

---

CRY 2024

Arithmétique

Alexandre Duc

1. Nombres Entiers

2. Nombres Premiers

3. Plus Grand Diviseur Commun

4. Exponentiation Rapide

# Entiers Naturels et Relatifs

## Définition (Ensemble des entiers naturels)

L'ensemble  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$  s'appelle l'**ensemble des entiers naturels**.


## Définition (Ensemble des entiers relatifs)

L'ensemble  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  s'appelle l'**ensemble des entiers relatifs**.

# Division Euclidienne

## Définition (Division euclidienne)

Soit  $a, b \in \mathbb{Z}$ , avec  $b \neq 0$ . La **division euclidienne** de  $a$  par  $b$  consiste à écrire  $a = qb + r$ , où  $q \in \mathbb{Z}$  s'appelle le **quotient** et  $0 \leq r < |b|$  s'appelle le **reste**.

 Le reste  $r$  s'écrit également

$$r = a \bmod b,$$

que l'on prononce « $a$  modulo  $b$ ».

 Une autre notation possible est

$$a \equiv r \pmod{b},$$

que l'on prononce « $a$  est congru à  $r$  modulo  $b$ ».

# Division Euclidienne – Exemple

$$472987 = 94597 \times 5 + 2$$

4 7 2 9 8 7	5
— 4 5	9 4 5 9 7
<u>2 2</u>	
— 2 0	
<u>2 9</u>	
— 2 5	
<u>4 8</u>	
— 4 5	
<u>3 7</u>	
— 3 5	
<u>2</u>	

# Entiers Naturels et Relatifs – Exemples

- $10 = 3 \cdot 3 + 1$

- $-13 = -4 \cdot 4 + 3$

- $472987 = 94597 \cdot 5 + 2$

- $100 = 33 \cdot 3 + 1$

- $65537 = 9362 \cdot 7 + 3$

- $10 \bmod 3 = 1$

- $-13 \bmod 4 = 3$

- $472987 \bmod 5 = 2$

- $100 \bmod 3 = 1$

- $65537 \bmod 7 = 3$

- $10 \equiv 1 \equiv 4 \pmod{3}$

- $-13 \equiv 3 \equiv 11 \pmod{4}$

- $472987 \equiv 2 \pmod{5}$

- $100 \equiv 1 \pmod{3}$

- $65537 \equiv 3 \pmod{7}$



1. Nombres Entiers
2. Nombres Premiers
3. Plus Grand Diviseur Commun
4. Exponentiation Rapide

# Nombres Premiers – Définition

## Définition (Nombre Premier)

Un **nombre premier**  $p \in \mathbb{N}$  est un entier naturel qui admet exactement deux diviseurs distincts, entiers et positifs, soit 1 et  $p$ .

Un nombre qui n'est pas premier est dit **composé**.

-  0 n'est pas un nombre premier, car il possède une infinité de diviseurs.
-  1 n'est pas un nombre premier, car il ne possède qu'un seul diviseur entier, qui est lui-même.



# Nombres Premiers – Exemples

- Exemples de nombre premiers :

- 2, 3, 5, 7, 13, 17

- 257, 65537

- 3490529510847650949147849619903898133417764638493387843990820577

- Exemples de nombres composés :

- $16 = 2^4$ ,  $21 = 3 \cdot 7$

- $111111111 = 3^2 \cdot 37 \cdot 333667$

- $4294967295 = 2^{32} - 1 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$

$$\begin{aligned}
 &12301866845301177551304949583849627207728535695953347921973224521517264005 \\
 &07263657518745202199786469389956474942774063845925192557326303453731548268 \\
 &50791702612214291346167042921431160222124047927473779408066535141959745985 \\
 &\quad 6902143413 = \\
 &33478071698956898786044169848212690817704794983713768568912431388982883793 \\
 &\quad 878002287614711652531743087737814467999489 \times \\
 &36746043666799590428244633799627952632279158164343087642676032283815739666 \\
 &\quad 511279233373417143396810270092798736308917
 \end{aligned}$$

# Nombres Premiers – Factorisation Unique

## Théorème (Factorisation Unique)

Tout nombre naturel  $n \in \mathbb{N}$ , avec  $n \geq 2$ , peut être écrit comme le produit unique de nombres premiers, à l'ordre des facteurs près.

- Exemples :

- $12 = 2^2 \cdot 3$

- $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

- $3216893761230000 = 2^4 \cdot 3 \cdot 5^4 \cdot 107229792041$

# Nombres Premiers – Infinité

Théorème (Euclide, 325 - 265 av. J.-C.)

Il existe une infinité de nombres premiers.

## Démonstration.

Admettons qu'il n'existe que  $k$  nombre premiers  $p_1, p_2, \dots, p_k$ . Le nombre  $p_1 p_2 \cdots p_k + 1$  n'est cependant pas divisible par  $p_i$ , pour  $1 \leq i \leq k$ , ce qui contredit l'hypothèse de départ.

# Nombres Premiers – Répartition

## Définition (Nombre de nombres premiers)

Le nombre de nombres premiers  $p \leq n$  est noté  $\pi(n)$ .

## Théorème (Répartition des nombres premiers)

$$\lim_{n \rightarrow +\infty} \frac{\pi(n)}{n / \ln n} = 1$$

$n$	$\pi(n)$	$n / \ln n$
$10^2$	25	$\approx 22$
$10^4$	1229	$\approx 1086$
$10^6$	78498	$\approx 72382$

# Nombre Premiers

## Question

Quelle est approximativement la probabilité pour qu'un nombre de maximum 100 chiffres soit premier ?

Les solutions des questions se trouvent à la fin des slides.

# Nombres Premiers – Crible d'Eratosthène

- Le **crible d'Eratosthène** est un algorithme qui permet de trouver tous les nombres premiers inférieurs à  $n$ .
- On écrit tous les entiers entre 2 et  $n$ .
- On répète le processus suivant :
  - i On barre tous les multiples du plus petit entier non barré.
  - ii On s'arrête lorsque le plus petit entier restant  $m > \sqrt{n}$ .

# Crible d'Eratosthène

## Question

Quel est le problème avec le crible d'Eratosthène ?

1. Nombres Entiers
2. Nombres Premiers
3. Plus Grand Diviseur Commun
4. Exponentiation Rapide



# PGCD – Définition

## Définition (Plus Grand Commun Diviseur)

On définit  $\text{pgcd}(a, b)$  pour  $a, b \in \mathbb{N}$  comme étant le **plus grand diviseur commun** non-nul de  $a$  et de  $b$ .

- Exemples :
  - $\text{pgcd}(3, 9) = 3$
  - $\text{pgcd}(15, 35) = 5$
  - $\text{pgcd}(333, 111) = 111$
  - $\text{pgcd}(65537, 111) = 1$
  - $\text{pgcd}(2048, 4096) = 2048$

## PGCD – Algorithme d'Euclide

- Pour calculer  $\text{pgcd}(a, b)$ , pour  $a > b$ , on calcule  $\text{pgcd}(b, a \bmod b)$  en répétant le calcul jusqu'à ce que le reste soit égal à zéro. Le plus grand diviseur commun est le reste précédent.
- En effet, si  $d$  divise à la fois  $a$  et  $b$ , il divisera également  $r = a - qb$  : avec  $a = \alpha d$  et  $b = \beta d$ , on a  $r = \alpha d - q\beta d = d(\alpha - q\beta)$ .
- Exemple :

$$\begin{aligned}\text{pgcd}(132, 18) &= \text{pgcd}(18, 6) \\ &= \text{pgcd}(6, 0) \\ &= 6\end{aligned}$$

# PGCD – Algorithme d'Euclide

- Exemple :

$$\begin{aligned}\text{pgcd}(65537, 7) &= \text{pgcd}(7, 3) \\ &= \text{pgcd}(3, 1) \\ &= \text{pgcd}(1, 0) \\ &= 1\end{aligned}$$

# Nombres Premiers Entre Eux

## Définition (Nombres Premiers Entre Eux)

On dit que  $a, b \in \mathbb{N}$  sont **premiers entre eux** si  $\text{pgcd}(a, b) = 1$ .

- Exemples :

- 5 et 7 sont premiers entre eux.
- 15 et 16 sont premiers entre eux.
- 18 et 30 ne sont pas premiers entre eux.

👉 Deux nombres sont premiers entre eux si leurs décompositions en facteurs premiers ne contiennent aucun facteur commun.

👉 Deux nombres premiers différents sont toujours premiers entre eux.

# Identité de Bézout

## Théorème (Bachet de Méziriac, 1581-1638)

Soit  $a, b \in \mathbb{Z}$  non tous nuls, ainsi que  $d = \text{pgcd}(a, b)$ . Il existe deux entiers relatifs  $x, y \in \mathbb{Z}$  tels que

$$ax + by = d \tag{1}$$

- 👉 L'équation (1) est appelée **l'identité de Bézout**.
- 👉 Les nombres  $x$  et  $y$  peuvent être calculés au moyen de **l'algorithme d'Euclide étendu**.

## Algorithme d'Euclide Étendu

Calculons  $\text{pgcd}(120, 23)$  en partant des équations suivantes :

$$120 = 120 \cdot 1 + 23 \cdot 0 \quad (2)$$

$$23 = 120 \cdot 0 + 23 \cdot 1 \quad (3)$$

On sait que  $120 = 5 \cdot 23 + 5$ . En soustrayant 5 fois l'équation (3) de l'équation (2), on obtient

$$5 = 120 \cdot 1 + 23 \cdot (-5) \quad (4)$$

De façon identique, on sait que  $23 = 5 \cdot 4 + 3$ . En soustrayant 4 fois l'équation (4) de l'équation (3), on obtient

$$3 = 120 \cdot (-4) + 23 \cdot 21 \quad (5)$$

## Algorithme d'Euclide Étendu

Lors de l'étape suivante, on sait que  $5 = 3 \cdot 1 + 2$ . En soustrayant 1 fois l'équation (5) de l'équation (4), on obtient

$$2 = 120 \cdot 5 + 23 \cdot (-26) \quad (6)$$

Finalement, on a  $3 = 2 \cdot 1 + 1$ . En soustrayant 1 fois l'équation (6) de l'équation (5), on obtient

$$1 = 120 \cdot (-9) + 23 \cdot 47 \quad (7)$$

Si on pose  $a = 120$  et  $b = 23$ , on a  $d = \text{pgcd}(a, b) = 1$ ,  $x = -9$  et  $y = 47$ .

# Algorithm d'Euclide Étendu – Méthode rapide

$x$	$y$	$q$	Calcul
$(120, 1, 0)$	$(23, 0, 1)$	5	$120 = 23 \cdot 5 + 5$
$(23, 0, 1)$	$(5, 1, -5)$	4	$23 = 5 \cdot 4 + 3$
$(5, 1, -5)$	$(3, -4, 21)$	1	$5 = 3 \cdot 1 + 2$
$(3, -4, 21)$	$(2, 5, -26)$	1	$3 = 2 \cdot 1 + 1$
$(2, 5, -26)$	$(1, -9, 47)$	2	$2 = 1 \cdot 2 + 0$
$(1, -9, 47)$	$(0, 23, -120)$	0	



# Nombres Premiers – Divisibilité d'un Produit

## Théorème (Lemme d'Euclide)

Si un nombre premier  $p$  divise le produit  $rs$ , alors  $p$  est un diviseur de  $r$  ou un diviseur de  $s$ .

- 👉 Le «ou» est non-exclusif. Par exemple 2 divise  $32 = 4 \cdot 8$ , et il divise à la fois 4 **et** 8.
- 👉 Ce résultat est faux si  $p$  n'est pas premier : 9 divise  $180 = 12 \cdot 15$ , mais il ne divise ni 12, ni 15.

# Nombres Premiers – Preuve du Lemme d'Euclide

On suppose  $p \nmid r$  ( $p$  ne divise pas  $r$ ).<sup>1</sup> On a donc  $r$  et  $p$  premiers entre eux. Comme  $p \mid rs$  ( $p$  divise  $rs$ ), on peut écrire  $rs = kp$ , pour un  $k$  entier. On veut montrer que  $p \mid s$ . Par Bézout, il existe des entiers  $\alpha, \beta$  tels que  $\alpha r + \beta p = 1$ . En multipliant tout par  $s$ , on obtient  $\alpha rs + \beta ps = s$ . Ceci est équivalent à  $(\alpha k + \beta s)p = s$ .  $s$  est donc divisible par  $p$ .

---

1. Si  $p \mid r$  on a fini.

1. Nombres Entiers
2. Nombres Premiers
3. Plus Grand Diviseur Commun
4. Exponentiation Rapide

### Question

Comment calculer  $m^e \bmod n$  pour de très grands nombres  $m, e, n$  ?

## Approche «Square-and-Multiply»

- En cryptographie, il est crucial de pouvoir calculer des opérations de type  $a^b \bmod c$  de manière efficace, même si  $a$ ,  $b$  et  $c$  sont de grands nombres.
- Les approches d'exponentiation rapide permettent de réduire la complexité de cette opération à un nombre d'opérations modulaires dépendant **logarithmiquement** de la valeur de l'exposant.
- On peut exprimer un exposant  $b$  de  $n$  bits en notation binaire :

$$b = \sum_{i=0}^{n-1} b_i 2^i.$$

- Donc, on a

$$a^b \equiv a^{\sum_{i=0}^{n-1} b_i 2^i} \equiv (a^{b_0})^{2^0} (a^{b_1})^{2^1} (a^{b_2})^{2^2} \dots (a^{b_{n-1}})^{2^{n-1}} \pmod{c}.$$

## Approche «Square-and-Multiply» (2)

- Pour  $b = 37 = 100101$ , on a donc

$$\begin{aligned}
 a^b &\equiv (a^1)^{2^0} (a^0)^{2^1} (a^1)^{2^2} (a^0)^{2^3} (a^0)^{2^4} (a^1)^{2^5} \pmod{c} \\
 &\equiv \left( \left( \left( \left( \left( (a^1)^2 a^0 \right)^2 a^0 \right)^2 a^1 \right)^2 a^0 \right)^2 a^1 \right) \pmod{c} \\
 &\equiv \left( \left( \left( \left( (1^2 \cdot a)^2 \right)^2 \cdot a \right)^2 \right)^2 \cdot a \right) \pmod{c}
 \end{aligned}$$

- Algorithme :**

- Écrire  $b = \sum_{i=0}^{n-1} b_i 2^i$ .
- $A \leftarrow 1$
- Pour  $i = n - 1 \dots 0$ , répéter :
  - $A \leftarrow A^2 \pmod{c}$ .
  - Si  $b_i = 1$ , alors  $A \leftarrow A \cdot a \pmod{c}$ .

# Solutions

# Nombre Premiers (solution)

## Question

Quelle est approximativement la probabilité pour qu'un nombre de maximum 100 chiffres soit premier ?

## Solution

Il y a environ  $10^{100} / \ln(10^{100})$  nombres premiers à 100 chiffres. Cela fait donc une probabilité de  $1 / \ln(10^{100}) = 1 / (100 \ln(10)) \approx 1/230$ .



# Crible d'Eratosthène

## Question

Quel est le problème avec le crible d'Eratosthène ?

## Solution

Pas du tout efficace. Il requière de stocker tous les nombres jusqu'à la racine de notre nombre. Pour des nombres utilisés en cryptographie de plusieurs milliers de bits, c'est inutilisable.