

The Ring of Integers Modulo n

Chao Qin

School of Mathematical Sciences

May 9th, 2024

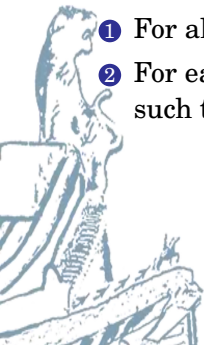


Congruences Modulo n

Definition (Group)

A *group* is a set G equipped with a binary operation $G \times G \rightarrow G$ (denoted by multiplication below) and an identity element $1 \in G$ such that:

- 1 For all $a, b, c \in G$, we have $(ab)c = a(bc)$.
- 2 For each $a \in G$, we have $1a = a1 = a$, and there exists $b \in G$ such that $ab = 1$.



Congruences Modulo n

Definition (Group)

A *group* is a set G equipped with a binary operation $G \times G \rightarrow G$ (denoted by multiplication below) and an identity element $1 \in G$ such that:

- 1 For all $a, b, c \in G$, we have $(ab)c = a(bc)$.
- 2 For each $a \in G$, we have $1a = a1 = a$, and there exists $b \in G$ such that $ab = 1$.

Definition (Abelian Group)

An *abelian group* is a group G such that $ab = ba$ for every $a, b \in G$.

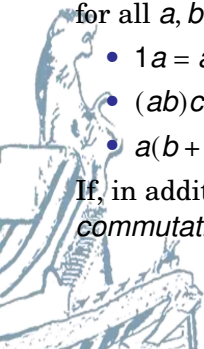
Congruences Modulo n

Definition (Ring)

A *ring* R is a set equipped with binary operations $+$ and \times and elements $0, 1 \in R$ such that R is an abelian group under $+$, and for all $a, b, c \in R$ we have

- $1a = a1 = a$
- $(ab)c = a(bc)$
- $a(b + c) = ab + ac$.

If, in addition, $ab = ba$ for all $a, b \in R$, then we call R a *commutative ring*.



Congruences Modulo n

Definition (Integers Modulo n)

The ring n of integers modulo n is the set of equivalence classes of integers modulo n . It is equipped with its natural ring structure:

$$(a + n\mathbf{Z}) + (b + n\mathbf{Z}) = (a + b) + n\mathbf{Z}$$

$$(a + n\mathbf{Z}) \cdot (b + n\mathbf{Z}) = (a \cdot b) + n\mathbf{Z}.$$



Congruences Modulo n

Example

For example,

$$\mathbf{Z}/3\mathbf{Z} = \{\{\dots, -3, 0, 3, \dots\}, \{\dots, -2, 1, 4, \dots\}, \{\dots, -1, 2, 5, \dots\}\}$$



Congruences Modulo n

Example

For example,

$$\mathbf{Z}/3\mathbf{Z} = \{\{\dots, -3, 0, 3, \dots\}, \{\dots, -2, 1, 4, \dots\}, \{\dots, -1, 2, 5, \dots\}\}$$

Definition (Field)

A *field* K is a ring such that for every nonzero element $a \in K$ there is an element $b \in K$ such that $ab = 1$.

Congruences Modulo n

Example

For example,

$$\mathbf{Z}/3\mathbf{Z} = \{\{\dots, -3, 0, 3, \dots\}, \{\dots, -2, 1, 4, \dots\}, \{\dots, -1, 2, 5, \dots\}\}$$

Definition (Field)

A *field* K is a ring such that for every nonzero element $a \in K$ there is an element $b \in K$ such that $ab = 1$.

For example, if p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a field

Congruences Modulo n

Definition (Reduction Map and Lift)

We call the natural reduction map $\mathbf{Z} \rightarrow n\mathbf{Z}$, which sends a to $a + n\mathbf{Z}$, reduction modulo n . We also say that a is a *lift* of $a + n\mathbf{Z}$. Thus, e.g., 7 is a lift of $1 \bmod 3$, since $7 + 3\mathbf{Z} = 1 + 3\mathbf{Z}$.

We can use that arithmetic in n is well defined to derive tests for divisibility by n .



Congruences Modulo n

Definition (Reduction Map and Lift)

We call the natural reduction map $\mathbf{Z} \rightarrow n\mathbf{Z}$, which sends a to $a + n\mathbf{Z}$, reduction modulo n . We also say that a is a *lift* of $a + n\mathbf{Z}$. Thus, e.g., 7 is a lift of $1 \pmod 3$, since $7 + 3\mathbf{Z} = 1 + 3\mathbf{Z}$.

We can use that arithmetic in n is well defined to derive tests for divisibility by n .

Theorem

A number $n \in \mathbf{Z}$ is divisible by 3 if and only if the sum of the digits of n is divisible by 3.

Congruences Modulo n



① Linear Equations Modulo n

② Eulers Theorem

③ Wilsons Theorem

Linear Equations Modulo n

Theorem (Cancellation)

If $\gcd(c, n) = 1$ and

$$ac \equiv bc \pmod{n},$$

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



Linear Equations Modulo n

Theorem (Cancellation)

If $\gcd(c, n) = 1$ and

$$ac \equiv bc \pmod{n},$$

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

Proof.

By definition

$$n \mid ac - bc = (a - b)c.$$

Since $\gcd(n, c) = 1$, it follows from FTA that $n \mid a - b$, so

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

as claimed.

Linear Equations Modulo n

Definition (Complete Set of Residues)

We call a subset $R \subset \mathbf{Z}$ of size n whose reductions modulo n are pairwise distinct a complete set of residues modulo n . In other words, a complete set of residues is a choice of representative for each equivalence class in $\mathbf{Z}/n\mathbf{Z}$.



Linear Equations Modulo n

Definition (Complete Set of Residues)

We call a subset $R \subset \mathbf{Z}$ of size n whose reductions modulo n are pairwise distinct a complete set of residues modulo n . In other words, a complete set of residues is a choice of representative for each equivalence class in $\mathbf{Z}/n\mathbf{Z}$.

Lemma

If R is a complete set of residues modulo n and $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$, then $aR = \{ax : x \in R\}$ is also a complete set of residues modulo n .

Linear Equations Modulo n

Theorem (Units)

If $\gcd(a, n) = 1$, then the equation $ax \equiv b \pmod{n}$ has a solution, and that solution is unique modulo n .



Linear Equations Modulo n

Theorem (Units)

If $\gcd(a, n) = 1$, then the equation $ax \equiv b \pmod{n}$ has a solution, and that solution is unique modulo n .

Proof.

Let R be a complete set of residues modulo n , so there is a unique element of R that is congruent to b modulo n . By the previous Lemma, aR is also a complete set of residues modulo n , so there is a unique element $ax \in aR$ that is congruent to b modulo n , and we have $ax \equiv b \pmod{n}$. □

Linear Equations Modulo n

Theorem (Solvability)

The equation $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a, n)$ divides b .



Congruences Modulo n



① Linear Equations Modulo n

② Eulers Theorem

③ Wilsons Theorem

Eulers Theorem

Definition (Order of an Element)

Let $n \in \mathbf{N}$ and $x \in \mathbf{Z}$ and suppose that $\gcd(x, n) = 1$. The *order* of x modulo n is the smallest $m \in \mathbf{N}$ such that

$$x^m \equiv 1 \pmod{n}.$$



Eulers Theorem

Definition (Euler's φ -function)

For $n \in \mathbf{N}$, let

$$\varphi(n) = \#\{a \in \mathbf{N} : a \leq n \text{ and } \gcd(a, n) = 1\}.$$



Eulers Theorem

Definition (Euler's φ -function)

For $n \in \mathbf{N}$, let

$$\varphi(n) = \#\{a \in \mathbf{N} : a \leq n \text{ and } \gcd(a, n) = 1\}.$$

For example,

$$\varphi(1) = \#\{1\} = 1,$$

$$\varphi(2) = \#\{1\} = 1,$$

$$\varphi(5) = \#\{1, 2, 3, 4\} = 4,$$

$$\varphi(12) = \#\{1, 5, 7, 11\} = 4.$$



Eulers Theorem

Theorem (Euler's Theorem)

If $\gcd(x, n) = 1$, then

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



Congruences Modulo n



① Linear Equations Modulo n

② Eulers Theorem

③ Wilsons Theorem

Wilsons Theorem

Theorem

An integer $p > 1$ is prime if and only if $(p - 1)! \equiv -1 \pmod{p}$.



Wilsons Theorem

Theorem

An integer $p > 1$ is prime if and only if $(p - 1)! \equiv -1 \pmod{p}$.

For example, if $p = 3$, then $(p - 1)! = 2 \equiv -1 \pmod{3}$.



Wilson's Theorem

Theorem

An integer $p > 1$ is prime if and only if $(p - 1)! \equiv -1 \pmod{p}$.

For example, if $p = 3$, then $(p - 1)! = 2 \equiv -1 \pmod{3}$. If $p = 17$, then

$$(p - 1)! = 20922789888000 \equiv -1 \pmod{17}.$$



Wilson's Theorem

Theorem

An integer $p > 1$ is prime if and only if $(p - 1)! \equiv -1 \pmod{p}$.

For example, if $p = 3$, then $(p - 1)! = 2 \equiv -1 \pmod{3}$. If $p = 17$, then

$$(p - 1)! = 20922789888000 \equiv -1 \pmod{17}.$$

But if $p = 15$, then

$$(p - 1)! = 87178291200 \equiv 0 \pmod{15},$$

so 15 is composite. Thus Wilson's theorem could be viewed as a primality test, though, from a computational point of view, it is probably one of the world's least efficient primality tests since computing $(n - 1)!$ takes so many steps.

