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 – Infinité de nombres premiers

On vérifie facilement que l'ensemble $\mathcal{P}$ des nombres premiers est infini.

Un théorème de Dirichlet nous dit que si a, b sont deux nombres entiers premiers entre eux, il existe alors une infinité de nombres premiers de la forme $an + b$. La démonstration de ce théorème n'étant pas élémentaire.

Dans quelques cas particuliers, la démonstration peut être simple.

1. Montrer qu'il existe une infinité de nombres premiers de la forme :
   (a) $4n - 1$, où $n \in \mathbb{N}$;
   (b) $6n - 1$, où $n \in \mathbb{N}$;
   (c) $4n + 1$, où $n \in \mathbb{N}$;
   (d) $8n + 5$, où $n \in \mathbb{N}$;
   (e) $pn + 1$, où $p \geq 2$ est un nombre premier fixé et $n \in \mathbb{N}$.
2.
   (a) Montrer que si on dispose d'une suite $(u_n)_{n\in\mathbb{N}}$ strictement croissante d'entiers naturels différents de 0 et 1 et deux à deux premiers entre eux, on peut alors en déduire que $\mathcal{P}$ infini.
   (b) En utilisant les nombres de Fermat, montrer que $\mathcal{P}$ infini.
   (c) Soient a, b deux entiers naturels non nuls premiers entre eux avec $b > a$. On définit la suite $(u_n)_{n\in\mathbb{N}}$ par :
   $$\begin{cases} u_0 = b \\ \forall n \geq 1,\ u_n - a = u_{n-1}(u_{n-1} - a) \end{cases}$$
   Par exemple, la suite $(F_n)_{n\in\mathbb{N}}$ des nombres de Fermat vérifie la relation de récurrence :
   $$\begin{cases} F_0 = 3 \\ \forall n \geq 1,\ F_n - 2 = F_{n-1}(F_{n-1} - 2) \end{cases}$$
      i. Montrer que $(u_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers naturels différents de 0 et 1.
      ii. Montrer que pour tous $m > n \geq 0$, on a :
      $$u_m \equiv a \mod u_n$$
      iii. Montrer que, pour tout $n \geq 0$, u_n est premier avec a.
      iv. Montrer que les u_n sont deux à deux premiers entre eux. Conclure.

– II – Fonction dzeta de Riemann et nombres premiers

On note $(p_n)_{n\in\mathbb{N}^*}$ la suite strictement croissante des nombres premiers.

1. Montrer que $\lim\limits_{\alpha\to 1^+} \zeta(\alpha) = +\infty$.
   Pour ce qui suit, on munit l'ensemble $\mathbb{N}^*$ de la tribu $\mathcal{P}(\mathbb{N}^*)$.
2. Soient $\alpha > 1$ un réel fixé et $\mathbb{P}$ une mesure de probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que :
   $$\forall n \in \mathbb{N}^*,\ \mathbb{P}(n\mathbb{N}^*) = \frac{1}{n^\alpha}$$
   Montrer que pour toute suite $(n_k)_{k\in\mathbb{N}^*}$ d'entiers deux à deux premiers entre eux, la suite $(n_k\mathbb{N}^*)_{k\in\mathbb{N}^*}$ est formée d'événements mutuellement indépendants.

3. Soient $\alpha > 1$ un réel fixé.

   (a) Montrer que l'on définit une mesure probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ qui vérifie l'hypothèse de la question précédente en posant :

   $$\forall n \in \mathbb{N}^*,\ \mathbb{P}(\{n\}) = \frac{1}{\zeta(\alpha)} \frac{1}{n^\alpha}$$

   (b) En utilisant la mesure probabilité de la question précédente, montrer que :

   $$\frac{1}{\zeta(\alpha)} = \prod_{n=1}^{+\infty} \left(1 - \frac{1}{p_n^\alpha}\right)$$

   (c) Montrer que que $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$.

   (d) Calculer $\mathbb{P}(A)$ où A est l'ensemble des entiers naturels non nuls sans facteurs carrés. Que vaut la limite de $\mathbb{P}(A)$ quand α tend vers 1^+ ?

4. Montrer que, pour $0 < \alpha \leq 1$, il n'existe pas de mesure de probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que :

   $$\forall n \in \mathbb{N}^*,\ \mathbb{P}(n\mathbb{N}^*) = \frac{1}{n^\alpha}$$

– III – Inégalités de Tchebychev

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 et :

$$\pi(n) = \operatorname{card}(\mathcal{P}_n)$$

son cardinal.

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

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

Dans cette partie, on se propose de montrer que :

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

Il résulte immédiatement de cet encadrement que $\pi(n) = \underset{n \to +\infty}{o}(n)$ (théorème de Legendre).

Les inégalités de Tchebychev peuvent être utilisées pour donner un encadrement de p_n et pour étudier la série numérique $\sum \frac{1}{p_n}$.

1. Avec cette question, on se propose de montrer que :

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

(a) Montrer que :

$$\forall n \in \mathbb{N}^*,\ 0 < I_n = \int_0^1 x^n (1-x)^n \, dx \leq \frac{1}{2^{2n}}$$

(b) En déduire que :

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

puis le résultat annoncé.

2. 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 :

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

et :

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

3. Pour tout entier $n \geq 2$, on note :

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

(a) Montrer que :

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

(b) Montrer que :

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

(c) En déduire que :

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

(d) Montrer que :

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

(e) En déduire que :

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

(on pourra utiliser la fonction $\varphi : x \mapsto x(\ln(x) - 1)$).

4. Des inégalités de Tchebychev, on peut déduire que :

$$\forall n \geq 2,\ \frac{1}{e} n \ln(n) \leq p_n \leq \frac{4}{\ln(2)} n \ln(n)$$

(a) Montrer que :

$$\forall n \geq 1,\ p_n > \frac{1}{e} n \ln(n)$$

(b) En exploitant la décroissance de la fonction $\psi : t \mapsto \dfrac{\ln(t)}{t}$ sur $[e, +\infty[$, montrer que :

$$\forall n \geq 1023,\ p_n \leq \frac{4}{\ln(2)} n \ln(n)$$

puis vérifier que cette inégalité est encore vraie pour n compris entre 2 et 1022.

5. Quelle est la nature de la série $\sum \frac{1}{p_n^{\alpha}}$, où α est un nombre réel ?

6. Quel est le rayon de convergence de la série entière $\sum \frac{z^{p_n}}{p_n}$.

7. Quelle est la nature de la série $\sum \frac{1}{p_n \ln(p_n)}$?

8. Pour tout entier $n \geq 1$, on désigne par :

$$S_n = \sum_{k=1}^{n} \frac{1}{p_k}$$

la somme partielle d'indice n de la série $\sum \frac{1}{p_n}$.

(a) Montrer que :

$$\forall n \geq 2,\ S_{\pi(n)} = \sum_{k=2}^{n} \frac{\pi(k) - \pi(k-1)}{k}$$

(b) Montrer qu'il existe deux réels $\alpha > 0$ et $\beta > 0$ tels que :

$$\forall n \geq 3,\ \alpha \ln(\ln(n)) \leq S_{\pi(n)} = \sum_{k=1}^{\pi(n)} \frac{1}{p_k} \leq \beta \ln(\ln(n))$$

9. Déduire des inégalités de Tchebychev que $\ln(p_n) \underset{n \to +\infty}{\sim} \ln(n)$, puis en admettant le théorème des nombres premiers montrer que :

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

et :

$$\sum_{k=1}^{n} \frac{1}{p_k} \underset{n \to +\infty}{\sim} \ln(\ln(n))$$

10. En admettant le théorème des nombres premiers, montrer que :

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

– IV – Un théorème de Cesàro

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

$$I_n = \{1, 2, \cdots, n\}$$

et $\mathcal{D}_n$ l'ensemble de tous les diviseurs strictement positifs de n.

On note $\mathbb{R}^{\mathbb{N}^*}$ l'ensemble des suites définies sur $\mathbb{N}^*$ et à valeurs réelles.

Le produit de convolution (de Dirichlet) de deux suites réelles u, v de $\mathbb{R}^{\mathbb{N}^*}$ est la suite $u * v$ définie par :

$$\forall n \in \mathbb{N}^*,\ (u * v)(n) = \sum_{d \in \mathcal{D}_n} u(d)\, v\left(\frac{n}{d}\right)$$

En notant $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers d'un entier $n \geq 2$ où $r \geq 1$, les p_i sont premiers deux à deux distincts et les α_i entiers naturels non nuls, on définit la fonction μ de Möbius par :

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \ \text{ si } n = \prod_{i=1}^{r} p_i \text{ (i. e. } n \text{ est sans facteurs carrés)} \\ 0 \text{ sinon} \end{cases}$$

La fonction indicatrice d'Euler est la fonction qui associe à tout entier naturel non nul n, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers avec n (pour $n = 1$, on a $\varphi(1) = 1$).

1. Pour tout entier $n \in \mathbb{N}^*$ et tout $d \in \mathcal{D}_n$, on note :

$$S_d = \{k \in \{1, \cdots, n\} \mid k \wedge n = d\}$$

   (a) Montrer que les S_d, pour d décrivant $\mathcal{D}_n$, forment une partition de I_n et que, pour tout $d \in \mathcal{D}_n$, on a $\operatorname{card}(S_d) = \varphi\left(\frac{n}{d}\right)$.

   (b) En déduire que :

$$\forall n \in \mathbb{N}^*,\ n = \sum_{d \in \mathcal{D}_n} \varphi(d)$$

   (formule de Möbius).

2. Montrer que l'ensemble $\mathbb{R}^{\mathbb{N}^*}$ des suites définies sur $\mathbb{N}^*$ et à valeurs réelles, muni des lois $+$ et $*$, est un anneau commutatif unitaire.
   On notera e l'élément unité.

3. Caractériser les éléments inversibles de l'anneau $\left(\mathbb{R}^{\mathbb{N}^*}, +, *\right)$.

4.

   (a) En notant ω la suite constante égale à 1 (i. e. $\omega(n) = 1$ pour tout $n \in \mathbb{N}^*$), montrer que $\mu * \omega = e$, c'est-à-dire que :

$$\forall n \geq 1,\ \sum_{d \in \mathcal{D}_n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geq 2 \end{cases}$$

   (b) Montrer que si u, v dans $\mathbb{R}^{\mathbb{N}^*}$ sont telles que :

$$\forall n \in \mathbb{N}^*,\ u(n) = \sum_{d \in \mathcal{D}_n} v(d)$$

   on a alors :

$$\forall n \in \mathbb{N}^*,\ v(n) = \sum_{d \in \mathcal{D}_n} \mu(d)\, u\left(\frac{n}{d}\right)$$

   (formule d'inversion de Möbius).

5. Montrer que :

$$\forall n \in \mathbb{N}^*, \varphi(n) = \sum_{d \in \mathcal{D}_n} \mu(d)\, \frac{n}{d}$$

6. Monter que si u, v dans $\mathbb{R}^{\mathbb{N}^*}$ sont telles que :

$$\forall n \in \mathbb{N}^*,\ u(n) = \sum_{d \in \mathcal{D}_n} v(d)$$

on a alors :

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} u(k) = \sum_{d=1}^{n} \left[\frac{n}{d}\right] v(d)$$

7. Montrer que :

$$\forall n \in \mathbb{N}^*,\ \sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right] = 1$$

8. Montrer que :

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} \varphi(k) = \frac{1}{2}\left(\sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right]^2 + 1\right)$$

9. Pour tout entier $n \geq 2$, on note r_n la probabilité pour que deux entiers a, b compris entre 1 et n soient premiers entre eux.
Montrer que :

$$\forall n \geq 2,\ r_n = \frac{1}{n^2}\left(2\sum_{k=1}^{n} \varphi(k) - 1\right) = \frac{1}{n^2}\sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right]^2$$

10. Pour u, v dans $\mathbb{R}^{\mathbb{N}^*}$, le produit de Dirichlet des deux séries numériques $\sum u(n)$ et $\sum v(n)$ est la série $\sum u * v(n)$.

    (a) On suppose que les suites u et v sont à valeurs réelles positives.
    Montrer que si les séries $\sum u(n)$ et $\sum v(n)$ sont convergentes, il en est alors de même de $\sum u * v(n)$ et on a :

    $$\sum_{n=0}^{+\infty} u * v(n) = \left(\sum_{n=0}^{+\infty} u(n)\right)\left(\sum_{n=0}^{+\infty} v(n)\right)$$

    (b) Montrer que si les séries $\sum u(n)$ et $\sum v(n)$ sont absolument convergentes, il en est alors de même de $\sum u * v(n)$ et on a :

    $$\sum_{n=0}^{+\infty} u * v(n) = \left(\sum_{n=0}^{+\infty} u(n)\right)\left(\sum_{n=0}^{+\infty} v(n)\right)$$

11. À toute suite $u \in \mathbb{R}^{\mathbb{N}^*}$ on associe la série de fonctions $\sum \frac{u(n)}{n^x}$. On dit que cette série de fonctions est la série de Dirichlet associée à u.

    (a) Soient u, v dans $\mathbb{R}^{\mathbb{N}^*}$. Montrer que si les séries de Dirichlet respectivement associées à u et v convergent absolument en un point x, alors la série de Dirichlet associée à $u * v$ converge absolument en x et on a :

    $$\left(\sum_{n=1}^{+\infty} \frac{u(n)}{n^x}\right)\left(\sum_{n=1}^{+\infty} \frac{v(n)}{n^x}\right) = \sum_{n=1}^{+\infty} \frac{u * v(n)}{n^x}$$

(b) Montrer que :

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$$

(c) En déduire que $\lim\limits_{n \to +\infty} r_n = \dfrac{6}{\pi^2}$ (théorème de Cesàro).