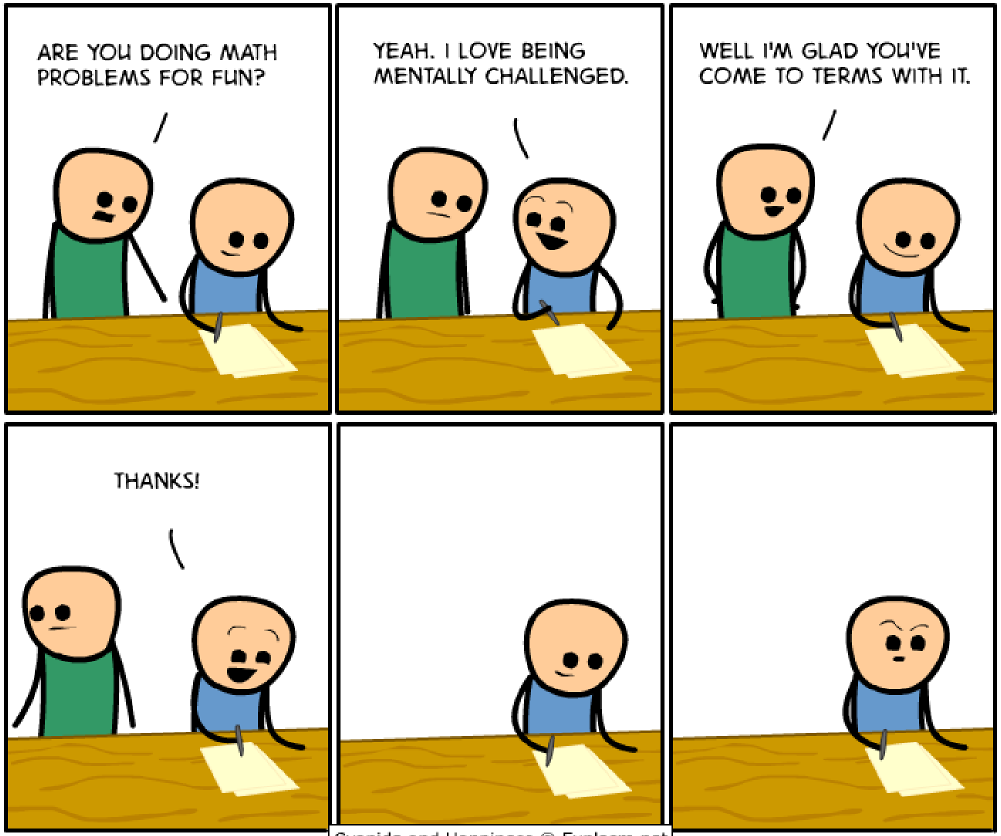
Spring 2015

Lecture 13: Primes, GCDs, modular inverses


ARE YOU DOING MATH PROBLEMS FOR FUN?
YEAH. I LOVE BEING MENTALLY CHALLENGED.
WELL I'M GLAD YOU'VE COME TO TERMS WITH IT.
THANKS!

Cyanide and Happiness © Explosm.net

review: repeated squaring

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: general algorithm

```
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$(a, k-1, m)) \bmod m$
```

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

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

primality

An integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*.

$p = 13$

A positive integer that is greater than 1 and is not prime is called *composite*.

$26 = 13 \times 2$

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

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

$$591 = 3 \cdot 197$$

$$45{,}523 = 45{,}523$$

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

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

$$1 = \underbrace{\qquad\qquad\qquad}_{\text{empty product}}$$

FACTORIZATION

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

$$n = p_1 \cdot p_2 \cdots p_k, \quad k \geq 2$$

If $p_1 > \sqrt{n}$, $p_2 > \sqrt{n}$

$$\Longrightarrow \quad p_1 \cdot p_2 > n$$

$n \geq$

contradiction.

EUCLID'S THEOREM

There are an infinite number of primes.

7. F

8. $F \to P$

9. P

Proof by contradiction:

Suppose that there are only a finite number of primes:

$p_1, p_2, \ldots, p_n$

$$\underbrace{p_1 p_2 \cdots p_n}_{} + 1 = p_{i_1} p_{i_2} \cdots p_{i_k}$$

$$4 \qquad 0 \qquad 1 \equiv 0 \pmod{p_{i_1}}$$

contradiction.

$p_1, \ldots, p_n$ first n primes

$$p_1 \cdots p_n + 1 = q_1 \cdots q_m \qquad \square$$

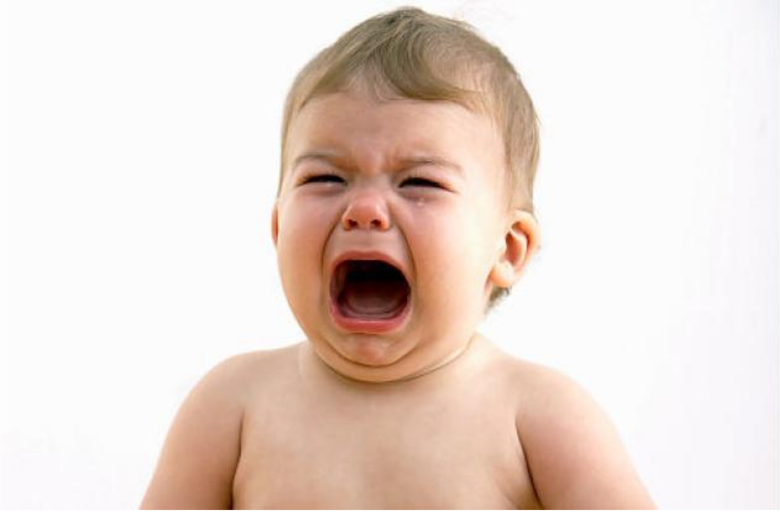
Famous Algorithmic Problems

- 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]:

123018668453011775513049495838496272077285
356959533479219732245215172640050726365751
874520219978646938995647494277406384592519
255732630345373154826850791702612214291346
167042921431160222124047927473779408066535
1419597459856902143413



1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

=

3347807169895689878604416984821269081770479498371376856891243138898288379387817 … 17
4308773781446799948

×

36746043666799590428244633799 … 643
430876426760322838157396665112 … 968
102700927987363089

GREATEST COMMON DIVISOR

GCD(a, b):

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

- GCD(100, 125) = 25
- GCD(17, 49) = 1
- GCD(11, 66) = 11
- GCD(13, 0) = 13
- GCD(180, 252) = $\boxed{36}$

$2^2 \cdot 3^2 \cdot 5$ $\quad$ $2^2 \cdot 3^2 \cdot 7$

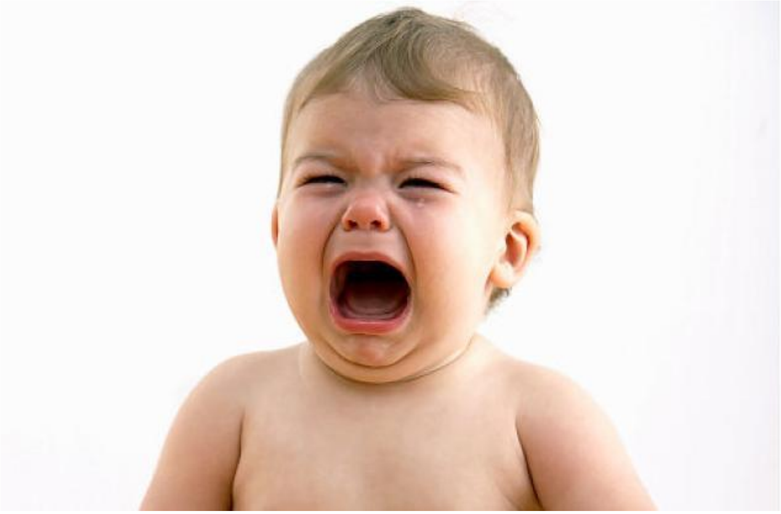
$2^2 \cdot 3^2 = \boxed{36}$

GCD and Factoring

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

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

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



Factoring is expensive!

Can we compute GCD(a,b) without factoring?

Useful GCD Fact

If a and b are positive integers, then

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

$a \equiv 0 \pmod{d}$

Proof:

By definition $\overset{0}{\cancel{a}} = \cancel{\overset{0}{(a \operatorname{div} b)} \cdot b} + \overset{0}{\cancel{\underline{(a \bmod b)}}} \pmod{d}$

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 $\underline{d \mid a}$.

EUCLID'S ALGORITHM

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

$$\begin{aligned}\mathrm{GCD}(660,126) &= \mathrm{GCD}(126, 30)\\ &= \mathrm{GCD}(30, 6)\\ &= \mathrm{GCD}(6, 0)\\ &= 6.\end{aligned}$$

$a > b$

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, a \bmod b)$$

Euclid's Algorithm

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

```
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

$$\gcd(a,b) = \boldsymbol{s}a + \boldsymbol{t}b$$

EXTENDED EUCLIDEAN ALGORITHM

$\underline{13(27}x) \equiv 4 \cdot 13 \pmod{35}$ $\qquad$ $1 \equiv 13 \cdot 27 \pmod{35}$

$x \equiv 17$

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

  $\gcd(a, b) = sa + tb$ $\qquad$ $1 = \gcd(35,27) = 13 \cdot 27 + (-10) \cdot 35$

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

$35 = 1 \cdot 27 + 8 \qquad 35 - 1 \cdot 27 = 8$

$27 = 3 \cdot 8 + 3 \qquad 27 - 3 \cdot 8 = 3$

$8 = 2 \cdot 3 + 2 \qquad 8 - 2 \cdot 3 = 2$

$3 = 1 \cdot 2 + 1 \qquad 3 - 1 \cdot 2 = 1$

$2 = 2 \cdot 1 + 0$

$27x \equiv 4 \pmod{35}$

$\Rightarrow$

$x \equiv 17 \pmod{35}$

- Substitute back from the bottom

$1 = 3 - 1 \cdot 2 \qquad = 3 - 1\,(8 - 2 \cdot 3) \qquad = (-1) \cdot 8 + 3 \cdot 3$

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

$=$

MULTIPLICATIVE INVERSE $\bmod m$

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

EXAMPLE

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