15-251

Great Theoretical Ideas in Computer Science

Number Theory and Modular Arithmetic

Lecture 13 (October 5, 2010)

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 ≥ 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:
GCD(x,y) =
greatest k ≥ 1 s.t. k|x and k|y.

Least Common Multiple:
LCM(x,y) =
smallest k ≥ 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
applied appropriately to the factorizations of x and y to prove the above fact…

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

a mod n = r

$\Leftrightarrow$

a = dn + r for some integer d

Definition: Modular equivalence

$a \equiv b$ [mod n]

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

$\Leftrightarrow$ n | (a-b)

31 $\equiv$ 81 [mod 2]
31 $\equiv_2$ 81

31 $\equiv$ 80 [mod 7]
31 $\equiv_7$ 80

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

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

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

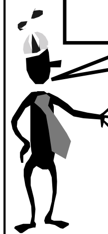
just do -2 * 2 = -4 = 247

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 (mod 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

Notation

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

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

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

Some properties of the operation $+_n$

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

Similar properties also hold for $*_n$

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 3

Finite set $Z_3 = \{0, 1, 2\}$

two associative, commutative operators on Z_3

Unique representation system mod 3

Finite set $Z_3 = \{0, 1, 2\}$

two associative, commutative operators on Z_3

+	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 2

Finite set $Z_2 = \{0, 1\}$

two associative, commutative operators on Z_2

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

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

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

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

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

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

For addition tables, rows and columns <u>always</u> 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 (mod 6)

4 + ___ = x (mod 6) for any x in Z_6

Subtraction mod n is well-defined

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

⇒ 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 (mod 6)

or, 5 * ___ = 1 (mod 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 $1/a \pmod n = a^{-1} \pmod n$ as the element b in Z_n such that $a * b = 1 \pmod n$

Then $x/y \pmod n$ = $x * 1/y \pmod n$

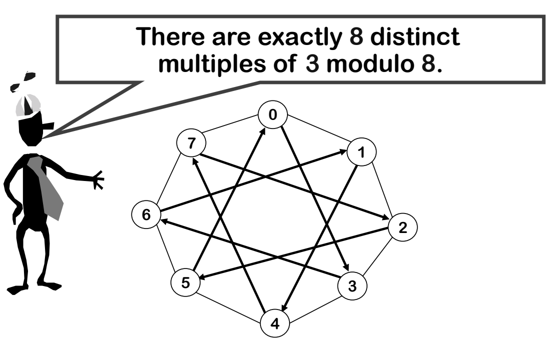
Hence we can divide out by only the y's for which 1/y is defined!

And which rows do have the permutation property?

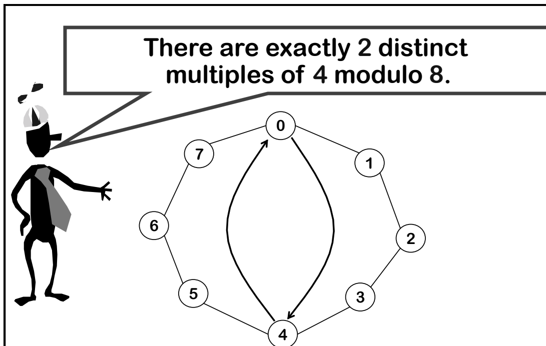
*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2						
3	0	3						
4	0	4						
5	0	5						
6	0	6						
7	0	7						

consider $*_8$ on Z_8

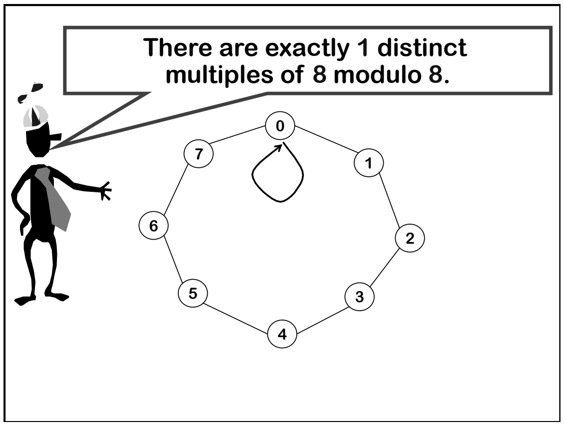
A visual way to understand multiplication and the "permutation property".

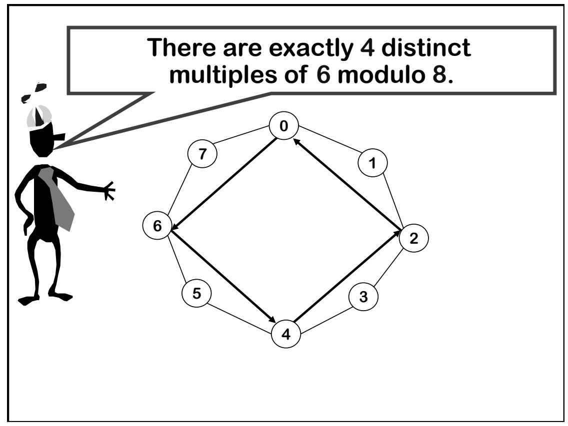


hit all numbers ⇔ row 3 has the "permutation property"



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





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 __________________ distinct

multiples of x modulo y

Theorem: There are exactly LCM(n,c)/c = n/GCD(c,n) distinct multiples of c 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:
$c*0, c*1, c*2, \ldots, c*(k-1)$

Also, k = 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.

Theorem: 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 n distinct multiples (i.e., the permutation property for $*_n$ on Z_n)

And remember, permutation property means you can divide out by c (working mod n)

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

Proof:

c*1, c*2, c*3, …, c*(n-1) are all in distinct residue classes modulo n.

Q E D.

If you want to extend to general c and n

$ca \equiv_n cb \Rightarrow a \equiv_{n/gcd(c,n)} b$

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) $cx \equiv_n cy \Rightarrow a \equiv_n b$ 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 ε Z_n^*, then ab (mod n) in Z_n^*

Proof: if gcd(a,n) = gcd(b,n) = 1,
then gcd(ab, n) = 1
then gcd(ab mod n, n) = 1

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

$*_{12}$	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 prime p, all $0 < x < p$ satisfy $gcd(x,p) = 1$

Euler Phi Function ϕ (n)

$\phi(n)$ = size of Z_n^*
= number of $1 \le k < n$ 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

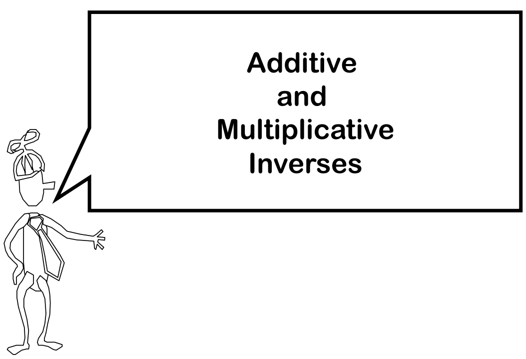
Theorem: if p,q distinct primes then $\phi(pq) = (p-1)(q-1)$

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 <u>both</u> p and q up to pq

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



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 ε Z_n^*

gcd(a, n) ? a in Z_n^* ⇒ gcd(a, n) = 1

suppose ra + sn = 1

then ra $\equiv_n$ 1

so, r = a^{-1} mod 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±B), and
x|(A±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.

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

Ocaml code for these algorithms

```
let rec gcd a b =
  if b=0 then a else gcd b (a mod b)

let rec euclid a b =
  if b=0 then (a,1,0) else
    let q = a/b in
    let r = a mod b in
    let (g, i, j) = euclid b r in (g, j, i-j*q)
```

Notes: This returns (g,i,j) where g is the GCD(a,b) and i and j are such that g=ia+jb.

It works because r = a-q*b and
g = i*b + j*r ➔ g = i*b + j*(a-q*b) ➔ g = j*a + (i-j*q) * b

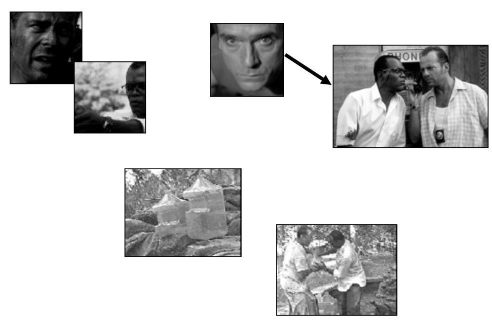
```
(* this is a proper mod function which is in [0...b-1] *)

let (%) a b = let x = a mod b in if x>=0 then x else x+b

let inverse a n =
  let (g, i, j) = euclid a n in   (* g = i*a + j*n *)
    if g != 1 then 0 else i % n
```

Finally, a puzzle…

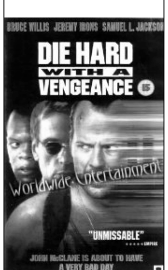
You have a 5 gallon bottle,
a 3 gallon bottle,
and lots of water.

How can you measure out
exactly 4 gallons?

why?



why?



Diophantine equations

Does the equality
$3x + 5y = 4$
have a solution where x,y are integers?

New bottles of water puzzle

You have a 6 gallon bottle,
a 3 gallon bottle,
and lots of water.

How can you measure out
exactly 4 gallons?

Invariant

Suppose stage of system is given by (L,S)
(L gallons in larger one, S in smaller)

Set of valid moves
1. empty out either bottle
2. fill up bottle (completely) from water source
3. pour bottle into other until first one empty
4. pour bottle into other until second one full

Invariant: L,S are both multiples of 3.

Generalized bottles of water

You have a P gallon bottle,
a Q gallon bottle,
and lots of water.

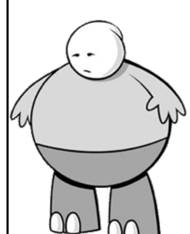
When can you measure out
exactly 1 gallon?

Recall that

if P and Q have gcd(P, Q) = 1
then you can find integers a and b so that
$a*P + b*Q = 1$

Suppose a is positive, then fill out P a times
and empty out Q b times

(and move water from P to Q as needed…)



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