Discrete Mathematics & Mathematical Reasoning Arithmetic Modulo *m*

Colin Stirling

Informatics

Some slides based on ones by Myrto Arapinis

Colin Stirling (Informatics)

Discrete Mathematics (Chap 4)

Today 1 / 10

- A - E - N

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

• 3 | (-12) 3 | 0 3 ∦7 (where ∦ "not divides")

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

• $3 \mid (-12)$ $3 \mid 0$ $3 \not\mid 7$ (where $\not\mid$ "not divides")

• If a|b and a|c, then a|(b+c)

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

- $3 \mid (-12)$ $3 \mid 0$ $3 \not\mid 7$ (where $\not\mid$ "not divides")
- If a|b and a|c, then a|(b+c)
- Proof $a|b \Leftrightarrow \exists k_b$. $b = k_b a$ and $a|c \Leftrightarrow \exists k_c$. $c = k_c a$. But then $b + c = (k_b + k_c)a$ which by definition implies that a|(b + c)

く 戸 と く ヨ と く ヨ と

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

- $3 \mid (-12)$ $3 \mid 0$ $3 \not\mid 7$ (where $\not\mid$ "not divides")
- If a|b and a|c, then a|(b+c)
- Proof $a|b \Leftrightarrow \exists k_b$. $b = k_b a$ and $a|c \Leftrightarrow \exists k_c$. $c = k_c a$. But then $b + c = (k_b + k_c)a$ which by definition implies that a|(b + c)
- If a|b, then a|bc

く 戸 と く ヨ と く ヨ と

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

- 3 | (-12) 3 | 0 3 $\cancel{7}$ (where $\cancel{1}$ "not divides")
- If a|b and a|c, then a|(b+c)
- Proof $a|b \Leftrightarrow \exists k_b$. $b = k_b a$ and $a|c \Leftrightarrow \exists k_c$. $c = k_c a$. But then $b + c = (k_b + k_c)a$ which by definition implies that a|(b + c)
- If a|b, then a|bc
- Proof $a|b \Leftrightarrow \exists k_b. b = k_b a$. But then $bc = k_b ac$ which by definition implies that a|bc

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

- 3 | (-12) 3 | 0 3 $\cancel{7}$ (where $\cancel{1}$ "not divides")
- If a|b and a|c, then a|(b+c)
- Proof $a|b \Leftrightarrow \exists k_b$. $b = k_b a$ and $a|c \Leftrightarrow \exists k_c$. $c = k_c a$. But then $b + c = (k_b + k_c)a$ which by definition implies that a|(b + c)
- If a|b, then a|bc
- Proof $a|b \Leftrightarrow \exists k_b. b = k_b a$. But then $bc = k_b ac$ which by definition implies that a|bc
- If a|b and b|c, then a|c

(人間) トイヨト イヨト ニヨ

Definition

If *a* and *b* are integers with $a \neq 0$, then *a* divides *b*, written a|b, if there exists an integer *c* such that b = ac

- 3 | (-12) 3 | 0 3 $\cancel{7}$ (where $\cancel{1}$ "not divides")
- If a|b and a|c, then a|(b+c)
- Proof $a|b \Leftrightarrow \exists k_b$. $b = k_b a$ and $a|c \Leftrightarrow \exists k_c$. $c = k_c a$. But then $b + c = (k_b + k_c)a$ which by definition implies that a|(b + c)
- If a|b, then a|bc
- Proof $a|b \Leftrightarrow \exists k_b. b = k_b a$. But then $bc = k_b ac$ which by definition implies that a|bc
- If a|b and b|c, then a|c
- Proof $a|b \Leftrightarrow \exists k_b$. $b = k_b a$ and $b|c \Leftrightarrow \exists k_c$. $c = k_c b$. But then $c = (k_c k_b) a$ which by definition implies that a|c

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \le r < d$, such that a = dq + r

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \le r < d$, such that a = dq + r

q is quotient and r the remainder; $q = a \operatorname{div} d$ and $r = a \operatorname{mod} d$

Division algorithm (not really an algorithm!)

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \le r < d$, such that a = dq + r

q is quotient and r the remainder; $q = a \operatorname{div} d$ and $r = a \operatorname{mod} d$

Proof.

Consider the largest *q* such that $dq \le a$; then a = dq + r for $0 \le r < d$: if $r \ge d$ then $d(q + 1) \le a$ which contradicts that *q* is largest. So, there is at least one such *q* and *r*. Assume that there is more than one: $a = dq_1 + r_1$, $a = dq_2 + r_2$, and $(q_1, r_1) \ne (q_2, r_2)$. If $q_1 = q_2$ then $r_1 = a - dq_1 = a - dq_2 = r_2$. Since $dq_1 + r_1 = dq_2 + r_2$, $d = \frac{r_1 - r_2}{q_2 - q_1}$ which is impossible because $r_1 - r_2 < d$.

Definition

If *a* and *b* are integers and *m* is a positive integer, then *a* is congruent to *b* modulo *m*, written $a \equiv b \pmod{m}$, iff m|(a - b)

• $17 \equiv 5 \pmod{6}$ because 6 divides 17 - 5 = 12

< 回 ト < 三 ト < 三

Definition

If *a* and *b* are integers and *m* is a positive integer, then *a* is congruent to *b* modulo *m*, written $a \equiv b \pmod{m}$, iff m|(a - b)

- $17 \equiv 5 \pmod{6}$ because 6 divides 17 5 = 12
- $-17 \not\equiv 5 \pmod{6}$ because 6 $\not\mid (-22)$

< 回 ト < 三 ト < 三

Definition

If *a* and *b* are integers and *m* is a positive integer, then *a* is congruent to *b* modulo *m*, written $a \equiv b \pmod{m}$, iff m|(a - b)

- $17 \equiv 5 \pmod{6}$ because 6 divides 17 5 = 12
- $-17 \neq 5 \pmod{6}$ because 6 $\cancel{(-22)}$
- $-17 \equiv 1 \pmod{6}$

< 回 > < 回 > < 回 >

Definition

If *a* and *b* are integers and *m* is a positive integer, then *a* is congruent to *b* modulo *m*, written $a \equiv b \pmod{m}$, iff m|(a - b)

- $17 \equiv 5 \pmod{6}$ because 6 divides 17 5 = 12
- $-17 \neq 5 \pmod{6}$ because 6 $\cancel{(-22)}$
- $-17 \equiv 1 \pmod{6}$
- $24 \neq 14 \pmod{6}$ because 6 $\cancel{10}$

Congruence is an equivalence relation

Theorem

 $a \equiv b \pmod{m}$ iff $a \mod m = b \mod m$

A (10) > A (10) > A

Congruence is an equivalence relation

Theorem

 $a \equiv b \pmod{m}$ iff a mod $m = b \mod{m}$

Proof.

Assume $a \equiv b \pmod{m}$; so m | (a - b). If $a = q_1 m + r_1$ and $b = q_2 m + r_2$ where $0 \le r_1 < m$ and $0 \le r_2 < m$ it follows that $r_1 = r_2$ and so $a \mod m = b \mod m$. If $a \mod m = b \mod m$ then a and b have the same remainder so $a = q_1 m + r$ and $b = q_2 m + r$; therefore $a - b = (q_1 - q_2)m$, and so m | (a - b).

(二回) (二回) (二回)

Congruence is an equivalence relation

Theorem

 $a \equiv b \pmod{m}$ iff a mod $m = b \mod{m}$

Proof.

Assume $a \equiv b \pmod{m}$; so m | (a - b). If $a = q_1 m + r_1$ and $b = q_2 m + r_2$ where $0 \le r_1 < m$ and $0 \le r_2 < m$ it follows that $r_1 = r_2$ and so $a \mod m = b \mod m$. If $a \mod m = b \mod m$ then a and b have the same remainder so $a = q_1 m + r$ and $b = q_2 m + r$; therefore $a - b = (q_1 - q_2)m$, and so m | (a - b).

• \equiv (mod *m*) is an equivalence relation on integers

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

A simple theorem of congruence

Theorem

 $a \equiv b \pmod{m}$ iff there is an integer k such that a = b + km

A (10) > A (10) > A (10)

A simple theorem of congruence

Theorem

 $a \equiv b \pmod{m}$ iff there is an integer k such that a = b + km

Proof.

If $a \equiv b \pmod{m}$, then by the definition of congruence m | (a - b). Hence, there is an integer *k* such that a - b = km and equivalently a = b + km. If there is an integer *k* such that a = b + km, then km = a - b. Hence, m | (a - b) and $a \equiv b \pmod{m}$.

< 回 > < 三 > < 三 >

Congruences of sums, differences, and products

Theorem

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$

Congruences of sums, differences, and products

Theorem

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$

Proof.

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the previous theorem, there are integers *s* and *t* with b = a + sm and d = c + tm. Therefore, b + d = (a + sm) + (c + tm) = (a + c) + m(s + t), and bd = (a + sm)(c + tm) = ac + m(at + cs + stm). Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Congruences of sums, differences, and products

Theorem

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$

Proof.

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the previous theorem, there are integers *s* and *t* with b = a + sm and d = c + tm. Therefore, b + d = (a + sm) + (c + tm) = (a + c) + m(s + t), and bd = (a + sm)(c + tm) = ac + m(at + cs + stm). Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Corollary

- $(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$
- *ab mod m* = ((*a mod m*)(*b mod m*)) *mod m*

•
$$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$$

- $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$
- $+_m$ on \mathbb{Z}_m is $a +_m b = (a + b) \mod m$

イロト イヨト イヨト イヨト

- $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$
- $+_m$ on \mathbb{Z}_m is $a +_m b = (a + b) \mod m$
- \cdot_m on \mathbb{Z}_m is define $a \cdot_m b = (a \cdot b) \mod m$

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

- $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$
- $+_m$ on \mathbb{Z}_m is $a +_m b = (a + b) \mod m$
- \cdot_m on \mathbb{Z}_m is define $a \cdot_m b = (a \cdot b) \mod m$
- Find $7 +_{11} 9$ and $-7 \cdot_{11} 9$

- $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$
- $+_m$ on \mathbb{Z}_m is $a +_m b = (a + b) \mod m$
- \cdot_m on \mathbb{Z}_m is define $a \cdot_m b = (a \cdot b) \mod m$
- Find $7 +_{11} 9$ and $-7 \cdot_{11} 9$
- $7 +_{11} 9 = (7 + 9) \mod 11 = 16 \mod 11 = 5$

- $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$
- $+_m$ on \mathbb{Z}_m is $a +_m b = (a + b) \mod m$
- \cdot_m on \mathbb{Z}_m is define $a \cdot_m b = (a \cdot b) \mod m$
- Find $7 +_{11} 9$ and $-7 \cdot_{11} 9$
- $7 +_{11} 9 = (7 + 9) \mod 11 = 16 \mod 11 = 5$
- $-7 \cdot_{11} 9 = (-7 \cdot 9) \mod 11 = -63 \mod 11 = 3$

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to \mathbb{Z}_m

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to \mathbb{Z}_m

Associativity If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to \mathbb{Z}_m

Associativity If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to \mathbb{Z}_m

Associativity If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo *m*, respectively. If $a \in \mathbb{Z}_m$ then $a +_m 0 = a$ and $a \cdot_m 1 = a$

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to \mathbb{Z}_m

Associativity If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo *m*, respectively. If $a \in \mathbb{Z}_m$ then $a +_m 0 = a$ and $a \cdot_m 1 = a$

Additive inverses If $0 \neq a \in \mathbb{Z}_m$, then m - a is the additive inverse of a modulo m. Moreover, 0 is its own additive inverse $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to \mathbb{Z}_m

Associativity If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo *m*, respectively. If $a \in \mathbb{Z}_m$ then $a +_m 0 = a$ and $a \cdot_m 1 = a$

Additive inverses If $0 \neq a \in \mathbb{Z}_m$, then m - a is the additive inverse of a modulo m. Moreover, 0 is its own additive inverse $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

Distributivity If $a, b, c \in \mathbb{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

 Over the reals, dividing by a number x is the same as multiplying by y = 1/x, so xy = 1

A (10) A (10) A (10)

- Over the reals, dividing by a number x is the same as multiplying by y = 1/x, so xy = 1
- Similarly for x mod m, we wish to find y mod m such that $xy \equiv 1 \pmod{m}$

A (10) A (10)

- Over the reals, dividing by a number x is the same as multiplying by y = 1/x, so xy = 1
- Similarly for x mod m, we wish to find y mod m such that $xy \equiv 1 \pmod{m}$
- x = 8 and m = 15. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)

- Over the reals, dividing by a number x is the same as multiplying by y = 1/x, so xy = 1
- Similarly for x mod m, we wish to find y mod m such that $xy \equiv 1 \pmod{m}$
- x = 8 and m = 15. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)
- *x* = 12 and *m* = 15

- Over the reals, dividing by a number x is the same as multiplying by y = 1/x, so xy = 1
- Similarly for x mod m, we wish to find y mod m such that $xy \equiv 1 \pmod{m}$
- x = 8 and m = 15. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)
- x = 12 and m = 15 The sequence {ax (mod m) | a = 0, 1, 2, ...} is periodic, and takes on the values {0, 12, 9, 6, 3}. So, 12 has no multiplicative inverse mod 15

- Over the reals, dividing by a number x is the same as multiplying by y = 1/x, so xy = 1
- Similarly for x mod m, we wish to find y mod m such that $xy \equiv 1 \pmod{m}$
- x = 8 and m = 15. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)
- x = 12 and m = 15 The sequence {ax (mod m) | a = 0, 1, 2, ...} is periodic, and takes on the values {0, 12, 9, 6, 3}. So, 12 has no multiplicative inverse mod 15

Not all integers have an inverse mod *m*. Return to this later