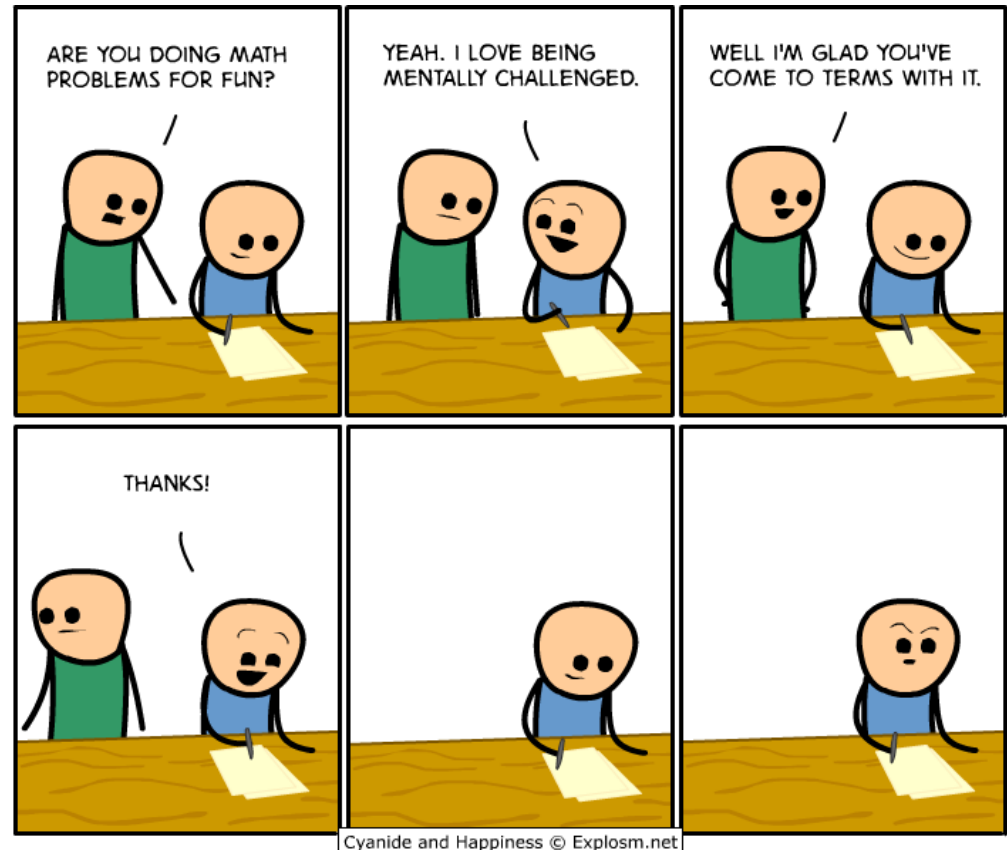


cse 311: foundations of computing

Fall 2015

Lecture 13: Primes, GCDs



- Compute 78365^{81453}
- Compute $78365^{81453} \bmod 104729$
- Output is small
 - need to keep intermediate results small

repeated squaring – small and fast

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

ModPow(a, k, m) should compute $a^k \bmod m$.

If $k == 0$ then

return 1

If $(k \bmod 2 == 0)$ then

return $\text{ModPow}(a^2 \bmod m, k/2, m)$

else

return $(a \times \text{ModPow}(a, k - 1, m)) \bmod m$

$$\begin{aligned} k &= 81453 \\ &= (10011111000101101)_2 \\ &= 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^5 + 2^3 + 2^2 + 2^0 \end{aligned}$$

Total # of arithmetic operations $\sim 4 \times 16 = 64$

fast exponentiation algorithm

Another way:

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

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

$$a^{81453} \bmod m =$$

$$\begin{aligned} & (\dots((((a^{2^{16}} \bmod m \cdot \\ & \quad a^{2^{13}} \bmod m) \bmod m \cdot \\ & \quad a^{2^{12}} \bmod m) \bmod m \cdot \\ & \quad a^{2^{11}} \bmod m) \bmod m \cdot \\ & \quad a^{2^{10}} \bmod m) \bmod m \cdot \\ & \quad a^{2^9} \bmod m) \bmod m \cdot \\ & \quad a^{2^5} \bmod m) \bmod m \cdot \\ & \quad a^{2^3} \bmod m) \bmod m \cdot \\ & \quad a^{2^2} \bmod m) \bmod m \cdot \\ & \quad a^{2^0} \bmod m) \bmod m \end{aligned}$$

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

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

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$$

$$591 = 3 \cdot 197$$

$$45,523 = 45,523$$

$$321,950 = 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137$$

$$1,234,567,890 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3,607 \cdot 3,803$$

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, \dots, p_n

Famous Algorithmic Problems

- **Primality Testing**

- Given an integer n , determine if n is prime
- Fermat's little theorem test:

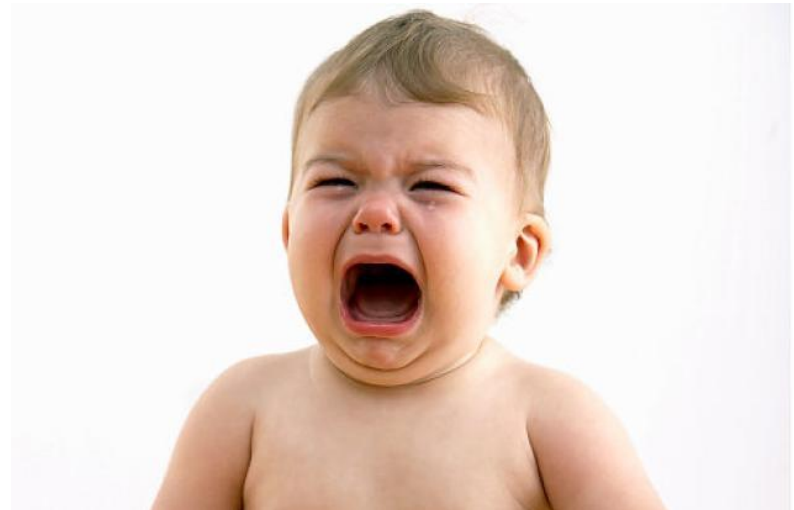
If p is prime and $a \neq 0$, then $a^{p-1} \equiv 1 \pmod{p}$

- **Factoring**

- Given an integer n , determine the prime factorization of n

Factor the following 232 digit number [RSA768]:

1230186684530117755130494958384962720772
8535695953347921973224521517264005072636
5751874520219978646938995647494277406384
5925192557326303453731548268507917026122
1429134616704292143116022212404792747377
94080665351419597459856902143413



123018668453011775513049495838496272077285356959533479
219732245215172640050726365751874520219978646938995647
494277406384592519255732630345373154826850791702612214
291346167042921431160222124047927473779408066535141959
7459856902143413

=

334780716989568987860441698482126908177047949837
13768568912431388982883793878 17
43087737814467999489

×

3674604366679959042824463379 643
4308764267603228381573966651 968
10270092798736308917



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 $\text{GCD}(a,b)$ without factoring?

Useful GCD Fact

If a and b are positive integers, then

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Proof:

By definition $a = (a \operatorname{div} b) \cdot b + (a \bmod b)$

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 GCD fact to reduce numbers
until you get $\text{GCD}(x, 0) = x$.

$\text{GCD}(660, 126)$

Euclid's Algorithm

$$\text{GCD}(x, y) = \text{GCD}(y, x \bmod y)$$

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

Example: GCD(660, 126)

Bezout's Theorem

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

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

Extended Euclidean Algorithm

- Can use Euclid's Algorithm to find s, t such that

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

- e.g. $\gcd(35, 27)$:
 $35 = 1 \cdot 27 + 8$ $35 - 1 \cdot 27 = 8$
 $27 = 3 \cdot 8 + 3$ $27 - 3 \cdot 8 = 3$
 $8 = 2 \cdot 3 + 2$ $8 - 2 \cdot 3 = 2$
 $3 = 1 \cdot 2 + 1$ $3 - 1 \cdot 2 = 1$
 $2 = 2 \cdot 1 + 0$

- Substitute back from the bottom

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 &= 3 - 1(8 - 2 \cdot 3) &= (-1) \cdot 8 + 3 \cdot 3 \\ & &= (-1) \cdot 8 + 3(27 - 3 \cdot 8) &= 3 \cdot 27 + (-10) \cdot 8 \\ & &= 3 \cdot 27 + (-10) \cdot (35 - 1 \cdot 27) &= -10 \cdot 35 + 13 \cdot 27 \end{aligned}$$

Multiplicative Inverse mod m

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

By Bézout'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 $a^{-1} = s \pmod{m}$, the multiplicative inverse of a modulo m
3. Set $x = (a^{-1} \cdot b) \pmod{m}$

Example

Solve: $7x \equiv 1 \pmod{26}$