Leçon 121 - Nombres premiers. Applications.

1. Arithmétique dans $\mathbb{Z}$. —

1. Nombres premiers, premiers entre eux. —

- Def : On dit que $n \in \mathbb{Z}$ est un nombre premier si $n \neq \mathbb{Z}$ et si ses seuls diviseurs positifs sont 1 et lui-même.
- Rem : Les nombres premiers sont les irréductibles de l'anneau $\mathbb{Z}$.
- Def : On note $\mathscr{P}$ l'ensemble des nombres premiers positifs.
- Pro : Tout entier $n \geq 2$ possède un diviseur premier.
- Def : On dit que deux nombres $a, b \in \mathbb{Z}$ sont premiers entre eux s'il n'existe aucun nombre premier p tel que $p|a$ et $p|b$. On note alors $a \wedge b = 1$.
- Théorème de Gauss : Soient $a, b, c \in \mathbb{Z}$. On a :
  i) Si $a \wedge b = 1$ et $a|bc$, alors $a|c$.
  ii) Si $a \wedge b = 1$, $a|c$, et $b|c$, alors $ab|c$.
- App : $p|\binom{p}{k}$ pour tout $1 \leq k \leq p-1$.
- Rem : Un test naïf pour savoir si n est premier revient à calculer la division euclidienne de n par d pour tout $1 \leq d \leq n$. On peut en réalité s'arrêter à $\sqrt{n}$.

2. Décomposition en facteurs premiers. —

- Théorème fondamental de l'arithmétique : Tout nombre entier n non-nul s'écrit de la forme : $n = \pm p_1^{a_1}...p_r^{a_r}$ avec $p_1, .., p_r \in \mathscr{P}$.
  De plus, cette décomposition est unique à l'ordre près.
- Rem : Cela équivaut à dire que $\mathbb{Z}$ est factoriel, càd que tout nombre admet une unique décomposition en produit d'irréductibles.
- Cor : $\mathscr{P}$ est infini.
- Def+Pro : $pgcd(a, b)$, $ppcm(a, b)$, leur forme.
- Rem : a et b sont premiers entre eux ssi leur pgcd vaut 1.
- Pro : Il existe une infinité de nombres premiers de la forme $6k + 5$.
- Théorème de Bézout : Soient $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = pgcd(a, b)$.

3. Fonctions arithmétiques. —

- On appelle fonction arithmétique toute fonction $f : \mathbb{N}^* \to \mathbb{C}$.
- Ex : $d(n)$ le nombre de diviseurs positifs de n.
- Def : On définit l'indicatrice d'Euler de n, $\phi(n)$, comme le nombre de $1 \leq k \leq n$ qui sont premiers à n.
- Def : On définit la fonction de Moëbius :
  $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par : $\begin{cases} 0 \text{ si n a un facteur carré} \\ (-1)^r \text{ si } n = p_1..p_r \text{ avec } p_i \text{ premiers distincts} \end{cases}$
- Def : Une fonction arithmétique f est multiplicative ssi pour tout $m \wedge n = 1$, on a $f(m.n) = f(m)f(n)$.
- Pro : ϕ et μ sont multiplicatives.
- Pro : On a $\phi(n) = n.\Pi_{p \in \mathscr{P}, p|n}(\frac{p-1}{p})$, et $n = \sum_{d|n} \phi(d)$
- Formule d'inversion de *Moëbius* : Pour $f, g : \mathbb{N}^* \to \mathbb{C}$, on a :
  $(g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}))$.
- App : $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.
- App : Pour $r > 1$, la série $\sum_n \frac{1}{n^r}$ est une série absolument convergente, avec :
  $(\sum_n \frac{1}{n^r})(\sum_n \frac{\mu(n)}{n^r}) = 1$

4. Répartition des nombres premiers. —

- Pro : Crible d'Eratosthène : Afin de trouver tous les nombres premiers compris entre 1 et n, enlève à l'ensemble $\{2, .., n\}$ tous les nombres multiples de 2. Le plus petit nombre restant dans cet ensemble sera alors premier.
  On réitère ensuite le procédé en enlevant de l'ensemble tous les nombres multiples du second nombre premier, et en regardant le plus petit élément restant après cela.
- Théorème de Dirichlet (version faible)(admis) : Pour tout $\lambda \geq 1$, il existe une infinité de nombres premiers de la forme $1 + \lambda.n$.
- Théorème des nombres premiers : Lorsque n tend vers $+\infty$, le nombre $\pi(n)$ de nombres premiers dans $\{1, .., n\}$ est équivalent à $\frac{n}{ln(n)}$.
- App : La série $\sum_{p \in \mathscr{P}} \frac{1}{p}$ diverge.

2. Corps finis. —

1. Propriétés des corps finis. —

- Def+Pro : Pour tout corps K, le noyau de l'unique morphisme d'anneaux de $\mathbb{Z}$ vers K est un idéal de $\mathbb{Z}$.
  Si cet idéal est réduit à $\{0\}$, on dit que K est de caractéristique 0. S'il est engendré par $n \geq 1$, on dit que K est de caractéristique n.
- Pro : Si $car(K) \neq 0$, alors $car(K) = p$ pour p premier.
- Pro : Les seuls anneaux $\mathbb{Z}/n\mathbb{Z}$ qui sont des corps sont les $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ pour p premier.
- Pro : Pour K un corps fini, $car(K) \neq 0$. Pour p la caractéristique de K, K est une $\mathbb{F}_p$-algèbre , de dimension finie en tant que $\mathbb{F}_p$-espace vectoriel.
  On a ainsi $Card(K) = p^n$ pour un $n \geq 1$.
- Rem : Il n'existe ainsi aucun corps de cardinal 4 ou 105.
- Thm : Pour tout p premier, pour tout $n \geq 1$, il existe un corps fini de cardinal p^n.
  Un tel corps est unique à isomorphisme de $\mathbb{F}_p$-algèbre près. On le note $\mathbb{F}_{p^n}$.
- Rem : L'ensemble des éléments de $\mathbb{F}_{p^n}$ est solution de $x^{p^n} = x$. Le polynôme $X^{p^n} - X$ est ainsi scindé à racines simples sur $\mathbb{F}_{p^n}$.
- Pro : Pour tout $d|n$, l'ensemble des $x \in \mathbb{F}_{p^n}^*$ d'ordre d est exactement l'ensemble des solutions de $X^{p^d} - 1$ dans $\mathbb{F}_{p^n}$.
- App : $\mathbb{F}_{p^n}^*$ possède des éléments d'ordre q. Ce groupe est donc cyclique d'ordre $p^n - 1$.
- App : Théorème de Wedderburn : Soit A un anneau intègre fini (non supposé unitaire ou commutatif). Alors A est un corps fini.

- Pro : Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ pour $d|n$, qui sont exactement les $\{x \in \mathbb{F}_{p^n} tq x^{p^d} = x\}$.
- Ex : Dessin d'un treillis d'extensions de $\mathbb{F}_2$.
- Cor : Les $x \in \mathbb{F}_{p^n}$ tels que $\mathbb{F}_{p^n} = \mathbb{F}_p(x)$ sont exactement les éléments tels que $ord(x)|p^n - 1$ et $ord(x)| \nmid p^d - 1$ pour tout $d|n$.
- Def : On définit le morphisme de Frobenius, Frob, sur $\mathbb{F}_{p^n}$ par $Frob(x) = x^p$.
- Pro : Frob est un automorphisme de $\mathbb{F}_{p^n}$ dont l'ensemble des points fixes est $\mathbb{F}_p$.
- Thm : Le groupe des automorphismes de $\mathbb{F}_{p^n}$ qui laissent $\mathbb{F}_p$ stable est cyclique, de cardinal n, engendré par Frob.

2. Carrés dans $\mathbb{F}_{p^n}$. —

- Def : On définit $\mathbb{F}_{p^n}^2$ l'image de $x \mapsto x^2$ sur $\mathbb{F}_{p^n}$.
  On définit de même $(\mathbb{F}_{p^n}^*)^2$ l'ensemble des carrés de $\mathbb{F}_{p^n}^*$.
- Pro : Si $p = 2$, alors tous les éléments de $\mathbb{F}_{p^n}$ sont des carrés.
  Si $p \neq 2$, $Card(\mathbb{F}_{p^n}^*) = \frac{p^n-1}{2}$.
- Pro : Si $p \neq 2$, $x \in \mathbb{F}_{p^n}^*$ est un carré ssi $x^{\frac{p^n-1}{2}} = 1$.
- App : -1 est un carré dans $\mathbb{F}_{p^n}$ ssi $p^n \equiv 1\ mod(4)$.
- App : Il existe une infinité de nombres premiers de la forme $4k + 1$.
- Def : Pour tout $x \in \mathbb{F}_p$, on définit $(\frac{x}{p}) = \begin{cases} 1 \text{ si x} \in (\mathbb{F}_p^*)^2 \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$ le symbole de Legendre.
- Pro : Le symbole de Legendre définit une fonction complètement multiplicative : $(\frac{mn}{p}) = (\frac{m}{p})(\frac{n}{p})$ pour tout $m, n \in \mathbb{N}^*$.
- Pro : $(\frac{x}{p}) = x^{\frac{p^n-1}{2}}$.
- Ex : $(\frac{-1}{p}) = (-1)^{\frac{p-1}{4}}$.
- Pro : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.
- **Dev** : Loi de réciprocité quadratique : Soient p,m des nombres premiers impairs distincts.
  Alors $(\frac{p}{m}) = (\frac{m}{p}).(-1)^{\frac{p-1}{2}.\frac{m-1}{2}}$.
- Ex : $(\frac{23}{59}) = -1$
- Thm : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ La loi de réciprocité quadratique, les formules pour -1 et 2, et la division euclidienne permettent de toujours calculer le symbole de Legendre $(\frac{q}{p})$.
- Ex : $(\frac{23}{59}) = -1$. L'équation $x^2 + 59y = 23$ n'a pas de solutions.

3. Réduction modulo p. —

- Pro : Soit $P \in \mathbb{Z}[X]$ et p premier ne divisant pas le coeff dominant de P. Si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.
- Critère d'Eisenstein : Soit $P(X) = a_n X^n + .. + a_0 \in \mathbb{Z}[X]$. Si il existe p premier tel que $p \nmid a_n$, $p|a_i\ \forall 0 \leq i \leq n-1$, $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Z}[X]$.
- **Dev** : Pour tout $n \geq 1$, on définit $\Phi_n(X) := \Pi_{k \wedge n = 1,\ k \leq n}(X - e^{2i\pi\frac{k}{n}} \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique.
  Alors Φ_n est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbb{Z}[X]$, de degré $\phi(n) = Card(\mathbb{Z}/n\mathbb{Z}^*)$ et tel que $\Pi_{d|n}\Phi_d = X^n - 1$.
- Def : On définit $\mathbb{Z}[i]$ l'anneau engendré par $\mathbb{Z}$ et i.
- Pro : $\mathbb{Z}[i]$ est un anneau euclidien pour $|x+iy| = \sqrt{(x+iy)(x-iy)}$, et ses éléments inversibles sont ± 1, $\pm i$.
- **Dev** : Théorème des deux carrés de Fermat : Les irréductibles de $\mathbb{Z}[i]$ sont les p premiers tq $p \equiv 3\ mod(4)$ et les $a + ib$ tq $a^2 + b^2$ est premier.
  L'équation diophantienne $x^2 + y^2 = n$ admet des solutions si et seulement si pour tout p premier tq $p \equiv 3$ mod(4), on a $v_p(n)$ pair.

3. Nombres premiers en théorie des groupes. —

1. Résultats sur les p-groupes. —

- Def : Un p-groupe est un groupe de cardinal une puissance de p.
- Ex : $\mathbb{Z}/125\mathbb{Z}$ est un 5-groupe. D_4 est un 2-groupe.
- Pro : Le centre d'un p-groupe est non-trivial.
- App : Les groupes d'ordre p^2 sont isomorphes à $\mathbb{Z}/p^2\mathbb{Z}$.
- Théorème de Cauchy : Pour G un groupe de cardinal n et p premier divisant n, il existe un $g \in G$ d'ordre p.

2. Théorème de Sylow. —

- Def : Soit G un groupe de cardinal n, et p premier tel que $n = p^a n'$, avec $n' \wedge p = 1$. Un p-Sylow de G est un sous-groupe de G de cardinal p^a.
- Ex : $Gl_n(\mathbb{F}_p)$ est de cardinal : $(p^n - 1)(p^n - p)...(p^n - p^{n-1}) = \pi_{i \geq 1}(p^i - 1).p^{\frac{n(n-1)}{2}}$.
  Le sous-groupe $UT_n(\mathbb{F}_p)$ est de cardinal $p^{\frac{n(n-1)}{2}}$, et est donc un p-Sylow de $Gl_n(\mathbb{F}_p)$.
- Lemme : Pour H sous-groupe de G, et S' un p-Sylow de H, il existe S un p-Sylow de G tel que $S' = S \cap H$.
- Pro : Tout groupe de cardinal divisible par p admet un p-Sylow.
- Théorème de Sylow : Tous les p-Sylow d'un groupe G sont conjugués.
  Pour n_p le nombre de p-Sylow de G, on a $n_p | n'$ et $n_p \equiv 1\ mod(p)$.
- App : Si un goupe G ne possède qu'un seul p-Sylow, alors celui-ci est distingué.
- App : Aucun groupe d'ordre 63 n'est simple.
- App : Les groupes d'ordre pq pour p,q premiers, $p < q$ et $q \neq 1\ mod(p)$ sont cycliques.

4. Utilisation des nombres premiers en cryptographie. —

1. Cryptage RSA. —

- Thm : Soient p,q premiers et $e, d \in \mathbb{N}$.
  Si $ed \equiv 1\ mod((p-1)(q-1))$, alors $\forall x \in \mathbb{N}$, $x^{ed} \equiv x\ mod(pq)$.
- Procédé : Un organisme choisit deux grands nombres premiers p et q au hasard, et calcule n=pq. Il choisit d premier avec $(p-1)(q-1)$ et calcule e l'inverse de d dans

$\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$.
Il émet alors une clé publique constituée de n et d.
Un utilisateur va choisir son message $x \in \mathbb{Z}/n\mathbb{Z}$, puis le chiffrer en calculant $m = x^d$ dans $\mathbb{Z}/n\mathbb{Z}$ avant d'envoyer son message chiffré m.
L'organisme peut alors déchiffrer le message chiffré en calculant $m^e = x^{ed} = x$.
Les calculs de chiffrement et de déchiffrement sont rapides grâce à de l'exponentiation binaire.
Trouver e revient exactement à trouver p et q, càd à factoriser n. La sécurité du cryptage repose sur le fait que les meilleurs algorithmes de factorisation d'entiers n'ont une complexité que sous-exponentielle, ce qui limite fortement le temps et la puissance de calcul nécessaires pour factoriser un entier $n = pq$ de taille $\sim 2^{1024}$.

Références

Gourdon : Nombres premiers, décomposition en facteurs premiers. Th de Dirichlet faible, Th des nombres premiers. $\mathbb{Z}/n\mathbb{Z}$ corps, théorème chinois. Chiffrement RSA.
Perrin : Corps finis, caractéristique, construction, Frobenius. $\mathbb{Z}[i]$, propriétés, Th des deux carrés.(Dev) Poly irréductibles, critère d'Eisenstein, réduction modulo p, exemples, contre-ex, Polynômes cyclotomiques.(Dev) p-groupes, p-Sylow.
Caldero,Germoni : Symbole de Legendre, propriétés, exemples, Loi de réciprocité quadratique.(Dev)
FGN (Algèbre 1): Fonction de Moëbius, formule de Moëbius.
FGN : $\sum_p \frac{1}{p}$ diverge.
Demazure : Fonctions arithmétiques.
Ulmer : p-groupes.

June 7, 2017

Vidal Agniel, École normale supérieure de Rennes