Concours Agrégation, Mathématiques générales

Leçon 21- Nombres premiers. Applications.

Commentaires du jury 2015 :

Il s'agit d'une leçon pouvant être abordée à divers niveaux. Il y a tant à dire sur la question que le candidat devra fatalement faire des choix. Attention toutefois à celui des développements, ils doivent être pertinents ; l'apparition d'un nombre premier n'est pas suffisant !. La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers est un résultat historique important, qu'il faudrait citer. Sa démonstration n'est bien-sûr pas exigible au niveau de l'Agrégation. Quelques résultats sur la géométrie des corps finis sont les bienvenus, ainsi que des applications en cryptographie.

Commentaires du jury 2016 :

Le sujet de cette leçon est très vaste. Aussi les choix devront être clairement motivés. La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers est un résultat historique important qu'il faudrait citer. Sa démonstration n'est bien sûr pas exigible au niveau de l'agrégation. Quelques résultats sur les corps finis et leur géométrie sont les bienvenus, ainsi que des applications en cryptographie.

Remarque : on trouve le théorème des nombres premiers ainsi que la preuve et l'équivalent du n-ième nombre premier (et la fonction zêta) dans [Q. Z.] chap. 12. Il faut définir la fonction zeta de Riemann pour s réel > 1 et savoir montrer que son développement en produit Eulérien est équivalent au théorème fondamental de l'arithmétique. Pour le théorème des nombres premiers et l'hypothèse de Riemann, voir :

`http://www.math.polytechnique.fr/xups/xups02-01.pdf`

et

`http://fr.wikipedia.org/wiki/Fonction_de_compte_des_nombres_premiers`

On lit que $lim_{x=\infty}\frac{\pi(x)}{xlnx} = 1$ constitue le théorème des nombres premiers, prouvé indépendamment par Hadamard et La Vallée Poussin, en 1896, grâce à la fonction zêta de Riemann. Une assertion équivalente est $lim_{x=\infty}\frac{\pi(x)}{li(x)} = 1$ où la fonction $li(x)$ est le logarithme intégral intégrale de 2 à x de $1/ln(t)$ est en fait une approximation plus précise. L'hypothèse de Riemann équivaut à une majoration beaucoup plus serrée de l'erreur dans l'approximation de $\pi(x)$, donc à une distribution plus régulière des nombres premiers : $\pi(x) = li(x) + O(x^{1/2}ln(x))$.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
Errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
Compléments et errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. F] Fresnel J. *Anneaux* (Hermann 2001)
et
[Pe.] Perrin D. *Cours d'algèbre* (ellipses 1996)
[Q. Z.] Queffelec H., Zuily C. *Analyse pour l'agrégation* (Dunod 2013)
[Se.] Serre J.P. *Cours d'arithmétique* (PUF 1970)

Développements conseillés :

(1) Le théorème de Dirichlet, [F. M. 1] $n°90$ p. 251, question 2 et éventuellement 3.
(2) Polynôme $\in \mathbb{Z}[X]$ sans racine dans $\mathbb{Q}$ et ayant une racine modulo $m\mathbb{Z}$ pour tout $m > 1$, [F. M. 1] $n°101$ p. 276.
(3) Sous-groupes finis de $GL_n(\mathbb{Z})$, [F. M. 1] $n°26$ p. 46, question 2 et éventuellement 1 et 3.
(4) Résultant et loi de réciprocité quadratique, [F. M. 2] p. 242.
(5) Entiers de Gauss, somme de 2 carrés, [F. M. 1] $n°94$ p. 260 ou [Pe.] p. 57.

(6) Un théorème de Schur sur les coefficients des polynômes cyclotomique, [F. M. 2] p. 249 question 5.

Exercice 1 Équivalent du n-ième nombre premier, [Q. Z.] chap. 12.

Exercice 2 Nombres de Fermat et nombres premiers.

(1) *Il y a une infinité de nombres premiers.*
   (a) Soit $n \in \mathbb{N}$, montrer que si $1 + 2^n$ est premier alors $n = 2^m$.
   (b) Pour $n \in \mathbb{N}$, on note $F_n := 1 + 2^{2^n}$ le n-ième nombre de Fermat. Montrer que si $n \neq m$ alors F_n et F_m sont premiers entre eux. En déduire qu'il y a une infinité de nombres premiers.

(2) *Le 5-ième nombre de Fermat n'est pas premier d'après Euler.*
   Soit $F_n := 2^{2^n} + 1$ le n-ième nombre de Fermat et p un diviseur premier de F_n.
   (a) Montrer que l'ordre de 2 modulo p est égal à 2^{n+1}
   Preuve. Puisque $(F_n - 1)^2 = 2^{2^{n+1}} = 1 \mod p$*; il suit que l'ordre de 2 modulo p divise* 2^{n+1} *et puisque* $2^{2^n} = -1 \mod p$*, il suit que l'ordre de 2 modulo p est égal à* 2^{n+1}*. ///*
   (b) On suppose que $n \geq 2$. En déduire que $p = 1$ modulo 8 et que 2^{n+1} divise $\frac{p-1}{2}$.
   Preuve. Puisque $8|2^{n+1}$*, il suit que* $2^{2^{n-2}}$ *est une racine primitive 8-ième modulo p. Ainsi par le théorème de Lagrange on a* $p = 1$ *modulo 8. Ainsi* 2 *est un carré modulo p (question 5.) et donc* $2^{\frac{p-1}{2}} = 1 \mod p$*. Ainsi l'ordre de 2 modulo p divise* $\frac{p-1}{2}$*. ///*
   (c) On suppose que $n = 5$. Soit p un diviseur premier de F_5. Montrer que $p = 1$ modulo 128. Montrer que $641 = 1$ modulo 128 est premier. On vérifie que $F_5 = 641 \times 6700417$. Ainsi $F_5 = 4294967297$ n'est pas premier.
   Preuve. Dans la question précédente on a montré que $2^{n+1} = 2^6$ *divise* $\frac{p-1}{2}$*. Ainsi* $128 = 2^7|(p-1)$*. ///*

Exercice 3 La série des inverses des nombres premiers diverge, [Fr. F] ex 1.9.35 p. 58.
Une autre preuve utilisant la divergence du produit eulerien $\prod_{p\in P}(1-1/p)$: remarquer que pour $p > 1$ premier $(1 - \frac{1}{p})^{-1} = 1 + \frac{1}{p} + \frac{1}{p^2} + ...$ Ainsi $\prod_{p<N, p\in P}(1 - \frac{1}{p})^{-1} = \sum_A \frac{1}{m}$ où P désigne l'ensemble des nombres premiers et A les entiers dont les facteurs premiers sont $< N$. Enfin $Log(1 - \frac{1}{p})^{-1} \sim \frac{1}{p}$; ainsi si la série $\sum_{p\in P} \frac{1}{p}$ convergeait la série harmonique convergerait.

Exercice 4 Les premiers qui divisent les valeurs d'un polynôme, [Fr. F] ex. 1.9.36 p. 59.
Soit $P(X) \in \mathbb{Z}[X]$ non constant.

(1) On suppose que $P(0) = 1$. En considérant les diviseurs premiers de $P(n!)$, montrer que P a une racine modulo p pour une infinité de nombre premiers p.
   Preuve. Puisque P n'est pas constant il existe $A > 0$ *avec* $|P(x)| > 1$ *pour tout* $x > A$*. Ainsi si* $n \in \mathbb{N}$ *avec* $n! > A$ *alors* $P(n!) \in \mathbb{Z} - \{-1, 0, 1\}$*, ainsi il existe* p_n *un diviseur premier de* $P(n!)$ *et donc* $n! \mod p_n$ *est une racine de P modulo* p_n*. Puisque* $P(0) = 1$ *il suit que* $p_n \nmid n!$ *et donc que* $p_n > n$*. ///*

(2) Même question dans le cas général (si $P(0) \neq 0$, on pourra considérer le polynôme $\frac{P(XP(0))}{P(0)}$).
   Preuve. Si $P(0) = 0$ *le résultat est trivial. Supposons que* $P(0) \neq 0$ *alors* $P = a_0 + a_1X + ... + a_dX^d$ *avec* $d > 0$*,* $a_k \in \mathbb{Z}$*, et* $a_0a_d \neq 0$*. Alors* $Q(X) := \frac{P(XP(0))}{P(0)} \in \mathbb{Z}[X]$ *et* $Q(0) = 1$*. On applique la question précédente à Q. ///*

Exercice 5 Il y a une infinité de nombres premiers congrus à $7 \mod 8$ en utilisant le symbole quadratique $(\frac{2}{p})$.

On rappelle, [Se.] p. 15 et exercice suivant que $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ (notez alors que l'exercice précédent montre qu'il y a une infinité de nombres premiers congrus à $\pm 7 \mod 8$).

On suppose qu'il n'y a qu'un nombre fini de nombres premiers congrus à $7 \mod 8$. Soit donc $\{p_1, p_2, ..., p_n\}$ l'ensemble des nombres premiers congrus à 7 modulo 8.

(1) Soit $p \neq 2$ un diviseur premier de $N := (4p_1...p_n)^2 - 2$. Montrer que $p = \pm 1 \mod 8$.
Preuve. On remarque que $2 = (4p_1...p_n)^2 \mod 8$ *ainsi par la question précédente* $p = \pm 1 \mod 8$. ///

(2) En déduire qu'il existe un diviseur premier q de N qui est congru à -1 modulo 8. Conclure.
Preuve. On a $\frac{N}{2} = 8(p_1...p_n)^2 - 1$, *ainsi il existe un diviseur premier* q *de* N *qui est congru à* -1 *modulo* 8 *mais* $q \notin \{p_1, p_2, ..., p_n\}$ *ce qui donne une contradiction.* ///

Exercice 6 Une formule explicite pour le symbole quadratique $(\frac{2}{p})$ d'après [Se.] p. 16.

Soit $p > 2$ un nombre premier et $\mathbb{F}_p$ le corps fini à p éléments et L un corps de décomposition du polynôme $X^8 - 1 \in \mathbb{F}_p[X]$.

(1) Soit $U_8 := \{x \in L, \mid x^8 = 1\}$. Justifier que U_8 est un sous-groupe cyclique d'ordre 8 de $L^\times$.
Preuve. Puisque L *est un corps commutatif* $|U_8| \leq \deg(X^8 - 1)$ *et puisque* $p > 2$, *il suit que* $PGCD(X^8 - 1, 8X^7) = 1$; *ainsi* $|U_8| = 8$. *Ainsi* U_8 *est un sous-groupe fini d'un corps commutatif; il est donc cyclique. Pus simplement on peut factoriser* $X^8 - 1 = (X^4 - 1)(X^4 + 1)$ *et ainsi partitionner les racines de* $X^8 - 1$ *en* $\{x \in L, \mid x^4 = 1\} \cup \{x \in L, \mid x^4 = -1\}$ *et puisque chaque partie est de cardinal* ≤ 4, *il suit que* $|\{x \in L, \mid x^4 = -1\}| = 4$; *on a ainsi exhibé* 4 *racines primitives 8-ième de l'unité.* ///

(2) Soit $\alpha \in L$, une racine primitive 8-ième de l'unité. Soit $y := \alpha + \alpha^{-1}$. Montrez que $y^2 = 2$.
Preuve. On développe $y^2 = \alpha^2 + 2 + \alpha^{-2} = 2$ *puisque* $\alpha^4 + 1 = 0$. ///

(3) On suppose que $p = \pm 1$ modulo 8. Montrer que $y \in \mathbb{F}_p$.
Preuve. On calcule $y^p = \alpha^p + \alpha^{-p}$ *et pour* $p = \pm 1$ *modulo 8 on retrouve* y. *Ainsi* $y \in \mathbb{F}_p$. ///

(4) On suppose que $p = \pm 5$ modulo 8. Montrer que $y \notin \mathbb{F}_p$.
Preuve. On calcule $y^p = \alpha^p + \alpha^{-p}$ *et pour* $p = \pm 5$ *modulo 8 on trouve* $-y$. *Ainsi* $y \notin \mathbb{F}_p$. ///

(5) En déduire que 2 est un carré modulo p si et seulement si $p = \pm 1$ modulo 8.
Preuve. Puisque $y^2 = 2$ *il suit que* 2 *est un carré modulo* p *si et seulement si* $y \in \mathbb{F}_p$. *Puisque* p *est impair il suit que* $p = \pm 1$ *ou* $p = \pm 5$ *modulo 8. Le résultat suit alors des questions précédentes.* ///

Exercice 7 Fonction de Mobius, [F. M. 1] $n°86$ p. 242.

Exercice 8 Sur les coefficients du polynôme cyclotomique, [F. M. 2] p. 248-253

(1) Soient p, q des nombres premiers distincts, alors les coefficients de $\Phi_{pq}(X)$ appartiennent à $\{0, 1, -1\}$, [F. M. 2] p. 249 question 4.

(2) Si $m \geq 1$ est un entier, alors il existe un entier n de façon que l'un des coefficients de $\Phi_n(X)$ soit de valeur absolue m, [F. M. 2] p. 249 question 5.

Exercice 9 Géométrie sur les corps finis.

Les groupes $PGL(2, \mathbb{F}_4)$ et $PGL(2, \mathbb{F}_5)$, [F. M. 1] $n°75$ p.190.