Leçon 121 : Nombres premiers. Applications

Cadre :

1. Rapport du jury. — 2017 : *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.*

2. Définition et premières propriétés. —

1. *Introduction.* —

- Def : Nombre premier dans $\mathbb{N}$ et dans $\mathbb{Z}$. Notation $\mathbb{P}$ pour l'ensemble des nombres premiers positifs.
- Pro : 1 et -1 sont les inversibles de $\mathbb{Z}$, $\mathbb{P} \cup -\mathbb{P}$ est l'ensemble des irréductibles de $\mathbb{Z}$. Par défaut on sera dans $\mathbb{N}$.
- *Notions utiles et voisines* : "premiers entre eux", pgcd, ppcm (attention : aux inversibles près).
- Pro :
  - (i) Deux nombres premiers sont premiers entre eux ;
  - (ii) Tout nombre premier p est premier avec tout $i \in [\![1, p-1]\!]$.
  - (iii) Un nombre premier est premier avec tout nombre qu'il ne divise pas.
  - (iv) Tout entier naturel supérieur à 2 possède au moins un diviseur premier.
  - (v) Gauss (Si p est premier, alors $(p|ab \Rightarrow p|a \ ou \ p|b)$)
  - (vi) Euclide (les idéaux engendrés par des nombres premiers sont des idéaux premiers)

Crible d'Eratosthène : Afin de trouver tous les nombres premiers compris entre 1 et n, on enlève à l'ensemble $2, \cdots n$ 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.

Exe Nous avons des familles de nombres associées historiquement aux nombres premiers :

- Nombres de Fermat ($F_t = 2^{2^t} + 1$). Fermat les imaginait premiers mais ils le sont "rarement" (on n'en connaît guère au-delà de F_4 et on conjecture qu'ils sont en nombre fini). $F_2 = 17$. Nota : $\Pi_{0 \leq k \leq n} = F_{n+1} - 2$ ce qui permet de prouver que $F_n \wedge F_m = 1$, et d'en déduire alors qu'il existe une infinité de nombres premiers.
- Nombres de Mersenne ($2^p - 1$) parmi lesquels se trouvent les plus grands nombres premiers "découverts". Nota : il est nécessaire que p soit lui-même premier pour que $2^p - 1$ puisse l'être (condition non suffisante).
- Nombres de Sophie Germain. Nombres premiers de la forme $2p+1$ où p est lui aussi premier.

Quelques propriétés

- *Test de Wilson* p est premier ssi $(p-1)! \equiv -1 \ (mod\, p)$. Théorème plus utile pédagogiquement que comme critère de primalité.
- *Petit théorème de Fermat* $\forall a \in \mathbb{Z}$, $\forall p \in \mathbb{P}$, $a^{p-1} \equiv 1 \ (mod.p)$
- *Remarque* : réciproque fausse et existence d'une infinité de nombres de Carmichael (admis).
- $\forall p \in \mathbb{P}$, $\forall k \in \mathbb{N}$ tel que $k \leq p$, $p|C_p^k$
- Si $n \notin \mathbb{P}$, il existe un nombre premier divisant n et inférieur ou égal à $\sqrt{n}$. Cela permet de réaliser des vérifications de primalités plus courtes.
- $\mathbb{Z}$ est euclidien, factoriel et principal. Ses idéaux premiers sont ceux engendrés par les nombres premiers. Ils sont maximaux. On a donc que : ($\mathbb{Z}/p\mathbb{Z}$ est intègre (ie (p) est premier)) ssi ($\mathbb{Z}/p\mathbb{Z}$ est un corps (ie (p) est maximal)) ssi (p est premier).

3. Répartition. —

- L'ensemble des nombres premiers est infini. Il existe plusieurs démonstrations :
  - Démonstration d'Euclide.
  - variante : construire un nombre premier supérieur au plus grand élément grâce au nombre de Mersenne associé à ce pge.
  - Preuve de Goldbach basée sur le caractère infini des nombres de Fermat pourtant deux à deux premiers entre eux.
  - La série harmonique limitée aux nombres premiers diverge : ils sont donc infinis.
- Il existe des séquences arbitrairement longues sans nombre premier : $\forall i$ tel que $2 \leq i \leq n$, $n! + i$ n'est pas premier car divisible par i.
- Développement - Le gap est cependant majoré par n : "*Il existe au moins un nombre premier entre n et 2n*".
- Il s'agit du *Postulat de Bertrand*. Conjecturé par Joseph Bertrand et démontré par Chebishef en 1850, démonstration grandement simplifié par la suite (notamment par Paul Erdos).
- (admis) Le gap entre deux nombres premiers consécutifs, qui est au plus n d'après Bertrand-Chebishef est ponctuellement inférieur à une constante : quelque soit $\mathbb{N}$, on peut trouver deux nombres entiers premiers p et q distants de moins d'une constante K. Résultat majeur prouvé par Yitang Zang en 2014 avec une constante de $K = 7.10^7$. Amélioré par la communauté des mathématiciens (PolyMath) en $K = 246$)
- (Admis)Théorème de Hadamard et de la Vallée Poussin - Le nombre $\pi(n)$ de nombres premiers dans $1, \cdots, n$ est équivalent au voisinage de ∞ à $\frac{n}{Ln(n)}$. On a donc l'ordre de grandeur de la probabilité d'occurrence d'un nombre premier .

1. *Exemple important : somme de deux carrés.* — Développement : 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 que la valuation p-adique $\nu_p(n)$ est paire.

– On montre au passage que les ensembles de nombres premiers congrus à 1 modulo 4 (resp. congrus à 3 modulo 4) sont tous deux infinis.
– Rem : ce résultat est un cas particulier d'un théorème célèbre, important et difficile dû à Dirichlet, le théorème de la progression arithmétique des nombres premiers. Etant donnés a, b premiers entre eux, il existe une infinité de nombres premiers de la forme $ka + b$.
– Rem : on observe cependant numériquement une probabilité d'occurrence plus forte des nombres premiers de la forme $4k + 3$ que de la forme $4k + 1$, phénomène connu comme le "*biais de Chebishev*".

4. Des entités omniprésentes en mathématiques et ailleurs. —

– Algèbre : caractéristique ($p \in \mathbb{P}$) et cardinal ($p^\alpha \in \mathbb{P}$)des corps finis.
– Algèbre : les groupes d'ordre p sont cycliques.
– Algèbre : théorème de Cauchy, de Sylow, de Wedderburn (Développement).
– Algèbre : Frobénius
– Biologie : symétries, périodes de reproduction des cigales, ...
– Transmission de signaux : aussi bien cryptographie (chiffrage à clef publique) que codes correcteurs.

5. Quelques conjectures et un théorème célèbres. —

– *Hypothèse de Goldbach* (un nombre pair est somme de deux nombres premiers)
– *Hypothèse de Riemann* : les zéros non triviaux sont sur la droite $Re(z) = 1/2$.
– *Infinité des nombres premiers jumeaux* : il existe une infinité de nombres premiers distant de 2 unités.(démontré pour une distance de 246, cf supra)
– *Problème de Lehmer* : Si n vérifie $n \equiv 1$ modulo $\phi(n)$, est-il nécessairement premier ?
– *Grand théorème de Fermat-Wiles* : $a^n + b^n = c^n$ n'a pas de solutions entières pour $n > 2$.

6. Applications importantes. —

– Grands nombres premiers : critère de Lucas-Lehmer pour les nombres de Mersenne.
– Grands nombres premiers : on exclue des nombres non premiers grâce à des conditions nécessaires de primalité. Exemples : Rabin-Miller ;

1. *Développements :* —

– Postulat de Bertrand
– Théorème des deux carrés

2. *Sources :* —

– YouTube
– Wikipédia
– Proofs from THE BOOK
– Francinou et Gianella

December 27, 2017

Bruno Nitrosso, EPP et indépendant