CSE 311 Foundations of Computing I

Lecture 14
Euclid's Algorithm
Mathematical Induction
Autumn 2012

Announcements

- Reading assignments
  - Today:
    - 5.1 7th Edition
    - 4.1 6th Edition
    - 3.2 5th Edition
- Homework 5

Highlight from last lecture: 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.

Every positive integer greater than 1 has a unique prime factorization

Greatest Common Divisor

- GCD(a, b): Largest integer d such that d|a and d|b
  - GCD(100, 125) = 25
  - GCD(18, 49) = 1
  - GCD(11, 66) = 11
  - GCD(180, 252) = 36

Euclid's Algorithm

Example: GCD(660, 126)

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

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


Extended Euclid's Algorithm

- If GCD(x, y) = g, there exist integers s, t, such sx + ty = g;
- The values x, y in Euclid's algorithm are linear sums of a, b.
  - A little book keeping can be used to keep track of the constants

Bézout's Theorem

If a and b are positive integers, then there exist integers s and t such that
$$gcd(a,b) = sa + tb.$$

Simple cipher

- Caesar cipher, a → b, b → c, . . .
  - HELLOWORLD → IFMMPXPSME
- Shift cipher
  - $f(x) = (x + k) \bmod 26$
  - $f^{-1}(x) = (x - k) \bmod 26$
- $f(x) = (ax + b) \bmod 26$
  - How good is the cipher $f(x) = (2x + 1) \bmod 26$

Multiplicative Cipher: f(x) = ax mod m

For a multiplicative cipher to be invertible:

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

must be one to one and onto

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

Multiplicative Inverse mod m

Suppose GCD(a, m) = 1

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

s is the multiplicative inverse of a:

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

Solve 7x mod 26 = 1

Hint: $3 \cdot 26 - 11 \cdot 7 = 1$

MATHEMATICAL INDUCTION

Induction Example

- Want to prove $3 \mid 2^{2n} - 1$ for all $n \geq 0$
  - n=0
  - n=1
  - n=2
  - n=3
  - …

Induction as a rule of Inference

Domain: integers ≥ 0

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

How would we use the induction rule in a formal proof?

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

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

How would we use the induction rule in a formal proof?

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

Base Case
1. Prove P(0)

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

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

Conclusion
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

5 Steps to Inductive Proofs in English

Proof:

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

Induction Example

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

$1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$ for all $n \geq 0$

$1+2+\ldots+n = \sum_{i=1}^{n} i = n(n+1)/2$ for all $n \geq 1$

Harmonic Numbers

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$$

Prove $H_{2^n} \geq 1 + \frac{n}{2}$ for all $n \geq 1$

Cute Application: Checkerboard Tiling with Trinominos

Prove that a $2^n \times 2^n$ checkerboard with one square removed can be tiled with: