Great Theoretical Ideas In Computer Science

Victor Adamchik — CS 15-251 — Spring 2010

Danny Sleator

Lecture 13 — Feb 23, 2010 — Carnegie Mellon University

Number Theory and Modular Arithmetic

$\equiv_p 1$

Greatest Common Divisor:
k=GCD(x,y)
greatest k ≥ 1 such that k|x and k|y.

Least Common Multiple:
k=LCM(x,y)
smallest k ≥ 1 such that 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.

a mod n = r

⇔

a = d n + r for some integer d

or

a = n + r k for some integer k

Definition: Modular equivalence

a ≡ b [mod n]
⇔ (a mod n) = (b mod n)
⇔ n | (a-b)

31 ≡ 81 [mod 2]
31 ≡$_2$ 81

31 ≡ 80 [mod 7]
31 ≡$_7$ 80

Written as a ≡$_n$ b, and spoken "a and b are equivalent or congruent modulo n"

$\equiv_n$ 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]

$\equiv_n$ 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: $(a \equiv_n b$ and $b \equiv_n c) \Rightarrow (a \equiv_n c)$

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

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:
x a = y b (mod n)

$(x \equiv_n y) \Rightarrow x = y + k\,n$
$(a \equiv_n b) \Rightarrow a = b + m\,n$

$x\,a = y\,b + n\,(y\,m + b\,k + k\,m)$

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:

$x = y + m\,n$
$n = a\,k$
$x = y + a\,m\,k$
$x \equiv_k y$

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 2

Finite set Z_2 = {0, 1}

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

$*_2$ AND	0	1
0	0	0
1	0	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, …, 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 $*_n$

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

+	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 * ___ = x (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 (mod 6)

multiple solutions! 3 * ___ = 3 (mod 6)

3 * ___ = 1 (mod 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!

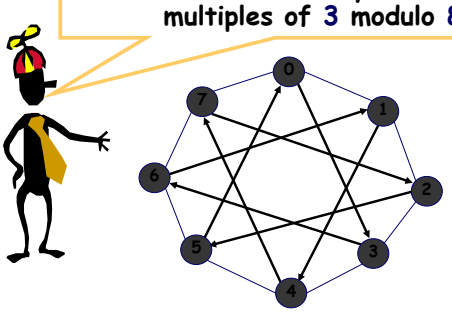
A visual way to understand multiplication and the "permutation property".

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	6	1	4	7	2	5
4	0	4						
5	0	5						
6	0	6						
7	0	7						

consider $*_8$ on Z_8

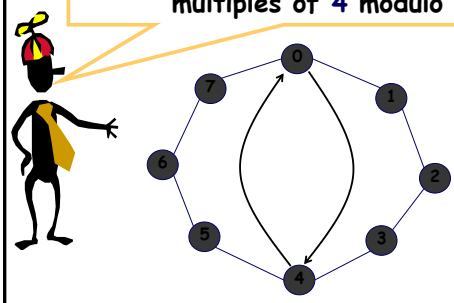
There are exactly 8 distinct multiples of 3 modulo 8.



3k mod 8

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

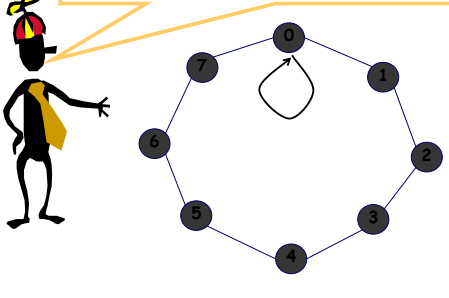
There are exactly 2 distinct multiples of 4 modulo 8.



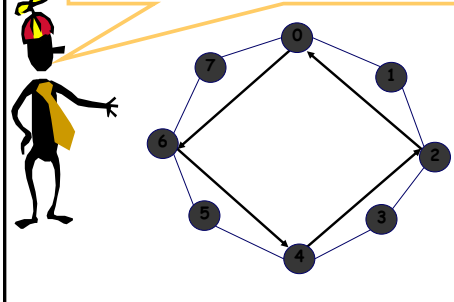
4k mod 8

row 4 does not have "permutation property" for $*_8$ on Z_8

There are exactly 1 distinct multiples of 8 modulo 8.



There are exactly 4 distinct multiples of 6 modulo 8.



6k mod 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 $\frac{y/GCD(x,y)}{\text{multiples of } x \text{ modulo } y}$ distinct

Theorem:

There are exactly

$LCM(y,x)/x = y/GCD(x,y)$

distinct multiples of x modulo y

Hence,
only those values of x with GCD(x,y) = 1 have n distinct multiples
(i.e., the permutation property for $*_n$ on Z_n)

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

Proof:

$c\,a =_n c\,b$ => n |(ca – cb) => n |c(a-b)

But GCD(n, c)=1, thus

n|(a-b) => $a =_n b$

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 in Z_n^*, then a b in Z_n^*

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

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

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

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 $\phi(n)$

$\phi(n)$ = 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 $\phi(p\ q) = (p-1)(q-1)$

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 $Z_{n\ =\ 4230493243}$?

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 $Z_{4230493243} = Z_n$?

Answer: $a^{-1} = 583739113$

How do you find multiplicative inverses fast ?

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^*

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

suppose $ra + sn = 1$

then $ra =_n 1$

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

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

Finally, a puzzle…

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

Can you measure out exactly 4 gallons?

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?**

Theorem

The linear equation

$a\,x + b\,y = c$

has an integer solution in x and y iff gcd(a,b)|c

The linear equation

$a\,x + b\,y = c$
has an integer solution in x and y iff gcd(a,b)|c

=>) gcd(a,b)|a and gcd(a,b)|b => gcd(a,b)|(a x + b y)

<=) gcd(a,b)|c => c = z * gcd(a,b)

On the other hand, $\gcd(a,b) = x_1 a + y_1 b$

$z \gcd(a,b) = z x_1 a + z y_1 b$

$c = z x_1 a + z y_1 b$

Hilbert's 10th problem

Hilbert asked for a universal method of solving all Diophantine equations
$P(x_1,x_2,\ldots,x_n)=0$
with any number of unknowns and integer coefficients.

In 1970 Y. Matiyasevich proved that the Diophantine problem is unsolvable.

Study Bee

- Working modulo integer n
- Definitions of Z_n, Z_n^*
- Fundamental lemmas of +,-,*,/
- Extended Euclid Algorithm
- Euler phi function $\phi(n) = |Z_n^*|$