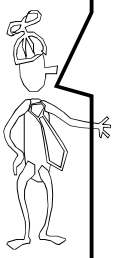
15-251

Great Theoretical Ideas in Computer Science

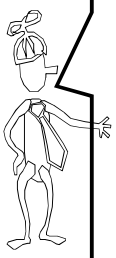
Number Theory and Modular Arithmetic

Lecture 13 (October 06, 2008)

$\equiv_p 1$

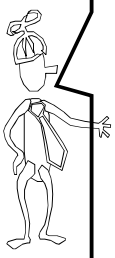


MAX(a,b) + MIN(a,b) = a+b



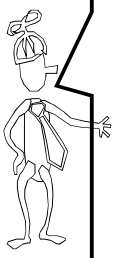
n|m means that m is an integer multiple of n.

We say that "n divides m".



Greatest Common Divisor:
GCD(x,y) =
greatest $k \geq 1$ s.t. k|x and k|y.

Least Common Multiple:
LCM(x,y) =
smallest $k \geq 1$ s.t. x|k and y|k.

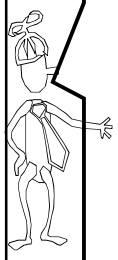


Fact:
GCD(x,y) × LCM(x,y) = x × y

You can use
MAX(a,b) + MIN(a,b) = a+b
to prove the above fact…

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

If $a = dn + r$ with $0 \leq r < n$
Then $r = (a \bmod n)$
and $d = (a \operatorname{div} n)$



Defn: Modular equivalence of integers a and b

$a \equiv b \pmod{n}$
$\Leftrightarrow (a \bmod n) = (b \bmod n)$
$\Leftrightarrow n|(a-b)$

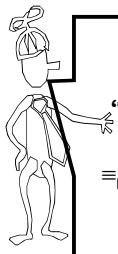
Written as $a \equiv_n b$, and spoken "a and b are equivalent modulo n"

$31 \equiv 81 \pmod{2}$
$31 \equiv_2 81$

$\equiv_n$ is an <u>equivalence relation</u>

In other words, it is

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



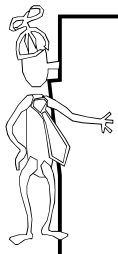
$a \equiv_n b \Leftrightarrow n|(a-b)$
"a and b are equivalent modulo n"

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

a and b are said to be in the same "residue class" or "congruence class" precisely when $a \equiv_n b$.

$a \equiv_n b \Leftrightarrow n|(a-b)$
"a and b are equivalent modulo n"

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



Residue Classes Mod 3:

[0] = { …, -6, -3, 0, 3, 6, ..}
[1] = { …, -5, -2, 1, 4, 7, ..}
[2] = { …, -4, -1, 2, 5, 8, ..}
[-6] = { …, -6, -3, 0, 3, 6, ..}
[7] = { …, -5, -2, 1, 4, 7, ..}
[-1] = { …, -4, -1, 2, 5, 8, ..}

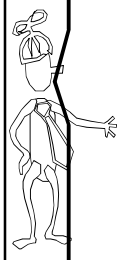
Fact: equivalence mod n implies equivalence mod any divisor of n.

If $(x \equiv_n y)$ and $(k|n)$
Then: $x \equiv_k y$

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

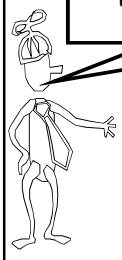
If $(x \equiv_n y)$ and $(k|n)$
then $x \equiv_k y$

Proof: by def^n, $n|x-y$
also $k|n$
$\Rightarrow k|x-y$
$\Rightarrow x \equiv_k y$ ☺



Fundamental lemma of plus, minus, and times mod n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$. Then
1) $x + a \equiv_n y + b$
2) $x - a \equiv_n y - b$
3) $x * a \equiv_n y * b$

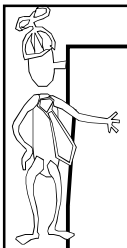


Proof of 3: xa = yb (mod n)

(The other two proofs are similar…)

Fundamental lemma of plus minus, and times modulo n:

When doing plus, minus, and times modulo n, I can at any time in the calculation replace a number with a number in the same residue class modulo n



Please calculate:
249 * 504 mod 251

when working mod 251

-2 * 2 = -4 = 247

A Unique Representation System Modulo n:

We pick exactly one representative from each residue class.

We do all our calculations using these representatives.

Unique representation system modulo 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 modulo 3

Finite set S = {0, 1, -1}

+ and * defined on S:

+	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

*	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

Perhaps the most convenient set of representatives:

The reduced system modulo n:

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Define operations $+_n$ and $*_n$:

$a +_n b = (a+b \bmod n)$
$a *_n b = (a*b \bmod n)$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a +_n b = (a+b \bmod n)$
$a *_n b = (a*b \bmod n)$

["Closed"]
$x, y \in Z_n \Rightarrow x +_n y \in Z_n$

["Associative"]
$x, y, z \in Z_n \Rightarrow (x +_n y) +_n z = x +_n (y +_n z)$

["Commutative"]
$x, y \in Z_n \Rightarrow x +_n y = y +_n x$

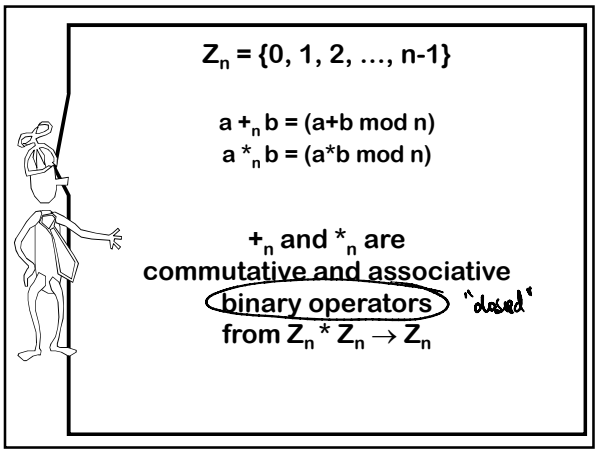
$Z_n = \{0, 1, 2, \ldots, n-1\}$

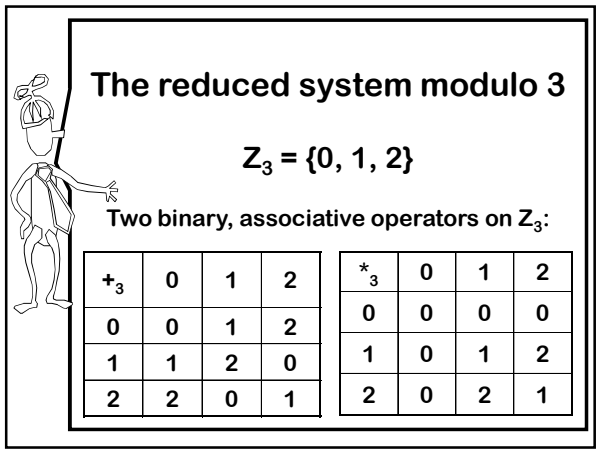
$a +_n b = (a+b \bmod n)$
$a *_n b = (a*b \bmod n)$

["Closed"]
$x, y \in Z_n \Rightarrow x *_n y \in Z_n$

["Associative"]
$x, y, z \in Z_n \Rightarrow (x *_n y) *_n z = x *_n (y *_n z)$

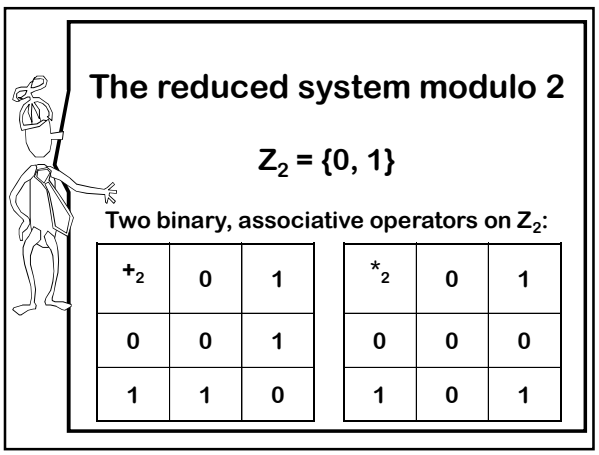
["Commutative"]
$x, y \in Z_n \Rightarrow x *_n y = y *_n x$





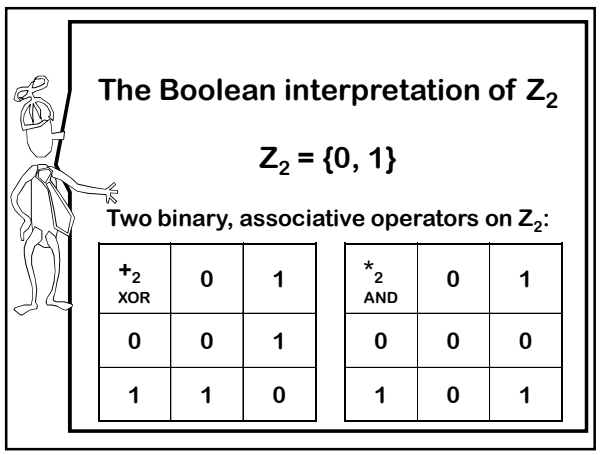
$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1



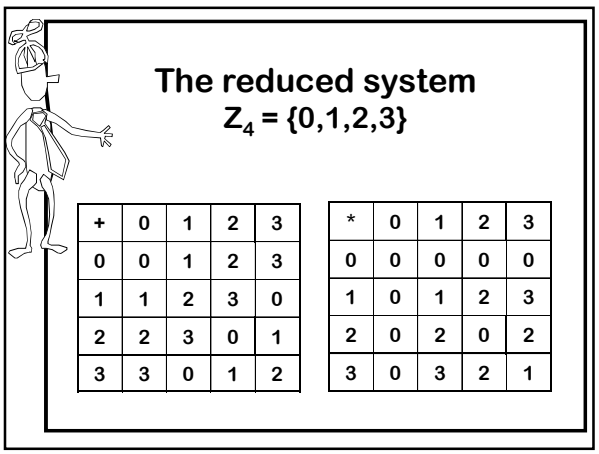
$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1



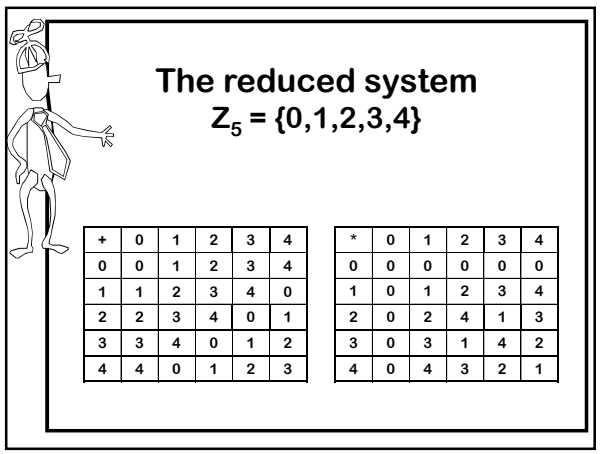
$+_2$ XOR	0	1
0	0	1
1	1	0

$*_2$ AND	0	1
0	0	0
1	0	1



+	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



+	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
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

The reduced system
$Z_6 = \{0,1,2,3,4,5\}$

+	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

The reduced system
$Z_6 = \{0,1,2,3,4,5\}$

+	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

An operator has the permutation property if each row and each column has a permutation of the elements.

For every n, $+_n$ on Z_n has the permutation property

+	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

An operator has the permutation property if each row and each column has a permutation of the elements.

What about multiplication? Does $*_6$ on Z_6 have the permutation property? No

*	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

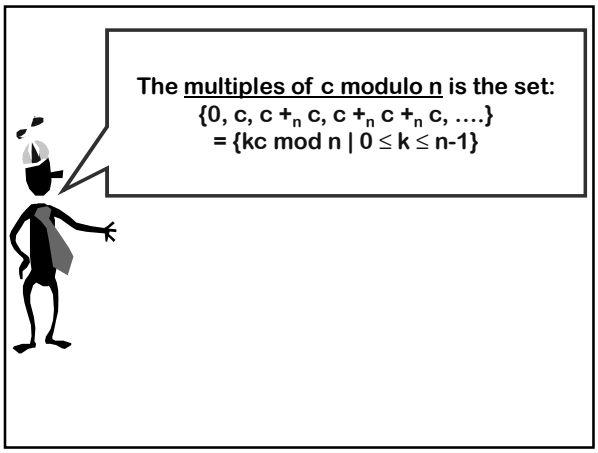
An operator has the permutation property if each row and each column has a permutation of the elements.

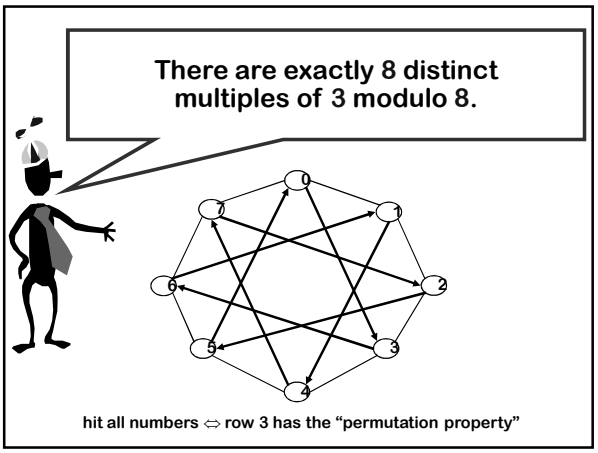
What about $*_8$ on Z_8?

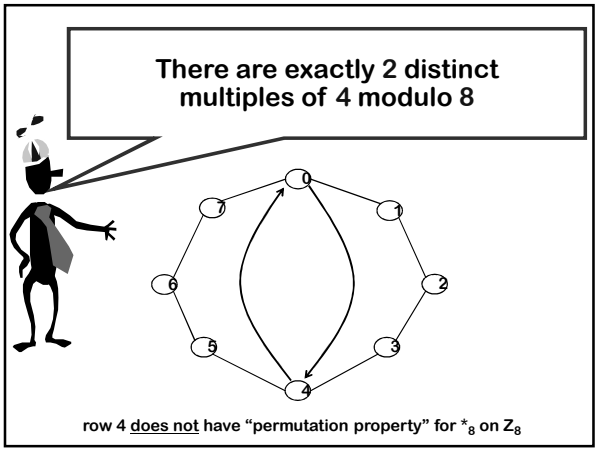
*	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

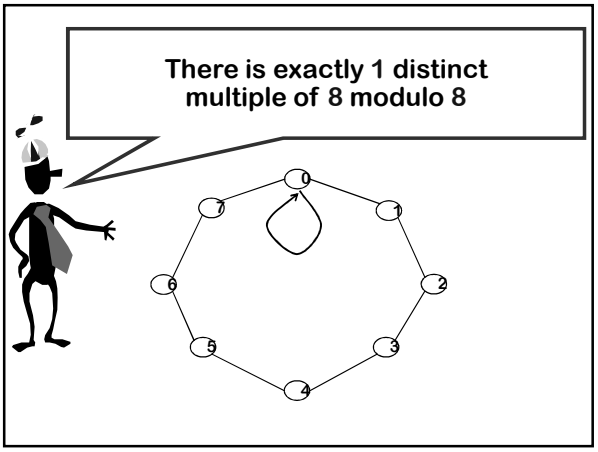
Which rows have the permutation property?

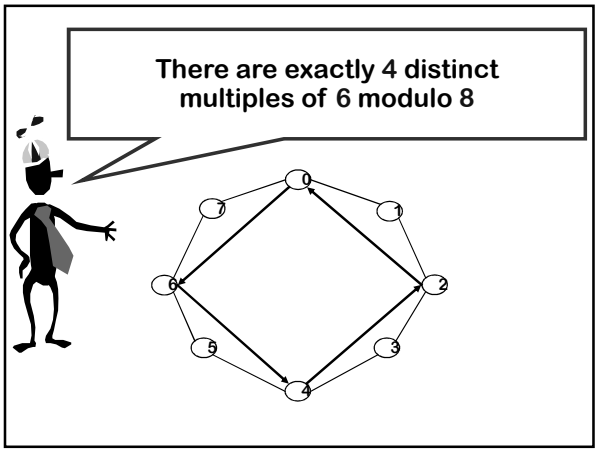
A visual way to understand multiplication and the "permutation property".









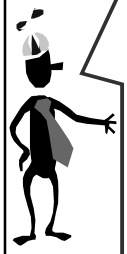


What's the pattern?

exactly 8 distinct multiples of 3 modulo 8.
exactly 2 distinct multiples of 4 modulo 8
exactly 1 distinct multiple of 8 modulo 8
exactly 4 distinct multiples of 6 modulo 8

exactly $\frac{y}{GCD(x,y)}$ distinct

multiples of x modulo y



There are exactly
LCM(n,c)/c = n/GCD(c,n)
distinct multiples of c modulo n

Hence,
only those values of c
with GCD(c,n) = 1
have the permutation
property for $*_n$ on Z_n

(that is, they have n distinct
multiples modulo n)

Theorem: There are exactly k = n/GCD(c,n) distinct multiples of c modulo n, and these multiples are { c*i mod n | $0 \le i < k$ }

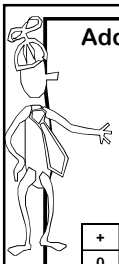
Proof:
Clearly, $c/GCD(c,n) \ge 1$ is a whole number

$ck = cn/GCD(c,n) = n(c/GCD(c,n)) \equiv_n 0$

$\Rightarrow$There are $\le k$ distinct multiples of c mod n:
c*0, c*1, c*2, …, c*(k-1)

$\Rightarrow$ Also, k = all the factors of n missing from c
$\Rightarrow cx \equiv_n cy \Leftrightarrow n|c(x-y) \Rightarrow k|(x-y) \Rightarrow x-y \ge k$
$\Rightarrow$ There are $\ge k$ multiples of c. Hence exactly k.

So, if we write the addition and multiplication tables for Z_n…



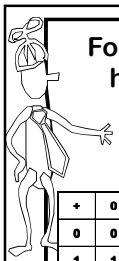
Addition on Z_n always has the permutation property

For some n, multiplication does…

$Z_5 = \{0,1,2,3,4\}$

+	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
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



For other n's multiplication does not have the permutation property…

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

+	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

Fundamental lemma of plus, minus, and times modulo 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) $x * a \equiv_n y * b$

Is there a fundamental lemma of division modulo n?

$cx \equiv_n cy \Rightarrow x \equiv_n y$?

Of course not!

If $c=0 \pmod n$, $cx \equiv_n cy$ for all x and y.

Canceling the c is like dividing by zero.

Let's fix that!
Repaired fundamental lemma of division modulo n?

if $c \neq 0 \pmod n$, then
$cx \equiv_n cy \Rightarrow x \equiv_n y$?

$6*3 \equiv_{10} 6*8$, but not $3 \equiv_{10} 8$.

$2*2 \equiv_6 2*5$, but not $2 \equiv_6 5$.

Bummer!

When can't I divide by c?

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

*	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

$3 \cdot 1 \equiv_6 3 \cdot 3$ but $1 \not\equiv_6 3$ ☹

When can't I divide by c?

Theorem: There are exactly n/GCD(c.n) distinct multiples of c modulo n.

Corollary: If GCD(c,n) > 1, then the number of multiples of c is less than n.

Corollary: If GCD(c,n) > 1 then you can't always divide by c.

Proof: There must exist distinct x,y<n such that c*x=c*y (but x≠y). Hence can't divide.

Fundamental lemma of division modulo n:
if GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Proof:

$n \mid ca-cb \Leftrightarrow n \mid c(a-b)$

but $GCD(n,c)=1$

$\Rightarrow n \mid a-b$ i.e. $a \equiv_n b$

☺

Corollary for general c:
$cx \equiv_n cy \Rightarrow x \equiv_{n/GCD(c,n)} y$

$n \mid cx-cy = c(x-y)$

$\frac{n}{gcd(c,n)} \mid \frac{c}{gcd(c,n)} \cdot (x-y)$

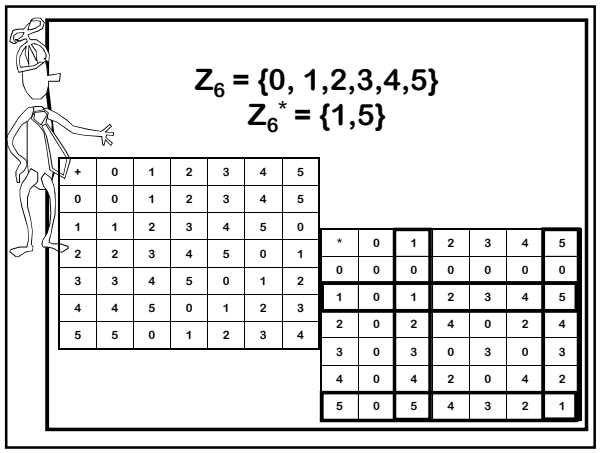
$\Rightarrow \quad x = y \left(\text{mod } \frac{n}{gcd(c,n)}\right)$

Fundamental lemma of division modulo n.
If GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Consider the set

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

Multiplication over this set Z_n^* will have 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

What are the properties of Z_n^*

For $*_n$ on Z_n we showed the following properties:

[Closure]
$x, y \in Z_n \Rightarrow x *_n y \in Z_n$

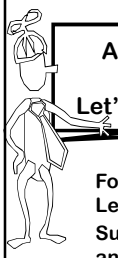
[Associativity]
$x, y, z \in Z_n \Rightarrow (x *_n y) *_n z = x *_n (y *_n z)$

[Commutativity]
$x, y \in Z_n \Rightarrow x *_n y = y *_n x$

What about $*_n$ on Z_n^*?

All these 3 properties hold for $*_n$ on Z_n^*.

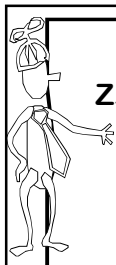
Let's show "closure": $x,y \in Z_n^* \Rightarrow x *_n y \in Z_n^*$



All these 3 properties hold for $*_n$ on Z_n^*.

Let's show "closure": $x,y \in Z_n^* \Rightarrow x *_n y \in Z_n^*$

Formal Proof:
Let z = xy. Let z' = z mod n. Then z = z' + kn.
Suppose z' not in Z_n*. Then GCD(z', n) > 1.
and hence GCD(z, n) > 1.
Hence there exists a prime p>1 s.t. p|z' and p|n.
$p|z \Rightarrow p|x$ or p|y. (say p|x)
Hence p|n, p|x, so GCD(x,n) > 1.
Contradiction of $x \in Z_n^*$

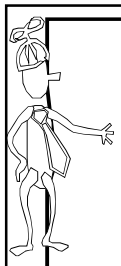


$Z_{12}^* = \{0 \le x < 12 \mid gcd(x,12) = 1\}$
$= \{1,5,7,11\}$

$*_{12}$	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



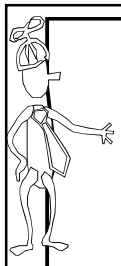
$Z_5^* = \{1,2,3,4\}$ $= Z_5 \setminus \{0\}$

$*_5$	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!

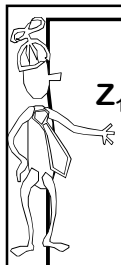
For a prime, all $0 < x < p$ satisfy $\gcd(x,p) = 1$



Euler Phi Function $\phi(n)$

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

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

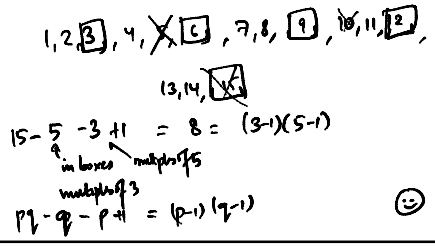


$Z_{12}^* = \{0 \le x < 12 \mid \gcd(x,12) = 1\}$
$= \{1,5,7,11\}$ $\phi(12) = 4$

$*_{12}$	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

The additive inverse of $a \in Z_n$ is the unique $b \in Z_n$ such that $a +_n b \equiv_n 0$.

We denote this inverse by "–a".

It is trivial to calculate: "-a" = (n-a).

The multiplicative inverse of $a \in Z_n^*$ is the unique $b \in Z_n^*$ such that $a *_n b \equiv_n 1$.

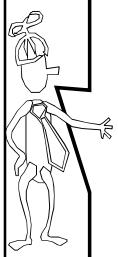
We denote this inverse by "a^{-1}" or "1/a".

The unique inverse of "a" must exist because the "a" row contains a permutation of the elements and hence contains a unique 1.

*	1	b	3	4
1	1	2	3	4
2	2	4	1	3
a	3	1	4	2
4	4	3	2	1

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

Answer: n – a = 3887540903



What is the multiplicative inverse of 342952340 in $Z_{4230493243}^*$?

Answer: 583739113

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

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

Extended Euclid Algorithm

Not only does it output GCD(A,B)
it also outputs integers r, s such that

r*A + s*B = GCD(A,B)

Extended Euclid Algorithm

Let <r,s> denote the number r*67 + s*29.
Calculate all intermediate values in this representation.

67=<1,0> 29=<0,1>

Euclid(67,29)	9=<1,0> – 2*<0,1>	9 =<1,-2>
Euclid(29,9)	2=<0,1> – 3*<1,-2>	2=<-3,7>
Euclid(9,2)	1=<1,-2> – 4*<-3,7>	1=<13,-30>
Euclid(2,1)	0=<-3,7> – 2*<13,-30>	0=<-29,67>

Euclid(1,0) outputs 1 = 13*67 – 30*29

<u>Efficient algorithm to compute a^{-1} from a and n.</u>

Run Extended Euclidean Algorithm
on the numbers a and n.

It will give two integers r and s
such that ra + sn = gcd(a,n) = 1

Taking both sides modulo n,
we obtain: $ra \equiv_n 1$

Output r, which is the inverse of a

Example

Multiplicative inverse of 29 in Z_{67}^* ?

1 = 13*67 – 30*29

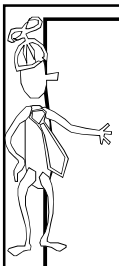
Hence: $29^{-1} = -30 = 37 \pmod{67}$

$Z_n = \{0, 1, 2, \ldots, n-1\}$
$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$

Define $+_n$ and $*_n$:
$a +_n b = (a+b \bmod n)$
$a *_n b = (a*b \bmod n)$

$<Z_n, +_n>$	$<Z_n^*, *_n>$
1. Closed	1. Closed
2. Associative	2. Associative
3. 0 is identity	3. 1 is identity
4. Additive Inverses	4. Multiplicative Inverses
5. Cancellation	5. Cancellation
6. Commutative	6. Commutative

$c *_n (a +_n b) \equiv_n (c *_n a) +_n (c *_n b)$

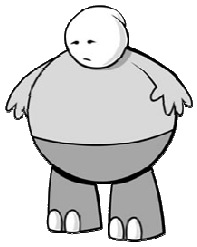


Euler Phi Function

$\Phi(n)$ = size of Z_n^*

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

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



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
How to calculate $c^{-1} \bmod n$.

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