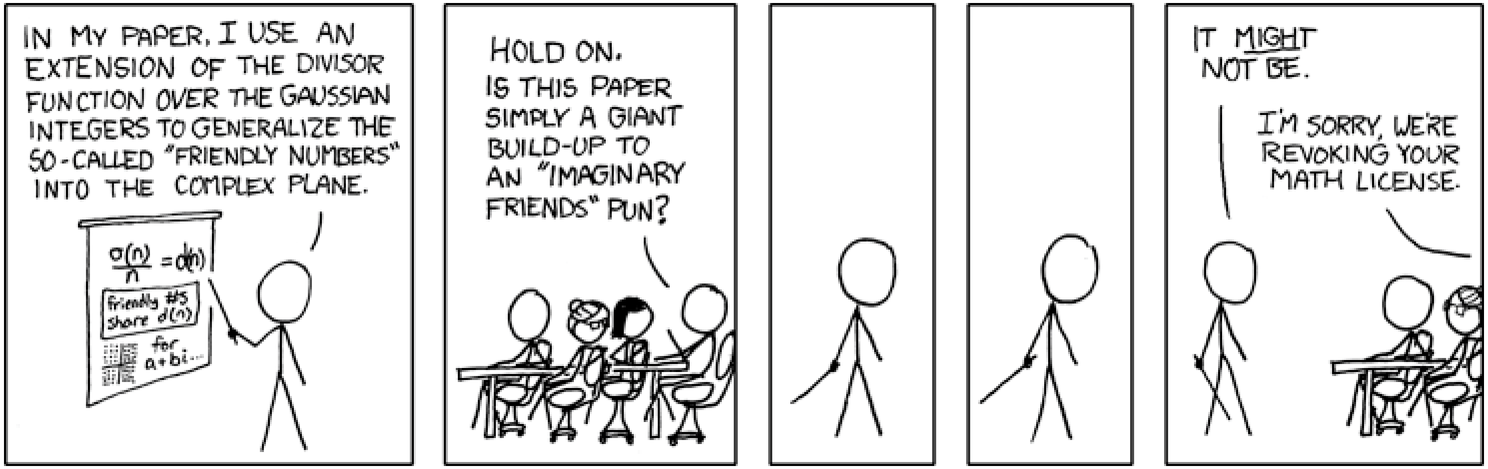
CSE 311: Foundations of Computing

Lecture 11: Modular Arithmetic and Applications



Divisibility

$a|b \leftrightarrow \exists k \quad b = ka$

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?

$5 \mid 1$	$25 \mid 5$	$5 \mid 0$	$3 \mid 2$
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
$1 \mid 5$	$5 \mid 25$	$0 \mid 5$	$2 \mid 3$
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Division Theorem

$a = -17 \quad d = 4$

$q = -5 \quad r = 3 \quad -17 = d \cdot (-5) + 3$

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 $a = dq + r$.

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

$a = dq + r$

$0 \leq r \leq d - 1$

$a = +17 \quad d = 4$

$+17 = d \cdot \underbrace{4}_{q} + \underbrace{1}_{r}$

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 $a = dq + r$.

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*

```
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`.

Arithmetic, mod 7

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

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

$6 \times 3 = 4$

$5 + 4 = 2$

$2 \times 6 = 5$

+	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 $m > 0$

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

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

x ≡ 0 (mod 2) $2 \mid x - 0$ $2 \mid x$

x is even.

-1 ≡ 19 (mod 5) $5 \mid -1 - 19 = -20$

true

y ≡ 2 (mod 7) $7 \mid y - 2$ $y = 7k + 2$

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

$\Rightarrow$
$\Leftarrow$

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

$m \mid a-b$ by definition of cong —

So $a-b = km$ for some integer k.

$a = b + km$. Take both sides mod m.

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

Conclusion $a \bmod m = b \bmod m$.

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

$a = m(a \text{ div } m) + a \bmod m$. by division Thm.

$b = m(b \text{ div } m) + b \bmod m$ by division Thm.

$a-b = m(a \text{ div } m - b \text{ div } m) + a \bmod m - b \bmod m = m(a \text{ div } m - b \text{ div } m)$.

$a-b = km$ for som k.

$m \mid a-b$

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

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

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

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

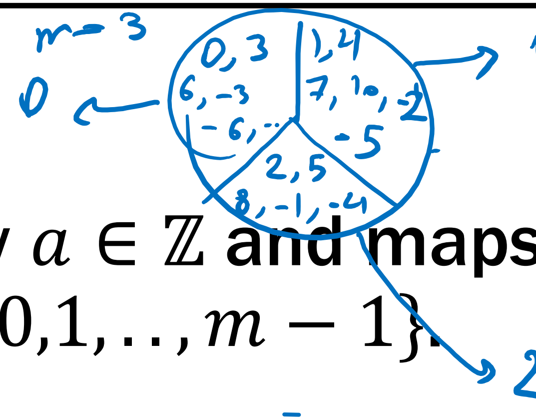
Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$

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

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

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

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



- What we have just shown
  - The $\mathrm{mod}\ m$ 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 $\mathrm{mod}\ m$ 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 $\mathrm{mod}\ m$ function has the same value on a and on b.

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

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 $\boldsymbol{a}+\boldsymbol{c} \equiv \boldsymbol{b}+\boldsymbol{d}\ (\mathbf{mod}\ \boldsymbol{m})$

pf. $m \mid a-b$ by def of cong

$a-b = km$ for some int k

$+$ $m \mid c-d$ by def of cong

$c-d = l \cdot m$ by def of div for some l.

$a+c-(b+d) = (\underbrace{k+l}_{n}) \cdot m$ by algebra.

$m \cdot n = a+c-(b+d)$ for some n.

$m \mid a+c-(b+d)$

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

Modular Arithmetic: Addition Property

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

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 $c - d = jm$.

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

Pf. $m \mid a-b$ by def of cong

$a-b = k \cdot m$ for some int k.

$m \mid c-d$ def of cong. $c-d = l \cdot m$ for som int l.

$a = b + km$

$c = d + lm$

multiply $ac = bd + blm + dkm + klm^2$

$$ac - bd = m(\underbrace{bl + dk + klm}_{n})$$

$ac - bd = n \cdot m$ for some int n.

$m \mid ac - bd$

$ac \equiv bd \mod m$

Modular Arithmetic: Multiplication Property

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

Suppose that $a \equiv b \pmod{m}$ 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 $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$.

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

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

Case 1 (n is even):

$n = 2k$ for some int k.

$n^2 = 4k^2$

$4 \mid n^2$

$n^2 \equiv 0 \pmod 4$.

Case 2 (n is odd):

$n = 2k+1$ for some int k

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k)+1$

$n^2 - 1 = 4(k^2 + k)$

$4 \mid n^2 - 1$

$n^2 \equiv 1 \pmod 4$.

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

$n \equiv 0 \pmod 2 \longrightarrow n^2 \equiv 0 \pmod 4$, and

$n \equiv 1 \pmod 2 \longrightarrow n^2 \equiv 1 \pmod 4$.

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):

Suppose $n \equiv 0 \pmod{2}$.
Then, $n = 2k$ for some integer 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 integer k.
So, $n^2 = (2k + 1)2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So, by definition of congruence, $n^2 \equiv 1 \pmod{4}$.

n-bit Unsigned Integer Representation

- Represent integer x as sum of powers of 2:

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

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

  99 = 64 + 32 + 2 + 1

  18 = 16 + 2

- For n = 8:

  99: 0110 0011

  18: 0001 0010

Sign-Magnitude Integer Representation

n-bit signed integers

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

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

99 = 64 + 32 + 2 + 1

18 = 16 + 2

For n = 8:

99: 0110 0011

-18: 1001 0010

Any problems with this representation?

Two's Complement Representation

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

Suppose that $0 \leq x < 2^{n-1}$,
x is represented by the binary representation of x

Suppose that $0 \leq x \leq 2^{n-1}$,
$-x$ is represented by the binary representation of $2^n - x$

Key property: Twos complement representation of any number $\boldsymbol{y}$ is equivalent to $\boldsymbol{y} \bmod \mathbf{2^n}$ so arithmetic works $\bmod \mathbf{2^n}$

99 = 64 + 32 + 2 + 1
18 = 16 + 2

For n = 8:
99: 0110 0011
-18: 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

Two's Complement Representation

- For $0 < x \leq 2^{n-1}$, $-x$ is represented by the binary representation of $2^n - x$
  - That is, the two's complement representation of any number y has the same value as y modulo 2^n.

- To compute this: Flip the bits of x then add 1:
  - All 1's string is $2^n - 1$, so

    Flip the bits of x $\equiv$ replace x by $2^n - 1 - x$

    Then add 1 to get $2^n - x$

Basic Applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher

Hashing

Scenario:

Map a small number of data values from a large domain $\{0, 1, \ldots, M-1\}$ …

…into a small set of locations $\{0,1, \ldots, n-1\}$ so one can quickly check if some value is present

- $\text{hash}(x) = x \bmod p$ for p a prime close to n
  - or $\text{hash}(x) = (ax + b) \bmod p$
- Depends on all of the bits of the data
  - helps avoid collisions due to similar values
  - need to manage them if they occur

Pseudo-Random Number Generation

Linear Congruential method

$$x_{n+1} = (a\, x_n + c) \bmod m$$

Choose random x_0, a, c, m and produce a long sequence of x_n's

Simple Ciphers

- **Caesar cipher**, A = 1, B = 2, . . .
  - HELLO WORLD
- **Shift cipher**
  - $f(p) = (p + k) \bmod 26$
  - $f^{-1}(p) = (p - k) \bmod 26$
- **More general**
  - $f(p) = (ap + b) \bmod 26$