

Plaquette 3 – Nombres premiers, valuations et factorielles

Arithmétique dans $\mathbb{Z}$ — Licence 1 (L1)

Exercices

Méthode

Les nombres premiers se manipulent avec trois outils : le **lemme d'Euclide** ($p \mid ab \Rightarrow p \mid a$ ou $p \mid b$), la **décomposition unique** lue exposant par exposant (la **valuation** v_p), et les **arguments de reste** (modulo 3, 4, 6, 8) qui limitent les formes possibles. On démontre des résultats classiques (infinité de premiers dans certaines classes, formule de Legendre, théorème de Wilson) et on les contrôle sur des exemples chiffrés.

Exercice 1 – Premiers de la forme $4k + 3$

- Rappeler la démonstration d'Euclide : il existe une infinité de nombres premiers.
- Montrer qu'un produit d'entiers tous congrus à 1 modulo 4 est congru à 1 modulo 4.
- Supposons qu'il n'y ait qu'un nombre fini de premiers congrus à 3 modulo 4, notés $p_1, \dots, p_k$. On pose $N = 4p_1p_2 \cdots p_k - 1$. Montrer que N a un facteur premier congru à 3 modulo 4 et conclure.
- Pourquoi la même méthode échoue-t-elle telle quelle pour les premiers congrus à 1 modulo 4 ?

Exercice 2 – Test de primalité par la racine

- Montrer que tout entier $n \geq 2$ non premier admet un diviseur premier p tel que $p^2 \leq n$.
- 221 est-il premier ? Et 223 ?
- Combien de divisions au plus faut-il pour tester $n = 10\,007$? (On sait que $\sqrt{10\,007} \approx 100,03$ et qu'il y a 25 nombres premiers inférieurs à 100.)
- Montrer que si $n > 1$ n'a aucun diviseur premier $\leq \sqrt[3]{n}$, alors n est premier ou produit de deux premiers.

Exercice 3 – Longues suites de nombres composés

- Soit $n \geq 2$. Montrer que les $n - 1$ entiers $n! + 2, n! + 3, \dots, n! + n$ sont tous composés.
- En déduire qu'il existe des intervalles aussi longs que l'on veut sans nombre premier.
- Donner explicitement cinq entiers consécutifs composés à l'aide de $6!$, puis en trouver cinq plus petits en cherchant à la main.
- Ce résultat contredit-il l'infinité des nombres premiers ?

Exercice 4 - Formule de Legendre

Soit p premier et $n \geq 1$.

- Montrer que le nombre d'entiers de $\{1, \dots, n\}$ divisibles par p^k est $\left\lfloor \frac{n}{p^k} \right\rfloor$.
- En déduire la formule $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$ (on comptera, pour chaque $m \leq n$, sa contribution $v_p(m)$).
- Par combien de zéros se termine l'écriture décimale de $100!$?
- Calculer $v_2(100!)$ et comparer avec c).

Exercice 5 - Binôme modulo p et Fermat

Soit p premier.

- Montrer que pour $1 \leq k \leq p-1$, p divise $\binom{p}{k}$ (on utilisera $k \binom{p}{k} = p \binom{p-1}{k-1}$).
- En déduire que $(a+b)^p \equiv a^p + b^p \pmod{p}$ pour tous entiers a, b .
- Démontrer par récurrence sur $a \in \mathbb{N}$ le **petit théorème de Fermat** : $a^p \equiv a \pmod{p}$.
- Contrôler avec $p = 5, a = 3$ puis $p = 7, a = 2$. Montrer que a) est faux pour $p = 4$.

Exercice 6 - Nombres de Fermat

Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ ($F_0 = 3, F_1 = 5, F_2 = 17, \dots$).

- Montrer que $F_{n+1} - 2 = (F_n - 2)F_n$, puis que $F_0 F_1 \cdots F_{n-1} = F_n - 2$.
- En déduire que deux nombres de Fermat distincts sont premiers entre eux.
- En déduire une nouvelle preuve de l'infinité des nombres premiers.
- Fermat pensait que tous les F_n sont premiers. Vérifier que $641 \times 6\,700\,417 = F_5$ (Euler, 1732).

Exercice 7 - Nombre de diviseurs

- Justifier que si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, les diviseurs positifs de n sont les $p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$, et que leur nombre est $d(n) = (\alpha_1 + 1) \cdots (\alpha_r + 1)$.
- Montrer que $d(n)$ est impair si et seulement si n est un carré parfait.
- Déterminer le plus petit entier ayant exactement 12 diviseurs.
- Application : dans un couloir, 100 portes fermées numérotées de 1 à 100 ; la personne numéro k change l'état des portes multiples de k , pour $k = 1, \dots, 100$. Quelles portes sont ouvertes à la fin ?

Exercice 8 - Identité de Sophie Germain

- Vérifier que pour tout réel n , $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$.
- En déduire les entiers naturels n pour lesquels $n^4 + 4$ est premier.
- Plus généralement, factoriser $a^4 + 4b^4$ et montrer que $n^4 + 4^n$ n'est jamais premier

pour $n \geq 2$.

d) Montrer que $n^2 - 1$ est premier si et seulement si $n = 2$ (pour $n \in \mathbb{N}$).

Exercice 9 - Carré d'un premier modulo 24

Soit $p \geq 5$ un nombre premier.

a) Montrer que $p \equiv \pm 1 \pmod{6}$.

b) Montrer que $8 \mid p^2 - 1$ (on écrira $p^2 - 1 = (p - 1)(p + 1)$ avec p impair).

c) Montrer que $3 \mid p^2 - 1$ et conclure : $24 \mid p^2 - 1$.

d) En déduire que si p et q sont deux premiers ≥ 5 , alors $24 \mid p^2 - q^2$. Contrôler avec $p = 11$, $q = 7$.

Exercice 10 - PGCD et PPCM par les valuations

a) Montrer que pour tous $a, b \geq 1$ et tout premier p , $\min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) = v_p(a) + v_p(b)$. En déduire $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = ab$.

b) Calculer pgcd et ppcm de $a = 2^3 \times 3^4 \times 7$ et $b = 2^5 \times 3 \times 5^2$.

c) Montrer que $\text{pgcd}(a^2, b^2) = \text{pgcd}(a, b)^2$.

d) Montrer que $a \mid b \Leftrightarrow a^2 \mid b^2$. La même équivalence vaut-elle pour $a^2 \mid b^3$ et $a \mid b$?

Exercice 11 - Triplets de premiers

a) Montrer que si p , $p + 2$ et $p + 4$ sont tous premiers, alors $p = 3$.

b) Montrer que si p et $p^2 + 2$ sont premiers, alors $p = 3$.

c) Montrer que si p et $8p^2 + 1$ sont premiers, alors $p = 3$, et vérifier que $8 \times 9 + 1$ est premier.

d) Quel est le point commun des trois démonstrations ?

Exercice 12 - Premiers entre n et $2n$

Soit $n \geq 1$ et $N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$.

a) Soit p premier avec $n < p \leq 2n$. Montrer que $p \mid (2n)!$ et $p \nmid (n!)^2$, et en déduire $p \mid N$.

b) En déduire que $\prod_{n < p \leq 2n} p$ divise N .

c) Montrer que $N \leq 4^n$ (utiliser $\sum_k \binom{2n}{k} = 4^n$). En déduire $\prod_{n < p \leq 2n} p \leq 4^n$.

d) Vérifier pour $n = 5$ et $n = 10$.

Exercice 13 - Diviseurs premiers de $n^2 + 1$

Soit p un nombre premier **impair** qui divise $n^2 + 1$ pour un certain entier n .

a) Montrer que $p \nmid n$ et que $n^2 \equiv -1 \pmod{p}$.

- b) En élevant à la puissance $\frac{p-1}{2}$ et en utilisant Fermat, montrer que $(-1)^{(p-1)/2} = 1$, puis que $p \equiv 1 \pmod{4}$.
- c) Vérifier sur les facteurs premiers de $n^2 + 1$ pour $n = 4, 5, 8, 12$.
- d) En déduire qu'il existe une infinité de nombres premiers $p \equiv 1 \pmod{4}$ (considérer $N = (2p_1 \cdots p_k)^2 + 1$).

Exercice 14 - Valuation 2-adique d'une puissance de 3

Pour $n \in \mathbb{N}$, on pose $u_n = 3^{2^n} - 1$ ($u_0 = 2$, $u_1 = 8$, $u_2 = 80$).

- a) Montrer que $u_{n+1} = u_n(3^{2^n} + 1)$.
- b) Montrer que pour $n \geq 1$, $3^{2^n} \equiv 1 \pmod{4}$, puis que $v_2(3^{2^n} + 1) = 1$.
- c) En déduire que $v_2(u_n) = n + 2$ pour tout $n \geq 1$. Que vaut $v_2(u_0)$?
- d) Contrôler pour $n = 1, 2, 3$.

Exercice 15 - Synthèse : théorème de Wilson

Soit p un nombre premier.

- a) Montrer que l'équation $x^2 \equiv 1 \pmod{p}$ a pour seules solutions $x \equiv \pm 1 \pmod{p}$. Est-ce vrai modulo 8 ?
- b) Pour $p \geq 3$, montrer que les éléments $2, 3, \dots, p-2$ se regroupent en paires $\{x, x'\}$ avec $xx' \equiv 1 \pmod{p}$ et $x \neq x'$.
- c) En déduire le **théorème de Wilson** : $(p-1)! \equiv -1 \pmod{p}$.
- d) Vérifier pour $p = 5, 7$ et 11 . Montrer que si $n \geq 6$ n'est pas premier, alors $(n-1)! \equiv 0 \pmod{n}$: la congruence de Wilson **caractérise** les nombres premiers.