Annexe 1. Formule d'addition de points pour $t^2 = x^3 + ax + b$.

Soit $P_1 = (x_1, t_1)$ et $P_2 = (x_2, t_2)$ avec $P_i \neq \Omega$.
$P_3 = P_1 + P_2 = (x_3, t_3)$
(1) si $x_1 \neq x_2$, la pente de la corde $\delta = \dfrac{t_2 - t_1}{x_2 - x_1}$
$x_3 = \delta^2 - x_1 - x_2$
$t_3 = \delta(x_1 - x_3) - t_1$

(2) si $P_1 = P_2$ et $t_1 = t_2 \neq 0$, la pente de la tangente $\delta = \dfrac{3x_1^2 + a}{2t_1}$
$x_3 = \delta^2 - 2x_1$
$t_3 = \delta(x_1 - x_3) - t_1$

Remarques: si $x_1 = x_2$ et $t_1 \neq t_2$, $P_1 + P_2 = \Omega$
si $P_1 = P_2$ et $t_1 = t_2 = 0$, $P_1 + P_2 = \Omega$
pour tout P, $P + \Omega = P$

Annexe 2. Algorithme.

Entrées: $k > 0$, P un point de la courbe elliptique.
Sortie: kP.
Règles: $\mapsto (\Omega, P, k)$
Si n impair: $(R, Q, n) \mapsto (R + Q, Q, n - 1)$
Si n pair et $n \neq 0$: $(R, Q, n) \mapsto (R, 2Q, n/2)$
Si $n = 0$: Sortir R.

Annexe 3. Résultats de calculs.

$323^{-1} = 658 \mod 751$

$386(0, 0) = (676, 182)$

$(562, 576) + (239, 1) = (385, 703)$

les points étant donnés par leurs coordonnées (x, y).