

ELEMENTERY NUMBER THEORY AND CRYPTOGRAPHY

DIVISIBILITY

If a and b are any two integers such that beto then we say what "b divides at it there wists an integer. I such that a= kb. And it is written as bla

Note

If "b divides a", then we say that "b is factor of a" or 'a is multiple of b".

DIVISION ALGORITHM

The and be are any two integers such that 6>0 then there exist unique integer q and x such that, a = bq + x

where q is called quotent.

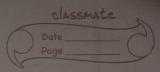
CONGRUENCE RELATION

Let m be a positive integer. Then an integer a is said to be unquient to an integer b' under modulo mit "m divides (a-b)". (m/(a-b)) symbolically it is written as a = b (mod m) or a = b (modulo m)

It is read a is congruent to b modulo m".

b is called remainder or residue of almost m)

OR b is remainder when m divides a



Properties of Congruence Relation 117 If a = 6 (mod m), bhem m (a-6) in I a = b (mod m) when b = a (mod m) (iii) Ib a=b(mod m) & b=c(mod m) then a=c(mod m) HODULAR ARITHEMATIC OFFRATION Ib a=b (mod m) phen bor K + O EZ ii) a+ K= b+K (mod m) 1997 a-K = b + K (mod m) (iii) a: k = b: k (mod m) (h+ d) = (3+0) (m) (iv) $a^{k} \equiv b^{k} \pmod{m}$ Properties of Modular Arithematic Residue system Modulo M Define the set Zm as a set of non-negative integers less than m, calded had and had an (sell + sel-se Zm = 10, 1, 2, 12-1-1 (m-1)3 It is called residue system modulo m. · Residue dasses Each introyer in 2m represents a residue doss and it is divided by [a] and defined by

[x] = fx: x = r (mod m) } For Example: (1) Residue system modulo 3 is 2/3 = 10,1,23 : Residue classes of elements of Z3 are (a) = $\{ \infty : \alpha \equiv 0 \pmod{3} \}$

classmate

Proposition of (onoquence - Relate let m be a positive integer and a=b (mod m) and c=d(mod) . Then prove that a+c = b+d (mod m). Then prove that a+ (= btd (mod m) and ac = bd (mod m)

Proof: Given a=b (mod m) and c=d (mod m) augus m/(ab) and im/(c-d). - () → m/(a-b)+(c-d) (m hom) path(d = b) + me(cod)

→ m/(a-b+c-d) (a boom) ph + (h=-ad-cb+bd)

> m /(a+c) - (b+d) (m hart) a > la+c = b+d (mod m) (m a∈m)

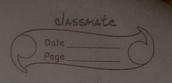
By @ we get Solomand Fra walnut to 25 rd regard a-b=Kim and c-d=Kim all modelies and c(a-b) = ckim and b(c-d) = b K2m ac-bc = (k16)m and bc-bd = (k2b)m ac-be +bc-bd = (kic) m + (Kb) m ac-bd = K'm+K"m where K!=K1C, K"=K20 ac-bd = (K'+K") m ac-bd = Km where KI = K1 + Kb & EZ

> m [(ac-bd) => ac = bd (mod m

PRIME NUMBER

An integer p = 2 is called prime number if it is divisible by 2 and itself. Otherwise a number & called composite number Ex: 1 Prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, (OHPOS) (omposite numbers are 4,6,8,9,10, ----

Note



Every composite number can be expressed as product of prime integers:

Ex: 010 = 2×5 (20 = 2×10 = 2×2×5 (35= 5×7

RELATIVELY PRIME NUMBER (CO-PRIME NUMBERS)

Two number a and b are said to be relatively prime if they have no common divisors other than 2.

(GCD (a, b) = 1)

Ex: 1) 10 and 21 are relatively prime as GCD (10,21)=1

GULER'S &- FUNCTION / EULER'S Tobient FUT

REDUCED RESIDUE SYSTEM HODULO M

The reduced residue system modulo m à the set of all elements from residue system modulo m. Zm=10,1,2...m-13 which are relatively prime to m.
i.e S = { >c : Cr(D (x, m) = 13

The Euler's & Function of an integer $n \ge 1$ is denoted by . $\beta(n)$ and defined by the number of non-zero positive integers less than n. that are relatively prime

 $E \times : (0) = 0$, $\phi(2) = n((1,2)) = 1$, $\phi(3) = n((1,2)) = 2$ $\phi(4) = n((1,3)) = 2$, $\phi(5) = n((1,2,3,4)) = 4$ $\phi(6) = n((1,3)) = 2$, $\phi(7) = 6$

Note

1 It n=p is a prime number then Fuler & function of

2 If n is number that can be expressed as the a product of recleability. prisme number (a, b) Euler's of function of n

Ex:-0. \$ (20) = \$ (4.5) = \$(4). \$ (5) = 2 × 4 = 8 6 \$ [35] = \$ (5.7) = \$\phi(5) \cdot \phi(7) = 4x6=24 3 Ø (10) = Ø (2.5) = Ø 6) · Ø(5) = 1 x 4 = 4

Euler's Theorem . IMM9-00) 939HUM 3MJ99 YJ3VITAJ3 Statement: Let n'and a be positive integer which are relatively prime (GCD (n,a)=1). Then where Q(n) - Q fuller Q - Function

Proof: 1 Jasiet Sasius | MOITOMUT - 6 2 93108 Given that na 1 Z such that GCD (na) =10 Euler &- function of Dis

Consider a reduced system modulo n

5= {a, ,a2, 93, 10 a och } - 6 = 513100

Take a to E Z such that GCD(n,a)=1 a 5= { aa, aa, aa, aa, aa, }

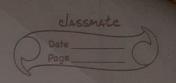
aq = a, (mod n); aq = q2 (mod n) ... aq x = a, c(mods)

Nech we Know bhat

aa: : aa2 · aa3 · aak = q · a2 · a; - ... are (mod n)

ak (a, a, a, a, , ... a, e) = (a, a, a, a, a, e) (mode

> ak = 1 (mod n)



$$\Rightarrow \left[a^{\otimes(n)} = i \pmod{n} \right]$$

FERMAT'S THEOREM / FERMAT'S UTTLE THEOREM

Stratement let P be a prime number and P / a . When

ap-1 = 1 (mod P)

or a P = a (mod P)

Given bhat, P is a prume number and P Xa

GCD (P, a) = 1

Euler & - function of prime no & is.

Q(P)=P-1

Consider a residue system modello P. 5 = {a, a2, 93...ap-1}

Take a \(\frac{1}{2}\) \(\int Z\) such that P\(\text{a}\) \(\lambda\) \(\lambd

aa, =a, (mod p); aa2 = a2 (mod p) aap = ap (mod p)

Next we know bhat aa, aa2-aa2----aap-1 = a, a2-a2--- ap-1 (mod p)

⇒ ap-1 (a, ·a, ·a, · · · · ap-1) = (a, ·a, · a, · · · ap-1) (mode

=> ap-1 = 1 (mod P)

⇒ a = a (mod p)

For example $4^{(7)} = 1 \pmod{7}$. $4^{(7)} = 6$ $4^{(7)} =$

(2) $-5\%(6) = 1 \pmod{6}$ $\emptyset(6) = n (\{1,3\}) = 2$ $5^2 = 1 \pmod{6}$

CHINESE REHAINDER THEOREM.

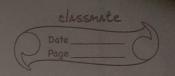
Statement: If m, m2 m3 - . . . mx are pairwise relative, prume numbers and $a_1a_2a_3$ a_{x} are any integrations; then; the simultaneous congrerus relations, $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$

 $x \equiv 0_3 \pmod{m_3}$

has a unique solution under modulo M,
where $M = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_1 \times 1000$

CHINESE THEOREM.

Step 2: (heck G(D (m_1^2, m_1^2) = 1 : for $i \neq j^2$ Step 2: $g = (M_1 \times_1 a_1 + M_2 \times_2 a_2 + \dots + M_K \times_K a_K)$ (mod H) where $M = M_1, M_2, \dots, M_K$ and $M_i^2 = M_1 = M_1, M_2, \dots, M_{i-1}^2 + M_{i+1}^2 + \dots + M_K$



Next, bo calculate xi°. Xi° is a multiplicative inverse of Hi under modulo mi i.e. Mixi = 1 (mod mi)

skp3: Using values of Mi and Xi in 1) we can find the

Examples

1) solve the following system of congruences by using. Thinese remainder bheorem.

 $x = 2 \pmod{3}$, $x = 1 \pmod{4}$, $x = 3 \pmod{5}$

(+ bom) = = (2 bom) 5 = = (8 bom) 6 = E

given,

 $x \equiv 2 \pmod{3}$

SC=1 (mod 4)

 $x = 3 \pmod{5}$.

 $\alpha_1 = 2, \alpha_2 = 1, \alpha_3 = 3$

m1=3 m2=5 m8=5

: 3,4,5 are pair wise relatively prime

Next, oc= (M, x, a, + M, x, a, + M, x, a, a) (mod m) -().
Where H=m, m, m, = 3.4.5=60

H=60.

 $M_1 = M = m_2 m_3 = 4.5 = 20$

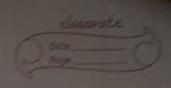
 $M_2 = M = m_1 m_3 = 3.5 = 15$

 $M_3 = M = m_1 m_3 = 3.4 = 12$

Checurate.

	Colculate X?
	MX = 1 (mod mi)
	H. X. = 1 (mod m) Hax= 1 (mod ma) Hax3= 1 (md)
-	8 25 x = ((mod 3-) 15 x2 = 1 (mod 3) 12 x3 = 1 (mod 3)
2 20	= 2x = (mod 2) 3x= (mod 4) 2x3=1 (mod)
@	: X1 = 2 as 3/2(2)-1 X2=3 as 4/331 X3=3 as 5/2
4	2. Rédation (1) becomes
	2 = (20-2-2 + 16-3-1 + 12-3-3) (mod 60)
237	'x = 100 + 45 + 108 mod 60 mod 60
2	2 = 233 (mod 60) - mi 12 m , (8 bom) 2 = 35
60 233	x = 53 (mod 60)
180	(E Dom) 5' = 36
	DC=53 (1 bom) 1 = 2
	(3 Joon) & Te
(2)) $z = 2 \pmod{3}$, $z = 3 \pmod{5}$, $z = 2 \pmod{7}$
-	
	m,=3 m=5 m=7 2 = 100 2 = 100
	G(D(3,5) = GCD(5,7) = GCD(3,7)= 1,000
	13,5,7 are pair wise relative prime.
	13,3,1 sat past postive pagine.
1	Neith (and (an x all) - 0 , m, m , 0, 30, 14) = 30 (disco)
	DC = (M, X, Q, + M2 X2 Q2 + M3 X3 Q3) (mod M) - ()
	wher M = m, m2 m3 = 3.5.7 = 105
	M = 105
	N - M - F 7 - 25
	$M_1 = \frac{M}{m_1} = 5.7 = 35$
	SERVE ADMINISTRATION OF MICHAEL MICHAE
	M2 = M = 3.7 = '21

M3 = M = 3.5 = 15



(alculate X;

$$M_1X_1 = 1 \pmod{m_1}$$
 $M_2X_2 = 1 \pmod{m_2}$ $M_3X_3 = 1 \pmod{m_2}$
 $35X_1 = 1 \pmod{3}$ $21X_2 = 1 \pmod{5}$ $15X_3 = 1 \pmod{7}$
 $2X_1 = 1 \pmod{3}$ $1X_2 = 1 \pmod{5}$ $1X_3 = 1 \pmod{3}$
 $X_1 = 2$ $3(2|2)-1$ $X_2 = 1$ $5(10)-1$ $X_3 = 1$ $7(1(1)-1)$

: Relation O becomes

$$= G(D(3, 4 \pmod{3}))$$

= $G(D(3, 1)$

	Date Page
**1	in to
(n)	\$2,52 G(D(52, 252) = G(D(52, 252 (mod52))
	G(D(52, 252) = G(D(52, 252)) $= G(D(52, 45))$
(m b-4	11 co (mod 55)
5 1	= G(D(44,8)) (Elementer)
4-0010	= GCD (8, 44 (mod 8))
	21- A \
	= G(D(4, # 8(mod4)) 1) naplated.
	2 G(D (4, 14 a (100 th)) 2 2 G(D + 4 a (100 th)) 0 2 4 8 1 th 0 2 1 5 3 c
	(20) bond EES = 30
<u>(üi)</u>	1201 Jam 1 25 7 Ja
	82 7 23
-	
4	GREATEST COMMON DIVISION BETWEEN THE PUBLIC
	National
	Find Gen between following pair of integer
	TE 001 (1)
	((celomo oot (2) and = (oo) se) and =
	(actor ma) =
	((achord 52 ac) 030 =
	(0,30) 0000
#	((a boot) again or its
1	(4.10.11.5-
4	Lichamis W. A.D. on 118
1	(E.J.) (1) 1) = (E.J.) (1) 1)
	(181000
	(Charles Marie