CPI1A

TD11 : Arithmétique

**Exercice 1 :** Soient $X$ un ensemble infini et $\mathbb{K}$ un corps. On considère $A = \mathcal{F}(X, \mathbb{K})$ l'anneau des applications de $X$ dans $\mathbb{K}$. Pour $f \in A$ on note $supp(f) = \{x \in X, tel\ que\ f(x) \neq 0\}$. On considère les parties de $A$ suivantes : $X^{(\mathbb{K})} = \{f \in A, tel\ que\ supp(f)\ est\ fini\}$ et pour $x_0 \in X$, $I_{x_0} = \{f \in A, tel\ que\ \ f(x_0) = 0\}$.

1. Montrer que $I_{x_0}$ est un idéal principal de $A$ .
2. Montrer que $X^{(\mathbb{K})}$ est un idéal non principal de $A$.

**Exercice 2 :** Déterminer, pour $n \in \mathbb{N}$ les restes de la division euclidienne de $4^n$ par 7.

**Exercice 3** : Soient $a, b \in \mathbb{N}^*$.

1. Montrer que : $\sqrt{a}$ est un entier ou un irrationnel.
2. Soit $a$ un entier $\geq 1$. Montrer que $a$ est carré entier si et seulement si $\forall p$ un nombre premier $v_p(a)$ est pair. ( $v_p(a)$ valuation p-adique de $a$).
3. En déduire que si $a$ et $ab$ sont des carrés des entiers alors $b$ est carré d'un entier.

**Exercice 4** :

1. Montrer que: $\forall n \in \mathbb{N}, (n+1) \wedge (2n+1) = 1$, en déduire que $n+1$ divise $C_{2n}^n$
2. Montrer que: Soit $n$ un entier naturel non nul. Montrer que :

$$(n^2+n) \ \wedge ( \ 2n+1) = 1 \text{ et } (n^2+1) \wedge ((n+1)^2+1) \in \{1, 5\} .$$

**Exercice 5 :**

1. Soit $\mathbb{K}$ un corps fini. Montrer que : $-1 = \prod_{x \in \mathbb{k}^*} x$
2. Soit $n$ un enrier $\geq 2$.Déduire que : $n$ est premier si et seulement si $(n-1)! \equiv -1\,[n]$ (théorème de Wilson).
3. soit $p$ un nombre premier.
   (a) Montrer que pour tout $k \in \{1,...,p-1\}$, $p | C_p^k$.
   (b) Déduire que $\forall\,(a,b) \in \mathbb{Z}^2$, $(a+b)^p = a^p + b^p\,[p]$ .
   (c) Si $p \geq 3$ , $n$ un entier naturel . Montrer que: $(1+p)^{p^n} \equiv \ 1 + p^{n+1} \ \left[p^{n+2}\right]$ .

**Exercice 6 :**

Soient $a, n, m$ des entiers $\geq 1$ avec $a \geq 2$ et $n \leq m$.

1. Soit $r$ le reste de la division euclidienne de $m\ par\ \ n$ , montrer que $a^r - 1$ est le reste de la division euclidienne de $a^m - 1$ par $a^n - 1$.
2. A quelle condition $a^n - 1$ divise $a^m - 1$ ?
3. Montrer que : $( a^m - 1) \wedge (a^n - 1 \ ) = a^d - 1$ où $d = m \wedge m$.

**Exercice 7 :**

1. Montrer que $11 | 2^{123} + 3^{121}$
2. Soit $a$ et $b$ deux entiers non nuls. Montrer que: $7|\ a^2 + b^2 \Longleftrightarrow 7|\ a$ et $7|\ b$.
3. Résoudre dans $\mathbb{Z}^2$ : $3x - 11y = 10$ .
4. Résoudre dans $\mathbb{Z}$ le système: $\left\{ \begin{array}{l} x \equiv 1\ [3] \\ x \equiv 3\ [4] \end{array} \right.$ .

**Exercice 8 :** Soit $n \in \mathbb{N}^*$.

1. Montrer que 5 divise $2^{4n+2} + 1$.
2. On suppose que $n \geq 2$.
   a. Montrer que : 5 divise $2^{2n+1} + 1 + 2^{n+1}$ ou $2^{2n+1} + 1 - 2^{n+1}$.
   b. En déduire que : $\frac{1}{5}(2^{4n+2} + 1)$ n'est pas un nombre premier.

**Exercice 9 :** Soit $a \in \mathbb{Z}$.

1. On suppose que $a$ impair, montrer que $a$ est la différence de deux carrés entiers.
2. On suppose que $a$ pair. Montrer que $a$ est la différence de deux carrés entiers si et seulement si $a \equiv 0[4]$.

**Exercice 10 :**

1. Soient $a, b, n, m \in \mathbb{N}^*$. Montrer que : $a \wedge b = 1 \Leftrightarrow a^n \wedge b^m = 1$.
2. Soient $a, b \in \mathbb{Z}$ et $l \in \mathbb{N}$, montrer que : $(a \wedge b)^l = a^l \wedge b^l$.

**Exercice 11 :** Soit $n \in \mathbb{N}^*$, on dit que $n$ est parfait si la somme des diviseurs positifs de $n$ est $2n$.

1) Exemple: vérifier que 28 est un nombre parfait.

Pour $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme des diviseurs positifs de $n$.

2) Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $p_i$ des nombres premiers deux à deux distincts.

En développant le produit suivant: $\prod_{i=1}^{r} \left( \sum_{\beta_i=0}^{\alpha_i} p_i^{\beta_i} \right)$, montrer que $\prod_{i=1}^{r} \frac{p_i^{1+\alpha_i}-1}{p_i-1} = \sigma(n)$.

3) Déduire que si $n, m \in \mathbb{N}^*$ et $n \wedge m = 1$, alors $\sigma(nm) = \sigma(n)\sigma(m)$.

4) Soient $d, n \in \mathbb{N}^*$, montrer que si $d$ divise $n$ alors $2^d - 1$ divise $2^n - 1$.

5) En déduire que si $2^n - 1$ est premier alors $n$ est premier.

6) Soit $n \in \mathbb{N}^*$, montrer que $2^{n-1} \wedge (2^n - 1) = 1$.

7) En déduire que si $p$ est premier et $2^p - 1$ est premier alors $2^{p-1}(2^p - 1)$ est parfait.

Dans la suite $n \in \mathbb{N}^*$ désigne un nombre parfait pair.

8) Montrer qu'il existe un entier $a > 1$ et $q$ impair tel que $n = 2^{a-1}q$.

9) Vérifier que $(2^a - 1)\sigma(q) = 2^a q$ et déduire qu'il existe $b \in \mathbb{N}^*$ tel que: $q = (2^a - 1)b$.

10) Déduire que: $\sigma((2^a - 1)b) = 2^a b$.

11) Soit $x \in \mathbb{N}^*$ tel que $x > 1$ et $\sigma(xb) = xb + b$, montrer que $b = 1$ puis $x$ premier.

12) En déduire que $n = 2^{a-1}(2^a - 1)$ avec $2^a - 1$ premier et $a$ premier.

**Exercice 12 :** Soit $p$ un nombre premier et $n$ un entier $\geq p$. On propose de montrer que : $C_n^p - E\left(\frac{n}{p}\right)$ est divisible par $p$. On considère la division euclidienne de $n$ par $p$ : $n = pq + r$ .

1. Etablir une relation entre $E\left(\frac{n}{p}\right)$ *et* $q$.
2. Montrer que : $p!\, C_n^p = pq \prod_{k=1}^{r}(pq + k) \prod_{k=r+1}^{p-1}(pq - p + k)$.
3. En déduire que : $(p-1)!\, C_n^p \equiv q(p-1)!\, [p]$
4. Conclure.

**Exercice 13** : (Equation de Fermat)

On cherche les triplets $(x, y, z) \in (\mathbb{N}^*)^3$ tel que : $x^2 + y^2 = z^2$.

1. Montrer que l'on peut se ramener au cas $pgcd(x, y, z) = 1$. On suppose dans la suite $pgcd(x, y, z) = 1$.
2. Montrer que $x$ *et* $y$ ont des parités différentes.
3. On suppose que $x$ est pair.
   a. Soit $d \in \mathbb{N}^*$ tel que $d^2$ divise $x^2$, montrer que $d$ divise $x$ . (on pourra utiliser exercice3).
   b. Montrer que : $pgcd(z - y, z + y) = 2$.
   c. Montrer l'existence $(m, n) \in (\mathbb{N}^*)^2$ premier entre eux tel que : $z + y = 2m^2$ *et* $z - y = 2n^2$.
   d. En déduire l'existence $(m, n) \in (\mathbb{N}^*)^2$ premier entre eux tel que : $x = 2mn$ ,$y = m^2 - n^2$ et $z = m^2 + n^2$.