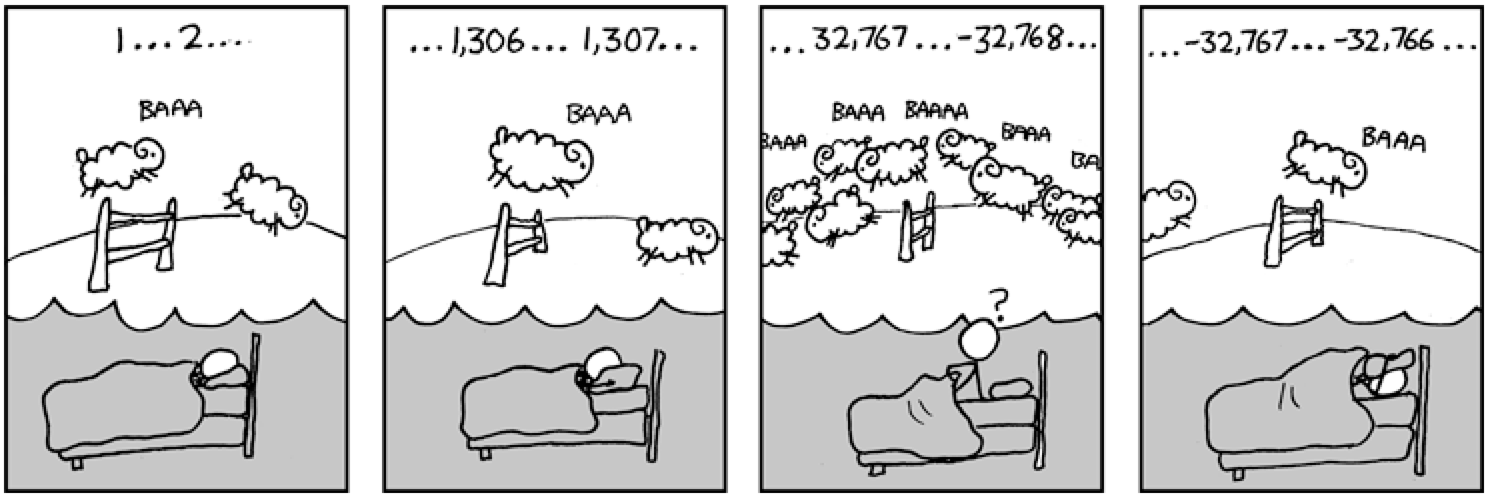
CSE 311: Foundations of Computing

Lecture 13: Number theory & modular arithmetic



Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing

- Many significant applications
  - Cryptography
  - Hashing
  - Security

- Important tool set

I’m ALIVE!

```
public class Test {
   final static int SEC_IN_YEAR = 364*24*60*60*100;
   public static void main(String args[]) {
      System.out.println(
         “I will be alive for at least ” +
         SEC_IN_YEAR * 101 + “ seconds.”
      );
   }
}
```

I’m ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            “I will be alive for at least ” +
            SEC_IN_YEAR * 101 + “ seconds.”
        );
    }
}
```

```
 ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

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

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
1 | 5	5 | 25	0 | 5	2 | 3

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?

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

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 $a = dq + r$.

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

Note: $r \geq 0$ even if $a < 0$.
Not quite the same as in Java

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** $q = a \textbf{ div } d$
and non-negative remainder $r = a \,\%\, d$

```
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 in Java

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) $\quad 2 \mid (x - 0) \equiv 2 \mid x$

$x \equiv 0$

-1 ≡ 19 (mod 5)

y ≡ 2 (mod 7)

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)

$5 \mid -1-19 \equiv 5 \mid -20 \equiv \exists k.\ -20 = 5k$

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

y ≡ 2 (mod 7)

$7 \mid y-2 \equiv \exists k.\ y-2 = 7k \equiv \exists k.\ y = 2+7k$

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.

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

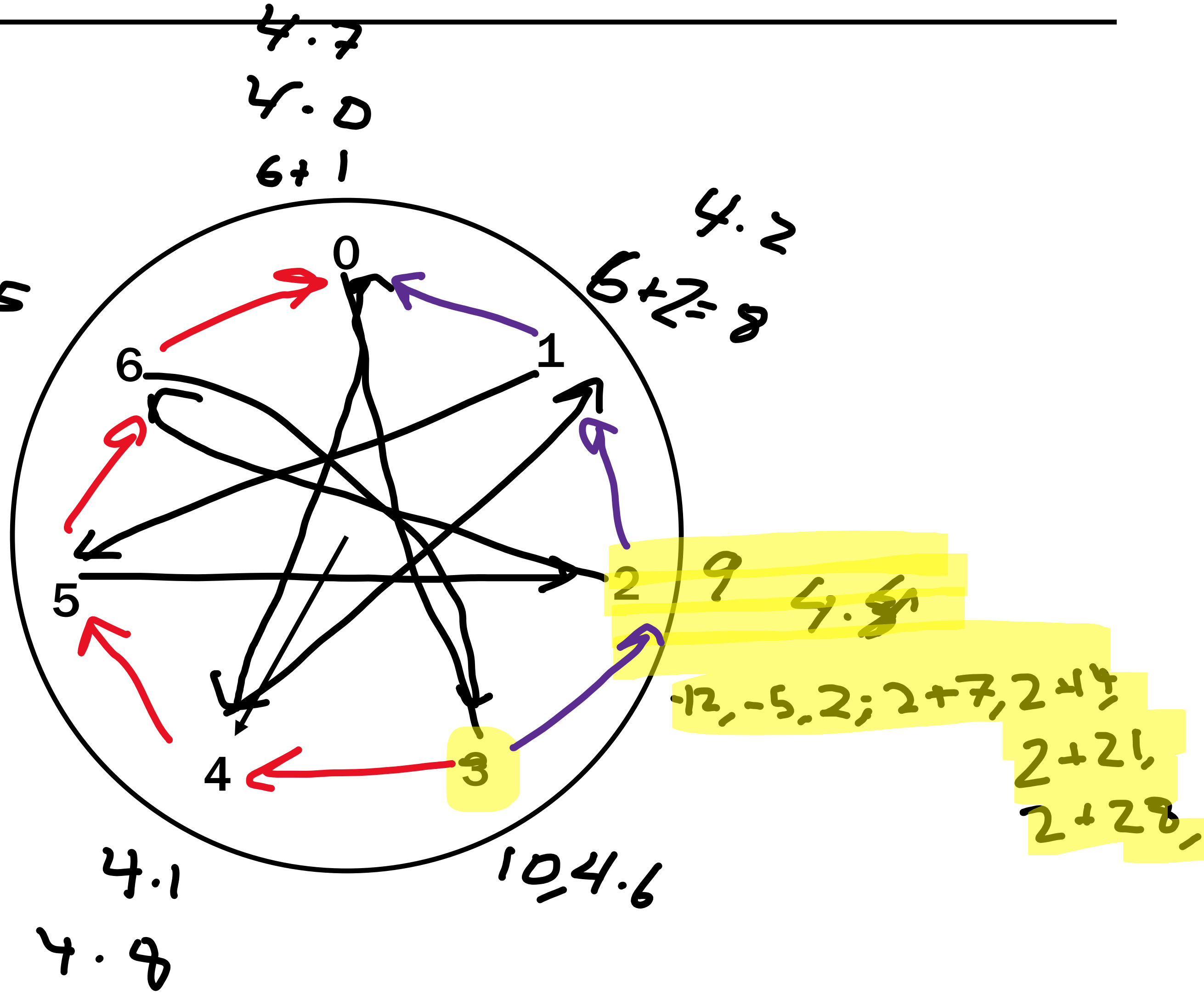
- % is a function (operator) with two arguments. The result is an integer
- ≡ … (mod m) is a predicate
  - "a is equivalent, modulo m, to b"
  - "a is equivalent to b (modulo m)"
  - $a \equiv b \pmod{m}$

Arithmetic, mod 7

4x

4.5

$1+5 \equiv 4\cdot 2+4 \equiv 4\cdot 3$
(mod 7)



Modular Arithmetic: A Property

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

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

Suppose that $a \,\%\, m = b \,\%\, m$.

Modular Arithmetic: A Property

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

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:

$$a \,\%\, m = (b + km) \,\%\, m = b \,\%\, m.$$

$\frac{b + km}{m}$

$b + km = qm + r$ 1

$b = (q - k)m + r$ 2

Suppose that $a \,\%\, m = b \,\%\, m$.

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

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

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

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

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

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

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

- What we have just shown
  - The $\% \, m$ function takes any $a \in \mathbb{Z}$ and maps it to a remainder $a \,\%\, m \in \{0,1,..,m-1\}$.

  - Imagine grouping together all integers that have the same value of the $\% \, m$ 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 $\% \, m$ 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 $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ and $\boldsymbol{b} \equiv \boldsymbol{c} \pmod{\boldsymbol{m}}$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \pmod{\boldsymbol{m}}$

Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.
Then, by the previous property, we have
$a \,\%\, m = b \,\%\, m$ and $b \,\%\, m = c \,\%\, m$.

Putting these together, we have $a \,\%\, m = c \,\%\, m$,
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 $\boldsymbol{a} \equiv \boldsymbol{b} \ (\mathbf{mod}\ \boldsymbol{m})$ and $\boldsymbol{c} \equiv \boldsymbol{d} \ (\mathbf{mod}\ \boldsymbol{m})$, then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \ (\mathbf{mod}\ \boldsymbol{m})$

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

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 $ac \equiv bd \pmod{m}$.

Lecture 13 Activity

You will be assigned to breakout rooms. Please:

- Introduce yourself
- Choose someone to share their screen, showing this PDF
- Consider the statement:

For all $a, b, c, m \in \mathbb{Z}, m > 0$ *one has*

$$a \equiv b \pmod{m} \rightarrow a + c \equiv b + c \pmod{m}.$$

- Discuss what the statement means.
- Prove the statement.

Definition: "a is congruent to b modulo m"

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

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

Fill out the poll everywhere for Activity Credit!
Go to pollev.com/philipmg and login with your UW identity

Definition: "a divides b"

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

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

Lecture 13 Activity

You will be assigned to breakout rooms. Please:

- Introduce yourself
- Choose someone to share their screen, showing this PDF
- Consider the statement:

For all $a, b, c, m \in \mathbb{Z}, m > 0$ *one has*

$$a \equiv b \pmod{m} \rightarrow a + c \equiv b + c \pmod{m}.$$

<u>Proof.</u>

Let $a, b, c \in \mathbb{Z}$ be arbitrary and let $m > 0$.
Assume that $a \equiv b \pmod{m}$.
Then $m \mid a - b$ and hence there is an integer x with $mx = a - b$.
Then $(a + c) - (b + c) = a - b = mx$ and so $m \mid (a + c) - (b + c)$.
Then $a + c \equiv b + c \pmod{m}$ by definition of mod.

Definition: "a is congruent to b modulo m"

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

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

Definition: "a divides b"

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

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

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 $\boldsymbol{n^2 \equiv 0 \ (\mathbf{mod}\ 4)}$ or $\boldsymbol{n^2 \equiv 1 \ (\mathbf{mod}\ 4)}$

Case 1 (n is even):

Suppose n is even.
Then, $n = 2k$ for some integer k.
So, $n^2 = (2k)2 = 4k^2$.
So, by 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

$n \equiv 0 \pmod 2 \longrightarrow n^2 \equiv 0 \pmod 4$, 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 $\boldsymbol{n^2 \equiv 1 \pmod 4}$

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:

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

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 the earlier property of mod,
we have $n^2 \equiv 1 \pmod 4$.

It looks like
n ≡ 0 (mod 2) ⟶ n^2 ≡ 0 (mod 4), and
n ≡ 1 (mod 2) ⟶ n^2 ≡ 1 (mod 4).

Result follows by "proof by cases": n is either even or not even (odd)

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 $b_{n-1} \ldots b_2\, b_1\, b_0$

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 $\boldsymbol{y}, \mathbf{mod}\ \mathbf{2^n}$ so arithmetic works $\mathbf{mod}\ \mathbf{2^n}$

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

- $\text{hash}(x) = x \;\%\; p$ for p a prime close to n
  - or $\text{hash}(x) = (ax + b)\% \; p$
- 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

$$x_{n+1} = (ax_n + c)\ \%\ m$$

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**
  - $f(p) = (p + k) \% 26$
  - $f^{-1}(p) = (p - k) \% 26$
- **More general**
  - $f(p) = (ap + b) \% 26$