Agrégation interne

Nombres premiers

[1]

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

- 103 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 104 Nombres premiers. Applications.
- 157. Arithmétique dans $\mathbb{Z}$.
- 302. Exercices faisant intervenir les notions de congruence et de divisibilité dans $\mathbb{Z}$.
- 305. Exercices faisant intervenir les nombres premiers.
- 357. Exercices utilisant le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

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. Niveau L1.* Dunod. (2007).
- P. Tauvel. *Mathématiques générales pour l'agrégation.* Masson (1993).

1. Le 01/01/2015

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 :

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

On convient que $\varphi(1) = 1$.

Pour $p \geq 2$ premier, $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps. On le note $\mathbb{F}_p$.

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).

Pour tout entier $n \geq 2$, on note $\mathcal{D}_n$ l'ensemble des diviseurs de n dans $\mathbb{N}^*$ et $\sigma(n)$ la somme de tous ces diviseurs.

On dit que n est parfait s'il est égal à la somme de ses diviseurs stricts, ce qui équivaut à :

$$\sigma(n) = \sum_{d \in \mathcal{D}_n} d = 2n$$

Exercice 1 ***Nombres premiers de Mersenne.***

1. *Soient $a \geq 2$, $m \geq 2$ deux entiers et $p = a^m - 1$.*
   (a) *Montrer que si p est premier, on a alors $a = 2$ et m est premier.*
   (b) *La réciproque est-elle vraie ?*
   On appelle nombre premier de Mersenne tout nombre premier de la forme $2^m - 1$.
   Le plus grand nombre premier de Mersenne connu au 25 janvier 2013 est $2^{57885161} - 1$ qui est formé de plus de 17 millions de chiffres en base 10 (exactement 17 425 170 chiffres).
2. *On appelle nombre d'Euclide tout entier de la forme $2^{m-1}(2^m - 1)$ où m est un nombre premier tel que $2^m - 1$ soit premier (de Mersenne).*
   Montrer qu'un entier n est un nombre d'Euclide si, et seulement si, il est pair et parfait.

Exercice 2 ***Tests de primalité.***

Pour tout entier $n \geq 2$, montrer que les assertions suivantes sont équivalentes :

1. *n est premier ;*
2. *pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\, n^{\alpha-1}$;*
3. *$\varphi(n) = n - 1$;*
4. *n est premier avec tout entier compris entre 1 et $n - 1$;*
5. *$\mathbb{Z}_n$ est un corps ;*
6. *$\mathbb{Z}_n$ est un intègre ;*
7. *$(n-1)! \equiv -1 \pmod{n}$ (théorème de Wilson) ;*
8. *$(n-2)! \equiv 1 \pmod{n}$;*
9. *pour tout k compris entre 1 et n, on a $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;*

10. $n = 2$ *ou* n *est impair et* $\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{n+1}{2}} \pmod{n}$;

11. *pour tout entier* k *compris entre* 1 *et* $n-1$, *on a* $\binom{n}{k} \equiv 0 \pmod{n}$;

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

13. *il existe un entier relatif* a *premier avec* n *tel que* $(X+\overline{a})^n = X^n + \overline{a}$ *dans* $\mathbb{Z}_n[X]$.
On pourra montrer que :

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (1)$$

puis :

$$(1) \Leftrightarrow (7),\ (7) \Leftrightarrow (8),\ (7) \Leftrightarrow (9),\ (7) \Leftrightarrow (10)$$
$$(1) \Rightarrow (11) \Rightarrow (12) \Rightarrow (1)$$
$$(1) \Leftrightarrow (13)$$

Exercice 3 ***Théorème de Wilson.***
Soit $n \geq 2$ *un entier naturel. Montrer que :*

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{si } n \text{ est premier} \\ 2 \pmod{n} & \text{si } n = 4 \\ 0 \pmod{n} & \text{si } n \neq 4 \text{ est non premier} \end{cases}$$

Exercice 4 ***Théorème de Fermat et tests de primalité.***

1. *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.

2. *Soit* $p \geq 2$ *un nombre premier. Expliquer comment utiliser le théorème de Fermat pour simplifier le calcul du reste dans la division euclidienne par* p *d'un entier de la forme* a^b, *où* a, b *sont des entiers plus grands que* p, *l'entier* p *ne divisant pas* a.

3. *Soient* $p \geq 2$ *un nombre premier et* $P(X) = X^p - X$ *dans* $\mathbb{F}_p[X]$.

   (a) *Sans utiliser l'implication* $(1) \Rightarrow (11)$ *de l'exercice 2, montrer que* $P\left(X + \overline{1}\right) = P(X)$ *dans* $\mathbb{F}_p[X]$.

   (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* $p-1$.

4. *La réciproque du théorème de Fermat est-elle vraie ?*

5. *Soit* $p \geq 3$ *un entier. Montrer que s'il existe un entier relatif* a *tel que* $a^{p-1} \equiv 1 \pmod{p}$ *et, pour tout diviseur* $d \in \{1, \cdots, p-2\}$ *de* $p-1$, $a^d \not\equiv 1 \pmod{p}$, *alors* p *est premier (test de primalité de Lehmer).*

6. *Soit* $p \geq 3$ *un entier. Montrer que si pour tout diviseur premier* d *de* $p-1$, *il existe un entier* a *tel que* $a^{p-1} \equiv 1 \pmod{p}$ *et* $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$, *alors* p *est premier (test de primalité de Lucas-Lehmer).*

Exercice 5 ***Pour*** $p \geq 2$ ***premier,*** $\mathbb{Z}_p^*$ ***est cyclique.***
Le résultat étant évident pour $\mathbb{Z}_2 = \left\{\overline{0}, \overline{1}\right\}$, *on s'intéresse au cas où* $p \geq 3$ *est un nombre premier impair.*

On utilise la décomposition en facteurs premiers, $p-1 = \prod_{k=1}^{r} p_k^{\alpha_k}$, *où* $2 \leq p_1 < \cdots < p_r$ *sont premiers et les* α_k, *pour* k *compris entre* 1 *et* r, *sont des entiers naturels non nuls.*

1. *Soient* k *compris entre* 1 *et* r, $q_k = \dfrac{p-1}{p_k^{\alpha_k}}$ *et* $x \in \mathbb{Z}_p^*$. *Montrer que* x^{q_k} *est d'ordre* $p_k^{r_{x,k}}$ *où* $0 \leq r_{x,k} \leq \alpha_k$.
2. *Montrer que, pour* k *compris entre* 1 *et* r, *il existe dans* $\mathbb{Z}_p^*$ *un élément d'ordre* $p_k^{\alpha_k}$.
3. *En déduire que* $\mathbb{Z}_p^*$ *est cyclique d'ordre* $p-1$.

Exercice 6 ***Nombres de Carmichaël.***
On appelle nombre de Carmichaël tout entier $n \geq 2$ *non premier tel que* $a^{n-1} \equiv 1 \pmod{n}$ *pour tout entier* a *premier avec* n, *ce qui revient à dire que, pour tout* $x \in \mathbb{Z}_n^\times$, *on a* $x^{n-1} = \overline{1}$

1. *Montrer qu'un nombre de Carmichaël est impair.*
2. *Soit* $a \in \mathbb{N}^*$ *tel que les entiers* $p_k = 6 \cdot k \cdot a + 1$ *pour* $k = 1, 2, 3$, *soient premiers. Montrer que* $n = p_1 p_2 p_3$ *est un nombre de Carmichaël.*
3. *Montrer qu'un nombre de Carmichaël est sans facteur carré.*
4. *Soit* $n \geq 3$ *un entier. Montrer que les assertions suivantes sont équivalentes :*
   (a) n *est un nombre de Carmichaël.*
   (b) *il existe un entier* $r \geq 3$ *et des nombres premiers* $3 \leq p_1 < \cdots < p_r$ *tels que* $n = \prod_{j=1}^{r} p_j$ *et, pour tout indice* j *compris entre* 1 *et* r, $p_j - 1$ *divise* $n-1$.

Exercice 7 ***Carrés dans*** $\mathbb{F}_p^*$, ***où*** p ***est premier et*** $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$.
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 $X^{\frac{p-1}{2}} - \overline{1} \in \mathbb{F}_p[X]$.

1. *Montrer que les carrés de* $\mathbb{F}_p^*$ *sont les racines du polynôme* $X^{\frac{p-1}{2}} - \overline{1} \in \mathbb{F}_p[X]$ *et qu'il y en* $\dfrac{p-1}{2}$.
2. *Soit* p *un nombre premier impair.*
   (a) *Monrer 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* $8n+5$.
3. *En désignant par* ψ *le morphisme de groupes :*

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

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

4. *On note* $S = \left\{1, 2, \cdots, \dfrac{p-1}{2}\right\}$ *et on se donne un entier relatif* a *non divisible par* p.
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*), l'application* $k \mapsto s_k$ *réalise une bijection de* S *sur lui même et on a :*
$$a^{\frac{p-1}{2}} \equiv \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k \pmod{p}$$

Exercice 8 ***Réciprocité quadratique.***
On dit qu'un entier a *non multiple de* p *est un résidu quadratique modulo* p *si il existe un entier* k *tel que* $k^2 \equiv a \pmod{p}$.
Pour tout entier relatif a *non divisible par* p, *on définit le symbole de Legendre* $\left(\dfrac{a}{p}\right)$ *par :*
$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est un résidu quadratique modulo } p \\ -1 \text{ sinon} \end{cases}$$

1. *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 :
$$\left(\frac{a}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k$$
(notations de l'exercice précédent).
2. *Calculer* $\left(\dfrac{-1}{p}\right)$ *et* $\left(\dfrac{2}{p}\right)$.
3. *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. *Montrer que pour tout entier naturel non nul* r, *il existe un polynôme unitaire* P_r *de degré égal à* r *tel que :*
$$\forall x \in \mathbb{R},\ \cos(2rx) = \frac{(-4)^r}{2} P_r\left(\sin^2(x)\right)$$
et pour tout entier naturel non nul r *et tout réel* $x \in \mathbb{R} \setminus \pi\mathbb{Z}$, *on a :*
$$\frac{\sin((2r+1)x)}{\sin(x)} = (-4)^r \prod_{k=1}^{r} \left(\sin^2(x) - \sin^2\left(\frac{2k\pi}{2r+1}\right)\right)$$
5. *Montrer que pour tout entier naturel impair* a *non divisible par* p, *on a :*
$$\left(\frac{a}{p}\right) = (-4)^{\frac{p-1}{2}\frac{a-1}{2}} \prod_{\substack{1 \leq j \leq \frac{a-1}{2} \\ 1 \leq k \leq \frac{p-1}{2}}} \left(\sin^2\left(\frac{2k\pi}{p}\right) - \sin^2\left(\frac{2j\pi}{a}\right)\right)$$

6. *Montrer 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).

7. *Soient $p \geq 3$ un nombre premier impair et n un entier impair de la forme $n = 2^\alpha m + 1$, où α est un entier supérieur ou égal à 2 et m un entier impair compris entre 1 et $2^\alpha - 1$.*
On suppose que p ne divise pas n et que n n'est pas un résidu quadratique modulo p.
Montrer que n est premier si, et seulement si, $p^{\frac{n-1}{2}} \equiv -1$ modulo n.

8. *En utilisant le test de primalité de la question précédente, montrer qu'un entier de Fermat, $F_n = 2^{2^n} + 1$ où n est un entier naturel non nul, est premier si, et seulement si, $3^{\frac{F_n-1}{2}}$ est congru à -1 modulo F_n.*