A3p1

September 26, 2023 12:57 PM

$n = p * a + b \pmod{71}$

① $(52a) + b = 6$
② $(20a) + b = 51$
③ $(4a) + b = 38$

taking ① - ② we get

$(52a) + b = 6$
$-\ (20a) + b = 51$
$32a = -45$

$26 \pmod{71} = 32a$

$a = 26 \cdot 32^{-1}$

Using Euclidean algorithm:

$71 = 32 \times 2 + 7$
$32 = 7 \times 4 + 4$
$7 = 4 \times 1 + 3$
$4 = 3 \times 1 + 1$

Extended Euclidean algorithm:

$7 = 71 - 32 \times 2$
$4 = 32 - 7 \times 4$
$3 = 7 - 4 \times 1$
$1 = 4 - 3 \times 1$

$1 = 4 - (7 - 4 \times 1) \times 1$
$= 4 \times 2 - 7$
$= (32 - 7 \times 4) \times 2 - 7$
$= 32 \times 2 - 7 \times 9$
$= 32 \times 2 - (71 - 32 \times 2) \times 9$
$1 = 32 \times 20 - 71 \times 9$
$1 + 71 \times 9 = 32 \times 20$
$1 \bmod 71 = 32 \times 20$

$32^{-1} \equiv 20 \pmod{71}$

$a = 26 \cdot 20$
$a = 23 \pmod{71}$

plugging into ③

$4(23) + b = 38$
$b = 38 - 4(23)$
$b = -54$
$b = 17 \pmod{71}$

$\therefore\ n = (p * 23) + 17 \bmod 71$

A3p3

September 27, 2023 10:56 AM

$$R_{i+2} = (aR_{i+1} + bR_i + c) \bmod (m)$$

$m = 467$

$R_2 = 28$

$R_3 = 137$

$R_4 = 41$

$R_5 = 118$

$R_6 = 105$

(1) $41 = (a\,137 + b\,28 + c) \pmod{467}$

(2) $118 = (a\,41 + b\,137 + c) \pmod{467}$

(3) $105 = (a\,118 + b\,41 + c) \pmod{467}$

1-2 = (4)

$$41 = 137a + 28b + c$$
$$-118 = 41a + 137b + c$$
$$-77 = 96a - 109b$$

2-3 = (5)

$$118 = 41a + 137b + c$$
$$-105 = 118a + 41b + c$$
$$13 = -77a + 96b$$

1-3 = (6)

$$41 = 137a + 28b + c$$
$$-105 = 118a + 41b + c$$
$$-64 = 19a - 13b$$

for (4): $-77 = 96a - 109b$ for (5): $13 = -77a + 96b$

$\rightarrow \frac{77}{109} = \frac{-96a}{109} + b$ $\rightarrow \frac{13}{96} = \frac{-77a}{96} + b$

for (6): $-64 = 19a - 13b$

$\rightarrow \frac{64}{13} = \frac{-19a}{13} + b$

4'-5' =

$\frac{77}{109} = \frac{96a}{109} + b$

$-\frac{13}{96} = \frac{-77a}{96} + b$

$\frac{5975}{10464} = \frac{-823a}{10464}$

4'-6'

$\frac{77}{109} = \frac{96a}{109} + b$

$-\frac{64}{13} = -\frac{19a}{13} + b$

$\frac{-5975}{1417} = \frac{823a}{1417}$

5'-6'

$\frac{13}{96} = \frac{-77a}{96} + b$

$-\frac{64}{13} = -\frac{19}{13} + b$

$-\frac{5975}{1248} = \frac{823}{1248} a$

$a = -5975 \cdot 823^{-1} \pmod{467}$

$a = 37 \pmod{467}$

for (4): $-77 = 96a - 109b$

$-77 = 96(37) - 109b$

$b = 3629 \cdot 109^{-1} \pmod{467}$

$b = 59$

for (5): $13 = -77a + 96b$

$13 = -77(37) + 96b$

$b = 2862 \times 96^{-1} \pmod{467}$

$b = 59$

$\equiv 107 \pmod{467}$

$b = 59$

$b = 59$

for (1):

$41 = a\,137 + b\,28 + c$

$41 = 37(137) + 59(28) + c$

$c = -6680 \pmod{467}$

$c = 325$

for (2):

$118 = a\,41 + b\,137 + c$

$118 = 37(41) + 59(137) + c$

$c = -9482 \pmod{467}$

$c = 325$

$\therefore R_{i+2} = (37R_{i+1} + 59R_i + 325) \pmod{467}$

$a = 37$
$b = 59$
$c = 325$
$R_0 = 1$
$R_1 = 3$
$R_7 = 145$