110 - Nombres premiers. Applications.

- On va commencer par voir les premières propriétés, théorèmes, et quelques applications en arithmétique : somme des deux carrés par exemple. On finira cette 1ère partie sur un exemple d'application : le cryptage RSA, qui motivera la localisation de nombres premiers et les tests de primalité.
- Seconde partie : localisation, tests de primalité
- Troisième partie : applications dans plusieurs domaines : théorie des groupes, des corps, polynômes…

Définition : nombre premier. On note P leur ensemble et π(x) le nombre de nombres premiers ≤ x [MatL1 292]

Déf : pee

Déf : indicatrice Euler.

I) Nombres premiers et arithmétique [MatL1]+[Comb]+[Zem]+[Perr]+[Del]

Prop : l'ensemble P est infini [MatL1] (par l'absurde, et on regarde p1…pr +1 [MatL1]

1) Théorème fondamental de l'arithmétique [MatL1]

Lemme de Gauss : a divise bc, a et b premiers entre eux. Alors a divise c [Mat L1] *(par Bézout on écrit au+bv=1, donc c=auc+bvc=a(cu+a'v) et c'est bon)*

Lemme (Euclide) : soit p un nb premier qui divise ab. Alors p divise a ou p divise b [MatL1] *(se sert du lemme de Gauss)*

Th fondamental : tout entier ≥ 2 se décompose de façon unique (à permutation près) en un produit de nombres premiers [MatL1] (récurrence sur n≥ 2. Pas de récurrence : n+1 a un diviseur premier p, et on applique l'HR à (n+1)/p. Pour l'unicité on utilise le lemme d'Euclide)

Prop-déf : valuation p-adique [MatL1]

Csq : expression du pgcd et du ppcm [MatL1]

2) Premières propriétés [Comb] + [Zem]

Théorème (Fermat) : si p premier, pour tout entier on a x^p congru à x modulo p *(on regarde ça dans Fp)*

Th (Fermat Euler) : pour tout k entier premier avec n, k^{phi(n)} est congru à 1 modulo n *(regarder l'ordre de k dans (Z/nZ)*)*

Théorème (Wilson) : p est un nb premier ssi (p-1) ! congru à -1 modulo p *(supp p premier. Alors par Fermat, pour tout x dans Fp*, x^{p-1}=1. Donc X^(p-1)=(X-1)(X-2)…(X-p+1). On écrit l'égalité des termes constants de ces polynômes et c'est bon. Réciproquement, si (p-1) ! est congru à -1 modulo p, alors aucun entier plus petit que p-1 ne divise p donc p est premier)*

Appl : trouver une racine carré de -1 dans Fp

Appl : quel est le chiffre des unités de 27^1995 ? *(on veut connaître le reste de la DE de ce nb par 10. 27 est congru à 7 modulo 10. Phi(10)=4. 7 est premier avec 10 donc 7^4 est congru à 1 modulo 10. On divise 1995 par 4 : 1995=4q+3. Donc 27^1995=7^1995=7^(4q+3)=(7^4)^q*7^3=7^3=3. Le chiffre des unités est 3)*

3) Indicatrice d'Euler [Zem]

Formules

Appl : tout sous groupe fini du groupe multiplicatif d'un corps est cyclique *(G un groupe fini d'ordre n. d un diviseur de n. Gd l'ensemble des éléments de G d'ordre d. Les éléments de Gd sont des racines de X^d-1 donc il y en a au plus d. G*

admet donc au plus un sous groupe d'ordre d (car ce sous groupe contient que des éléments qui vérifient x^d-1=0, ça en fait déjà d, il ne peut pas y en avoir d'autres). G admet donc au plus un groupe cyclique d'ordre d. S'il y en a zéro, alors Gd=∅. S'il y en a un, alors Gd est inclus dans ce groupe, et le cardinal de Gd est le nombre d'elt d'ordre d dans $\mathbb{Z}/d\mathbb{Z}$, c'est-à-dire phi(d). Donc #Gd=0 ou Phi(d). Dans les deux cas, #Gd≤phi(d). Or n=∑#Gd=∑ phi(d) donc égalité. En particulier, #Gn=phi(n)≠ 0. Il y a des éléments d'ordre n. G est cyclique)

4) Somme de deux carrés [Perr]

Déf : Σ l'ensemble des nombres somme de deux carrés. Z[i]. N la norme.

Prop : Σ stable par multiplication *(vient de l'identité de Lgrange, et faut passer par Z[i] en disant que n∈Σ ssi ∃ z ∈ $\mathbb{Z}$[i] tq n=N(z))*

Prop : $\mathbb{Z}$[i] est euclidien *(on prend z et t dans Z[i], on défini le complexe z/t, et on prend l'élément q de Z[i] le plus proche de z/t. On mq z=qt+(z-qt) avec N(z-qt)<N(t) et c'est bon)*

Théorème : p nb premier. p∈Σ ssi p=2 ou p congru à 1 modulo 4 *(un sens facile : si n est somme de deux carrés, alors n est congru à 0,1 ou 2 modulo 4. Comme p est premier il peut pas être congru à 0 ou 2, donc il est congru à 1. l'autre sens est balèze. Il faut mq p∈Σ ssi p n'est pas irréductible dans Z[i], ça se fait bien. Z[i] principal donc p non irréductible ssi $\mathbb{Z}$[i]/(p) non intègre. On mq Z[i]/(p)=Fp[X]/(X²+1). Du coup Z[i]/(p) n'est pas intègre ssi X²+1 est réductible dans Fp, ie si -1 est un carré modulo p, ie si p congru à 1 modulo 4)*

Théorème : n ∈Σ ssi vp(n) est pair pour p congru à 3 modulo 4 *(un sens clair avec la stabilité par multiplication. Pour l'autre, on fixe p congru à 3, et on montre par récurrence sur vp(n) que vp(n) est pair, en montrant que vp(n/p²) reste dans Σ)*

5) Une application : le cryptage RSA [Del]

Théorème : p, q deux nombres premiers. On pose n=pq. Si e est premier avec (p-1)(q-1), alors il existe d>0 tq ed=1 mod((p-1)(q-1)). Si on prend a premier avec n, on a a^ed=a (mod n) *(a^ed=a^[k*(p-1)(q-1)+1]=(a^(p-1)(q-1)]^k*a. Or Phi(n)=(p-1)(q-1), donc comme a et n sont pee, a^phi(n)=1 (mod n) par Fermat Euler. On a donc a^ed=a (mod n))*

Appl : le RSA. Je choisis p,q, puis e un nb premier avec (p-1)(q-1). On calcule l'inverse de e modulo (p-1)(q-1). On pose n=pq. Je rend public n et e, mais surtout pas p,q,d. L'expéditeur qui veut m'envoyer un message transforme son message en des nombres A plus petit que n. Il calcule ensuite B=A^e (mod n). Moi je reçois le message B et je calcule B^d, qui me fait retomber sur A d'après le th.

Précautions à prendre :
- p et q grands (sinon on peut les trouver en factorisant n)
- |p-q| grand sinon √n est proche de p et on peut trouver p.
- p-1 et q-1 ne doivent pas être trop friables
- e doit pas être trop petit

II) Localisation des nombres premiers [Zem] + [FG] + [Goz] + [Del]

1) Répartition [Zem] + [FG] + [Goz]

Prop : il existe des « trous » aussi grand qu'on veut dans la répartition des nb premiers (pas de nb premier entre n !+2 et n !+n)

Prop : la série des 1/p diverge [FG]

Th : Dirichlet faible [Goz]

Th : Tchebychev [Zem] *(technique. On parle de coeff binomiaux, majorations, on trouve des produits de nb premiers, on passe au log, ça donne des sommes…)*

Rq sur le th des nombres premiers

2) Nombres remarquables [Del]

Déf : nombre de Fermat (2^2^n+1)

Ex : Fn est premier pour n=1,2,3,4. F5 n'est pas premier. On ne sait pas s'il y en a une infinité de premiers.

Déf : nombre de Mersenne (2^p-1) Mp est premier pour p=2,3,5,7,13,17,19,31,61… Pour tous les autres, ils sont pas premiers (enfin les autres plus petits, on sait pas non plus s'il y en a une infinité).

Prop : si a^n-1 est premier, alors a=2 et p est premier (ie les nb de Mersenne sont les seuls candidats du type a^n-1)

3) Tests de primalité [Del]

Crible d'Eratosthène (-250 avant JC) ; on teste la primalité en remarquant que les diviseurs sont plus petits que √(n)

Test de Fermat : on veut voir si n est premier. On choisit a au hasard. On calcul a^{n-1}. Si a{n-1} n'est pas congru à 1 modulo n, alors n n'est pas premier (th de Fermat). Sinon, on dit que p est pseudo premier en base a.

En pratique, ce test marche bien. Ceci dit, même si on l'applique pour un grand nb de bases différentes, on n'est pas sûr qu'un nombre vérifiant chaque test est premier. Il existe les nb de Carmichael qui vérifient le test pour tout a premier avec n, et qui ne sont pas premiers (il existe une infinité de nb de Carmichael, les premiers sont 561,1105, 1729…). Si ojn fait le test de Fermat avec un nb de Carmichael, le résultat de a^n-1 va nous donner 1 tout le temps, sauf quand a sera un diviseur de n.

Test de Lucas-Lehmer (pour les nb de Mersenne) : on définit S(1)=4 et S(n+1)=S(n)²-2. Mp est un nb premier ssi Mp divise S(p-1) *(raisonnement par l'absurde, on finit dans l'anneau Z[√3])*

III) Applications diverses [Perr]

1) Théorie des groupes [Per]

Prop : si #G=p alors P est cyclique, et G≅Z/nZ.

Prop : Z /nZ est simple ssi n est premier

Th de Sylow

Si #G=p² alors il est abélien

2) Théorie des corps [Per]

a) Généralités

Prop : l'anneau Z/nZ est un corps ssi n est premier

Prop : soit K un corps. Alors carac(K)=0 ou p.

Prop : pour tout p, pour tout n, il existe un unique corps à p^n éléments (à isomph près) et c'est le corps de décomposition de X^q-X sur Fp.

On a souvent besoin de savoir si un nombre est un carré modulo un autre : résolution d'équation sur des corps finis, formes quadratiques etc.

b) Résidus quadratiques [Goz]

Déf : symbole de Legendre

Prop : Euler. Version pour (2,p)=(-1)^(p²-1)/8

Csq : le symbole de Legendre est multiplicatif

Csq : il suffit de savoir calculer les (p,q).

Th : loi de réciprocité quadratique

Ex : au lieu de devoir calculer (2,17), on peut calculer (17,2) (à un signe près) qui nous donne (1,2)=1.

Appl : test de Pépin. Un nd de Fermat Fn est premier ssi 3^(Fn-1)/2+1 congru à 0 modulo 3 *(on remarque que 2^2 congru à 1 modulo 3, donc 2^2^n congru à 1 mod 3. Donc Fn et 3 sont pee. Supp la congruence du test vérifiée. On note w l'ordre de 3 dans (Z/FnZ)*, on mq w=Fn-1, ce qui donne que Fn est premier. Si on supp Fn premier, par la LRQ, on a que (3,Fn)=(Fn,3). Fn congru à 2 mod 3 donc (Fn,3)=(2,3)=-1. Donc (3,Fn)=-1=3^(Fn-1)/2 donc c'est bon)*

Rq : le symbole de Legendre se généralise au symbole de Jacobi, où le nombre en bas est pas obligé d'être premier, et ça reste multiplicatif.

3) Réduction de polynômes

Eisenstein

Exemple

Réduction modulo p : P un polynôme de Z [X], Q sa réduction modulo p. On suppose que le coefficient dominant n'est pas nul dans Fp. Alors si Q est irred sur Fp, Q est irred sur Q *(facile à montrer : par l'absurde)*

Exemple

Développements :
1 - Loi de réciprocité quadratique via les fq [???] (**)
2 - Théorème de Dirichlet faible [Goz 84] (**)
3 - La série des inverses des nb premiers diverge [FG 96] (* ou **)

Bibliographie :
[MatL1] Marco & Lazzarini
[Comb] Combes – Algèbre et géométrie
[Perr] Perrin
[Zem] Zemor - Cryptographie
[Del] Delahaye – Merveilleux nombres premiers
[Goz] Gozard – Théorie de Galois
[FG] Francinou-Gianella

A savoir :

- Algorithme de Karatsuba : permet de multplier deux nombres entre eux. Au lieu de fairel a multiplication brutale, on coupe le nombre en 2.

Par ex, 235 254 123 = 235*10^6 + 254 123 = a*10^6 + b, et 12 365 125 = 12*10^6 + 365 125 = c*10^6 + d. Le produit donne alors ac*10^12+(ad+bc)*10^6+bd, ce qui revient à faire des multiplications de nombres bcp moins importants.

- Exponentiation rapide : le but est de calculer a^b mod(n). Dans un premier temps, on calcule a^2 mod(n), ça donne x1. Puis on calcule a^4=x1^2 mod(n), ça donne x2, etc. Ensuite o ndécompose b en base 2, et il reste à multiplier les x_i tels que la i-ème décimale de b en base 2 est non nulle.

Rapport du jury : la répartition des nombres premiers est un résultat historique important. Sa démonstration n'est bien-sûr pas exigible au niveau de l'Agrégation. Il faut savoir si 89 est un nombre premier ! Attention aux choix des développements, ils doivent être pertinents. Cette leçon est classique et bien balisée, encore faut-il l'organiser de façon cohérente. Il est absurde de vouloir déduire que l'ensemble des nombres premiers est infini de la divergence de la série

des 1/p. Il peut être intéressant de consacrer une section à la répartition des nombres premiers, à des exemples de nombres premiers, à la recherche de nombres premiers, aux applications en algèbre, en géométrie. Par contre le choix du développement doit être bien réfléchi ; le candidat ne peut se contenter de proposer un théorème de Sylow sous prétexte qu'un nombre premier apparait en cours de route, ou le critère d'Eisenstein. Dans ces leçons, la loi de réciprocité quadratique devient un point de développement courant. La démonstration est souvent bien apprise, mais les idées sous-jacentes ne sont pas mises en valeur. En bref, on assiste à une suite de calculs incompréhensibles, car sans ligne directrice. Pour le codage RSA, il serait utile de connaitre la taille des nombres premiers intervenant et une méthode de calcul de a^k mod N efficace : l'exponentiation rapide. Certaines identifications rendent les exposés confus, voire faux : Z/nZ identifié au sous-ensemble {0, 1, 2, . . . , n−1} de Z. Dans ces leçons, la loi de réciprocité quadratique est souvent proposée, mais les candidats ne proposent aucune application et ne savent pas calculer le symbole (2/p). Par ailleurs il faut faire très attention à l'extension dans laquelle on travaille. En bref, on assiste souvent à une suite de calculs incompréhensibles. Il faudrait connaitre les idéaux de Z/nZ. Il serait bon de ne pas donner des résultats tels que la caractérisation des nombres de Carmichael si l'on ne peut en exhiber un, savoir (au moins) qu'il en existe une infinité. A l'énoncé d'un résultat, il est toujours utile de se poser la question de la réciproque. Ainsi, certains candidats ont retrouvé (découvert ?) avec l'aide du jury le plus souvent que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$ si, et seulement si $n \wedge m = 1$. Par ailleurs, sur ces leçons, le jury attend que les candidats apportent des éléments du niveau de l'agrégation. La leçon "Propriétés élémentaires des nombres premiers" n'est pas nécessairement une leçon facile, quoi qu'en puissent penser les candidats. L'attribut "élémentaire" signifie d'une part que les candidats ne sont pas réputés s'attaquer à la théorie analytique des nombres, et d'autre part que les propriétés les plus élémentaires ne doivent pas faire défaut. Il est indispensable à cette occasion de parler de la décomposition en facteurs premiers dans l'anneau des entiers relatifs, et de s'intéresser aux congruences modulo un nombre premier. La nature de la série des inverses des nombres premiers relève elle aussi de techniques élémentaires.