Comments on Wednesday's class problems

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Class Problem 1

- How do we compute inverses modulo n? Two options:
  - The Pulverizer
    - If $gcd(x,n)=1$ then the pulverizer finds s,t such that $sx+tn=1$. Then $s \equiv x^{-1} \pmod n$
  - Euclid's Theorem
    - Need to know how to compute $\phi(n)$
    - $x^{-1} \equiv x^{\phi(n)-1} \pmod n$
    - How do we calculate the above?

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Computing large powers

- Need to compute x^r for large r
  - To use Euclid's theorem in order to find inverse
  - To encrypt message
  - To decrypt transmission

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Computing large powers

- Compute x^r with as few multiplications as possible
  - What if $r=4$?
    - $x \cdot x \rightarrow x^2$, $x \cdot x^2 \rightarrow x^3$, $x \cdot x^3 \rightarrow x^4$
    - *2* multiplications suffice: $x \cdot x \rightarrow x^2$, $x^2 \cdot x^2 \rightarrow x^4$
  - $r=2^i$?
    - Repeated squaring uses i multiplies: $x \cdot x \rightarrow x^2$, $x^2 \cdot x^2 \rightarrow x^4$, $x^4 \cdot x^4 \rightarrow x^8$

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Computing large powers

- Compute x^r with as few multiplications as possible
  - $r=6$?
    - 4 multiplications: $x \cdot x \rightarrow x^2$, $x^2 \cdot x^2 \rightarrow x^4$, $x \cdot x \rightarrow x^2$, $x^2 \cdot x^4 \rightarrow x^6$
    - *3* multiplications suffice!
  - repeated squaring gives ***all*** x^{2^j} for $j \le l$ with only l multiplies

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Computing large powers

Computing x^r with as few multiplications as possible:

- Binary representation of r is $b_l, b_{l-1}, \ldots, b_1, b_0$
  i.e., $r = b_l 2^l + b_{l-1} 2^{l-1} + \ldots + b_0 2^0$
- So $x^r = x^{b_l 2^l} \cdot x^{b_{l-1} 2^{l-1}} \cdot \ldots \cdot x^{b_0 2^0}$
  $x^6 = x^{1 \cdot 2^2} \cdot x^{1 \cdot 2^1} \cdot x^{0 \cdot 2^0} = x^{2^2} \cdot x^{2^1}$
- Total multiplications: at most $\log r$ for repeated squaring and another at most $\log r$ for putting them together

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

As few as possible?

- Is this the best method?
  - Can do better for some r
    - Try r = 101101 (in binary) 45 (in decimal)
    - Our bound gives 12 multiplies
    - Can get it with 7
  - But can't do better than $\log r - 1$

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Next difficulty

- Squaring a 100 bit number gives a 200 bit result
- Repeated squaring gives huge numbers
- Solution: the answer is supposed to be *rem n*, so do all partial work *rem n* as well
  - Why is that ok?

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Using rem to simplify intermediate work:

Why does

$((a \text{ rem } n) \cdot (b \text{ rem } n)) \text{ rem } n = (a \cdot b) \text{ rem } n$?

$((a \text{ rem } n) \cdot (b \text{ rem } n)) \text{ rem } n = (a \cdot b) \text{ rem } n$

iff $((a \text{ rem } n) \cdot (b \text{ rem } n)) \equiv a \cdot b \pmod{n}$

iff $a \cdot b \equiv a \cdot b \pmod{n}$

(using: (1) $(a \text{ rem } n) \equiv a \pmod{n}$

(2) $a \equiv b \pmod{n}$ iff $a \text{ rem } n = b \text{ rem } n$

from Number Theory lecture 2)

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Problem 2

- Why is $m^{de} \equiv m \pmod{pq}$?

  (we have that $de = 1 + k\,\phi(pq)$ for some k)

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Problem 2

- First show that $m^{de} \equiv m \pmod{p}$:
  - if m is a multiple of p then easy
  - else, can use Fermat's theorem:

$$m^{de} \equiv m^{1+k(p-1)(q-1)} \pmod{p}$$
$$\equiv m(m^{(p-1)})^{k(q-1)} \pmod{p}$$
$$\equiv m1^{k(q-1)} \pmod{p}$$
$$\equiv m \pmod{p}$$

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.

Problem 2

Same proof shows that $m^{de} \equiv m \pmod{q}$

$\Rightarrow$ both p,q divide $m^{de} - m$

$\Rightarrow$ both p,q in prime factorization of $m^{de} - m$

$\Rightarrow p \cdot q$ divides $m^{de} - m$

$\Rightarrow m^{de} \equiv m \pmod{pq}$

Copyright © Albert R. Meyer and Ronitt Rubinfeld, 2005. All rights reserved.