Feuille d'exercices n°1

Arithmétique.

Exercice 1 (Nombres de Mersenne).

1. Soit a un entier, $a > 2$. Montrer que pour $n > 1$, $a^n - 1$ n'est pas premier.
2. Montrer que si $2^n - 1$ est premier, alors n est premier.

Exercice 2 (Nombres de Fermat). On définit pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.

1. Montrer que si $2^n + 1$ est un nombre premier, n est une puissance de 2.
2. Montrer que $5 \times 2^7 + 1$ divise $5^4 \times 2^{28} - 1$ et que $5^4 + 2^4$ divise $5^4 \times 2^{28} + 2^{32}$. En déduire que 641 divise F_5.
3. Montrer que pour tout couple (m, n) d'entiers distincts F_n et F_m sont premiers entre eux. (On pourra supposer que $n > m$ et utiliser l'identité $2^{2^n} + 1 = (2^{2^m})^{2^{n-m}} - (-1)^{2^{n-m}} + 2$.)

Exercice 3 (Triplets Pythagoriciens). On se propose de résoudre l'équation $x^2 + y^2 = z^2$ dans $\mathbb{N}^*$.

1. Soit (x, y, z) une solution telle que x, y et z sont premiers entre eux. Montrer qu'ils sont premiers entre eux deux à deux.
2. Montrer que x et y ne peuvent pas être impairs tous les deux. On supposera par exemple que x est pair.
3. Montrer que $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont des carrés d'entiers de parité différente et premiers entre eux.
4. En déduire l'ensemble des solutions.

Exercice 4. On se place dans l'espace euclidien orienté $\mathbb{R}^2$. On note $O = (0, 0)$ l'origine. On rappelle que étant donnés deux points A et B de $\mathbb{R}^2$ non alignés avec l'origine, le nombre $det(\overrightarrow{OA}, \overrightarrow{OB})$ est égal à l'aire algébrique du parallélogramme de sommets $O, A, B, O + \overrightarrow{OA} + \overrightarrow{OB}$ (en particulier, ce nombre est un entier pour $A, B \in \mathbb{Z}^2$). Deux points distincts A et B de $\mathbb{R}^2$ sont dits *visibles l'un de l'autre* si le segment ouvert $]A, B[$ ne contient aucun point de $\mathbb{Z}^2$ ($]A, B[\cap \mathbb{Z}^2 = \emptyset$).

1. Soit $A = (a, a') \in \mathbb{Z}^2 \setminus \{O\}$. Montrer que A est visible de l'origine O si et seulement si a et a' sont premiers entre eux.
2. On suppose les points $A = (a, a')$ et $B = (b, b')$ de $\mathbb{Z}^2$ visibles depuis O et non alignés avec O.
   a. En utilisant l'algorithme d'Euclide, montrer qu'il existe une matrice inversible $P \in \mathcal{M}_2(\mathbb{Z})$ telle que $\begin{pmatrix} a \\ a' \end{pmatrix} = P \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Soit $\begin{pmatrix} c \\ c' \end{pmatrix} = P^{-1} \begin{pmatrix} b \\ b' \end{pmatrix}$ et $C = (c, c') \in \mathbb{Z}^2$. On pose aussi $I = (1, 0) \in \mathbb{Z}^2$. Montrer que le nombre de points de $\mathbb{Z}^2$ situés à l'intérieur du parallélogramme de sommets $O, A, B, O + \overrightarrow{OA} + \overrightarrow{OB}$ est le même que le nombre de points de $\mathbb{Z}^2$ situés à l'intérieur du parallélogramme de sommets $O, I, C, O + \overrightarrow{OI} + \overrightarrow{OC}$
   b. En déduire que l'entier naturel $|\det(\overrightarrow{OA}, \overrightarrow{OB})|$ est égal au nombre de points de $\mathbb{Z}^2$ situés à l'intérieur du parallélogramme de sommets $O, A, B, O + \overrightarrow{OA} + \overrightarrow{OB}$ plus 1.
3. Si le point $A = (a, a') \in \mathbb{Z}^2$ est visible depuis O, décrire géométriquement les points $M = (m, m') \in \mathbb{Z}^2$ vérifiant la relation de Bézout $am' - ma' = \pm 1$.

Exercice 5 (Théorème de Wilson).
Soit n un entier au moins égal à 2. Montrer que $(n-1)!$ est congru modulo n à :

a) -1 si n est premier,

b) 2 si $n = 4$,

c) 0 sinon.

Exercice 6. Résoudre dans $\mathbb{Z}$ les deux systèmes de congruences suivants :

(1) $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}$ (2) $\begin{cases} x \equiv 4 \pmod{21} \\ x \equiv 10 \pmod{33} \end{cases}$

Exercice 7.

1. Quel est le dernier chiffre de 7777^{7777} ?
2. Quels sont les restes des divisions euclidiennes de 900^{2000} et de $101^{102^{103}}$ par 13 ?
3. Quel est le reste de la division euclidienne de $31^{32^{33}}$ par 7 ?
4. Quel est le reste de la division euclidienne de $100^{100^{100}}$ par 12 ?

Exercice 8.

1. Vérifier que 171 et 212 sont premiers entre eux.
2. Résoudre dans $\mathbb{Z}^2$: $212x + 171y = 1$.
3. Résoudre dans $\mathbb{Z}/212\mathbb{Z}$: $171x = 7$.

Exercice 9 (Résidus quadratiques).
Soit p un nombre premier impair. Une classe $a \in \mathbb{Z}/p\mathbb{Z}$ est un carré s'il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $a = x^2$. Un entier k est appelé *résidu quadratique modulo* p si sa classe $\overline{k}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

1. Donner les carrés modulo p pour $p \in \{3, 5, 7, 11, 13\}$.
2. Montrer qu'il y a exactement $\frac{1}{2}(p-1)$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   Indication : on pourra utiliser l'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\varphi(x) = x^2$.
3. Montrer que l'application $\varepsilon : (\mathbb{Z}/p\mathbb{Z})^* \to \{\overline{+1}, \overline{-1}\}$ définie par $\varepsilon(a) = a^{(p-1)/2}$ est un morphisme de groupes surjectif. En déduire que pour tout entier k, $\overline{k}$ est un carré modulo p si et seulement si $k^{(p-1)/2} \equiv 1 \pmod{p}$.
4. A quelle condition sur p, -1 est-il un résidu quadratique modulo p ?

L'expression $(\frac{k}{p})$ qui vaut 1 si k est résidu quadratique modulo p et -1 sinon s'appelle le *symbole de Legendre*.

Exercice 10. Résoudre les équations suivantes :

1. $x^2 + 4x - 1 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
2. $x^2 + 5x + 2 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
3. $x^2 + 6x - 13 = 0$ dans $\mathbb{Z}/21\mathbb{Z}$.
4. $x^2 + 3x + 2 = 0$ dans $\mathbb{Z}/6\mathbb{Z}$.
5. $x^2 + 4x + 6 = 0$ dans $\mathbb{Z}/9\mathbb{Z}$.

Exercice 11 (Système RSA).
Soit deux nombres premiers distincts p et q. On pose $n = pq$. Soit c un entier premier à $\varphi(n)$. Le couple (n, c) est appelé la *clé publique*.

1. Justifier l'existence d'un entier d tel que $cd \equiv 1 \pmod{\varphi(n)}$. On fixe un tel d, appelé *clé secrète*.
2. Montrer que pour tout $a \in \mathbb{Z}$, on a $a^{cd} \equiv a \pmod{n}$.