Lecture 37

29 November 2021 11:52

Unit 6: Number Theory and its Applications in Cryptography

Text Book: Chapter 4

Divisibility and Modular Arithmetic

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

$a|b \Rightarrow$ a divides b

- **Let n and d be positive integers then no. of positive integers not exceeding n, that are divisible by d are $\left\lfloor \frac{n}{d} \right\rfloor$.**

$\lfloor\ \ \rfloor \rightarrow$ Floor fn / GINT

Q1. How many numbers from 1 to 1500 are divisible by 9?

(A) 165 (B) 166 (C) 167 (D) 160

$\left\lfloor \frac{1500}{9} \right\rfloor = \lfloor 166.7 \rfloor$

Theorem 1:

Let a, b, and c be integers, where $a \neq 0$. Then

(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(*ii*) if $a \mid b$, then $a \mid bc$ for all integers c;
(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

$a|b \Rightarrow b = k_1 a$
$a|c \Rightarrow c = k_2 a$
$b + c = (k_1 + k_2)a$

Corollary 1:

Corollary 1:

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

The Division Algorithm

Theorem 2: Let a be an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

remainder

Dividend Divisor quotient a mod d

a div d

Q2. What are the quotients and remainders when

(i) 777 is divided by 21?

$q = 777 \text{ div } 21 = 37$

$r = 777 \bmod 21 = 0$

(ii) -111 is divided by 11?

$-111 = 11(-10) - 1$

$-111 = 11(-11) + 10$

$r > 0$

$q = -111 \text{ div } 11 = -11$

$r = -111 \bmod 11 = 10$

Q3. Find the value of

(i) 1,234,567 div 1001 $= 1233$

$100 = 101(0) + 100$

(ii) $-100 \; mod \; 101 =$ 1

$-100 = 101(-1) + 1$

Q4. What time does a 12-hour clock read

(i) 80 hours after it reads 11:00?

(i) 80 hours after it reads 11:00?

$80 = 12(6)+8$ 　　 7:00

(ii) 40 hours before it reads 12:00?

(A) 4:00 　 (B) 8:00 　 (C) 10:00 　 (D) 6:00

$40 = 12(3)+4$

Modular Arithmetic

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a-b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

$m \mid (a-b)$ 　 $a \equiv b \bmod m$ 　 $a \bmod m = b$

Theorem 3:

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mathbin{\mathbf{mod}} m = b \mathbin{\mathbf{mod}} m$.

$a-b$

Theorem 4:

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

$m \mid a-b =$ 　 $a-b=km,$ 　 $a=b+km$

Theorem 5:

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

$a = b + k_1 m,$ 　 $c = d + k_2 m$

$a = b + k_1 m$, $c = d + k_2 m$

$a + c = (b+d) + (k_1 + k_2)m$

Corollary 2:

Let m be a positive integer and let a and b be integers. Then

$$(a+b) \mathbf{~mod~} m = ((a \mathbf{~mod~} m) + (b \mathbf{~mod~} m)) \mathbf{~mod~} m$$

and

$$ab \mathbf{~mod~} m = ((a \mathbf{~mod~} m)(b \mathbf{~mod~} m)) \mathbf{~mod~} m.$$

$15 \bmod 3 = 0$

$(8+7)$

$8 \bmod 3 + 7 \bmod 3$

$2 + 1 = 3 \bmod 3 = 0$

To be noted:

- $a \equiv b \bmod m \Rightarrow ac \equiv bc \bmod m$

  $m \mid (a-b) \Rightarrow m \mid (a-b)c$

- $a \equiv b \bmod m \Rightarrow a^c \equiv b^c \bmod m$

  $m \mid a-b$

  $m \mid (a^2 - b^2)$

- $a \equiv b \bmod m$ and $c \equiv d \bmod m \nRightarrow a^c \bmod m \equiv b^d \bmod m$

- $ac \equiv bc \bmod m \nRightarrow a \bmod m \equiv b \bmod m$

  $21 \equiv 9 \bmod 6$

  $7 \not\equiv 3 \bmod 6$

Theorem 6: Let m be a positive integer and let a, b and c be integers. If $ac \equiv bc \bmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \bmod m$.

Q5.

Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and

Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \le c \le 12$ such that

a) $c \equiv 9a \pmod{13}$.
b) $c \equiv 11b \pmod{13}$.
c) $c \equiv a + b \pmod{13}$.
d) $c \equiv 2a + 3b \pmod{13}$.
e) $c \equiv a^2 + b^2 \pmod{13}$.
f) $c \equiv a^3 - b^3 \pmod{13}$.

(c) $a+b \equiv 13 \pmod{13}$

$a+b = 0 \pmod{13}$, $c=0$

(a) $a \equiv 4 \pmod{13}$

$9a \equiv 36 \pmod{13}$, $9a \equiv 10 \pmod{13}$, $c=10$

(b) $b \equiv 9 \pmod{13}$, $11b \equiv 99 \pmod{13}$, $11b \equiv 8 \pmod{13}$

$c=8$