110: nombres premiers. Applications.

Pierre Lissy

January 5, 2010

1 Nombres premiers en arithmétique

1.1 Définition, premières propriétés

Définition 1. *On appelle nombre premier entier naturel dont les seuls diviseurs sont 1 et lui-même (en dehors de 1).*

Proposition 1 (crible d'erastosthène)**.** *On considère un entier N, et on appelle E l'ensemble des nombres compris entre 2 et N. On appelle pour $n \leqslant \sqrt{N}$ E_n l'ensemble des multiples de n plus petits que N. Alors l'ensemble des nombres premiers est E privé de tous les E_n. De plus, on peut même se restraindre aux E_n avec n premier. L'algorithme suivant permet de trouver tous les nombres premier sentre 0 et N (on décrit l'étape d'initialisation, la boucle et le test pour sortir de la boucle)*

1. *On pose $a_1 = 2$. On raye tous les éléments de E_{a_1}.*
2. *On suppose rayé tous les multiples des E_{a_i} avec $a_i \leqslant a_n$. On pose a_{n+1} le plus petit entier qui soit non rayé. On raye ses multiples inférieures à 100.*
3. *On s'arrête dès que l'on a dépassé $\sqrt{N}$*

Exemple 1. *N=100, on trouve 25 nombres premiers:* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73$
Ici $\sqrt{N} = 10$, on a fait en fait exactement 3 passages dans la boucle (+ le cas $n = 2$)

Théorème 1. *L'ensemble des nombres premiers est infini.*

La méthode d'Euclide permet de montrer bien d'autres résultats.

Proposition 2. *Il existe une infinité de nombres premiers de la forme:*

1. $3k + 2$
2. $4k + 3$
3. $6k + 5$

Remarque 1. *En fait on connait de manière plus précise la répartition des nombres premiers: on montre que le nombre de nombre premiers inférieurs ou égaux à x (noté $\pi(x)$)est équivalent à $x/ln(x)$ quand x tend vers ∞. C'est un résultat important mais assez difficile à démontrer.*

On en déduit le théorème de raréfaction de Legendre.

Théorème 2. *$\pi(x)/x$ tend vers 0.*

Mais on peut estimer un peu mieux cette raréfaction grâce au théorème d'Euler.

Théorème 3 (Euler)**.** *La série des $1/p$ est divergente.*

1.2 Théorème fondamental de l'arithmétique

Lemme 1. *Tout nombre admet un diviseur premier.*

Théorème 4. *Tout nombre entier naturel s'écrit de manière unique (à une permutation des indices près) sous la forme $p_1^{\alpha_1} \dots p_n^{\alpha_n}$ avec les p_i premiers. On a donc une écriture unique sous la forme $p_1^{\alpha_1} \dots p_n^{\alpha_n}$ en imposant $p_1 < p_2 \dots p_n$.*

Exemple 2.

Définition 2. *On appelle valuation p-adique d'un entier naturel x (notée $v_p(x)$) l'exposant de p dans la décomposition de x en facteurs premiers (0 si il n'apparait pas).*

On a les propriétés:

Proposition 3. *$v_p(ab) = v_p(a) + v_p(b)$, $v_p(a^n) = nv_p(a)$, idem pour un nombre fini de termes.*

On peut réécrire le théorème sous la forme suivante:

Proposition 4. *Tout nombre entier peut s'écrire de manière unique sous la forme $\prod_p p^{v_p(x)}$.*

Remarque 2. *On se limite aux naturels ici mais on peut passer aux relatifs en mettant -1 devant. Donc tout entier s'écrit de manière unique sous la forme $(-1)^{\varepsilon(x)} p_1^{\alpha_1} \dots p_n^{\alpha_n} = \prod_p p^{v_p(x)}$.*

1.3 Applications du théorème fondamental de l'arithmétique

[3]

1.3.1 Nombres de diviseurs

Application 1. *Soit a et b deux entiers. une CNS pour que a/b est que pour tout p, $v_p(a) \leqslant v_p(b)$*

Corollaire 1. *Le nombre de diviseurs de a est $\prod(1 + v_p(a))$.*

1.3.2 $a^n | b^n$

Corollaire 2. *[3] a/b ssi $a^n | b^n$ pour un $n \leqslant 1$.*

1.3.3 Valuation p-adique d'un rationnel et application

Définition 3. *On appelle valuation p-adique d'un rationnel la différence entre la valuation de son numérateur et de son dénominateur.*

On a les mêmes propriétés que celle de la valuation sur $\mathbb{Z}$.

Proposition 5. *Un rationnel est entier ssi tous les v_p sont positifs ou nuls.*

Application 2. *On considère les suites partielles de la série harmonique $\sum \frac{1}{n}$. Alors sauf pour $n = 1$, ces sommes partielles ne sont jamais entières (car la valuation 2-adique est toujours strictement négative.)*

1.3.4 Théorème des 4 carrés

Définition 4. *On note Σ l'ensemble des nombres s'écrivant comme somme de quatre carrés.*

Proposition 6. *Σ est stable par produit (par l'identité d'Euler)*

Lemme 2. *Σ contient tous les nombres premiers.*

Théorème 5. *Tout nombre s'écrit comme somme de 4 carrés.*

2 Tests de primalité. Classes de nombres premiers

On sait qu'il y a une infinité de nombres premiers mais ce n'est pas pour cela qu'on sait en construire d'aussi grands que l'on veut. D'où ce paragraphe.

2.1 Critères de primalité

Remarque 3. *Ces critères sont tous assez peu intéressant car pas effectifs. On verra après des méthdoes un peu plus effectives.*

Théorème 6 (Wilson)**.** *p premier ssi* $(p-1)! \equiv 1[p]$.

Théorème 7. *[1][page 277] p premier ssi* $(p!)^2 \equiv +-1[p]$.

2.2 Autour du petit théorème de Fermat

On connait le théorème suivant (Fermat):

Proposition 7. *Si p est premier,* $a^p \equiv a[p]$.

On a une réciproque partielle.

Théorème 8. *Soit un entier* $n \geqslant 2$ *vérifiant:* $\exists a \in \mathbb{Z}$ *tel que* $a^{(n-1)} \equiv 1[n]$ *et* $\forall k < n-1$, $a^k \not\equiv [n]$. *Alors n est premier.*

Théorème 9. *Soit un entier* $n \geqslant 2$ *dont la décomposition en facteurs premiers est* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *vérifiant:* $\forall i, \exists a_i \in \mathbb{Z}$ *tel que* $a_i^{(n-1)/p_i} \simeq 1[n]$ *et* $\forall k < n-1$, $a^k \not\simeq 1[n]$. *Alors n est premier.*

Théorème 10. *Soit p un nombre premier. Soit* $h \in \{1, \dots, p-1\}$. *On pose* $n := 1 + hp^2$ *et on suppose que* $2^{n-1} \simeq 1[n]$ *mais* $2^h \not\simeq 1[n]$. *Alors n est premier.*

Ce dernier test permet d'obtenir des grands nombres premiers.

Exemple 3. $p = 2^{127} - 1$ *est premier et* $h = 190$ *convient, donc* $1 + 190p^2$ *est premier).*

2.3 Nombres de Mersenne

[2]

Théorème 11. *Pour qu'un nombre de la forme* $a^n - 1$ *soit premier, il est nécessaire que* $a = 2$ *et n est un nombre premier.*

Définition 5. *Des nombres de la forme* $2^p - 1$ *sont appelés nombres de Mersenne noté* M_p

Réciproque fausse.

Exemple 4. $2^1 1 - 1 = 23 * 89$.

On aime bien utiliser les nombres de Mersenne pour trouver des grands nombres premiers car le résultat suivant donne encore une condition nécessaire plus forte.

Théorème 12. *Si p est un nombre premier de la forme* $4k+3$ *et si* $2p+1$ *est premier alors* M_p *n'est pas premier.*

Mais en fait,o n a même une CNS pour qu'un nombre de Mersenne soit premier.

Théorème 13. *On définit la suite* Y_n *la suite définie par* $Y_0 = 2$ *et* $Y_{n+1} = 2Y_n^2 - 1$. *Pour* $n \geqslant 3$, M_n *est premier ssi* $(2^n - 1) | Y_{n-2}$.

Ce test a permis d'exhiber le plus grand nombre premier connu à ce jour: $2^{3112609} - 1$. On ne sait toujours pas à l'eheure actuelle si il y a un nombre fini ou infini de M_p premiers...

3 Applications

3.1 Corps finis

Théorème 14. *Tout corps fini k est de caractéristique non nulle et donc sa caractéristique est un nombre premier p. k est donc un $\mathbb{Z}/p\mathbb{Z} - ev$ de dimension finie et il existe un n tel que $|k| = p^n$.*

On a aussi la récriproque.

Théorème 15. *Soit $q = p^n$. Alors il existe un corps de cardinal q et de caractéristique p, on peut prendre par exemple le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. De plus, K est unique à isomorphisme près. Ce corps est noté $\mathbb{F}_q$.*

Les nombres premiers sont donc un outil indispensable en théorie des corps. Pour les corps intermédiaires citons:

Proposition 8. *$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ ssi $n|m$.*

3.2 Résidus quadratiques et conséquences

Définition 6. *Un résidu quadratique modulo p est un carré de $\mathbb{F}_p$.*

Proposition 9. *Il y a (p+1)/2 résidus quadratiques dans $\mathbb{F}_p$ ((p-1)/2 si on exclut 0)*

Proposition 10. *a est un résidu quadratique ssi l'équation $x^2 - a = 0$ a une solution dans $\mathbb{F}_p$ ssi il existe un diviseur premier de la forme $x^2 - 5y^2$ avec x et y premiers entre eux.*

Corollaire 3. *-1 est un carré dans K ssi q est congru à 1 modulo 4.*

Lemme 3. *Un nombre premier est somme de deux carrés ssi il vaut 2 ou est congru à 1 modulo 4.*

Application 3 (Théorème des deux carrés)**.** *Un entier est somme de deux carrés ssi la valuation de tous les nombres premiers congrus à 3 modulo 4 est paire.*

Ce théorème donne en plus une caractérisation de tous les irréductibles de l'anneau des entiers de Gauss $\mathbb{Z}[i]$ car on montre qu'un élément irréductible est soit nombre premier congru à 3 modulo 4 soit un entier de gauss dont la norme est un nombre premier.

Application 4. *Il existe une infinité de nombres premiers vérifiant $p = 4m + 1$.*

3.3 Symbole de Legendre, réciprocité quadratique

Définition 7. *Symbole de Legendre $(\frac{p}{q}) = p^{\frac{q-1}{2}}$.*

Proposition 11. *Le symbole est un morphisme de groupe de $\mathbb{Z}/p\mathbb{Z}$ sur $\{-1, 1\}$. Donc l'ensemble des carrés est un groupe abélien.*

Proposition 12. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

On a l'important théorème suivant

Théorème 16 (réciprocité quadratique[2])**.** $(\frac{p}{q})(\frac{q}{p}) = (-1)^{(\frac{p-1}{2}\frac{q-1}{2})}$

Exemple 5. *-627 est un carré dans $\mathbb{F}_17$. 5 n'est pas un carré dans $\mathbb{F}_{1987}$. -5 est un carré dans $\mathbb{F}_p$ ssi p est un nombre premier de la forme $20k + 1, 3, 7, 9$.*

Application 5. *Il existe une infinité de nombres premiers de la forme:*

1. *6n+1*
2. *10n-1*

3. 4n-1

Remarque 4. *Cas particuliers du théorème de Dirichlet qui dit : si a et b sont premiers entre eux il existe une infinité de nombre premiers de la forme a+nb, mais ces démonstrations ont l'avantage d'être élémentaires.*

On peut démontrer à l'ai de des polynômes cyclotomiques et de manière élémentaire le résultat suivant:

Théorème 17 (Petit theroreme de Dirichlet)**.** *[1][page 272] Il existe une infinité de nombres premiers de la forme an+1.*

3.4 Irréductibilité de polynômes

Théorème 18 (Réduction modulo p)**.** *Soit p un nombre premier premier et soit* $P \in \mathbb{Z}[X]$, $P = a_nX^n + \ldots + a_0$. *On pose* $\bar{P} = C_I(a_n)X^n + \ldots + C_I(a_0)$. *Si* $\bar{P}$ *est irréductible dans* $\mathbb{Z}/p\mathbb{Z}$, *alors P est irréductible dans* $\mathbb{Q}[X]$ *(et donc dans* $\mathbb{Z}[X]$ *si P est primitif).*

Exemple 6. *Soit p un nombre premier.* $X^p - X - 1$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/p\mathbb{Z}$*).*

Rappelons les lemmes suivants, bien utiles.

Lemme 4. *Un polynôme de degré 2 ou 3 est irréductible ssi il admet une racine*

Exemple 7. *En application directe du théorème et du lemme précédent on a aussi l'irréductibilité des polynômes suivants:*

1. $X^3 + 462X^2 + 2433X - 67691$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/2\mathbb{Z}[X]$*)*
2. $X^3 + 4X^2 - 5X + 7$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/2\mathbb{Z}[X]$*)*
3. $X^3 - 6X^2 - 4X - 13$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/3\mathbb{Z}[X]$*)*
4. $X^3 + 30X^2 + 6X + 1$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/5\mathbb{Z}[X]$*)*

Signalons le lemme suivant, qui est aussi utile.

Lemme 5. $X^2 + X + 1$ *est l'unique polynôme irréductible de degré 2 sur* $\mathbb{F}_2$. *Donc tout polynôme n'admettant pas de racines dans* $\mathbb{F}_2$ *et distinct de* $(X^2 + X + 1)^2 = 1 + X^2 + X^4$ *est irréductible.*

Exemple 8.
1. $5X^4 + 17X^3 - X^2 - 6X + 23$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/2\mathbb{Z}[X]$*)*
2. $X^4 + 5X^3 - 3X^2 - X + 7$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/2\mathbb{Z}[X]$*)*

dans $\mathbb{F}_3$ on a

Lemme 6. *Les polynômes irréductibles unitaires de degré 2 sont* X^2+1, X^2-X-1 *et* X^2+X-1. *Donc tout polynôme de degré 4 sans racines dans* $\mathbb{F}_3$ *et non divisible par un de ces polynômes est irréductible.*

Exemple 9.

$X^4 + 7X^24X + 1$ *est irréductible sur* $\mathbb{Z}$ *(car il l'est sur* $\mathbb{Z}/3\mathbb{Z}[X]$*, alors qu'i lest réductible sur* $\mathbb{Z}/2\mathbb{Z}[X]$*)*

On peut généraliser cette méthode à des polynôems de degré plus grands. On a aussi une application plus subtile du théorème.

Exemple 10. $X^4 + 4X^3 + 3X^2 + 7X - 4$ *est réductible modulo* $2, 3, 5, 7et11$*, on n'arrive donc pas à conclure directement. Mais on montre en utilisant la forme factorisée modulo 3 que P ne peut admettre de racines dans* $\mathbb{Z}$ *et on montre en utilisant la forme factorisée modulo 2 qu'il ne peut pas non plus se mettre sous forme de produits de polynômes de degré 2 irréductibles. Il est donc bien irréductible.*

Réciproque du théorème de réduction fausse.

Exemple 11. $X^4 + 1$ *irréductible sur* $\mathbb{F}_p$ *mais réductible sur tous les* $\mathbb{F}_p$.

3.5 Système de cryptage RSA.[1]

Ce système repose sur le principe suivant: Si l'on se donne un nombre N grand, (ayant par exemple une écriture décimale à 150 ou 200 chiffres), un ordinateur mettrait des dizaines d'années à calculer les facteurs premiers de N. Soit E un réseau de personnes souhaitant communiquer entre elles. Le chef du réseau choisit deux entiers premiers très grands p et q, pose $N := pq$ et calcule $\varphi(n) = (p-1)(q-1)$. Pour chaque membre A du réseau, il choisit e_A premier avec $\varphi(N)$ et il calcule un inverse d_A de e_A modulo $\varphi(N)$. Il publie e_A et N mais garde secret $\varphi(N)$. Il communique à chaque membre du réseau son d_A que celui-ci garde secret. Pour envoyer un message, l'expéditeur A (qui souhaite communiquer avec B) code les caractères du message en nombres, puis fabrique des suites de nombres de longueur strictement inférieur à la longueur de p et q (pour assurer que ces suites de nombres soient premières à N). Soit M une telle suite. A calcule le reste X modulo N de M^{e_B} et le transmet à B. Celui-ci peut reconstituer la suite (grâce au théorème d'Euler) en calculant X^{d_B}.

Developpements: réduction modulo p + exemple non trivial, théorème des 4 carrés, théorème des deux carrés.

References

[1] Combes

[2] Gourdon algèbre

[3] arithmétique pour amateurs

[4] Perrin

[5] Ortiz

[6] Lang