

Bharathidasan University

Tiruchirappalli - 620 024 Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title: Theory of Numbers

COurse Code: 21M04CC

Chinese Remainder Theorem

Dr. V. Piramanantham Professor

Department of Mathematics

Let fix) be the polynomial with integral coefficient Theorem Let m=n, mz, where m, 4 mz are relatively primes. If N(m) denotes the no. of solution of fcx) = 0 (mod m), then $N(m) = N(m_1) N(m_2)$

Proof Let $\mathcal{E}(M) = \{1, 2, ..., m\}$. Then $\mathcal{E}(M)$ is a complete residue system (mod m).

N(m) is the number of solutions of $f(x) \equiv 0 \pmod{m}$ in f(m).

Let $A = \{ a + \mathcal{E}(m) \mid f(n) = 0 \pmod{m} \}$

$$A_i = \{a_i \in G(m_i) \mid f(a_i) = 0 \pmod{m_i}\}$$
 $i = 1, 2$

So |A|=N(m), |A, |=N(m,) & |A2|=N(m2)

To prove the result it is enough to

A ~ A(XA2,

Let $a \in A$. Then $f(a) = o \pmod{m}$ since mi m i=1,29 $f(\alpha) \equiv 0 \pmod{m_i}$ Since E(mi) is a complete residue system (mod mi) Flait & (mi) & a = ai (mod mi) =) f(ai) = 0 (mod mi) a; EAi, i=1,2

Thus for each a = A, there corresponds (a_1, a_2) in $A_1 \times A_2$. a unique pair Suppose that (a, a2) & A, ×A2. Then $f(a_i) \equiv 0 \pmod{m_i}$ $f(a_2) \equiv o \pmod{m_2}$ $(m_1, m_2)=1.$ $\begin{cases} x = a_1(m_0)m_1 \\ x = a_2(m_0)m_1 \end{cases}$ Given Mat Chinose remainder c. PCm) euch that

$$a \equiv a_i \pmod{m_i}, i \equiv 1,2$$
.

$$\frac{1}{2}$$
 $f(a) = 0 \pmod{m}$

We have established a one-one correspondence between A and A, XA2

$$N(M) = N(M_1)N(M_2)$$

Note:
$$f(x) \equiv O(mod m) - O$$
 $M = M_1 M_2$, $(M_1, M_2) \equiv 1$; $L M_1 L M$
 $L M_2 \leq M$
 $L M_2$

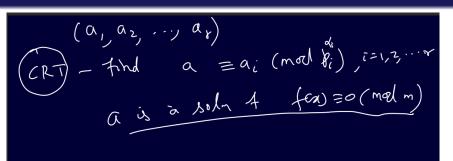
Apply the Chinese remainder theorem on
$$x = b_i \pmod{m_i} - 2$$

we find a salution $a_{ij} \pmod{m}$

Salvidaying $n = rs$.

《口》《圖》《意》《意》

canonical M= p, p2--- p, 2 Note: factorization (\dot{z}_{i}) (\dot{z}_{i}) (\dot{z}_{i}) (\dot{z}_{i}) As a generalization of the previous theorem $N(m) = N(\beta^{1})N(\beta^{2}) \cdots N(\beta^{r})$ f(x)=0(mol b; (f(x)=0 (mod aj is a solution A [=1, 2, -- Y,



Polynomial congruence with prime power modulii

Solve the congrence

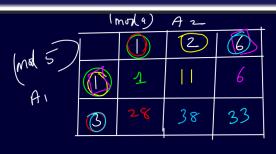
$$x^3 + 2x - 3 = 0 \pmod{4.5}$$

has the solutions I and 3

has the solutions 1,2,6,

$$A_1 = \{1, 3\}$$

$$A_2 = \{1, 2, 6\}$$



$$|A_1 \times A_2| = 6$$

$$11^{3} + 2 \cdot 11 - 3 \equiv 0 \pmod{45}$$

$$|1^{3}+2\cdot 1|-3=|2\cdot 1|+22-3$$

= $3|\cdot 1|+|9$

$$\begin{cases} 2 \equiv 1 \pmod{5} \\ 2 = 1 \pmod{9} \\ 1 \in RT \end{cases}$$

$$\int_{a} z | (mod 5)$$

$$\int_{a} z = g (mod 9)$$

$$+ 5.2.2$$
 $= 36 + 20$

$$= 31.11+19$$

$$= 36+20$$

$$= 36+20$$

$$= 36+20$$

$$= 56 \text{ (mod 45)}$$

$$= 0 \text{ (mod 45)}$$

$$= 0 \text{ (mod 45)}$$

$$= 0 \text{ (mod 5)}$$

$$= 6 \text{ (mod 9)}$$

$$= 9.4.1 + 5.2.6$$

$$= 36+60=96 \text{ (mod 45)}$$

) 9 (3

$$(RT) \quad x = 3 \pmod{5} \quad n = 1 \pmod{9}$$

$$7_0 = 9 \cdot 4 \cdot 3 + 5 \cdot 2 \cdot 1$$

$$= 36 \cdot 3 + 10$$

$$= 108 + 10 = 118 = 28 \pmod{45}$$

CRT
$$x = 3 \pmod{5}$$
 $x = 2 \pmod{9}$
 $x_6 = 9.4 \cdot 3 + 5.2 \cdot 2$
 $= 108 + 20 = 128$
 $= 38 \pmod{45}$

CRT
$$x = 3 \pmod{5}$$
 $x = 6 \pmod{9}$
 $x_0 = 9.4.3 + 5.2.6$
 $= 108 + 60 = 168$
 $= 33 \pmod{45}$

The solutions of $x^3 + 2x - 3 = 0 \pmod{45}$

one 1, 6, 11, 28, 32, 38.

EXERCISE:

$$x^{3} + 4x + 8 = 0 \pmod{15}$$

$$\frac{\text{method}: \quad \chi^3 + 4 \times + 8 = 0 \pmod{3}}{\pmod{5}}$$

$$\frac{CRT}{R} \qquad x = a_1 \pmod{3} \qquad x = a_2 \pmod{5}$$

$$x_{0} = \frac{m}{m}, b_{1} = \frac{m}{m_{2}} b_{2} = \frac{q_{2}}{m_{1}}$$

$$= 5. 2 \alpha_{1} + 3.6 \alpha_{2}$$

$$5.5 = 10\alpha_{1} + 18\alpha_{2}$$

$$3.2 = 10\alpha_{1} + 18\alpha_{2}$$

$$2 = 10\alpha_{1} + 18\alpha_{2}$$

