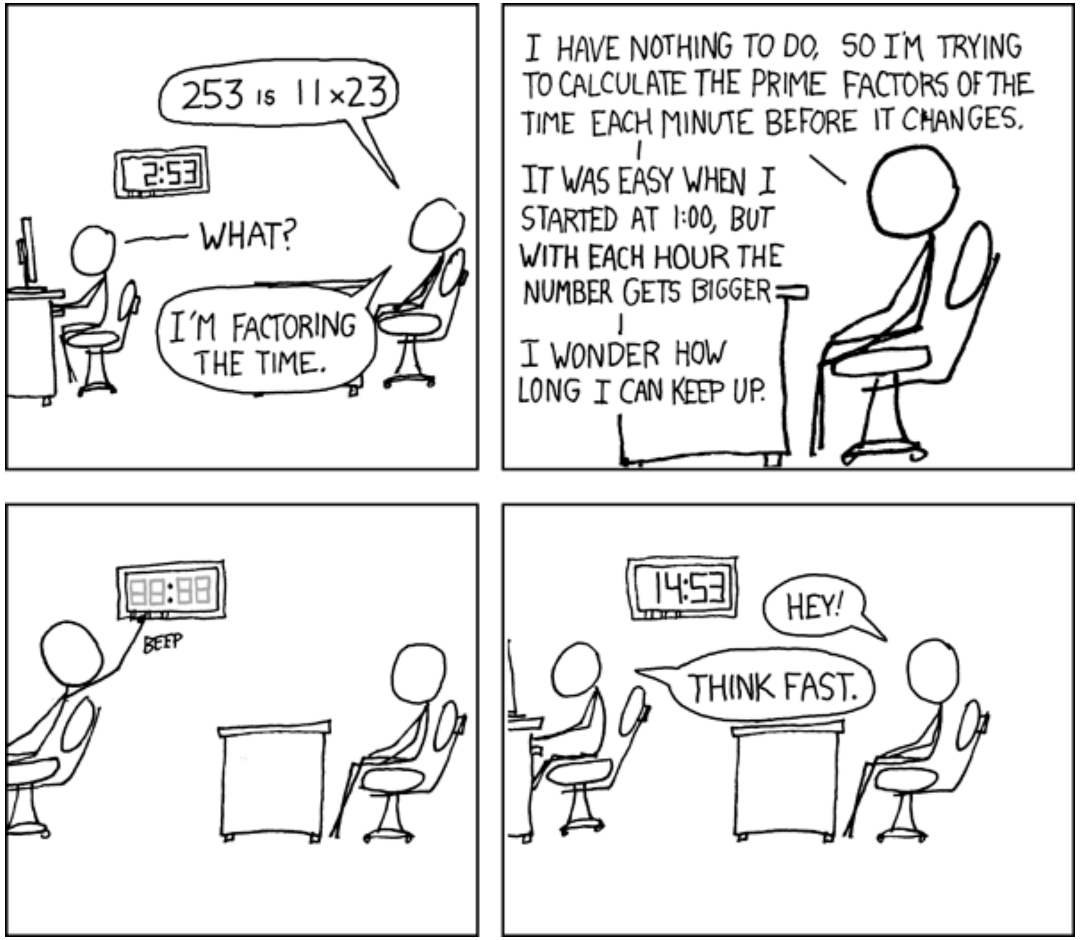


xkcd.com/247

# GCD and the Euclidian Algorithm

CSE 311 Fall 2020
Lecture 13

# Try using the contrapositive yourselves!

Show for any sets $A, B, C$: if $A \nsubseteq (B \cup C)$ then $A \nsubseteq C$.

1. What do the terms in the statement mean?
2. What does the statement as a whole say?
3. Where do you start?
4. What's your target?
5. Finish the proof ☺

Fill out the poll everywhere for Activity Credit!

Go to pollev.com/cse311 and login with your UW identity
Or text cse311 to 37607

# Try it yourselves!

Show for any sets $A, B, C$: if $A \nsubseteq (B \cup C)$ then $A \nsubseteq C$.

Proof:

We argue by contrapositive,

Let $A, B, C$ be arbitrary sets, and suppose $A \subseteq C$.

Let $x$ be an arbitrary element of $A$. By definition of subset, $x \in C$. By definition of union, we also have $x \in B \cup C$. Since $x$ was an arbitrary element of $A$, we have $A \subseteq (B \cup C)$.

Since $A, B, C$ were arbitrary, we have: if $A \nsubseteq (B \cup C)$ then $A \nsubseteq C$.

# Divisors and Primes

# Inverses

## Inverse

Given a function $f \colon N \rightarrow N$,

if $x \neq y$ implies $f(x) \neq f(y)$

then define the *inverse* of $f$, called $f^{-1}$,

to be $f^{-1}(y) = x$ for $f(x) = y$.

Why is there one unique such $f^{-1}$?

What is $f^{-1}(f(\mathrm{x}))$?

What is $f(f^{-1}(\mathrm{x}))$?

# Inverses of operations

## Inverse (modular arithmetic)

Fix two integers $i, n \geq 0$.

We call *j* an *additive inverse of i mod n* if $(i + j) \equiv 0 \pmod{n}$

We call *j* a *multiplicative inverse of i mod n* if $(i \cdot j) \equiv 1 \pmod{n}$

# Primes and FTA

## Prime

An integer $p > 1$ is prime iff its only positive divisors are 1 and $p$. Otherwise it is "composite"

## Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization.

# GCD and LCM

## Greatest Common Divisor

The Greatest Common Divisor of $a$ and $\boldsymbol{b}$ (gcd(a,b)) is the largest integer $\boldsymbol{c}$ such that $\boldsymbol{c}|\boldsymbol{a}$ and $\boldsymbol{c}|\boldsymbol{b}$

## Least Common Multiple

The Least Common Multiple of $a$ and $\boldsymbol{b}$ (lcm(a,b)) is the smallest positive integer $\boldsymbol{c}$ such that $\boldsymbol{a}|\boldsymbol{c}$ and $\boldsymbol{b}|\boldsymbol{c}$.

# Try a few values…

gcd(100,125)

gcd(17,49)

gcd(17,34)

gcd(13,0)

lcm(7,11)

lcm(6,10)

```
public int Mystery(int m, int n){
     if(m<n){
          int temp = m;
          m=n;
          n=temp;
     }
     while(n != 0) {
          int rem = m % n;
          m=n;
          n=rem;
     }
     return m;
}
```

# How do you calculate a gcd?

You could:

Find the prime factorization of each

Take all the common ones. E.g.

gcd(24,20)=gcd($2^3 \cdot 3, 2^2 \cdot 5) = 2\text{^}\{\min(2,3)\} = 2\text{^}2 = 4$.

(lcm has a similar algorithm – take the maximum number of copies of everything)

But that's….really expensive. Mystery from a few slides ago finds gcd.

# Two useful facts

## gcd Fact 1

**If $a, b$ are positive integers, then gcd$(a, b)$ = gcd$(b, a\%b)$**

Tomorrow's lecture we'll prove this fact.  For now: just trust it.

## gcd Fact 2

**Let $a$ be a positive integer: gcd$(a, 0) = $ a**

Does $a|a$ and $a|0$? Yes $a \cdot 1 = a$; $a \cdot 0 = a$.

Does anything greater than $a$ divide $a$?

```
public int Mystery(int m, int n){
     if(m<n){
          int temp = m;
          m=n;
          n=temp;
     }
     while(n != 0) {
          int rem = m % n;
          m=n;
          n=rem;
     }
     return m;
}
```

# Euclid’s Algorithm

```
while(n != 0) {
        int rem = m % n;
        m=n;
        n=rem;
    }
```

gcd(660,126)

# Euclid's Algorithm

```
while(n != 0) {
        int rem = m % n;
        m=n;
        n=rem;
    }
```

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

Tableau form

$$
\begin{aligned}
660 &= 5 \cdot 126 + 30\\
126 &= 4 \cdot 30 + 6\\
30 &= 5 \cdot 6 + 0
\end{aligned}
$$

Starting Numbers

Final answer

# Bézout's Theorem

**Bézout's Theorem**

**If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that**
**gcd(a,b)$= sa + tb$**

We're not going to prove this theorem…

But we'll show you how to find $s$,$t$ for any positive integers $a, b$.

# Extended Euclidian Algorithm

**Step 1 compute gcd(a,b); keep tableau information.**

Step 2 solve all equations for the remainder.

Step 3 substitute backward

gcd(35,27)

# Extended Euclidian Algorithm

**Step 1 compute gcd(a,b); keep tableau information.**

Step 2 solve all equations for the remainder.

Step 3 substitute backward

gcd(35,27) = gcd(27, 35%27) = gcd(27,8)
= gcd(8, 27%8) = gcd(8, 3)
= gcd(3, 8%3) = gcd(3, 2)
= gcd(2, 3%2) = gcd(2,1)
= gcd(1, 2%1) = gcd(1,0)

$$35 = 1 \cdot 27 + 8$$
$$27 = 3 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

# Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

**Step 2 solve all equations for the remainder.**

Step 3 substitute backward

$$
\begin{aligned}
35 &= 1 \cdot 27 + 8 \\
27 &= 3 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}
$$

# Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

**Step 2 solve all equations for the remainder.**

Step 3 substitute backward

$$35 = 1 \cdot 27 + 8$$
$$27 = 3 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

$$8 = 35 - 1 \cdot 27$$
$$3 = 27 - 3 \cdot 8$$
$$2 = 8 - 2 \cdot 3$$
$$1 = 3 - 1 \cdot 2$$

# Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

# Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

**Step 3 substitute backward**

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

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

# Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

**Step 3 substitute backward**

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

gcd(27,35) = $13 \cdot 27 + (-10) \cdot 35$

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

When substituting back, you keep the larger of $m, n$ and the number you just substituted. Don't simplify further! (or you lose the form you need)

# So…what's it good for?

Suppose I want to solve $7x \equiv 1(mod\ n)$

Just multiply both sides by $\frac{1}{7}$…

Oh wait. We want a number to multiply by $\mathbf{7}$ to get $\mathbf{1}$.

If the gcd(7,n) = 1

Then $s \cdot 7 + tn = 1$, so $7s - 1 = -tn$ i.e. $n|(7s - 1)$ so $7s \equiv 1(mod\ n)$.

So the $s$ from Bézout's Theorem is what we should multiply by!

# Try it

Solve the equation $7y \equiv 3(mod\ 26)$

What do we need to find?

The multiplicative inverse of $7(\mathbf{mod}\ 26)$

# Multiplicative Inverse

The number $b$ is a multiplicative inverse of $a$ (mod $n$) if $ba \equiv 1(mod\ n)$.

If gcd$(a, n) = 1$ then the multiplicative inverse exists.

If gcd$(a, n) \neq 1$ then the inverse does not exist.

Arithmetic $(mod\ p)$ for $p$ prime is really nice for that reason.

Sometimes equivalences still have solutions when you don't have inverses (but sometimes they don't)

# Finding the inverse…

gcd(26,7) = gcd(7, 26%7) = gcd(7,5)

= gcd(5, 7%5) = gcd(5,2)

= gcd(2, 5%2) = gcd(2, 1)

= gcd(1, 2%1) = gcd(1,0)= 1.

$$26 = 3 \cdot 7 + 5\ ;\ 5 = 26 - 3 \cdot 7$$

$$7 = 5 \cdot 1 + 2\ ;\ 2 = 7 - 5 \cdot 1$$

$$5 = 2 \cdot 2 + 1\ ;\ 1 = 5 - 2 \cdot 2$$

$$1 = 5 - 2 \cdot 2$$
$$= 5 - 2(7 - 5 \cdot 1)$$
$$= 3 \cdot 5 - 2 \cdot 7$$
$$= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7$$
$$3 \cdot 26 - 11 \cdot 7$$

$-11$ is a multiplicative inverse.
We'll write it as 15, since we're working mod 26.

# Try it

Solve the equation $7y \equiv 3(mod\ 26)$

What do we need to find?
The multiplicative inverse of $7\ (mod\ 26)$.

$15 \cdot 7 \cdot y \equiv 15 \cdot 3(mod\ 26)$

$y \equiv 45(mod\ 26)$

Or $y \equiv 19(mod\ 26)$

So $26|19 - y$, i.e. $26k = 19 - y$ (for $k \in \mathbb{Z}$) i.e. $y = 19 - 26 \cdot k$ for any $k \in \mathbb{Z}$

So $\{\dots, -7, 19, 45, \dots 19 + 26k, \dots\}$

# And now, for some proofs!

# GCD fact

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

How do you show two gcds are equal?

Call $a = \text{gcd}(w, x), b = \text{gcd}(y, z)$

If $b|w$ and $b|x$ then $b$ is a common divisor of $w, x$ so $b \leq a$

If $a|y$ and $a|z$ then $a$ is a common divisor of $y, z,$ so $a \leq b$

If $a \leq b$ and $b \leq a$ then $a = b$

# gcd(a,b) = gcd(b, a % b)

Let $\mathrm{x} = \mathrm{gcd}(a, b)$ and $y = \mathrm{gcd}(b, a\%b)$.

We show that $y$ is a common divisor of $a$ and $b$.

By definition of gcd, $y|b$ and $y|(a\%b)$. So it is enough to show that $y|a$.

Applying the definition of divides we get $b = yk$ for an integer $k$, and $(a\%b) = yj$ for an integer $j$.

By definition of mod, $a\%b$ is $a = qb + (a\%b)$ for an integer $q$.

Plugging in both of our other equations:

$a = qyk + yj = y(qk + j)$. Since $q, k$, and $j$ are integers, $y|a$. Thus $y$ is a common divisor of $a, b$ and thus $y \leq x$.

# gcd(a,b) = gcd(b, a % b)

Let $\mathrm{x} = \mathrm{gcd}(a, b)$ and $y = \mathrm{gcd}(b, a\%b)$.

We show that $x$ is a common divisor of $b$ and $\mathrm{a}\%b$.

By definition of gcd, $\mathrm{x}|b$ and $x|a$. So it is enough to show that $\mathrm{x}|(a\%b)$.

Applying the definition of divides we get $b = xk'$ for an integer $k'$, and $\mathrm{a} = xj'$ for an integer $j'$.

By definition of mod, $a\%b$ is $a = qb + (a\%b)$ for an integer $q$

Plugging in both of our other equations:

$xj' = qxk' + a\%b$. Solving for $a\%b$, we have $a\%b = xj' - qxk' = x(j' - qk')$. So $x|(a\%b)$. Thus $x$ is a common divisor of $b, a\%b$ and thus $x \leq y$.

# gcd(a,b) = gcd(b, a % b)

Let $\mathrm{x} = \gcd(a, b)$ and $y = \gcd(b, a\%b)$.

We show that $x$ is a common divisor of $b$ and $\mathrm{a}\%b$.

We have shown $x \leq y$ and $y \leq x$.

Thus $x = y$, and $\gcd(a, b) = \gcd(b, a\%b)$.