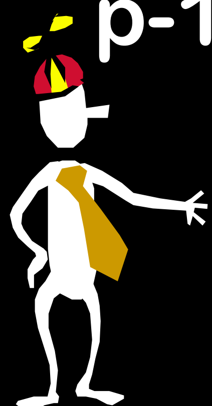
Number Theory and Modular Arithmetic



$^{p-1} \equiv_p 1$

Divisibility:

An integer a divides b (written "a|b") if and only if there exists an Integer c such that c*a = b.

Primes:

A natural number p $\geq$ 2 such that among all the numbers 1,2…p only 1 and p divide p.

Fundamental Theorem of Arithmetic:

Any integer greater than 1 can be uniquely written (up to the ordering of the factors) as a product of prime numbers.

Greatest Common Divisor:

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

greatest $k \geq 1$ s.t. $k|x$ and $k|y$.

Least Common Multiple:

$\mathrm{LCM}(x,y) =$

smallest $k \geq 1$ s.t. $x|k$ and $y|k$.

Fact:

$$GCD(x,y) \times LCM(x,y) = x \times y$$

(a mod n) means the remainder when a is divided by n.

$$a \bmod n = r$$

$$\Leftrightarrow$$

$$a = dn + r \text{ for some integer } d$$

Definition: Modular equivalence

$a \equiv b$ [mod n]

$\Leftrightarrow$ (a mod n) = (b mod n)

$\Leftrightarrow$ $n \mid (a-b)$

Written as $a \equiv_n b$, and spoken "a and b are **equivalent** or **congruent** modulo n"

$31 \equiv 81$ [mod 2]

$31 \equiv_2 81$

$31 \equiv 80$ [mod 7]

$31 \equiv_7 80$

$\equiv_n$ is an equivalence relation

In other words, it is

Reflexive: $a \equiv_n a$

Symmetric: $(a \equiv_n b) \Rightarrow (b \equiv_n a)$

Transitive: $(a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c)$

$\equiv_n$ induces a natural partition of the integers into n “residue” classes.

(“residue” = what left over = “remainder”)

Define residue class [k] = the set of all integers that are congruent to k modulo n.

Residue Classes Mod 3:

$[0] = \{ \ldots, -6, -3, 0, 3, 6, ..\}$

$[1] = \{ \ldots, -5, -2, 1, 4, 7, ..\}$

$[2] = \{ \ldots, -4, -1, 2, 5, 8, ..\}$

$[-6] = \{ \ldots, -6, -3, 0, 3, 6, ..\} = [0]$

$[7] = \{ \ldots, -5, -2, 1, 4, 7, ..\} = [1]$

$[-1] = \{ \ldots, -4, -1, 2, 5, 8, ..\} = [2]$

Why do we care about these residue classes?

Because we can replace any member of a residue class with another member when doing addition or multiplication mod n and the answer will not change

To calculate: 249 * 504 mod 251

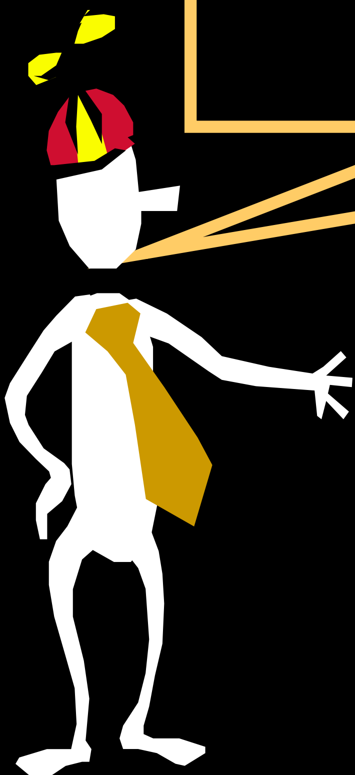
just do -2 * 2 = -4 = 247

We also care about it because computers do arithmetic modulo n, where n is 2^32 or 2^64.

Fundamental lemma of plus and times mod n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$. Then

1) $x + a \equiv_n y + b$
2) $x * a \equiv_n y * b$



Proof of 2: $xa = yb \pmod n$

(The other proof is similar…)

$x \equiv_n y$ iff $x = i\,n + y$ for some integer i

$a \equiv_n b$ iff $a = j\,n + b$ for some integer j

$$xa = (i\,n + y)(j\,n + b) = n(ijn+ib+jy) + yb$$

$$\equiv_n yb$$

Another Simple Fact:
If $(x \equiv_n y)$ and $(k|n)$, then: $x \equiv_k y$

Example: $10 \equiv_6 16 \Rightarrow 10 \equiv_3 16$

Proof:

$x \equiv_n y$ iff $x = in + y$ for some integer i

Let $j=n/k$, or $n=jk$ Then we have:

$$x = ijk + y$$

$x = (ij)k + y$ therefore $x \equiv_k y$

A Unique Representation System Modulo n:

We pick one representative from each residue class and do all our calculations using these representatives.

Unsurprisingly, we use 0, 1, 2, …, n-1

Unique representation system mod 3

Finite set S = {0, 1, 2}

+ and * defined on S:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Unique representation system mod 4

Finite set S = {0, 1, 2, 3}

+ and * defined on S:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

For addition tables, rows and columns always are a permutation of Z_n

(A group as we'll see later in the course.)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

For multiplication, some rows and columns are permutation of Z_n, while others aren't…

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

what's happening here?

For addition, the permutation property means you can solve, say,

$$4 + \_\_\_ = 1 \pmod 6$$

$$4 + \_\_\_ = x \pmod 6 \text{ for any } x \text{ in } Z_6$$

Subtraction mod n is well-defined

Each row has a 0, hence $-a$ is that element such that $a + (-a) = 0$

$\Rightarrow a - b = a + (-b)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

For multiplication, if a row has a permutation you can solve, say,

$$5 * \_\_\_ = 4 \pmod 6$$

$$\text{or,}\quad 5 * \_\_\_ = 1 \pmod 6$$

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

But if the row does not have the permutation property, how do you solve

no solutions! $3 * \_\_\_ = 4 \pmod{6}$

multiple solutions! $3 * \_\_\_ = 3 \pmod{6}$

$3 * \_\_\_ = 1 \pmod{6}$

no multiplicative inverse!

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Division

If you define 1/a (mod n) = a^{-1} (mod n)
as the element b in Z_n
such that a * b = 1 (mod n)

Then x/y (mod n)
=
x * 1/y (mod n)

Hence we can divide out by only the y's
for which 1/y is defined!

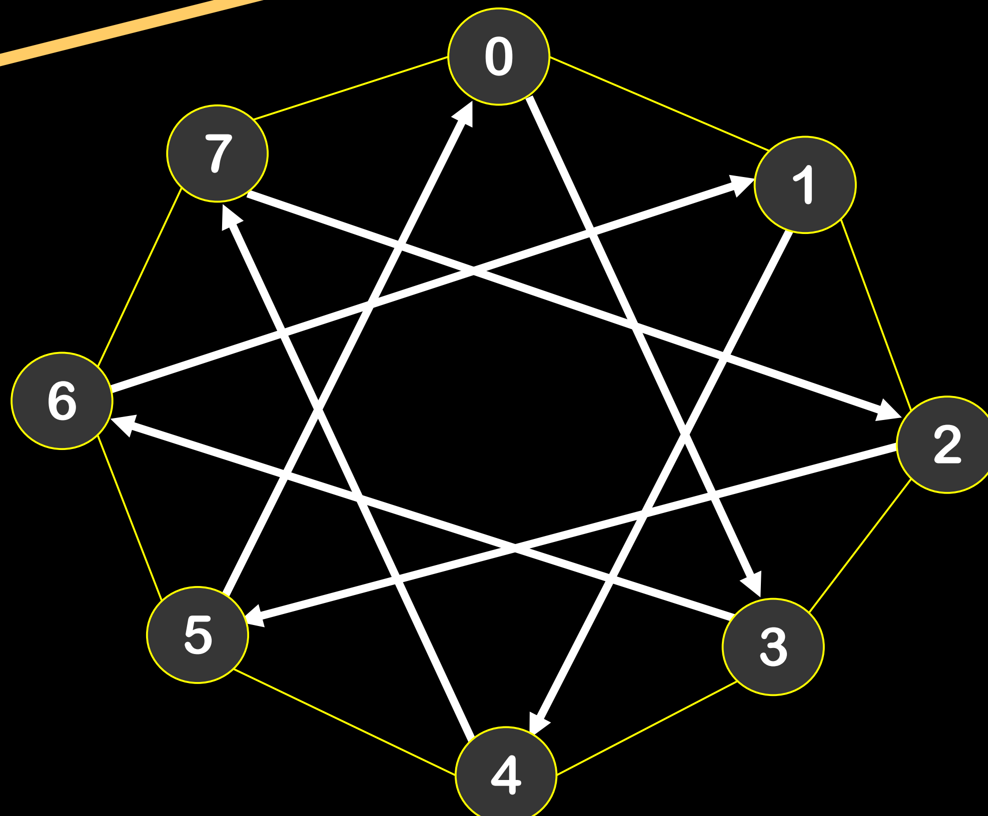
And which rows do have the permutation property?

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2						
3	0	3						
4	0	4						
5	0	5						
6	0	6						
7	0	7						

consider $*_8$ on Z_8

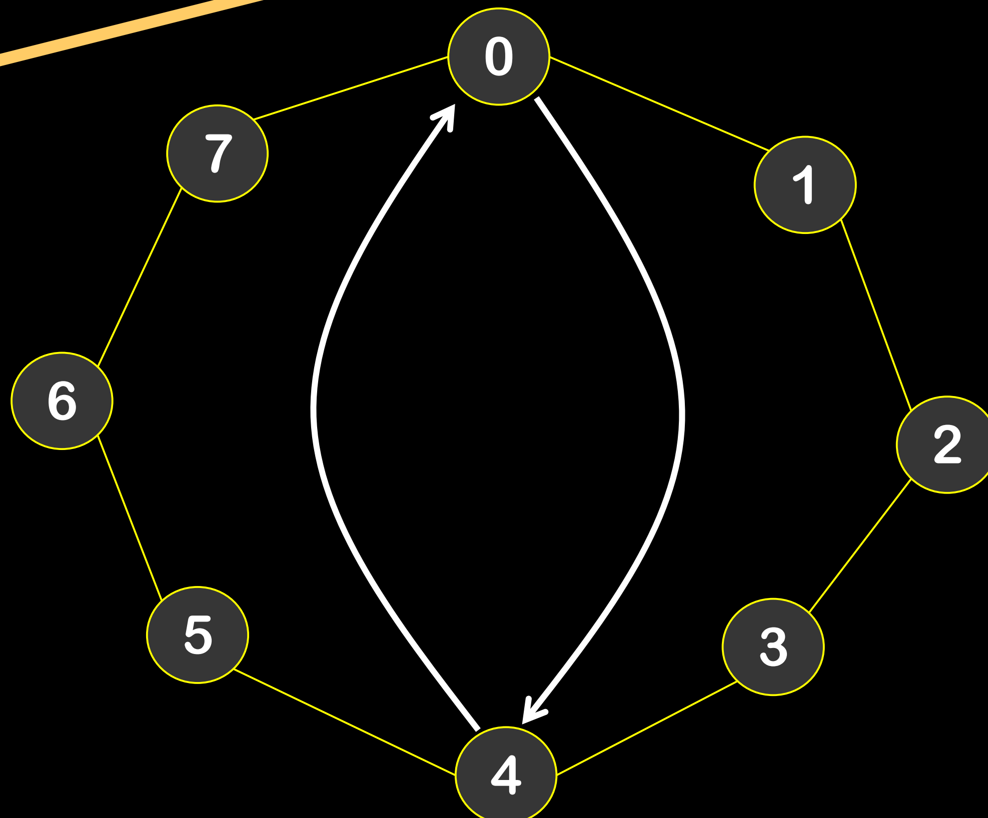
A visual way to understand multiplication and the “permutation property”.

There are exactly 8 distinct multiples of 3 modulo 8.

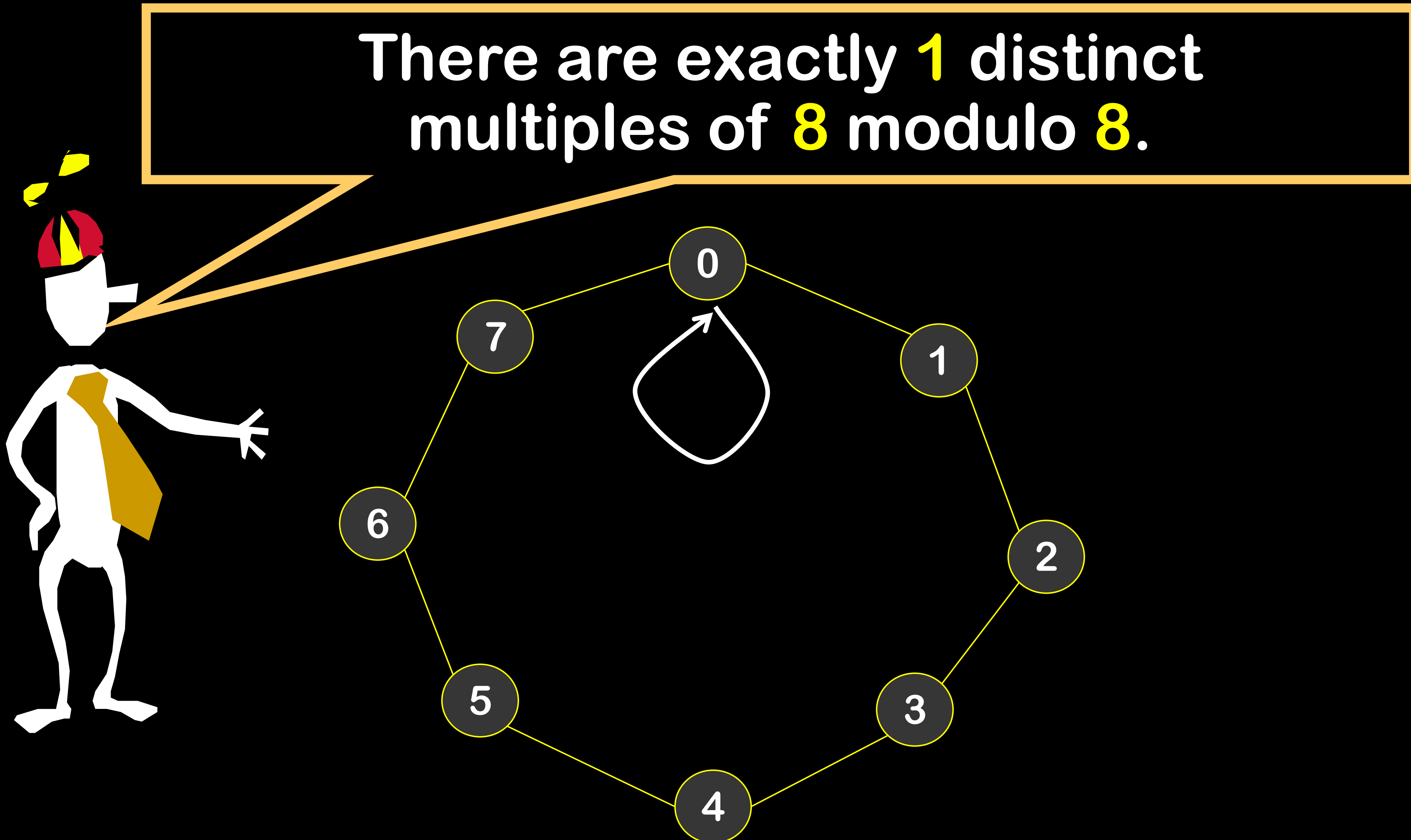


hit all numbers ⇔ row 3 has the “permutation property”

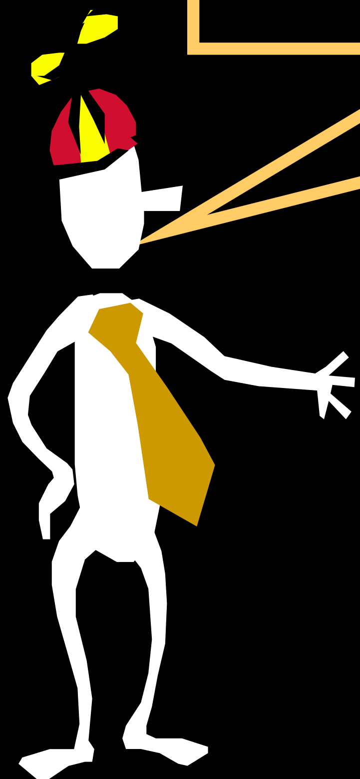
There are exactly 2 distinct multiples of 4 modulo 8.

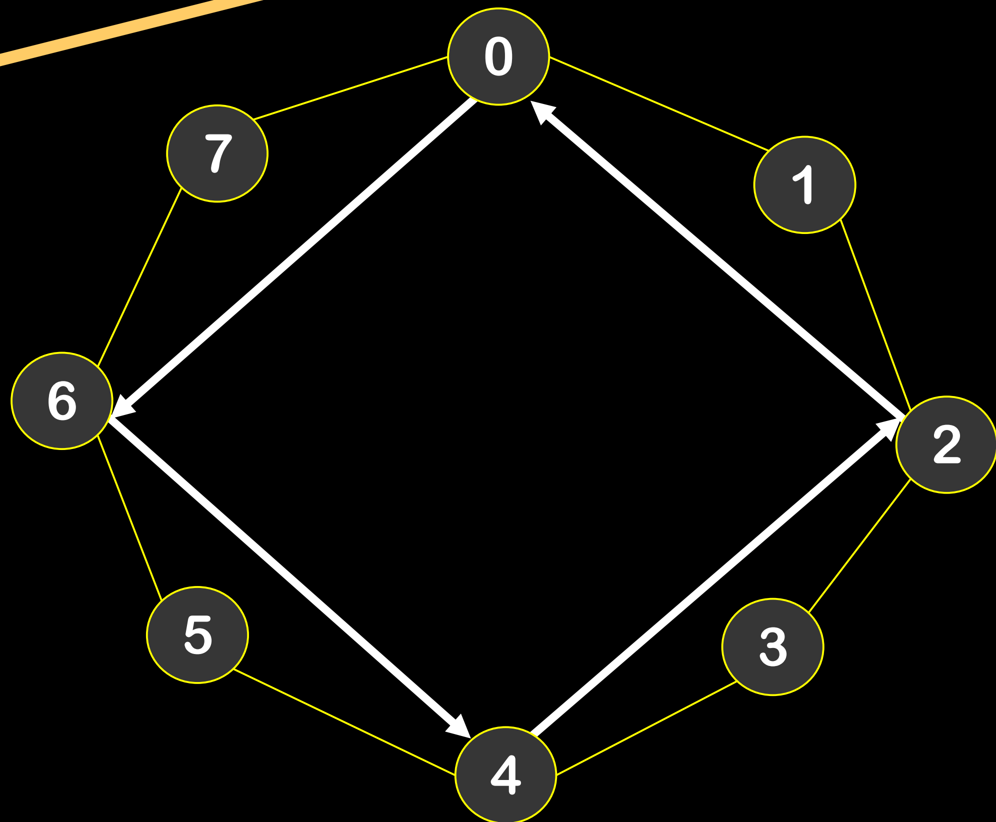


row 4 <u>does not</u> have “permutation property” for $*_8$ on Z_8


There are exactly 1 distinct multiples of 8 modulo 8.
0
1
2
3
4
5
6
7

There are exactly **4** distinct multiples of **6** modulo **8**.





Fundamental lemma of division modulo n:

if GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Proof:

Fundamental lemmas mod n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$. Then

1) $x + a \equiv_n y + b$
2) $x * a \equiv_n y * b$
3) $x - a \equiv_n y - b$
4) $cx \equiv_n cy \Rightarrow a \equiv_n b$ $\boxed{\text{if } \gcd(c,n)=1}$

New definition:

$$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$$

Multiplication over this set Z_n^* has the cancellation property.

$$Z_6 = \{0, 1,2,3,4,5\}$$
$$Z_6^* = \{1,5\}$$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

We've got closure

Recall we proved that Z_n was "closed" under addition and multiplication?

What about Z_n^* under multiplication?

Fact: if $a,b \in Z_n^*$, then $ab \pmod n$ in Z_n^*

Proof: if $\gcd(a,n) = \gcd(b,n) = 1$,
then $\gcd(ab, n) = 1$
then $\gcd(ab \bmod n, n) = 1$

$$Z_{12}^* = \{0 < x < 12 \mid \gcd(x,12) = 1\}$$
$$= \{1,5,7,11\}$$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Z_{15}^*

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

$$Z_5^* = \{1,2,3,4\}$$

$$\boxed{= Z_5 \setminus \{0\}}$$

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Fact:

For prime p, the set $Z_p^* = Z_p \setminus \{0\}$

Proof:

It just follows from the definition!

For prime p, all $0 < x < p$ satisfy $\gcd(x,p) = 1$

Euler Phi Function ϕ (n)

$\phi(n)$ = size of Z_n^*
= number of $1 \leq k < n$ that are relatively prime to n.

p prime
$\Rightarrow Z_p^* = \{1,2,3,\ldots,p-1\}$
$\Rightarrow \phi(p) = p-1$

$$Z_{12}^* = \{0 < x < 12 \mid \gcd(x,12) = 1\}$$
$$= \{1,5,7,11\}$$

$$\boxed{\phi(12) = 4}$$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Theorem: if p,q distinct primes then $\phi(pq) = (p-1)(q-1)$

How about $p = 3$, $q = 5$?

Theorem: if p,q distinct primes then $\phi(pq) = (p-1)(q-1)$

pq = # of numbers from 1 to pq

p = # of multiples of q up to pq

q = # of multiples of p up to pq

1 = # of multiple of both p and q up to pq

$$\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$$

Additive and Multiplicative Inverses

Additive inverse of a mod n
= number b such that a+b=0 (mod n)

What is the additive inverse
of a = 342952340 in
$Z_{4230493243}$?

Answer: n – a
= 4230493243-342952340
=3887540903

Multiplicative inverse of a mod n
= number b such that a*b=1 (mod n)

Remember,
only defined for numbers a in Z_n^*

Multiplicative inverse of a mod n
= number b such that a*b=1 (mod n)

What is the multiplicative inverse
of a = 342952340 in
$Z^*_{4230493243}$?

Answer: a^{-1} = 583739113

How do you find multiplicative inverses <u>fast</u>?

Theorem: given positive integers X, Y, there exist integers r, s such that

$$r X + s Y = \gcd(X, Y)$$

and we can find these integers fast!

Now take n, and $a \in Z_n^*$

$\gcd(a, n)$?   a in $Z_n^* \Rightarrow \gcd(a, n) = 1$

suppose $ra + sn = 1$

then $ra \equiv_n 1$

so, $r = a^{-1} \bmod n$

Theorem: given positive integers X, Y, there exist integers r, s such that

$$r X + s Y = \gcd(X, Y)$$

and we can find these integers fast!

How?

Extended Euclid Algorithm

Euclid's Algorithm for GCD

```
Euclid(A,B)
If B=0 then return A
        else return Euclid(B, A mod B)
```

Euclid(67,29)	67 – 2*29 = 67 mod 29 = 9
Euclid(29,9)	29 – 3*9 = 29 mod 9 = 2
Euclid(9,2)	9 – 4*2 = 9 mod 2 = 1
Euclid(2,1)	2 – 2*1 = 2 mod 1 = 0
Euclid(1,0) outputs 1	

Proof that Euclid is correct

```
Euclid(A,B)
If B=0 then return A
        else return Euclid(B, A mod B)
```

Let G = {g | g|A and g|B}
The GCD(A,B) is the maximum element of G.
Let G’ = {g | g|B and g|(A mod B)}

Claim: G = G’

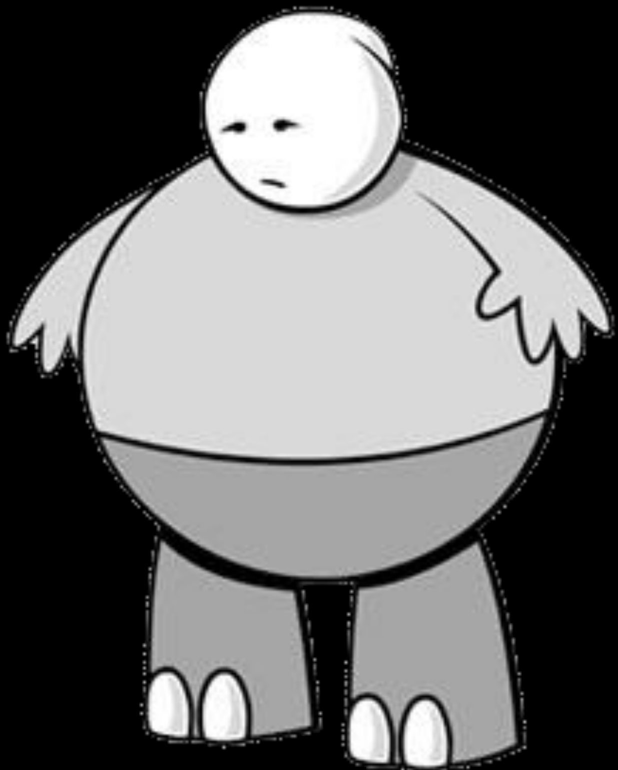
G’=G, because consder x in G.
Then x|A and x|B. Therefore x|($A \pm B$), and x|($A \pm 2B$) … But A mod B is just A+kB for some integer k. Similarly if x is in G’ then x is in G.

This combined with the base case completes the proof. QED.

Finally, a puzzle…

You have a 5 gallon bottle,
a 3 gallon bottle,
and lots of water.

How can you measure out
exactly 4 gallons?



Here's What You Need to Know…

Working modulo integer n

Definitions of Z_n, Z_n^*
and their properties

Fundamental lemmas of +,-,*,/
When can you divide out

Extended Euclid Algorithm
How to calculate c^{-1} mod n.

Euler phi function $\phi(n) = |Z_n^*|$