Petit Théorème de Fermat – Système RSA

« Petit » Théorème de Fermat :

- Soit p un nombre premier et x un entier non divisible par p. Alors $x^{p-1} \equiv 1 \mod p$.
- Soit p un entier premier et x un entier quelconque. Alors $x^p - x$ est divisible par p.

I Un exemple de nombre de Poulet

Un entier $n \geqslant 1$ est dit « de Poulet » lorsque qu'il est composé et vérifie : $2^{n-1} \equiv 1\ [n]$.

1) Justifier que $2^{36} \equiv 1\ [37]$. En déduire que $2^{2700} - 1$ est divisible par 37.

2) Justifier que $2^9 \equiv 1\ [73]$. En déduire que $2^{2700} - 1$ est divisible par 73.

3) Démontrer que 2701 est un entier « de Poulet ».

II Nombres de Carmichaël

Un entier $n \in \mathbb{N}^*$ est dit « de Carmichaël » lorsqu'il est composé et que pour tout entier relatif a, on a : $a^n \equiv a\ [n]$.

1) Soit p un entier premier et $n \in \mathbb{N}^*$ tel que $p-1$ divise $n-1$. Prouver que pour tout entier relatif a : $a^n \equiv a\ [p]$.

2) Montrer que 561 est un entier de Carmichaël.

III Cryptographie : la base du système RSA

Dans toute la suite, p et q désignent deux entiers premiers distincts.

1)a) Prouver que si a est entier qui n'est divisible ni par p, ni par q, alors : $a^{(p-1)(q-1)} \equiv 1\ [pq]$.

1)b) Soit $a \in \mathbb{Z}$. Prouver que : $k \equiv 1\ [(p-1)(q-1)] \Rightarrow a^k \equiv a\ [pq]$.

2) Soit c un entier naturel premier avec $n = (p-1)(q-1)$ tel que $1 < c < n$.

2)a) Pourquoi l'équation (E) : $cx + ny = 1$ d'inconnue $(x; y) \in \mathbb{Z}^2$ possède-t-elle au moins une solution $(x_0; y_0)$?

2)b) Donner alors toutes les solutions de l'équation (E) en utilisant $(x_0; y_0)$.

2)c) Montrer qu'il existe un unique entier naturel $d < n$ tel que $cd \equiv 1\ [n]$.

2)d) Soit $(a; b) \in \mathbb{Z}^2$ tel que $b \equiv a^c\ [pq]$. Établir que $b^d \equiv a\ [pq]$.

*Les résultats de la partie III sont à la base de la méthode de cryptographie appelée RSA, inventée en 1978 par trois mathématiciens, Ronald **R**ivest, Adi **S**hamir et Léonard **A**dleman. Dans ce système, le message initial a est codé par b grâce à la formule $b \equiv a^c\ [pq]$. On retrouve ensuite a grâce à la formule $b^d \equiv a\ [pq]$. Le produit pq est public ainsi que c, ce qui permet à chacun de crypter un message. Mais les entiers p et q proprement dits ne sont pas connus, ce qui interdit de calculer $n = (p-1)(q-1)$ et l'entier d. Il n'est donc pas possible de décrypter un message. Pour garder p et q inconnus tout en rendant public le produit pq, on doit prendre deux nombres premiers suffisamment grands pour la factorisation du produit pq soit impossible dans un délai raisonnable.*