DM n°25

Facultatif : verso.

Exercice 1. Soit $P \in \mathbb{C}[X]$. On note $D = \text{pgcd}(P, P')$.

1. Pour $P = (X-1)^3(X-2)^4$, calculer P' et expliciter D.
2. Exprimer $\deg D$ en fonction de $n = \deg P$ et du nombre r de racines distinctes de P. Justifier.
3. En déduire quels sont les polynômes unitaires $P \in \mathbb{C}[X]$ tels que $P' \mid P$.

Exercice 2. Théorème de Sophie-Germain.

I. Soit $q > 5$ un nombre premier.

1) Soit $a \in \mathbb{Z}$. Que dire du reste de a^{q-1} modulo q ?

2) Déterminer tous les entiers $x \in [\![1, q-1]\!]$ tels que $x^2 \equiv 1[q]$.

3) En déduire que si $a, b, c \in \mathbb{Z}$ satisfont

$$a^{\frac{q-1}{2}} + b^{\frac{q-1}{2}} + c^{\frac{q-1}{2}} \equiv 0[q]$$

alors q divise abc.

II. Soit p un nombre premier p tel que $q = 2p+1$ soit aussi un nombre premier.

L'objectif est de montrer que l'équation diophantienne $x^p + y^p + z^p = 0$ n'a pas de solution non triviale.

On considère un triplet d'entiers $(x, y, z) \in \mathbb{Z}^3$ tel que $x^p + y^p + z^p = 0$ et que p ne divise pas xyz.

1) Justifier qu'il suffit de traiter le cas où $\text{pgcd}(x, y, z) = 1$. On fait cette hypothèse dans la suite.

2) Montrer que $y + z$ et $\sum_{k=0}^{p-1}(-y)^k z^{p-1-k}$ sont premiers entre eux.

3) Montrer que pour $u, v \in \mathbb{N}^*$, si $u \wedge v = 1$ et uv est une puissance p-ème, alors u et v sont des puissances p-ème.

4) En déduire qu'il existe $a, u \in \mathbb{Z}$ tels que $a \wedge u = 1$ et

$$y + z = a^p \quad \text{et} \quad \sum_{k=0}^{p-1}(-1)^k y^k z^{p-1-k} = u^p$$

De même, il existe $b, c \in \mathbb{Z}$ tels que $x + y = b^p$ et $x + z = c^p$.

5) Montrer que q divise au moins l'un des trois entiers x, y ou z.

Dans la suite, on suppose que q divise x.

6) Montrer que q divise abc puis que q divise a.

7) En considérant u^p et b^p modulo q, aboutir à une contradiction.

Exercice 3. Pour $n \geqslant 2$, on note $\mathcal{P}(n)$ l'ensemble des nombres premiers inférieurs ou égaux à n et $\pi(n)$ le cardinal de $\mathcal{P}(n)$.

I. Inégalité de Erdös

1) En remarquant que $\binom{2n}{n}$ est le plus grand des coefficients binomiaux $\binom{2n}{k}$, montrer que pour $n \geqslant 1$, on a $\frac{4^n}{2n+1} \leqslant \binom{2n}{n} \leqslant 4^n$ et $\binom{2n+1}{n} \leqslant 4^n$.

2) Montrer que si $n+1 < p \leqslant 2n+1$ est un nombre premier, p divise $\binom{2n+1}{n}$. En déduire que pour $n \geqslant 2$, on a

$$\prod_{p \in \mathcal{P}(2n+1) \setminus \mathcal{P}(n+1)} p \leqslant 4^n.$$

Puis que $\pi(2n) - \pi(n) \leqslant \frac{n \ln 4}{\ln n}$.

3) En discutant selon la parité de n, montrer par récurrence que

$$\prod_{p \in \mathcal{P}(n)} p \leqslant 4^{n-1}.$$

II. Théorème de Legendre

1) Soit a, b deux entiers positifs non nuls. Montrer que le nombre de multiples non nuls de a inférieurs ou égaux à b est $E(\frac{b}{a})$, où $E(x)$ est la partie entière de x.

2) Si p est un nombre premier et n un entier, on note $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. Montrer que

$$v_p(n!) = \sum_{k=1}^{n} v_p(k) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right).$$

Noter que dans la dernière somme, les termes sont nuls à partir d'un certain rang.

3) Application : quel est le nombre de 0 à la fin de 100! ?

III. Théorème de Tchébycheff

1) Soit p un nombre premier. Déterminer $v_p(\binom{2n}{n})$ si $\frac{2n}{3} < p \leqslant n$ et si $\sqrt{2n} < p \leqslant \frac{2n}{3}$.

2) En utilisant $\binom{2n}{n} = \prod_{p\in\mathcal{P}(2n)} p^{v_p(\binom{2n}{n})}$, montrer que

$$\prod_{p\in\mathcal{P}(2n)\setminus\mathcal{P}(n)} p \geqslant \frac{4^n}{2n+1}\frac{1}{4^{2n/3-1}(2n)^{\sqrt{2n}+1}}.$$

3) En déduire une minoration de $\pi(2n)-\pi(n)$ et une version faible du théorème de Tchébycheff : pour n assez grand, il existe un nombre premier entre n et $2n$.

Exercice 4. Soit P un polynôme à coefficients entiers non constant, montrer que l'ensemble des nombres premiers p qui divisent un des $P(n)$, $n \in \mathbb{N}$ est infini.

Exercice 5. ★ *Centrale.* Soit $\varphi\colon \mathbb{N} \to \mathbb{R}$ telle que $\varphi(0) = 0$, $\varphi(1) = 1$ et $\forall n \in \mathbb{N}$, $\varphi(2n) = \varphi(n)$ et $\varphi(2n+1) = \varphi(n) + \varphi(n+1)$.

1. Montrer que $\forall n \in \mathbb{N}$, $\varphi(n) \wedge \varphi(n+1) = 1$.

2. Montrer que si $a \wedge b = 1$, il existe $n \in \mathbb{N}$ tel que $a = \varphi(n)$ et $b = \varphi(n+1)$.

3. Montrer que $n \mapsto (\varphi(n), \varphi(n+1))$ réalise une bijection de $\mathbb{N}$ sur l'ensemble des couples d'entiers premiers entre eux.

Exercice 6. ★ Soit $n \geqslant 2$ et $a_1, \dots, a_n$ des éléments de $\mathbb{Z}$ deux à deux distincts. Montrer que le polynôme $P = (X-a_1)\dots(X-a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 7. ★ *X 2022.* Soit $p \geqslant 3$ premier et $t \in \mathbb{N}^*$. On considère $p_1, \dots, p_r$ des nombres premiers congrus à 1 modulo p^t. On pose $a = 2p_1 \dots, p_r$ et $c = a^{p^{t-1}}$.

1. Montrer que $c \equiv 2[p]$.

2. Montrer que $m = 1 + c + \dots + c^{p-1}$ et $c-1$ sont premiers entre eux.

3. Soit q un facteur premier de m. Montrer que $q \equiv 1[p^t]$.

4. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo p^t.

Exercice 8. ★ *ENS 2023.*

1. CNS sur n pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps.

2. On suppose cette condition satisfaite. Combien y a-t-il de polynômes de degré $d \in \mathbb{N}$ fixé dans $\mathbb{Z}/n\mathbb{Z}$?

3. Soit p premier. Montrer qu'il existe des polynômes irréductibles de degré 2 et 3 dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 9. ★ *X MP 2024.* Quels sont les $m \in \mathbb{N}^*$ tels qu'il existe m éléments consécutifs de $\mathbb{N}^*$ divisibles par des cubes d'éléments de $\mathbb{N}^*\setminus\{1\}$?

Indications Exercice 1.

2. On trouve $\deg D = \deg P - r$.

Indications Exercice 2.

II. 1) On veut montrer que l'équation n'a pas de solutions. Pour cela on considère une solution, et on aboutit à une contradiction. Est-il possible, à partir d'une solution (x, y, z), d'en construire une nouvelle (x', y', z') vérifiant $\operatorname{pgcd}(x', y', z') = 1$.

2) Si d est un diviseur de $y+z$, alors $y \equiv -z[d]$.

Indications Exercice 3.

I. 1) Considérer $\sum_{k=0}^{2n}\binom{2n}{k}$.

II. 2) Une possibilité est de justifier que $v_p(n!) = \sum_{k=1}^{+\infty} k\left(\left\lfloor\frac{n}{p^k}\right\rfloor - \left\lfloor\frac{n}{p^{k+1}}\right\rfloor\right)$

Indications Exercice 4. Procéder comme dans la preuve de l'infinité des nombres premiers. Commencer éventuellement par le cas où $P(0) = 1$.

Indications Exercice 6. Écrire $P = AB$, évaluer en a_i. Introduire un polynôme C à partir de A et B, qui a beaucoup de racines.

Indications Exercice 8. Devrait faire intervenir la notion d'ordre, d'une manière ou d'une autre : si $a^k \equiv 1[p]$ alors k est divisible par l'ordre de a, qui est un diviseur de $p-1$.

Indications Exercice 9. Lemme chinois