cse 311: foundations of computing
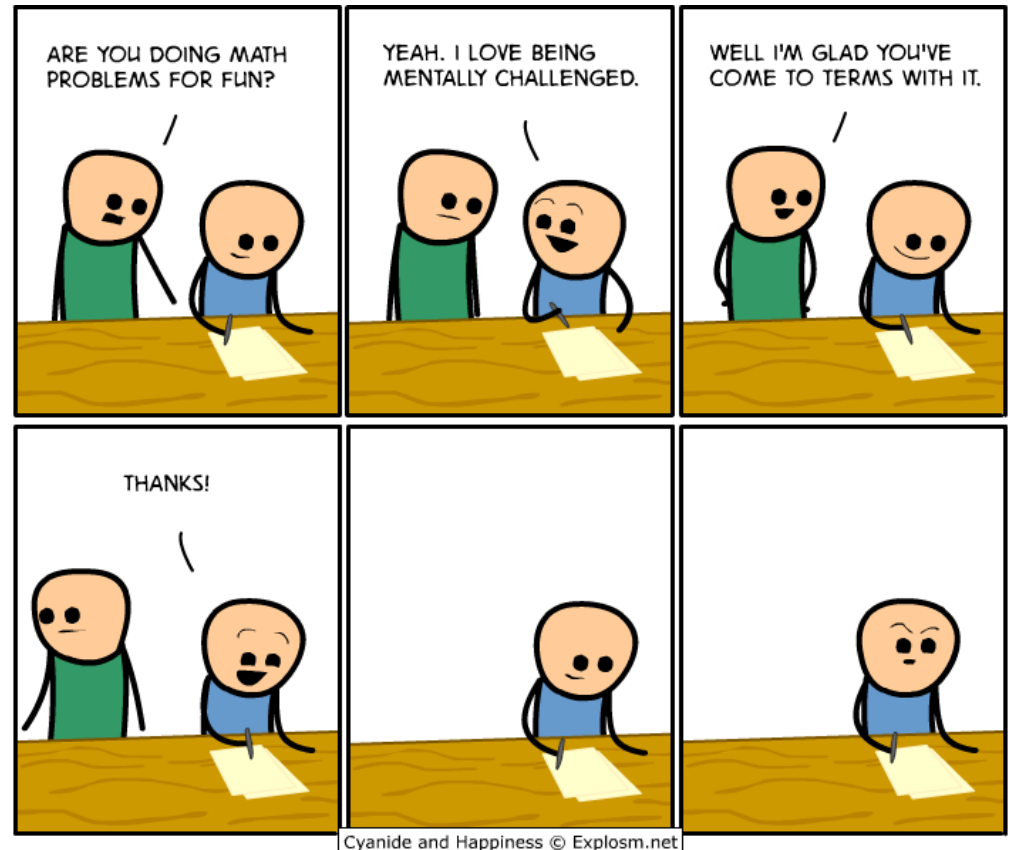
Spring 2015
Lecture 13: Primes, GCDs, modular inverses

Since   a mod m $\equiv$ a (mod m) for any a

we have a^2 mod m   = (a mod m)^2 mod m

and a^4 mod m   = (a^2 mod m)^2 mod m

and a^8 mod m   = (a^4 mod m)^2 mod m

and a^{16} mod m = (a^8 mod m)^2 mod m

and a^{32} mod m = (a^{16} mod m)^2 mod 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 ModPow$(a^2 \bmod m, k/2, m)$

    else

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

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

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

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*.

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*.

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

If n is composite, it has a factor of size at most $\sqrt{n}$.

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes:

$p_1, p_2, \ldots, p_n$

- ## 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]:

12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434113

123018668453011775513049495838496272077285356959533479219
732245215172640050726365751874520219978646938995647494277
406384592519255732630345373154826850791702612214291346167
042921431160222124047927473779408066535141959745985690214
3413

=

334780716989568987860441698482126908177047949837
137685689124313889288379387█████████████████████17
43087737814467999489

×

3674604366679959042824463379█████████████████643
43087642676032283815739666511█████████████████968
10270092798736308917

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)   =

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

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

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

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

If a and b are positive integers, then
$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Proof:

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

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 $d \mid a$.

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

GCD(660,126)

GCD(x, y) = GCD(y, x mod 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)

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** • 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

  =

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

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 $ax \equiv b \pmod{m}$ 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 $x = (a^{-1} \cdot b) \bmod m$

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