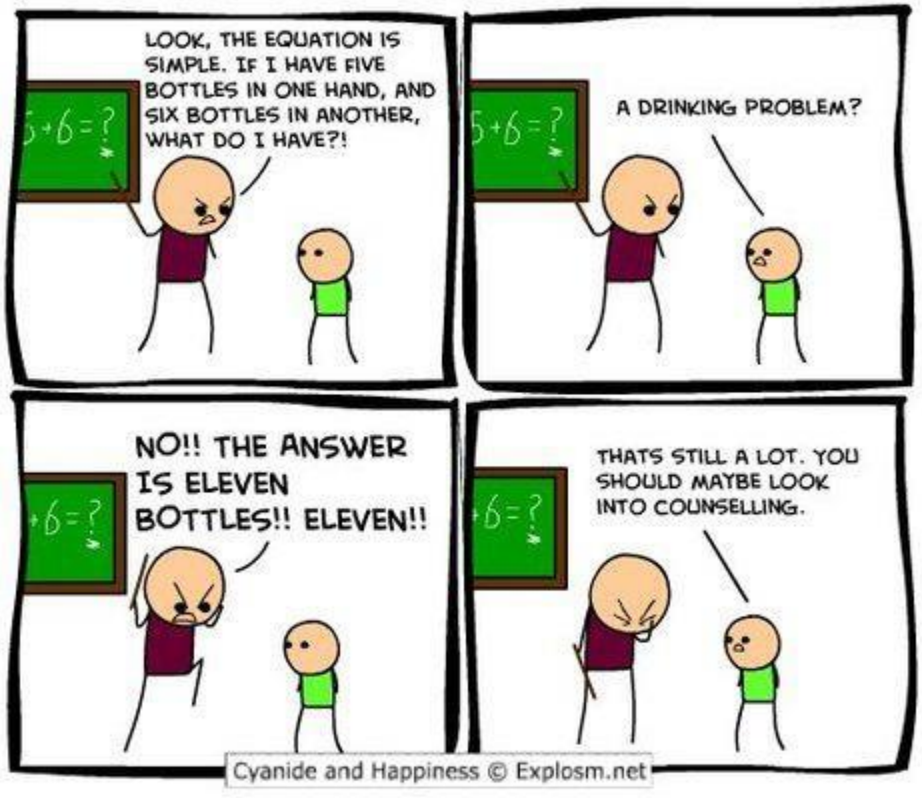
Fall 2015

Lecture 14: Modular congruences



If a and b are positive integers, then
$$\gcd(a,b) = \gcd(b, a \bmod b)$$

$gcd(10,12) = gcd(10,2)$

Proof:

mod $d=0$ mod $d=0$

By definition $a = (a \text{ div } b)\cdot b + (a \bmod b)$

If $d \mid a$ and $d \mid b$ then $d \mid (a \bmod b)$. $C \subseteq D$

If $d \mid b$ and $d \mid (a \bmod b)$ then $d \mid a$. $D \subseteq C$

$C = \{d : d \mid a, d \mid b\}$ $D = \{d : d \mid b, d \mid a \bmod b\}$

$C \subseteq D$
$D \subseteq C$ $\rightarrow$ $C = D$

$\max\{d \in C\} = \max\{d \in D\}$
$gcd(a,b) = gcd(b, a \bmod b)$

Euclid's Algorithm

GCD(x, y) = GCD(y, x mod y)

```
int GCD(int a, int b){ /* a >= b, b > 0 */
    int tmp;
    while (b > 0) {
        tmp = a % b;
        a = b;
        b = tmp;
    }
    return a;
}
```

a, b

new a = b

new b = a mod b.

gcd(12,10)

a=12, b=10

a=10, b=2

a=2, b=0

returns 2.

Example: GCD(660, 126)

Goal: Solve $ax \equiv b \pmod{m}$ for unknown x.

Idea: Find a number z such that $za \equiv 1 \pmod{m}$.

Multiply both sides by z:

$$ax \equiv b \pmod{m}$$

$$\underbrace{za}_{\equiv 1}x \equiv zb \pmod{m}$$

$$x \equiv zb \pmod{m}$$

$3x = 4 \bmod 7$

$3^{-1} = 5$

$3 \cdot 5 \equiv 1 \bmod 7$

$5 \cdot 3x \equiv 4 \cdot 5 \equiv 6 \bmod 7$

$x \equiv 6 \bmod 7$

If such an element exists, we use the notation a^{-1} so that

$$a^{-1}a \equiv aa^{-1} \equiv 1 \pmod{m}$$

a^{-1} is called the **multiplicative inverse of a modulo m.**

Theorem: a has a multiplicative inverse modulo m **if and only if** $\gcd(a, m) = 1$.

only if part is easy

if $\gcd(a, m) \neq 1$ then a may not have multiplicative inverse

suppose $a = 2$
$m = 4$

2^{-1} doesn't exist

$2x \equiv 1 \mod 4$.

no answer

$$\boxed{\text{If } \gcd(a, m) = 1 \rightarrow a^{-1} \text{ exists}}$$

Bezout's Theorem

If *a* and *b* are positive integers, then there exist integers ***s*** and ***t*** such that

gcd*(a,b)* = ***sa*** + ***tb***

For example: $1 = \gcd(27,35) = \underbrace{\underbrace{13}_{s} \cdot 27}_{351} + \underbrace{\underbrace{(-10)}_{t} \cdot 35}_{350} = 1$

If $\gcd(a,m) = 1$ then we can write

$$1 = \gcd(a,m) = sa + tm \equiv sa \bmod m$$

$sa \equiv 1 \bmod m$

for some integers s, t.

So $sa \equiv 1 \pmod{m}$.

Thus $a^{-1} = s$ is the inverse!

extended Euclidean algorithm

$\gcd(35,27) = (-10)\cdot 35 + 13\cdot 27$

$13 = 27^{-1} \bmod 35$

- Can use Euclid's Algorithm to find s, t such that

  $\gcd(a,b) = sa + tb$

- e.g. gcd(35,27):

	$35 = 1 \cdot 27 + 8$	$35 - 1 \cdot 27 = 8$
$= \gcd(27,8)$	$27 = 3 \cdot 8 + 3$	$27 - 3 \cdot 8 = 3$
$= \gcd(8,3)$	$8 = 2 \cdot 3 + 2$	$8 - 2 \cdot 3 = 2$
$= \gcd(3,2)$	$3 = 1 \cdot 2 + 1$	$3 - 1 \cdot 2 = \underline{\underline{1}}$
$= \gcd(2,1)$	$2 = 2 \cdot 1 + 0$	
$= \gcd(1,0) = 1$		

- Substitute back from the bottom

$$1 = 3 - 1 \cdot 2 \quad = 3 - 1\,(8 - 2 \cdot 3) \quad = (-1) \cdot 8 + 3 \cdot 3$$

$$= (-1) \cdot 8 + 3\,(27 - 3 \cdot 8) \quad = 3 \cdot 27 + (-10) \cdot 8$$

$$= 3 \cdot 27 + (-10) \cdot (35 - 1 \cdot 27) \quad = -10 \cdot 35 + 13 \cdot 27$$

$13 \cdot 27 \equiv 1 \mod 35$

Solving $ax \equiv b \pmod{m}$ for unknown x when $\gcd(a, m) = 1$.

1. Find s such that $sa + tm = 1$
2. Compute $a^{-1} = s \bmod m$, the multiplicative inverse of a modulo m
3. Set $x = (a^{-1} \cdot b) \bmod m$

$$x \equiv a^{-1} b \mod m$$

$$ax \equiv a(a^{-1} b) \mod m$$

$$\equiv (a a^{-1}) b \mod m$$

$$\equiv b \mod m$$

$15 \cdot 7x \equiv 15 \cdot 3 = 45 \mod 26$

$\boxed{x \equiv 45 \equiv 19 \mod 26}$

example

Solve: $7x \equiv 3 \pmod{26}$

$\gcd(26, 7)$ $\quad 26 = 3 \cdot 7 + 5 \quad 5 = 26 - 3 \cdot 7$

$= \gcd(7, 5)$ $\quad 7 = 1 \cdot 5 + 2 \quad 2 = 7 - 1 \cdot 5$

$= \gcd(5, 2)$ $\quad 5 = 2 \cdot 2 + 1 \quad 1 = 5 - 2 \cdot 2$

$= \gcd(2, 1)$ $\quad 2 = 2 \cdot 1 + 0$

$= \gcd(1, 0) = 1$

Find s, t, $s\,7 + t\,26 = 1$

$7^{-1} = -11 \equiv 15 \mod 26$

$$1 = 5 - 2 \cdot 2 = 5 + (-2)(7 - 1 \cdot 5)$$
$$= (-2)\,7 + 3 \cdot 5$$
$$= (-2)\,7 + 3 \cdot (26 - 3 \cdot 7)$$
$$= \underbrace{3}_{s} \cdot 26 + \underbrace{(-11)}_{t} \cdot 7$$

multiplicative cipher: $f(x) = ax \bmod m$

For a multiplicative cipher to be **invertible**:

$$f : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$$

$$f(x) = ax \bmod m$$

must be one-to-one and onto.

If m is prime
$\forall\ 0 \leq a \leq m-1$
$\gcd(a, m) = 1$
$\to f$ is one-to-one
onto

$\forall x \quad (a^{-1}(ax \bmod m)) \bmod m = x$

Lemma: If there is an integer b such that $ab \bmod m = 1$, then the function $f(x) = ax \bmod m$ is one-to-one and onto.

$x_1 = x_2$
$\uparrow$
$x_1 \equiv x_2 \bmod m$
$\uparrow$
$x_1 - x_2 \equiv 0 \bmod m$

Enough to show f is one-to-one.

$ax_1 \bmod m = a x_2 \bmod m$
$\downarrow$
$ax_1 \equiv a x_2 \bmod m \to$

$a(x_1 - x_2) \equiv 0 \bmod m$
$a^{-1}a(x_1 - x_2) \equiv 0 \bmod m$

could we prove this?

If *a* and *b* are positive integers, then there exist integers ***s*** and ***t*** such that

$$\gcd(a,b) = sa + tb$$

Need a **new inference rule**.

Method for proving statements about all integers ≥ 0

- A new logical inference rule!
  - It only applies over the natural numbers
  - The idea is to **use** the special structure of the naturals to prove things more easily
- Particularly useful for reasoning about programs!

```
for(int i=0; i < n; n++) { … }
```

  - Show P(i) holds after i times through the loop

```
public int f(int x) {
    if (x == 0) { return 0; }
        else { return f(x-1)+1; }}
```

  - $f(x) = x$ for all values of $x \geq 0$ naturally shown by induction.

prove: for all $n > 0$, a is odd $\rightarrow a^n$ is odd

Let $n > 0$ be arbitrary.

Suppose that a is odd. We know that if a, b are odd, then ab is also odd.

So: $(\cdots \cdot ((a \cdot a) \cdot a) \cdot \cdots \cdot a) = a^n$ [n times]

Those "$\cdots$"s are a problem! We're trying to say "we can use the same argument over and over…"

We'll come back to this.

induction is a rule of inference

Domain: Natural Numbers

$$\begin{array}{l} P(0) \\ \forall\, k\ (P(k)\ \rightarrow\ P(k+1)) \\ \hline \therefore\ \forall\, n\ P(n) \end{array}$$

using the induction rule in a formal proof

$$\frac{\begin{array}{l} P(0) \\ \forall\, k\, (P(k) \rightarrow P(k+1)) \end{array}}{\therefore\ \forall\, n\, P(n)}$$

1. Prove P(0)
2. Let k be an arbitrary integer ≥ 0
   3. Assume that P(k) is true
   4. ...
   5. Prove P(k+1) is true
6. P(k) → P(k+1) Direct Proof Rule
7. ∀ k (P(k) → P(k+1)) Intro ∀ from 2-6
8. ∀ n P(n) Induction Rule 1&7

format of an induction proof

$$\frac{\begin{array}{l} P(0) \\ \forall\, k\, (P(k) \rightarrow P(k+1)) \end{array}}{\therefore\ \forall\, n\, P(n)}$$

1. Prove P(0)

Base Case

2. Let k be an arbitrary integer ≥ 0
   3. Assume that P(k) is true

Inductive Hypothesis

   4. ...
   5. Prove P(k+1) is true

Inductive Step

6. P(k) → P(k+1)	Direct Proof Rule
7. ∀ k (P(k) → P(k+1))	Intro ∀ from 2-6
8. ∀ n P(n)	Induction Rule 1&7

Conclusion

inductive proof in five easy steps

Proof:

1. "We will show that P(n) is true for every $n \geq 0$ by **induction**."
2. "Base Case:" Prove P(0)
3. "Inductive Hypothesis:"

   Assume P(k) is true for some arbitrary integer $k \geq 0$"
4. "Inductive Step:" Want to prove that P(k+1) is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume P(k+1) !)
5. "Conclusion: Result follows by induction."

- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 4 = 7$
- $1 + 2 + 4 + 8 = 15$
- $1 + 2 + 4 + 8 + 16 = 31$

Can we describe the pattern?

$$1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$$

proving $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

- We could try proving it normally…
  - We want to show that $1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$.
  - So, what do we do now? We can sort of explain the pattern, but that's not a proof…
- We could prove it for n=1, n=2, n=3, … (individually), but that would literally take forever…

inductive proof in five easy steps

Proof:

1. "We will show that P(n) is true for every n ≥ 0 by **induction**."
2. "Base Case:" Prove P(0)
3. "Inductive Hypothesis:"

   Assume P(k) is true for some arbitrary integer k ≥ 0"
4. "Inductive Step:" Want to prove that P(k+1) is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume P(k+1) !)
5. "Conclusion: Result follows by induction."

proving $1 + 2 + \ldots + 2^n = 2^{n+1} - 1$

proving $1 + 2 + \ldots + 2^n = 2^{n+1} - 1$

1. Let P(n) be "$1 + 2 + \ldots + 2^n = 2^{n+1} - 1$". We will show P(n) is true for all natural numbers by induction.
2. Base Case (n=0): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$
3. Induction Hypothesis: Suppose that P(k) is true for some arbitrary $k \geq 0$.
4. Induction Step:

   Goal: Show P(k+1), i.e. show $1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1$

   $1 + 2 + \ldots + 2^k = 2^{k+1} - 1$ by IH

   Adding 2^{k+1} to both sides, we get:

   $1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1$

   Note that $2^{k+1} + 2^{k+1} = 2(2^{k+1}) = 2^{k+2}$.

   So, we have $1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1$, which is exactly P(k+1).
5. Thus P(k) is true for all $k \in \mathbb{N}$, by induction.

another example of a pattern

- $2^0 - 1 = 1 - 1 = 0 = 3 \cdot 0$
- $2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1$
- $2^4 - 1 = 16 - 1 = 15 = 3 \cdot 5$
- $2^6 - 1 = 64 - 1 = 63 = 3 \cdot 21$
- $2^8 - 1 = 256 - 1 = 255 = 3 \cdot 85$
- $\ldots$

prove: $3 \mid 2^{2n} - 1$ for all $n \geq 0$

For all $n \geq 1$: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$