Foundation of Cryptography

Session 19

Date: 16 March 2021

Dr. V. K. Pachghare

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Chinese Remainder Theorem

1. Problem first express as a system of congruences

$$p \equiv b_i \pmod{n_i}$$

where n_i are relatively prime numbers: n_1, n_2, n_3 and so on

b_i is the respective remainder for modulo n_i such that b_1 for n_1, b_2 for n_2 and so on.

p is the value of solution.

2. Calculate the value of N $\quad N = n_1 * n_2 * \ldots * n_i$
3. Calculate the value of $N_i = N/n_i$ such that $N_1 = N/n_1$, $N_2 = N/n_2$ and so on
4. Calculate the multiplicative inverse for $y_i \equiv (N_i)^{-1} \pmod{n_i}$

   Where y_i is the multiplicative inverse of N_i mod n_i.
5. The value of p is calculated as

$$p \equiv (b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r) \bmod N$$

where p is the solution of the problem.

Find the smallest multiple of 10 which has remainder 1 when divided by 3, remainder 6 when divided by 7 and remainder 6 when divided by 11.

The factors of 10 are: 2 and 5.

Problem is now expressed as a system of congruences as below:

$p \equiv b_i \pmod{n_i}$

where $n = 2, 3, 5, 7$, and 11 which are relatively prime and $b = 0, 1, 0, 6$ and 6 are the remainders for respective value of n.

$p = 0 \bmod 2$,

$p = 1 \bmod 3$,

$p = 0 \bmod 5$,

$p = 6 \bmod 7$

$P = 6 \bmod 11$

To solve for p we first calculate the value of N as

$N = n_1 * n_2 * \ldots * n_r$

$N = 2 * 3 * 5 * 7 * 11$

$= \mathbf{2310}$

and find the value of $N_i = N/n_i$ as below:

~~$N_2 = 2310/2 = 1155;$~~

$N_3 = 2310/3 = 770;$

~~$N_5 = 2310/5 = 462;$~~

$N_7 = 2310/7 = 330;$

$N_{11} = 2310/11 = 210$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

~~$y_2 = (1155)^{-1} \pmod{2} = 1$~~

$y_3 = (770)^{-1} \pmod{3} = 2$

~~$y_5 = (462)^{-1} \pmod{5} = 3$~~

$y_7 = (330)^{-1} \pmod{7} = 1$

$y_{11} = (210)^{-1} \pmod{11} = 1$

The solution for above problem is:

$$p \equiv b_1N_1y_1 + b_2N_2y_2 + \dots + b_rN_ry_r \pmod N,$$

$$p = 0(N_2 * y_2) + 2(N_3 * y_3) + 0(N_5 * y_5) + 6(N_7 * y_7) + 6(N_{11} * y_{11})$$

$$= \cancel{0(1155)(1)} + 1(770)(2) + \cancel{0(462)(3)} + 6(330)(1) + 6(210)(1)$$

$$= 0 + 1540 + 0 + 1980 + 1260$$

$$= 4780 \bmod 2310$$

$$= 160.$$

What is the smallest natural number p with the properties

$p = 1 \bmod 3$

$p = 3 \bmod 8$

$p = 2 \bmod 5$?

$p = 1 \bmod 3$

$p = 3 \bmod 8$

$p = 2 \bmod 5$

Here $n_1 = 3$,

$n_2 = 8$ and

$n_3 = 5$

$p = 1 \bmod 3$

$p = 3 \bmod 8$

$p = 2 \bmod 5$

Here

$\mathbf{n_1 = 3,}$	$\mathbf{b_1 = 1,}$
$\mathbf{n_2 = 8}$	$\mathbf{b_2 = 3}$
$\mathbf{n_3 = 5}$	$\mathbf{b_3 = 2}$

p = 1 mod 3

p = 3 mod 8

p = 2 mod 5

Here $n_1 = 3$, $n_2 = 8$ and $n_3 = 5$

$b_1 = 1$, $b_2 = 3$ and $b_3 = 2$

$$N = n_1 * n_2 * n_3$$

$$= 3 \times 8 \times 5$$

$$= 120$$

$p = 1 \bmod 3$
$p = 3 \bmod 8$
$p = 2 \bmod 5$

Here $n_1 = 3$, $n_2 = 8$ and $n_3 = 5$

$b_1 = 1$, $b_2 = 3$ and $b_3 = 2$

N = 120

The value of $N_i = N/n_i$

$N_1 = 120/3 = 40$;

$N_2 = 120/8 = 15$;

$N_3 = 120/5 = 24$

Now find out the multiplicative inverse as below:

$$y_i \equiv (N_i)^{-1} \pmod{n_i}$$

$N_1 = 40;$ $N_2 = 15;$ $N_3 = 24$

$y_1 = (40)^{-1} \pmod 3 = (40 \times 1) \bmod 3 = 1$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$N_1 = 40$; $N_2 = 15$; $N_3 = 24$

$y_1 = (40)^{-1} \pmod 3 = (40 \times 1) \bmod 3 = 1$

$y_2 = (15)^{-1} \pmod 8 = (15 \times 7) \bmod 8 = 7$

Now find out the multiplicative inverse as below:

$\mathbf{y_i \equiv (N_i)^{-1} \pmod{n_i}}$

$N_1 = 40;$ $N_2 = 15;$ $N_3 = 24$

$y_1 = (40)^{-1} \pmod{3} = (40 \times 1) \bmod 3 = 1$

$y_2 = (15)^{-1} \pmod{8} = (15 \times 7) \bmod 8 = 7$

$y_3 = (24)^{-1} \pmod{5} = (24 \times 4) \bmod 5 = 4$

The solution for above problem is:

$$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$$

$b_1 = 1$, $b_2 = 3$ $b_3 = 2$

$N_1 = 40$, $N_2 = 15$, $N_3 = 24$

$y_1 = 1$, $y_2 = 7$, $y_3 = 4$ and $N = 120$

The solution for above problem is:

$$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$$

$b_1 = 1$, $b_2 = 3$ $b_3 = 2$

$N_1 = 40$, $N_2 = 15$, $N_3=24$

$y_1 = 1$, $y_2 = 7$, $y_3 = 4$ and $N = 120$

$$= [1(40)(1) + 3(15)(7) + 2(24)(4)] \bmod 120$$

The solution for above problem is:

$$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$$

$b_1 = 1$, $b_2 = 3$ $b_3 = 2$
$N_1 = 40$, $N_2 = 15$, $N_3=24$
$y_1 = 1$, $y_2 = 7$, $y_3 = 4$ and $N = 120$

$$= [1(40)(1) + 3(15)(7) + 2(24)(4)] \bmod 120$$
$$= [40 + 315 + 19] \bmod 120$$

The solution for above problem is:

$$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$$

$b_1 = 1$, $b_2 = 3$ $b_3 = 2$

$N_1 = 40$, $N_2 = 15$, $N_3=24$

$y_1 = 1$, $y_2 = 7$, $y_3 = 4$ **and** $N = 120$

$$= [1(40)(1) + 3(15)(7) + 2(24)(4)] \bmod 120$$

$$= [40 + 315 + 19] \bmod 120$$

$$= 547 \bmod 120$$

The solution for above problem is:

$$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$$

$b_1 = 1$, $b_2 = 3$ $b_3 = 2$
$N_1 = 40$, $N_2 = 15$, $N_3=24$
$y_1 = 1$, $y_2 = 7$, $y_3 = 4$ and $N = 120$

$$= [1(40)(1) + 3(15)(7) + 2(24)(4)] \bmod 120$$
$$= [40 + 315 + 192] \bmod 120$$
$$= 547 \bmod 120$$
$$= 67$$

So the solution is 67

Find a solution using Chinese remainder theorem to $13p = 1 \pmod{70}$

$70 = 2 \times 5 \times 7$

$13b_1 = 1 \bmod 2$ >> $13b_1 \bmod 2 = 1$ (multiplicative inverse)
$13b_2 = 1 \bmod 5$
$13b_3 = 1 \bmod 7$

Obtaining $b_1 = 1$, $b_2 = 2$, and $b_3 = 6$. Now solve
$p = 1 \pmod{2}$
$p = 2 \pmod{5}$
$p = 6 \pmod{7}$

Here $n_1 = 2, n_2= 5 , n_3 = 7$

$b_1 = 1, b_2= 2, b_3 = 6$

$N = n_1 * n_2 * n_3 * n_4$

$= 2x\ 5\ x\ 7$

$= 70$

and find the value of $N_i = N/n_i$ as below:

$N_1 = 70/2 = \mathbf{35}$

$N_2 = 70/5 = \mathbf{14}$

$N_3 = 70/7 = \mathbf{10}$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_1 = (35)^{-1} \pmod 2 \quad = 1$

$y_2 = (14)^{-1} \pmod 5 \quad = -1$

$y_3 = (10)^{-1} \pmod 7 \quad = 5$

The solution for above problem is:

$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$

$b_1 = 1,\quad b_2 = 2,\quad b_3 = 6$

$N_1 = 35,\quad N_2 = 14,\quad N_3 = 10$

$y_1 = 1,\quad y_2 = -1,\quad y_3 = 5 \quad$ and $N = 70$

$= 1(35)(1) + 2(14)(-1) + 6(10)(5) \bmod 70$

$= 35 - 28 + 300$

$= 307 \bmod 70$

$= 27 \bmod 70$

So the solution is 27