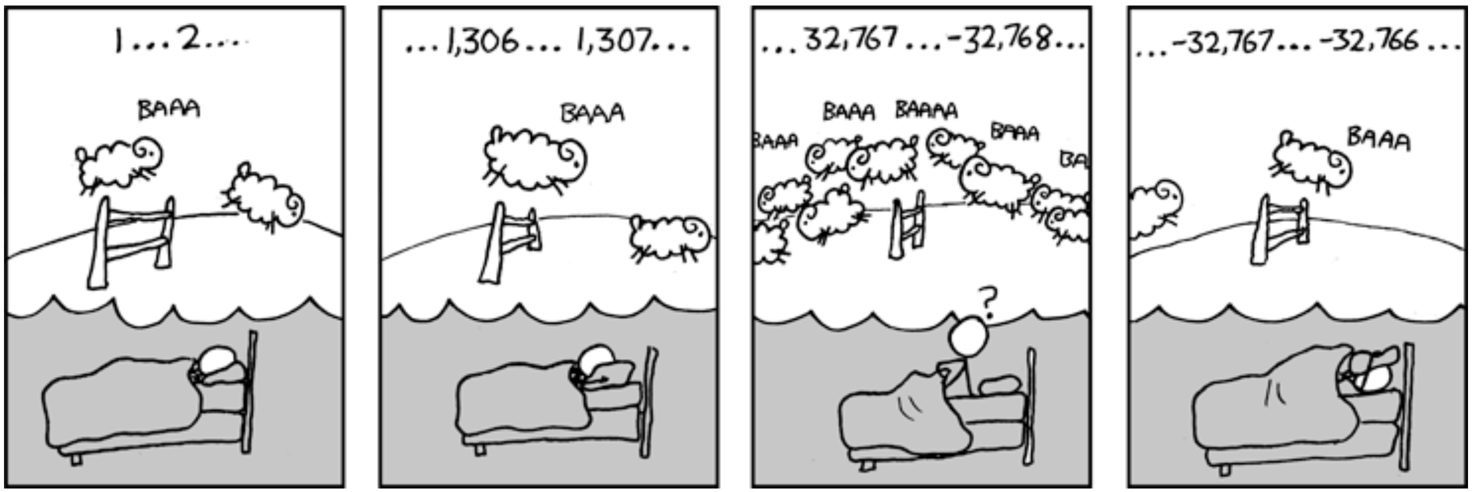
CSE 311: Foundations of Computing

Lecture 11: Modular Arithmetic and Applications



Last Class: Divisibility

Definition: "b divides a"

For a, b with $b \neq 0$:

$$b \mid a \leftrightarrow \exists q \ \ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \mid a$, then, by definition, we have $a = qb$ for some q.
The number q is called the quotient.

Dividing both sides by b, we can write this as

$$\frac{a}{b} = q$$

(We want to stick to integers, though, so we'll write $a = qb$.)

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \nmid a$, then we end up with a *remainder* r with $0 < r < b$. Now,

instead of $\dfrac{a}{b} = q$ we have $\dfrac{a}{b} = q + \dfrac{r}{b}$

Multiplying both sides by b gives us $a = qb + r$
(A bit nicer since it has no fractions.)

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \mid a$, then we have $a = qb$ for some q.
If $b \nmid a$, then we have $a = qb + r$ for some q, r with $0 < \mathrm{r} < \mathrm{b}$.

In general, we have $a = qb + r$ for some q, r with $0 \leq r < b$, where $r = 0$ iff $b \mid a$.

Division Theorem

Domain of Discourse
Integers

Division Theorem

For a, b with $b > 0$
there exist *unique* integers q, r with $0 \le r < b$
such that $a = qb + r$.

To put it another way, if we divide b **into** a**, we get a unique quotient** q = a **div** b
and non-negative remainder r = a **mod** b

Note: r ≥ 0 even if a < 0.
Not quite the same as `a % d`.

div and mod

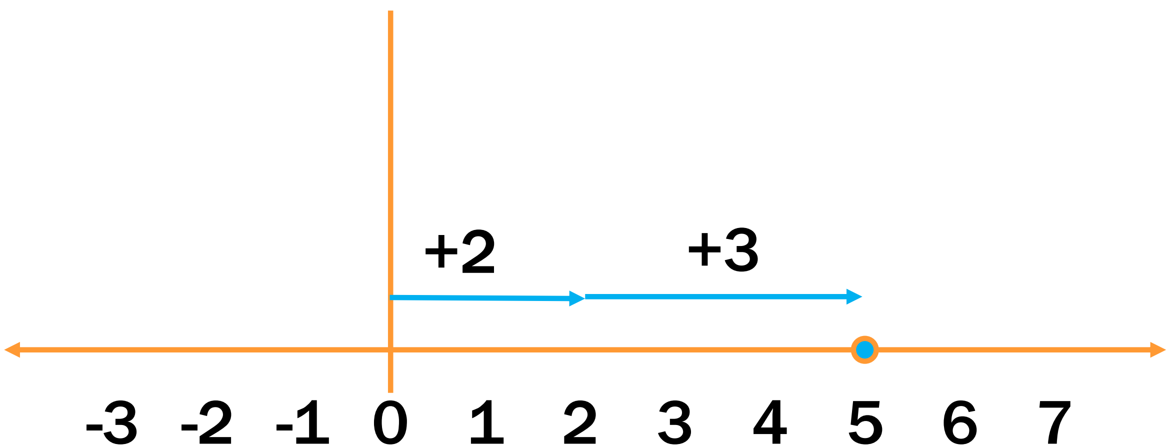
$$x = 7 \cdot (x \text{ div } 7) + (x \text{ mod } 7)$$

x mod 7	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1
x div 7	0	0	0	0	0	0	0	1	1	1	1	1	1	1	2	2
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

$7 \cdot 0$ $7 \cdot 1$ $7 \cdot 2$

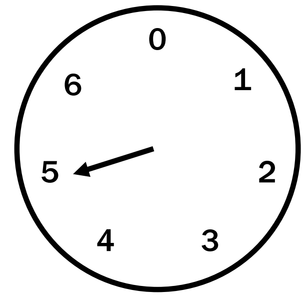
Ordinary arithmetic

$$2 + 3 = 5$$

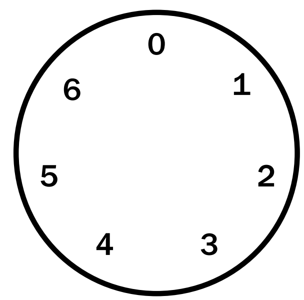


Arithmetic on a Clock

$2 + 3 = 5$



$23 = 3 \cdot 7 + 2$

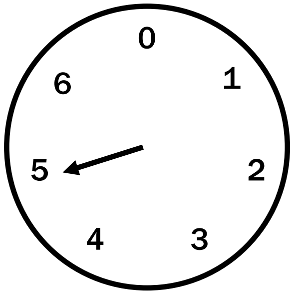


If $a = 7q + r$, then r $(= a \bmod b)$ is
where you stop after taking a steps on the clock

Arithmetic, mod 7

$(a + b) \bmod 7$

$(a \times b) \bmod 7$



+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Domain of Discourse
Integers

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv_m b \leftrightarrow m \mid (a - b)$$

New notion of "sameness" that will help us understand modular arithmetic

Modular Arithmetic

Domain of Discourse
Integers

Definition: “a is congruent to b modulo m”

For a, b, m with $m > 0$

$$a \equiv_m b \leftrightarrow m \mid (a - b)$$

The standard math notation is

$$a \equiv b \pmod{m}$$

A chain of equivalences is written

$$a \equiv b \equiv c \equiv d \pmod{m}$$

Many students find this confusing,
so we will use $\equiv_m$ instead.

Modular Arithmetic

Domain of Discourse
Integers

Definition: “a is congruent to b modulo m”

For a, b, m with $m > 0$

$$a \equiv_m b \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

$x \equiv_2 0$

This statement is the same as saying “x is even”; so, any x that is even (including negative even numbers) will work.

$-1 \equiv_5 19$

This statement is true. 19 - (-1) = 20 which is divisible by 5

$y \equiv_7 2$

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Goal: show $a \equiv_m b$, i.e., $m \mid (a - b)$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Goal: show $a \equiv_m b$, i.e., $m \mid (a - b)$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Therefore, $m \mid (a - b)$ and so $a \equiv_m b$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \mathbf{\ mod\ } \boldsymbol{m} = \boldsymbol{b} \mathbf{\ mod\ } \boldsymbol{m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \textbf{ mod } \boldsymbol{m} = \boldsymbol{b} \textbf{ mod } \boldsymbol{m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \textbf{ mod } \boldsymbol{m} = \boldsymbol{b} \textbf{ mod } \boldsymbol{m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Combining these, we have $qm + (a \bmod m) = a = b + km$
or equiv., $\mathrm{b} = qm - km + (a \bmod m) = (q - k)m + (a \bmod m)$.
By the Division Theorem, we have $b \bmod m = a \bmod m$.

The $\mathrm{mod}\ m$ function vs the $\equiv_m$ predicate

- What we have just shown
  - The $\mathrm{mod}\ m$ function maps any integer a to a remainder $a \bmod m \in \{0,1,..,m-1\}$.
  - Imagine grouping together all integers that have the same value of the $\mathrm{mod}\ m$ function

    That is, the same remainder in $\{0,1,..,m-1\}$.
  - The $\equiv_m$ predicate compares integers a, b. It is true if and only if the $\mathrm{mod}\ m$ function has the same value on a and on b.

    That is, a and b are in the same group.

Recall: Familiar Properties of "="

- **If $a = b$ and $b = c$, then $a = c$.**
  - **i.e., if $a = b = c$, then $a = c$**

- **If $a = b$ and $c = d$, then $a + c = b + d$.**
  - **in particular, since $c = c$ is true, we can "$+ c$" to both sides**

- **If $a = b$ and $c = d$, then $ac = bd$.**
  - **in particular, since $c = c$ is true, we can "$\times c$" to both sides**

These are the facts that allow us to use algebra to solve problems

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$.

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$. Then, by the previous property, we have $a \bmod m = b \bmod m$ and $b \bmod m = c \bmod m$.

Putting these together, we have $a \bmod m = c \bmod m$, which says that $a \equiv_m c$, by the previous property.