CSE 311 Foundations of Computing I

Lecture 12

Primes, GCD, Modular Inverse

Spring 2013

Announcements

- Reading assignments
  - Today :
    - 7^{th} Edition: 4.3-4.4 (the rest of the chapter is interesting!)
    - 6^{th} Edition: 3.5, 3.6
  - Monday: Mathematical Induction
    - 7^{th} Edition: 5.1, 5.2
    - 6^{th} Edition: 4.1, 4.2

Fast modular exponentiation

```
namespace _311ConsoleApp {
    class Program {
        static void Main(string[] args) {
            FastExp(2, 16, 10000);
            System.Console.ReadLine();
        }

        static int FastExp(int x, int n, int modulus) {
            long v = (long)x;
            int exp = 1;
            for (int i = 1; i <= n; i++) {
                v = (v * v) % modulus;
                exp = exp + exp;
                System.Console.WriteLine("i: " + i
                    + "  exponent: " + exp + " v: " + v);
            }
            return (int)v;
        }
    }
}
```

```
file:///C:/Users/Richard/D...
i: 1  exponent: 2 v: 4
i: 2  exponent: 4 v: 16
i: 3  exponent: 8 v: 256
i: 4  exponent: 16 v: 5536
i: 5  exponent: 32 v: 7296
i: 6  exponent: 64 v: 1616
i: 7  exponent: 128 v: 1456
i: 8  exponent: 256 v: 9936
i: 9  exponent: 512 v: 4096
i: 10  exponent: 1024 v: 7216
i: 11  exponent: 2048 v: 656
i: 12  exponent: 4096 v: 336
i: 13  exponent: 8192 v: 2896
i: 14  exponent: 16384 v: 6816
i: 15  exponent: 32768 v: 7856
i: 16  exponent: 65536 v: 6736
```


Fast exponentiation algorithm

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

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

$78365^{81453} = 78365^{2^{16}}\ 78365^{2^{13}}\ 78365^{2^{12}}\ 78365^{2^{11}} \ldots$

The fast exponentiation algorithm computes $a^n \bmod m$ in time $O(\log n)$

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

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

$=$

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

$\times$

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(13, 0) =
  - GCD(180, 252) =

GCD and Factoring

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

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

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

Factoring is expensive!
Can we compute GCD(a,b) without factoring?

Useful GCD fact

If *a* and *b* are positive integers, then
gcd(a,b) = gcd(b, a mod *b)*

Proof:
By definition $a = (a \text{ div } b)\, b + (a \bmod b)$

If d|*a* and d|*b* then d|(*a* mod *b*):

If d|*b* and d|(*a* mod *b*) then d|*a* :

Euclid's Algorithm

Repeatedly use the GCD fact to reduce numbers until you get GCD(x,0)=x

GCD(660,126)

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;
}
```


Bézoit's Theorem

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

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

Extended Euclid's Algorithm

- Can use Euclid's Algorithm to find s,t such that $sa+tb=\gcd(a,b)$
- e.g. gcd(35,27):

$35 = 1 \bullet 27 + 8$	$35 - 1 \bullet 27 = 8$
$27 = 3 \bullet 8 + 3$	$27 - 3 \bullet 8 = 3$
$8 = 2 \bullet 3 + 2$	$8 - 2 \bullet 3 = 2$
$3 = 1 \bullet 2 + 1$	$3 - 1 \bullet 2 = 1$
$2 = 2 \bullet 1 + 0$	

$1 = 3 - 1 \bullet 2 = \quad 3 - 1\,(8 - 2 \bullet 3) \quad = (-1) \bullet 8 + 3 \bullet 3$

$= (-1) \bullet 8 + 3\,(27 - 3 \bullet 8) = \quad 3 \bullet 27 + (-10) \bullet 8$

$=$

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

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

Multiplicative Cipher: $f(x) = ax \bmod m$

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 $ab \bmod m = 1$, then the function $f(x) = ax \bmod m$ is one to one and onto.