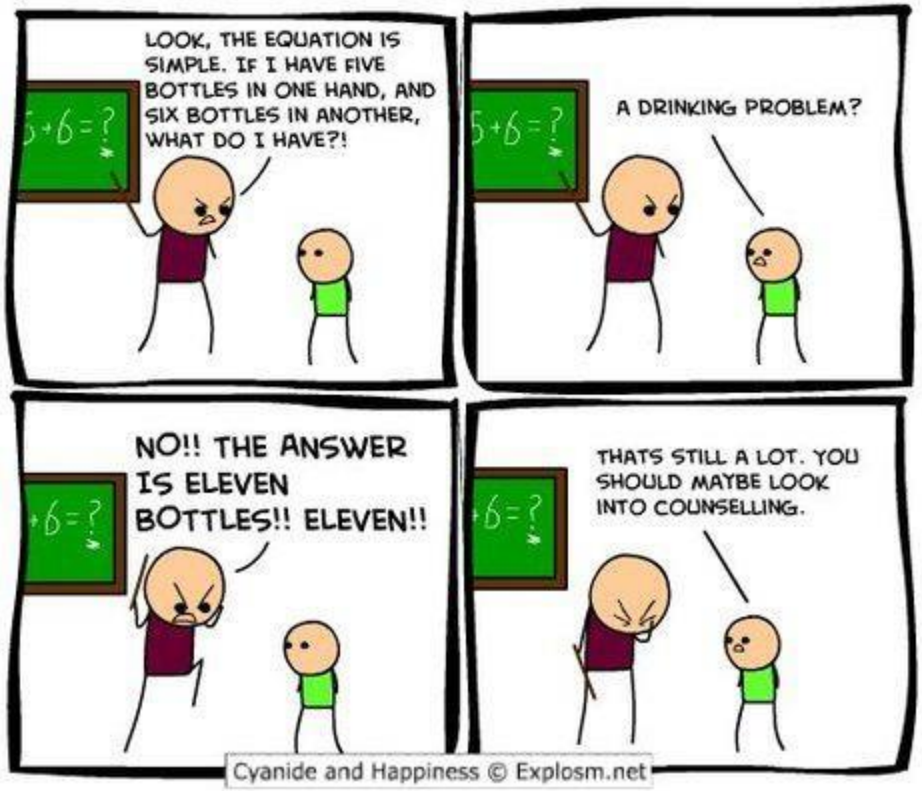
cse 311: foundations of computing

Spring 2015

Lecture 14: Modular congruences



Solving Modular Equations

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:

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

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.**

When is there an inverse?

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

Bezout's Theorem

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

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

27, 35

For example: $1 = \gcd(2\cancel{5}, 3\cancel{7}) = \boxed{13 \cdot 27} + (-10) \cdot 35$

351 −350

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

$$\underline{1 = \gcd(a, m) = sa + tm}$$

for some integers s, t.

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

$13 \cdot 27 \equiv 27 \cdot 13$

$\equiv 1 \pmod{35}$

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

Extended Euclidean Algorithm

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

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

$1 = \gcd(1, 0)$

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (8 - 2 \cdot 3)$$

$$= 3 \cdot 3 + (-1) 8$$

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

$$= (-10) \cdot 8 + 3 \cdot 27 \;//$$

$$(-10) 35 + 13 \cdot 27 .$$

$$\parallel$$

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

Solving Modular Equations

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

$2 \cdot x \equiv 1 \pmod{6}$

$6k + 1$

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

$$ax \equiv a(a^{-1}b) \pmod{m}$$
$$\equiv (aa^{-1})\, b \pmod{m}$$
$$\equiv b \pmod{m}$$

EXAMPLE

$15(7x) \equiv 15 \cdot 3 \pmod{26}$

$x \equiv 45 \pmod{26}$

$7x \equiv 3 \pmod{26}$ $\equiv 19 \pmod{26}$

Solve: $7x \equiv 1 \pmod{26}$

$26 = 3 \cdot 7 + 5$

$\gcd(26, 7) = \gcd(7, 5)$ $7 = 5 \cdot 1 + 2$

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

$(-11) \cdot 7 \equiv 1 \pmod{26}$ $= \gcd(2, 1)$ $2 = 2 \cdot 1 + 0$

$15 \cdot 7 \equiv 1 \pmod{26}$ $= \gcd(1, 0)$ $1 = 1 \cdot 1 + 0$

$= 1$

$x \equiv 15 \pmod{26}$

Goal: $1 = s \cdot 7 + t \cdot 26$

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

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

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

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

$15 \cdot 7 + (-4) 26$

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

$m = p$
prime

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

$$f : \{0, \dots, m-1\} \rightarrow \{0, \dots, m-1\}$$

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

$a + x \pmod m$

$m = 26$

must be one-to-one and onto.

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

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.

$x_1 = x_2$

$\Uparrow$

$x_1 - x_2 \equiv 0 \pmod m$

$\Uparrow$

If $\gcd(a, m) = 1$ then $f(x) = ax \bmod m$ is 1-1

Suppose $ax_1 \bmod m = ax_2 \bmod m \Longrightarrow a^{-1}a(x_1 - x_2) \overset{a^{-1}}{\equiv} 0 \pmod m$

could we prove this?

If a and b are positive integers, then there exist integers $\boldsymbol{s}$ and $\boldsymbol{t}$ such that

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

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 $x \geq 0$ 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. $P(k) \rightarrow P(k+1)$ Direct Proof Rule
7. $\forall$ k $(P(k) \rightarrow P(k+1))$ Intro $\forall$ from 2-6
8. $\forall$ 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 ≥ 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."

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

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

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

   $1 + 2 + \ldots + 2^k = 2^{k+1} - 1$ 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 $n \geq 1$: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$