$C_1 a_n + C_2 a_{n-1} + C_3 a_{n-2} = f(n)$

Given $a_n^{(P)}$ = form of $f(n)$ (some)

Substitute and solve for coefficients in $a_n^{(P)}$

$$\boxed{a_n = A a_n^{(H)} + a_n^{(P)}}$$

11/10/23

Chinese Remainder Theorem

Solve

$n \equiv a_1 \pmod{n_1}$

$n \equiv a_2 \pmod{n_2}$

$\vdots$

$n \equiv a_k \pmod{n_k}$

$GCD(n_i, n_j) = 1,\ i \neq j$ (Mutually pairwise coprime)

Ex Solve for n

$n \equiv 2 \pmod 3$ | $n \equiv 0 \pmod 3$

$n \equiv 3 \pmod 5$ | $n \equiv 0 \pmod 5$

$n \equiv 4 \pmod 7$ | $n \equiv 0 \pmod 7$

$n = 70 + 105m$

$n \equiv 1 \pmod 3$

$n \equiv 0 \pmod 5$

$n \equiv 0 \pmod 7$

$n = 105m + 70$

$x \equiv 0 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 0 \pmod 7$
$21 + 105m$

$x \equiv 0 \pmod 3$
$x \equiv 0 \pmod 5$
$x \equiv 1 \pmod 7$
$15 + 105m$

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod 7$
$2 \times 70 + 3 \times 21 + 4 \times 15 + 105m$
$= \boxed{53} + 105m$

$x \equiv 0 \pmod{n_1}$
$\vdots$
$x \equiv 0 \pmod{n_k}$

$x = \left(\prod_{i=1}^{k} n_i\right) = P$

$x \equiv 1 \pmod{n_1}$
$x \equiv 0 \pmod{n_2}$
$\vdots$
$x \equiv 0 \pmod{n_k}$

$x = \left(\prod_{i=2}^{k} n_i\right) \cdot m$

$x = \frac{P}{n_i}\left[\left(\frac{P}{n_1}\right)^{-1} \pmod{n_1}\right]$

$a^{-1} \pmod n = b = (X \bmod n)$
$ab \equiv 1 \pmod n$
$\gcd(a, n) = 1$
$ax + Yn = 1 \pmod n$
$ax \equiv 1 \pmod n$

$x \equiv 0 \pmod{n_1}$
$x \equiv 1 \pmod{n_2}$
$x \equiv 0 \pmod{n_3}$
$\vdots$
$x \equiv 0 \pmod{n_k}$

$$x \equiv \frac{P}{n_2}\left[\left(\frac{P}{n_2}\right)^{-1} \pmod{n_2}\right]$$

$x \equiv 0 \pmod{n_1}$
$x \equiv 1 \pmod{n_i}$
$\vdots$
$x \equiv 0 \pmod{n_k}$

$$x \equiv \frac{P}{n_i}\left[\left(\frac{P}{n_i}\right)^{-1} \pmod{n_i}\right]$$

There's a unique $0 \le x < \prod_{i=1}^{k} n_k$
namely:

$$x = \left(\sum_{i=1}^{k} a_i \frac{P}{n_i}\left[\left(\frac{P}{n_i}\right)^{-1} \pmod{n_i}\right]\right) \bmod P$$

$g(a,b) = 1 \quad aX + bY = 1$
How to find X?
$g(a,b) = g(b, a \bmod b)$
$a \ge b$

GCD (a,b)
if $b == 0$ return a
else return GCD$(b, a \% b)$

GCD$(91, 56)$
↓
GCD$(56, 35)$

$91x + 56y = 1$

$91 = 56 \cdot 1 + 35$

$91(1) + 56(-1) = 35$

$56 = 35 \times 1 + 21$

$56 \times 1 = (1, -1)\,1 + 21$

$\leftarrow (-1, 2) = 21$

$[91 \times -1 + 56 \times 2]\ 35 = 21 \times 1 + 14$

$(1, -1) = (-1, 2) \times 1 + 14$

$(2, -3) = 14$

$21 = 14 \times 1 + 7$

$(-1, 2) = (2, -3) + 7$

$7 = (-3, 5)$

$14 = 2 \times 7 + 0$

$\downarrow$

GCD(35, 21)

$\downarrow$

GCD(21, 14)

$\downarrow$

GCD(14, 7)

$\downarrow$

GCD(7, 0)

$hcd(91, 56) = 7$

$ax + by = 7$

$-3 \times 91 + 5 \times 56 = 7$

Solve

$x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x = 1(15)(15^{-1} \bmod 2) + 2(10)(10^{-1} \bmod 3) + 3(6)(6^{-1} \bmod 5) \bmod 30$

$= [15 + 20 + 18] \bmod 30$

$= [23]$

32

Solve

$x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 4 \pmod 7$

$x \equiv 23 \pmod{30}$

$x \equiv 4 \pmod 7$

$x \equiv 23 \cdot 7 (7^{-1} \bmod 30) + 4 \cdot 30 (30^{-1} \bmod 7)$

$\equiv 23 \times 7 \times 13 + 4 \times 30 \times 4 \bmod 210$

$\equiv 203 + 60$

$\equiv \boxed{53}$