Math 325K - Lecture 23
Section 8.4

Bo Lin

November 27th, 2018

Outline

- Congruence modulo n.
- Properties of congruence modulo n.
- The commutative ring $\mathbb{Z}_n$.

Examples of congruence modulo n

The congruence modulo n is widely used in our everyday lives. Here are some examples.

- Days in a week are modulo 7.

Examples of congruence modulo n

The congruence modulo n is widely used in our everyday lives. Here are some examples.

- Days in a week are modulo 7.
- Time within a day - hours are modulo 12, minutes and seconds are modulo 60.

Examples of congruence modulo n

The congruence modulo n is widely used in our everyday lives. Here are some examples.

- Days in a week are modulo 7.
- Time within a day - hours are modulo 12, minutes and seconds are modulo 60.
- Codes with check digit - International Standard Book Number (ISBN-13) and Universal Product Code (UPC) are modulo 10.

Equivalent characterizations of congruence

Theorem

Let a, b and $n > 1$ be integers. The following statements are all equivalent:

1. $a \equiv b \pmod{n}$;
2. $n \mid (a - b)$;
3. $a = b + kn$ *for some integer* k;
4. a *and* b *have the same (nonnegative) remainder when divided by* n;
5. $a \mod n = b \mod n$.

Equivalent characterizations of congruence

Proof.

$(1) \Rightarrow (2)$: this is the definition of congruence. $(2) \Rightarrow (3)$: this is the definition of divisibility.

Equivalent characterizations of congruence

Proof.

$(1) \Rightarrow (2)$: this is the definition of congruence. $(2) \Rightarrow (3)$: this is the definition of divisibility. $(3) \Rightarrow (4)$: suppose $a = qn + r$ where q is the quotient and $0 \leq r < n$ is the remainder, then $b = (q-k)n + r$. By the uniqueness of remainder, b has the same remainder when divided by n.

Equivalent characterizations of congruence

Proof.

$(1) \Rightarrow (2)$: this is the definition of congruence. $(2) \Rightarrow (3)$: this is the definition of divisibility. $(3) \Rightarrow (4)$: suppose $a = qn + r$ where q is the quotient and $0 \leq r < n$ is the remainder, then $b = (q-k)n + r$. By the uniqueness of remainder, b has the same remainder when divided by n. $(4) \Rightarrow (5)$: this is the definition of $a \bmod n$.

Equivalent characterizations of congruence

Proof.

$(1) \Rightarrow (2)$: this is the definition of congruence. $(2) \Rightarrow (3)$: this is the definition of divisibility. $(3) \Rightarrow (4)$: suppose $a = qn + r$ where q is the quotient and $0 \leq r < n$ is the remainder, then $b = (q - k)n + r$. By the uniqueness of remainder, b has the same remainder when divided by n. $(4) \Rightarrow (5)$: this is the definition of $a \mod n$. $(5) \Rightarrow (1)$: by (5), a and b have the same remainder when divided by n. So there exists integers q_1, q_2, r such that $a = q_1 n + r, b = q_2 n + r$. Then $a - b = (q_1 - q_2)n$ is divisible by n, and (1) holds. □

Residues modulo n

Definition

Given integers a and n with $n > 1$, the **residue** *of a modulo n is $a \bmod n$, the nonnegative remainder obtained when a is divided by n. A set S of integers is called a* **complete set of residues** *modulo n if and only if for any integer a, there is a unique element $x \in S$ such that $a \equiv x \pmod{n}$.*

Residues modulo n

Definition

Given integers a and n with $n > 1$, the **residue** *of a modulo n is $a \mod n$, the nonnegative remainder obtained when a is divided by n. A set S of integers is called a* **complete set of residues** *modulo n if and only if for any integer a, there is a unique element $x \in S$ such that $a \equiv x \pmod{n}$.*

Remark

The numbers $0, 1, 2, \ldots, n-1$ form a complete set of residues modulo n. In some cases, another complete set of residues modulo n is also used, which consists n integers not congruent to each other modulo n with least absolute values. For example, such a set for $n = 7$ would be $\{-3, -2, -1, 0, 1, 2, 3\}$.

Exercise: characterization of complete set of residues

Exercise

Show that a set S of integer is a complete set of residues modulo n if and only if the cardinality of S is n and any two elements of S are not congruent to each other modulo n.

Exercise: characterization of complete set of residues

Exercise

Show that a set S of integer is a complete set of residues modulo n if and only if the cardinality of S is n and any two elements of S are not congruent to each other modulo n.

Proof.

For the equivalent relation modulo n, there are n equivalence classes. By definition of complete set of residues, S contains at least one element in each class, and at most one. Then $|S| = n$ and any two elements belong to distinct classes, so they are not congruent to each other modulo n. □

Arithmetic properties

Theorem

Let a, b, c, d *and* $n > 1$ *be integers, and suppose* $a \equiv c \pmod{n}, b \equiv d \pmod{n}$. *Then*

- (a) $(a + b) \equiv (c + d) \pmod{n}$;
- (b) $(a - b) \equiv (c - d) \pmod{n}$;
- (c) $ab \equiv cd \pmod{n}$;
- (d) $a^m \equiv c^m \pmod{n}$ *for all positive integers* m.

Properties of congruence modulo n

Proof.

We only prove (c). Since $a \equiv c \pmod{n}$, there exists an integer s such that $a = c + sn$; since $b \equiv d \pmod{n}$, there exists an integer t such that $b = d + sn$. Then

$$ab - cd = (c+sn)(d+tn) - cd = ctn + snd + stn^2 = (ct + ds + stn) \cdot n$$

is a multiple of n, so $ab \equiv cd \pmod{n}$. □

Exercise: congruences

Exercise

Are the following congruence relations true or false?

a. $12 \equiv 39 \pmod 9$;
b. $46 \equiv 89 \pmod{13}$;
c. $16 \equiv -5 \pmod 7$.

Exercise: congruences

Exercise

Are the following congruence relations true or false?

- (a) $12 \equiv 39 \pmod 9$;
- (b) $46 \equiv 89 \pmod{13}$;
- (c) $16 \equiv -5 \pmod 7$.

Solution

(a) $12 - 39 = -27 = 9 \cdot 3$, *so it is true.*

Exercise: congruences

Exercise

Are the following congruence relations true or false?

(a) $12 \equiv 39 \pmod 9$;
(b) $46 \equiv 89 \pmod{13}$;
(c) $16 \equiv -5 \pmod 7$.

Solution

(a) $12 - 39 = -27 = 9 \cdot 3$, *so it is true.*
(b) $46 - 89 = -43$ *is not a multiple of* 13, *so it is false.*

Exercise: congruences

Exercise

Are the following congruence relations true or false?

(a) $12 \equiv 39 \pmod 9$;
(b) $46 \equiv 89 \pmod{13}$;
(c) $16 \equiv -5 \pmod 7$.

Solution

(a) $12 - 39 = -27 = 9 \cdot 3$, *so it is true.*
(b) $46 - 89 = -43$ *is not a multiple of* 13, *so it is false.*
(c) $16 - (-5) = 21 = 7 \cdot 3$, *so it is true.*

Units digit

Definition

For a positive integer n, its **units digit** *is its right-most digit in the decimal representation.*

Units digit

Definition

For a positive integer n, its **units digit** *is its right-most digit in the decimal representation.*

Proposition

For any positive integer n, its units digit is just $n \mod 10$.

Units digit

Definition

For a positive integer n, its **units digit** *is its right-most digit in the decimal representation.*

Proposition

For any positive integer n, its units digit is just $n \mod 10$.

Proof.

Suppose the decimal representation of n is $a_1 a_2 \cdots a_k$, then

$$n = 10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k.$$

So $n \equiv a_k \pmod{10}$, and k is the units digit of n. □

Exercise: find units digits

Exercise

Find the units digit of 3^{10}.

Exercise: find units digits

Exercise

Find the units digit of 3^{10}.

Solution

Note that $3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81 \equiv 1 \pmod{10}$. *So for any* $m \in \mathbb{N}$, *we have*

$$3^{4m} = \left(3^4\right)^m \equiv 1^m = 1 \pmod{10}.$$

Then $3^{10} = 3^8 \cdot 3^2 \equiv 1 \cdot 3^2 = 9 \pmod{10}$, *the answer is* 9.

$\mathbb{Z}_n$ and $+, \cdot$ on it

Definition

For each integer $n > 1$, $\mathbb{Z}_n$ is the set of distinct equivalence classes for congruence modulo n:

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

$\mathbb{Z}_n$ and $+, \cdot$ on it

Definition

For each integer $n > 1$, $\mathbb{Z}_n$ is the set of distinct equivalence classes for congruence modulo n:

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

Definition

We define addition and multiplication on the set $\mathbb{Z}_n$. For elements $[a], [b]$, we let

$$[a] + [b] = [a+b], [a] \cdot [b] = [a \cdot b].$$

By properties we just introduced, the addition and multiplication on $\mathbb{Z}_n$ are well-defined.

Commutative rings

Definition

Let S be a set with two binary operations called addition $+$ and multiplication $\cdot$. S is called a **commutative ring** *if and only if the following properties hold: For all elements $a, b, c \in S$,*

- *(commutative properties): $a + b = b + a, a \cdot b = b \cdot a$;*
- *(associative properties):* $(a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- *(distributive property): $a \cdot (b + c) = a \cdot b + a \cdot c$;*
- *(identity for addition): there exists an element in S, denoted by 0, such that $a + 0 = a$, and there exists an element $d \in S$ such that $a + d = 0$. This d is unique and is called the inverse of a, denoted by $-a$.*
- *(identity for multiplication): there exists an element in S, denoted by 1, such that $a \cdot 1 = a$.*

$\mathbb{Z}_n$ is a commutative ring

Proposition

The set $\mathbb{Z}_n$ with addition and multiplication defined above is a commutative ring.

$\mathbb{Z}_n$ is a commutative ring

Proposition

The set $\mathbb{Z}_n$ with addition and multiplication defined above is a commutative ring.

Sketch of proof.

The commutative, associative and distributive properties follow from the corresponding properties of addition and multiplications of integers. In addition, $[0]$ serves as the identity for addition and $[1]$ serves as the identity for multiplication. The inverse of any $[a]$ is simply $[-a]$. □

Exercise: uniqueness of identity for addition

Exercise

Show that in a commutative ring $(S, +, \cdot)$ *if two elements* x, y *are both identities for addition, then* $x = y$.

Exercise: uniqueness of identity for addition

Exercise

Show that in a commutative ring $(S, +, \cdot)$ if two elements x, y are both identities for addition, then $x = y$.

Proof.

Since x is an identity for addition, and $y \in S$, we have $y + x = y$; since y is an identity for addition, and $x \in S$, we have $x + y = x$. By the commutative property, $x + y = y + x$, so $x = y$. □

HW # 12 for this section

Exercise 5, 13, 24.