



# Foundations of Computing I

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

## 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  
 4737794080665351419597459856902143413

12301866845301177551304949583849627207728535695953347  
 92197322452151726400507263657518745202199786469389956  
 47494277406384592519255732630345373154826850791702612  
 21429134616704292143116022212404792747377940806653514  
 19597459856902143413

=

334780716989568987860441698482126908177047949837  
 137685689124313889828837938780022876147116525317  
 43087737814467999489

×

367460436667995904282446337996279526322791581643  
 430876426760322838157396665112792333734171433968  
 10270092798736308917

## 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

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

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

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

Factoring is expensive!

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

## Useful GCD Fact

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

Proof:

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

Let  $d = \text{gcd}(a,b)$ . Then  $d \mid a$  and  $d \mid b$  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  $d \leq \text{gcd}(b, a \bmod b)$ .

Now, let  $e = \text{gcd}(b, a \bmod b)$ . 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  $e \leq \text{gcd}(a, b)$ .

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

## Euclid's Algorithm

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

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

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

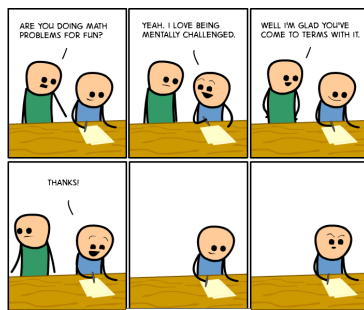
## Euclid's Algorithm

Repeatedly use the fact to reduce numbers until you get

$$\begin{aligned} \text{gcd}(660, 126) &= \text{gcd}(126, 660 \bmod 126) = \text{gcd}(126, 30) \\ &= \text{gcd}(30, 126 \bmod 30) = \text{gcd}(30, 6) \\ &= \text{gcd}(6, 30 \bmod 6) = \text{gcd}(6, 0) \\ &= 6 \end{aligned}$$

## CSE 311: Foundations of Computing

### Lecture 13: Modular Inverses, Induction



## Bézout's theorem

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

$$\text{gcd}(a,b) = sa + tb.$$

## 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):

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

## 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  $m$ ):

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

## Extended Euclidean algorithm

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

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

Step 3 (Backward Substitute Equations):

$8 = 35 - 1 * 27$	
$3 = 27 - 3 * 8$	$1 = 3 - 1 * 2$
$2 = 8 - 2 * 3$	$= 3 - 1 * (8 - 2 * 3)$
$1 = 3 - 1 * 2$	$= 3 - 8 + 2 * 3$
	$= (-1) * 8 + 3 * 3$
	$= (-1) * 8 + 3 * (27 - 3 * 8)$
	$= (-1) * 8 + 3 * 27 + (-9) * 8$
	$= 3 * 27 + (-10) * 8$
	$= 3 * 27 + (-10) * (35 - 1 * 27)$
	$= 3 * 27 + (-10) * 35 + 10 * 27$
	$= 13 * 27 + (-10) * 35$

## 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  $a$ :

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

## Example

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

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

$$26 = 7 * 3 + 5 \quad 5 = 26 - 7 * 3$$

$$7 = 5 * 1 + 2 \quad 2 = 7 - 5 * 1$$

$$5 = 2 * 2 + 1 \quad 1 = 5 - 2 * 2$$

$$1 = 5 - (7 - 5 * 1) * 2$$

$$= (-7) * 2 + 5 * 3$$

$$= (-7) * 2 + (26 - 7 * 3) * 3$$

$$= 7 * (-11) + 26 * 3$$

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