IS Practical 1

classmate
Date
Page

Chinese Remainder Theorem

→ solve congruent equation (set of) with one variable but different modulus which are relatively prime.

Congruent eq^n -

$a \equiv b \pmod{m}$

a & b are congruent modulo m if they have same remainder by m

BDA - 1, 2, 3
IS - ~~1~~, 2, 3

one variable

$$\left\{\begin{array}{l} x \equiv a1 \pmod{m1} \\ x \equiv a2 \pmod{m2} \\ x = a3 \pmod{m3} \end{array}\right\} \text{diff moduli}$$

till k.

above eq^n

→ have unique solution if moduli are relatively prime

$\boxed{\text{relatively prime} = \text{no common factors except } \pm 1}$

Steps

Step 1 – find M → common modulo

$M = m1 \times m2 \times m3 \ldots mk$

Step 2

$M1 = \frac{M}{m1}$ $M2 = \frac{M}{m2} \ldots$

Step 3 find multiplicative inverses of $M1, M2 \ldots$

Multiplicative inverse

$5 \times 5^{-1} = 1$

$\left(\frac{1}{5}\right)$

$A \times \frac{1}{A} = 1$

A^{-1}

Under mod n

$A \times A^{-1} \equiv 1 \mod n$

$3 \times ? \equiv 1 \mod 5$

when this is divided by 5 we should get 1 as remainder

$12 \equiv k \bmod 11.$

$6 \equiv 1 \bmod 5.$

$5 \overline{)\,6\,}$ 1
5
1

Step 4 Put values in eqⁿ

$$X = (a1 \times M \times M1^{-1} + a2 \times M2 \times M2^{-1}) \bmod M.$$

<u>Example</u>

$$X = 4 \bmod 5$$
$$X = 6 \bmod 8$$
$$X = 8 \bmod 9$$

1) <u>M</u> $5 \times 9 \times 9$
$= \underline{360}$

2) $M1 = \frac{M}{m1} = \frac{360}{5} = 72$

$M2 = \frac{360}{8} = 45$

$M3 = \underline{40}$

$$\boxed{\begin{aligned} s &= s_1 - q s_2 \\ t &= t_1 - q t_2 \end{aligned}}$$

Initial default values

GCD (161, 28).

$\underbrace{\text{Euclidean}}$ method

q	a	b	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	
	GDD			S			t		

$$s \cdot x a + t \times b = \gcd(a, b)$$

$$\boxed{(-1)(161) + 6(28) = 7}$$

$1 - 5(0)$

$0 - 1(1)$

-1

IS Practical 3

RSA Algorithm

1) two prime nos $p = 17$ & $q = 11$

2) $n = pq = 187$

3) $\phi(n) = (p-1)(q-1) = 160$

4) Select e such that relatively prime to $\phi(n)$ & less than $\phi(n)$

$\gcd(\phi n, e) = 1$ $e = 7$. ~~$\gcd(\phi n, e)$~~ ~~$\phi(n)$~~

5) ~~d such that $d\,e \equiv 1 \pmod{160}$~~

~~$d < 160$~~ ~~$\phi(n)$~~ ~~by EEA~~

~~$d = 23$.~~

EEA

$\gcd(\phi(n), e)$.

q r1 r2 r t1 t2 t

classmate

Date

Page

6) En^n

$C = M^e \bmod n$

7) De^n

$M = C^d \bmod n$.