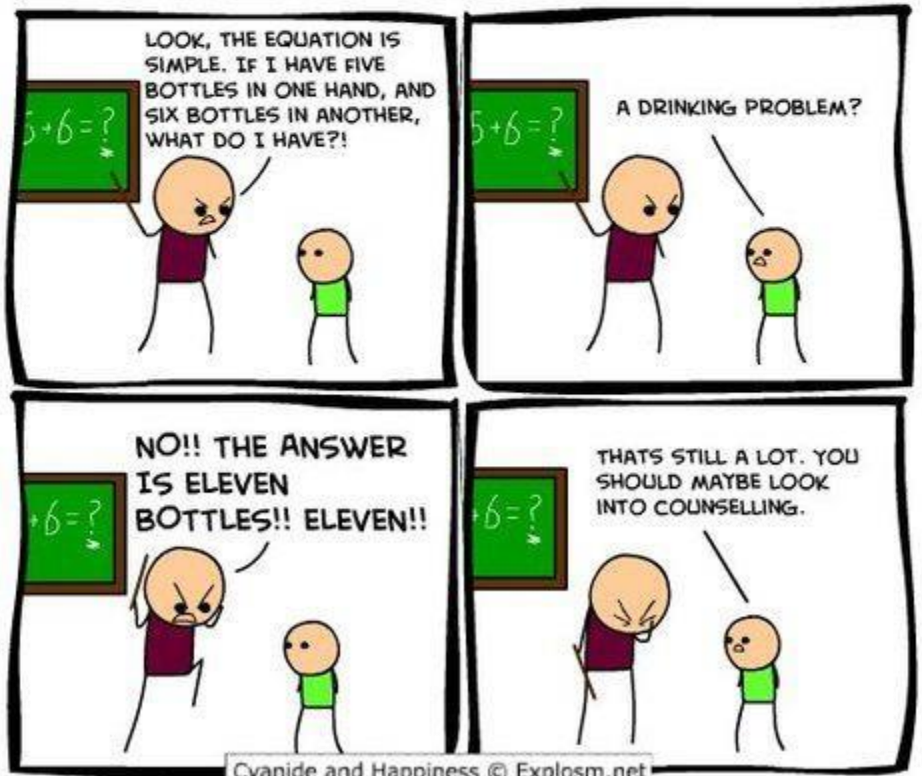
Fall 2015
Lecture 14: Modular congruences



If a and b are positive integers, then

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

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

Proof:

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 $d \mid a$. $D \subseteq C$

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

$C \subseteq D$, $D \subseteq C \Rightarrow C = D$

$\max\{d \in C\} = \max\{d \in D\}$

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

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;
}
```

new a = b

new b = tmp = a mod b.

GCD(12, 10)

tmp = 2   a = 10   b = 2

tmp = 10 mod 2 = 0 ,   a = 2   b = tmp = 0

b = 0   return 2 = a .

Example: GCD(660, 126)

solving modular equations

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

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

Multiply both sides by z:

$$ax \equiv b \pmod{m}$$
$$zax \equiv zb \pmod{m}$$
$$x \equiv zb \pmod{m}$$

$3x \equiv 2 \mod 7$

$3^{-1} = 5$

$3.5 \equiv 1 \mod 7$

$5.3x \equiv 2.5$

$x \equiv 3 \mod 7$

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

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

if $\gcd(a,m) = 1 \rightarrow \exists a^{-1}$ $a \cdot a^{-1} \equiv 1 \mod m$.

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

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

For example: $1 = \gcd(27, 35) = 13 \cdot 27 + (-10) \cdot 35$ $= 1$

351 $\quad -350$

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

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

for some integers s, t.

$sa \equiv 1 \mod m$

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

$27^{-1} = 13$

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

extended Euclidean algorithm

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

- Can use Euclid's Algorithm to find s, t such that $\gcd(a, b) = sa + tb$
- e.g. gcd(35,27):

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

- Substitute back from the bottom

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

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

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

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 $x = (a^{-1} \cdot b) \bmod m$

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

$x \equiv 19 \mod 26.$

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

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

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

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

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

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

Find s, t such that $s \cdot 7 + t \cdot 26 = 1$ $3 \cdot 26 + (-11) \cdot 7 = 1$

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

$= 3 \cdot 5 + (-2) 7$

$= 3 \cdot (26 - 3 \cdot 7) + (-2) \cdot 7$

$= 3 \cdot 26 + (-11) \cdot 7$

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

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

For a multiplicative cipher to be **invertible**: If m is prime

$$f : \{0, \dots, m-1\} \to \{0, \dots, m-1\} \quad \forall\, 0 \leq a \leq m-1$$

gcd(a, m) = 1

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

If m is prime f is one-to-one onto

must be one-to-one and 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.

It enough to show f is one-to-one.

$ax_1 \bmod m = a x_2 \bmod m$

$ax_1 \equiv ax_2 \bmod m \Rightarrow a(x_1 - x_2) \equiv 0 \bmod m$

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

$x_1 - x_2 \equiv 0 \bmod m$

$\uparrow$

$x_1 \equiv x_2 \bmod m$

$\uparrow$

$x_1 = x_2$

could we prove this?

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

$$\gcd(a,b) = \boldsymbol{s}a + \boldsymbol{t}b$$

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 ≥ 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: $\left(\cdots \cdot \left((a \cdot a) \cdot a\right) \cdot \cdots \cdot a\right) = a^n$ [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

$$P(0)$$
$$\forall\, k\, (P(k) \rightarrow P(k+1))$$

$$\therefore \forall\, n\, P(n)$$

using the induction rule in a formal proof

$$\frac{P(0) \qquad \forall k\,(P(k) \to P(k+1))}{\therefore \forall n\, P(n)}$$

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. $P(k) \to P(k+1)$ — Direct Proof Rule
7. $\forall k\,(P(k) \to P(k+1))$ — Intro ∀ from 2-6
8. $\forall n\, P(n)$ — Induction Rule 1&7

format of an induction proof

$$P(0)$$
$$\forall\, k\; (P(k) \;\rightarrow\; P(k+1))$$
$$\therefore\; \forall\, n\; P(n)$$

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 ≥ 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."

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

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 $n \geq 0$ 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."

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

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

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

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