



## Énigme elliptique

Cette énigme a été créée par **Saint Erulo**

Indice : On pourra s'aider de la fiche de cours sur les courbes elliptiques ainsi que du site :

<https://andrea.corbellini.name/ecc/interactive/modk-mul.html>

Alice et Bob souhaitent s'adresser des messages chiffrés par courbe elliptique.

Ils se mettent d'accord sur les données suivantes :

- équation de la courbe :  $y^2 = x^3 + 2x + 3$
- point initial sur la courbe :  $P(3,6)$
- champ  $F_{103}$  soit  $p = 103$

Alice choisit secrètement un nombre  $d_A$  et calcule les coordonnées du point  $P_A = d_A * P$ , soit  $P_A(96, 77)$ , qu'elle communique à Bob.

Bob choisit secrètement un nombre  $d_B = 3$  et calcule les coordonnées du point  $P_N = d_B * P_A$ , dont le résultat est  $P_N(x_N, y_N)$  et qui constitue leur clé commune. La solution de l'énigme est la somme des coordonnées  $x_N$  et  $y_N$  du point  $P_N$ .