Cryptographie et arithmétique – Feuille 3

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

Exercice 2. 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 3 (critères de divisibilité).

1. Démontrer qu'un entier naturel est divisible par 3 si, et seulement si la somme de ses chiffres (en écriture décimale) est divisible par 3. De même en remplaçant 3 par 9.
2. Démontrer qu'un entier naturel est divisible par 4 si, et seulement si l'entier naturel formé par ses deux derniers chiffres (en écriture décimale) est divisible par 4.
3. Démontrer qu'un entier naturel est divisible par 11 si, et seulement si la somme alternée de ses chiffres (en écriture décimale) est divisible par 11.

Exercice 4. Soit $n \geqslant 1$ un entier naturel.

1. Montrer qu'il existe un nombre ne comportant que des 1 et des 0 (en écriture décimale) divisible par n (indication : utiliser le principe des tiroirs dans $\mathbb{Z}/n\mathbb{Z}$).
2. Montrer que si n et 10 sont premiers entre eux, alors il existe un nombre ne comportant que des 1 (en écriture décimale) divisible par n.

Exercice 5. 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 6 (somme de deux carrés). Soit p un nombre premier tel que $p \equiv 1 \mod 4$. Par l'exercice 13 du TD2, 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 $p \equiv 3 \mod 4$, alors p ne peut pas s'écrire comme somme de deux carrés.

Exercice 7 (équation diophantienne). En raisonnant par l'absurde, on veut montrer que l'équation $y^2 = x^3 + 7$ 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.

Exercice 8 (nombres premiers particuliers). 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 9. 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 10 (applications du théorème des restes chinois).

1. Résoudre les systèmes de congruence :

$$\begin{cases} n \equiv 16 \mod 47 \\ n \equiv 25 \mod 31 \end{cases}, \qquad \begin{cases} 2n \equiv 10 \mod 63 \\ 3n \equiv 9 \mod 12 \end{cases}.$$

2. Soit $n \geqslant 2$ un entier de la forme $n = p_1 \cdots p_r$, où les p_i sont des nombres premiers distincts deux à deux. Compter le nombre de solutions à l'équation $\bar{x}^2 = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.
3. 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*.
   Si m et n ne sont pas premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$ où on a posé $d = \text{pgcd}(m, n)$. Cette identité ne se démontre pas avec le théorème des restes chinois.

Exercice 11. Montrer que pour tout $n \geqslant 1$, $\sum_{d|n} \varphi(d) = n$ (la somme est indexée par l'ensemble des diviseurs positifs d de n).

Exercice 12 (fonction de Möbius). On note $\mu : \mathbb{N}^* \to \mathbb{R}$ la fonction définie par :

$$\mu(n) = \begin{cases} 0 & \text{s'il existe } p \text{ premier tel que } p^2 \text{ divise } n, \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombres premiers distincts.} \end{cases}$$

Montrer que pour tout $n \geqslant 1$, on a $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$ (la somme est indexée par l'ensemble des diviseurs positifs d de n). En déduire, en utilisant également l'exercice précédent, que $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.
Cette formule peut être utilisée pour estimer le nombre moyen d'entiers premiers à n : on a $\lim_{n\to+\infty} \frac{1}{n^2} \sum_{k=1}^{n} \varphi(k) = \frac{3}{\pi^2}$.

Exercice 13. 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.