EXERCICE 4 Candidats ayant suivi l'enseignement de spécialité 5 points

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adelman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.
Les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage, la question 4 le décryptage.

1. Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.

1.a. Vérifier que $8^7 \equiv 2 \mod 55$
En déduire le reste de la division euclidienne par 55 du nombre 8^{21}

1.b. Vérifier que $8^2 \equiv 9 \mod 55$ puis déduire de la question a, le reste de la division euclidienne par 55 de 8^{23}.

2. Dans cette question, on considère l'équation (E) : $23x-40y=1$, dont les solutions sont des couples $(x;y)$ d'entiers relatifs.

2.a. Justifier le fait que l'équation que l'équation (E) admet au moins un couple solution.

2.b. Donner un couple, solution particulière de l'équation (E).

2.c. Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).

2.d. En déduire qu'il existe un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23d \equiv 1 \mod 40$

3. Cryptage dans le système RSA.
Une personne A choisit deux nombres premiers p et q , puis calcule les produits $N=pxq$ et $n=(p-1)x(q-1)$ elle choisit également un entier naturel c premier avec n.
La personne publie le couple $(N;c)$ qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté.
Les messages sont numérotés et transformés en une suite d'entiers compris entre 0 et N-1.
Pour crypter un entier a de cette suite, on procède ainsi:on calcule le reste b dans la division euclidienne par N du nombre a^c et le nombre crypté est l'entier b.
Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres.
On va l'envisager ici avec des nombres plus simples : p=5 et q=11.
La personne A choisit également c=23.

3.a. Calculer les nombres N et n, puis justifier que c vérifie la condition voulue.

3.b. Un émetteur souhaite envoyer à la personne A le nombre a=8.
Déterminer la valeur du nombre crypté b.

4. Décryptage dans le système RSA.
La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions :
$0 \leqslant d < n$ et $cd \equiv 1 \mod n$.
Elle garde secret le nombre d qui lui permet, et à elle , de décrypter les nombres qui lui ont été envoyés cryptés avec la clé publique.
Pour décrypter un nombre crypté b, la personne A calcule le reste de la division euclidienne par N du nombre b^d , et le nombre en clair (c'est à dire le nombre avant le cryptage) est le nombre a.
On admet l'existence et l'unicité de l'entier d, est le fait que le décryptage fonctionne.
Les nombres choisis par A sont encore p=5, q=11 et c=23.

3.a. Quelle est la valeur de d ?

3.b. En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est b=17.

CORRECTION

1.a. En utilisant la calculatrice, on effectue la division euclidienne de 8^7 par 55.
$8^7=2097152=38130\times55+2$
donc $8^7\equiv2 \mod 55$
$21=7\times3$ donc $8^{21}=(8^7)^3$ et $8^{21}\equiv2^3 \mod 55$ soit $8^{21}\equiv8 \mod 55$

1.b. $8^2=64=55\times1+9$ donc $8^2\equiv9 \mod 55$
$8^{23}=8^{21}\times8^2$ et $8^{23}\equiv8\times9 \mod 55$
$8\times9=72=55\times1+17$ donc $8^{23}\equiv17 \mod 55$

2. $(E):\ 23x-40y=1$

2.a. 23 et 40 sont premiers entre eux donc le théorème de Bezout nous permet d'affirmer qu'ils existent deux entiers relatifs x et y tels que 23x-40y=1.
Conséquence
L'équation (E) admet au moins un couple solution.

2.b. On trouve assez facilement comme solution particulière le couple (7;4), ou bien on détermine une solution particulière en utilisant l'algorithme d'Euclide.

	1	1	2	1
40	23	17	6	5
17	6	5	1	

$17=1\times40-1\times23$
$6=1\times23-1\times17$
$5=1\times17-2\times6$
$1=1\times6-1\times5$
$1=1\times6-1\times(1\times17-2\times6)=3\times6-1\times17=3\times(1\times23-1\times17)-1\times17=3\times23-4\times17$
$1=3\times23-4\times(1\times40-1\times23)=7\times23-4\times40$
donc (7;4) est une solution particulière de l'équation.

2.c. $(E):\ 23x-40y=1 \Leftrightarrow 23x-40y=23\times7-40\times4 \Leftrightarrow 23\times(x-7)=40\times(y-4)$
23 divise $40\times(y-4)$ et 23 est premier avec 40, le théorème de Gauss nous permet d'affirmer que 23 divise (y-4) donc il existe un entier relatif t tel que y-4=23t et on a $23\times(x-7)=40\times23t \Leftrightarrow x-7=40t$ donc le couple (40t+7;23t+4) est solution de (E).
Vérification
Pour tout entier relatif t :
$23\times(40t+7)-40\times(23t+4)=23\times40t+23\times7-40\times23t-40\times4=1$
Conclusion
L'ensemble des solutions de (E) est l'ensemble des couples (40t+7;23t+4) lorsque t décrit $\mathbb{Z}$.

2.d. $23d\equiv1 \mod 40$ si et seulement s'il existe un entier relatif z tel que 23d=40z+1 donc le couple (d;z) est une solution de (E) donc d=40t+7.
$0\leqslant d<40$ donc t=0 et d=7.
Conclusion
7 est l'unique entier vérifiant : $0\leqslant7<40$ et $23\times7\equiv1 \mod 40$

3.a. $N=p\times q=5\times11=55$
$n=(p-1)\times(q-1)=(5-1)\times(11-1)=4\times10=40$
c=23 est premier avec 40.

3.b. a=8 $a^c=8^{23}$
Nous avons démontrer dans le 1.b. que $8^{23}\equiv17 \mod 55$

Conclusion
b=17

4.a. $0 \leqslant d < 40$ et $23d \equiv 1 \mod 40$
Nous avons démontre dans le 2.d. que **d=7.**

4.b. $b=17$ $b^d = 17^7$
En utilisant la calculatrice on obtient :
$17^7 = 410338673 = 7460703 \times 55 + 8$
Conclusion
a=8.