Examen

ARITHMÉTIQUE

Les calculatrices et les documents sont interdits.

La rédaction sera prise en compte dans la notation.

Cours et application. (7 points=2,5+1+1,5+2)

La notation $\dot{x}$ désigne la classe de x dans l'ensemble quotient considéré.

- 1) Expliquer le principe du codage RSA.
- 2)a) A quelle condition nécessaire et suffisante a-t-on: "il existe $u \in \mathbb{Z}$ tel que $\dot{u}.\dot{x} = \dot{1}$ dans $\mathbb{Z}/n\mathbb{Z}$ "?
- b) Le démontrer.
- c) Trouver l'inverse de 51 dans $\mathbb{Z}/106\mathbb{Z}$.

Exercice 1. (4 points=1,5+1,5+1)

La notation $[x]_n$ désigne la classe de x dans l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$. On cherche à trouver tous les $x \in \mathbb{Z}$ tels que

$$x \equiv 1 [3] \quad \text{et} \quad x \equiv -1 [4] \quad \text{et} \quad x \equiv 2 [5]$$

ou encore (avec une formulation équivalente)

$$[x]_3 = [1]_3 \quad \text{et} \quad [x]_4 = [-1]_4 \quad \text{et} \quad [x]_5 = [2]_5$$

1) Montrer que si $x_0 \in \mathbb{Z}$ est une solution particulière alors l'ensemble des solutions est $x_0 + 60\mathbb{Z} = \{x_0 + 60k \mid k \in \mathbb{Z}\}$.

2) Trouver

- $b_1 \in \mathbb{Z}$ tel que la classe de $20.b_1$ soit $[1]_3$ dans $\mathbb{Z}/3\mathbb{Z}$?
- $b_2 \in \mathbb{Z}$ tel que la classe de $15.b_2$ soit $[1]_4$ dans $\mathbb{Z}/4\mathbb{Z}$?
- $b_3 \in \mathbb{Z}$ tel que la classe de $12.b_3$ soit $[1]_5$ dans $\mathbb{Z}/5\mathbb{Z}$?

3) Conclure en considérant $a = 20b_1 - 15b_2 + 24b_3$.

Exercice 2. (11 points=(1,5+1,5)+1+(1+1,5)+(0,5+0,5)+1+1+1,5)

On note $\mathcal{P} = \{p_k | k \geq 1\}$ l'ensemble des nombres premiers, avec $p_k < p_{k+1}$. Ainsi $p_1 = 2$, $p_2 = 3, \dots$. On veut démontrer (avec une preuve différente du cours) que la série des inverses des p_k diverge. On suppose le contraire.

1)a) Justifier que tout entier $n \geq 1$ s'écrit a^2b où $a, b \in \mathbb{N}$ et b est un produit de termes $p_i^{\varepsilon_i}$ où les $\varepsilon_i \in \{0, 1\}$ et sont nuls à partir d'un certain rang.

b) Montrer que b n'est divisible par aucun carré de nombre premier et que cette écriture est unique.

Pour $N \in \mathbb{N}$ avec $N \geq 1$, et $j \geq 1$ on note

$$\mathcal{E}_j(N) = \left\{ 1 \leq n \leq N \mid n \text{ n'est divisible par aucun des } p_i \text{ où } i > j \right\}$$

Enfin, $C_j(N) = \text{card}(\mathcal{E}_j(N))$.

2) Soit $n \in \mathcal{E}_j(N)$. On sait que n a une écriture comme dans la question 1. Justifier que $a \leq \sqrt{N}$ et que b est un élément de $\left\{ \prod_{i=1}^j p_i^{\varepsilon_i} \mid \varepsilon_i \in \{0, 1\} \right\}$.

3)a) Montrer que l'application F suivante est bien définie et injective:

$$\left| \begin{array}{ll} \mathcal{E}_j(N) & \longrightarrow \{1, \dots, \sqrt{N}\} \times \left\{ \prod_{i=1}^j p_i^{\varepsilon_i} \mid \varepsilon_i \in \{0, 1\} \right\} \\ n & \longmapsto (a, b) \end{array} \right.$$

b) En déduire que $C_j(N) \leq \sqrt{N} \cdot 2^j$.

4)a) Montrer que le complémentaire de $\mathcal{E}_j(N)$ dans $\{1, \dots, N\}$ est l'ensemble

$$\bigcup_{k>j} \{1 \leq n \leq N \mid p_k \text{ divide } n\}.$$

b) Justifier qu'il existe $j_N > j$ tel que: pour tout $k > j_N$, on a $\{1 \leq n \leq N \mid p_k \text{ divide } n\} = \emptyset$.

5) En déduire que $N - C_j(N) \leq N \cdot \sum_{j < k < j_N} \frac{1}{p_k}$ (où j_N est celui de la question précédente).

6) Que vaut $\limsup_{j \rightarrow \infty} \sum_{j' > j} \sum_{k=j+1}^{j'} \frac{1}{p_k}$?

7) Conclure (en soignant la rédaction).