Cryptographie et arithmétique – Feuille 3

Exercice 1. Soit $p \geqslant 5$ un nombre premier. Montrer que 24 divise $p^2 - 1$.

Exercice 2. On note $\Lambda : \mathbb{N}^* \to \mathbb{R}$ la fonction définie par :

$$\Lambda(n) = \begin{cases} \ln(p) \text{ si } n = p^k & (p \text{ premier}, k \geqslant 1) \\ 0 \text{ sinon.} \end{cases}$$

Montrer que pour tout $n \geqslant 1$, on a $\sum_{d|n} \Lambda(d) = \ln(n)$ (la somme est indexée par l'ensemble des diviseurs positifs d de n).

Exercice 3. On veut montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

1. Montrer que tout entier naturel congru à 3 mod 4 admet un diviseur premier congru à 3 mod 4.
2. En déduire le résultat voulu (indication : s'inspirer de la démonstration d'Euclide de l'infinité des nombres premiers).

Exercice 4. Soit $n \geqslant 2$ un entier et p un nombre premier. Montrer que la multiplicité de p dans la décomposition en facteurs premiers de $n! = 1 \times 2 \times \cdots \times (n-1) \times n$ est exactement $\sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor$, où, pour tout réel x, $[x]$ désigne la partie entière de x. En déduire le nombre de zéros à la fin de l'écriture décimale de 100!.

Exercice 5. Soit p un nombre premier. On cherche à déterminer pour quelles valeurs de p il existe une solution entière s à l'équation $s^2 \equiv -1 \mod p$.

1. Étudier le cas $p = 2$.

   Supposons à présent $p \geqslant 3$. On partitionne l'ensemble $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ en regroupant chaque élément x de cet ensemble avec son opposé $-x$, son inverse x^{-1} et l'opposé de son inverse $-x^{-1}$. Les sous-ensembles ainsi obtenus ont au plus quatre éléments.
2. Déterminer à quelle condition ces sous-ensembles ont strictement moins de quatre éléments (indication : étudier les équations $x \equiv -x \mod p$, $x \equiv x^{-1} \mod p$ et $x \equiv -x^{-1} \mod p$).
3. En déduire que l'équation $s^2 \equiv -1 \mod p$ admet deux solutions mod p si, et seulement si p est de la forme $4n + 1$.

Exercice 6. Soit p un nombre premier de la forme $4n+1$. Par l'exercice précédent, il existe une solution s à l'équation $s^2 \equiv -1 \mod p$.

1. Dénombrer le nombre de couples d'entiers (a, b) tels que $0 \leqslant a, b \leqslant \sqrt{p}$.
2. En déduire qu'il existe deux couples distincts (a, b) et (c, d) de cette forme tels que $a - sb \equiv c - sd \mod p$ (indication : utiliser le principe des tiroirs).
3. On pose $x = |a - c|$ et $y = |b - d|$. Montrer que $p = x^2 + y^2$.
4. Montrer que si p est de la forme $4n + 3$, alors p ne peut pas s'écrire comme somme de deux carrés.

Exercice 7. Soit $p \geqslant 2$ un entier naturel. Montrer que $(p-1)! \equiv -1 \mod p$ si, et seulement si p est premier. Que dire si p n'est pas premier ?

Exercice 8. Montrer que le groupe $(\mathbb{Q}, +)$ n'a pas un nombre fini de générateurs ; autrement dit, pour tout ensemble fixé $\{r_1, \ldots, r_n\}$ de rationnels, il existe des nombres rationnels qui ne sont pas de la forme $a_1 r_1 + \cdots a_n r_n$ avec $a_1, \ldots, a_n$ entiers.

Exercice 9. En raisonnant par l'absurde, on veut montrer que l'équation diophantienne $y^2 = x^3 + 7$ d'inconnue $(x, y) \in \mathbb{Z}^2$ n'a pas de solution. Supposons l'existence d'une telle solution (x, y).

1. Montrer que x est impair.
2. Montrer que $y^2 + 1$ possède un facteur premier p congru à $3 \mod 4$ (indication : factoriser $x^3 + 8$ par $x + 2$).
3. Conclure en étudiant y^{p-1} de deux manières différentes.

Exercice 10. Soient $a \geqslant 2$ et $n \geqslant 2$ deux entiers naturels.

1. Montrer que si $a^n - 1$ est un nombre premier, alors $a = 2$ et n est un nombre premier. Un tel nombre est appelé nombre de Mersenne. Que dire de la réciproque ?
2. Montrer que si $2^n + 1$ est un nombre premier, alors n est une puissance de 2. Un tel nombre est appelé nombre de Fermat.

Exercice 11. Soit p un nombre premier, et q un diviseur premier de $2^p - 1$.

1. Quel est l'ordre de $\bar{2}$ dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$?
2. En déduire une nouvelle preuve de l'infinité des nombres premiers.

Exercice 12. On considère m et n deux entiers non nuls.

1. Soient x et a deux entiers. Montrer que si $x \equiv a \mod mn$, alors $x \equiv a \mod m$ et $x \equiv a \mod n$. Ceci permet de définir une application
$$\Phi : \begin{cases} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x \mod mn & \mapsto & (x \mod m, x \mod n) \end{cases}.$$
2. On suppose que m et n sont premiers entre eux. Montrer que Φ est une bijection. Décrire Φ^{-1} (indication : on peut commencer par déterminer $\Phi^{-1}(1,0)$ et $\Phi^{-1}(0,1)$ grâce à une relation de Bézout entre m et n).

   L'affirmation que Φ est une application bijective est le *théorème des restes chinois* ; les questions suivantes en sont des applications.
3. Résoudre le système de congruences $\begin{cases} n \equiv 3 \mod 7 \\ n \equiv 7 \mod 11 \end{cases}$.
4. On nomme *nombre de Carmichael* un entier naturel n qui, sans être un nombre premier, vérifie toutefois que pour entier a premier à n, on a $a^{n-1} \equiv 1 \mod n$. Montrer que 561 est un nombre de Carmichael. Rapprocher ces nombres du petit théorème de Fermat.
5. Si $n \geqslant 1$ est un entier, on note $\varphi(n)$ le nombre d'entiers naturels dans $[\![1, n]\!]$ qui sont premiers à n. Montrer que si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$. La fonction φ ainsi définie est appelée *indicatrice d'Euler*.