CRT and Basic Number Theory - 1 (Solve a, b, c)
Chinese Remainder Theorem

1. Solve each of the following sets of simultaneous congruences:

(a) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

(b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$

(c) $x \equiv 5 \pmod 6$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

Ans:

(a) System: $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

Total modulus $N = 3 \cdot 5 \cdot 7 = 105$

for each congruence $\equiv a_i \pmod{n_i}$ compute $N_i = N/n_i$ and the inverse y_i of N_i modulo n_i.

↳ $n_1 = 3$, $a_1 = 1$; $N_1 = 105/3 = 35$

$35 \equiv 2 \pmod 3$. Solve $2y_1 \equiv 1 \pmod 3 \Rightarrow y_1 \equiv 2$

Contribution ; $a_1 N_1 y_1 = 1 \cdot 35 \cdot 2 = 70$.

↳ $n_2 = 5$, $a_2 = 2$; $N_2 = 105/5 = 21$.

$21 \equiv 1 \pmod 5$, so $y_2 \equiv 1$.

Contribution : $2 \cdot 21 \cdot 1 = 42$.

↳ $n_3 = 7$, $a_3 = 3$; $N_3 = 105/7 = 15$

$15 \equiv 1 \pmod 7$. so $y_3 \equiv 1$.

Contribution ; $3 \cdot 15 \cdot 1 = 45$.

Sum: $70+42+45=157$. Reduce modulo 105: $157 \equiv 157-105=52$.

$\therefore x \equiv 52 \pmod{105}$

$\therefore$ 52 mod 3 = 1, 52 mod 5 = 2, 52 mod 7 = 3.

(b) System: $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$.

$N = 11 \cdot 29 \cdot 31 = 9889$

$\hookrightarrow n_1 = 11$, $a_1 = 5$: $N_1 = 9889/11 = 899$.

$899 \equiv 8 \pmod{11}$. Solved $8y_1 \equiv 1 \pmod{11}$

$\hookrightarrow y_1 \equiv 7$ (since $8 \cdot 7 = 56 \equiv 1$).

contribution: $5 \cdot 899 \cdot 7 = 5 \cdot 6293 = 31465$.

$\hookrightarrow n_2 = 29$, $a_2 = 14$: $N_2 = 9889/29 = 341$.

$341 \equiv 22 \pmod{29}$. Solve $22y_2 \equiv 1 \pmod{29}$

$\rightarrow y_2 \equiv 4$ (since $22 \cdot 4 = 88 \equiv 1$).

contribution: $14 \cdot 341 \cdot 4 = 14 \cdot 1364 = 19096$.

$\hookrightarrow n_3 = 31$, $a_3 = 15$: $N_3 = 9889/31 = 319$.

$319 \equiv 9 \pmod{31}$. Solve $9y_3 \equiv 1 \pmod{31}$

$\rightarrow y_3 \equiv 7$ (since $9 \cdot 7 = 63 \equiv 1$).

contribution: $15 \cdot 319 \cdot 7 = 15 \cdot 2233 = 33495$

Sum: $31965 + 19096 + 33495 = 84056$. Reduce modulo 9889: $9889 \cdot 8 = 79112$, $84056 - 79112$
$= \cancel{45}\,4944$

$\therefore x \equiv 4944 \pmod{9889}$

$\therefore 4944 \bmod 11 = 5$, $4944 \bmod 29 = 14$,
$4944 \bmod 31 = 15$.

(c) System: $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$.
$N = 6 \cdot 11 \cdot 17 = 1122$.

↳ $n_1 = 6$, $a_1 = 5$: $N_1 = 1122/6 = 187$.
$187 \equiv 1 \pmod{6} \rightarrow y = 1$.
contribution: $5 \cdot 187 \cdot 1 = 935$.

↳ $n_2 = 11$, $a_2 = 4$: $N_2 = 1122/11 = 102$.
$102 \equiv 3 \pmod{11}$. Solve $3y_2 \equiv 1 \pmod{11} \rightarrow y_2 \equiv 4$
Contribution: $4 \cdot 102 \cdot 4 = 4 \cdot 408 = 1632$.

↳ $n_3 = 17$, $a_3 = 3$: $N_3 = 1122/17 = 66$.
$66 \equiv 15 \pmod{17}$. Solve $15y_3 \equiv 1 \pmod{17}$.
Note $15 \equiv -2$, so, $-2y_3 \equiv 1 \rightarrow 2y_3 \equiv 16 \rightarrow y_3 \equiv 8$.
contribution: $3 \cdot 66 \cdot 8 = 3 \cdot 528 = 1584$.

Sum: $935 + 1632 + 1584 = 4151$! Reduce modulo 1122: $1122 \cdot 3 = 3366$, $4151 - 3366$
$= 785$.

$$x = 785 \pmod{1122}$$

$\therefore$ $785 \bmod 6 = 5$, $785 \bmod 11 = 4$,
$785 \bmod 17 = 3$.