CSE 311 Foundations of Computing I

Lecture 13

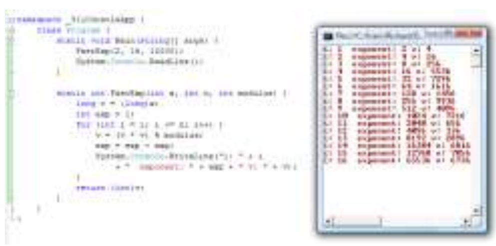
Number Theory

Autumn 2012

Announcements

- Reading assignments
  - Today :
    - 7th Edition: 4.3 (the rest of the chapter is interesting!)
    - 6th Edition: 3.5, 3.6
    - 5th Edition: 2.5, 2.6 up to p. 191
  - Wednesday
    - 7th Edition: 5.1, 5.2
    - 6th Edition: 4.1, 4.2
    - 5th Edition: 3.3, 3.4

Fast modular exponentiation



Fast exponentiation algorithm

- Compute 78365^{65336} mod 104729

- Compute 78365^{81453} mod 104729

Fast exponentiation algorithm

- What if the exponent is not a power of two?

$81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^{9} + 2^{5} + 2^{3} + 2^{2} + 2^{0}$

The fast exponentiation algorithm computes a^n mod m in time O(log n)

Basic applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher

Hashing

- Map values from a large domain, 0…M-1 in a much smaller domain, 0…N-1
- Index lookup
- Test for equality
- Hash(x) = x mod p
- Often want the hash function to depend on all of the bits of the data
  - Collision management

Pseudo random number generation

- Linear Congruential method

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

Simple cipher

- Caesar cipher, A = 1, B = 2, . . .
  - HELLO WORLD
- Shift cipher
  - $f(p) = (p + k) \bmod 26$
  - $f^{-1}(p) = (p - k) \bmod 26$
- $f(p) = (ap + b) \bmod 26$

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.

Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization

48 = 2 • 2 • 2 • 2 • 3
591 = 3 • 197
45,523 = 45,523
321,950 = 2 • 5 • 5 • 47 • 137
1,234,567,890 = 2 • 3 • 3 • 5 • 3,607 • 3,803

Factorization

- If n is composite, it has a factor of size at most sqrt(n)

Euclid's theorem

There are an infinite number of primes.

Proof:

By contradiction

Suppose there are a finite number of primes: $p_1, p_2, \ldots, p_n$

Distribution of Primes

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89
97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173
179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263
269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359

- If you pick a random number n in the range [x, 2x], what is the chance that n is prime?

Famous Algorithmic Problems

- Primality Testing:
  - Given an integer n, determine if n is prime
- Factoring
  - Given an integer n, determine the prime factorization of n

Factoring

- Factor the following 232 digit number [RSA768]:

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434 13

=

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

×

36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

Greatest Common Divisor

- GCD(a, b): Largest integer d such that $d|a$ and $d|b$
  - GCD(100, 125) =
  - GCD(17, 49) =
  - GCD(11, 66) =
  - GCD(180, 252) =

GCD, LCM and Factoring

$a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46{,}200$

$b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204{,}750$

$GCD(a, b) = 2^{\min(3,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(2,3)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} \cdot 13^{\min(0,1)}$

$LCM(a, b) = 2^{\max(3,1)} \cdot 3^{\max(1,2)} \cdot 5^{\max(2,3)} \cdot 7^{\max(1,1)} \cdot 11^{\max(1,0)} \cdot 13^{\max(0,1)}$

Theorem

Let *a* and *b* be positive integers. Then

$a \cdot b = gcd(a, b) \cdot lcm(a, b)$

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) mod 26
  - $f^{-1}(x)$ = (x – k) mod 26
- f(x) = (ax + b) mod 26
  - How good is the cipher f(x) = (2x + 1) mod 26

Multiplicative Cipher: f(x) = ax mod m

For a multiplicative cipher to be invertible:

f(x) = ax mod m : {0, m-1} → {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) mod m = sa mod m