Great Theoretical Ideas In CS

Victor Adamchik — CS 15-251

Lecture 23 — Carnegie Mellon University

Number Theory and Modular Arithmetic

p-1

$\equiv_p$ **1**

Outline

Working modulo integer n

Definitions of Z_n, Z_n^*

Fundamental lemmas of +,-,*,/

Extended Euclid Algorithm

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

Fundamental lemma of powers

Euler Theorem

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

a mod n = r

$\Leftrightarrow$

a = d n + r for some integer d

or

a = n + r k for some integer k

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"

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

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 4

Finite set $Z_4 = \{0, 1, 2, 3\}$

+	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 $*_n$

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 + x = 1 (mod 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 * x = 4 (mod 6)

3 * x = 4 (mod 6)

no solutions!

3 * x = 3 (mod 6)

multiple solutions!

*	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

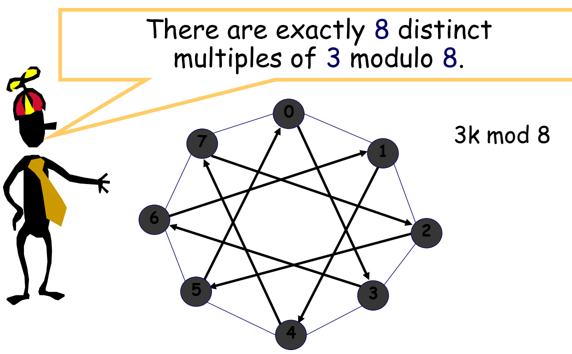
Multiplicative Inverse

Definition. Let a in Z_n An element b in Z_n is called a multiplicative inverse of a, if a * b = 1 (mod n)

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

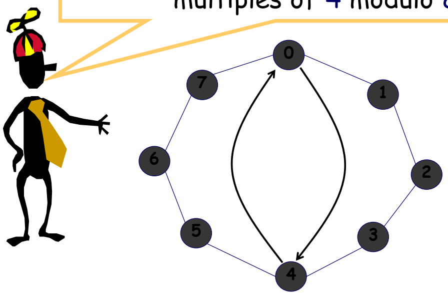
Consider $*_8$ on Z_8

*	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						



hit all numbers $\Leftrightarrow$ row 3 has the "permutation property"

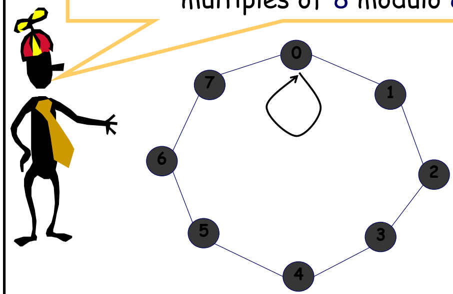
There are exactly 2 distinct multiples of 4 modulo 8.



4k mod 8

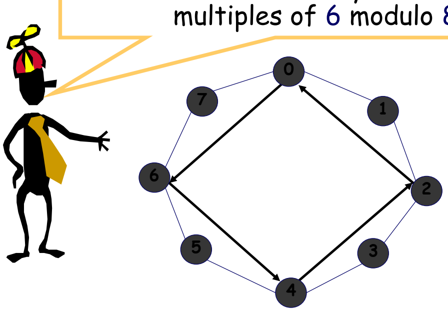
row 4 does not have "permutation property" for $*_8$ on Z_8

There are exactly 1 distinct multiples of 8 modulo 8.



8k mod 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 ___y/GCD(x,y)___ distinct multiples of x modulo y

Theorem:

There are exactly

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:

$c\,a =_n c\,b \Rightarrow n \mid (ca - cb) \Rightarrow n \mid c(a-b)$

But GCD(n, c)=1, thus

$n \mid (a-b) \Rightarrow a =_n b$

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 $1 \leq k < n$ that are relatively prime to n.

p prime

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

$\Rightarrow \phi(p) = p-1$

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

$= \{1,5,7,11\}$

$\phi(12) = 4$

$*_{12}$	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 <u>both</u> p and q up to pq

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

$\phi(15) = \phi(3*5) = (3-1)(5-1) = 8$

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

Remember,
only defined for numbers a in Z_n^*

What is the multiplicative inverse

of a = 342952340 in $Z_{4230493243} = Z_n$?

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!

Extended Euclid Algorithm

Now take n, and a in Z_n^*

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

Thus, we can find r and s s.t. r*a + s*n = 1

then r*a $=_n$ 1

so, r = a^{-1} mod n

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

Let <r,s> denote the number r*67 + s*29 = 1. 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*0, 0-2*1>
Euclid(29,9)	2=<0,1> – 3*<1,-2>	2=<0-3,1+6>
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 equation

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

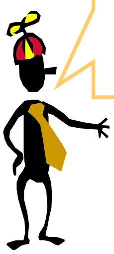
$z\, gcd(a,b) = z x_1 a + z y_1 b$

$c = z x_1 a + z y_1 b$

Hilbert's 10^{th} 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.



Exponentiation

How do you compute…

5^8 using few multiplications?

First idea:

$5 \quad 5^2 \quad 5^3 \quad 5^4 \quad 5^5 \quad 5^6 \quad 5^7 \quad 5^8$

$= 5*5$

$= 5^2*5$

How do you compute…

5^8

Better idea:

$5 \quad 5^2 \quad 5^4 \quad 5^8$
$= 5*5$
$= 5^2*5^2$
$= 5^4*5^4$

Used only 3 mults instead of 7 !!!

Repeated squaring calculates
a^{2^k}
in k multiply operations

compare with
$(2^k - 1)$ multiply operations
used by the naïve method

How do you compute…

5^{13}

Use repeated squaring again?

$5 \quad 5^2 \quad 5^4 \quad 5^8$

Note that 13 = 8+4+1

$13_{10} = (1101)_2$

So $a^{13} = a^8 * a^4 * a^1$

Two more multiplies!

To compute a^m

Suppose $2^k \leq m < 2^{k+1}$

$a \quad a^2 \quad a^4 \quad a^8 \quad . \; . \; . \quad a^{2^k}$

This takes k multiplies

Now write m as a sum of distinct powers of 2

say, $m = 2^k + 2^{i_1} + 2^{i_2} \ldots + 2^{i_t}$

$a^m = a^{2^k} * a^{2^{i_1}} * \ldots * a^{2^{i_t}}$

at most k more multiplies

Hence, we can compute
a^m
while performing at most

$2 \lfloor \log_2 m \rfloor$ multiplies

How do you compute…

5^{13} (mod 11)

First idea: Compute 5^{13} using 5 multiplies

$5 \quad 5^2 \quad 5^4 \quad 5^8 \quad 5^{12} \quad 5^{13} \quad = 1\,220\,703\,125$
$= 5^8*5^4 \quad = 5^{12}*5$

then take the answer mod 11

1220703125 (mod 11) = 4

How do you compute…

5^{13} (mod 11)

Better idea: keep reducing the answer mod 11

5	5^2	5^4	5^8	5^{12}	5^{13}
	25		$\equiv_{11}$ 81	$\equiv_{11}$ 36	$\equiv_{11}$ 15
	$\equiv_{11}$ 3	$\equiv_{11}$ 9	$\equiv_{11}$ 4	$\equiv_{11}$ 3	$\equiv_{11}$ 4

Hence, we can compute
a^m (mod n)
while performing at most
$2 \lfloor \log_2 m \rfloor$ multiplies

where each time we multiply together numbers with $\lfloor \log_2 n \rfloor + 1$ bits

How do you compute…

$5^{121242653}$ (mod 11)

The current best idea would still need about 54 calculations

answer = 4

Can we exponentiate any faster?

OK, need a little more number theory for this one…

Fundamental lemma of powers?

If $(x \equiv_n y)$
Then $a^x \equiv_n a^y$?

NO!

$(2 \equiv_3 5)$, but it is not the case that: $2^2 \equiv_3 2^5$

(Correct) Fundamental lemma of powers.

If $a \in Z_n^*$ and $x \equiv_{\phi(n)} y$ then $a^x \equiv_n a^y$

Equivalently,

for $a \in Z_n^*$, $a^x \equiv_n a^{x \bmod \phi(n)}$

How do you compute…

$5^{121242653} \pmod{11}$

$121242653 \pmod{10} = 3$

$5^3 \pmod{11} = 125 \bmod 11 = 4$

for $a \in Z_n^*$, $a^x \equiv_n a^{x \bmod \phi(n)}$

Why did we take mod 10?

---

for $a \in Z_n^*$, $a^x \equiv_n a^{x \bmod \phi(n)}$

Hence, we can compute
$a^m \pmod{n}$
while performing at most
$2 \lfloor \log_2 \phi(n) \rfloor$ multiplies

where each time we multiply
together numbers
with $\lfloor \log_2 n \rfloor + 1$ bits

$343280^{327847324} \bmod 39$

Step 1: reduce the base mod 39

Step 2: reduce the exponent mod $\phi(39) = 24$

you should check that gcd(343280,39)=1 to use lemma of powers

Step 3: use repeated squaring to compute 2^4, taking mods at each step

---

How do you prove the lemma for powers?

for $a \in Z_n^*$, $a^x \equiv_n a^{x \bmod \phi(n)}$

Use Euler's Theorem

For $a \in Z_n^*$, $a^{\phi(n)} \equiv_n 1$

Corollary: Fermat's Little Theorem

For p prime, $a \in Z_p^* \Rightarrow a^{p-1} \equiv_p 1$

Proof of Euler's Theorem: for $a \in Z_n^*$, $a^{\phi(n)} \equiv_n 1$

Define $a Z_n^* = \{a *_n x \mid x \in Z_n^*\}$ for $a \in Z_n^*$

By the permutation property, $Z_n^* = aZ_n^*$

$\prod x \equiv_n \prod ax$ [as x ranges over Z_n^*]

$\prod x \equiv_n \prod x \; (a^{\text{size of } Zn^*})$ [Commutativity]

$1 =_n a^{\text{size of } Zn^*}$ [Cancellation]

$a^{\phi(n)} =_n 1$

Here's What You Need to Know…

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