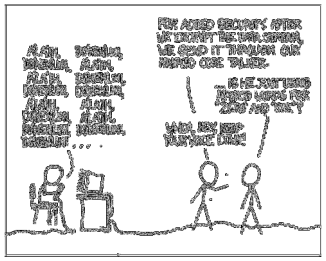
CSE 311



Foundations of Computing I

Fall 2014

Useful GCD Fact

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

Proof:

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

Let $d=\gcd(a,b)$. Then $d|a$ and $d|b$ so $a=kd$ and $b=jd$ for some integers k and j.
Therefore $(a \bmod b) = a - qb = kd - qjd = d(k - qj)$.
So, $d \mid (a \bmod b)$ and since $d \mid b$ we must have $d \le \gcd(b, a \bmod b)$.

Now, let $e=\gcd(b, a \bmod b)$. Then $e \mid b$ and $e \mid (a \bmod b)$. It follows that $b=me$ and $(a \bmod b) = ne$ for some integers m and n. Therefore

$a = qb + (a \bmod b) = qme + ne = e(qm+n)$

So, $e \mid a$ and since $e \mid b$ we must have $e \le \gcd(a, b)$.

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

Euclid's Algorithm

Repeatedly use the fact to reduce numbers until you get

gcd(660,126) = gcd(126, 660 mod 126) = gcd(126, 30)
= gcd(30, 126 mod 30) = gcd(30, 6)
= gcd(6, 30 mod 6) = gcd(6, 0)
= 6

660 = 5 • 126 + 30
126 = 4 • 30 + 6
30 = 5 • 6

Euclid's Algorithm

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

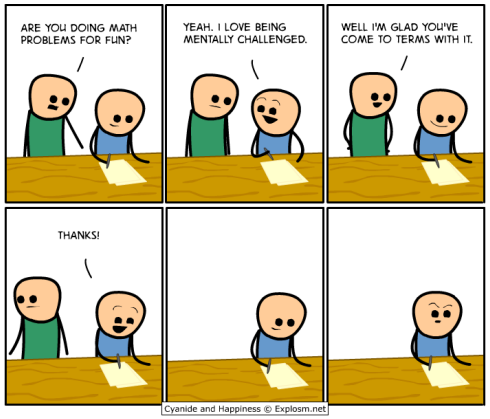
```
int GCD(int a, int b){ /* a >= b, b > 0 */
    int tmp;
    while (y > 0) {
        tmp = a % b;
        a = b;
        b = tmp;
    }
    return a;
}
```

Example: GCD(660, 126)

CSE 311: Foundations of Computing

Fall 2014

Lecture 13: Modular Inverses, Induction



Bézout's theorem

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

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

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* • 27 + 8 — 35 - *1* • 27 = 8

27= *3* • 8 + 3 — 27- *3* • 8 = 3

8 = *2* • 3 + 2 — 8 - *2* • 3 = 2

3 = *1* • 2 + 1 — 3 - *1* • 2 = 1

2 = *2* • 1 + 0

- **Substitute back from the bottom**

1= 3 - *1* • 2 = 3 – *1* (8 - *2* • 3) = (*-1*) • 8 + *3* • 3

= (*-1*) • 8 + *3* (27- *3* • 8) = *3* • 27 + (*-10*) • 8

=

multiplicative inverse $\bmod m$

Suppose $\mathrm{GCD}(a, m) = 1$

By Bézout's Theorem, there exist integers s **and** t **such that** $sa + tm = 1$.

$s \bmod m$ **is the multiplicative inverse of** a**:**

$$1 = (sa + tm) \bmod m = sa \bmod m$$

Solving Modular Equations

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

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

For a multiplicative cipher to be invertible:

$f(x) = ax \bmod m : \{0, \ldots, m-1\} \rightarrow \{0, \ldots, m-1\}$

must be one-to-one and onto

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.

Example

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

Mathematical Induction

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 → 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,

$$(\ldots \bullet ((a \bullet a) \bullet a) \bullet \ldots \bullet a) = a^n$$

(n times)

Those "…"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

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

Using The Induction Rule In A Formal Proof

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

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) → 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

Instead, Let's Use Induction

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

1. Prove P(0) — **Base Case**
2. Let k be an arbitrary integer ≥ 0 — **Inductive Hypothesis**
    3. Assume that P(k) is true
    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

5 Steps To Inductive Proofs In English

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"

What can we say about $1 + 2 + 4 + 8 + \ldots + 2^n$

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

- Can we describe the pattern?
  - $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

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

- We could try proving it normally…
  - We want to show that $1 + 2 + 4 + \ldots + 2^n = 2^{n+1}$.
  - 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…

5 Steps To Inductive Proofs In English

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

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

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

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