Exo 1

On trouve que
n = 187,
d = 83,
et y = 10^{27} mod 187 = 54
et x = 54^{83} mod 187 = 10

TD3 - Exercice 1 **Calcul de d, inverse modulaire de 27 modulo 160**

Utilisation de l'algorithme d'Euclide étendu

$d \equiv 27^{-1} \pmod{160}$

```
160 % 27 = 25
27 % 25 = 2
25 % 2 = 1  (le PGCD est 1 : 160 et 27 sont premiers entre eux)
2 % 1 = 0
```

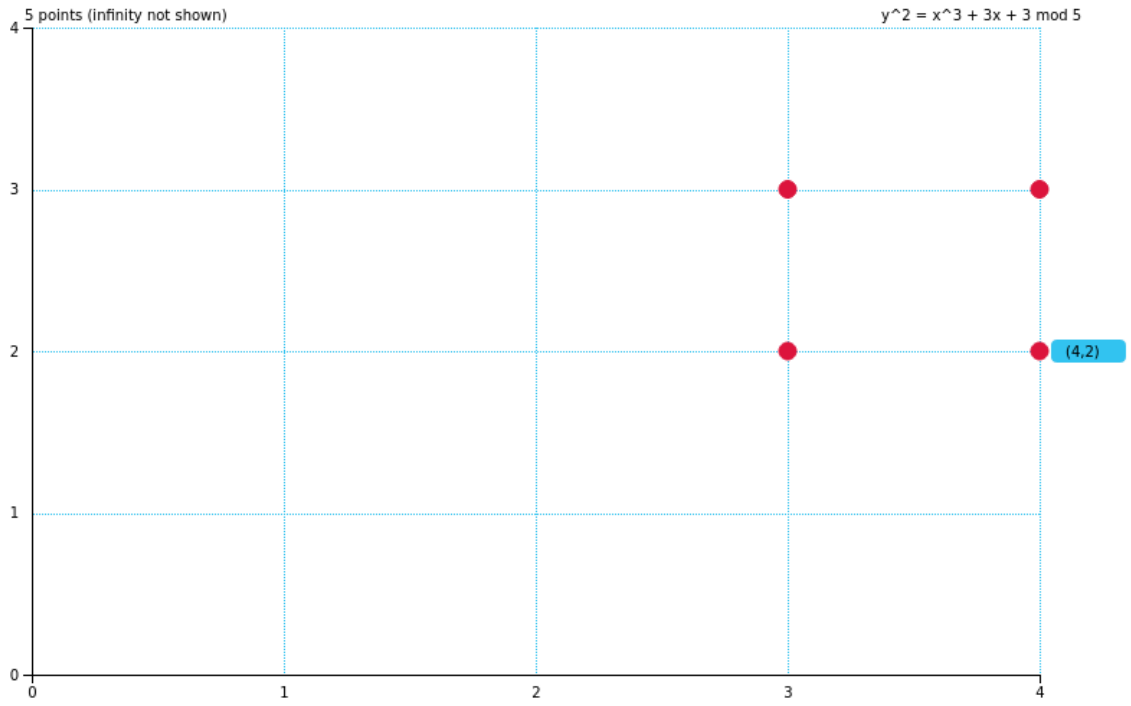
INIT	x=0	y=1				
	x=1	y=0	x_1=0	y_1=1	a=1	b=2
	x=-12	y=1	x_1=1	y_1=0	a=2	b=25
	x=13	**y=-12**	x_1=-12	y_1=1	a=25	b=27
	x=-77	y=13	x_1=13	y_1=-12	a=27	b=160

$x = y_1 - \lfloor b/a \rfloor \times x_1$

```
d = (-77 % 160 + 160) % 160
d = (83 + 160) % 160
d = 243 % 160
d = 83
```

Exo 3

Draw the elliptic curve $y^2 = x^3 + ax + b \mod r$, where a: 3 b: 3 r: 5 DRAW!



Point Detail

Point:	(4,2)
Inverse:	(4,3)
Order of subgroup:	5
Generated subgroup:	(4,2) → (3,2) → (3,3) → (4,3) → ∞

Table of Point Additions

+	∞	(3,2)	(3,3)	(4,2)	(4,3)
∞	∞	(3,2)	(3,3)	(4,2)	(4,3)
(3,2)	(3,2)	(4,3)	∞	(3,3)	(4,2)
(3,3)	(3,3)	∞	(4,2)	(4,3)	(3,2)
(4,2)	(4,2)	(3,3)	(4,3)	(3,2)	∞
(4,3)	(4,3)	(4,2)	(3,2)	∞	(3,3)

Exo 4

TD4 - Exercice 1 **Résolution d'un système de congruences (2)**

Exemple :

- $x \equiv 3 \pmod 5$
- $x \equiv 1 \pmod 7$
- $x \equiv 6 \pmod 8$

On vérifie que $\text{PGCD}(5, 7) = \text{PGCD}(5, 8) = \text{PGCD}(7, 8) = 1$

NB : pour de petites valeurs, on peut calculer l'inverse modulaire sans l'algorithme d'Euclide étendu

- $56x_1 \equiv 1 \pmod 5$
  - $x_1 \equiv 1 \pmod 5$ car 56%5 = 1
- $40x_2 \equiv 1 \pmod 7$
  - $5x_2 \equiv 1 \pmod 7$ car 40%7 = 5
  - $x_2 \equiv 3 \pmod 7$ car (3×5)%7 = 1
- $35x_3 \equiv 1 \pmod 8$
  - $3x_3 \equiv 1 \pmod 8$ car 35%8 = 3
  - $x_3 \equiv 3 \pmod 8$ car (3×3)%8 = 1

b_i	N_i	x_i	$b_i N_i x_i$
3	56	1	168
1	40	3	120
6	35	3	630

Solution :

$N = 5 \times 7 \times 8 = 280$

$x = 168 + 120 + 630 = 918 \pmod{280}$

$x = 78 \pmod{280}$