat in $\mathbb{Z}_n$ after n steps, forming a cycle. We've been used to seeing such cycles end and start at 0. However, when we restrict ourselves to $\mathbb{Z}_n^*$, 0 is excluded. We'll find that cycles in $\mathbb{Z}_n^*$ jump by powers of $\alpha \in \mathbb{Z}_n^*$, starting and ending at 1.

Definition 5.1: Multiplicative Order

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n^*$. The multiplicative order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Theorem 5.1: Multiplicative Order Interval

Let $n \in \mathbb{Z}^+$ and $\alpha \in \mathbb{Z}_n^*$. The multiplicative order k repeats every k steps. Therefore, for every index:

- $i \in \mathbb{Z}$, $\alpha^i \equiv 1 \pmod{n} \iff k \mid i$, i.e., $i \equiv 0 \pmod{k}$.
- $i, j \in \mathbb{Z}$, $\alpha^i \equiv \alpha^j \pmod{n} \iff i \equiv j \pmod{k}$.

Example: Let $n = 7$ and take $\alpha = 1, \ldots, 6$.

- $\alpha = 1$: order 1.
- $\alpha = 2$: order 3.
- $\alpha = 3$: order 6.
- $\alpha = 4$: order 3.
- $\alpha = 5$: order 6.
- $\alpha = 6$: order 2.

i	1	2	3	4	5	6
1^i mod 7	1	1	1	1	1	1
2^i mod 7	2	4	1	2	4	1
3^i mod 7	3	2	6	4	5	1
4^i mod 7	4	2	1	4	2	1
5^i mod 7	5	4	6	2	3	1
6^i mod 7	6	1	6	1	6	1

We see that $\alpha = 2$ for $i = 3$ and $i = 6$, 3 is the smallest k such that $2^k \equiv 1 \pmod{7}$. Additionally, we see the relationship $2^i \equiv 2^j \pmod{7}$ if and only if $i \equiv j \pmod{3}$.

Theorem 5.2: Euler's Theorem

Let $n \in \mathbb{Z}^+$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\varphi(n)} \equiv 1 \pmod{n}$, when multiplicative order α divides $\varphi(n)$.

Proof 5.1: Euler's Theorem

For every $\beta \in \mathbb{Z}_n^*$, theres an $\alpha \in \mathbb{Z}_n^*$ such that $\alpha\beta \in \mathbb{Z}_n^*$ (4.2):

$$\prod_{\beta \in \mathbb{Z}_n^*} \beta = \prod_{\beta \in \mathbb{Z}_n^*} \alpha\beta = \alpha^{\varphi(n)} \prod_{\beta \in \mathbb{Z}_n^*} \beta$$

Where $\varphi(n)$ is the number of elements in $\mathbb{Z}_n^*$. Then take the inverse of $\prod_{\beta \in \mathbb{Z}_n^*} \beta$ results in:

$$1 = \alpha^{\varphi(n)}$$

■

Theorem 5.3: Fermat's Little Theorem

For every prime p and residue classes $\alpha \in \mathbb{Z}_p^*$: $\alpha^p = \alpha$.

Proof 5.2: Fermat's Little Theorem

Since p is prime, $\varphi(p) = p - 1$. By Euler's Theorem, $\alpha^{p-1} = 1$. Therefore, multiplying α to both sides yields, $\alpha^{p-1}(\alpha) = 1(\alpha)$. Hence $\alpha^p = \alpha$. ■

Definition 5.2: Primitive Root

Let $n \in \mathbb{Z}^+$ and $\alpha \in \mathbb{Z}_n^*$. If the multiplicative order of α modulo n is $\varphi(n)$, then α is a primitive root modulo n.

Example: In the above example modulo 7, residues 3 and 5 are primitive roots.

Theorem 5.4: Multiplicative Order of Powers

If $\alpha \in \mathbb{Z}_n^*$ has multiplicative order k. Then from every new residue produced by α^m where $m \in \mathbb{Z}$, the multiplicative order of α^m is:

$$\frac{k}{\gcd(m, k)}$$

Example: Let $n = 7$ and $\alpha = 1, \ldots, 6$.

- $\alpha = 2^1 = 2$: has order $\dfrac{3}{\gcd(1,3)} = 3$.
- $\alpha = 2^2 = 4$: has order $\dfrac{3}{\gcd(2,3)} = 3$.
- $\alpha = 2^3 = 8 = 1$: has order $\dfrac{3}{\gcd(3,3)} = 1$.

i	1	2	3	4	5	6
1^i mod 7	1	1	1	1	1	1
2^i mod 7	2	4	1	2	4	1
3^i mod 7	3	2	6	4	5	1
4^i mod 7	4	2	1	4	2	1
5^i mod 7	5	4	6	2	3	1
6^i mod 7	6	1	6	1	6	1

Raising $\alpha = 2^3$ gave us 8, which is congruent to 1 modulo 7, and $\alpha = 1$ has order 1.
We will abstract variables to emphasize definitions.

Proof 5.3: Multiplicative Order of Powers

We abstract the residue produced by $\alpha^m := \beta$. Then β's multiplicative order is the smallest l such that $\beta^l \equiv 1 \pmod{n}$. Then by (5.1),

$$\alpha^{m \cdot l} \equiv 1 \,(\mathrm{mod}\ n) \iff ml \equiv 0 \,(\mathrm{mod}\ k)$$

We can drop m as a common factor by taking $\gcd(m, k)$ from k, yielding:

$$l \equiv 0 \,(\mathrm{mod}\ \frac{k}{\gcd(m, k)})$$

Meaning l is our multiplicative order, as for β, we also have $\beta^l \equiv 1 \pmod{n}$.

■

1.6 Quadratic Residues