Agrégation externe

Nombres premiers

Ce problème est en relation avec les leçons d'oral suivantes :

- 120 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 121 Nombres premiers. Applications.
- 123 Corps finis. Applications.

On pourra consulter les ouvrages suivants.

- V. Beck, J. Malick, G. Peyre. *Objectif Agrégation.* H et K (2004).
- O. Bordelles. *Thèmes d'arithmétique.* Ellipses (2006).
- J. M. De Koninck, A. Mercier. *1001 problèmes en théorie classique des nombres.* Ellipses. (2003).
- M. Demazure. *Cours d'algèbre.* Cassini. (1997).
- S. Francinou, H. Gianella, S. Nicolas. *Oraux X-ENS. Algèbre 1.* Cassini (2009).
- X. Gourdon. *Les Maths en tête. Algèbre.* Ellipses.
- D. Perrin. *Cours d'algèbre.* Ellipses (1996).
- J. P. Ramis, A. Warusfel. *Mathématiques tout en un pour la licence. L1, L2, L3.* Dunod.
- F. Moulin, J. P. Ramis, A. Warusfel. Cours de m*athématiques pures et appliquées. Algèbre et géométrie.* De Boeck. (2010).
- P. Tauvel. *Mathématiques générales pour l'agrégation.* Masson (1993).

– I – Répartition des nombres premiers

On note $(p_n)_{n\in\mathbb{N}}$ la suite strictement croissante des nombres premiers et $\mathcal{P}$ l'ensemble des nombres premiers.

Pour tout entier naturel non nul n, on note :

$$\mathcal{P}_n = \mathcal{P} \cap [1, n]$$

l'ensemble des nombres premiers compris entre 1 et n.

Le théorème des nombres premiers (de démonstration délicate) nous dit que :

$$\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln(n)}$$

1. En admettant le théorème des nombres premiers montrer que :

$$p_n \underset{n\to+\infty}{\sim} n\ln(n)$$

2. Quelle est la nature de la série $\sum \dfrac{1}{p_n^{\alpha}}$, où α est un nombre réel ?
3. Quel est le rayon de convergence de la série entière $\sum \dfrac{z^{p_n}}{p_n}$.
4. En admettant le théorème des nombres premiers, montrer que :

$$\pi(n) \underset{n\to+\infty}{\sim} \int_e^n \frac{dt}{\ln(t)}$$

5. En admettant le théorème des nombres premiers sous la forme $\pi(x) = \operatorname{card}(\mathcal{P} \cap [1, x]) \underset{x\to+\infty}{\sim} \dfrac{x}{\ln(x)}$, où x est une variable réelle, montrer que l'ensemble des nombres rationnels de la forme $r = \dfrac{p}{q}$, où p et q sont des nombres premiers, est dense dans $\mathbb{R}^{+,*}$.
6. Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$ [resp. $6n + 5$].
7. Soit p un nombre premier impair.
   (a) Montrer que $\overline{(-1)}$ est un carré dans $\mathbb{F}_p$ si, et seulement si, p est congru à 1 modulo 4.
   (b) En déduire qu'il existe une infinité de nombres premiers de la forme $4n + 1$.
   (c) Montrer que s'il existe deux entiers a, b premiers entre eux tels que p divise $a^2 + b^2$, on a alors $p \equiv 1\ (4)$.
   (d) Montrer qu'il existe une infinité de nombres premiers de la forme $8n + 5$.
8. On se fixe un nombre premier $p \geq 2$ et on se propose de montrer qu'il existe une infinité de nombres premiers de la forme $pn + 1$, où n est un entier naturel non nul.
   (a) Montrer que les diviseurs premiers de l'entier $m = 2^p - 1$ sont de la forme $pn + 1$, où n est un entier naturel non nul (il existe donc de tels nombres premiers).
   (b) On suppose qu'il n'y a qu'un nombre fini $p_1 < \cdots < p_r$ de nombres premiers de la forme $pn + 1$ et on note :

$$N = p_1 \cdot \cdots \cdot p_r,\ m = (N+1)^p - N^p$$

En désignant par $q \geq 2$ un diviseur premier de m, montrer que $\overline{N} \neq \overline{0}$ dans le corps $\mathbb{F}_q = \dfrac{\mathbb{Z}}{q\mathbb{Z}}$, que $\overline{(N+1)} \cdot \overline{N}^{-1}$ est d'ordre p et conclure.

9. Le n-ème polynôme cyclotomique est le polynôme :

$$\Phi_n(X) = \prod_{z \in R_n} (X - z)$$

où R_n est l'ensemble de toutes les racines primitives n-èmes de l'unité.
$\mathcal{D}_n$ est l'ensemble des diviseurs positifs de $n \geq 1$.

(a) Soient $n \geq 2$ un entier naturel et a un entier relatif.
Montrer que si p est un nombre premier qui divise $\Phi_n(a)$ mais aucun des $\Phi_d(a)$ pour tout d dans $\mathcal{D}_n \setminus \{n\}$, p est alors de la forme $\lambda n + 1$ avec $\lambda \in \mathbb{N}^*$.

(b) Soient n un entier naturel au moins égal à 2 et $\Psi_n = \prod_{d \in \mathcal{D}_n \setminus \{n\}} \Phi_d(X)$.
Montrer qu'il existe deux polynômes U, V à coefficients entiers relatifs et un entier relatif a tels que :

$$\begin{cases} U\Phi_n + V\Psi_n = a \\ \Phi_n(a) \notin \{-1, 0, 1\} \end{cases}$$

(c) Montrer que pour tout entier $m \geq 2$ fixé, il existe une infinité de nombres premiers de la forme $\lambda m + 1$ avec $\lambda \in \mathbb{N}^*$.

10. On se propose de montrer que :

$$\forall n \geq 2,\ \ln(2)\frac{n-2}{\ln(n)} \leq \pi(n) \leq e\frac{n}{\ln(n)}$$

(théorème de Tchebychev).
Pour tout entier naturel $n \geqslant 2$, on note :

$$\mu_n = \operatorname{ppcm}(1, 2, \cdots, n)$$

Pour tout nombre premier p et tout entier naturel non nul n, on note $\nu_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers avec $\nu_p(n) = 0$ si p ne figure pas dans cette décomposition et $\nu_p(1) = 0$ (valuation p-adique de n).
La décomposition en facteurs premiers de n peut donc s'écrire sous la forme :

$$n = \prod_{p \in \mathcal{P}_n} p^{\nu_p(n)}$$

(a) On se propose de montrer que pour tout entier naturel $n \geqslant 2$, on a :

$$\mu_n = \operatorname{ppcm}(1, 2, \cdots, n) \geq 2^{n-2}$$

Pour tout entier $n \in \mathbb{N}^*$, on, note :

$$I_n = \int_0^1 x^n (1-x)^n \, dx$$

i. Montrer que :

$$\forall n \in \mathbb{N}^*,\ 0 < I_n \leq \frac{1}{2^{2n}}$$

ii. En déduire que :

$$\forall n \in \mathbb{N}^*,\ \mu_{2n+1} \geq 2^{2n}$$

puis le résultat annoncé.
(On peut en fait montrer que $\mu_n \geq 2^n$ pour tout $n \geq 7$).

(b) En utilisant la décomposition en facteurs premiers de μ_n, montrer que :

$$\forall n \geq 2,\ \mu_n \leq n^{\pi(n)}$$

puis en déduire que :

$$\forall n \geq 2,\ \ln(2)\frac{n-2}{\ln(n)} \leq \pi(n)$$

(c) Pour tout entier $n \geq 2$, on note :

$$P_n = \prod_{p \in \mathcal{P}_n} p$$

i. Montrer que :

$$\forall n \geq 2,\ P_n \geq \pi(n)!$$

ii. Montrer que :

$$\forall n \geq 2,\ \frac{P_{2n+1}}{P_{n+1}} \leq \binom{2n+1}{n} \leq 2^{2n}$$

iii. En déduire que :

$$\forall n \geq 2,\ P_n \leq 2^{2n}$$

iv. Montrer que :

$$\forall n \geq 2,\ \ln(n!) \geq n(\ln(n) - 1)$$

v. En déduire que :

$$\forall n \geq 2,\ \pi(n) \leq e\frac{n}{\ln(n)}$$

– II – La série $\sum_{n=1}^{+\infty} \frac{1}{p_n}$

On rappelle que le produit de Cauchy de deux séries numériques à termes positifs $\sum u_n$ et $\sum v_n$ qui sont convergentes est convergent et :

$$\left(\sum_{n=0}^{+\infty} u_n\right)\left(\sum_{n=0}^{+\infty} v_n\right) = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} u_k v_{n-k}\right) = \sum_{(\alpha_1,\alpha_2)\in\mathbb{N}^2} u_{\alpha_1} v_{\alpha_2}$$

Plus généralement, le produit de Cauchy de $r \geq 2$ séries numériques à termes positifs $\sum u_{k,n}$ qui sont convergentes est convergent et :

$$\left(\sum_{n=0}^{+\infty} u_{1,n}\right)\cdots\left(\sum_{n=0}^{+\infty} u_{r,n}\right) = \sum_{(\alpha_1,\cdots,\alpha_r)\in\mathbb{N}^r} u_{1,\alpha_1}\cdots u_{r,\alpha_r}$$

1. On note $2 = p_1 < p_2 < \cdots < p_n < \cdots$ la suite strictement croissante des nombres premiers et on se propose de montrer la divergence de la série $\sum \frac{1}{p_n}$.

   (a) Justifier le fait que la série $\sum \frac{1}{p_n}$ est de même nature que la série $\sum \ln\left(1 - \frac{1}{p_n}\right)$.

(b) En désignant par $(u_n)_{n\geq 1}$ la suite définie par :

$$\forall n \geq 1,\ u_n = \frac{1}{\prod\limits_{k=1}^{n}\left(1-\frac{1}{p_k}\right)}$$

montrer que :

$$\left(\sum_{n=1}^{+\infty}\frac{1}{p_n} = +\infty\right) \Leftrightarrow \left(\lim_{n\to+\infty} u_n = +\infty\right)$$

(c) En désignant, pour tout entier $n \in \mathbb{N}^*$, par E_n l'ensemble des entiers naturels non nuls qui ont tous leurs diviseurs premiers dans $\mathcal{P}_n = \{p_1, \cdots, p_n\}$, montrer que :

$$\forall n \in \mathbb{N}^*,\ u_n = 1 + \sum_{j\in E_n}\frac{1}{j}$$

déduire que :

$$\forall n \in \mathbb{N}^*,\ u_n \geq \sum_{j=1}^{p_n}\frac{1}{j}$$

et conclure.

2. On propose de montrer le résultat précédent en raisonnant par l'absurde.
Pour ce faire, on suppose que la série $\sum \frac{1}{p_n}$ converge et on se donne un entier $r \geq 1$ tel que :

$$\sum_{k=r+1}^{+\infty}\frac{1}{p_k} \leq \frac{1}{2}$$

Montrer que, dans ce cas, en notant $P = p_1 \cdots p_r$, on a :

$$\forall m \in \mathbb{N}^*,\ \sum_{n=1}^{m}\frac{1}{1+nP} \leq \sum_{j=1}^{+\infty}\left(\frac{1}{2}\right)^j$$

et conclure.

– III – Nombres premiers et groupes

1. Montrer qu'un groupe d'ordre premier est cyclique.
2. Soit G un groupe commutatif fini d'ordre $n \geq 2$.
Montrer que, pour tout diviseur premier p de n, il existe dans G un élément d'ordre p (théorème de Cauchy dans le cas commutatif).
On peut procéder par récurrence sur $n \geq 2$.
3. Montrer qu'un groupe commutatif d'ordre $n = \prod\limits_{k=1}^{r} p_k$, où $(p_k)_{1\leq k\leq r}$ est une suite de $r \geq 2$ nombres premiers deux à deux distincts, est cyclique.
4. Soient G un groupe commutatif et $(g_k)_{1\leq k\leq r}$ une suite de $r \geq 2$ éléments de G, chaque g_k, pour k compris entre 1 et r, étant d'ordre $n_k \geq 2$, les entiers $n_1, n_2, \cdots, n_r$ étant deux à deux premiers entre eux.
Montrer que $g = \prod\limits_{k=1}^{r} g_k$ est d'ordre $n = \prod\limits_{k=1}^{r} n_k$.

5. Soient G un groupe commutatif et $(g_k)_{1\leq k\leq r}$ une suite de $r \geq 2$ éléments deux à deux distincts dans G, chaque g_k, pour k compris entre 1 et r, étant d'ordre $m_k \geq 2$.
   Montrer qu'il existe un élément de G d'ordre égal au ppcm de ces ordres.
6. Soit $(G, \cdot)$ un groupe commutatif fini. Montrer que :

$$\max_{g\in G} \theta(g) = \operatorname{ppcm}\{\theta(g) \mid g \in G\}$$

   ($\max\limits_{g\in G} \theta(g)$ est l'exposant de G).
7. Soient G un groupe commutatif fini d'ordre $n \geq 2$ et $m = \operatorname{ppcm}\{\theta(g) \mid g \in G\}$ son exposant. Montrer que n et m ont les mêmes facteurs premiers.
8. En utilisant la question précédente, retrouver le théorème de Cauchy dans le cas commutatif.
9. Soit G un groupe fini d'ordre $n \geq 2$.
   En faisant agir G sur lui même par automorphismes intérieurs et en utilisant le théorème de Cauchy dans le cas commutatif, montrer que, pour tout diviseur premier p de n, il existe dans G un élément d'ordre p (théorème de Cauchy).
10. Soient $2 \leq p < q$ deux nombres premiers. Un groupe d'ordre pq est-il cyclique ?
11. Montrer (de manière élémentaire) que, pour tout nombre premier impair $p \geq 3$, un groupe d'ordre $2p$ est soit commutatif et cyclique, soit non commutatif et diédral.

– IV – Les anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$, théorèmes de Fermat et de Wilson

Pour tout entier $n \geq 2$, on note $\mathbb{Z}_n$ l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ des classes résiduelles modulo n et $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$.

On rappelle que, pour tout entier relatif a, on a :

$$\left(\overline{a} \in \mathbb{Z}_n^\times\right) \Leftrightarrow (a \wedge n = 1) \Leftrightarrow \left(\mathbb{Z}_n^\times = \langle \overline{a} \rangle\right)$$

et la fonction indicatrice d'Euler est définie, pour $n \geq 2$, par :

$$\begin{aligned}\varphi(n) &= \operatorname{card}\left(\mathbb{Z}_n^\times\right) = \operatorname{card}\{a \in \{1, \cdots, n-1\} \mid a \wedge n = 1\} \\ &= \operatorname{card}\left\{a \in \{1, \cdots, n-1\} \mid \mathbb{Z}_n^\times = \langle \overline{a} \rangle\right\}\end{aligned}$$

en convenant que $\varphi(1) = 1$.

Du théorème de Lagrange, on déduit les résultats suivants, où $n \geq 2$ est un entier :

pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ (n)$ (théorème d'Euler) ;

si p est un nombre premier, alors pour tout entier relatif a premier avec p, on a $a^{p-1} \equiv 1 \ (p)$ et pour tout entier relatif a, on a $a^p \equiv a \ (p)$ (théorème de Fermat).

1. Montrer que, pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes :
   (a) n est premier ;
   (b) pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\, n^{\alpha-1}$;
   (c) $\varphi(n) = n - 1$;
   (d) $\mathbb{Z}_n$ est un corps ;
   (e) $\mathbb{Z}_n$ est un intègre ;
   (f) $(n-1)! \equiv -1 \ (n)$ (théorème de Wilson) ;
   (g) $(n-2)! \equiv 1 \ (n)$;

(h) pour tout k compris entre 1 et n, on a $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;

(i) pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$;

(j) pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$ et $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$.

2. Soit $p \geq 2$ un nombre premier et $P(X) = X^p - X$ dans $\mathbb{Z}_p[X]$.
   (a) Montrer que $P\left(X+\overline{1}\right) = P(X)$ dans $\mathbb{Z}_p[X]$.
   (b) Retrouver le fait que $\binom{p}{k} \equiv 0 \pmod{p}$ et $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ pour tout entier k compris entre 1 et $p-1$.
3. Soit $p \geq 2$ un nombre premier. Montrer que pour tout entier $n \geq 2$ et tout n-uplet $(a_1, \cdots, a_n)$ d'entiers relatifs, on a :
$$(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \pmod{p}$$
   et retrouver le théorème de Fermat.
4. Soit $n \geq 2$ un entier naturel. Montrer que :
$$(n-1)! \equiv \begin{cases} -1 \pmod{n} \text{ si } n \text{ est premier} \\ 2 \pmod{n} \text{ si } n = 4 \\ 0 \pmod{n} \text{ si } n \neq 4 \text{ est non premier} \end{cases}$$
5. Montrer qu'un entier naturel impair $n \geq 3$ est premier si, et seulement si, $\left(\left(\frac{n-1}{2}\right)!\right)^2$ est congru à $(-1)^{\frac{n-1}{2}}$ modulo n.
6. Déduire du théorème de Fermat un test de non primalité.
7. Soit $n \geq 2$ un entier non premier qui ne soit pas un nombre de Carmichael. Montrer qu'il y a au moins une chance sur 2 pour qu'un entier a compris entre 1 et $n-1$ premier avec n soit un témoin de non primalité pour le test de Fermat (i. e. n ne divise pas $a^{n-1}-1$).
8. Soit $n \geq 3$ un entier. Montrer que si pour tout diviseur premier p de $n-1$, il existe un entier a tel que n divise $a^{n-1}-1$ et n ne divise pas $a^{\frac{n-1}{p}}-1$, alors n est premier (test de primalité de Lucas-Lehmer).
9. Soit $n \geq 3$ un entier. Montrer que s'il existe un entier relatif a tel que n divise $a^{n-1}-1$ et, pour tout diviseur $d \in \{1, \cdots, n-2\}$ de $n-1$, n ne divise pas $a^d - 1$, alors n est premier (test de primalité de Lehmer).

– V – Réciprocité quadratique

On se donne un nombre premier impair $p \geq 3$ et on note $\mathbb{F}_p$ le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

On dit qu'un entier a non multiple de p est un résidu quadratique modulo p si il existe un entier k tel que $k^2 \equiv a \pmod{p}$.

1. On note :
$$C_p = \left\{x^2 \mid x \in \mathbb{F}_p^*\right\}$$
   l'ensemble des carrés de $\mathbb{F}_p^*$ et :
$$\Sigma_p = \left\{x \in \mathbb{F}_p^* \mid x^{\frac{p-1}{2}} - \overline{1}\right\}$$
   l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - \overline{1} \in \mathbb{F}_p[X]$.

(a) Montrer que $\mathrm{card}\,(C_p) = \dfrac{p-1}{2}$ et que $C_p = \Sigma_p$.

(b) On désigne par ψ le morphisme de groupes :

$$\psi : \begin{array}{ccc} \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ x & \mapsto & x^{\frac{p-1}{2}} \end{array}$$

Montrer que $\ker(\psi) = C_p$ et $\mathrm{Im}\,(\psi) = \left\{-\overline{1}, \overline{1}\right\}$.

2. On note $S = \left\{1, 2, \cdots, \dfrac{p-1}{2}\right\}$ et on se donne un entier relatif a non divisible par p.

(a) Montrer que, pour tout entier $k \in S$, il existe un unique couple (ε_k, s_k) dans $\{-1, 1\} \times S$ tel que :

$$\overline{ka} = \varepsilon_k \overline{s_k}$$

(en fait (ε_k, s_k) dépend de k et de a), puis que l'application $k \mapsto s_k$ réalise une bijection de S sur lui même.

(b) Montrer que $a^{\frac{p-1}{2}} \equiv \displaystyle\prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k \pmod{p}$.

3. Pour tout entier relatif a non divisible par p, on définit le symbole de Legendre $\left(\dfrac{a}{p}\right)$ par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est un résidu quadratique modulo } p \\ -1 \text{ sinon} \end{cases}$$

(a) Montrer que, pour tout entier relatif a non divisible par p, on a :

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

et en déduire que :

$$\left(\frac{a}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k$$

(notations de la question **IV.2a**).

(b) Calculer $\left(\dfrac{-1}{p}\right)$ et $\left(\dfrac{2}{p}\right)$.

(c) Montrer que, pour tout entier relatif a non divisible par p, on a :

$$\left(\frac{a}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} \frac{\sin(ax_k)}{\sin(x_k)}$$

où :

$$x_k = \frac{2k\pi}{p} \quad \left(1 \leq k \leq \frac{p-1}{2}\right)$$

4.

(a) Montrer que, pour tout entier naturel non nul r, il existe un polynôme unitaire P_r de degré égal à r tel que :

$$\forall x \in \mathbb{R},\ \cos(2rx) = \frac{(-4)^r}{2} P_r\left(\sin^2(x)\right)$$

(b) Montrer que pour tout entier naturel non nul r et tout réel $x \in \mathbb{R} \setminus \pi\mathbb{Z}$, on a :

$$\frac{\sin\left((2r+1)\,x\right)}{\sin(x)} = (-4)^r \prod_{k=1}^{r} \left(\sin^2(x) - \sin^2\left(\frac{2k\pi}{2r+1}\right)\right)$$

5.

(a) Montrer que, pour tout entier naturel impair a non divisible par p, on a :

$$\left(\frac{a}{p}\right) = (-4)^{\frac{p-1}{2}\frac{a-1}{2}} \prod_{\substack{1 \leq j \leq \frac{a-1}{2} \\ 1 \leq k \leq \frac{p-1}{2}}} \left(\sin^2\left(\frac{2k\pi}{p}\right) - \sin^2\left(\frac{2j\pi}{a}\right)\right)$$

(b) En déduire que, pour tout nombre premier impair $q \neq p$, on a :

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

(formule de réciprocité quadratique).