Devoir Commun 3 - Correction

Exercice 1 2018 CentresEtrangers Spé

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}.

   Correction

   On donne donc la division euclidienne de 8^7 par 55, on obtient :

   $$8^7 = 38130 \times 55 + 2$$

   On en déduit donc

   $$8^7 \equiv 2 \mod 55$$

   De plus $8^{21} = \left(8^7\right)^3 \equiv (2)^3 \mod 55 \equiv 8 \mod 55$

   Le reste dans la division euclidienne de 8^{21} par 55 est donc 8

   (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}.

   Correction

   On a $8^2 = 64 = 55 + 9 \equiv 9 \mod 55$. On en déduit à l'aide de la question précédente que :

   $8^{23} = 8^{21} \times 8^2 \equiv 8 \times 9 \mod 55$
   $8^{23} = 8^{21} \times 8^2 \equiv 72 \mod 55$
   $8^{23} = 8^{21} \times 8^2 \equiv 17 \mod 55$

   Le reste dans la division euclidienne de 8^{23} par 55 est donc 17

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.

   Correction

   Comme les nombres 23 et 40 sont premiers entre eux, **le théorème de Bezout** nous dit qu'il existe un couple d'entier u et v tel que :

   $$u \times 23 + v \times 40 = 1$$

   Il suffit donc de choisir $x = u$ et $y = -v$

   Le théorème de Bezout nous donne l'existence.

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

Correction

Comme 40 est un multiple de 10 il faut pour que l'égalité soit vérifié que $x \times 23$ finisse par 9 ou 1. Donc x finit par 3 ou 7

Or $3 \times 23 = 69$ qui ne peut fonctionner car 70 n'est pas un multiple de 40 et $7 \times 23 = 161 = 160 + 1 = 4 \times 40 + 1$.

On choisit donc $x = 7$ et $y = 4$

Remarque : Ce résultat se retrouve par des divisions euclidiennes successives.

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

Correction

Le couple $(7\ ;\ 4)$ est une solution particulière on en déduit donc que l'on a le système d'équation suivant : $\begin{cases} 23 \times 7 - 40 \times 4 = 1 \\ 23 \times x - 40 \times y = 1 \end{cases}$

Ce qui nous donne

$$23 \times (7 - x) - 40 \times (4 - y) = 0$$

Ce qui s'écrit également

$$23 \times (7 - x) = 40 \times (4 - y)$$

Or comme 23 et 40 sont premiers entre eux on en déduit d'après le **théorème de Gauss** que $\begin{cases} 40 \text{ divise } (x-7) \\ 23 \text{ divise } (4-y) \end{cases}$

Donc il existe k et k' dans $\mathbb{Z}$ tel que :

$\begin{cases} (x-7) = 40k \\ (4-y) = 23k' \end{cases}$

En repportant donc ces solutions dans l'équation (E) on obtient :

$23 \times 40k - 40 \times 23k' = 0 \implies k = k'$,

on a donc montré que les solutions de l'équation (E) sont de la forme :

$$(7 + 40k\ ;\ 4 + 23k) \qquad \text{avec } k \in \mathbb{Z}$$

Réciproquement : soit $k \in \mathbb{Z}$ il est clair que le couple $(7 + 40k\ ;\ 4 + 23k)$ est solution de (E)

Finalement :

les solutions de l'équation (E) sont les couples $(7 + 40k\ ;\ 4 + 23k)$ avec $k \in \mathbb{Z}$

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

Correction

On a donc :

$$23x - 40y = 1 \iff 23x = 1 + 40y \iff 23x \equiv 1 \mod 40$$

, on en déduit donc que $23d \equiv 1 \mod 40 \implies d = 7 + 40k \quad k \in \mathbb{Z}$. Or $0 \leqslant d < 40$

La seule solution est donc $k = 0$ et $d = 7$

Il existe une seule solution $d = 7$

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.

Correction

$N = p \times q = 5 \times 11 = 55$ et $n = (p-1)(q-1) = 4 \times 10 = 40$.

De plus l'entier $c = 23$ est bien premier avec 40

$$N = 55 \text{ et } n = 40$$

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

Correction

Il nous faut donc calculer le reste de la division euclidienne de 8^{23} par 55.

Nous savons que ce reste est 17 d'après la question 1.(b).

Finalement

$$b = 17$$

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 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 ?

Correction

$$\begin{cases} n = 40 \text{ et } c = 23 \\ 0 \leq d < 40 \\ 23d \equiv 1 \mod 40 \end{cases}$$

On obtient donc d'après la question 2.(d) que $d = 7$

$$d = 7$$

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

Correction

Il nous faut donc calculer le reste de la division euclidienne de $bd = 17^7$ par $N = 55$.

Or on a $17^2 = 289 \equiv 14 \mod 55$

Et donc $17^7 = \left((17)^2\right)^3 \times 17 \equiv 14^3 \times 17$
Or :
$14^2 = 196 \equiv 31 \mod 55$
Et ainsi $17^7 \equiv 31 \times 14 \times 17 \equiv 7378 \equiv 1878 \equiv 778 \equiv 228 \equiv 8 \mod 55$

Le nombre a est donc 8