Basic Number Theory

Lecture 15-16

Importance of Number Theory

Number theory is crucial for encryption algorithms and hence to security.

Of utmost importance to everyone from Bill Gates, to the CIA, to Osama Bin Laden.

The encryption algorithms depend heavily on modular arithmetic.

Machinery (notations and techniques) for manipulating numbers

Divisors

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

$$a = b \cdot c$$

- b and c are **factors** of a
- 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:

$$b \mid a \wedge c \mid a .$$

Divisors Examples

Which of the following is true?

1. $77 \mid 7$
2. $7 \mid 77$
3. $24 \mid 24$
4. $0 \mid 24$
5. $24 \mid 0$

Divisors Examples

1. 77 | 7: false bigger number can't divide smaller positive number
2. 7 | 77:
3. 24 | 24:
4. 0 | 24:
5. 24 | 0:

Divisors Examples

1. $77 \mid 7$: false bigger number can't divide smaller positive number
2. $7 \mid 77$: true because $77 = 7 \cdot 11$
3. $24 \mid 24$:
4. $0 \mid 24$:
5. $24 \mid 0$:

Divisors Examples

1. $77 \mid 7$: false bigger number can't divide smaller positive number
2. $7 \mid 77$: true because $77 = 7 \cdot 11$
3. $24 \mid 24$: true because $24 = 24 \cdot 1$
4. $0 \mid 24$:
5. $24 \mid 0$:

Divisors Examples

1. 77 | 7: false bigger number can’t divide smaller positive number
2. 7 | 77: true because 77 = 7 · 11
3. 24 | 24: true because 24 = 24 · 1
4. 0 | 24: false, only 0 is divisible by 0
5. 24 | 0:

Divisors Examples

1. $77 \mid 7$: false bigger number can't divide smaller positive number
2. $7 \mid 77$: true because $77 = 7 \cdot 11$
3. $24 \mid 24$: true because $24 = 24 \cdot 1$
4. $0 \mid 24$: false, only 0 is divisible by 0
5. $24 \mid 0$: true, 0 is divisible by every number ($0 = 24 \cdot 0$)

Multiples up to given *n*

How many positive multiples of 15 are less than 100?

Just list them:

15, 30, 45, 60, 75, 90

Therefore the answer is 6.

Q: How many positive multiples of 15 are less than 1,000,000?

Multiples up to given n

A: Listing is too much of a hassle. $\lfloor 1{,}000{,}000/15 \rfloor$.

In general: The number of d-multiples less than N is given by:

$$|\{m \in \mathbf{Z}^+ \mid d \mid m \text{ and } m \leq N\}| = \lfloor N/d \rfloor$$

Divisor Theorem

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

1. $a|b \land a|c$ □ $a|(b + c)$
2. $a|b$ □ $a|bc$
3. $a|b \land b|c$ □ $a|c$

EG:

Divisor Theorem

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

1. $a|b \land a|c$ □ $a|(b + c)$
2. $a|b$ □ $a|bc$
3. $a|b \land b|c$ □ $a|c$

EG:

1. $17|34 \land 17|170$ □ $17|204$

Divisor Theorem

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

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

EG:

1. $17|34 \land 17|170 \;\square\; 17|204$
2. $17|34 \;\square\; 17|340$

Divisor Theorem

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

1. $a|b \land a|c$ □ $a|(b + c)$
2. $a|b$ □ $a|bc$
3. $a|b \land b|c$ □ $a|c$

EG:

1. $17|34 \land 17|170$ □ $17|204$
2. $17|34$ □ $17|340$
3. $6|12 \land 12|144$ □ $6 | 144$

Divisor Theorem

In general, such statements are proved by starting from the definitions and manipulating to get the desired results.

EG. *Proof of no. 2* ($a|b$ □ $a|bc$):

Suppose $a|b$.

Then there exist m such that $b = am$.

Multiply both sides by c to get $bc = amc = a\,(mc)$.

Consequently, bc has been expressed as a times the integer mc so by definition of "|", $a|bc$ □

Prime Numbers

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***.

Q: Which of the following are prime?

0,1,2,3,4,5,6,7,8,9,10

Prime Numbers

A: 0, and 1 not prime since not positive and greater or equal to 2

2 is prime as 1 and 2 are only factors

3 is prime as 1 and 3 are only factors.

4,6,8,10 not prime as *non-trivially* divisible by 2.

5, 7 prime.

$9 = 3 \cdot 3$ not prime.

Last example shows that not all odd numbers are prime.

Fundamental Theorem of Arithmetic

Any number $n \geq 2$ is expressible as a unique product of 1 or more prime numbers.

Note: prime numbers are considered to be "products" of 1 and prime.

We'll need induction and some more number theory tools to prove this.

Q: Express each of the following number as a product of primes: 22, 100, 12, 17

Fundamental Theorem of Arithmetic

$$22 = 2 \cdot 11,$$
$$100 = 2 \cdot 2 \cdot 5 \cdot 5,$$
$$12 = 2 \cdot 2 \cdot 3,$$
$$17 = 17$$

Primality Testing

Prime numbers are very important in encryption schemes. Essential to be able to verify if a number is prime or not. It turns out that this is quite a difficult problem. First try:

```
boolean isPrime(integer n)
  if ( n < 2 ) return false
  for(i = 2 to n -1)
     if( i |n )    // "divides"
        return false
  return true
```

Q: What is the running time of this algorithm?

Primality Testing

A: Assuming divisibility testing is a basic operation –then above primality testing algorithm is $O(n)$.

Q: What is the running time in terms of the input size k ?

Primality Testing

A: Consider n = 1,000,000. The input size is $k = 7$ because n was described using only 7 digits. In general we have

$n = O(10^k)$. Therefore, running time is $O(10^k)$.

Q: Can we improve the algorithm?

Primality Testing

A:

- Don't try number bigger than $n/2$
- After trying 2, don't try any other even numbers, because know n is odd by this point.
- In general, try only smaller prime numbers
- In fact, only need to try to divide by prime numbers no larger than $\sqrt{n}$ as we'll see next:

Primality Testing

LEMMA: If *n* is a composite, then its smallest prime factor is ≤ $\sqrt{n}$

Proof (by contradiction). 1<a<n

n=ab

a<=n or b<=n

if a> $\sqrt{n}$ and b> $\sqrt{n}$ then ab> n

Primality Testing

EG: Test if 139 and 143 are prime.
List all primes up to $\sqrt{n}$ and check if they divide the numbers.

2: Neither is even

3: Sum of digits trick: 1+3+9 = 13, 1+4+3 = 8 so neither divisible by 3

5: Don't end in 0 or 5

7: 140 divisible by 7 so neither div. by 7

11: Alternating sum trick: 1-3+9 = 7 so 139 not div by 11. 1-4+3 = 0 so 143 *is* divisible by 11.

STOP! Next prime 13 need not be examined since bigger than $\sqrt{n}$.

Conclude: 139 is prime, 143 is composite.

Division

Remember long division?

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

d the ***divisor***

a the ***dividend***

q the ***quotient***

r the ***remainder***

117 = 31·3 + 24

$a = dq + r$

Division

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

$$a = dq + r$$

GCD and 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*** if gcd(a,b) = 1, so no prime common divisors.

GCD and 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.

GCD and Relatively Prime

EG: More realistic. Find gcd(98,420).

Find prime decomposition of each number and find all the common factors:

98 = $2\cdot 49 = 2\cdot 7\cdot 7$

420 = $2\cdot 210 = 2\cdot 2\cdot 105 = 2\cdot 2\cdot 3\cdot 35 = 2\cdot 2\cdot 3\cdot 5\cdot 7$

Underline common factors: $\underline{2\cdot 7}\cdot 7$, $2\cdot\underline{2}\cdot 3\cdot 5\cdot\underline{7}$

Therefore, gcd(98,420) = 14

Least Common Multiple

DEF: The ***least common multiple*** of *a*, and *b* (lcm(*a*,b)) is the smallest number *m* which is divisible by both *a* and *b*.

Q: Find the lcm's:

1. lcm(10,100)
2. lcm(7,5)
3. lcm(9,21)

Least Common Multiple

A:

1. lcm(10,100) = 100
2. lcm(7,5) = 35
3. lcm(9,21) = 63

THM: *lcm(a,b)* = *ab / gcd(a,b)*

Modular Arithmetic

There are two types of "mod" (confusing):

- the **mod** function
  - Inputs a number *a* and a base *b*
  - Outputs *a* **mod** *b* a number between 0 and $b-1$ inclusive
  - This is the remainder of a÷b
  - Similar to Java's % operator.
- the (mod) congruence
  - Relates two numbers *a, a'* to each other relative some base *b*
  - $a \equiv a'$ (mod *b*) means that *a* and *a'* have the same remainder when dividing by *b*

mod function

Similar to Java's "%" operator except that answer is always positive. E.G.

-10 **mod** 3 = 2, but in Java –10%3 = -1.

Q: Compute

1. 113 **mod** 24
2. -29 **mod** 7

mod function

A: Compute

1. 113 **mod** 24:

$$24\overline{\smash{)}113}$$

2. -29 **mod** 7

mod function

A: Compute

1. 113 **mod** 24:

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

2. -29 **mod** 7

mod function

A: Compute

1. 113 **mod** 24:

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

2. -29 **mod** 7

$$7\overline{)-29}$$

mod function

A: Compute

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

Let a, a' be integers and b be a positive integer. We say that a is congruent to a' modulo b (denoted by $a \equiv a' \pmod{b}$) iff $b \mid (a - a')$.

Equivalently: a **mod** $b = a'$ **mod** b

Q: Which of the following are true?

1. $3 \equiv 3 \pmod{17}$
2. $3 \equiv -3 \pmod{17}$
3. $172 \equiv 177 \pmod{5}$
4. $-13 \equiv 13 \pmod{26}$

(mod) congruence

- A:
- $3 \equiv 3 \pmod{17}$ True.

  any number is congruent to itself ($3-3 = 0$, divisible by all)
- $3 \equiv -3 \pmod{17}$ False.

  $(3-(-3)) = 6$ isn't divisible by 17.
- $172 \equiv 177 \pmod{5}$ True.

  $172-177 = -5$ is a multiple of 5
- $-13 \equiv 13 \pmod{26}$ True.

  $-13-13 = -26$ divisible by 26.

Modular arithmetic harder examples

Q: Compute the following.

1. 307^{1001} **mod** 102

2. $$\left(\sum_{i=4}^{23} 10^i\right) \bmod 11$$

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

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

$$307^{1001} \textbf{ mod } 102 \equiv 307^{1001} \pmod{102}$$
$$\equiv 1^{1001} \pmod{102} \qquad (102X3)$$
$$\equiv 1 \pmod{102}.$$

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

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

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

$$\left(\sum_{i=4}^{23} 10^i\right) \bmod 11 \equiv \left(\sum_{i=4}^{23} 10^i\right) \pmod{11}$$

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

10-(-1)

$$\equiv (1-1+1-1+\ldots+1-1) \pmod{11}$$

$$\equiv 0 \pmod{11}$$

Therefore, the answer is 0.

Simple Encryption

Variations on the following have been used to encrypt messages for thousands of years.

1. Convert a message to capitals.
2. Think of each letter as a number between 1 and 26.
3. Apply an invertible modular function to each number.
4. Convert back to letters (0 becomes 26).

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example: $f(a) = (a+3)$ **mod** 26

P	m	e	e	t		m	e		a	f	t	e	r		t	h	e		t	o	g	a		p	a	r	t	y
C	P	H	H	W		P	H		D	I	W	H	U		W	K	H		W	R	J	D		S	D	U	W	B

Caesar Cipher

- can define transformation as:

  a b c d e f g h i j k l m n o p q r s t u v w x y z

  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- then have Caesar cipher as:

  $c = \mathrm{E}(p) = (p + k) \bmod (26)$

  $p = \mathrm{D}(c) = (c - k) \bmod (26)$

Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Monoalphabetic Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters (1 to 25 in the previous case)
- do need to recognize when have plaintext

Example Cryptanalysis

- given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- count relative letter frequencies
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:

  it was disclosed yesterday that several informal but
  direct contacts have been made with political
  representatives of the viet cong in moscow

Thank You

(mod) congruence

- A congruence of the form $ax \equiv b$ (mod m),
- where m is a positive integer, a and b are integers, and x is a variable, is called a **linear congruence**.
- One method that we will describe uses an integer $\bar{a}$ such that $a.\bar{a} \equiv 1$ (mod m) if such an integer exists. Such an integer $\bar{a}$ is said to be an **inverse** of a modulo m. Here, **gcd (a, m) must be 1.**
- **Example**
- What are the solutions of the linear congruence $3x \equiv 4$ (mod 7)?
  - with $x \equiv 6$ (mod 7) is a solution because,
  - $3x \equiv 3 \cdot 6 = 18 \equiv 4$ (mod 7),
- We conclude that the solutions to the congruence are the integers x such that $x \equiv 6$ (mod 7), namely, 6, 13, 20, . . . and −1, −8, −15, ...

Chinese Reminder Theorem

- Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ *arbitrary integers*. Than the system

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

- has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Chinese Reminder Theorem

- To construct a simultaneous solution, first, let

$$M_k = m/m_k$$

- for $k = 1, 2, \ldots, n$.
- we know that there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

- To construct a simultaneous solution, form the sum

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n.$$

Chinese Reminder Theorem

- **Example**
- What is the smallest positive integer, when divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?
- This puzzle can be translated into the following question: What are the solutions of the systems of congruences

$$x \equiv 2 \pmod 3,$$

$$x \equiv 3 \pmod 5,$$

$$x \equiv 2 \pmod 7$$

- At first let $m = 3 \cdot 5 \cdot 7 = 105$,
- $M_1 = m/3 = 35, M_2 = m/5 = 21$, and $M_3 = m/7 = 15$

Chinese Reminder Theorem

- **Example**
- We see that 2 is an inverse of $M1 = 35$ modulo 3, because

$$35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod{3};$$

- 1 is an inverse of $M2 = 21$ modulo 5, because $21 \equiv 1 \pmod{5}$;
- 1 is an inverse of $M3 = 15 \pmod{7}$, because $15 \equiv 1 \pmod{7}$.
- The solutions to this system are those x such that
- $x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$

$$= 233 \equiv 23 \pmod{105}.$$

It follows that 23 is the smallest positive integer that is a simultaneous solution.