CSE 311

Foundations of Computing I

* All slides are a combined effort between previous instructors of the course

Famous Algorithmic Problems

- **Primality Testing** ← "easy"
  - Given an integer n, determine if n is prime
- **Factoring** ← "hard"
  - Given an integer n, determine the prime factorization of n

There are SIX handouts today. Please make sure to get all of them!! :)

Factoring

Factor the following 232 digit number [RSA768]:

123018668453011775513049495838496272077
285356959533479219732245215172640050726
365751874520219978646938995647494277406
384592519255732630345373154826850791702
612214291346167042921431160222124047927
4737794080665351419597459856902143413

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

$=$

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

$\times$

36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

Factoring

Uh…fun?

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

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

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

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

Factoring is expensive!

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

Useful GCD Fact

If *a* and *b* are positive integers, then

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

$d \mid a$ and $d \mid b$

$d \mid b$

$F_{a,b} = \{d : d \mid a \wedge d \mid b\}$

$F_{b,m} = \{d : d \mid b \wedge d \mid a \bmod b\}$

note $\max(F_{a,b}) = \gcd(a,b)$

WTP: $F_{a,b} = F_{b,m}$

Suppose $d \in F_{a,b}$. So, $d \mid a$ and $d \mid b$ by def. $F_{a,b}$.

$a = k_a d$, $b = k_b d$.

$a = a \bmod b + bq$

$a \bmod b = a - bq$

$= k_a d - (k_b d)q$

$= d(k_a - k_b q)$

Then $d \in F_{b,m}$

Useful GCD Fact

If a and b are positive integers, then

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

Proof:

By definition of mod, $a = qb + (a \bmod b)$ for some integer $q = a \text{ div } b$.

Let $d = \gcd(a,b)$. Then $d|a$ and $d|b$ so $a=kd$ and $b=jd$ for some integers k and j.
Therefore $(a \bmod b) = a - qb = kd - qjd = d(k - qj)$.
So, $d \mid (a \bmod b)$ and since $d \mid b$ we must have $d \le \gcd(b, a \bmod b)$.

Now, let $e = \gcd(b, a \bmod b)$. Then $e \mid b$ and $e \mid (a \bmod b)$. It follows that $b=me$ and $(a \bmod b) = ne$ for some integers m and n. Therefore

$$a = qb + (a \bmod b) = qme + ne = e(qm+n)$$

So, $e \mid a$ and since $e \mid b$ we must have $e \le \gcd(a, b)$.

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

Euclid's Algorithm

gcd(a, b) = GCD(b, a mod b)

```
int gcd(int a, int b){ /* a >= b, b > 0 */
    if (b == 0) {
        return a;
    }
    else {
        return gcd(b, a % b);
    }
```

gcd(660, 126) = gcd(126, 660 % 126)

= gcd(126, 30)

Example: GCD(660, 126)

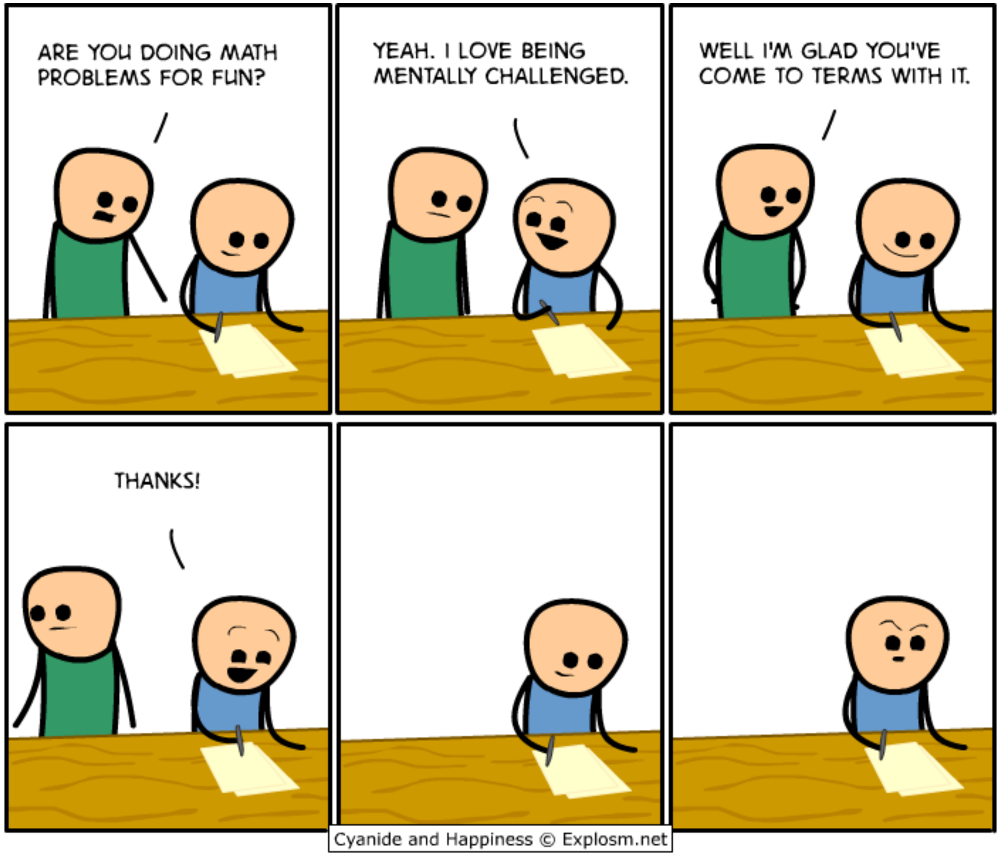
Euclid’s Algorithm

Repeatedly use the fact to reduce numbers until you get

gcd(660,126) = gcd(126, 660 mod 126) = gcd(126, 30)
= gcd(30, 126 mod 30) = gcd(30, 6)
= gcd(6, 30 mod 6) = gcd(6, 0)
= 6

CSE 311: Foundations of Computing

Lecture 13: Modular Inverses, Induction



Bézout's theorem

If a and b are positive integers, then there exist integers $\boldsymbol{s}$ and $\boldsymbol{t}$ such that

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

Extended Euclidean algorithm

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

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

Step 1 (Compute GCD & Keep Intermediary Information):

a b b (a mod b = m) b m a = q * b + m

$$\gcd(35, 27) = \gcd(27, 35 \bmod 27) = \gcd(27, 8) \quad (35 = 1 * 27 + 8)$$

Extended Euclidean algorithm

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

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

Step 1 (Compute GCD & Keep Intermediary Information):

a b	b a mod b = m	b m	a = q * b + m
$\gcd(35, 27)$	$= \gcd(27, 35 \bmod 27)$	$= \gcd(27, 8)$	$(35 = 1 * 27 + 8)$
	$= \gcd(8, 27 \bmod 8)$	$= \gcd(8, 3)$	$(27 = 3 * 8 + 3)$
	$= \gcd(3, 8 \bmod 3)$	$= \gcd(3, 2)$	$(8 = 2 * 3 + 2)$
	$= \gcd(2, 3 \bmod 2)$	$= \gcd(2, 1)$	$(3 = 1 * 2 + 1)$
	$= \gcd(1, 2 \bmod 1)$	$= \gcd(1, 0)$	

Extended Euclidean algorithm

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

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

Step 2 (Solve the equations for m):

a = q * b + m	m = a – q * b
$35 = 1 * 27 + 8$	$8 = 35 - 1 * 27$
$27 = 3 * 8 + 3$	$3 = 27 - 3 * 8$
$8 = 2 * 3 + 2$	$2 = 8 - 2 * 3$
$3 = 1 * 2 + 1$	$= 3 - 1 * 2$

gcd(35,27) = 1

$1 = 3 - 1 * (8 - 2 * 3)$

$= 3 * 3 + (-1) * 8$

$= 3 * (27 - 3 * 8) + (-1) * 8$

$= 3 * 27 + (-10) * 8$

Extended Euclidean algorithm

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

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

Step 2 (Solve the equations for m):

a = q * b + m	m = a – q * b
$35 = 1 * 27 + 8$	$8 = 35 - 1 * 27$
$27 = 3 * 8 + 3$	$3 = 27 - 3 * 8$
$8 = 2 * 3 + 2$	$2 = 8 - 2 * 3$
$3 = 1 * 2 + 1$	$1 = 3 - 1 * 2$

Extended Euclidean algorithm

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

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

Step 3 (Backward Substitute Equations):

$8 = 35 - 1 * 27$

$3 = 27 - 3 * 8$

$2 = 8 - 2 * 3$

$1 = 3 - 1 * 2$

Plug in the def of 2

$$1 = 3 - 1 * (8 - 2 * 3)$$
$$= 3 - 8 + 2 * 3$$
$$= (-1) * 8 + 3 * 3$$

Re-arrange into 3's and 8's

Plug in the def of 3

$$= (-1) * 8 + 3 * (27 - 3 * 8)$$
$$= (-1) * 8 + 3 * 27 + (-9) * 8$$
$$= 3 * 27 + (-10) * 8$$

Re-arrange into 8's and 3's

$$= 3 * 27 + (-10) * (35 - 1 * 27)$$
$$= 3 * 27 + (-10) * 35 + 10 * 27$$
$$= 13 * 27 + (-10) * 35$$

Re-arrange into 27's and 35's

multiplicative inverse $\mathrm{mod}\ m$

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:

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

Example

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

$7x + 26y = 1$

$\gcd(26, 7) = \gcd(7, 26 \bmod 7)$
$= \gcd(5, 7 \bmod 5)$
$= \gcd(2, 1)$
$= \gcd(1, 0)$

$26 = 3 * 7 + 5$
$7 = 1 * 5 + 2$
$5 = 2 * 2 + 1$
$2 =$

Example

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

gcd(26, 7) = gcd(7, 5) = gcd(5, 2) = gcd(2, 1) = 1

26 = 7*3 + 5	5 = 26 – 7*3
7 = 5*1 + 2	2 = 7 – 5*1
5 = 2*2 + 1	1 = 5 – 2*2

1 = 5 – (7 – 5*1)*2
= (–7)*2 + 5*3
= (–7)*2 + (26 – 7*3)*3
= 7*(-11) + 26*3

So, $x = 15 + 26k$ for $k \in \mathrm{N}$.