Des opérations inhabituelles

Activités

Tenerife - Novembre 2021

1 Remplir la table d'addition modulo 7.

+	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

2 Remplir la table de multiplication modulo 7.

X	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

3 Modulo 17, calculer 3^{16} puis 3^{81}.

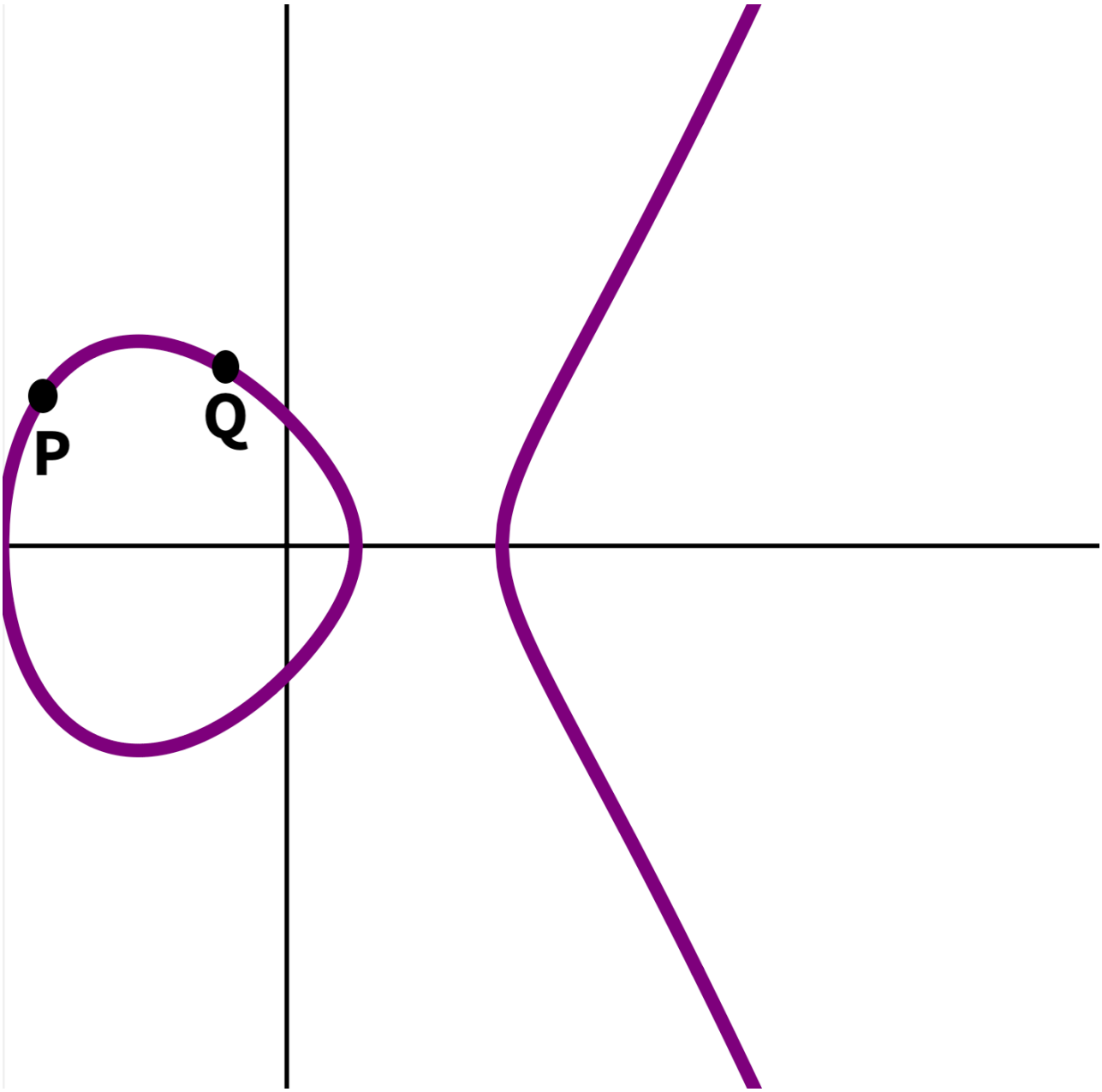
4 Modulo 17, exprimer chacun des entiers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 comme une puissance de 3.

5 Vous savez qu'il existe un nombre x tel que $3x = 1$. Ce nombre est $x = \frac{1}{3}$. Modulo 17, trouvez un entier tel que $3x \equiv 1$.

6 Donner l'allure générale des courbes elliptiques d'équation

- $y^2 = x^3 - x + 1$
- $y^2 = x^3 - x + \frac{1}{4}$.

7 Tracer $P + Q$.



8 **Un exemple de cryptographie RSA.**

Alice veut envoyer à Bob le message CNRS. Pour manipuler des nombres petits, on suppose que les messages transmis ne font qu'une lettre[1]. Alice va donc transmettre

[1] Évidemment, en réalité on ne fait pas comme ça. Il serait bien trop facile de décrypter les messages secrets puisqu'il suffirait de crypter chaque lettre, et de reconnaître chaque cryptage de lettre dans le message crypté pour le décrypter. On travaille avec des très grands nombres à l'aide d'ordinateurs et on ne connaît pas à l'avance la longueur des messages. Il y a donc un très grand nombre de messages possibles (et non pas simplement 26 si les messages ne sont constitués que d'une lettre).

successivement plusieurs messages cryptés : le message C, puis le message N, puis le message R, et enfin le message S. On remplace chaque lettre par un nombre suivant la table suivante

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	6	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Bob choisit $p = 5$ et $q = 11$. Il calcule alors

$$n = 5 \times 11 = 55$$

puis

$$\varphi = (5-1) \times (11-1) = 4 \times 10 = 40.$$

Il choisit $e = 7$. Il est bien premier à $\varphi = 40$.

Montrer que l'entier $d = 23$ vérifie bien $de \equiv 1 \pmod{\varphi}$.

Bob publie dans un annuaire $n = 55$ et $e = 7$. Donc Alice les connaît. Alice veut crypter la lettre C. Cette lettre C est codée par le nombre $M = 3$. Alice calcule donc

$$M^e = 3^7 \equiv 42 \pmod{55}.$$

Alice transmet alors 42 à Bob. Bob calcule $42^d = 42^{23} \equiv 3 \pmod{55}$. Il retrouve bien la lettre C.

Montrer que la lettre N est cryptée par 9, la lettre R par 17 et la lettre S par 24.

Alice envoie à Bob le message 33-4-33-25-23-25-24-7-1-15-2-24. Pouvez-vous le décrypter ?[2]

[2] Envoyez-moi le message décrypté et expliquez-moi si vous êtes d'accord ou non (en justifiant votre avis) à emmanuel.royer@math.cnrs.fr