F3a: modular arithmetic I

tkkwon@snu.ac.kr

some slides from Zeph Grunschlag@Columbia
and Chris Brooks@USFCA
and Suleyman Kondakci@IEU

Number Theory

- is a branch of pure mathematics devoted primarily to the study of the integers
  - often its focus is on prime numbers
- modular arithmetic is very relevant to cryptography
  - a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the modulus
  - for this, we start with division

Divisor/divisibility

- DEF: Let *a*, *b* and *c* be integers such that

$$a = b \cdot c \text{ .}$$

- Then *b* and *c* are said to ***divide*** (or are ***factors*** of) *a,* while *a* is said to be a ***multiple*** of *b* (as well as of *c*). The pipe symbol "|" denotes "divides" so the situation is summarized by:

$$b \mid a \;\wedge\; c \mid a \text{ .}$$

- a is dividend
- b, c are divisors
- $\nmid$

Divisors: Examples

1. $7 \mid 77$: true because $77 = 7 \cdot 11$
2. $24 \mid 24$: true because $24 = 24 \cdot 1$
3. $0 \mid 24$: false, only 0 is divisible by 0
4. $24 \mid 0$: true, 0 is divisible by every number ($0 = 24 \cdot 0$)

Divisor Theorem

THM: Let *a*, *b*, and *c* be integers. Then:

1. $a|b \wedge a|c \; \square \; a|(b + c)$
2. $a|b \; \square \; a|bc$
3. $a|b \wedge b|c \; \square \; a|c$

Prime Numbers

DEF: A number $n \geq 2$ ***prime*** if it is only divisible by 1 and itself. A number $n \geq 2$ which isn't prime is called ***composite***.

Primality Testing

- Prime numbers are very important in encryption schemes. Essential to be able to verify if a number is prime or not.

boolean NaivePrimeTest(integer *n*)

if ($n < 2$) return false

for($i = 2$ to $\sqrt{n}$)

if($i \mid n$) // "another factor"

return false

return true

Primality Testing

- the previous algorithm’s complexity is too high
- there are more efficient algorithms
  - Fermat’s primality test
  - Miller-Rabin primality test
  - …

Now focus is on division with remainder

Division

Remember long division?

b the ***divisor***

$$\begin{array}{r} 3 \\ 31\overline{)117} \\ 93 \\ \hline 24 \end{array}$$

q the ***quotient***

a the ***dividend***

r the ***remainder***

$117 = 31 \cdot 3 + 24$

$a = bq + r$

Division

THM: Let a be an integer, and b be a positive integer. There are unique integers q, r with $r \in \{0,1,2,\ldots,b\text{-}1\}$ satisfying

$$a = bq + r$$

The proof is a simple application of long-division. The theorem is called the ***division algorithm***.

mod: Modulo operation

There are two types of “mod” (pronounced mod or modulo)

- the mod function
  - Inputs a number a and a base n (aka modulus)
  - Outputs a **mod** n
    - a number between 0 and $n-1$ inclusive
  - This is the remainder from a÷n
- the (mod) congruence
  - Relates two numbers a, b to each other relative some base n
  - $a \equiv b \pmod{n}$ means that a and b have the same remainder when dividing by n

mod function

1. 113 **mod** 24:

$$\begin{array}{r} 4 \\ 24\overline{)113} \\ 96 \\ \hline 17 \end{array}$$

2. -29 **mod** 7

$$\begin{array}{r} -5 \\ 7\overline{)-29} \\ -35 \\ \hline 6 \end{array}$$

(mod) congruence: Formal Definition

DEF: Let a, b be integers and n be a positive integer. We say that a is congruent to b modulo n

($a \equiv b$ (mod n)) iff n | ($a - b$)

Equivalently: a **mod** n = b **mod** n

* '≡' and '=' are often interchanged
* parentheses around mod are often omitted

(mod) congruence

1. $3 \equiv 3 \pmod{17}$ True. any number is congruent to itself (3-3 = 0, divisible by all)
2. $3 \equiv -3 \pmod{17}$ False. (3-(-3)) = 6 isn't divisible by 17.
3. $172 \equiv 177 \pmod{5}$ True. 172-177 = -5 is a multiple of 5
4. $-13 \equiv 13 \pmod{26}$ True: -13-13 = -26 divisible by 26.

(mod) congruence

The (mod) congruence is useful for manipulating expressions involving the **mod** function. It lets us view modular arithmetic relative a fixed base, as creating a number system inside of which all the calculations can be carried out.

- a **mod** $n \equiv a \pmod{n}$
- Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ Then:
  - $a+c \equiv (b+d) \pmod{n}$
  - $ac \equiv bd \pmod{n}$
  - $a^k \equiv b^k \pmod{n}$
  - $a\ (mod\ n) \equiv (a\ mod\ n) \pmod{n}$

(a + b) mod n ≡ [(a mod n) + (b mod n)] mod n
ab mod n ≡ [(a mod n)(b mod n)] mod n
a^k mod n ≡ (a mod n)^k (mod n)

proof of one of the theorems

Using proof by induction,

If $a^k \equiv b^k \pmod{n}$,

$a\, a^k \equiv a\, b^k \equiv b\, b^k \pmod{n}$, by multiplication rule

$\therefore a^{k+1} \equiv b^{k+1} \pmod{n}$

modular arithmetic

- modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the modulus
  - if modulus is n, then numbers circle in the range of 0..(n-1)

Modular arithmetic: harder examples

Q: Compute the following.

1. 307^{1001} **mod** 102
2. (-45 · 77) **mod** 17
3. $$\left(\sum_{i=4}^{23} 10^i\right) \bmod 11$$

Modular arithmetic: harder examples

1. Using multiplication rules before multiplying (or exponentiating) can reduce modulo 102:

307^{1001} **mod** $102 \equiv 307^{1001} \pmod{102}$

$\equiv (307 \text{ mod } 102)^{1001} \pmod{102}$

$\equiv 1^{1001} \pmod{102} \equiv 1 \pmod{102}$.

Therefore, 307^{1001} **mod** $102 = 1$.

Modular arithmetic: harder examples

2. Repeatedly reduce after each multiplication:

$(-45\cdot 77)$ **mod** $17 \equiv (-45\cdot 77) \pmod{17}$

$\equiv (6\cdot 9) \pmod{17} \equiv 54 \pmod{17} \equiv 3 \pmod{17}$.

Therefore $(-45\cdot 77)$ **mod** $17 = 3$.

Modular arithmetic: harder examples

3. Similarly, before taking sum can simplify modulo 11:

$$\left(\sum_{i=4}^{23} 10^i\right)(\mathrm{mod}\ 11) \equiv \left(\sum_{i=4}^{23} 10^i\right)(\mathrm{mod}\ 11) \equiv \left(\sum_{i=4}^{23} (-1)^i\right)(\mathrm{mod}\ 11)$$

$$\equiv (1-1+1-1+\ldots\ +1-1)(\mathrm{mod}\ 11) \equiv 0\,(\mathrm{mod}\ 11)$$

Therefore, the answer is 0.

equivalent classes

- When modulus n = 4, we have 4 congruence/residue classes as follows:
- [0]={ … , −8, −4, 0, 4, 8, …..}
  [1]={ …., −7, −3, 1, 5, 9,……}
  [2]={ …., −6, −2, 2, 6, 10,……}
  [3]={ …., −5, −1, 3, 7, 11,……}

equivalent classes

- Consider the relation $R = \{ (a,b) \mid a \equiv b \pmod{m} \}$
- Is it reflexive: (a,a) $\in R$ means that $m \mid a\text{-}a$
  - $a\text{-}a = 0$, which is divisible by m
- Is it symmetric: if $(a,b) \in R$ then $(b,a) \in R$
  - (a,b) means that $m \mid a\text{-}b$
  - Or that $km = a\text{-}b$. Negating that, we get $b\text{-}a = -km$
  - Thus, $m \mid b\text{-}a$, so (b,a) $\in R$
- Is it transitive: if $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$
  - (a,b) means that $m \mid a\text{-}b$, or that $km = a\text{-}b$
  - (b,c) means that $m \mid b\text{-}c$, or that $lm = b\text{-}c$
  - (a,c) means that $m \mid a\text{-}c$, or that $nm = a\text{-}c$
  - Adding the top two equations, we get $km+lm = (a\text{-}b) + (b\text{-}c)$
  - Or $(k+l)m = a\text{-}c$
  - Thus, m divides $a\text{-}c$, where $n = k+l$
- so, congruence modulo m is an equivalence relation

modular arithmetic

- A set of congruence classes $Z_n = \{0,1,\ldots,n-1\}$ is *closed* under modular addition and multiplication.

- $(a+b) \pmod{n} = (a \pmod{n} + b \pmod{n}) \pmod{n}$
- $(ab) \pmod{n} = (a \pmod{n}\ b \pmod{n}) \pmod{n}$

identities and inverses

- An identity is a number that maps a number to itself under some operation.
  - 0 in normal addition, 1 in multiplication.
- An inverse is a number (within the input set) and maps a given number (say, a) to the identity
  - a * 1/a, a + (-a) in integer math
- We are particularly interested in multiplicative inverses for modular arithmetic.
  - $aa^{-1} = 1 \pmod{n}$

Modular multiplicative Inverses

- 3 and 2 are multiplicative inverses mod 5.
- 7 and 6 are multiplicative inverses mod 41.
- 5 and 2 are multiplicative inverses mod 9.

- For base N > 1, if *a* and *N* are relatively prime, there is a unique x such that
  - $ax = 1 \ (mod\ N)$
  - what is the relation between *a* and *x*?
  - what if *N* is a prime number?

If a,b are relative prime, gcd(a,b) = 1

Modular multi. Inverses

DEF: The ***inverse*** of a modulo N is the number a^{-1} between 1 and N-1 such that

$$a\, a^{-1} \equiv 1 \pmod{N}$$

if such a number exists.

Q1: When does it exist?

Q2: What is the inverse of 3 modulo 26?

Modular multi. Inverses

A2: 9 because $9 \cdot 3 = 27 \equiv 1 \pmod{26}$.

Q3: What is the inverse of 4 modulo 8?

Modular Inverses

- A3: *Trick Question!* No inverse can exist because $4x$ is always 0 or 4 modulo 8!

- condition for inverse existence
  - a has an inverse modulo N if and only if a and N are relatively prime.

Proof of multi. inverse condition

- Given a, $ax=1 \pmod N$ for some integer x iff gcd(a,N)=1
- Extended Euclidean Algorithm (EEA)

  a,b are positive integers, then there are integers u and v,
  s.t. au+bv = gcd(a,b)
- From EEA

  there exist u,v such that ua+vN = 1 if gcd(a,N)=1
- Proof

if gcd(a,N)=1 then there exist u,v s.t. ua+vN=1
ua = 1-vN = 1 (mod N)

since ax = 1+kN, ax-kN = 1
then gcd(a,N) divides ax–kN, so gcd(a,N) = 1

GCD: Relatively Prime

DEF Let a,b be integers, not both zero. The ***greatest common divisor*** of a and b (or gcd(a,b)) is the biggest number d which divides both a and b.

DEF: a and b are said to be ***relatively prime*** (or co-prime) if gcd(a,b) = 1, so no common divisors/factors.

GCD: Relatively Prime

1. gcd(11,77) = 11
2. gcd(33,77) = 11
3. gcd(24,36) = 12
4. gcd(24,25) = 1. Therefore 24 and 25 are relatively prime.

NOTE: A prime number are relatively prime to all other numbers which it doesn't divide.

* what is gcd(x,p)? given that p is prime and 0<x<p

how to calculate gcd(a,b)?

- factorization
- Euclid’s algorithm

Euclidean Algorithm (EA)

- an efficient way to find GCD(a,b)
- uses theorem that:
  - `GCD(a,b) = GCD(b, a mod b)`
- Euclidean Algorithm to compute GCD(a,b) is:

```
Euclid(a,b)
  if (b=0) then return a;
  else return Euclid(b, a mod b);
```

How EA Works

- Start with two integers for which you want to find the GCD. Apply the division algorithm, dividing the smaller number into the larger.
- Example: $a = 320$, $b = 296$.
- $320 = 296 \cdot 1 + 24$
- The first quotient is q_1 and the first remainder is r_1.
- some textbooks use different indexes
  - like q_0 r_0 or q_1 r_2

How EA Works (cont.)

- If you get a remainder of 0, stop.
- If not, the divisor from the previous step becomes the dividend of the next step. The remainder from the previous step becomes the divisor of the previous step.

- $320 = 296 \cdot 1 + 24$
- $296 = 24 \cdot 12 + 8$

- Continue until you get a remainder of 0.

EA: whole example

- $320 = 296 \cdot 1 + 24$
- $296 = 24 \cdot 12 + 8$
- $24 = 8 \cdot 3 + 0$

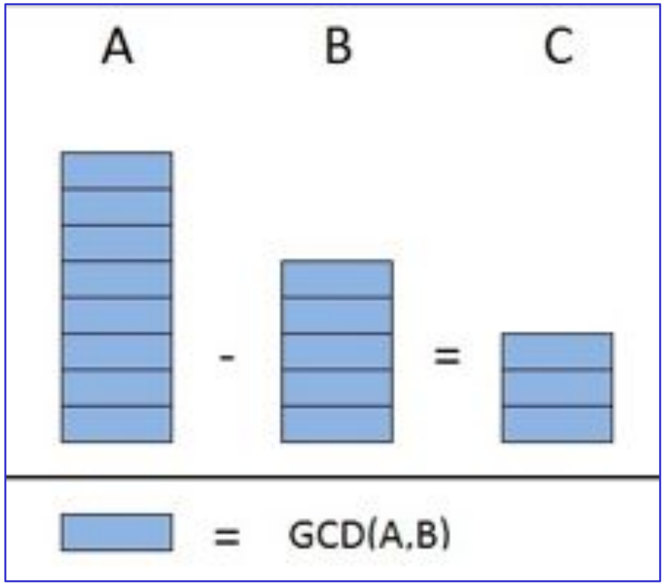
- We get a remainder of 0, so we stop. The last nonzero remainder is the GCD, so gcd(320, 296) is equal to 8.

Another EA Example

- Compute gcd(592,346).

- $592 = 346 \cdot 1 + 246$
- $346 = 246 \cdot 1 + 100$
- $246 = 100 \cdot 2 + 46$
- $100 = 46 \cdot 2 + 8$
- $46 = 8 \cdot 5 + 6$
- $8 = 6 \cdot 1 + 2$
- $6 = 2 \cdot 3 + 0$

- So gcd(346, 592) = 2.



source: khanacademy.org

Extended Euclidean Algorithm (EEA)

- We can use the Euclidean Algorithm to find the integers u and v, s.t. ua+vb = gcd(a,b)

- As an example, let's use the Euclidean Algorithm to show that (324, 148) = 4.

- $324 = 148 \cdot 2 + 28$
- $148 = 28 \cdot 5 + 8$
- $28 = 8 \cdot 3 + 4$
- $8 = 4 \cdot 2 + 0$

- $a = b \cdot q1 + r1$
- $b = r1 \cdot q2 + r2$
- $r1 = r2 \cdot q3 + r3$
- $r2 = r3 \cdot q4 + r4$

Finding u and v: EEA

- We want to find integers u and v such that $324u + 148v = \gcd(324,148) = 4$.

- Take all of the equations (except the last one) and solve for the remainder.

- $28 = 324 – 148 \cdot 2$
- $8 = 148 – 28 \cdot 5$
- $4 = 28 – 8 \cdot 3$

- $r1 = \boxed{a - b \cdot q1}$
- $r2 = b - r1 \cdot q2$
- $r3 = r1 - r2 \cdot q3$

$$\boxed{4 = 324 \cdot 16 + 148 \cdot (-35)}$$

how to find an inverse? Use EEA

- Finding Inverses in Z_n
  - What is the inverse of 15 in mod 26?
  - First use the Euclidean Algorithm to determine if 15 and 26 are relatively prime
  - gcd(26,15)
    - 26 = 1 * 15 + 11
    - 15 = 1 * 11 + 4
    - 11 = 2 * 4 + 3
    - 4 = 1 * 3 + 1
    - 3 = 3 * 1 + 0

So, gcd (26, 15) = 1

Finding multi. inverse

- Finding Inverses in Z_n
  - What is the inverse of 15 in mod 26? Now we now they are relatively prime – so an inverse must exist.
  - We can use EEA to work backward to create 1 (the gcd(26, 15)) as a linear combination of 26 and 15:
    - $1 = u * 26 + v * 15$
  - Why would we want to do this?

Finding multi. inverse

- Finding Inverses in Z_n
  - Convert $1 = u * 26 + v * 15$ to mod 26 and we get:
  - $v * 15 = 1 \pmod{26}$
  - Then if we find v, we find the inverse of 15 in mod 26.
  - So we start from 1 and work backward…

finding multi. inverse: EEA

- 26 = 1 * 15 + 11 => 11 = 26 – (1*15)
- 15 = 1 * 11 + 4 => 4 = 15 – (1*11)
- 11 = 2 * 4 + 3 => 3 = 11 – (2*4)
- 4 = 1 * 3 + 1 => 1 = 4 – (1*3)

Step 1) 1 = 4 – (1 * 3) = 4 – 3

Step 2) 1 = 4 – (11 – (2 * 4)) = 3 * 4 - 11

Step 3) 1 = 3 * (15 – 11) – 11 = 3 * 15 – 4 * 11

Step 4) 1 = 3 * 15 – 4(26 – (1*15))

Step 5) 1 = 7 * 15 – 4 * 26 = 105 – 104