

**CSE
31F**

Foundations of Computing I

* All slides are a combined effort between
previous instructors of the course

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a \in \mathbb{Z}, b \in \mathbb{Z}, m \in \mathbb{Z}$:

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

Check Your Understanding. What do each of these mean?

When are they true?

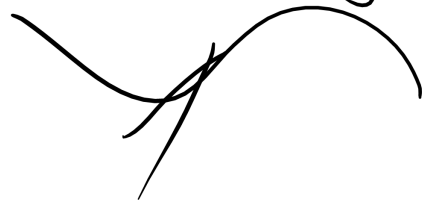
$$A \equiv 0 \pmod{2} \leftrightarrow 2 \mid A \leftrightarrow A = 2k$$

for some
 $k \in \mathbb{Z}$

$$\leftrightarrow \text{Even}(A)$$

for some $k \in \mathbb{Z}$

See handout
for a reminder
of the
definition



$$A \equiv -1 \pmod{17}$$

$$\leftrightarrow 17 \mid (A - (-1)) \leftrightarrow A + 1 = 17k$$

for some $k \in \mathbb{Z}$

Modular Arithmetic

Definition: “a is congruent to b modulo m”

For $a \in \mathbb{Z}, b \in \mathbb{Z}, m \in \mathbb{Z}$:

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

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

$$A \equiv 0 \pmod{2}$$

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

$$1 \equiv 0 \pmod{4}$$

This statement is false. If we take it mod **1** instead, then the statement is true.

$$A \equiv -1 \pmod{17}$$

If $A = 17x - 1 = 17x + 16$, then it works.

Note that $(m - 1) \pmod{m} = ((m \pmod{m}) + (-1 \pmod{m})) \pmod{m}$
 $= (0 + -1) \pmod{m} = -1 \pmod{m}$

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?

$$5 \mid 1$$

$$5 \mid 1 \text{ iff } 1 = 5k$$

$$25 \mid 5$$

$$25 \mid 5 \text{ iff } 5 = 25k$$

$$5 \mid 5$$

$$5 \mid 5 \text{ iff } 5 = 5k$$

$$3 \mid 2$$

$$3 \mid 2 \text{ iff } 2 = 3k$$

$$1 \mid 5$$

$$1 \mid 5 \text{ iff } 5 = 1k$$

$$5 \mid 25$$

$$5 \mid 25 \text{ iff } 25 = 5k$$

$$0 \mid 1$$

$$0 \mid 1 \text{ iff } 1 = 0k$$

$$2 \mid 3$$

$$2 \mid 3 \text{ iff } 3 = 2k$$

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}^+$:

Then, there exists *unique* integers q, r with $0 \leq r < d$ such that $a = dq + r$.

To put it another way, if we take a/d , we get a dividend

and a remainder: $q = a \text{ div } d$ $r = a \text{ mod } d$

```
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: $r \geq 0$ even if $a < 0$.
Not quite the same as $a \% d$.

Arithmetic, mod 7

$$a +_7 b = (a + b) \bmod 7$$

$$a \times_7 b = (a \times b) \bmod 7$$

+	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

This Course So Far

Framework for Reasoning:

Logic \rightarrow More Logic \rightarrow More More Logic \rightarrow Proofs

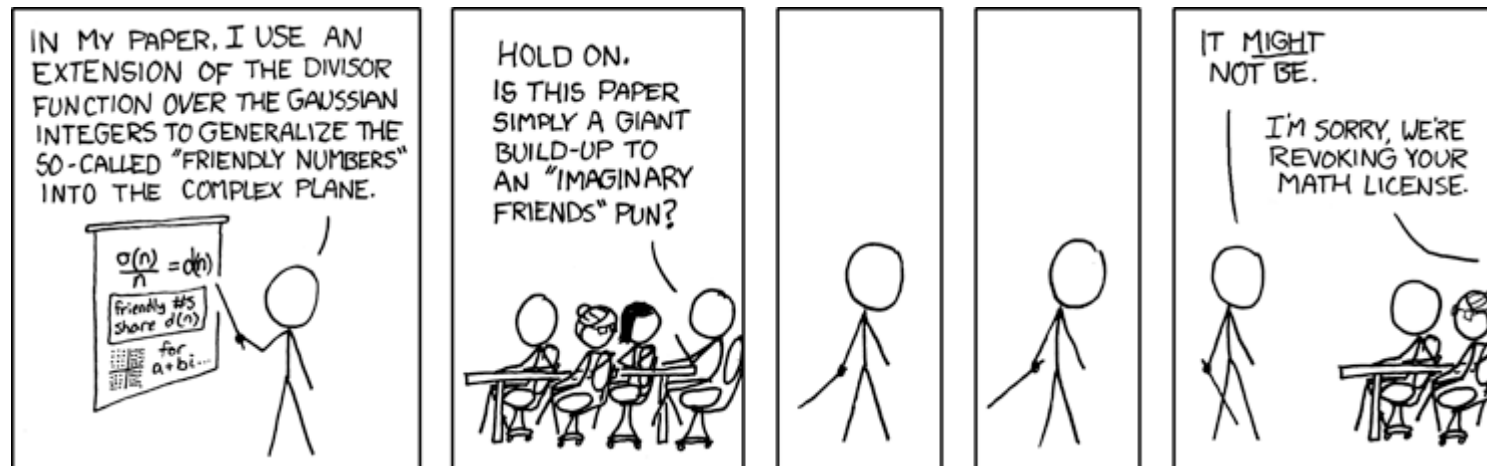
Things to Reason About

Number Theory

Sets (more more more logic...?)

CSE 311: Foundations of Computing

Lecture 11: Modular Arithmetic and Applications



Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer. Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

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

By def. of \equiv , $m \mid (a-b)$.

By def of \mid , $km = a-b$ for some $k \in \mathbb{Z}$.

Take both sides mod m : $a \bmod m = (km + b) \bmod m$

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

By div. thm.

$$a = my + (a \bmod m)$$

$$b = mz + (b \bmod m)$$

$$a - b = m(y - z) + (a \bmod m) - (b \bmod m)$$

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



Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer. Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

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:

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

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

By the division theorem, $a = mq + (a \bmod m)$ and

$$b = ms + (b \bmod m) \text{ for some integers } q, s.$$

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

$$= m(q - s) + (a \bmod m - b \bmod m)$$

$$\equiv m(q - s) \text{ since } a \bmod m = b \bmod m$$

Therefore, $m \mid (a - b)$ and so $a \equiv b \pmod{m}$.

Modular Arithmetic: Another Property

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

Suppose $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$.

By def. of \equiv , $m \mid (a-b)$
 $m \mid (c-d)$

By def. of \mid , $a-b = km$

$\Rightarrow (a+c) - (b+d) = (k+l)m$
So by def of \mid , we have $m \mid ((a+c) - (b+d))$.
So, $a+c \equiv b+d \pmod{m}$

Modular Arithmetic: Another Property

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

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. 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 $a + c \equiv b + d \pmod{m}$.

Modular Arithmetic: Another-nother Property

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

Suppose $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$
 Arith def $\left\{ \begin{array}{l} \lfloor m \rfloor (a-b) \\ \text{divides} \end{array} \right.$ def of Cong.
 Arith def
 { logic
 Arith def
 Arith def $\left\{ \begin{array}{l} \text{So,} \\ ac \equiv bd \pmod{m} \end{array} \right.$

Modular Arithmetic: Another-nother Property

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

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. 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 $ac = (km + b)(jm + d) = \cancel{kjm^2} + \cancel{kmd} + \cancel{jmb} + bd.$ $\text{mod } m$

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

Example

Let n be an integer.

Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Let's start by looking at a small example:

$$\begin{array}{l} 0^2 = 0 \equiv 0 \pmod{4} \\ 1^2 = 1 \equiv 1 \pmod{4} \\ 2^2 = 4 \equiv 0 \pmod{4} \\ 3^2 = 9 \equiv 1 \pmod{4} \\ 4^2 = 16 \equiv 0 \pmod{4} \end{array}$$

Example

Let n be an integer.

Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Case 1 (n is even):

Let's start by looking at a small example:

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

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

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

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

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

Suppose n is even.

~~$\{ \Rightarrow n = 2m$ for some $m \in \mathbb{Z}$
 \rightarrow so $n^2 = (2m)^2 = 4m^2$. So, $4 | n^2$.~~

~~$\left[\text{So, } n^2 \equiv 0 \pmod{4} \right]$~~

Case 2 (n is odd):

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 n be an integer.

Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Case 1 (n is even):

Suppose $n \equiv 0 \pmod{2}$.

Then, $n = 2k$ for some k .

So, $n^2 = (2k)^2 = 4k^2$. So, by definition of congruence, $n^2 \equiv 0 \pmod{4}$.

Case 2 (n is odd):

Suppose $n \equiv 1 \pmod{2}$.

Then, $n = 2k + 1$ for some k .

So, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. So, by definition of congruence, $n^2 \equiv 1 \pmod{4}$.

Let's start by looking at 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

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

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

n-bit Unsigned Integer Representation

- Represent integer x as sum of powers of 2:

If $x = \sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0,1\}$

then representation is $b_{n-1} \dots b_2 b_1 b_0$

$$99 = 64 + 32 + 2 + 1$$

$$18 = 16 + 2$$

Handwritten expansion of 125 in base 10:

$$1 \times 10^2 + 2 \times 10^1 + 5 \times 10^0$$

- For $n = 8$:

99: 0110 0011

18: 0001 0010

Handwritten expansion of 11 in base 2:

$$(11)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Sign-Magnitude Integer Representation

n-bit signed integers

Suppose $-2^{n-1} < x < 2^{n-1}$

First bit as the sign, n-1 bits for the value

$$99 = 64 + 32 + 2 + 1$$

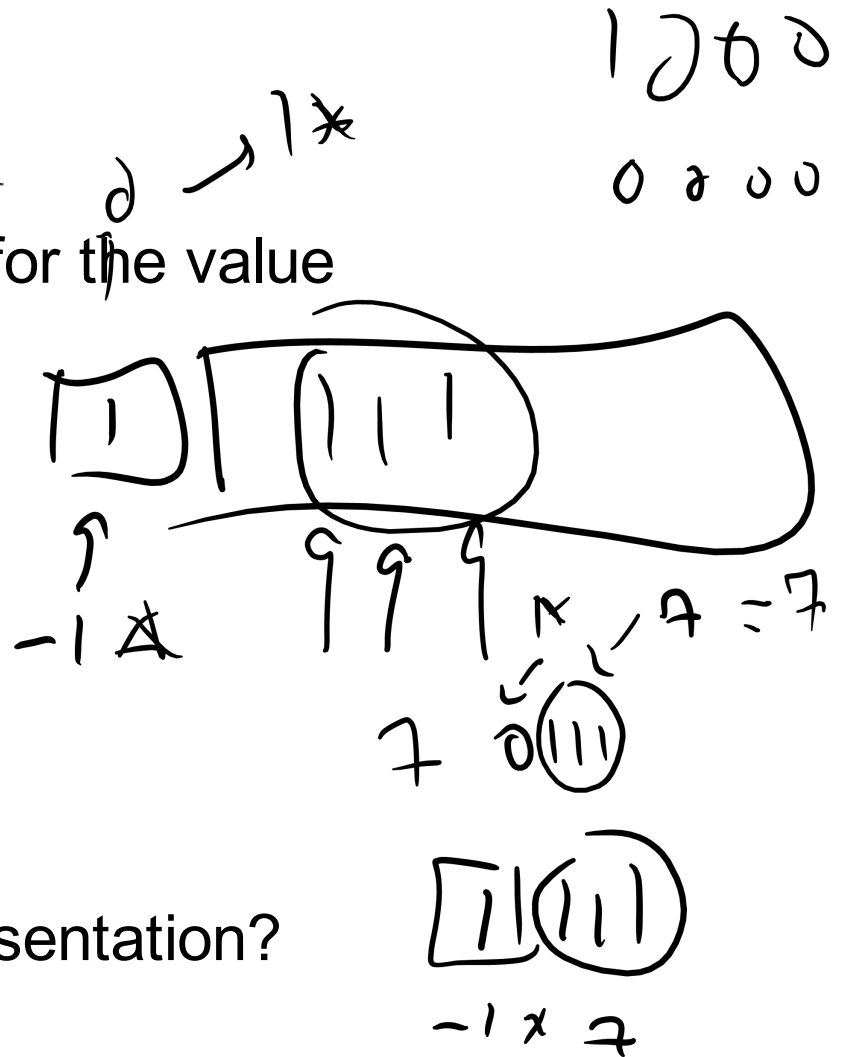
$$18 = 16 + 2$$

For n = 8:

$$99: \quad 0110 \quad 0011$$

$$-18: \quad 1001 \quad 0010$$

Any problems with this representation?



Two's Complement Representation

n bit signed integers, first bit will still be the sign bit

Suppose $0 \leq x < 2^{n-1}$,

x is represented by the binary representation of x

Suppose $0 \leq x \leq 2^{n-1}$,

$-x$ is represented by the binary representation of $2^n - x$

Key property: Two's complement representation of any number y is equivalent to $y \bmod 2^n$ so arithmetic works mod 2^n

$$99 = 64 + 32 + 2 + 1$$

$$18 = 16 + 2$$

For $n = 8$:

$$99: \quad 0110\ 0011$$

$$-18: \quad 1110\ 1110$$

Sign-Magnitude vs. Two's Complement

-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
1111	1110	1101	1100	1011	1010	1001	0000	0001	0010	0011	0100	0101	0110	0111

Sign-bit

-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111

Two's complement