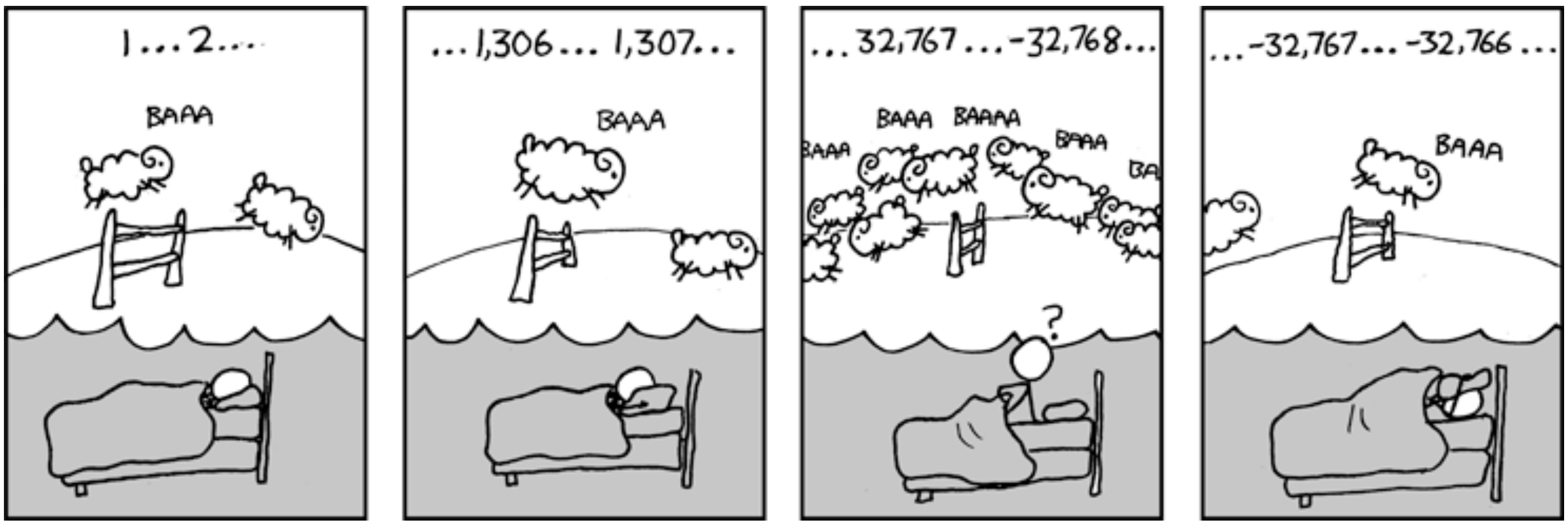
CSE 311: Foundations of Computing

Lecture 11: Modular Arithmetic and Applications



Last Class: Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

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

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers *q*, *r* with $0 \leq r < d$
such that $a = qd + r$.

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

Can then write $a = (a \operatorname{div} d)\, d + (a \bmod d)$

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers q, r with $0 \leq r < d$
such that $a = qd + r$.

Application: take d = 2…

$$a = 2q + r \text{ with } r \in \{0, 1\}$$

- **If r = 0, then a is even**
- **If r = 1, then a is odd**

Even(x) := ∃y (x=2y)
Odd(x) := ∃y (x=2y+1)

Hence, every integer is either even or odd.

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers *q*, *r* with $0 \leq r < d$
such that $a = qd + r$.

q = *a* **div** *d**r* = *a* **mod** *d*

In Java, we have (almost)

div = “/ ” and mod = “ % ”

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers *q*, *r* with $0 \leq r < d$
such that $a = qd + r$.

```
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

```
 ----jGRASP exec: java Test2
-1

 ----jGRASP: operation complete.
```

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

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers *q, r* with $0 \leq r < d$
such that $a = qd + r$.

q = *a* **div** *d*

r = *a* **mod** *d*

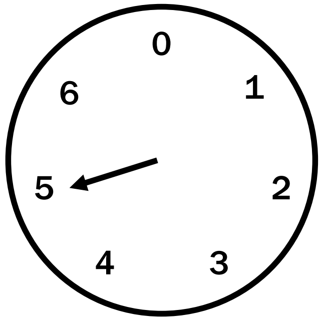
While div is more familiar, our focus is on mod:

- **provides a bound on the size** $(0 \leq r < d)$
- **need to connect that somehow to arithmetic…**

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

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

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

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

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

x ≡ 0 (mod 2)

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

-1 ≡ 19 (mod 5)

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

y ≡ 2 (mod 7)

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

Suppose that $a \equiv b \pmod{m}$.

Modular Arithmetic: A Property

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

Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.

So, $a - b = km$ for some integer k by definition of divides.

Therefore, $a = b + km$.

Taking both sides modulo m we get:

$$a \bmod m = (b + km) \bmod m = b \bmod m.$$

Modular Arithmetic: A Property

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

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

Modular Arithmetic: A Property

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

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

The $\bmod m$ function vs the $\equiv \pmod{m}$ predicate

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

    That is, the same remainder in $\{0,1,..,m-1\}$.
  - The $\equiv \pmod{m}$ predicate compares $a, b \in \mathbb{Z}$. It is true if and only if the $\bmod m$ function has the same value on a and on b.

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

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \ (\mathbf{mod}\ \boldsymbol{m})$ and $\boldsymbol{b} \equiv \boldsymbol{c} \ (\mathbf{mod}\ \boldsymbol{m})$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \ (\mathbf{mod}\ \boldsymbol{m})$

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b}\ (\mathbf{mod}\ \boldsymbol{m})$ and $\boldsymbol{b} \equiv \boldsymbol{c}\ (\mathbf{mod}\ \boldsymbol{m})$,
then $\boldsymbol{a} \equiv \boldsymbol{c}\ (\mathbf{mod}\ \boldsymbol{m})$

Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.
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 $a \equiv c \pmod{m}$, by definition.

So "≡" behaves like "=" in that sense.
And that is not the only similarity...

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{\boldsymbol{m}}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \pmod{\boldsymbol{m}}$

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv \boldsymbol{b} \ (\mathbf{mod}\ \boldsymbol{m})$ and $\boldsymbol{c} \equiv \boldsymbol{d} \ (\mathbf{mod}\ \boldsymbol{m})$, then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \ (\mathbf{mod}\ \boldsymbol{m})$

Suppose that $a \equiv b \ (\mathrm{mod}\ m)$ and $c \equiv d \ (\mathrm{mod}\ m)$. Unrolling definitions gives us some k such that $a - b = km$, and some j such that $c - d = jm$.

Adding the equations together gives us $(a + c) - (b + d) = m(k + j)$. Now, re-applying the definition of congruence gives us $a + c \equiv b + d \ (\mathrm{mod}\ m)$.

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{\boldsymbol{m}}$, then $\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{\boldsymbol{m}}$

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv b \ (\mathrm{mod}\ m)}$ and $\boldsymbol{c \equiv d \ (\mathrm{mod}\ m)}$, then $\boldsymbol{ac \equiv bd \ (\mathrm{mod}\ m)}$

Suppose that $a \equiv b \ (\mathrm{mod}\ m)$ and $c \equiv d \ (\mathrm{mod}\ m)$. Unrolling definitions gives us some k such that $a - b = km$,
and some j such that $c - d = jm$.

Then, $a = km + b$ and $c = jm + d$. Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$.

Re-arranging gives us $ac - bd = m(kjm + kd + bj)$.
Using the definition of congruence gives us $ac \equiv bd \ (\mathrm{mod}\ m)$.

Modular Arithmetic: Properties

If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ and $\boldsymbol{b} \equiv \boldsymbol{c} \pmod{\boldsymbol{m}}$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \pmod{\boldsymbol{m}}$

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

Corollary: If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{c} \pmod{\boldsymbol{m}}$

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

Corollary: If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$, then $\boldsymbol{ac} \equiv \boldsymbol{bc} \pmod{\boldsymbol{m}}$

Modular Arithmetic: Properties

If $\boldsymbol{a} \equiv \boldsymbol{b} \ (\mathbf{mod}\ \boldsymbol{m})$ and $\boldsymbol{b} \equiv \boldsymbol{c} \ (\mathbf{mod}\ \boldsymbol{m})$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \ (\mathbf{mod}\ \boldsymbol{m})$

If $\boldsymbol{a} \equiv \boldsymbol{b} \ (\mathbf{mod}\ \boldsymbol{m})$, then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{c} \ (\mathbf{mod}\ \boldsymbol{m})$

If $\boldsymbol{a} \equiv \boldsymbol{b} \ (\mathbf{mod}\ \boldsymbol{m})$, then $\boldsymbol{ac} \equiv \boldsymbol{bc} \ (\mathbf{mod}\ \boldsymbol{m})$

"≡" allows us to solve problems in modular arithmetic, e.g.

- **add / subtract numbers from both sides of equations**
- **chains of "≡" values shows first and last are "≡"**
- **substitute "≡ " values in equations (not proven yet)**

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod 4}$ or $\boldsymbol{n^2 \equiv 1 \pmod 4}$

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod 4$

$1^2 = 1 \equiv 1 \pmod 4$

$2^2 = 4 \equiv 0 \pmod 4$

$3^2 = 9 \equiv 1 \pmod 4$

$4^2 = 16 \equiv 0 \pmod 4$

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod{4}}$ or $\boldsymbol{n^2 \equiv 1 \pmod{4}}$

Case 1 (n is even):

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$
$4^2 = 16 \equiv 0 \pmod{4}$

It looks like

$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$, and
$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$.

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod{4}}$ or $\boldsymbol{n^2 \equiv 1 \pmod{4}}$

Case 1 (n is even):

Suppose n is even.
Then, $n = 2k$ for some integer k.
So, $n^2 = (2k)^2 = 4k^2 = 0 + 4k^2$.
So, by the definition of congruence,
we have $n^2 \equiv 0 \pmod{4}$.

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$
$4^2 = 16 \equiv 0 \pmod{4}$

It looks like

$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$, and
$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$.

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \ (\mathrm{mod}\ 4)}$ or $\boldsymbol{n^2 \equiv 1 \ (\mathrm{mod}\ 4)}$

Case 1 (n is even): Done.

Case 2 (n is odd):

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod 4}$ or $\boldsymbol{n^2 \equiv 1 \pmod 4}$

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like
$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

Case 1 (n is even): Done.

Case 2 (n is odd):

Suppose n is odd.
Then, $n = 2k + 1$ for some integer k.
So, $n^2 = (2k + 1)^2$
$= 4k^2 + 4k + 1$
$= 4(k^2 + k) + 1$.
So, by definition of congruence,
we have $n^2 \equiv 1 \pmod 4$.

Result follows by proof by cases since n is either even or odd