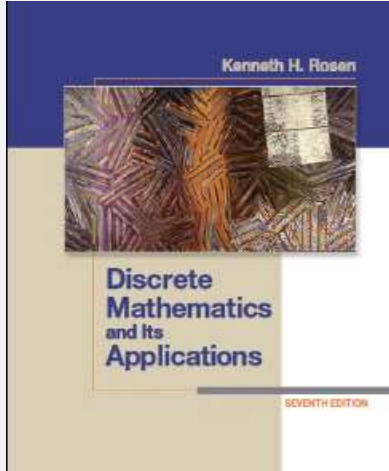


CSE 101: Discrete Mathematics



Slide 09

Number Theory

Presented by

Md. Sultanul Islam Ovi

Lecturer

Department of Computer Science and Engineering(CSE)

Green University of Bangladesh(GUB)

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**.

Numbers are of two types (PARITY): EVEN(**$2k$**) or ODD(**$2k - 1$**)

$$\text{Even} + \text{Even} = \text{Even}$$

$$\text{Even} + \text{Odd} = \text{Odd}$$

$$\text{Odd} + \text{Odd} = \text{Even}$$

$$\text{Even} \times \text{Even} = \text{Even}$$

$$\text{Even} \times \text{Odd} = \text{Even}$$

$$\text{Odd} \times \text{Odd} = \text{Odd}$$

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. $77 \mid 7$ **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 ($0 = 24 \cdot 0$)
6. $7 \mid -14$ **True** because $-14 = 7 \cdot (-2)$

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?

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

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

1. $a|b \wedge a|c \Rightarrow a|(b + c)$

2. $a|b \Rightarrow a|bc$

3. $a|b \wedge b|c \Rightarrow a|c$

1. $17|34 \wedge 17|170 \Rightarrow 17|204$

2. $17|34 \Rightarrow 17|340$

3. $6|12 \wedge 12|144 \Rightarrow 6|144$

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* ($a|b \Rightarrow a|bc$):

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 “|”, $a|bc \Rightarrow$

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

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.

Fundamental Theorem of Arithmetic

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

$$22 = 2 \cdot 11,$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5,$$

$$12 = 2 \cdot 2 \cdot 3,$$

$$17 = 17$$

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(  $i \mid n$  )    // “divides”
```

```
            return false
```

```
    return true
```

Primality Testing

Q: What is the running time of this algorithm?

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 ?

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:

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

Proof (by contradiction). $1 < a < n$

$$n = ab \implies a \leq n \text{ or } b \leq n$$

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?

— d the
divisor

— a the
dividend

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

— q the
quotient

— r the
remainder

$$117 = 31 \cdot 3 + 24$$

$$a = dq + r$$

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

GCD and Relatively Prime

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 .

- a and b are said to be **relatively prime** if $\text{gcd}(a, b) = 1$, so **no prime common divisors**.
- $\text{gcd}(11, 77) = 11$
- $\text{gcd}(33, 77) = 11$
- $\text{gcd}(24, 36) = 12$
- $\text{gcd}(24, 25) = 1$. 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: $\underline{2} \cdot \underline{7} \cdot 7$, $2 \cdot \underline{2} \cdot 3 \cdot 5 \cdot \underline{7}$

Therefore, $\gcd(98,420) = 14$

Least Common Multiple

The ***least common multiple*** of a , and b ($\text{lcm}(a,b)$) is the smallest number m which is divisible by both a and b .

Find the lcm:

1. $\text{lcm}(10,100) = 100$
2. $\text{lcm}(7,5) = 35$
3. $\text{lcm}(9,21) = 63$

$$\text{lcm}(a,b) = ab / \text{gcd}(a,b)$$

Modular Arithmetic

There are two types of “mod” (confusing):

→ the **mod** function

- ◆ Inputs a number a and a base b
- ◆ Outputs $a \bmod b$ a number between 0 and $b - 1$ inclusive
- ◆ This is the remainder of $a \div b$

→ 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

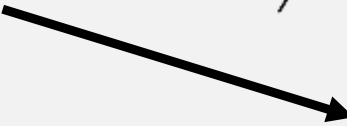
mod function

answer is always
positive. E.G.

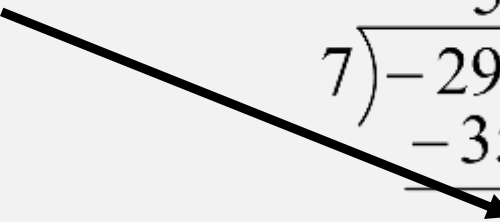
$$-10 \bmod 3 = 2.$$

A: Compute

1. $113 \bmod 24$

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


1. $-29 \bmod 7$

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


(mod) congruence Formal Definition

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

Equivalently: $a \bmod n = b \bmod n$

Which of the following are true?

1. $3 \equiv 3 \pmod{17}$ True.
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.

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

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

$$\begin{aligned} 307^{1001} \bmod 102 &\equiv 307^{1001} \pmod{102} \\ &\equiv 1^{1001} \pmod{102} \quad (102 \times 3) \\ &\equiv 1 \pmod{102}. \end{aligned}$$

Therefore, $307^{1001} \bmod 102 = 1$.

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

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

$$\begin{aligned}\left(\sum_{i=4}^{23} 10^i\right) \bmod 11 &\equiv \left(\sum_{i=4}^{23} 10^i\right) (\bmod 11) \\ &\equiv \left(\sum_{i=4}^{23} (-1)^i\right) (\bmod 11) && 10 \equiv (-1) \\ &\equiv (1 - 1 + 1 - 1 + \dots + 1 - 1) (\bmod 11) \\ &\equiv 0 (\bmod 11)\end{aligned}$$

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

- **Example:** replace each letter by 3rd letter on
 - $f(a) = (a+3) \bmod 26$
- **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:**
 - cipher text, $c = \text{Encryption}(p) = (p + k) \bmod (26)$
 - plain text, $p = \text{Decryption}(c) = (c - k) \bmod (26)$

Example: Apply caesar cipher with $k = 2$ in the plain text “HELLO”

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

- 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**)
- do need to recognize when have plaintext

Book References

- Chapter 4.1 (Page 237)
- Chapter 4.3 (Page 257)
- Chapter 4.4 (Page 274)
 - ◆ Problem (Problem 01 - 10) (Page 284)

Thank You