Aperçu de l’étude des nombres premiers

Bodart Corentin Jonathan Dauwe Azalais Davin Thomas Lemaire Robin Petit Alex Ternes

Université Libre de Bruxelles

4 mai 2016

Plan de la présentation

Euclide

les nbres de Wilson

Objectif

Prouver le théorème suivant grâce à la théorie des groupes :

Théorème (Petit théorème de Fermat (1640))

Soient $a, p \in \mathbb{Z}$ *tels que* p *est premier et* a *n'est pas divisible par* p*.*
Alors $a^{p-1} - 1$ *est un multiple de* p*, c'est-à-dire :*

$$a^{p-1} - 1 \equiv 0 (\mod p).$$

Préliminaires à la preuve

Définition

Soient G un groupe et $a \in G$. L'**ordre** de a est :

- le plus petit $m \in \mathbb{N}^*$ tel que $a^m = e$, où e est le neutre de G ;
- le cardinal du sous-groupe engendré par a, c-à-d : $\langle a \rangle := \{e = a^0, a^1, \ldots, a^{m-1}\}$.

L'ordre de a est noté $\operatorname{ord}(a)$.

Théorème (Thorème de Lagrange)

Si G est un groupe fini et $H \subseteq G$ un sous-groupe, alors $|H|$ divise $|G|$.

Rappel (Petit théorème de Fermat)

$\forall a, p \in \mathbb{Z} : (p \text{ premier } \wedge p \nmid a) \Rightarrow (a^{p-1} - 1 \equiv 0 (\bmod p))$

Preuve du petit théorème de Fermat - partie 1/2

On considère le groupe $(\mathbb{Z}/p\mathbb{Z}^*, \cdot, 1)$. En effet, $\mathbb{Z}/p\mathbb{Z}^* = \{[1], [2], \ldots, [p-1]\}$ car p est premier.
Soit maintenant $[a] \in \mathbb{Z}/p\mathbb{Z}^*$. a n'est pas divisible par p car $[0] = [p] = [kp] \notin \mathbb{Z}/p\mathbb{Z}^*$ pour $k \in \mathbb{Z}$.
Prenons $m \coloneqq \mathrm{ord}([a])$. Alors on sait :

- $[a]^m = [1]$;
- $\big|\langle a \rangle\big| = m$.

Puisque $\langle a \rangle$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}^*$, on sait par Lagrange que $m = \big|\langle a \rangle\big|$ divise $\big|\mathbb{Z}/p\mathbb{Z}^*\big| = p - 1$.

Rappel (Petit théorème de Fermat)

$\forall a, p \in \mathbb{Z} : (p \text{ premier } \wedge p \not| a) \Rightarrow (a^{p-1} - 1 \equiv 0 (\mod p))$

Preuve du petit théorème de fermat - partie 2/2.

On sait $m|p-1$, que l'on peut réécrire comme suit :

$$\exists k \in \mathbb{N} \text{ t.q. } m \cdot k = p - 1.$$

Finalement, on a :

$$\left[a^{p-1}\right] = [a]^{p-1} = [a]^{mk} = \left([a]^m\right)^k = [1]^k = [1].$$

On a effectivement $\left[a^{p-1}\right] = [1]$, ce qui signifie :

$$a^{p-1} \equiv 1 (\mod p).$$

$\square$

Généralisation du petit théorème de Fermat

Théorème (Théorème d'Euler (1761))

Soient $n \in \mathbb{N}^*$ *et* $a \in \mathbb{N}$ *tels que* a, n *soient premiers entre eux. Alors :*

$$a^{\phi(n)} \equiv 1(\textit{ mod } n)$$

Preuve.

La démonstration est assez similaire à celle du théorème de Fermat : on prend le groupe $(\mathbb{Z}/n\mathbb{Z}^*, \cdot, 1)$ qui correspond aux classes d'entiers inversibles $\mod n$ et dont le cardinal vaut $\phi(n)$. $\square$

Carmichaël

Lemme 1

Lemme (1)

Soit n, un entier naturel. $\sum_{d|n} \varphi(d) = n$.

Preuve du lemme (1) - partie 1/2

On effectue un double comptage :

$$n = \#\left\{1, 2, \ldots, n\right\} = \# \bigcup_{d|n} \left\{1 \leq x \leq n \mid \gcd(n, x) = d\right\}$$

$$= \sum_{d|n} \#\left\{1 \leq x \leq n \mid \gcd(n, x) = d\right\}$$

$$= \sum_{d|n} \#\left\{1 \leq \frac{x}{d} \leq \frac{n}{d} \mid \gcd\left(\frac{n}{d}, \frac{x}{d}\right) = 1\right\}$$

$$= \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d'|n} \varphi(d')$$

Preuve du lemme (1) - partie 2/2.

En effet,

- le plus grand diviseur commun de n et x est un diviseur de n ;
- puisque $\gcd(n, x)$ est bien défini, ces ensembles sont disjoints ;
- $\gcd(n, x) = d \iff \gcd\left(\frac{n}{d}, \frac{x}{d}\right) = 1$;
- par définition, $\varphi(d) = \#\{1 \leq x \leq d \mid \gcd(d, x) = 1\}$;
- en prenant $d \cdot d' = n$.

$\square$

Lemme 2

Lemme (2)

Soit p, un nombre premier et d, un diviseur de $p-1$. On prouve que

$$X^d - 1 = 0 \pmod{p}$$

a exactement d racines (distinctes) dans $\mathbb{Z}/p\mathbb{Z}$.

Preuve du lemme (2) - partie 1/2

On travaille sur le corps $\mathbb{Z}/p\mathbb{Z}$. On rappelle que
$A \cdot B = 0 \iff A = 0 \vee B = 0$.
De plus, par la division euclidienne des polynômes, on sait qu'un polynôme de degré n a au plus n racines.
Par le Petit Théorème de Fermat, on sait que :

$$X^{p-1} - 1 = 0$$

a exactement $p-1$ racines (les résidus inversibles/premier avec p).
De plus,

$$X^{p-1} - 1 = \left(X^d - 1\right) \cdot \left(X^{\frac{p-1}{d}\cdot(d-1)} + X^{\frac{p-1}{d}\cdot(d-2)} + \cdots + X^{\frac{p-1}{d}} + 1\right).$$

Ainsi, pour tout $x \neq 0$,

$$p(x) = x^d - 1 = 0 \vee q(x) = x^{\frac{p-1}{d}\cdot(d-1)} + \cdots + 1 = 0.$$

Preuve du lemme (2) - partie 2/2.

On a donc :

$$\begin{aligned} p-1 &\leq \#\{x \text{ t.q. } p(x)=0\} + \#\{x \text{ t.q. } q(x)=0\} \\ &\leq d + \frac{p-1}{d} \cdot (d-1) \\ &= p-1. \end{aligned}$$

Finalement, les inégalités sont des égalités : $\#\{x \text{ t.q. } p(x)=0\} = d$.
On a donc exactement d solutions distinctes à l'équation
$X^d - 1 = 0$. □

Théorème (Existence d'une racine primitive)

Soit p, un nombre premier. Alors il existe un élément g de $\mathbb{Z}/p\mathbb{Z}$ tel que l'ordre de g est égal à $p-1$ c'est-à-dire :

$$g^{p-1} - 1 \equiv 0 \wedge g^d - 1 \not\equiv 0 \quad \forall d \mid p-1.$$

Preuve du théorème - partie 1/2

On démontre un résultat plus général : si $d \mid p-1$, il existe $\varphi(d)$ éléments de $\mathbb{Z}/p\mathbb{Z}$ dont l'ordre est égal à d. On résonne par « récurrence forte » sur les diviseurs de $p-1$.
<u>Initiation : $d = 1$</u>. On a bien $\varphi(1) = 1$ élément d'ordre 1 :

$$x^1 - 1 \equiv 0 \iff x \equiv 1.$$

<u>Récurrence :</u> soit d, un diviseur de $p-1$. Supposons que le résultat soit vrai pour tout $d' < d$, diviseur de $p-1$.

Preuve du théorème - partie 2/2.

Par le second lemme, il existe d solutions à l'équation $X^d - 1 \equiv 0$. De plus, comme vu dans la preuve du théorème de Euler/Fermat, si $x^d - 1 \equiv 0$, alors l'ordre de x modulo p divise d. Ainsi :

$$d = \sum_{d' | d} \text{(nombre de solution d'ordre d')} .$$

Par hypothèse de récurrence, le nombre de solutions d'ordre d' est égal à $\varphi(d')$ pour $d' < d$. Dès lors,

$$\text{nombre de solutions d'ordre d} = d - \sum_{d' | d \wedge d' < d} \varphi(d').$$

Enfin, puisque $\sum_{d' | d} \varphi(d') = d$, le nombre de solutions d'ordre d est bien $\varphi(d)$.
Finalement, en prenant $d = p - 1$, on a bien $\varphi(p-1) \geq 1$ racines primitives dans $\mathbb{Z}/p\mathbb{Z}$. $\square$

Nombres de Mersenne

Définition

Un nombre de Mersenne (nommé selon Marin Mersenne, 16-17e siècle) est nombre sous la forme $M_n = 2^n - 1$.

Lemme

Soit $p \in \mathbb{N}^*$*. Si* p *est divisible par* $m \in \mathbb{N}$*, alors le nombre de Mersenne* M_m *divise* M_p*.*

Remarque

Ce lemme veut dire qu'il n'est pas nécessaire de tester la primalité de M_n pour n non premier car si n n'est pas premier, alors M_n ne l'est pas non plus. La réciproque n'est pas vraie. Exemple : $p = 11$ est premier, or $M_p = 2^{11} - 1 = 2047 = 23 \times 89$.

Preuve.

La preuve est uniquement calculatoire. Supposons qu'il existe $m, t \in \mathbb{N} \setminus \{1, p\}$ tels que $p = mt$. On a alors :

$$M_n = 2^n - 1 = 2^{mt} - 1 = (2^m)^t - 1 = \frac{(2^m)^t - 1}{2^m - 1}(2^m - 1)$$
$$= \sum_{i=0}^{t-1}(2^m - 1)(2^m)^k = (2^m - 1)\sum_{i=0}^{t-1} 2^{mk} = M_m \sum_{i=0}^{t-1} 2^{mk}$$

Où, par la formule de la somme d'une suite géométrique, on a :

$$\sum_{i=0}^{n} u_n = u_0 \frac{q^{n+1} - 1}{q - 1},$$

avec $u_k = u_0 q^k$. □

Test Lucas-Lehmer

Le test de Lucas-Lehmer permet de déterminer si un nombre de Mersenne est premier ou non. Il est basé sur la suite naturelle :

$$\begin{cases} L_0 & = 4 \\ L_n & = (L_{n-1})^2 - 2 \text{ si } n \geq 1 \end{cases}$$

dont les premiers termes sont les suivants :

$$4, 14, 194, 37\,634, 1\,416\,317\,954, \ldots$$

Théorème (Test de Lucas-Lehmer)

Soit $p \in \mathbb{N}^*$. M_p *est premier si et seulement si* M_p *divise* L_{p-2}.

Remarque

Le théorème est une double implication. Il faut donc montrer les deux pour démontrer le théorème. Nous ne montrerons ici pas le fait que si M_p est premier, alors M_p divise L_{p-2}.

Lemme (Lemme préliminaire)

Soit G *un groupe. Soit* $a \in G$ *un élément. Alors* $\mathrm{ord}(a) \leq |G|$.

Preuve - partie 1/3

Montrons que $L_{p-2} = kM_p \Rightarrow M_p$ premier. Une manière d'exprimer la divisibilité de L_{p-2} par M_p est de dire que $L_{p-2} \equiv 0 (\mod M_p)$. Premièrement, on remarque que l'on peut exprimer la suite (L_n) définie récursivement comme une suite directe. Posons $\omega = 2 + \sqrt{3}, \bar{\omega} = 2 - \sqrt{3}$. On trouve dès lors $L_n = \omega^{2^n} + \bar{\omega}^{2^n}$.
On suppose qu'il existe $k \in \mathbb{N}$ tel que :

$$L_{p-2} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = kM_p.$$

En multipliant par $\omega^{2^{p-2}}$ des deux côtés et en réarrangeant les termes, on obtient :

$$\left(\omega^{2^{p-2}}\right)^2 = \omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - \bar{\omega}^{2^{p-2}}\omega^{2^{p-2}} = 1.$$

Preuve - partie 2/3

Supposons par l'absurde que M_p est composite (n'est pas premier). On prend donc $2 < q < M_p$ le plus petit diviseur premier de M_p. On prend alors $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ l'ensemble des entiers modulo q, et on pose :

$$X := \{a + b\sqrt{3} \text{ t.q. } a, b \in \mathbb{Z}_q\},$$

où
$\forall x = (a + b\sqrt{3}), y = (c + d\sqrt{3}) \in X : x \cdot y = (ac + 3bd) + (ac + bd)\sqrt{3}$.
On pose $X^* = \{x \in X \text{ t.q. } \exists x^{-1} \in X\}$ le groupe des éléments de X admettant un inverse (preuve que X^* est un groupe est omise). On sait que $0 \notin X^*$, donc $|X^*| \leq |X| - 1 = q^2 - 1$.
De plus, on sait $q > 2$, donc $\omega, \bar{\omega} \in X^*$. Également, $M_p \equiv 0(\mod q)$, donc, dans X, on a :

$$kM_p\omega^{2^{p-2}} = 0.$$

Preuve - partie 3/3

On a vu que $\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1 = 0 - 1 = -1$ dans X. En mettant au carré l'équation, on obtient :

$$\left(\omega^{2^{p-1}}\right)^2 = \omega^{2^p} = 1.$$

Dès lors, on sait que $\omega \in X^*$ et est d'un ordre qui divise 2^p. Or, $\mathrm{ord}(\omega)$ ne divise pas 2^{p-1}. Donc $\mathrm{ord}(\omega) = 2^p$. Par le lemme préliminaire, on a :

$$2^p \leq |X^*| \leq q^2 - 1.$$

Et comme q est un diviseur de M_p, on a $q^2 \leq M_p = 2^-1$. On a alors $2^p \leq 2^p - 2$, ce qui est une contradiction. Notre hypothèse disant que M_p est composite est donc fausse. M_p est bien premier.