www.freemaths.fr

Maths Expertes
Terminale

Arithmétique

ÉNONCÉ DE L'EXERCICE

ARITHMÉTIQUE

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 Adleman, 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.

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

b) Vérifier que $8^2 \equiv 9 \mod 55$, puis déduire de la question **a)** le reste dans 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.

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

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

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

d) En déduire qu'il existe un unique entier d vérifiant les conditions $0 \leq d < 40$ 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 $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n.
La personne A publie le couple (N, c), qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté.

Les messages sont numérisés 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 $c = 23$.

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

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 $0 \leq d < n$ et $c\,d \equiv 1 \mod n$. Elle garde secret ce nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique.

Pour décrypter un nombre crypté b, la personne A calcule le reste a dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre a.
On admet l'existence et l'unicité de l'entier d, et le fait que le décryptage fonctionne.

Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.

a) Quelle est la valeur de d ?

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