IF YOU ASSUME CONTRADICTION AXIOMS, YOU CAN DERIVE ANYTHING. IT'S CALLED THE PRINCIPLE OF EXPLOSION.

ANYTHING? LEMME TRY.

HEY, YOU'RE RIGHT! I STARTED WITH PA-
AND DERIVED YOUR MOM'S PHONE NUMBER!

THAT'S NOT HOW THAT WORKS.

WAIT, THIS IS HER NUMBER! HOW-

Hi, I'm a friend of... why, yes, I am free tonight!

MOM!

NO! BOX WINE SOUNDS LOVELY!
What we have proven so far:

- Let $a, b, c, d$ and $m > 0$ be integers.
  
  • If $a \equiv_m b$, then $b \equiv_m a$.
  
  • If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.
  
  • If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.
  
  • If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

Todo:

- $a \equiv_m b$ if and only if $a \% m = b \% m$. 
Claim 5: For integers $a, b$ and $m > 0$, $a \equiv_m b$ if and only if $a \% m = b \% m$. 
For integers $a, b$ and $m > 0$, $a \equiv_m b$ if and only if $a \% m = b \% m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv_m b$. Then $m \mid (a - b)$. So there exists some integer $k$ such that $a - b = km$. So $a = km + b$.

By the Division Theorem, $a = qm + (a \% m)$ for some integer $q$, where $0 \leq a \% m < m$. Thus:

$$km + b = qm + (a \% m)$$

$$b = qm - km + (a \% m)$$

$$b = (q - k)m + (a \% m)$$

By the Division Theorem again, we have that $b \% m = a \% m$.

Since $a, b, m$ were arbitrary, the claim holds.
For integers \( a, b \) and \( m > 0 \), \( a \equiv_m b \) if and only if \( a \% m = b \% m \).

\[ \iff a, b, m > 0 \text{ are arbitrary integers, and suppose } a \% m = b \% m. \text{ By the Division Theorem, } a = mq + (a \% m) \text{ for some integer } q, \text{ and } b = ms + (b \% m) \text{ for some integer } s. \text{ Thus:} \]

\[ a - b = (mq + (a \% m)) - (ms + (b \% m)) \]

\[ a - b = mq - ms + (a \% m) - (b \% m) \]

\[ a - b = m(q - s) \]

Since \( q, s \) are integers, \( q - s \) is an integer. So \( m \mid (a - b) \). So \( a \equiv_m b \).

Since \( a, b, m \) were arbitrary, the claim holds.
Summary: Properties of Mod

- Let $a, b, c, d$ and $m > 0$ be integers.
  
  - If $a \equiv_m b$, then $b \equiv_m a$.
  
  - If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.
  
  - If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.
  
  - If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.
  
  - $a \equiv_m b$ if and only if $a \% m = b \% m$. 
Another contrapositive example
Another Proof

For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:
Let $a, b, c$ be arbitrary integers, and suppose $a \nmid (bc)$. Then there is not an integer $z$ such that $az = bc$

... 

So $a \nmid b$ or $a \nmid c$
Another Proof

For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:
Let $a, b, c$ be arbitrary integers, and suppose $a \nmid (bc)$.
Then there is not an integer $z$ such that $az = bc$

... 

So $a \nmid b$ or $a \nmid c$
Another Proof

For all integers, \( a, b, c \): Show that if \( a \nmid (bc) \) then \( a \nmid b \) or \( a \nmid c \).

There has to be a better way!
If only there were some equivalent implication...
One where we could negate everything...

Take the contrapositive of the statement:
For all integers, \( a, b, c \): Show if \( a | b \) and \( a | c \) then \( a | (bc) \).
Claim: For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let $a, b, c$ be arbitrary integers, and suppose $a|b$ and $a|c$.

Therefore $a|bc$
By contrapositive

Claim: For all integers, $a, b, c$: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let $a, b, c$ be arbitrary integers, and suppose $a \mid b$ and $a \mid c$.

By definition of divides, $ax = b$ and $ay = c$ for integers $x$ and $y$.

Multiplying the two equations, we get $axay = bc$

Since $a, x, y$ are all integers, $xay$ is an integer. Applying the definition of divides, we have $a \mid bc$. 
Logical Ordering
Logical Ordering

• When doing a proof, we often work from both sides...
• But we have to be careful!
• When you read from top to bottom, every step has to follow only from what’s before it, not after it.

• Suppose our target is $q$ and I know $q \rightarrow p$ and $r \rightarrow q$.
• What can I put as a “new target?”
Logical Ordering

• So why have all our prior steps been ok backward?

• They’ve all been either:
  - A definition (which is always an “if and only if”)
  - An algebra step that is an “if and only if”

• Even if your steps are “if and only if” you still have to put everything in order – start from your assumptions, and only assert something once it can be shown.
A bad proof (Backwards Proof)

Claim: if $x$ is positive then $x + 5 = -x - 5$.

\[
\begin{align*}
x + 5 &= -x - 5 \\
x + 5 &= -x - 5 \\
|x + 5| &= |-x - 5| \\
|x + 5| &= |-(x + 5)| \\
|x + 5| &= |x + 5| \\
0 &= 0
\end{align*}
\]

This claim is false – if you’re trying to do algebra, you need to start with an equation you know (say $x = x$ or $2 = 2$ or $0 = 0$) and expand to the equation you want.
Algorithmic Problems

• Multiplication
  - Given primes $p_1, p_2, ..., p_k$, calculate their product $p_1 p_2 ... p_k$

• Factoring
  - Given an integer $n$, determine the prime factorization of $n$
Factoring

Factor the following 232 digit number [RSA768]:

```
123018668453011775513049495838496272
077285356959533479219732245215172640
050726365751874520219978646938995647
494277406384592519255732630345373154
826850791702612214291346167042921431
160222124047927473779408066535141959
7459856902143413
```
123018668453011775513049495838496272077285356959
533479219732245215172640050726365751874520219978
646938995647494277406384592519255732630345373154
826850791702612214291346167042921431160222124047
9274737794080665351419597459856902143413

= 

334780716989568987860441698482126908177047949837
137685689124313889828837938780022876147116525317
43087737814467999489

×

367460436667995904282446337996279526322791581643
430876426760322838157396665112792333734171433968
10270092798736308917
Famous Algorithmic Problems

- **Factoring**
  - Given an integer $n$, determine the prime factorization of $n$

- **Primality Testing**
  - Given an integer $n$, determine if $n$ is prime

- **Factoring** is hard
  - (on a classical computer)

- **Primality Testing** is easy
Prime and Composite

- **Definition:**
  An integer \( p > 1 \) is prime iff its only positive divisors are 1 and \( p \).

- An integer \( p > 1 \) is composite iff it is not prime.
Fundamental Theorem of Arithmetic

Every Positive integer greater than 1 has a “unique” prime factorization:

e.g: $42 = 2 \times 2 \times 2 \times 3$, $591 = 3 \times 197$, etc...
Greatest Common Divisor

- **Definition:**
  The Greatest Common Divisor of integers $a$ and $b$ (denoted $\text{gcd}(a, b)$) is the largest integer $c$ such that $c \mid a$ and $c \mid b$.

- **Useful Fact:** Let $a$ be a positive integer. The $\text{GCD}(a, 0) = a$

- **For Example:**
  
  $\text{gcd}(99, 18) = 9$  \hspace{1cm}  $\text{gcd}(7, 11) = 1$
  
  $\text{gcd}(100, 125) = 25$  \hspace{1cm}  $\text{gcd}(13, 0) = 13$
Calculating the GCD: Approach 1

- **Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 has a unique prime factorization.

- Approach 1 to finding $\gcd(a, b)$:
  1. Find the prime factorization of $a$
  2. Find the prime factorization of $b$
  3. Identify all common prime factors.
  4. Multiply the common prime factors together. This is the GCD.

**VERY INEFFICIENT**
Calculating the GCD: Approach 2

- Claim: For positive integers $a, b$, $gcd(a, b) = gcd(b, a \% b)$.

- For example:
  - $gcd(10, 6) = gcd(6, 4)$
  - $gcd(110, 30) = gcd(30, 20)$

- We’ll prove this in a minute. But first: how can we use this fact to devise an algorithm for computing $gcd(a, b)$?
Calculating the GCD: Approach 2

- Euclid’s Algorithm. To find \( \text{gcd}(a, b) \):
  - Repeatedly use \( \text{gcd}(a, b) = \text{gcd}(b, a \mod b) \) to reduce numbers
  - Stop once you reach \( \text{gcd}(g, 0) \). Return \( g \).

- For Example:
  \[
  \begin{align*}
  \text{gcd}(660, 126) &= \text{gcd}(126, 30) \\
  &= \text{gcd}(30, 6) \\
  &= \text{gcd}(6, 0) \\
  &= 6
  \end{align*}
  \]
Euclid’s Algorithm in Java

- // assumes a >= 0 and b >= 0
- public int gcd(int a, int b) {
-     if (b == 0) {
-         return a;
-     } else {
-         return gcd(b, a % b);
-     }
- }

Proof of Claim

- Claim: For positive integers $a, b$, $\gcd(a, b) = \gcd(b, a \% b)$.

- How do you show that two GCDs are equal?
  • First consider some arbitrary common divisor of $a$ and $b$, call it $d$. Prove that $d$ is a divisor of $a \% b$.
  • Then consider some arbitrary common divisor of $b$ and $a \% b$, call it $d$. Prove that $d$ is a divisor of $a$.
  • Thus $a$ and $b$ have the same common divisors as $b$ and $a \% b$. So their GCDs are equal.
Claim: For positive integers \( a, b, \gcd(a, b) = \gcd(b, a \mod b) \).

Let \( a, b \) be arbitrary positive integers. By the Division Theorem, \( a = qb + (a \mod b) \) for some int \( q \).

Let \( d \) be arbitrary. Suppose \( d \mid b \) and \( d \mid a \mod b \). We aim to show that \( d \mid a \). By definition of divides, \( b = kd \) and \( a \mod b = jd \) for some integers \( k, j \). Then it follows that:

\[
a = qb + (a \mod b) = q \cdot kd + jd = d(qk + j)
\]

Since \( q, k, j \) are integers, \( qk + j \) is an integer. So \( d \mid a \).

Now suppose \( d \mid a \) and \( d \mid b \). We aim to show that \( d \mid a \mod b \). By definition of divides, \( a = md \) and \( b = nd \) for some integers \( m, n \). Then it follows that:

\[
a \mod b = a - qb = md - qnd = d(m -qn)
\]

Since \( q, m, n \) are integers, \( m - qn \) is an integer. So \( d \mid a \mod b \).

Thus \( a \) and \( b \) have the same common divisors as \( b \) and \( a \mod b \). So \( \gcd(a, b) = \gcd(b, a \mod b) \).

Since \( a, b \) were arbitrary, the claim holds.
Bézout’s theorem

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

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

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

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

Step 1 (Compute GCD & Keep Tableau Information):

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>b</th>
<th>a mod b = r</th>
<th>b</th>
<th>r</th>
<th>a = q * b + r</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>27</td>
<td>27</td>
<td>35 mod 27 = 8</td>
<td>27</td>
<td>8</td>
<td>35 = 1 * 27 + 8</td>
</tr>
</tbody>
</table>
## Extended Euclidean algorithm

- Can use Euclid’s Algorithm to find $s, t$ such that
  \[
gcd(a, b) = sa + tb
\]

### Step 1 (Compute GCD & Keep Tableau Information):

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$b$</th>
<th>$a$ mod $b$</th>
<th>$r$</th>
<th>$b$</th>
<th>$r$</th>
<th>$a = q * b + r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>27</td>
<td>27</td>
<td>35 mod 27</td>
<td>8</td>
<td>27</td>
<td>3</td>
<td>35 = 1 * 27 + 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>35</td>
<td>27 mod 8</td>
<td>3</td>
<td>8</td>
<td>3</td>
<td>27 = 3 * 8 + 3</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>8</td>
<td>8 mod 3</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>8 = 2 * 3 + 2</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>3</td>
<td>3 mod 2</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>3 = 1 * 2 + 1</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2</td>
<td>2 mod 1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1</td>
<td>1 mod 0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
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 $r$):

\[
\begin{align*}
   a &= q \cdot b + r \\
   35 &= 1 \cdot 27 + 8 \\
   27 &= 3 \cdot 8 + 3 \\
   8 &= 2 \cdot 3 + 2 \\
   3 &= 1 \cdot 2 + 1 \\
\end{align*}
\]

\[
\begin{align*}
   r &= a - q \cdot b \\
   8 &= 35 - 1 \cdot 27
\end{align*}
\]
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 $r$):

\[
\begin{align*}
  a &= q \times b + r \\
  35 &= 1 \times 27 + 8 \\
  27 &= 3 \times 8 + 3 \\
  8 &= 2 \times 3 + 2 \\
  3 &= 1 \times 2 + 1
\end{align*}
\]

\[
\begin{align*}
  r &= a - q \times b \\
  8 &= 35 - 1 \times 27 \\
  3 &= 27 - 3 \times 8 \\
  2 &= 8 - 2 \times 3 \\
  1 &= 3 - 1 \times 2
\end{align*}
\]
Extended Euclidean algorithm

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

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

**Step 3 (Backward Substitute Equations):**

$$8 = 35 - 1 \times 27$$

$$3 = 27 - 3 \times 8$$

$$2 = 8 - 2 \times 3$$

$$\boxed{1 = 3 - 1 \times 2}$$
Extended Euclidean algorithm

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

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

Step 3 (Backward Substitute Equations):

Plug in the def of 2

$1 = 3 - 1 \cdot (8 - 2 \cdot 3)$

$= 3 - 8 + 2 \cdot 3$

$= (-1) \cdot 8 + 3 \cdot 3$

Re-arrange into 3’s and 8’s

$8 = 35 - 1 \cdot 27$

$3 = 27 - 3 \cdot 8$

$2 = 8 - 2 \cdot 3$

$1 = 3 - 1 \cdot 2$
Extended Euclidean algorithm

- Can use Euclid’s Algorithm to find \( s, t \) such that

\[
gcd(a, b) = sa + tb
\]

Step 3 (Backward Substitute Equations):

\[
8 = 35 - 1 \times 27
\]
\[
3 = 27 - 3 \times 8
\]
\[
2 = 8 - 2 \times 3
\]
\[
1 = 3 - 1 \times 2
\]

\[
1 = 3 - 1 \times (8 - 2 \times 3)
= 3 - 8 + 2 \times 3
= (-1) \times 8 + 3 \times 3
= (-1) \times 8 + 3 \times (27 - 3 \times 8)
= (-1) \times 8 + 3 \times 27 + (-9) \times 8
= 3 \times 27 + (-10) \times 8
\]

Plug in the def of 2
Re-arrange into 3’s and 8’s
Plug in the def of 3
Re-arrange into 8’s and 27’s
Extended Euclidean algorithm

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

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

**Step 3 (Backward Substitute Equations):**

1. **Plug in the def of 2**
   
   
   $$8 = 35 - 1 \times 27$$
   
   $$3 = 27 - 3 \times 8$$
   
   $$2 = 8 - 2 \times 3$$
   
   $$1 = 3 - 1 \times 2$$

   2. **Re-arrange into 3’s and 8’s**

   $$1 = 3 - 1 \times (8 - 2 \times 3)$$
   
   $$= 3 - 8 + 2 \times 3$$
   
   $$= (-1) \times 8 + 3 \times 3$$

   3. **Plug in the def of 3**

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

   4. **Re-arrange into 8’s and 27’s**

   $$= 3 \times 27 + (-10) \times (35 - 1 \times 27)$$
   
   $$= 3 \times 27 + (-10) \times 35 + 10 \times 27$$
   
   $$= 13 \times 27 + (-10) \times 35$$
Let $0 \leq a, b < m$. Then, $b$ is the multiplicative inverse of $a$ (modulo $m$) iff $ab \equiv_m 1$.

$$
\begin{array}{c|ccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\
3 & 0 & 3 & 6 & 2 & 5 & 1 & 4 \\
4 & 0 & 4 & 1 & 5 & 2 & 6 & 3 \\
5 & 0 & 5 & 3 & 1 & 6 & 4 & 2 \\
6 & 0 & 6 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
$$

mod 7

$$
\begin{array}{c|ccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
2 & 0 & 2 & 4 & 6 & 8 & 0 & 2 & 4 & 6 & 8 \\
3 & 0 & 3 & 6 & 9 & 2 & 5 & 8 & 1 & 4 & 7 \\
4 & 0 & 4 & 8 & 2 & 6 & 0 & 4 & 8 & 2 & 6 \\
5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 & 0 & 5 \\
6 & 0 & 6 & 2 & 8 & 4 & 0 & 6 & 2 & 8 & 4 \\
7 & 0 & 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \\
8 & 0 & 8 & 6 & 4 & 2 & 0 & 8 & 6 & 4 & 2 \\
9 & 0 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
$$

mod 10
Suppose $\gcd(a, m) = 1$

By Bézout’s Theorem, there exist integers $s$ and $t$ such that $sa + tm = 1$.

$s$ is the multiplicative inverse of $a$ (modulo $m$):

$$1 = sa + tm \equiv_m sa$$

So... we can compute multiplicative inverses with the extended Euclidean algorithm

These inverses let us solve modular equations...
Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$  
Find multiplicative inverse of $7$ modulo $26$
Example: Solve a Modular Equation

Solve: \( 7x \equiv_{26} 3 \)  
Find multiplicative inverse of 7 modulo 26

\[
gcd(26, 7) = gcd(7, 5) = gcd(5, 2) = gcd(2, 1) = 1
\]
Example: Solve a Modular Equation

Solve: \( 7x \equiv_{26} 3 \)  
Find multiplicative inverse of 7 modulo 26

\[
gcd(26, 7) = gcd(7, 5) = gcd(5, 2) = gcd(2, 1) = 1
\]

\[
26 = 3 \times 7 + 5
\]
\[
7 = 1 \times 5 + 2
\]
\[
5 = 2 \times 2 + 1
\]
Example: Solve a Modular Equation

Solve:  \[ 7x \equiv_{26} 3 \]  
Find multiplicative inverse of 7 modulo 26

\[
gcd(26,7) = gcd(7,5) = gcd(5,2) = gcd(2,1) = 1
\]

\[
26 = 3 \times 7 + 5 \\
7 = 1 \times 5 + 2 \\
5 = 2 \times 2 + 1
\]

\[
5 = 26 - 3 \times 7 \\
2 = 7 - 1 \times 5 \\
1 = 5 - 2 \times 2
\]
Example: Solve a Modular Equation

Solve: \( 7x \equiv_{26} 3 \)  

Find multiplicative inverse of 7 modulo 26

\[
gcd(26, 7) = gcd(7, 5) = gcd(5, 2) = gcd(2, 1) = 1
\]

\[
26 = 3 \times 7 + 5 \quad 5 = 26 - 3 \times 7 \\
7 = 1 \times 5 + 2 \quad 2 = 7 - 1 \times 5 \\
5 = 2 \times 2 + 1 \quad 1 = 5 - 2 \times 2
\]

\[
1 = 5 - 2 \times (7 - 1 \times 5)
\]

\[
= (-2) \times 7 + 3 \times 5
\]

\[
= (-2) \times 7 + 3 \times (26 - 3 \times 7)
\]

\[
= (-11) \times 7 + 3 \times 26
\]
Example: Solve a Modular Equation

Solve: \( 7x \equiv_{26} 3 \)

Find multiplicative inverse of 7 modulo 26

\[
gcd(26, 7) = gcd(7, 5) = gcd(5, 2) = gcd(2, 1) = 1
\]

\[
26 = 3 \times 7 + 5 \quad 5 = 26 - 3 \times 7
\]
\[
7 = 1 \times 5 + 2 \quad 2 = 7 - 1 \times 5
\]
\[
5 = 2 \times 2 + 1 \quad 1 = 5 - 2 \times 2
\]

\[
1 = 5 - 2 \times (7 - 1 \times 5)
\]
\[
= (-2) \times 7 + 3 \times 5
\]
\[
= (-2) \times 7 + 3 \times (26 - 3 \times 7)
\]
\[
= (-11) \times 7 + 3 \times 26
\]

"the" multiplicative inverse

Now \((-11) \mod 26 = 15.\) 

(-11 is also "a" multiplicative inverse)
Example: Solve a Modular Equation

Solve: \( 7x \equiv_{26} 3 \)

Find multiplicative inverse of 7 modulo 26... it’s 15.

Multiplying both sides by 15 gives

\[ 15 \cdot 7x \equiv_{26} 15 \cdot 3 \]

Simplify on both sides to get

\[ x \equiv_{26} 15 \cdot 7x \equiv_{26} 15 \cdot 3 \equiv_{26} 19 \]

So, all solutions of this congruence are numbers of the form \( x = 19 + 26k \) for some \( k \in \mathbb{Z} \).
Example: Solve a Modular Equation

Solve:  $7x \equiv_{26} 3$

Conversely, suppose that $x \equiv_{26} 19$.

Multiplying both sides by 7 gives

$$7x \equiv_{26} 7 \cdot 19$$

Simplify on right to get

$$7x \equiv_{26} 7 \cdot 19 \equiv_{26} 3$$

So, all numbers of form $x = 19 + 26k$ for any $k \in \mathbb{Z}$ are solutions of this equation.
Example: Solve a Modular Equation

Solve: \( 7x \equiv_{26} 3 \) (on HW or exams)

Step 1. Find multiplicative inverse of 7 modulo 26

\[ 1 = \ldots = (-11) \cdot 7 + 3 \cdot 26 \]

Since \((-11) \mod 26 = 15\), the inverse of 7 is 15.

Step 2. Multiply both sides and simplify

Multiplying by 15, we get \( x \equiv_{26} 15 \cdot 7x \equiv_{26} 15 \cdot 3 \equiv_{26} 19 \).

Step 3. State the full set of solutions

So, the solutions are \( 19 + 26k \) for any \( k \in \mathbb{Z} \)

(must be of the form \( a + mk \) for all \( k \in \mathbb{Z} \) with \( 0 \leq a < m \))
Math mod a prime is especially nice

\[
\gcd(a, m) = 1 \text{ if } m \text{ is prime and } 0 < a < m \text{ so can always solve these equations mod a prime.}
\]

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

\[
\times \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \\
---
0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \\
1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \\
2 \quad 0 \quad 2 \quad 4 \quad 6 \quad 1 \quad 3 \quad 5 \\
3 \quad 0 \quad 3 \quad 6 \quad 2 \quad 5 \quad 1 \quad 4 \\
4 \quad 0 \quad 4 \quad 1 \quad 5 \quad 2 \quad 6 \quad 3 \\
5 \quad 0 \quad 5 \quad 3 \quad 1 \quad 6 \quad 4 \quad 2 \\
6 \quad 0 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2 \quad 1 \\
\]  
mod 7
Multiplicative Inverses and Algebra

Adding to both sides easily reversible:

\[-c \quad \xrightarrow{\text{+c}} \quad x \equiv_m y \quad \xrightarrow{\text{+c}} \quad \]

\[x + c \equiv_m y + c\]

The same is not true of multiplication...

unless we have a multiplicative inverse \(cd \equiv_m 1\)

\[\times d \quad \xrightarrow{\text{\times c}} \quad x \equiv_m y \quad \xrightarrow{\text{\times c}} \quad \]

\[cx \equiv_m cy\]
Questions?
## Modular Exponentiation mod 7

<table>
<thead>
<tr>
<th>x</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>α</th>
<th>α^1</th>
<th>α^2</th>
<th>α^3</th>
<th>α^4</th>
<th>α^5</th>
<th>α^6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>
Exponentiation

- Compute $78365^{81453}$

- Compute $78365^{81453} \mod 104729$

- Output is small
  - need to keep intermediate results small
Small Multiplications

Since \( b = qm + (b \mod m) \), we have \( b \mod m \equiv_m b \).

And since \( c = tm + (c \mod m) \), we have \( c \mod m \equiv_m c \).

Multiplying these gives \( (b \mod m)(c \mod m) \equiv_m bc \).

By the Lemma from a few lectures ago, this tells us \( bc \mod m = (b \mod m)(c \mod m) \mod m \).

Okay to mod \( b \) and \( c \) by \( m \) before multiplying if we are planning to mod the result by \( m \).
Repeated Squaring – small and fast

Since \( b \mod m \equiv_m b \) and \( c \mod m \equiv_m c \)
we have \( bc \mod m = (b \mod m)(c \mod m) \mod m \)

So \( a^2 \mod m = (a \mod m)^2 \mod m \)
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 \( a^k \mod m \) for \( k = 2^i \) in only \( i \) steps
What if \( k \) is not a power of \( 2 \)?
Fast Exponentiation Algorithm

81453 in binary is 10011111000101101

\[ 81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^5 + 2^3 + 2^2 + 2^0 \]

\[ a^{81453} = a^{2^{16}} \cdot a^{2^{13}} \cdot a^{2^{12}} \cdot a^{2^{11}} \cdot a^{2^{10}} \cdot a^9 \cdot a^5 \cdot a^3 \cdot a^2 \cdot a^0 \]

\[ a^{81453} \mod m = \]

\[ \left( \cdots \left( \left( a^{2^{16}} \mod m \cdot \right) \mod m \cdot \left( a^{2^{13}} \mod m \right) \mod m \cdot \left( a^{2^{12}} \mod m \right) \mod m \cdot \left( a^{2^{11}} \mod m \right) \mod m \cdot \left( a^{2^{10}} \mod m \right) \mod m \cdot \left( a^9 \mod m \right) \mod m \cdot \left( a^5 \mod m \right) \mod m \cdot \right. \]

\[ \left. \left( a^3 \mod m \right) \mod m \cdot \left( a^2 \mod m \right) \mod m \cdot \left( a^0 \mod m \right) \mod m \right) \mod m \]

Uses only \(16 + 9 = 25\) multiplications

The fast exponentiation algorithm computes

\[ a^k \mod m \text{ using } \leq 2\log k \text{ multiplications } \mod m \]
Fast Exponentiation: $a^k \mod m$ for all $k$

Another way:

$$a^{2j} \mod m = (a^j \mod m)^2 \mod m$$

$$a^{2j+1} \mod m = ((a \mod m) \cdot (a^{2j} \mod m)) \mod m$$
public static int FastModExp(int a, int k, int modulus) {
    if (k == 0) {
        return 1;
    } else if ((k % 2) == 0) {
        long temp = FastModExp(a, k/2, modulus);
        return (temp * temp) % modulus;
    } else {
        long temp = FastModExp(a, k-1, modulus);
        return (a * temp) % modulus;
    }
}

\[
a^{2j} \mod m = (a^j \mod m)^2 \mod m \\
a^{2j+1} \mod m = ((a \mod m) \cdot (a^{2j} \mod m)) \mod m
\]
Using Fast Modular Exponentiation

- Your e-commerce web transactions use SSL (Secure Socket Layer) based on RSA encryption

- RSA
  - Vendor chooses random 512-bit or 1024-bit primes \( p, q \) and 512/1024-bit exponent \( e \). Computes \( m = p \cdot q \)
  - Vendor broadcasts \( (m, e) \)
  - To send \( a \) to vendor, you compute \( C = a^e \mod m \) using fast modular exponentiation and send \( C \) to the vendor.
  - Using secret \( p, q \) the vendor computes \( d \) that is the multiplicative inverse of \( e \mod (p - 1)(q - 1) \).
  - Vendor computes \( C^d \mod m \) using fast modular exponentiation.
  - Fact: \( a = C^d \mod m \) for \( 0 < a < m \) unless \( p \mid a \) or \( q \mid a \)