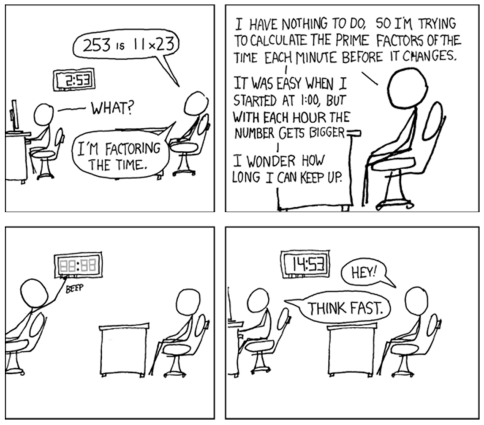
## CSE 311: Foundations of Computing

**Fall 2013**

**Lecture 12: Primes, GCD, modular inverse**




## announcements

**Reading assignment**

**Primes, GCD, modular inverses**

4.3-4.4, 7th edition

3.5-3.6, 6th edition

## review: repeated squaring for fast exponentiation

**Compute** $78365^{81453}$ mod 104729

Since $a \bmod m \equiv a \pmod m$ for any $a$

we have $a^2 \bmod m = (a \bmod m)^2 \bmod m$

and $a^4 \bmod m = (a^2 \bmod m)^2 \bmod m$

and $a^8 \bmod m = (a^4 \bmod m)^2 \bmod m$

and $a^{16} \bmod m = (a^8 \bmod m)^2 \bmod m$

and $a^{32} \bmod m = (a^{16} \bmod m)^2 \bmod m$

…

**Can compute** $a^k \bmod m$ **for** $k=2^i$ **in only** $i$ **steps**

## review: fast exponentiation algorithm

```
int FastExp(int a, int n, m){
   long v = (long) a;
   int exp = 1;
   for (int i = 1; i <= n; i++){
      v = (v * v) % m;
      exp = exp + exp;
      Console.WriteLine("i : " + i + ", exp :
          " + exp + ", v : " + v  );
   }
   return (int)v;
}
```

```
i : 1,   exp : 2,      v : 82915
i : 2,   exp : 4,      v : 95592
i : 3,   exp : 8,      v : 70252
i : 4,   exp : 16,     v : 26992
i : 5,   exp : 32,     v : 74970
i : 6,   exp : 64,     v : 71358
i : 7,   exp : 128,    v : 20594
i : 8,   exp : 256,    v : 10143
i : 9,   exp : 512,    v : 61355
i : 10,  exp : 1024,   v : 68404
i : 11,  exp : 2048,   v :  4207
i : 12,  exp : 4096,   v : 75698
i : 13,  exp : 8192,   v : 56154
i : 14,  exp : 16384,  v : 83314
i : 15,  exp : 32768,  v : 99519
i : 16,  exp : 65536,  v : 29057
```

## review: fast exponentiation algorithm

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

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

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

$a^{81453} \bmod m = (a^{2^{16}} \bmod m \cdot a^{2^{13}} \bmod m \cdot a^{2^{12}} \bmod m \cdot a^{2^{11}} \bmod m \cdot a^{2^{10}} \bmod m \cdot a^{2^9} \bmod m \cdot a^{2^5} \bmod m \cdot a^{2^3} \bmod m \cdot a^{2^2} \bmod m \cdot a^{2^0} \bmod m) \bmod m$

**The fast exponentiation algorithm computes $a^n \bmod m$ using $O(\log n)$ multiplications modulo $m$**

## 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 that there are only 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]:

123018668453011775513049495838496272077
285356959533479219732245215172640050726
365751874520219978646938995647494277406
384592519255732630345373154826850791702
612214291346167042921431160222124047927
473779408066535141959745985690214341 3

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341336478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089171

## greatest common divisor

GCD(a, b):

**Largest integer $d$ such that $d \mid a$ and $d \mid b$**

- GCD(100, 125) =
- GCD(17, 49) =
- GCD(11, 66) =
- GCD(13, 0) =
- GCD(180, 252) =

## GCD and factoring

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

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

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

**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** $a = (a \operatorname{div} b)b + (a \bmod b)$

**If** $d \mid a$ **and** $d \mid b$ **then** $d \mid (a \bmod b)$.

**If** $d \mid b$ **and** $d \mid (a \bmod b)$ **then** $d \mid a$.

## euclid's algorithm

**Repeatedly use the $\mathrm{GCD}$ fact to reduce numbers until you get $\mathrm{GCD}(x, 0) = x$.**

GCD(660,126)

## euclid's algorithm

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;
}
```

Example: GCD(660, 126)

## bézoit's theorem

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

gcd*(a,b)* = ***s****a* + ***t****b*.

## extended euclid algorithm

- **Can use Euclid's Algorithm to find $s, t$ such that** $\gcd(a, b) = sa + tb$

- e.g. gcd(35,27):

| | | |
|---|---|---|
| 35 = *1* • 27 + 8 | 35 - *1* • 27 = 8 |
| 27= *3* • 8 + 3 | 27- *3* • 8 = 3 |
| 8 = *2* • 3 + 2 | 8 - *2* • 3 = 2 |
| 3 = *1* • 2 + 1 | 3 - *1* • 2 = 1 |
| 2 = *2* • 1 + 0 | |

- **Substitute back from the bottom**

1= 3 - *1* • 2 = 3 – *1* (8 - *2* • 3) = (*-1*) • 8 + *3* • 3

= (*-1*) • 8 + *3* (27- *3* • 8 ) = *3* • 27 + (*-10*) • 8

=

## multiplicative inverse $\bmod m$

**Suppose** $\mathrm{GCD}(a, m) = 1$

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

$s \bmod m$ **is the multiplicative inverse of** $a$**:**

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

## 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** $x = (a^{-1} \cdot b) \bmod m$

## multiplicative cipher: $f(x) = ax \bmod m$

**For a multiplicative cipher to be invertible:**

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

**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.**