# Mod (III)

## The Integers and Division

If a & b are Integers with $a \neq 0$, we say that 'a divides b' if there is an Integer c s.t. $b = ac$

when a divides b' we say that a is a factor of b & that b is a multiple of a. The notation a/b denotes that 'a divides b'. we write $a \times b$ when a does not divide b

we can express a/b using quantifiers as $\exists c(ac=b)$ where the Universe of dispose is the set of Integers

Determine whether 3/7 and whether 3/12

we have 3 divides 7 but $\frac{7}{3}$ is not an Integer

but 3 divides 12 bc $\frac{12}{3}=4$ is an Integer

- Let n & d be +ve Integers. How many +ve Integers not exceeding n are divisible by d.

The +ve Integers divisible by d are all the Integers of the form dk where k is a +ve Integer.

Hence the no. of +ve Integers divisible by d that do not exceed n equals the no. of Integers k with $0 \leq dk \leq n$ or with $0 < k \leq \frac{n}{d}$. Hence there

are $\& \lfloor \frac{n}{a} \rfloor$ +ve Integers not exceeding n that are divisible by a.

Theorem

Let a, b & c be Integers then

1) If a/b and a/c then a/b+c
2) If a/b then a/bc for all Integers c
3) If a/b and b/c then a/c

1. Proof

Given that a, b, & c are Integers

~~Let~~

1. assume that a/b & a/c

To P.T a/b+c

$a/b \Rightarrow b = as$ for some Integer s

$a/c \Rightarrow c = at$ for some Integer t

Consider $\frac{b+c}{a} = \frac{as+at}{a} = \frac{a(s+t)}{a} = s+t$

$\Rightarrow \frac{b+c}{a} = s+t$

$\Rightarrow b+c = a(s+t)$

$\Rightarrow a/b+c$

2. Assume that a/b

To P.T a/bc, where c is an Integer

$a/b \Rightarrow b = as$ for some Integer s

Consider $\frac{bc}{a} = \frac{asc}{a} = sc$

$$\frac{bc}{a} = sc$$

$$bc = (sc)\,a$$

$$\Rightarrow a \mid bc$$

Assume that $a \mid b$ & $b \mid c$

To P.T $a \mid c$.

$$\frac{a}{b} \Rightarrow bs \text{ for some Integer } s$$

$$a \Rightarrow \frac{bs}{b}$$

$$\frac{b}{c} \Rightarrow c = bt \text{ for some Integer } c$$

$$\frac{b}{a} = s$$

Consider $\frac{c}{a} = \frac{bt}{a}$

=

Corollary

If a, b and c are Integers such that $a \mid b$ & $a \mid c$ then $a \mid mb + nc$ where m and n are Integers

$a \mid b \Rightarrow b = as$ for some I s.

$a \mid c \Rightarrow c = at$ for some I t

$$\frac{mb + nc}{a} = \frac{m \times as + n \times at}{a}$$

$$= a\,\frac{(ms + nt)}{a}$$

$= ms + nt$ (4)

$\therefore a/mb+nc$

$\therefore$ a divides $mb+nc$.

## The Division Algorithm

Let ab an Integer and da +ve integer then there are unique Integers $q$ and $r$ with $0 \le r < d$ such that $a = dq + r$.

In the equality given in the division algorithm d is called the divisor a is called divident, q is called the quotient & $r$ is called the remainder. The following notation is used to express the quotient and remainder.

$$q = a \text{ div } d$$
$$r = a \bmod d$$

$$\begin{array}{r} 9 \\ 11\overline{)101} \\ 99 \\ \hline 2 \end{array}$$

→ what are the quotient when 101 is divide by 11

$101 = 11 \times 9 + 2$.

quotient $= 9$

$$2 = 101 \bmod 11$$

→ What are the quotient & remainder when -11 is divide by 3.

$$-4 = -11 \text{ div } 3$$
$$1 = -11 \bmod 3$$

$$\begin{array}{r} -3 \\ 3\overline{)-11} \\ -9 \\ \hline -2 \end{array}$$

$-11 = 3x-3-2$

$= 3x-4+1$

(To make remainder +ve)

→ What are the quotient & remainder when 19 is divides by 7

→ -111 is dividing by 11

$$111 = 11 \times 10 + 1$$
$$-111 = 11 \times -10 - 1$$
$$= 11 \times -11 + 10$$

- 789 is divide by 23
- 0-1 is divide by 3

Definition

If a and b are Integers and m is a +ve Integer, then a is a Congruent to b modulo m if m divides a-b (a-b is divisible by m). we use the notation

$a \equiv b \pmod{m}$ to indicate that a is congruent to b mod m if a & b are not congruent modulom we write $a \not\equiv b \pmod{m}$

Let a and b be Integers and let m be a +ve Integer then $a \equiv b \pmod{m}$ if and only if and only if $a \bmod m = b \bmod m$

- Assume that $a \equiv b \pmod{m}$

To prove that $a \bmod m = b \bmod m$

$$a \equiv b \pmod{m} \Rightarrow m / a-b$$
$$\Rightarrow a-b = ms \text{ for some Integer } s$$
$$\Rightarrow a = b+ms$$

→ Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6

To P.T 17 congruent to 5 modulo 6

$17 - 5 = 12$

$\frac{12}{6} = 2$

$17 \equiv 5 \pmod 6$

$24 - 14 = 10$

10 does not $10 \times 6$

$24 \not\equiv 14 \pmod 6$

Evaluate $-17 \bmod 2$

$17 = 2 \times (-8) - 1$

$= 2x - 9 + 1$

- $144 \bmod 7$

$7 \times 20 + 4$

- Let m be a +ve Integer the Integers a & b are Congruent modulo m if and only if there is an Integer k such that $a = b + km$.

Proof

Assume that a & b are congruent modulo m

i.e $a \equiv b \pmod m$

$a \equiv b \pmod m \Rightarrow m \mid a - b$

$\Rightarrow a - b = mk$ for some Integer k

$\Rightarrow a = b + km$ for some Integer k

Hence there is an Integer $k$ s.t $a = b + km$

Case 2:

Assume that $a = b+km$ for some Integer $k$.

$a \equiv b+km$ for some Integer $k \Rightarrow a-b = km$

$\Rightarrow m/a-b$

$\Rightarrow a \equiv b \bmod m$

- Let $m$ be a positive Integer $a \equiv b \pmod m$ and $c$ congruent to $d \pmod m$ then $a+c \equiv b+d \pmod m$ & $ac$ congruent to $bd \pmod m$

Given that $a \equiv b \pmod m$ & $c \equiv d \pmod m$ then there are Integers $s$ & $t$ with $a-b = ms$

$c-d = mt$

i.e $a = b+ms$ — ①

$c = d+mt$ — ②

Consider (adding ① & ②)

$a+c = b+d+ms+mt$

$a+c = b+d+m(s+t)$

$(a+c)-(b+d) = m(s+t)$

$a+c \equiv b+d \pmod m$

① × ②

$ac = (b+ms)(d+mt)$

$bd + bmt + dms + m^2ts$

$= bd + m(bt + ds + mts)$

$ac - bd = m(bt + ds + mts)$

$\Rightarrow ac \equiv bd \pmod m$ //

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$7+11 \equiv (2+1) \pmod 5$

$18 = 3 \pmod 5$

$11 \times 7 \equiv (2 \times 1) \pmod 1$

$77 \equiv 2 \pmod 5$

## Result

Let m be a +ve Integer and let a & b be Integers

then $a+b \pmod m$ $(a+b) \bmod m = ((a \bmod m)+(b \bmod m)) \bmod m$

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

we have $a \equiv (a \bmod m) \pmod m$.

$b \equiv (b \bmod m) \pmod m$

By the above theorem

$a+b \equiv ((a \bmod m)+(b \bmod m)) \pmod m$

$ab = ((a \bmod m)(b \bmod m)) \bmod m$

$(a+b) \bmod m = (a \bmod m)+ b \bmod m$

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

$(\because a \equiv b \pmod m$ iff $a \bmod m = b \bmod m)$

## Applications of Congruences:-

Pseudorandom Numbers:- randomly choosen no's are often needed for computer

Stimulation. The most commonly used proudure for generating pseudo random nos is the linear congruential method we choose 4 integers:

(1) the modulus m, multiplier a, increment c and seed $x_0$ $a \leq a < m$, $0 \leq c < m$ & $0 \leq x_0 < m$. we generate a sequence of pseudo random nos $\{x_n\}$ with $0 \leq x_n < m$ for all n by sucessively using the congruence $x_{n+1} \equiv (a x_n + c) \pmod m$

- what sequence of pseudo random nos is generated using the linear congruential generator $x_{n+1}$ congruent $(x_{n+1} + c) \pmod m$ where $m = 9$, $a = 7$, $c = 4$ & $x_0 = 3$

$$x_1 \equiv (7 \times 3 + 4) \pmod 9$$
$$= 25 \pmod 9$$
$$x_1 = 25 \pmod 9$$
$$x_1 = 7$$

$$x_2 \equiv (7 x_1 + 4) \bmod 9$$
$$\equiv (7 \times 7 + 4) \bmod 9$$
$$= 53 \bmod 9$$
$$x_2 = 8$$

$$x_3 = (7 x_2 + 4) \bmod 9 = (56 + 4) \bmod 9$$
$$= 60 \bmod 9)$$
$$x_3 = 6$$

$$x_4 \equiv (7 \times 6 + 4) \bmod 9 = 42 + 4$$
$$= 46 \pmod 9$$
$$\equiv 1$$

$x_5 = 2$ $x_7 = 4$ $x_9 = 3$
$x_6 = 0$ $x_8 = 5$

Hence the sequence is 3, 7, 8, 2, 0, 4, 5, 3, 7, 8 ....
This sequence contain 9 different nos before repeating

what sequence of pseudo nos is generated using the pure multiplicative generator $x_{n+1} = 3x_n \pmod{11}$ with seed $x_0 = 2$

$x_1 = 3 \times 2 \pmod{11}$
$x_1 = 6 \pmod{11}$
$x_1 = 6$

$x_2 = 3 \times 6 \pmod{11}$
$x_2 = 18 \pmod{11}$
$x_2 = 7$

$x_3 \equiv 3 \times 7 \pmod{11}$
$= 21 \pmod{11}$
$x_3 = 10$

$x_4 = 3 \times 10 \pmod{11}$
$= 30 \pmod{11}$
$= 8$

$x_5 = 3 \times 8 \pmod{11}$
$= 24 \pmod{11}$
$x_5 = 2$

what sequence of pseudo numbers is generated using the linear congruential generator $x_{n+1} \equiv (4x_n + 1) \pmod{7}$ with seed $x_0 = 3$.

## Cryptography

Encription means the process of making a message secret. The process of determine the orginal message from the encripted message is called decription.

## Caesar Cipher (cipher means codes)



To express ~~tea~~ Caesar's encription process mathematically 1st replace each letters by an Integer from 0 to 25 based on its position in the alphabet

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Caesar's Encript$^n$ method can be represented by the function $f$ that assigns to the non negative Integer $p$, $p \leq 25$, the Integer $f(p) \in \{0, 1, 2 \cdots 25\}$ with $f(p) \equiv (p+3) \pmod{26}$

or $c \equiv p+3 \pmod{26}$

To recover the orginal message from a Secret mesage encrypted by the function $f^{-1}$ the inverse of $f$ is used i.e $f^{-1}(p) \equiv (p-3) \pmod{26}$

What is the secret message produced from the message "MEET YOU IN THE PARK" using the Ceasar cipher.

1st replace the letters in the message with nos.

No Next replace each of the nos p by $C = f(p) \equiv p+3 \pmod{26}$ Translateing this back letters produces the encripted message.

MEET YOU IN THE PARK
12 04 04 19 24 14 20 08 13 19 07 04 15 00 17 10
15 07 07 22 01 17 23 11 11 22 10 07 18 03 20 13

$f(p) = p+3 \pmod{26}$

PHHW BRX LQ WKH SPUN

Encripted message is (PHHW BRX LQ WKH SPUN)

- what letter replaces the letter k when the function $f(p) = (7p+3) \bmod 26$ is used for Encription.

we have 10 represents k

$\therefore P = 10$, $f(p) = (7 \times 10 + 3) \bmod 26$

$= 73 \pmod{26}$

$\therefore$ 21 represent V

$\therefore$ k is replaced by V in the encripted message.

- Encript the message "DO NOT PASS GO". by translating the letters into numbers applying the encription function & then translating the nos back to letters.

1) $f(p) = (p+3) \bmod 26$
2) $f(p) = (p+13) \bmod 26$.
3) $f(p) = (3p+7) \bmod 26$.

- Decript the messages encripted using the ceaser cipher

| E | O | X | H | M | H | D | Q | V |
|---|---|---|---|---|---|---|---|---|
| 04 | 14 | 23 | 07 | 12 | 07 | 03 | 16 | 21 |
| 01 | 11 | 20 | 04 | 9 | 04 | 00 | 13 | 18 |
| B | L | U | E | J | E | A | N | S |

H.w

- W H V W W R G D B
- H D W G L P V X P

## Primes and Greatest Common Divisor :-

### Definition

A +ve Integer p greater than 1 is called prime is the only +ve factors of p are 1 & p. A +ve Integer i.e greater than 1 & is not prime is called composite.

### Remark

The Integer n is composite if and only if there exist an Integer n s.t $a/n$, $1<a<n$.

Ex: The Integer 7 is prime, the Integer 9 is composite.

The fundamental theorem of arithmetic Every +ve Integer greater than 1 can be written uniquely as a prime or as the product of 2/more primes where the prime factors are written in oder of non decreasing size.

- Find the prime factorization of 1024

$1024 = 2^{10}$

$641 = 641$

$999 = 3^3 \times 37$

| 641 |
|---|

| 999 |
|---|
| 3 |
| 3 |
| 3 |
| 37 |

| 1024 |
|---|
| 2 |
| 2 |
| 2 |
| 2 |
| 2 |
| 2 |
| 2 |
| 2 |

If $n$ is a composite Integer then $n$ has a prime divisor $\leq \sqrt{n}$

If $n$ is composite by the definition of a composite Integer we know that it has a factor $a$ with $1 < a < n$. Then we can write $n = ab$ for some Integer $b > 1$

To P.T $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

If possible assume that $a > \sqrt{n}$ & $b > \sqrt{n}$

Then $ab > \sqrt{n} \cdot \sqrt{n} = n$ i.e $ab > n$ which is a contradiction.

∴ $n$ has a positive divisor not exceeding $\sqrt{n}$

This divisor is either prime or composite. If this divisor is composite then by fundamental theorem of arithmetic. This divisor has a prime divisor less than itself. In either case $n$ has a prime divisor less than or equal to $\sqrt{n}$.

- S.T 101 is prime

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5 & 7 but ~~the only pr~~ 101 is not divisible by

2, 3, 5 or 7

∴ 101 is prime

- Find the prime factorization of 7007

To find the prime factorization of 7007 none of the primes 2, 3 & 5 divides 7007

$7007 = 7^2 \times 11 \times 13$

7 | 7007
7 | 1001
11 | 143
13

- Show that there are infinetley many primes:-

The proof is by contradict$^n$ there are only finating many primes $P_1, P_2 \cdots P_n$ Let $q = P_1 \times P_2 \cdots P_n + 1$

By the fundamental theorem of aeithmetic q is either peime or it can be written as the product of 2 or more primes. But none of the primes $P_1, P_2 \cdots P_n$ divides q.

∴ q is either peime or composite if q is compost then q has a peime factor othee than $P_1, P_2 \cdots P_n$ which is a contradiction we assume that thee are only finately many peimes.

## The peime number theorem

The ratio of the no. of primes not exceding x and $x/\ln x$ approaches 1 as x grows without bount. Here $\ln x$ is the

natural logarithm of $x$. Greatest common divisors & least common multiples. let a & b be integers not more 0 the largest Integer d s.t $d|a$ & $d|b$ is called the greatest common divisor of a & b. The greatest common divisor of A & B denoted by gcd(a,b).

what is the greatest common divisor of 24 & 36

G.C.D = 2 × 2 × 3
= 12

| | |
|---|---|
| 2 | 24, 36 |
| 2 | 12, 18 |
| 3 | 6, 9 |
| | 2, 3 |

gcd(24, 36) = 12

- what is the greatest common divisor of 17 & 22.

17, 22

G.C.D of 17, 22 = 1

- The Integers a & b are relatively prime if their greatest common divisor is 1.

17 & 22 are relatively primes.

- The Integers $a_1, a_2 \ldots\ldots a_n$ pair wise relatively prime if $G.C.D(a_i, a_j) = 1$ if $1 \le i < j \le n$
- Determine whether the Integers 10, 17 & 21 are Pairwise relatively prime & whether the Integers 10, 19, 24 are pairwise relatively prime.

gcd(10, 17) = 1
gcd(17, 21) = 1
gcd(10, 21) = 1

10, 17, & 21 is Pairwise relatively prime

Consider the gcd of 10, 24 $< 1$

$\therefore$ they are not pairwise relatively prime

Note: Suppose that the prime factorization of a & b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where $p_1, p_2 \cdots$ are prime nos

the gcd of a b $= p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

→ Find the G.C.D of 120 & 500

$120 = 2^3 \cdot 3 \cdot 5$

$500 = 2^2 \cdot 5^3$

$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)}$

$= 4 \times 5 = 20$

→ what are the greatest common divisors of the pair of integers.

1) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

$\gcd(a,b) = 2^{\min(0,11)} \cdot 3^{\min(7,5)} 5^{\min(3,9)} \cdot 7^{\min(3,0)}$

$= 2^0 \cdot 3^5 \cdot 5^3 \cdot 7^0$

$= \underline{3^5 \cdot 5^3}$

2) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

The least common multiple of the +ve integers (a & b) is the smallest +ve

Integers that is divisible by a & b. The least common multiple of a & b is denoted by Lcm of (a,b)

By using the same definition of a & b

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

(18)

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

- What is the least common multiple of $2^3 3^5 7^2$ and $2^4 \cdot 3^3$

$$\text{L.C.M of } (2^3 3^5 7^2, 2^4 \cdot 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)}$$

$$= 2^4 \cdot 3^5 \cdot 7^2$$

- what is the least common multiple of each pairs

1) $3^7 5^3 7^3, 2^{11} \cdot 3^5 \cdot 5^9$

2) $11 \cdot 13 \cdot 17, 2^9, 3^7 \cdot 5^5, 7^3$.

Let a & b be +ve integers then g.c.d of ab

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

let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$

$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ ...

Prime factors of a & b

$$ab = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \times$$