# CSE 321 Discrete Structures

February 8th, 2010

Lecture 14: Modulo Arithmetic

# Outline

- Finish Euclid's Algorithm
- Representation of integers
- Modular Arithmetic
- Applications
- Fermat's Theorem
- Chinese reminder's theorem

Read: Rosen 3.4, 3.5, 3.6, 3.7

# Running Time of Euclid's Algorithm

If x > y then GCD(x, y) = GCD(y, x **mod** y)

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

**Lame's Theorem** Let $x \geq y > 0$. If GCD(x,y) takes n steps, then $x \geq f_n$

# Proof By Strong Induction

If x > y then GCD(x, y) = GCD(y, x **mod** y)

If $x \geq y > 0$ and GCD(x,y) takes n steps, then $x \geq f_n$

**Base cases**: n=1: $x \geq y > 0 \rightarrow x \geq 1 = f_1$
n=2 → $x \geq 2 = f_2$ (because if x=1 then y=1 and it takes only n=1 step)

**Inductive step**: If GCD(x,y) takes n > 2 steps, then:

- GCD(y, x **mod** y) takes n-1 steps → $y \geq f_{n-1}$
- GCD(x **mod** y, y **mod** (x **mod** y)) takes n-2 steps → x **mod** $y \geq f_{n-2}$

Since x > y it follows: $x \geq y + (x \textbf{ mod } y) \geq f_{n-1} + f_{n-2}$

# Representation of Integers

Let b > 1 be an integer. Every integer n > 0 can be expressed uniquely in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b + a_0$$

Proof by strong induction (in class)

# Representation of Integers

- Binary representation:
  - E.g. $1011010_2 = 2^6 + 2^4 + 2^3 + 2^1 = 90$
- Hexadecimal representation:
  - E.g. $A06F_{16} = 10 \times 16^3 + 6 \times 16 + 15 = 41071$
- Converting binary to hexadecimal:
  - E.g. 1100 0011 1010 1101 = C3AD

# Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

# Arithmetic mod 7

- $a +_7 b = (a + b) \bmod 7$
- $a \times_7 b = (a \times b) \bmod 7$

Denoted $\mathbf{Z}_7$

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | | | | | | | |
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | | | | | | | |
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |

# Group Theory

- A group G=(S, •) is a set S with a binary operator • that is "well behaved":
  - Closed under •
  - Associative: $x \bullet (y \bullet z) = (x \bullet y) \bullet z$
  - Has an identity: $\exists e. \forall x.\ e \bullet x = x \bullet e = x$
  - Each x has an inverse: $\forall x. \exists y.\ x \bullet y = y \bullet x = e$
    Note: the inverse is written as $y = x^{-1}$
- G is commutative if: $\forall x.\ \forall y.\ x \bullet y = y \bullet x$

# Groups, mod 7

$\{0,1,2,3,4,5,6\}$ is a commutative group under $+_7$

$\{1,2,3,4,5,6\}$ is a commutative group under $\times_7$

# Multiplicative Inverses

- Euclid's theorem: if $x$ and $y$ are relatively prime, then there exists integers $s$, $t$, such that:

$$sx + ty = 1$$

- Prove $a \in \{1, 2, 3, 4, 5, 6\}$ has a multiplicative inverse under $\times_7$

# Generalizations

- ({0,…, $n$-1}, $+_n$ ) forms a group for all positive integers $n$
- ({1,…, $n$-1}, $\times_n$ ) is a group if and only if $n$ is prime  WHY ???

- For every n
  - Let  C = {x | 1 ≤ x < n, gcd(x,n)=1}
  - Then (C, , $\times_n$ ) is a group
  - Note: |C| is denoted φ(n) = # of coprimes of n

# Application 1: Hash Tables

- Map values from a large domain, 0…M-1 in a much smaller domain, 0…n-1

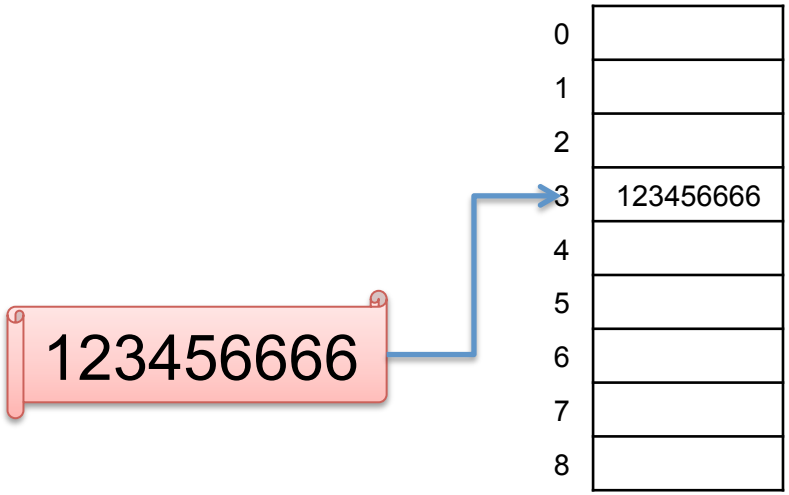
Hash(x) = x **mod** M

- Used for: index lookup, or equality test
- Often want the hash function to depend on all of the bits of the data

# Application 1: Hash Tables

- Example: map Social Security Numbers to a table with 9 entries

$$\text{Hash}(123456666) = 123456666 \bmod 9 = 3$$



# Application 2: Pseudo Random number generation

- Linear Congruential method

$$x_{n+1} = (a\, x_n + c) \bmod m$$

(see book for an example…)

# Application 3: Simple cipher

- Caesar cipher, A = 0, B = 1, . . . Z = 25
  - HELLO WORLD
- Shift cipher
  - $f(x) = (x + k) \bmod n$
  - $f^{-1}(x) = (x - k) \bmod n$
- Affine cipher
  - $f(x) = (ax + b) \bmod n$
  - $f^{-1}(x) = (a^{-1}(x-b)) \bmod n$

| | A | B | C | D | E | F | G | … |
|---|---|---|---|---|---|---|---|---|
| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | … |
| f(x) | 4 | 5 | 6 | 7 | 8 | 9 | 10 | … |
| $f^{-1}(x)$ | 21 | 22 | 23 | 24 | 25 | 0 | 1 | … |

# Modular Exponentiation

| x | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

| a | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |

# Modular Exponentiation

| x | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

| a | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |

# Fermat's Little Theorem

**Theorem** If p is prime, $0 < a \leq p-1$, $a^{p-1} \equiv 1 \pmod{p}$

# Proof 1

We prove the following by induction on n:

If p is prime, then forall n, $p \mid n^p - n$

Why does this prove Fermat's ?

**Base case:** $0^p - 0 = 0$

**Inductive step:** assume $p \mid n^p - n$.

$$(n+1)^p - (n+1) = n^p + \Sigma_{k=1,p-1} \binom{p}{k} n^k + 1 - n - 1 =$$
$$= (n^p - n) + \Sigma_{k=1,p-1} \binom{p}{k} n^k$$

We know that $p \mid n^p - n$. We also know that $p \mid \binom{p}{k}$ (in class)
Hence $p \mid (n+1)^p - (n+1)$

# Proof 2

Let G=(S, •) be a commutative group, e its identity.
Denote $a^k = a \bullet a \bullet \ldots \bullet a$ (k times)
The ***order*** of the group is n = |G|.

$\forall a \in G, \quad a^n = e$

Why does this prove Fermat's ?

Poof. Let $G = \{a_1, \ldots, a_n\}$. Consider the elements

$b_1 = a \bullet a_1, \ldots, \; b_n = a \bullet a_n$

$b_1, \ldots, b_n$ are distinct because:

if $b_i = b_j \rightarrow a \bullet a_i = a \bullet a_j \rightarrow a^{-1} \bullet a \bullet a_i = a^{-1} \bullet a \bullet a_j \rightarrow a_i = a_j \rightarrow i=j$

The set $\{a \bullet a_1, \ldots, a \bullet a_n\}$ is the same as $\{a_1, \ldots, a_n\}$, in a different order.

Hence $a \bullet a_1 \bullet \ldots \bullet a \bullet a_n = a_1 \bullet \ldots \bullet a_n$

Multiply with $(a_1 \bullet \ldots \bullet a_n)^{-1}$ and obtain $a^n = e$

# Proof 2: A consequence

- Index of a, smallest i > 0 such that $a^i = e$

$\forall a \in G$, the index of a divides the order of G

- Show by induction on #steps of GCD(i,j):

If $a^i = e$ and $a^j = e$ then $a^{GCD(i,j)} = e$

  - **Base step**: i=j. Then GCD(i,j) = i.
  - **Inductive step**: assume i>j.
  - $a^i = e$ and $a^j = e$ → $a^i \bullet (a^j)^{-1} = e$ → $a^{i-j} = e$.
  - By induction, $a^{GCD(i-j,j)} = e$; we use GCD(i-j,j) = GCD(i,j)

- Let n = order(G)
  - $a^i = e$ and $a^n = e$ → $a^{GCD(i,n)} = e$.
  - GCD(i,n)<i → GCD(i,n) = 0.

# Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime
Let $M = m_1 \times m_2 \times \ldots \times m_k$
Let $a_1 \in Z_{m1}, a_2 \in Z_{m2}, \ldots, a_k \in Z_{mk}$
Then there exists a unique x in $Z_M$ s.t.:

$x \equiv a_1 \mod m_1,$
$x \equiv a_2 \mod m_2,$
. . .
$x \equiv a_k \mod m_k,$

Example: Find an x in [0 . . . 11484] such that

x mod 11 = 9
x mod 29 = 7
x mod 36 = 14

# Proof

Let $M_1 = M / m_1$, $M_2 = M / m_2$, … $M_k = M / m_k$

Let $x = z_1 \times M_1 + z_2 \times M_2 + \ldots z_k \times M_k$

Note that $x = z_1 \times M_1 \mod m_1$ (WHY ???);
Similarly $x = z_2 \times M_2 \mod m_2$ … $x = z_k \times M_k \mod m_k$

Hence, we choose:

$z_1 = a_1 \times (M_1)^{-1} \mod m_1$
$z_2 = a_2 \times (M_2)^{-1} \mod m_2$
. . .
$z_k = a_k \times (M_k)^{-1} \mod m_k$