Es: CRT System

$$\begin{cases} x \equiv 4 \bmod 11 \\ x \equiv 3 \bmod 17 \\ x \equiv 6 \bmod 18 \end{cases}$$

$N = 3366$

$b_1 = 4$; $N_1 = 306$
$b_2 = 3$; $N_2 = 198$
$b_3 = 6$; $N_3 = 187$

b_i	N_i	x_i	$b_i N_i x_i$
4	306	5	6120
3	198	14	8316
6	187	13	14586

$x_1 = 306^{-1} \bmod 11$

$306 \equiv 9 \bmod 11 \Rightarrow 9^{-1}$

$11 = 9 \times 1 + 2$
$9 = 2 \times 4 + 1$
$4 = 1 \times 4 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 2 \bmod 11 = 10$
$p_3 = 1 - 10 \times 4 \bmod 11 \equiv 5$

$198 \equiv 11 \bmod 17$
$17 = 11 \times 1 + 6$
$11 = 6 \times 1 + 5$
$6 = 5 \times 1 + 1$
$5 = 1 \times 5 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 1 \bmod 17 = 16$
$p_3 = 1 - 16 = 2$
$p_4 = 16 - 2 = 14$

$187 \equiv 7 \bmod 18$

$18 = 7 \times 2 + 4$
$7 = 4 \times 1 + 3$
$4 = 3 \times 1 + 1$
$3 = 1 \times 3 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 2 = 16$

$p_3 = 1 - 16 = 3$
$p_3 = 16 - 3 = 13$

$$x = 6120 + 8316 + 14586 = 2754 + 1584 + 1122 \equiv 2094 \bmod 3366$$

Es: CRT

Find $x \in 401$ such that

$$x \cdot 29 \equiv 1 \bmod 401$$
$$5x \equiv 14 \bmod 401$$

$$x = 29^{-1} \bmod 401$$

$401 = 29 \times 13 + 24$
$29 = 24 \times 1 + 5$
$24 = 5 \times 4 + 4$
$5 = 4 \times 1 + 1$
$4 = 1 \times 4 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 13 = 388$
$p_3 = 1 - 388 = 14$
$p_4 = 388 - 14 \times 4 = 332$
$p_5 = 14 - 332 = 83$

$$5 \times 83 = 415 \equiv 14 \bmod 401$$

$$x = 83$$

Es: EC

Let $E: y^2 \equiv x^3+7$ be the elliptic curve defined on $\mathbb{Z}_{11}$
Let $P=(2,2)$ and $Q=(7,3)$

If $P, Q \in E$, then compute the x-component of $P+Q$

Else answer NO

Check if $P \in E$

$2^2 = 2^3+7 \bmod 11$
$4 = 8+7 \equiv 4$ OK

Check if $Q \in E$

$3^2 = 7^3+7 \bmod 11$
$9 = 7^2 \cdot 7 + 7 \bmod 11 \equiv 9$ OK

$P+Q = R(x_3, y_3)$

$$\lambda = \frac{y_2-y_1}{x_2-x_1} = 1 \cdot 5^{-1} \bmod 11 \equiv 9$$

$$x_3 = \lambda^2 - x_1 - x_2 = 4 - 2 - 7 = 6$$

Es: Galois

Let $GF(8)$ be the Galois field defined by the polynomial $G(x) = x^3+x+1 \in \mathbb{Z}_2[x]$

Let $a(x) \in GF(8)$ be the polynomial $a(x) = x^2+x$

The multiplicative inverse of $a(x)$ is

a) $x+1$

b) x

c) x^2+x+1

d) x^2+x

Solution

$$
\begin{array}{l|l}
x^3 + 0x^2 + x + 1 & x^2+x \\
\cline{2-2}
x^3 \quad\; x^2 & x+1 \\
\cline{1-1}
\quad\;\; x^2 + x + 1 & \\
\quad\;\; x^2 + x & \\
\cline{1-1}
\qquad\qquad\; 1 &
\end{array}
$$

$$(x^2+1, x^3+x+1) \xrightarrow[x+1]{} (1, x^2+x) \xrightarrow[x^2+1]{} (0, 1)$$

Reverse rule:

$$(y+qx, x) \longleftarrow (x, y)$$

$$(0, 1) \xrightarrow[x^2+1]{} (1, 0) \xrightarrow[x+1]{} (x+1, 1)$$