## Number theory

The division algorithm: let a be an integer and d a positive integer. Then there are unique integers q and  $\pi$ , with  $0 \le \pi < d$  such that  $\alpha = dq + \pi$ 

Here, d is called divisor, a is called the dividend q is called the quotient, r is called the remainder  $q = a \, div \, d$ ,  $r = a \, mod \, d$ 

divided by 11 and -11 divided by 3?

DOIN: we have 101 = 11.9 + 2

 $d = 11, q = 9, \pi = 2.$ 

d=3, q=-4,  $\pi=1$ 

\* Modular arithmatic:

pegn. If a and b are integers and m, in a positive integer, then air congruent to b modulo m if m divides a-b. We use the notation a=b(mod m) to indicate that a is congruent to b modulo m. If

a and b arre not congruent modulo m, we write a to (mod m)

integers, then a = b (mod m) if and only if a mod m=

1. Determine whether 17 is anythent to 5 modulo .
6 and whether 24 and 14 are congruent modulo .
6?

DOIN: 6 divides so, 17-5 = 12 Now  $17 = 5 \pmod{6}$  but 24 -14 = 10 which is not divisible by 6 so, 24 \neq 14 (mod 6).

Theorem: let m be a positive integers. The integers a and b are congruent modulo m if and only if there is an integer K such that a = b + km.

so that  $a = b \pmod{m}$  then  $m \mid (a-b)$ . This means that there is an integer k such that a - b = km so that a = b + km. Conversely there is an integer k such that a = b + km. km = a - b there m + div ides a - b so that  $a = b \pmod{m}$ 

st in former a difference of the same are often which

in a survey of lastranger or bell strained of

Theorem: let in be a positive integer, if a = 6 (modelm) and a = d (mod m) then a to = b +d (mod m) and ac = (a in 1) ? . (b) - 1 ; . bd (mod m)

proof: Decause a = b (mod m) and a = d (mod m) there arre integers s and t with b = a + sm and d=c+tm b+d = a + sm + c + tm crala ... ale pro -10 co

= (ata) + m (n++)

: atc = (b+d) (mod m)

bd = (a+sm) (a++m)

 $ac = bd \pmod{m}$ 

angptology:

1. What letter replace the letter k when the sunc tion fre) =(7P+3) mod 26 is used for encryption?

[1] 1 1, in 1/11

SOIT:- K MEPTIONENTA 10 so that,

f(10) = (7.10+3) mod 26

= 21

s. (PLED by . 100 which represents v so k is replace by v. alone in a straight and a straight and a single

estains at the sex . :

2. What is the Least common multiple of 23 57 and 501":- We have, 10m = 2 max (3,4) 3 max (5,3) x max (2,0) = 24357 \* Euclidean algorithm: 1 - 141 110 500 procedure: ged (a, b) 1 . (11 11 ) hor X: = a p - ( ) ( ) ( ) ( ) ( ) y; = b the second of th while y \$ 0 begin 15 - 10001 100 r: = x mody to tall a comme to prove the stall X: = X y: = r the teacher of worth and the end [ ged (a,b) in x] If a=ba+r and a, b, a and II are integers. Then ged (a,b) = ged (b,r) a = bai + ri o < ri < b × b=1, a2 + 12 05 12 < 17 17 = 12 ag + 13 OS 13 < 12

 $r_{n-3} = r_{n-2} a_{n-1} + r_{n-1}$ 

Defny. The integers a, az - an ant paintoise relative prime if ged (ai, aj) =1. whenever 15icjen. 1. Determine whether the integers 10,17.21 are pain wise relatively prime and whether the integers 10,19. 24 are pairroise relatively prime? soln: gcd (10,17) =1 (introduction specialist ged (10,21) =1 gcd (17:21) =1 they are pairwise relatively prime. ged (10,24) =271 they are not pairtwise relatively prime. 1. Using prime factorizations the ged of 120 and 500 2 5017:- Herre, 120 = 23.3.5 500 = 2.53 ged (120, 500) = 2 min (3.2) min (1.0) min (4.2)

= 2, 30, 51

= 20

of Decause x=2 (mod 5) and 11 = 1 (mod 5) it follows the theorem that woom bod . or a north (mission he is but) for by minist 18 = 7+11 = 2+1 = 3 (mod 5) xx = x·11 = 21 = 2 (mod 5) Theorem 1:- Let a, b and c arre, integers then had w all and all then albte (them to (oth) proofe- if alb and alc then defn of divisibility the re arre integers s and + b=as, e=at : bte = astat = a(st) .: a divides beta so that alletal Carlon int = 00 ... GICD and LCM 1. What is the greatest common divisor of 24 and 367 The second of the second of the second of the second son: ged (24, 36) = 12 Inthe Matamina de se 2. What is the greatest common division of 17 and 22) sol?: gcd (17.22) =1 pefn: The integers arm relatively prime if their

gcd = 1

1 . 1 X 3 . 31 rn-2 = rn-1 an + rn, 0 ≤ rn < rn-1 11 1 X 7 when n=0, then gcd (a,b) = 17n-1 11-140 . 1 № 15 a = 37, b = 8 then g cd (a,b) = ? 1-142: 0 1+ 24, - 3. 37 = 8×4 +5 : · n : 8 = 5×1 +3 1 . (3.01) 000 5 = 3×1 +2 3 = 2×1 +1 to the state of the control of 2 = 1x2 +0 2000 1 1000 - 1000 - 1000 1221 18 1. · (1,0) bop : gcd (a,b) =1 1. (1.1) 100 37 = 8×5 -3 ch ib.  $8 = 3 \times 3 - 1$ \*\* 3 = 4 ×3 -0 gcd (a, b) =1 it is called minimal remainder.

Lame's theorems. Let a>b, both positive and let n be the number of division in Euclidean's algorithm, for a and b, then n \( \) 5t, where tis the number of digits in b.

Ex:- If a = 13, b = 8, Here a>b and t=1

n=5, n=5t = 5×1 = 5

2 = 1x2 +0

\* Knonecken's theorem: M(a,b) < E(a,b)

Theo rum: The god is unique. ged (a, b) =di gcd (a,b) = d2

Theorem: Let a, az ... an be any nonther into egen's whose ged is d, then there exists integenment x1, x2, · · · xn such that, be to holler of 4 a121 + a222 + · · · + anxn = d

rain a security of the state of the

& 15 ged (252, 198) = 18 find Linean combination of 252 and 198? 252×12+198×2=18 and in him in him allowable

252×198×1+54 -0.

198 = 154 ×3 + 36 (-(i))

54 = 36×1 + 18 — (iii)

- : 36 = 18×2 +0 -(iv)
- (i) 54 = 252 198x1
- (U) 36 = 198 54×3
  - = 198 (252-198XI) X3
  - = 4×198-252×3
- (111) 18 = 54 -36x1
  - $= 54 (4 \times 198 252 \times 3)$
- = (252 198 ×1) (4×198 252×3)

and Profit

(x! - 1) 1 . x ... 10 10 10

- $= 252 \times 4 198 \times 5$   $\times 4 198 \times 5 10$
- : 252×4 198×5 = 18
- 1. x1=9, x2 = -5
- such that ged (a,b) = 1 and albe then alc.
- If p is a prime and play, az. . . an where ai
- is an integer then plai fort some i.
- Theorem: Let m be a ponitive integer and let a, b, and c be integers.
- if ac = bc (mod m) and ged (c,m) =1
  then a = b (mod m)

\* x = 2 (mod 3) ploy 1 1 10 10 10 100 2 1 10 x=2 (mod x) M= BX 5XX  $M_{1} = \frac{m}{mp} = \frac{105}{3} = 35$  $M_2 = 21$ ,  $M_3 = 15$ (men ham) 1' & = inverse of M, mod my (201 1200) 0 = " " 35 " 3 (mail ma) S= {0, 1,2} confirmation in allibour institute. 22' pian 35% mod 3=1 -> 35%=1 (mod 3) : 35x mod 3 = 1 mod 3 Jul - 61, 100  $\chi = 0$ ,  $35.0 = 0 \mod 3 = 0$ x=1 35:1 = 35 mod 3=2 P = (9100 ...) x = 2,  $352 = 70 \mod 3 = 1$ (am bomi) 1 2 i. y = 2 are of the mod me 82 = 1, y3 =1

x = a1 M14 # a2 M242 + a3M3 d3

=2×35×2+3×21×1 +2×15×1 =233

Scanned by CamScanner

Theorem: If a and m are relatively prime integer and m>1 then inverse of a mod m exist. [ V 117 T 1 2 2 2 ged (a,m) =1 ged (3.3) =1 The ahiness remainders theorem: Let mi, me...mn be pairwise prime positive integer and a, az. an antitriary integers. then the system.  $x = a_1 \pmod{m_1}$ proposed to proposed the  $x = a_2 \pmod{m_2}$ x = an (mod mn) modulo m, where m=m1m2.-mn has a unique solution 1 - 5 War x 35 m = mim2 . . . ma schools as boar & s. Mr = m ie  $M_1 = \frac{m}{m_1}$ ,  $M_2 = \frac{m}{m_0}$ 0.8120 - 100 - 1 0 - 4 11 - 11 - 1 - 1 - 1 - 1 - 1 gcd (MK, MK) =1 regularia and a control of a me MKYK = 1 (mod mK) inverse of Mr mod mr x = aM, y, + a2 M2 y2 + a3 M3 y2 + ... + an Mayn

600 = 1000 x = 1000 x + 1000 x + 1000 x = 1000 x

prioos: Given that, ac = bc (mod m)

m|ac-bc

m|c(a-b)

Here, gcd(e,m) = 1, and mle(a,b) = 50 ml(a-b) [Euclidin first theorem]by  $des^n a = b \pmod{m}$ 

a positive integers and a and b arre integers, and a is a variable, is called linear congruence.

> 3x = 4 (mod x) find x = 5

 $Solv: -3x = 4 \pmod{7}$ 

3x mod 7 = 4 mod 7

= 4 10 0 1 1

Herre, s = {0,1,2,3,4,5.6}

x=0, 3x = 0, 0 mod x = 0

X=1, 3.1 = 3, 3 mod \$ = 3

x = 6, 3.6 = 18,  $18 \mod 7 = 4$ 

: x = 6 (Aws;)

•

- :. x = 233 mod 105 = 23 (Amst) \* FERMET'S LITTLE THEOREM: - If p is a prime and a is an integer not divisible them;  $a^{p-1} = 1 \pmod{p}$
- 0 = 341,  $\alpha = 2$   $2^{340} = 1 \pmod{341}$ Let be be  $\alpha = 341$
- \* Let b be a positive integer if n is a composit positive number and band = 1 (mod n) bethernin called , preudopnime to the bone b.
- \* A composite integer that satisfies the congruen ce b^-1 = 1 (mod m) for all positive integer b with ged (b, n) = 1 is called carmichael number.
- Example: The integer 561 1's" a Carimichael number because 561 is composite 561 = 3.11.17

3:10000

- if ged (b, 561) = 1 then, ged (b, 3) =1
  - gcd (b,11) =1 ged (6, 17) = 1
- Now,  $b = 1 \pmod{3}$ ,  $b^{10} = 1 \pmod{3}$ ,  $b^{16} = 1 \pmod{3}$

if follows that, b 560 = (b) 280 = 1 (mod 11) b = (b16) 35 16 (mod 17) b<sup>560</sup> = 1 (mod 561) so that god (b,567) =1 so it Now. is an can michael number. \* public key and private key:-(1 br pcm) 1 = 020 a Energyption : c = (P+k) mod 26  $C = (A + 3) \mod 26$   $C = (A + 3) \mod 26$   $C = (A + 3) \mod 26$ =(1+3) mod 26, 1100 1.00 100 of samon > 3 THE = 4 and a willion the total (a boat) = 1-0 & o .: Q ='D' ... | (0.1) in below below in 1 : (0.1) in Decryption: p=(a-k) mod 26 =(4-3) mod 26 = 1 mod 26 1 - 11.13 6 00 = 1 1 . (1.1) in a D = A 1 = (x1 i) bug (Stram): " of (Mosell) by a lebrary

RSA algorithm:

- 1. Solect p.q.
- 2. n=pq
- $3 \cdot \varphi(0) = (p-1)(q-1)$ 
  - 4. select e, gcd  $(e, \varphi(n)) = 1$ 
    - Kp < 90)
- 5. Calculate de ≡ 1 (mod φ(n))
- 6. public key 2 p, ns
  - \* EX. 1. P= 17, Q=11
    - 2. n= 17×11
      - =187
      - 3. p(n) = 16 × 10 = 160
      - 4 e=7. ged (7, 160) =1
      - 5. d = 23 de =1 (mod 160)
        - d. x = 1 (mod 160)
    - 6. public key (7.187)

private key 223, 1875

- plain text 88 -> 88 mod 187 = 11
- " " 88 -> 11 23 mod 184 = 88