Feuille d'exercices : Arithmétique

Dans toute cette feuille d'exercice, on appellera $\mathbb{P}$ l'ensemble des nombres premiers.

Exercice 1: (Différentes démonstrations du petit théorème de Fermat)

Petit théorème de Fermat : Si p est un nombre premier alors pour tout entier a qui n'est pas un multiple de p, $a^{p-1} \equiv 1 \pmod{p}$.

1. Soit $k \in [\![1; p-1]\!]$ et $ka = qp + r_k$ la division euclidienne de ka par p.
   (a) Justifier que $\forall i, j \in [\![1; p-1]\!]$, $i \neq j$, on a $r_1 \neq r_j$.
   (b) En considérant le produit $\prod_{k=1}^{p-1} ka \pmod{p}$, démontrer le petit théorème de Fermat.
2. (a) Montrer que $\forall k \in [\![1; p-1]\!]$, p divise $\binom{p}{k} = \frac{p!}{(p-k)!k!}$.
   (b) En déduire que pour tout $a \in \mathbb{N}$, on a $(1+a)^p \equiv 1 + a^p \pmod{p}$ puis $a^p \equiv a \pmod{p}$ et le petit théorème de Fermat.
3. Démontrer le petit théorème de Fermat en utilisant le théorème de Lagrange.

Exercice 2: (Une petite application)

Soit $p \in \mathbb{P}$.

1. Montrer qu'il existe $k \in \mathbb{N}^*$ tel que $2^k \equiv 1 \pmod{p}$.
2. Soient $k \in \mathbb{N}^*$ tel que $2^k \equiv 1 \pmod{p}$ et $n\mathbb{N}$. Montrer que si $k|n$ alors $2^n \equiv 1 \pmod{p}$.
3. Soit b le plus petit entier naturel tel que $2^b \equiv 1 \pmod{p}$. Montrer que si l'on a $2^n \equiv 1 \pmod{p}$ alors $b|n$.

Exercice 3: (Les nombres de Carmichaël)

On appelle nombre de Carmichaël un entier $ngeqslant2$, $n \notin \mathbb{P}$ tel que $\forall a$ tel que $a \wedge n = 1$ on a $a^{n-1} \equiv 1 \pmod{n}$

1. Montrer qu'un nombre de Carmichaël est impair.
2. Soit $a \in \mathbb{N}^*$ tel que $p_k = 6ka + 1 \in \mathbb{P}$ pour $p = 1, 2, 3$. Montrer que $n = p_1 p_2 p_3$ est un nombre de Carmichaël.
3. Montrer que la décomposition en facteurs premiers d'un nombre de Carmichaël ne comporte pas de facteurs premiers.
4. Soit $n \geqslant 3$. Montrer que si n est un nombre de Carmichaël si et seulement si $\exists r \geqslant 3$ et $3 \leqslant p_1 < p_2 < ... < p_r$ r nombres premiers tels que $n = \prod_{i=1}^{r} p_i$ et $\forall i \in [\![1; r]\!]$, on a $(p_i - 1)|(n-1)$.

Exercice 4: (Les nombres parfaits)

On appelle nombre parfait, un nombre qui est égal à la somme de ses diviseurs autres que lui-même.
Exemples : $6 = 1 + 2 + 3$ et $28 = 1 + 2 + 4 + 7 + 14$.

1. Soient $(a, n) \in \mathbb{N}$ avec $a \geqslant 2$ et $n \geqslant 2$. Montrer que si $a^n - 1 \in \mathbb{P}$ alors $a = 2$ et $n \in \mathbb{P}$.
2. $\forall n \in \mathbb{N}^*$ on note $\sigma(n) = \sum_{\substack{d \in [\![1;n]\!] \\ d|n}} d$ et $n = d_1^{\alpha_1} d_2^{\alpha_2} ... d_k^{\alpha_k}$ la décomposition en facteurs premiers de n. Exprimer $\sigma(n)$ en fonction de d_1, d_2,...,d_k.
3. Montrer que si $n \wedge m = 1$ alors $\sigma(nm) = \sigma(n)\sigma(m)$.
4. Montrer que si $2^p - 1$ est premier alors $2^{p-1}(2^p - 1)$ est parfait.
5. Montrer qu'un nombre parfait pair est de la forme $n = 2^{p-1}(2^p - 1)$.

Exercice 5: (Critère d'Eisenstein)

Soit $P \in \mathbb{Z}[X]$, $P = \sum_{k=0}^{n} a_k X^k$.
Si il existe $p \in \mathbb{P}$ tel que

— $p|a_k$ pour $k \in [\![0; n-1]\!]$.
— $p \nmid a_n$.
— $p^2 \nmid a_0$.

Alors P est irréductible sur $\mathbb{Q}[X]$.