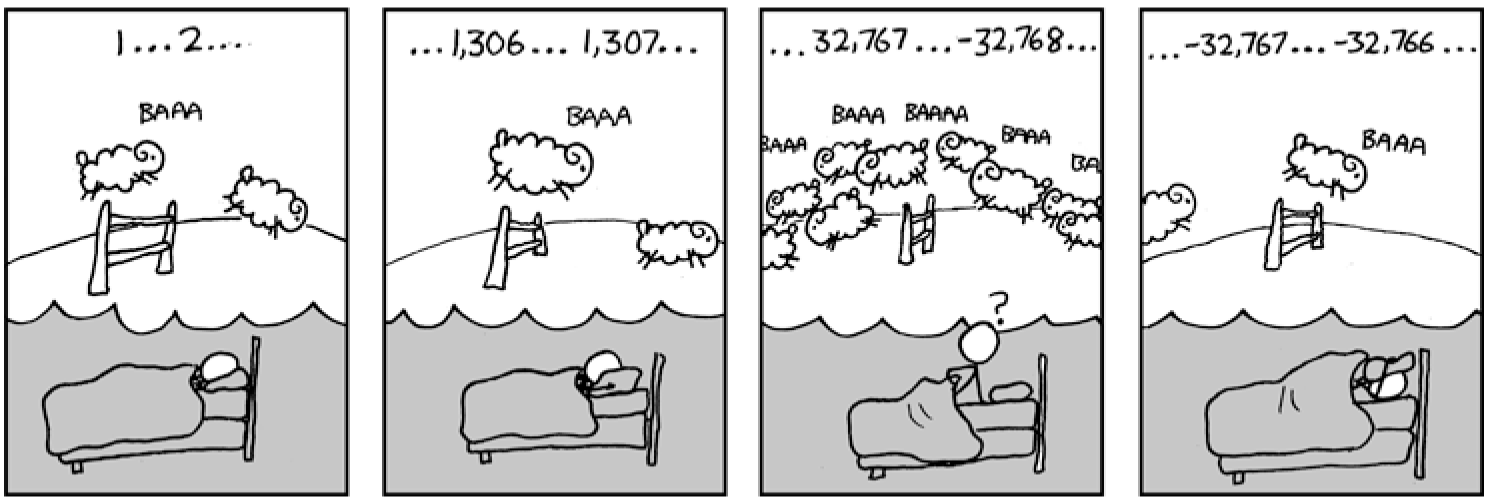
CSE 311: Foundations of Computing

Lecture 11: Modular Arithmetic, Applications and Factoring



Please pick up solns
for HW3

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

Last Class: Division Theorem

Division Theorem

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

To put it another way, if we divide *d* **into** *a*, **we get a unique quotient** $\boxed{q = a \text{ div } \cancel{d}}$ m
and non-negative remainder $\boxed{r = a \text{ mod } \cancel{d}}$ m

```
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`**.

Last Class: 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

Last Class: Modular Arithmetic

Definition: "a is congruent to b modulo m"

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

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

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 $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

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

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, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + \underbrace{(a \bmod m - b \bmod m)}_{=0}$
$= m(q - s)$ since $a \bmod m = b \bmod m$

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

Last Class: $\bmod m$ function vs $\equiv \pmod{m}$ 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: Addition 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 $c \equiv d \pmod{m}$

$m \mid (c-d)$

$\therefore \exists$ integer k, l s.t.

$m \mid (a-b)$

$a - b = km$ and $c - d = lm$

$\therefore a = b + km$ and $c = d + lm$

$\therefore a + c = b + d + km + lm = b + d + (k+l)m$

$\therefore (a+c) - (b+d) = (k+l)m$

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

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

by defn

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 $a \equiv b \pmod m$ 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: Multiplication Property

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

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

$\therefore a = b + km$ and $c = d + lm$ for some integers k, l,

$$a \cdot c = (b + km)(d + lm)$$
$$= b \cdot d + blm + kmd + klm^2$$
$$= b \cdot d + m(\underbrace{bl + kd + klm}_{\text{integer}})$$

$$ac - bd = m(bl + kd + klm)$$

$\therefore m \mid (ac - bd)$ $\therefore ac \equiv bd \pmod{m}$ $\blacksquare$

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

Let's start by looking a a small example:

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

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

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

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

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

Any integer n is either even or odd. $\equiv 0 \pmod{2}$ $\equiv 1 \pmod{2}$

Case 1 n is even

$\therefore n = 2k$ for some integer k

$\therefore n^2 = 4k^2 \quad \therefore n^2 \equiv 0 \pmod{4}$ ✓

Case 2 n is odd

$\therefore n = 2l+1$ for some integer l

$\therefore n^2 = (2l+1)^2 = 4l^2 + 4l + 1$

$= 4(l^2 + l) + 1$ ✓

$\therefore n^2 \equiv 1 \pmod{4}$

~~Both cases its true~~

∎

Example

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

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):

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 2 (n is odd):

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:

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

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

  99 = 64 + 32 + 2 + 1

  18 = 16 + 2

- For n = 8:

  128 64 32 16, 8 4 2 1

  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

2^n n+1 bit

99 = 64 + 32 + 2 + 1

18 = 16 + 2

-0

For n = 8:

99: 0110 0011

-18: 1001 0010

$+0$

Any problems with this representation?

18

-18

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 $\mathbf{mod}$ $\mathbf{2^n}$

-2^{n-1} $2^{n-1}-1$

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

18 0001 0010
-18 1110 1110
1 0000 0000

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	9	10	11	12	13	14	15								
-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

mod 16

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.

$\underbrace{11111111}_{+1}$ $(2^n - 1) - x$

- 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 $2^n - x$

$$\begin{array}{rr} & 11111111 \\ x & 01101110 \\ \hline & 10010001 \end{array}$$

Basic Applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher

These applications work well because of how we can solve equations involving mods

– To understand that we need a bit more number theory…

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

- $\text{hash}(x) = (ax + b) \bmod p$ for a prime p close to n and values a and b

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**
  - $f(p) = (ap + b) \bmod 26$

Primality

An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.

A positive integer that is greater than 1 and is not prime is called *composite*.

Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization

48 = 2 • 2 • 2 • 2 • 3
591 = 3 • 197
45,523 = 45,523
321,950 = 2 • 5 • 5 • 47 • 137
1,234,567,890 = 2 • 3 • 3 • 5 • 3,607 • 3,803

Euclid's Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

$p_1 p_2 p_3 \cdots p_n$ is divisible by all

$p_1 p_2 \cdots p_n + 1$

Case 1 $p_1 p_2 \cdots p_n + 1$ is prime ✓

new

Euclid's Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

Define the number $P = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$ and let

$$Q = P + 1.$$

Euclid's Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

Define the number $P = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$ and let

$$Q = P + 1.$$

Case 1: Q is prime: Then Q is a prime different from all of $p_1, p_2, \ldots, p_n$ since it is bigger than all of them.

Case 2: Q is composite

∎

Euclid's Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

Define the number $P = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$ and let

$$Q = P + 1.$$

Case 1: Q is prime: Then Q is a prime different from all of $p_1, p_2, \ldots, p_n$ since it is bigger than all of them.

Case 2: $Q > 1$ is not prime: Then Q has some prime factor p (which must be in the list). Therefore $p|P$ and $p|Q$ so $p|(Q - P)$ which means that $p|1$.

impossible

Both cases are contradictions so the assumption is false. ∎

Famous Algorithmic Problems

$\sqrt{n}$

- Primality Testing
  - Given an integer n, determine if n is prime
- Factoring
  - Given an integer n, determine the prime factorization of n

Factoring

Factor the following 232 digit number [RSA768]:

1230186684530117755130494958384962720772
8535695953347921973224521517264005072636
5751874520219978646938995647494277406384
5925192557326303453731548268507917026122
1429134616704292143116022212404792747377
9408066535141959745985690214 3413

1230186684530117755130494958384962720772853569595334 7
9219732245215172640050726365751874520219978646938995 6
4749427740638459251925573263034537315482685079170261 2
2142913461670429214311602221240479274737794080665351 4
19597459856902143413

=

3347807169895689878604416984821269081770479498 37
1376856891243138898288379387800228761471165253 17
430877378144679994 89

×

3674604366679959042824463379962795263227915816 43
4308764267603228381573966651127923337341714339 68
102700927987363089 17

Greatest Common Divisor

GCD(a, b):

Largest integer d such that $d \mid a$ and $d \mid b$

- GCD(100, 125) = 25
- GCD(17, 49) = 1
- GCD(11, 66) = 11
- GCD(13, 0) = 13
- GCD(180, 252) = 36

$3 \cdot 6 \cdot 5 \cdot 2$

$3 \cdot 84$

$3 \cdot 2 \cdot 42$

$\underline{3 \cdot 2} \cdot 6 \cdot 7$

GCD and Factoring

$a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46{,}200$

$b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204{,}750$

$$GCD(a, b) = 2^{\min(3,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(2,3)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} \cdot 13^{\min(0,1)}$$

Factoring is expensive!

Can we compute GCD(a,b) without factoring?

Useful GCD Fact

If a and b are positive integers, then

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

Useful GCD Fact

If *a* and *b* are positive integers, then
gcd(*a*,*b*) = gcd(*b*, *a* mod *b*)

Proof:
By definition of mod, $a = qb + (a \bmod b)$ for some integer $q = a \operatorname{div} b$.

Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$ so $a = kd$ and $b = jd$ for some integers k and j.

Therefore $(a \bmod b) = a - qb = kd - qjd = (k - qj)d$.
So, $d|(a \bmod b)$ and since $d|b$ we must have $d \leq \gcd(b, a \bmod b)$.

Now, let $e = \gcd(b, a \bmod b)$. Then $e|b$ and $e\,|(a \bmod b)$ so $b = me$ and $(a \bmod b) = ne$ for some integers m and n.

Therefore $a = qb + (a \bmod b) = qme + ne = (qm + n)e$.
So, $e|a$ and since $e|b$ we must have $e \leq \gcd(a, b)$.

It follows that $\gcd(a, b) = \gcd(b, a \bmod b)$. ■

Another simple GCD fact

If a is a positive integer, gcd(a,0) = a.