

# Aperçu de l'étude des nombres premiers

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

Université Libre de Bruxelles

4 mai 2016

# Plan de la présentation

- 1 Théorèmes fondamentaux d'Euclide, de Wilson, d'Euler
  - Existence d'une infinité de nombres premiers
  - Nombres de Wilson
  - Fonction indicatrice d'Euler
- 2 Théorèmes de Fermat et Euler
- 3 Nombres de Carmichael
- 4 Les racines primitives
  - Lemmes préliminaires et démonstrations
- 5 Mersenne et Lucas-Lehmer
  - Introduction aux nombres de Mersenne
  - Test de Lucas-Lehmer

## Section 1

# Théorèmes fondamentaux d'Euclide, de Wilson, d'Euler

## Définition

Soient  $a, b \in \mathbb{N}$ . On dit que  $a$  est divisible par  $b$  si  $\exists c \in \mathbb{N}$  tel que  $a = b \cdot c$ .

## Propriétés

- 1 si  $n > 0$ , il n'admet pas de diviseur supérieur à lui-même ;
- 2 tout nombre naturel admet au moins un diviseur ;
- 3 2 est le premier nombre premier.

# Infinité de nombres premiers

## Théorème (Théorème d'Euclide)

*Il existe une infinité de nombres premiers distincts.*

### Preuve.

Soit  $\mathbb{P} \subset \mathbb{N}^*$  l'ensemble des nombres premiers. Supposons par l'absurde que  $\mathbb{P}$  est fini et de cardinalité  $n$ . On note  $N = \prod_{p \in \mathbb{P}} p$  le produit de tous les nombres de  $\mathbb{P}$ . Il y a dès lors deux cas distincts concernant  $N + 1$  : soit  $N + 1$  est premier, soit  $N + 1$  est composé. Dans le premier cas, il y a contradiction car  $N + 1$  est un nombre premier n'appartenant pas à  $\mathbb{P}$ .

Dans le second cas, on prend  $1 < Q < N + 1$ , un diviseur premier de  $N + 1$ . Or,  $Q \notin \mathbb{P}$  car  $\forall p \in \mathbb{P} : p|N$  et donc  $p \nmid N + 1$ . Il y a contradiction car  $Q$  est premier mais n'est pas dans  $\mathbb{P}$ .

Ces deux contradictions impliquent que la supposition est fausse, et donc  $\mathbb{P}$  est infini. □

# Bézout et restes chinois

## Théorème (Théorème de Bachet-Bézout)

*Soient  $a, b, x, y \in \mathbb{Z}$ . L'équation suivante (en  $x, y$ ) :*

$$ax + by = 1$$

*admet des solutions si et seulement si  $a$  et  $b$  sont premiers entre eux.*

## Théorème (Théorème des restes chinois)

*Soient  $m_1, \dots, m_k \in \mathbb{N}$  premiers deux à deux et  $a_1, \dots, a_k \in \mathbb{N}$ . Le système :*

$$x \equiv a_i \pmod{m_i} \qquad \text{pour } i = 1, 2, \dots, k$$

*possède une solution unique modulo  $n := \prod_{i=1}^k m_i$ .*

# Preuve du théorème des restes chinois

Preuve par récurrence. Commençons par le pas initial avec  $k = 2$ . Par Bézout, on sait qu'il existe  $u_1, u_2 \in \mathbb{Z}$  t.q.  $m_1 u_1 + m_2 u_2 = 1$ . Donc il existe

$$k_1, k_2 \in \mathbb{Z} \text{ t.q. } : \begin{cases} (m_2 u_2)x &= (m_2 u_2)m_1 k_1 + (m_2 u_2)a_1 \\ (m_1 u_1)x &= (m_1 u_1)m_2 k_2 + (m_1 u_1)a_2 \end{cases}.$$

Ce qui est équivalent à :

$$\begin{aligned} (m_1 u_1 + m_2 u_2)x &= m_1 m_2 (u_1 k_2 + u_2 k_1) + m_1 u_1 a_2 + m_2 u_2 a_1 \\ 1 \cdot x &\equiv m_1 u_1 a_2 + m_2 u_2 a_1 \pmod{m_1 m_2} \end{aligned}$$

Pour le pas de récurrence, prenons  $k \geq 2$ . Notons  $M := \prod_{i=1}^{k-1} m_i$ . On sait que  $M$  et  $m_n$  sont premiers entre eux. On peut donc dire  $x \equiv a_n \pmod{m_n}$  et  $x \equiv a_M \pmod{M}$  si et seulement si  $x$  a une solution unique modulo  $n := m_n M$ .

## Théorème (Théorème de Wilson)

*Soit  $p > 1$  un nombre entier.  $p$  est premier si et seulement si*  
 $(p - 1)! + 1 \equiv 0 \pmod{p}$

## Propriétés préparatoires

- ❶ si  $p$  est un nombre premier et  $a \in \{1, \dots, p - 1\}$ , alors il existe un unique  $b$  (modulo  $p$ ) tel que  $a \cdot b \equiv 1 \pmod{p}$  ;
- ❷ si  $p$  est premier, alors  $a \times a \equiv 1 \pmod{p}$  si et seulement si  $a \equiv 1 \pmod{p}$  ou  $a \equiv p - 1 \pmod{p}$

## Preuve du sens direct du théorème

Par les propriétés ci-dessus, on a immédiatement :

$$(p - 1)! \equiv (p - 1) \pmod{p} \equiv -1 \pmod{p}.$$



## Preuve du sens indirect du théorème.

Faisons la preuve par contraposée : montrons que si  $p$  n'est pas premier, alors on a  $(p-1)! \not\equiv -1 \pmod{p}$ .

Un cas particulier : prenons  $p = 4$ . On trouve alors :

$$(p-1)! = 3! = 6 \equiv 2 \pmod{4}.$$

pas de récurrence : soit  $p > 4$ , un nombre composé. Soient  $a, b \in \mathbb{N}^*$  t.q.  $p = ab$ . Deux cas sont à distinguer :

- si  $a \neq b$ , en calculant  $(p-1)!$ , on peut regrouper  $a$  et  $b$  (en les mettant en évidence). On a alors :  
$$(p-1)! = a \cdot b \cdot 1 \cdots (p-1) \equiv 0 \pmod{p} ;$$
- si  $a = b$ , alors  $p$  est un carré parfait tel que  $p = a^2 > 2a$ . Par conséquent,  $a$  et  $2a$  apparaissent tous deux dans  $(p-1)!$  et on peut mettre en évidence :  
$$(p-1)! = a \cdot 2a \cdot 1 \cdots (p-1) = 2(a \cdot b)1 \cdots (p-1) \equiv 0 \pmod{p}.$$



## Définition

Soit

$$\varphi : \mathbb{N} \rightarrow \mathbb{N}^* : n \mapsto \varphi(n) = \left| \{m \in \mathbb{N} \text{ t.q. } (m < n) \wedge (\gcd(m, n) = 1)\} \right|.$$

On appelle  $\varphi$  la fonction indicatrice d'Euler.

## Section 2

# Théorèmes de Fermat et Euler

## 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 :*

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

# 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 :  
 $\langle a \rangle := \{e = a^0, a^1, \dots, a^{m-1}\}.$

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

## 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)

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

## Preuve du petit théorème de Fermat - partie 1/2

On considère le groupe  $(\mathbb{Z}/p\mathbb{Z}^*, \cdot, 1)$ . En effet,

$\mathbb{Z}/p\mathbb{Z}^* = \{[1], [2], \dots, [p-1]\}$  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  $m := \text{ord}([a])$ . Alors on sait :

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

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

## Rappel (Petit théorème de Fermat)

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

## 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 :

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

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

$$a^{p-1} \equiv 1 \pmod{p}.$$



# 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 :*

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

## *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  $\pmod{n}$  et dont le cardinal vaut  $\phi(n)$ . □



## Section 3

# Nombres de Carmichael

### Définition

Un nombre de Carmichael est un nombre qui ne respecte pas la réciproque du petit théorème de Fermat

### Réciproque du petit théorème de Fermat

$(\forall a \text{ t.q. } \gcd(a, p) = 1 : a^{p-1} - 1 \equiv 0 \pmod{p}) \Rightarrow p \text{ est premier}$

## Exemple de nombre de Carmichael - partie 1/2

Exemple d'un nombre de Carmichael : prenons  $p = 561$ . On sait que  $p = 3 \times 11 \times 17$  est un nombre composé. On remarque que  $3 - 1$ ,  $11 - 1$ , et  $17 - 1$  divisent  $p - 1$  :

$$\frac{560}{3-1} = \frac{560}{2} = 280 ; \quad \frac{560}{11-1} = \frac{560}{10} = 56 ; \quad \frac{560}{17-1} = \frac{560}{16} = 35.$$

Et donc :

$$561 \equiv 1 \begin{cases} \pmod{3-1} \\ \pmod{11-1} \\ \pmod{17-1}. \end{cases}$$

## Exemple de nombre de Carmichael - partie 2/2

Prenons maintenant  $a$  non-divisible par 3, 11, et 17. Dès lors, par le petit théorème de Fermat, on a :

$$\textcircled{1} \quad a^{561-1} = (a^{280})^{3-1} = (a^{(1)})^{3-1} \equiv 1 \pmod{3} ;$$

$$\textcircled{2} \quad a^{561-1} = (a^{56})^{11-1} = (a^{(2)})^{11-1} \equiv 1 \pmod{11} ;$$

$$\textcircled{3} \quad a^{561-1} = (a^{35})^{17-1} = (a^{(3)})^{17-1} \equiv 1 \pmod{17}.$$

Et par les règles de calculs de congruence, on obtient finalement :

$$a^{561-1} \equiv 1 \pmod{(3 \times 11 \times 17)} = 1 \pmod{561}.$$

## Section 4

# Les racines primitives

# 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 :

$$\begin{aligned} n &= \# \{1, 2, \dots, n\} = \# \bigcup_{d|n} \{1 \leq x \leq n \mid \gcd(n, x) = d\} \\ &= \sum_{d|n} \# \{1 \leq x \leq n \mid \gcd(n, x) = d\} \\ &= \sum_{d|n} \# \left\{ 1 \leq \frac{x}{d} \leq \frac{n}{d} \mid \gcd\left(\frac{n}{d}, \frac{x}{d}\right) = 1 \right\} \\ &= \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d'|n} \varphi(d') \end{aligned}$$

## 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  $d \cdot d' = n$ .



# 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,

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

Ainsi, pour tout  $x \neq 0$ ,

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

## 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 raisonne par « récurrence forte » sur les diviseurs de  $p - 1$ .

Initiation :  $d = 1$ . On a bien  $\varphi(1) = 1$  élément d'ordre 1 :

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

Récurrence : 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 :

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

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

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

Enfin, puisque  $\sum_{d' \mid d} \varphi(d') = d$ , 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  $\mathbb{Z}/p\mathbb{Z}$ . □

## Section 5

# Mersenne et Lucas-Lehmer

# 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  $m, t \in \mathbb{N} \setminus \{1, n\}$  tels que  $n = mt$ . On a alors :

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

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

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

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, ...



## 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  $\text{ord}(a) \leq |G|$ .*

# 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  $L_{p-2} \equiv 0 \pmod{M_p}$ .

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 :

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

# Preuve - partie 2/3

Supposons par l'absurde que  $M_p$  est composé (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  $\forall x = (a + b\sqrt{3}), y = (c + d\sqrt{3}) \in X :$

$$x \cdot y = ((ac + 3bd) \pmod q) + ((ac + bd) \pmod q) \sqrt{3}.$$

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,  $M_p \equiv 0 \pmod q$ , 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,  $\text{ord}(\omega)$  ne divise pas  $2^{p-1}$ . Donc  $\text{ord}(\omega) = 2^p$ . 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  $q^2 \leq M_p = 2^p - 1$ . On a alors  $2^p \leq 2^p - 2$ , ce qui est une contradiction. Notre hypothèse disant que  $M_p$  est composé est donc fausse.  $M_p$  est bien premier.



# Remerciements et questions

**Merci pour votre écoute.**

**À vos questions !**