2. CONGRUENCES ET PETIT THÉORÈME DE FERMAT

Exercice 1. Écrire les tables de l'addition et de la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n=5$, $n=6$, $n=7$ et $n=8$. Dans chaque cas, déterminer tous les éléments inversibles, puis tous les éléments α de $\mathbb{Z}/n\mathbb{Z}$ tels que $\alpha^2=1$, puis enfin tous les éléments α tels que $\alpha^4=1$.

Exercice 2. Démontrer qu'un nombre entier de la forme $8k-1$ n'est jamais la somme de trois carrés.

Exercice 3. Soient a, b et c trois nombres entiers relatifs. Démontrer que, si $a^3+b^3+c^3$ est divisible par 7, alors nécessairement l'un des trois nombres a, b ou c est divisible par 7.

Exercice 4. Déterminer l'inverse de 8 modulo 43, puis l'inverse de 11 modulo 128.

Exercice 5. (*La fonction indicatrice d'Euler*) Étant donné un entier naturel $n\geq 1$, on rappelle que l'on note $\varphi(n)$ le nombre d'éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$; de manière équivalente, $\varphi(n)$ est le nombre d'entiers naturels m tels que

$$1\leq m\leq n \text{ et } \operatorname{pgcd}(n,m)=1.$$

L'application $\varphi:\mathbb{N}-\{0\}\to\mathbb{N}$ ainsi définie est la *fonction indicatrice d'Euler*.

1. Déterminer directement $\varphi(n)$ pour $1\leq n\leq 8$.
2. Soient n, n' deux entiers naturels non nuls et premiers entre eux. Démontrer que l'on a $\varphi(nn')=\varphi(n)\varphi(n')$.
3. Calculer $\varphi(p^k)$ pour tout nombre premier p et tout nombre entier naturel k.
4. Déduire des questions (ii) et (iii) une formule explicite pour $\varphi(n)$, quel que soit le nombre entier $n\geq 1$.
5. Calculer $\varphi(60)$ et $\varphi(100)$.
6. On va finalement montrer que, pour tout nombre entier $n\geq 1$,

$$\sum_{d|n}\varphi(d)=n,$$

la somme portant sur l'ensemble des entiers $d\geq 1$ divisant n.

Posons $\Phi(n)=\sum_{d|n}\varphi(d)$.

– Vérifier que $\Phi(nn')=\Phi(n)\Phi(n')$ pour tous n,n' tels que $\operatorname{pgcd}(n,n')=1$.
– Calculer $\Phi(p^k)$ pour tout nombre premier p et tout nombre entier naturel k.
– Conclure.

Exercice 6. (*Le théorème de Fermat-Euler, 1*) Démontrer que les quatre énoncés suivants sont équivalents.

1. Quel que soit le nombre premier p, $a^{p-1}\equiv 1 \pmod p$ pour tout nombre entier a tel que $p\nmid a$.
2. Quel que soit le nombre premier p, $a^p\equiv a \pmod p$ pour tout nombre entier a.
3. Quels que soient le nombre premier p et l'entier naturel $k\geq 1$, $a^{p^{k-1}(p-1)}\equiv 1 \pmod{p^k}$ pour tout nombre entier a tel que $p\nmid a$.
4. Quel que soit le nombre entier $n\geq 1$, $a^{\varphi(n)}\equiv 1 \pmod n$ pour tout nombre entier a tel que $\operatorname{pgcd}(a,n)=1$.

(*Indication : démontrer les implications* $1\Rightarrow 2\Rightarrow 3\Rightarrow 4\Rightarrow 1$. *Pour* $2\Rightarrow 3$, *raisonner par récurrence sur* k *en écrivant* $a^{p^{k-1}(p-1)}-1=A^p-1$ *avec* $A=a^{p^{k-2}(p-1)}$.)

Exercice 7. (*Le théorème de Fermat-Euler, 2*) Soit $n\geq 1$ un nombre entier et soit $a\in\mathbb{Z}$ premier avec n.

1. Notons M le produit de tous les entiers $m\in\{1,\dots,n-1\}$ tels que $\operatorname{pgcd}(n,m)=1$. En considérant la multiplication par a dans $\mathbb{Z}/n\mathbb{Z}$, démontrer que l'on a : $a^{\varphi(n)}M\equiv M \pmod n$.

2. En déduire le théorème de Fermat-Euler :

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

3. Déterminer le dernier chiffre de 13^{2009} dans l'écriture décimale. Même question avec $13^{100!}$.
4. Déterminer le dernier chiffre de 2007^{2008} dans l'écriture hexadécimale (c'est-à-dire en base 16).

Exercice 8. (*Le petit théorème de Fermat*) Soit p un nombre premier.

1. Démontrer que, pour tout entier $k \in \{1, \ldots, p-1\}$, p divise le coefficient binomial $\binom{p}{k}$.
2. En déduire que l'on a $(a+b)^p \equiv a^p + b^p \pmod{p}$ pour tous $a,\ b \in \mathbb{Z}$.
3. En déduire le petit théorème de Fermat :

$$\forall a \in \mathbb{Z},\ \ a^p \equiv a \pmod{p}.$$

Exercice 9. (*Le théorème RSA (Rivest-Shamir-Adleman, 1977)*) Soient p et q deux nombres premiers distincts. On pose $N = pq$ et on choisit un nombre entier $e > 1$ premier à $\varphi(N) = (p-1)(q-1)$.

1. Justifier qu'il existe un nombre entier d tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$.
2. Démontrer que, pour tout nombre entier a, $a^{ed} \equiv a \pmod{p}$ et $a^{ed} \equiv a \pmod{q}$.
3. En déduire que, pour *tout* nombre entier a,

$$a^{ed} \equiv a \pmod{N}.$$

Cette variante du théorème de Fermat-Euler est le fondement du système de cryptographie RSA, introduit par Ron Rivest, Adi Shamir et Len Adleman en 1977 et utilisé aujourd'hui de manière quasi universelle... Pour en savoir plus, voir la fiche complémentaire « Cryptographie » ainsi que les différents documents regroupés sur ma page personnelle [(1)]*, dont l'article original de Rivest, Shamir et Adleman.*

Exercice 10. (*Le théorème de Wilson, 1*) Soit p un nombre premier.

1. Déterminer tous les éléments α du corps $\mathbb{Z}/p\mathbb{Z}$ tels que $\alpha^2 = 1$.
2. En regroupant chaque élément avec son inverse, démontrer que le produit de tous les éléments non nuls du corps $\mathbb{Z}/p\mathbb{Z}$ est égal à -1.
3. En déduire le théorème de Wilson :

$$(p-1)! \equiv -1 \pmod{p}.$$

Exercice 11. (*Le théorème de Wilson, 2*) Soit p un nombre premier.

1. Démontrer que le polynôme $T^{p-1} - 1$ est scindé à racines simples sur le corps $\mathbb{Z}/p\mathbb{Z}$.
2. En déduire que l'on a : $(p-1)! \equiv -1 \pmod{p}$.
3. Démontrer qu'un nombre entier $n \geq 2$ est premier si et seulement si

$$(n-1)! \equiv -1 \pmod{n}.$$

[(1)] http ://math.univ-lyon1.fr/ thuillier/enseignements/ATN