Edition 2023

Nombre et systèmes complexes

Les nombres, instruments de contrôle du monde sensible et portes ouvertes sur l'inconnaissable.

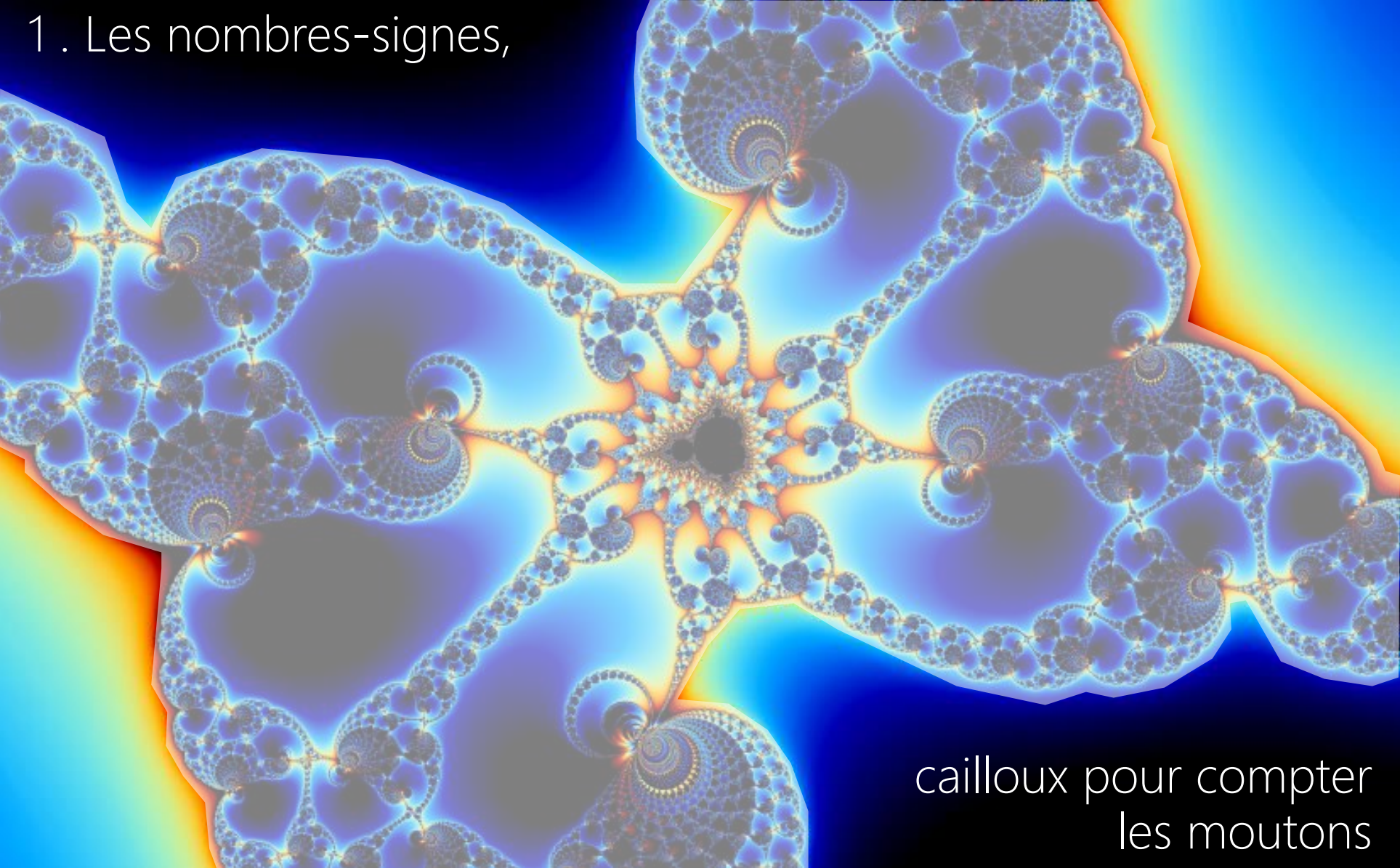
Philippe Lemoisson
Janvier 2023

Les nombres, instruments de contrôle du monde sensible

1. Les nombres-signes, cailloux pour compter les moutons
2. Choisir les bons cailloux pour les bons problèmes
3. Les nombres-concepts, cailloux pour les jeux de l'esprit
4. Les limites du contrôle, cailloux dans la chaussure
5. Une vue sur les cailloux qui donne le vertige

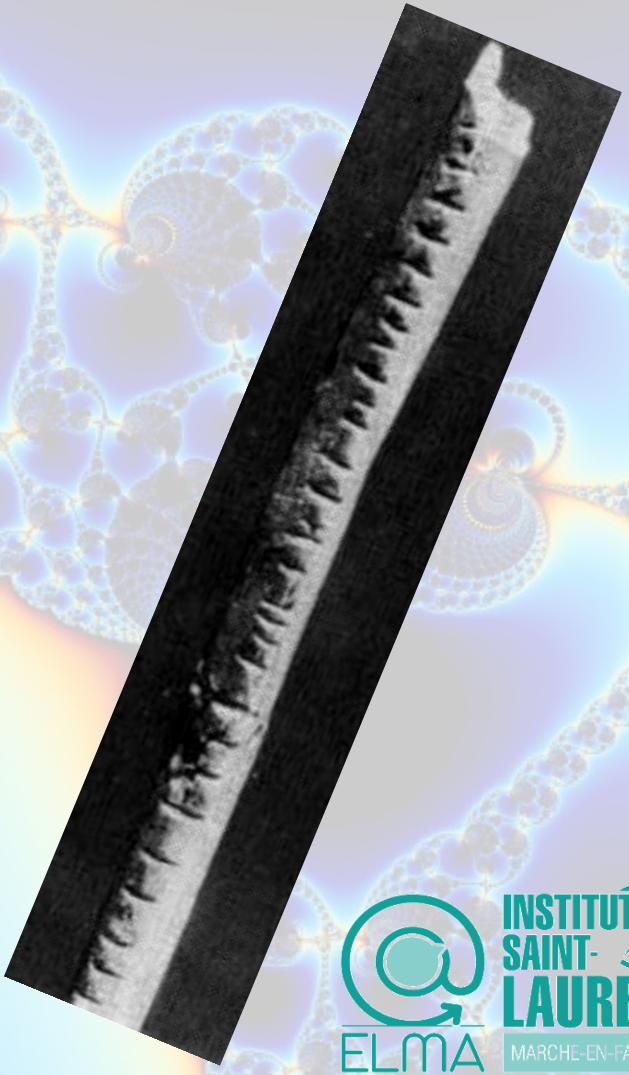
… et portes ouvertes sur l'inconnaissable

1 . Les nombres-signes,



cailloux pour compter
les moutons

- 35 000 Afrique du Sud



– 18 000 Rép. Dém. Congo

- 3 500 : les débuts du contrôle de gestion…

Période d'Uruk : … le développement des institutions étatiques s'accompagne de celui des instruments de gestion permettant l'encadrement des travailleurs et des autres ressources ; l'écriture apparaît vers -3400 -3300 …

Les calculi de Mésopotamie

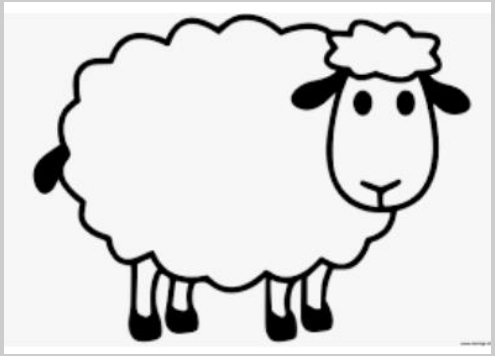
En 8000 av. J.-C., pour laisser une trace de leurs différentes transactions, les Sumériens attribuèrent différentes valeurs à de petits jetons en argile, appelés calculi, dont la valeur dépendait de leur taille et de leur forme : le petit cône  pour l'unité, la bille  pour la dizaine, le grand cône  pour la soixantaine, le grand cône perforé  pour dix soixantaines ...

Ces jetons d'argiles que l'on pourrait apparenter à nos actuelles pièces de monnaie, étaient glissés dans une sphère creuse en argile marquée par des sceaux qui en garantissaient l'origine et l'intégralité. Ainsi, par exemple, si la bulle de terre contenait le dénombrement d'un troupeau confié à un berger, lorsque celui-ci le ramenait, il leur suffisait de briser la bulle-enveloppe pour vérifier qu'aucune bête ne manquait.

Apparition de l'écriture

Petit à petit, l'homme commença à noter le contenu de la bulle d'argile sur le dessus de celle-ci, afin de réaliser des contrôles intermédiaires sans avoir à la casser : les petits calculi devinrent inutiles et les bulles-enveloppes se transformèrent en tablettes. Ainsi, c'est une invention majeure qui permit une nouvelle avancée dans l'histoire de la numération : l'apparition de l'écriture.

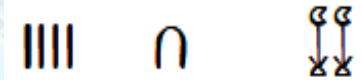
Ecriture des nombres-signes



Systèmes de numération ADDITIONNELS

Les systèmes de numération additionnels sont les tout premiers utilisés. Ils fonctionnent par addition des symboles représentant une unité, une dizaine, une centaine, etc.

Egyptiens : 2014 =4+10+2*1000

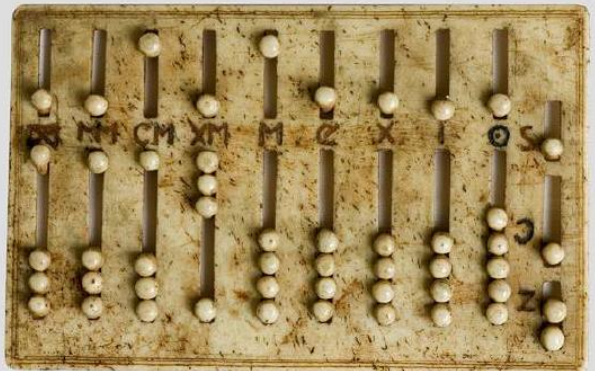


Grecs (attique) : 1974 =1*1000+1*500+4*100+1*50+2*10+4*1

Grecs (ionien) : 1974 =1*1000+1*900+1*70+1*4

Romains : 4724 =4*1000+500+2*100+2*10+(5-1)

MMMMDCCXXIV



L'addition est ardue,

la multiplication pas facile non plus …

(Poème romain)

ELMA INSTITUT SAINT-LAURENT MARCHE-EN-FAMENNE

Systèmes de numération HYBRIDES

Ces systèmes utilisent une **base**, c'est-à-dire une quantité qui va constituer des **paquets**,

puis des **paquets de paquets,**

puis des **paquets de paquets de paquets …**

(puissances successives de la base).

Une *convention de position relative* permet de repérer les puissances successives.

On *juxtapose/additionne des symboles* pour indiquer le nombre de paquets.

Systèmes de numération HYBRIDES

Vers – 3000, les **Babyloniens** utilisent une numération sexagésimale héritée des Sumériens et des Akkadiens. Ils sont les précurseurs du système positionnel.

Deux signes :

- le clou pour 1 : 
- le chevron pour 10 : 

59 s'écrit : 

Au delà de 59, la numération obéit à un principe de position à **base 60**.

63 s'écrit : 

Pour éviter les erreurs, un symbole est apparu pour représenter l'espace vide entre les nombres. Il s'agit du plus vieux zéro de l'histoire, mais ce n'était pas un nombre :

INSTITUT SAINT-LAURENT
ELMA
MARCHE-EN-FAMENNE

Systèmes de numération HYBRIDES

Entre 300 av. J.-C. et 1200 ap. J.-C., les mayas ont utilisé un système en **base 20**.

$4X20^3$

$+ 0x20^2$

$+14x20$

$+ 6 \qquad = 32\,286$

Systèmes de numération HYBRIDES

0	零	*ling*
1	一	*i*
2	二	Erh
3	三	San
4	四	Ssu
5	五	Wu
6	六	Liu
7	七	Chhi
8	八	Pa
9	九	Chiu
10	十	Shih
100	百	Pai
1000	千	Chhien
10000	万	wan

En Chine et au Japon, sur des écailles de tortues et des os, on a trouvé des traces datées 1500 av. J.-C d'un système de numération en **base 10** :

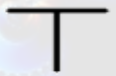
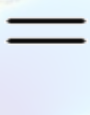
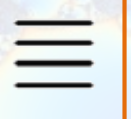
- neuf symboles représentant les chiffres de 1 à 9
- trois symboles représentant 10, 100, 1000 et 10 000
- places vides pour « zéro »

Le système est hybride car il met en jeu la multiplication des quantités et la juxtaposition des symboles.

≡ *1999 s'écrit :*

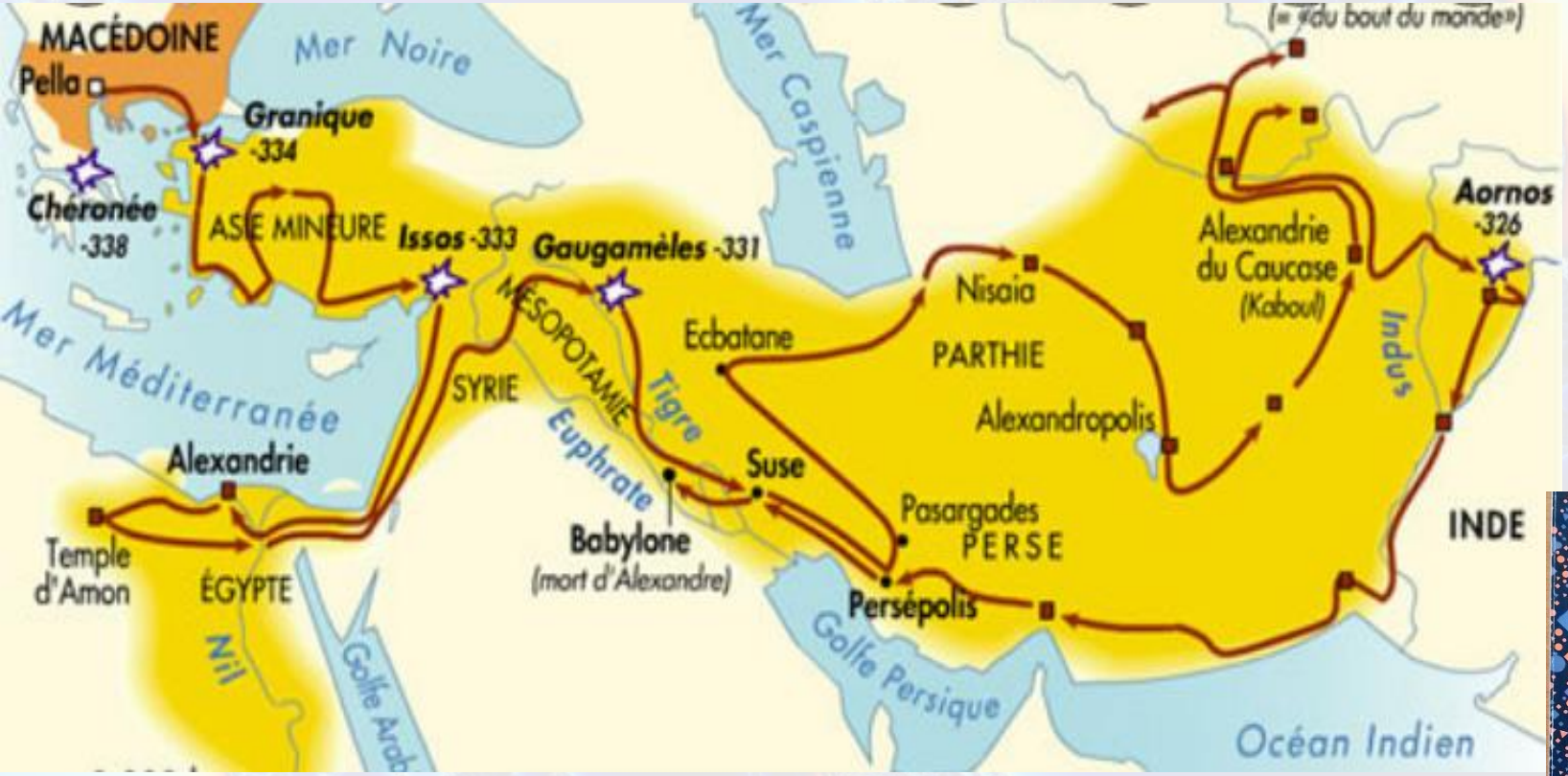
Systèmes de numération HYBRIDES

Au Ier siècle av. J.-C. et durant plusieurs siècles, dans la civilisation chinoise antique, les savants employaient une numération de positionnelle en **base 10**. Ce système de numération à bâtons utilise deux séries de chiffres selon le **rang** (pair ou impair). Le zéro est représenté par un espace vide sans risque d'erreur grâce à l'alternance des rangs.

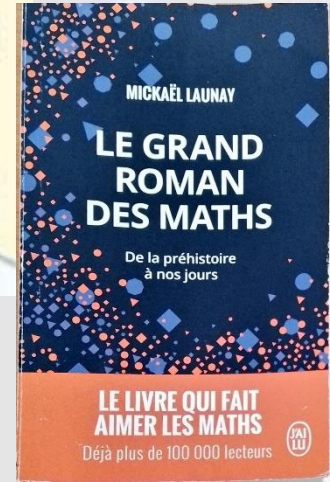
	1	2	3	4	5	6	7	8	9
Chiffres de rang pair									
Chiffres de rang impair									

ELMA INSTITUT SAINT-LAURENT MARCHE-EN-FAMENNE

- 330 : Alexandre le Grand atteint l'Indus



Une partie de la culture grecque s'intègre en Inde.



Numération positionnelle en base 10

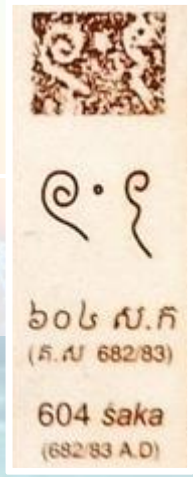
0 1 2 3 4 5 6 7 8 9

Jusqu'au Vème siècle, les mathématiciens indiens restent dans une tradition orale ; ensuite ils rayonnent dans le monde entier. Dans la philosophie hindoue, le vide et l'infini sont dans l'essence même du cosmos.

- Aryabhata calcule de très bonnes approximations de PI
- En 630, Bhaskara1 écrit le zéro positionnel sous forme de cercle et utilise scientifiquement le système décimal
- Au XII siècle, Bhaskara2 établira que 1/0 = ∞

Le zéro positionnel sous forme de cercle

682/3 A.D. - Sambor - Cambodge



Numération positionnelle en base 10

En 628, **Brahmagupta**, un astronome indien et l'un des plus grands mathématiciens de son époque, achève son premier ouvrage : le *Brahmasphutasiddhanta*.

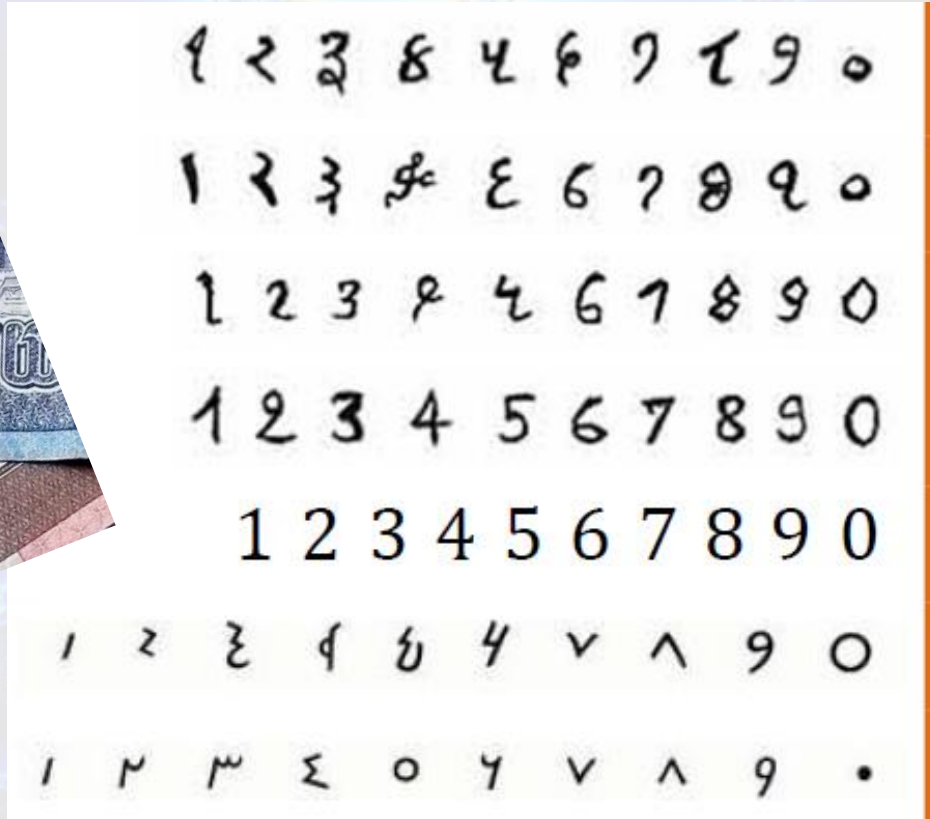
Il présente un **système positionnel en base 10**, définit le zéro, les nombres négatifs et décrit leurs propriétés mathématiques :

- le résultat de la soustraction d'un nombre par lui-même vaut zéro
- un nombre auquel on ajoute ou soustrait zéro reste inchangé

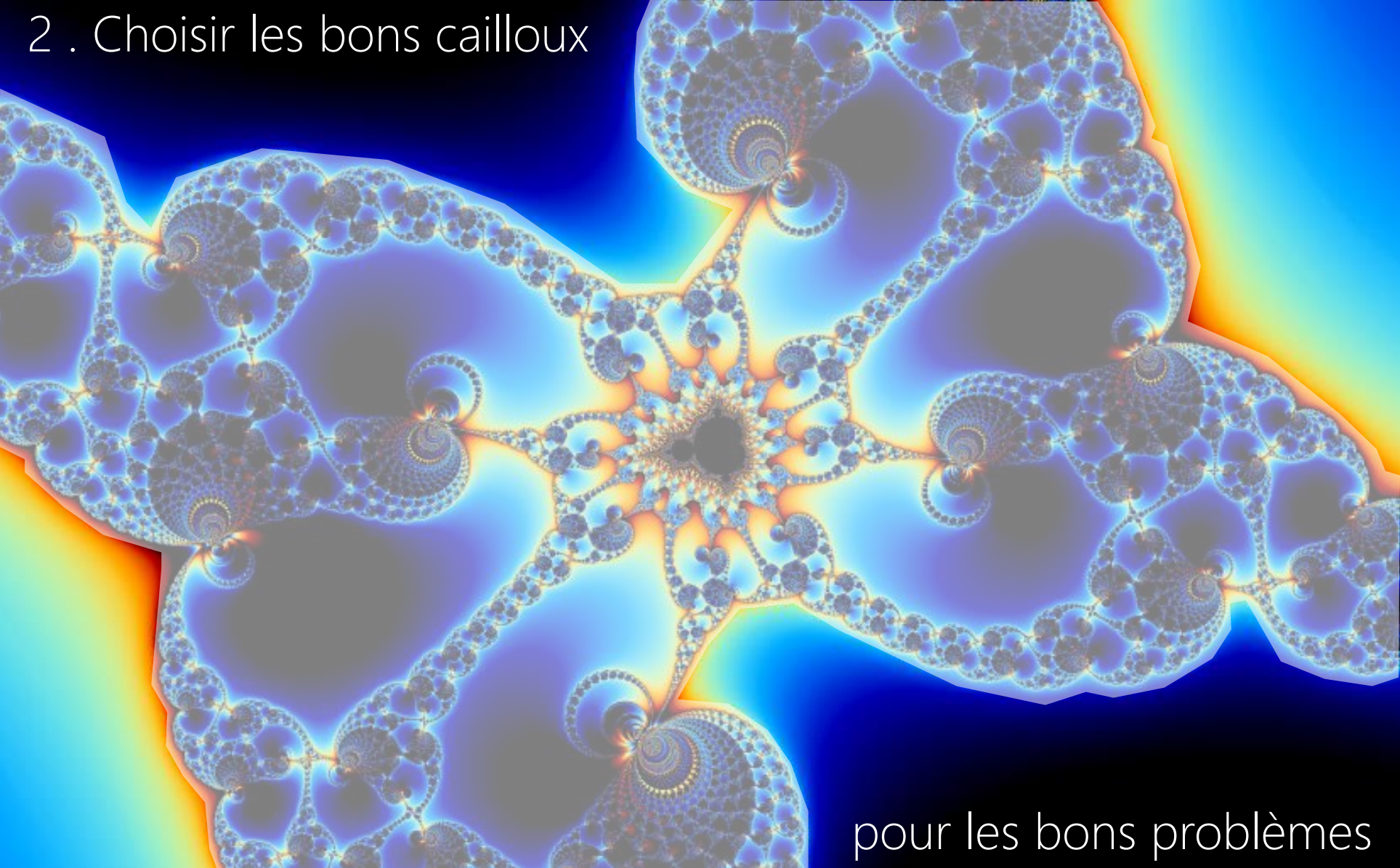
Numération positionnelle en base 10

Tout nombre s'écrit comme une suite de chiffres qui correspondent chacun au coefficient multiplicateur d'une puissance de 10.

Très pratique pour les grands nombres et pour les opérations !



2 . Choisir les bons cailloux



pour les bons problèmes

La numération positionnelle en base 2

Système binaire : tout nombre s'écrit comme une suite de *0* et de *1* qui correspondent chacun au coefficient multiplicateur d'une puissance de *2*.

Quick links

- IEEE754
- NNMEA2KML
- World sat image

Latest article

- Erfahrungsbericht Fotoprints

Contact

Tools & Thoughts

IEEE-754 Floating Point Converter

Translations: de

This page allows you to convert between the decimal representation of numbers (like "1.02") and the binary format used by all modern CPUs (IEEE 754 floating point).

IEEE 754 Converter (JavaScript), V0.22

	Sign	Exponent	Mantissa
Value:	+1	2^{-4}	1.600000023841858
Encoded as:	0	123	5033165
Binary:	☐	☐☑☑☑☑☑☑☑	☑☐☐☑☑☐☐☑☑☐☐☑ ☑☐☐☑☑☐☐☑☑☐☑

You entered: 0.1

Value actually stored in float: 0.100000001490116119384765625

Error due to conversion: 1.4901161193847656 25E-9

Binary Representation: 00111101110011001100110011001101

+1 -1

Une numération positionnelle en base 3

Système ternaire équilibré : tout nombre s'écrit comme une suite de *-1*, *0*, *1* qui correspondent chacun au coefficient multiplicateur d'une puissance de *3*.

$7 = 1 \times 3^2 - 1 \times 3^1 + 1 \times 3^0$ s'écrit *1-1 1*

$27 = 1 \times 3^3 + 0 \times 3^2 + 0 \times 3^1 + 0 \times 3^0$ s'écrit *1 0 0 0*

Théorème. *Tout entier relatif n dont la valeur absolue vérifie $|n| \leqslant \frac{3^p - 1}{2}$ s'écrit de manière unique sous la forme $n = \sum_{k=0}^{p-1} \varepsilon_k 3^k$ avec $\varepsilon_k \in \{-1, 0, 1\}$ pour tout k.*

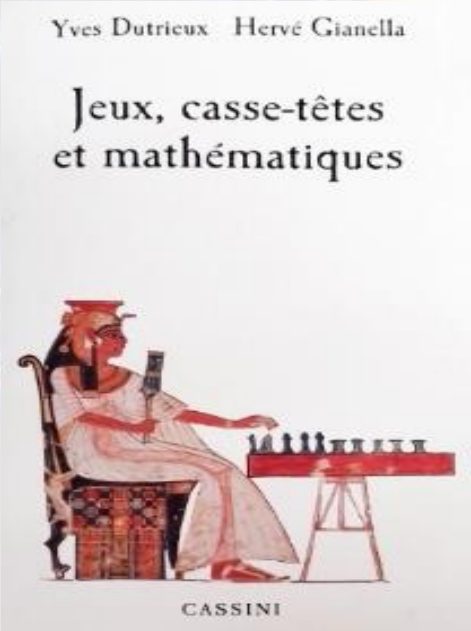
- adapté à l'électronique où le potentiel peut être négatif, neutre ou positif
- en 1958 un Ordinateur ternaire, le Setun, est développé à Moscou par des universitaires ; son système est basé sur une logique à trois états. Avant que l'URSS n'ait accès aux transistors, les (50) machines Setun étaient plus rapides et moins gourmandes en énergie que les ordinateurs binaires.

Problèmes plaisants et délectables qui se font par les nombres

Claude-Gaspard Bachet de Méziriac (1581-1638)

Trouver une série de poids avec lesquels on puisse faire toutes les pesées en nombres entiers depuis 1 jusqu'à la somme des poids employés,

cette somme étant la plus grande possible relativement au nombre de ces poids.

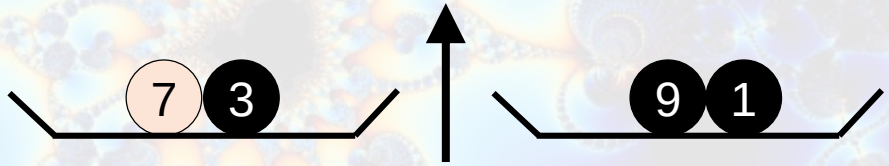


Problèmes plaisants et délectables qui se font par les nombres

On utilise les poids de masse 1, 3, 3^2, 3^3, … 3^{p-1} pour faire toutes les pesées en nombres entiers depuis 1 jusqu'à $(3^p - 1)/2$.

Exemple : les poids 1, 3, 9, 27 permettent toutes les pesées jusqu'à 40

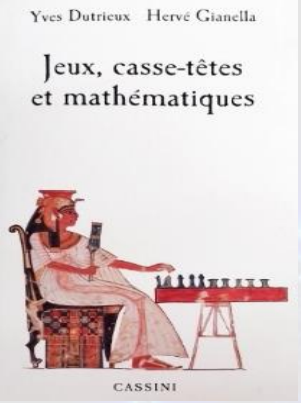
7 =1-3+9



23 =-1-3+27

39 =3+9+27

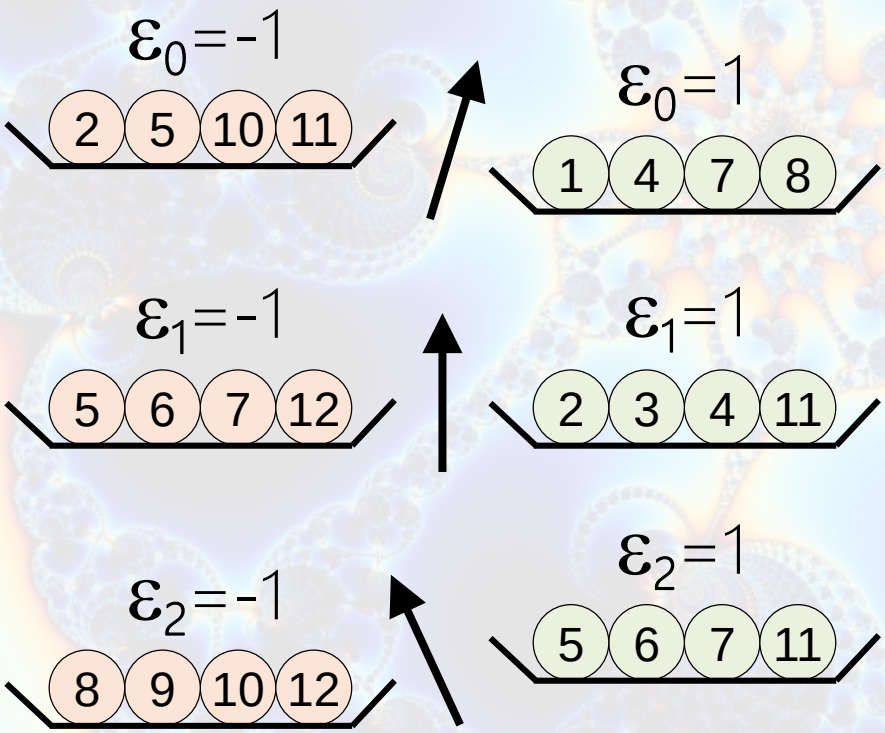
3^3	3^2	3^1	3^0
0	1	-1	1
1	0	-1	-1
1	1	1	0



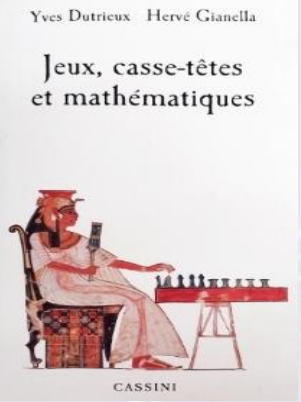
1945 : le problème de la fausse pièce

12 pièces de monnaie dont l'une est fausse ; elle n'a pas exactement la même masse que les autres ; on ignore si elle est plus lourde ou plus légère. Comment la trouver en 3 pesées ?

Solution publiée par Dyson en 1946



n	ε_2	ε_1	ε_0
1 = 0*9+0*3+1	0	0	1
2 = 0*9+1*3-1	0	1	-1
3 = 0*9+1*3+0	0	1	0
4 = 0*9+1*3+1	0	1	1
5 = 1*9-1*3-1	1	-1	-1
6 = 1*9-1*3+0	1	-1	0
7 = 1*9-1*3+1	1	-1	1
-8 = -1*9+0*3+1	-1	0	1
-9 = -1*9+0*3+0	-1	0	0
-10 = -1*9+0*3-1	-1	0	-1
11 = 1*9+1*3-1	1	1	-1
-12 = -1*9-1*3+0	-1	-1	0

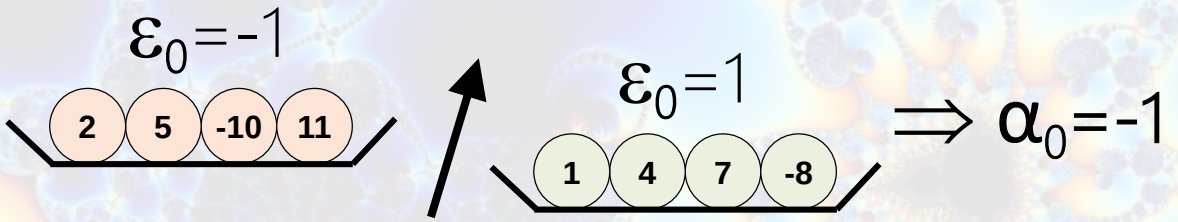


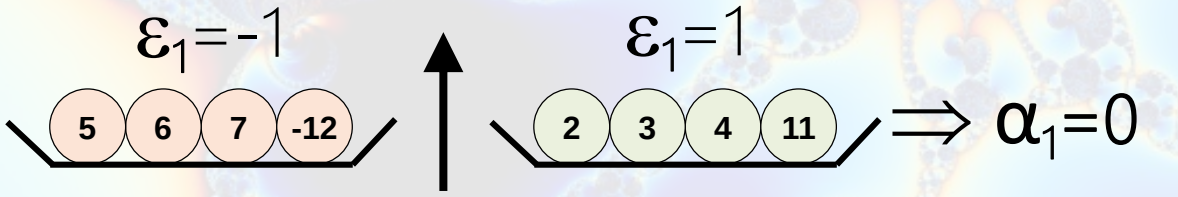
1945 : le problème de la fausse pièce

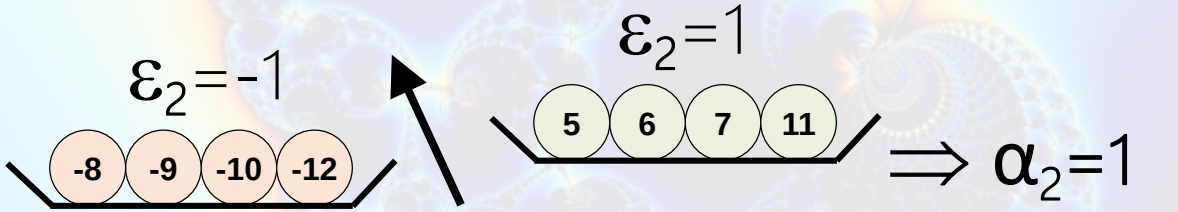
Notons la pièce recherchée $\alpha_2\ \alpha_1\ \alpha_0$

Dans le cas des pesées précédentes,

Si la pièce est plus légère ...

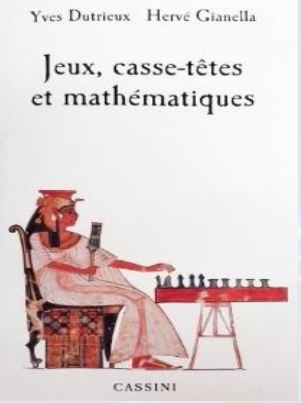






n		ε_2	ε_1	ε_0
1	= 0*9+0*3+1	0	0	1
2	= 0*9+1*3-1	0	1	-1
3	= 0*9+1*3+0	0	1	0
4	= 0*9+1*3+1	0	1	1
5	= 1*9-1*3-1		-1	-1
6	= 1*		-1	0
7	= 1*	1	-1	1
-8	= -1*9+0*3+1	-1	0	1
-9	= -1*9+0*3+0	-1	0	0
-10	= -1*9+0*3-1	-1	0	-1
11	= 1*9+1*3-1	1	1	-1
-12	= -1*9-1*3+0	-1	-1	0

1 0 -1

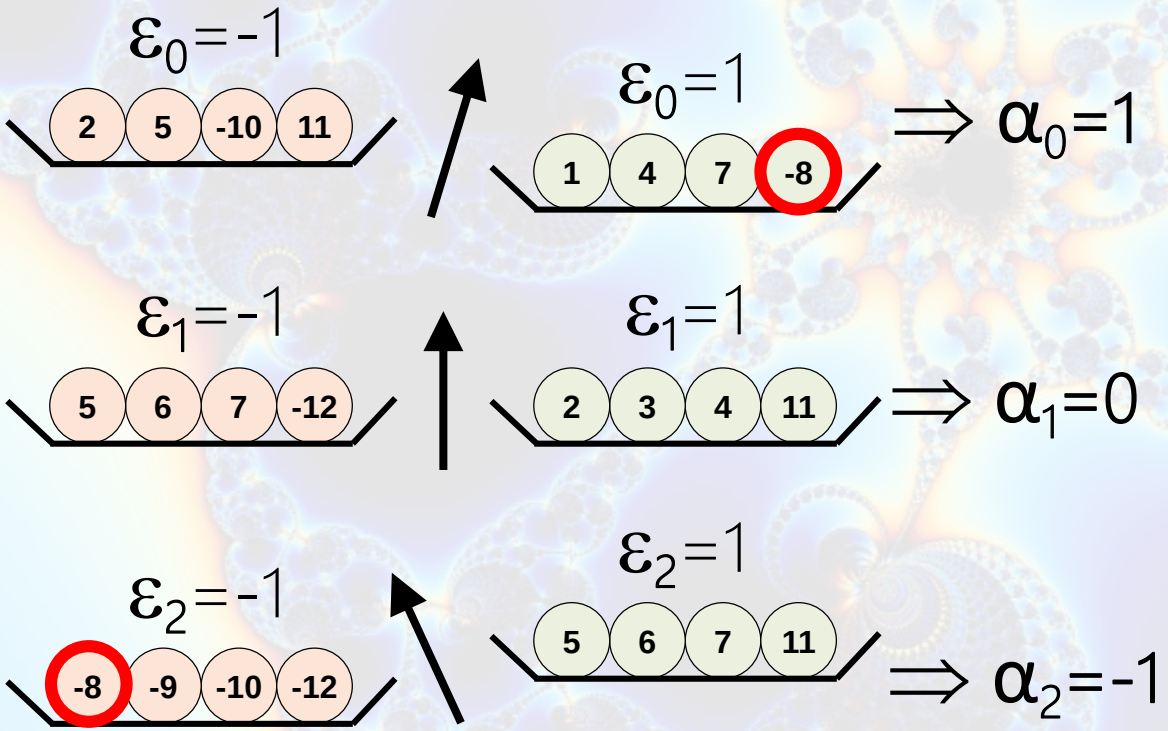


1945 : le problème de la fausse pièce

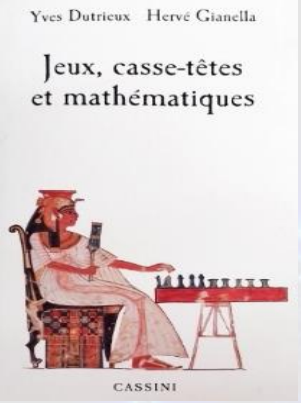
Notons la pièce recherchée $\alpha_2\ \alpha_1\ \alpha_0$

Dans le cas des pesées précédentes,

Si la pièce est plus lourde …



n	ε_2	ε_1	ε_0
1 = 0*9+0*3+1	0	0	1
2 = 0*9+1*3-1	0	1	-1
3 = 0*9+1*3+0	0	1	0
4 = 0*9+1*3+1	0	1	1
5 = 1*9-1*3-1	1	-1	-1
6 = 1*9-1*3+0	1	-1	0
7 = 1*9-1*3+1	1	-1	1
-8 = -1*9+0*3+1	-1	0	1
-9 = -1*9+0*3+0	-1	0	0
-10 = -1*9+0*3-1	-1	0	-1
11 = 1*9+1*3-1	1	1	-1
-12 = -1*9-1*3+0	-1	-1	0



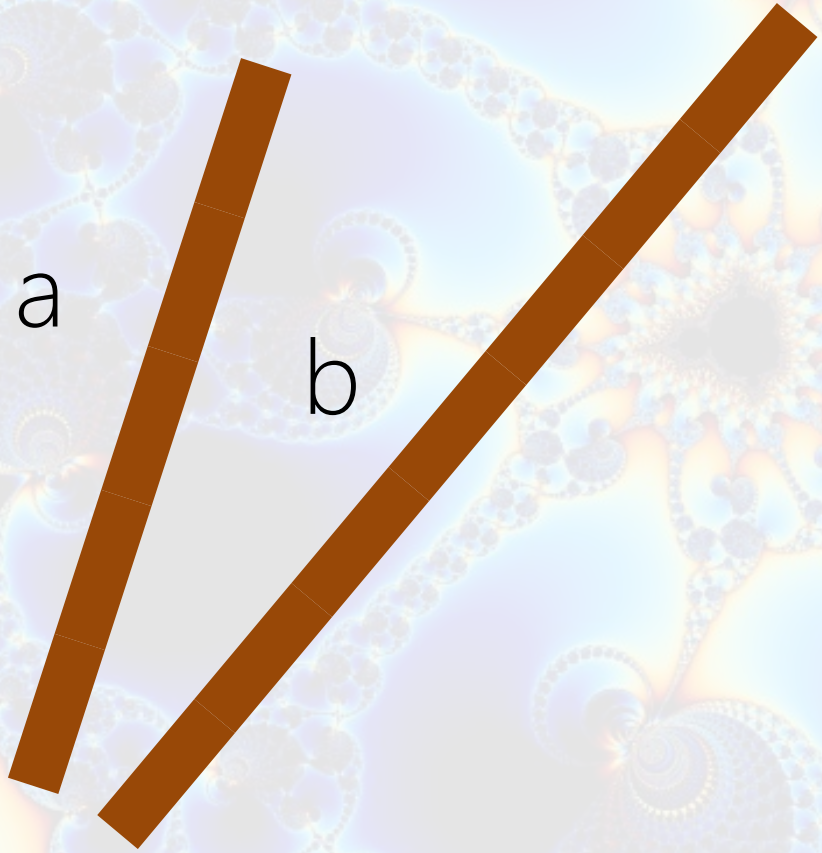
1945 : le problème de la fausse pièce

n = nb pièces $n=(3^p-3)/2$	p = nb pesées
3	2
12	**3**
120	5
1 092	7
88 572	11
797 160	13
64 570 080	17
581 130 732	19
47 071 589 412	23

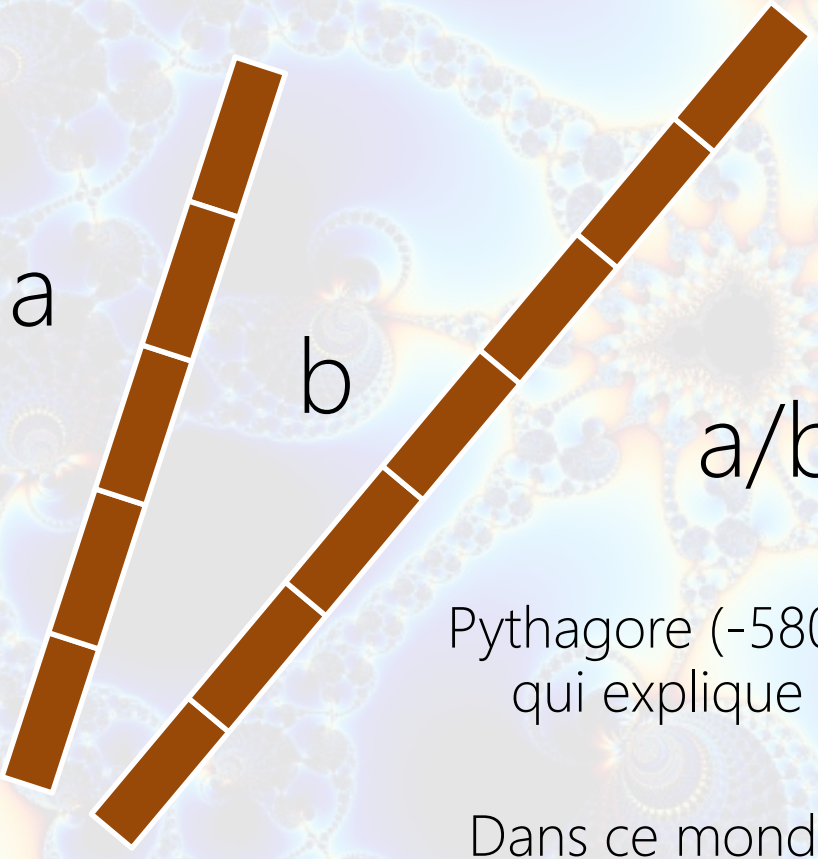
1945 : le problème de la fausse pièce

n = nb pièces $n=(3^p-3)/2$	p = nb pesées	q = nb pièces par plateau $q=n/3$	nb mvts $= 2*p*q$
3	2	1	4
12	**3**	**4**	24
120	5	40	400
1 092	7	364	5 096
88 572	11	29 524	649 528
797 160	13	265 720	6 908 720
64 570 080	17	21 523 360	731 794 240
581 130 732	19	193 710 244	7 360 989 272
47 071 589 412	23	15 690 529 804	721 764 370 984

Mesurer le monde avec les « rationnels



Mesurer le monde avec les « rationnels »



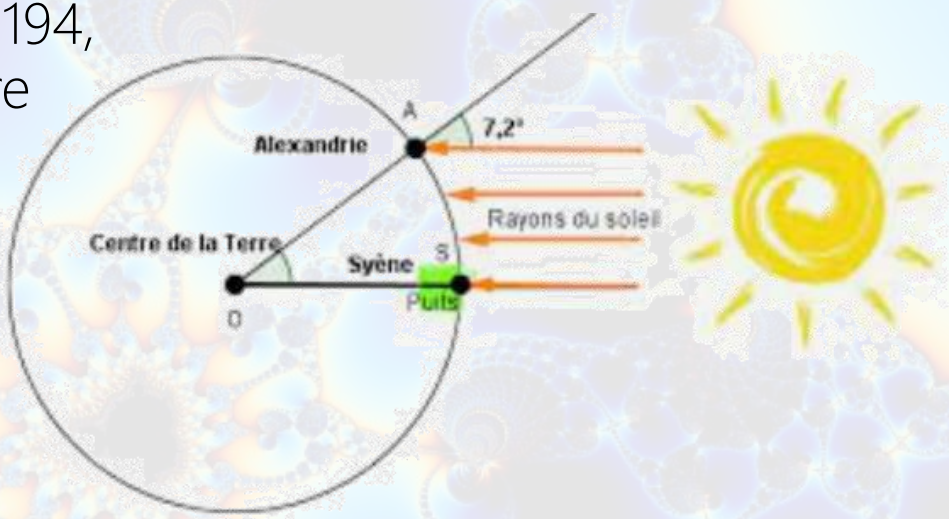
$$a/b = 5/7$$

Pythagore (-580 ; -495) développe une pensée qui explique le monde à travers les nombres entiers et leurs rapports.

Dans ce monde, tout est « commensurable » !

Mesurer la circonférence de la terre

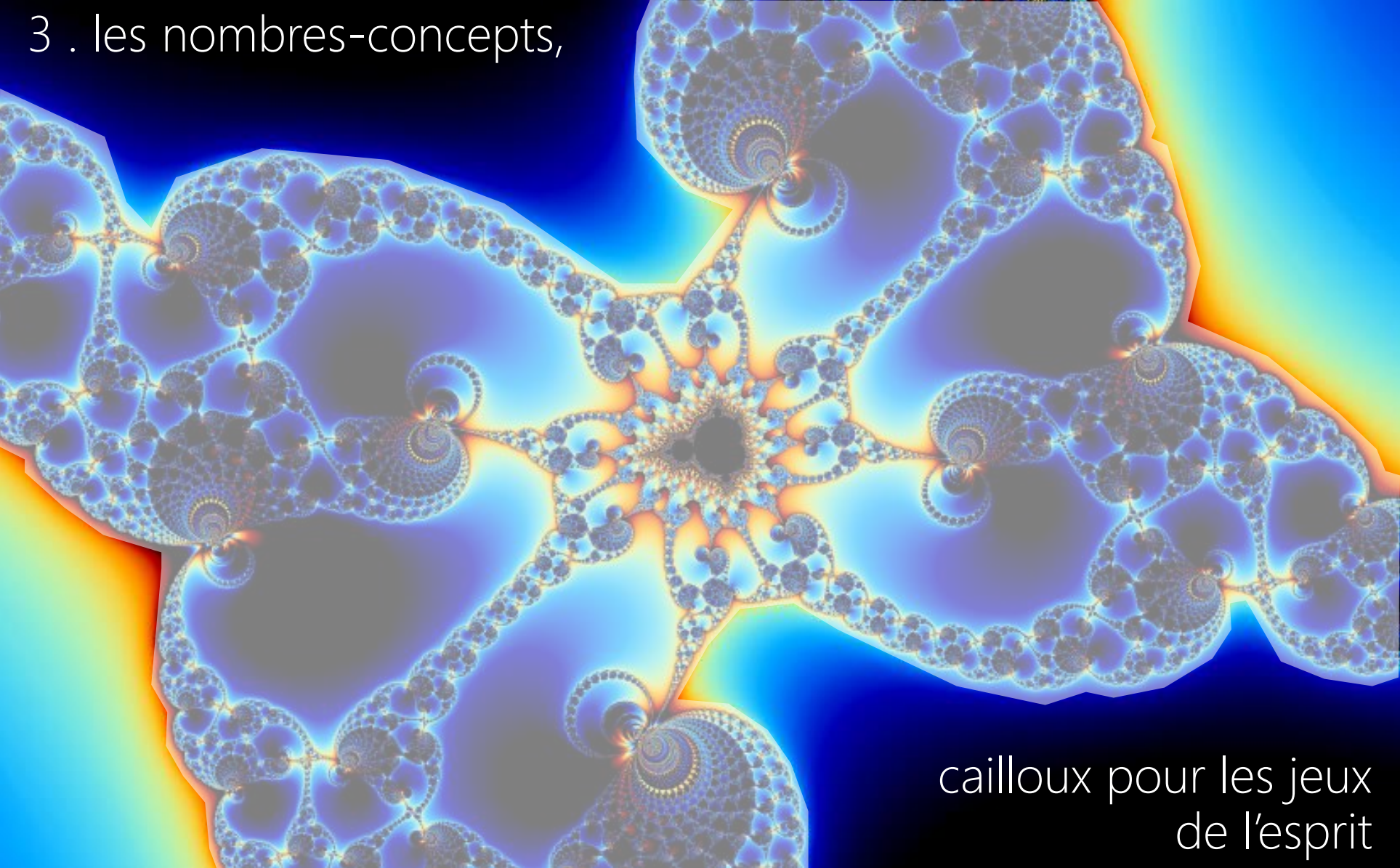
Un jour en Egypte, entre -276 et -194, *Eratosthène*, qui pense que la Terre est ronde, décide de mesurer sa circonférence.



En observant la différence d'inclinaison des rayons du Soleil entre les villes de Syène/Assouan et d'Alexandrie, il calcule que la distance entre les deux cités doit représenter 1/50 de cette circonférence. Des bématistes (avec leurs chameaux), après de longues journées de voyage le long du Nil donnent la distance entre les deux villes : 5 000 stades ⇒ circonférence (Terre) = 250 000 stades = 39 375 kilomètres …

… aujourd'hui on estime cette circonférence à 40 008 kilomètres.

3 . les nombres-concepts,



cailloux pour les jeux
de l'esprit

Degrés de l'Ecole Pythagoricienne

500 av. J-C

MATHÉMATICIEN

CONNAISSANCE

DÉMONSTRATIONS

ACOUSMATICIEN

SERMENT DE SILENCE
DÉBUT DE L'ENSEIGNEMENT
MISE EN PRATIQUE

5 ans

NÉOPHYTE

PERSÉVERANCE

DÉSIR D'APPRENDRE

3 ans

POSTULANT

Entretiens d'observation

ATTITUDE
RIRE
FRÉQUENTATIONS
DÉSIRS

Découverte de l'incommensurabilité

source : wikipedia

Hippase de Métaponte (Pythagoricien)
Mathématicien de l'école pythagoricienne (Maître d'Héraclite ?)

- construction du pentagone régulier
- **incommensurabilité** de certains segments de figures construites géométriquement

⇒ **certains nombres constructibles sont irrationnels :**

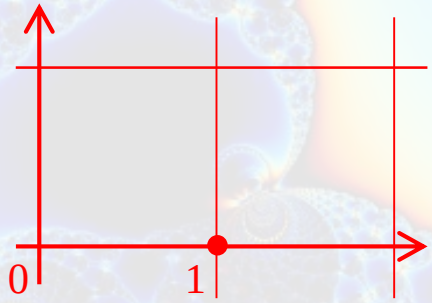
- la diagonale du carré de côté 1 : $\sqrt{2}$
- le nombre d'or $(1+\sqrt{5})/2 \sim 1{,}618\ 033\ 988\ 749\ 894\ 848\ 204\ 586\ 834\ 365\ 638\ 117\ 720\ 309\ 179\ 805\ 762\ 862\ 135\ 448\ 622\ 705\ 260\ 462\ 818\ 902\ 449\ 707\ 207\ 204$

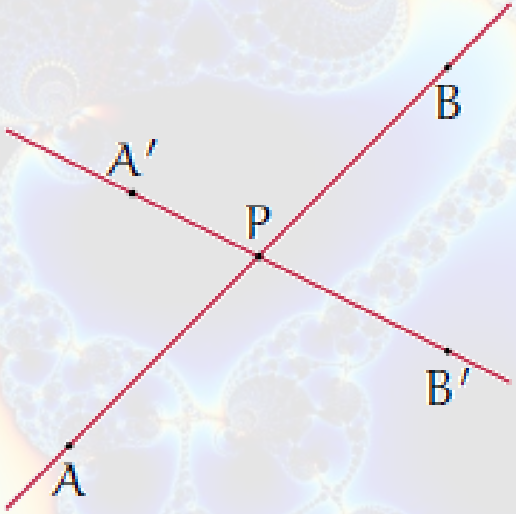
La découverte de l'incommensurabilité jeta le trouble dans la confrérie et ouvrit une profonde crise philosophique.

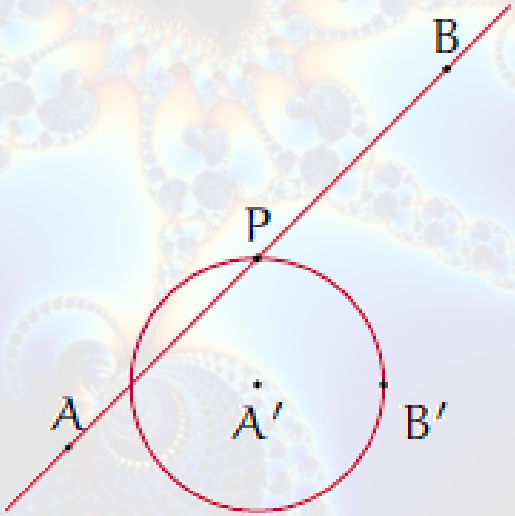
Théorie des constructibles

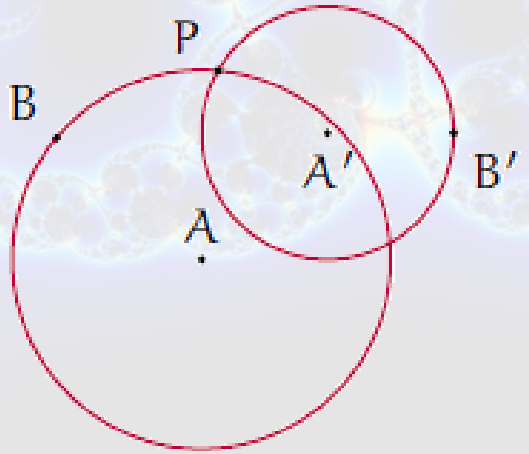
$\mathcal{C}_0 = \{O, I\}$ où $O = (0,0)$ et $I = (1,0)$.
Pour $i \geq O$, $\mathcal{C}_{i+1}$ est l'ensemble des ***points élémentairement constructibles*** à partir de $\mathcal{C}_i$, c'est-à-dire : $P \in \mathcal{C}_{i+1}$ si et seulement si

1. $P \in (AB) \cap (A'B')$ avec $A, B, A', B' \in \mathcal{C}_i$
2. ou $P \in (AB) \cap \mathcal{C}(A', A'B')$ avec $A, B, A', B' \in \mathcal{C}_i$
3. ou $P \in \mathcal{C}(A, AB) \cap \mathcal{C}(A', A'B')$ avec $A, B, A', B' \in \mathcal{C}_i$



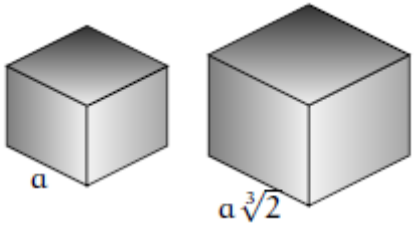






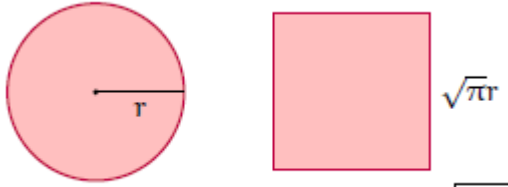
Théorie des constructibles

Théorème 2. $\sqrt[3]{2}$ n'est pas un nombre constructible.



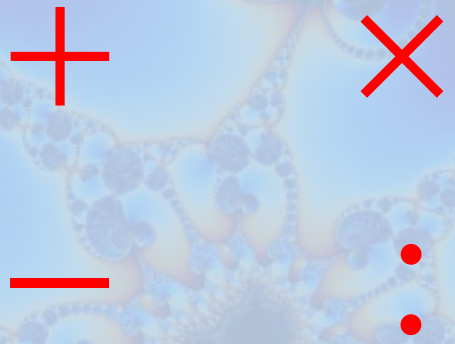
La duplication du cube ne peut s'effectuer à la règle et au compas.

Théorème 3. π n'est pas un nombre algébrique (donc n'est pas constructible).



La quadrature du cercle ne peut s'effectuer à la règle et au compas.

Idées-Formes-Modèles



Fabrication des pots

Multiplication des pains

Vol de moutons

Partage du gâteau

Monde sensible-Expérimentation

Idées-Formes-Modèles

Problème d'arithmétique
= classe d'équivalence
de questions propres aux quantités

Problème d'algèbre
= classe d'équivalence
de questions propres aux équations

Quels sont les entiers naturels qui n'ont que 2 diviseurs ?

quantité
= classe d'équivalence
de collections

équation
= classe d'équivalence
de problèmes

Monde sensible-Expérimentation

Naissance et développement de l'algèbre

Dès l'Antiquité égyptienne ou babylonienne, les scribes disposaient de procédures pour déterminer une quantité soumise à certaines conditions.

Au 3ème siècle de l'ère chrétienne, Diophante d'Alexandrie pratique une forme d'algèbre pré-symbolique en introduisant une inconnue sur laquelle il opère des calculs.

Naissance et développement de l'algèbre

En 711, un jeune commandant arabe de 20 ans défait avec 2000 cavaliers une armée de 50 000 hommes et envahit le delta de l'Indus.

Vers 825, dans une époque d'essor des sciences et techniques islamiques, le mathématicien d'origine persane **Al-Khwarizmi** est à Bagdad. Il rédige un ouvrage dédié au calcul d'héritage, à l'arpentage, aux échanges commerciaux : « **al-djabr** ».

Le titre de ce livre signifie réduction d'une fracture, réunion des morceaux, reconstruction, connexion, restauration, reboutement.

Par la suite, le mot « algèbre » désignera la science de transformation /résolution des **équations**.

Naissance et développement de l'algèbre

Le système indien, sera transmis par les arabes à l'Occident médiéval et se développera sous l'impulsion du pape Gerbert d'Aurillac (945-1003), mais mettra plusieurs siècles à supplanter le système de numération romain.

Ce système sera promu par le mathématicien italien Léonard de Pise, dit **Fibonacci**.

Notons que le mot *chiffre* vient de l'arabe *sifr* qui signifie «vide» et le mot zéro vient de l'ancien italien *zefiro* qui lui-même vient de l'arabe sifr.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Le passage d'un ensemble à un ensemble plus grand se justifie par la volonté de résoudre davantage d'équations :

- passage de $\mathbb{N}$ à $\mathbb{Z}$ pour résoudre des équations du type $x+7=0$,
- passage de $\mathbb{Z}$ à $\mathbb{Q}$ pour résoudre des équations du type $5x=4$,
- passage de $\mathbb{Q}$ à $\mathbb{R}$ pour résoudre des équations du type $x^2=4$,
- passage de $\mathbb{R}$ à $\mathbb{C}$ pour résoudre des équations du type $x^2=-1$,

Mais en fait le passage de $\mathbb{Q}$ à $\mathbb{R}$ est un saut beaucoup plus «grand» que les autres : $\mathbb{Q}$ est un ensemble dénombrable (il existe une bijection entre $\mathbb{Z}$ et $\mathbb{Q}$) alors $\mathbb{R}$ ne l'est pas.

Nous allons définir et étudier deux ensembles intermédiaires :

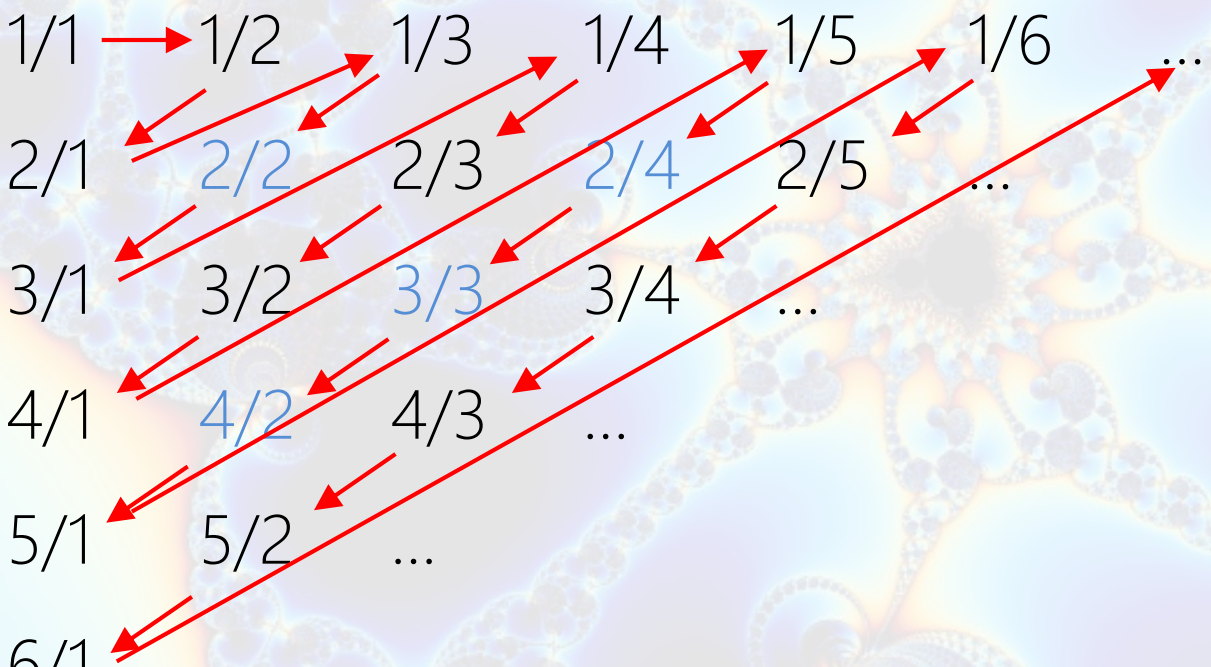
$$\mathbb{Q} \subset \mathcal{C}_{\mathbb{R}} \subset \overline{\mathbb{Q}} \subset \mathbb{R}$$

où

- $\mathcal{C}_{\mathbb{R}}$ est l'ensemble des nombres constructibles à la règle et au compas,
- $\overline{\mathbb{Q}}$ est l'ensemble des nombres algébriques : ce sont les réels x qui sont solutions d'une équation $P(x)=0$, pour un polynôme P à coefficients dans $\mathbb{Q}$.

Q est dénombrable

(peut être mis en bijection avec N)



729/16777216

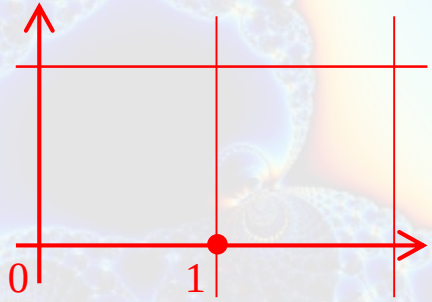
Diagonal de Cantor

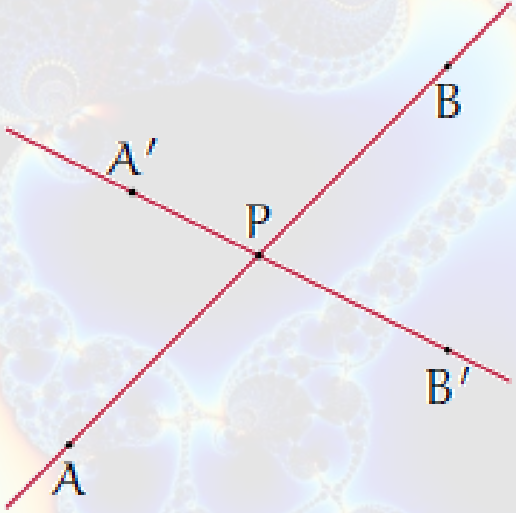
Supposons qu'on puisse énumérer les réels, et construisons un tableau semi-infini à deux entrées dont la *n*-ième ligne représenterait le *n*-ième réel sous forme d'une liste infinie de décimales.
Construisons maintenant un réel tel que sa *n*-ième décimale soit différente de la *n*-ième décimale de la *n*-ième ligne du tableau (diagonale).
Ce réel ne trouve pas sa place dans la liste !

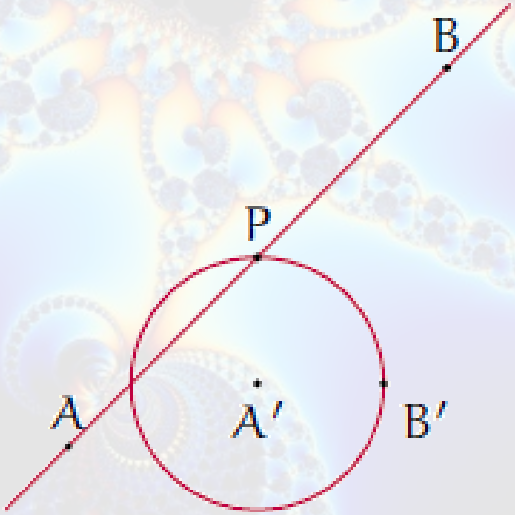
Théorie des constructibles

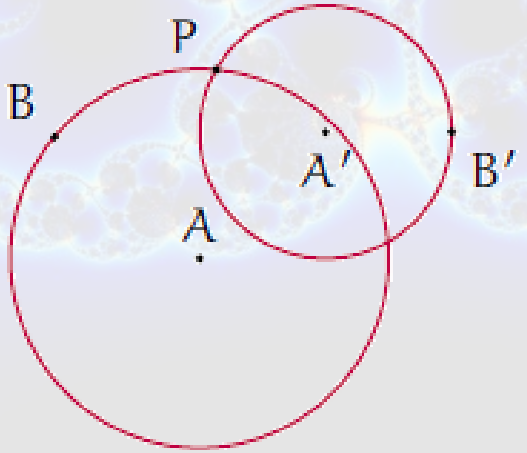
$\mathcal{C}_0 = \{O, I\}$ où $O = (0,0)$ et $I = (1,0)$.
Pour $i \geq O$, $\mathcal{C}_{i+1}$ est l'ensemble des ***points élémentairement constructibles*** à partir de $\mathcal{C}_i$, c'est-à-dire : $P \in \mathcal{C}_{i+1}$ si et seulement si

1. $P \in (AB) \cap (A'B')$ avec $A, B, A', B' \in \mathcal{C}_i$
2. ou $P \in (AB) \cap \mathcal{C}(A', A'B')$ avec $A, B, A', B' \in \mathcal{C}_i$
3. ou $P \in \mathcal{C}(A, AB) \cap \mathcal{C}(A', A'B')$ avec $A, B, A', B' \in \mathcal{C}_i$



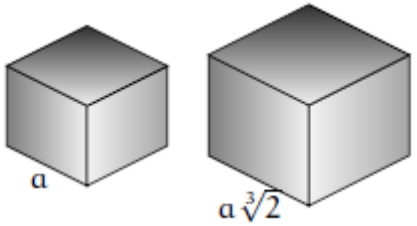






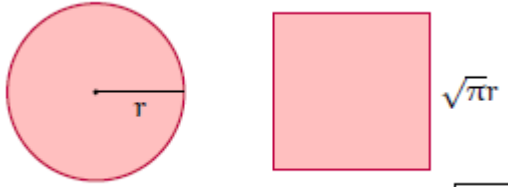
Théorie des constructibles

Théorème 2. $\sqrt[3]{2}$ n'est pas un nombre constructible.



La duplication du cube ne peut s'effectuer à la règle et au compas.

Théorème 3. π n'est pas un nombre algébrique (donc n'est pas constructible).



La quadrature du cercle ne peut s'effectuer à la règle et au compas.

Algébriques VERSUS Transcendants

- Les **rationnels** sont dénombrables
- Les **irrationnels** ne sont pas dénombrables

*Définition : les **algébriques** sont solutions d'équations polynomiales à coefficient dans* Q

$$13/25 \times x^5 + 2/3\, x = 11/17$$

- Les **constructibles** sont **algébriques**
- Les **algébriques** sont dénombrables

*Définition : les non-algébriques sont appelés **transcendants***

π *est un nombre transcendant*

- Les **transcendants** ne sont pas dénombrables

Les nombres premiers

Définition des nombres premiers

Un entier naturel p est premier s'il admet exactement deux diviseurs : 1 et lui-même.

Exemples

Exemples : 2, 3, 5, 7, 11, 13, 17, 19, etc.

Contre-Exemples : 0, 1, 4, 6, 8, 9, 10, etc.

Plus grand exemple connu (2008) : $2^{43112609} - 1$

Décomposition en nombres premiers

Selon le théorème fondamental de l'arithmétique, tout entier strictement positif possède une unique décomposition en facteurs premiers.

$5 = 5$

$25 = 5 \times 5 = 5^2$

$125 = 5 \times 5 \times 5 = 5^3$

$360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 = 2^3 \times 3^2 \times 5$

$1\,001 = 7 \times 11 \times 13$

$1\,010\,021 = 17 \times 19 \times 53 \times 59$

Tout rationnel peut s'écrire de façon unique comme fraction irréductible

$50/70 = 5/7$

Lectures from
Avinash Kak
India

Arithmétique modulo n

$$a = b \ (mod\ 4)$$

si et seulement si les restes des divisions par 4 de a et b sont égaux.

$$Z_4 = \{0, 1, 2, 3\}$$

0	0	4	8	12	16	...
1	1	5	9	13	17	...
2	2	6	10	14	18	...
3	3	7	11	15	19	...

$$0 \times x = 0$$

$$0 + x = x$$

$$1 \times x = x$$

$$x \times y \stackrel{?}{=} 1$$

Arithmétique modulo n

$$a = b \ (mod\ 7)$$

si et seulement si les restes des divisions par 7 de a et b sont égaux.

Quand p est premier, tous les éléments de Z_p sauf 0 ont un inverse unique pour la multiplication.

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$1 \times 1 = 1 \ mod\ 7$

$2 \times 4 = 1 \ mod\ 7$

$3 \times 5 = 1 \ mod\ 7$

$6 \times 6 = 1 \ mod\ 7$

Les nombres premiers

Théorème d'Euclide (≈300 av. J.-C.)

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Démonstration

Supposons que $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$.

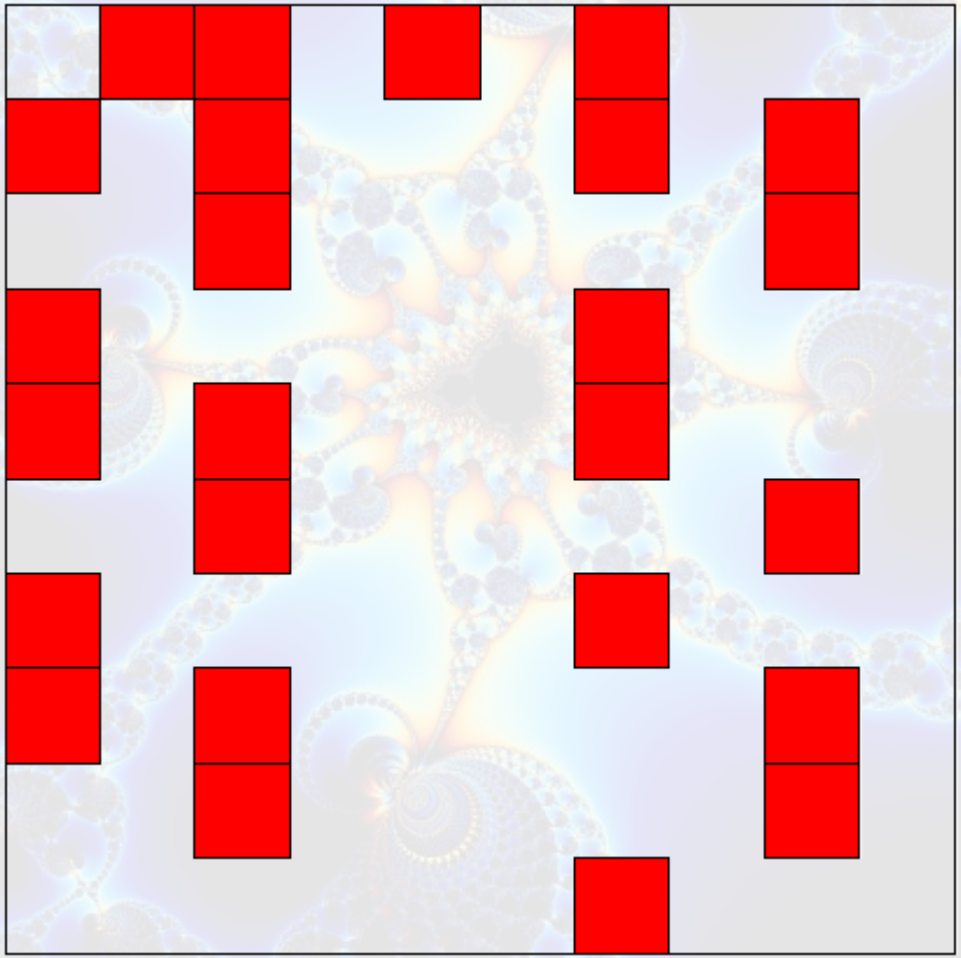
$$p = 1 + p_1 \times p_2 \times \cdots \times p_n$$

Alors $p \in \mathcal{P}$ mais $p \notin \{p_1, p_2, \ldots, p_n\}$. □

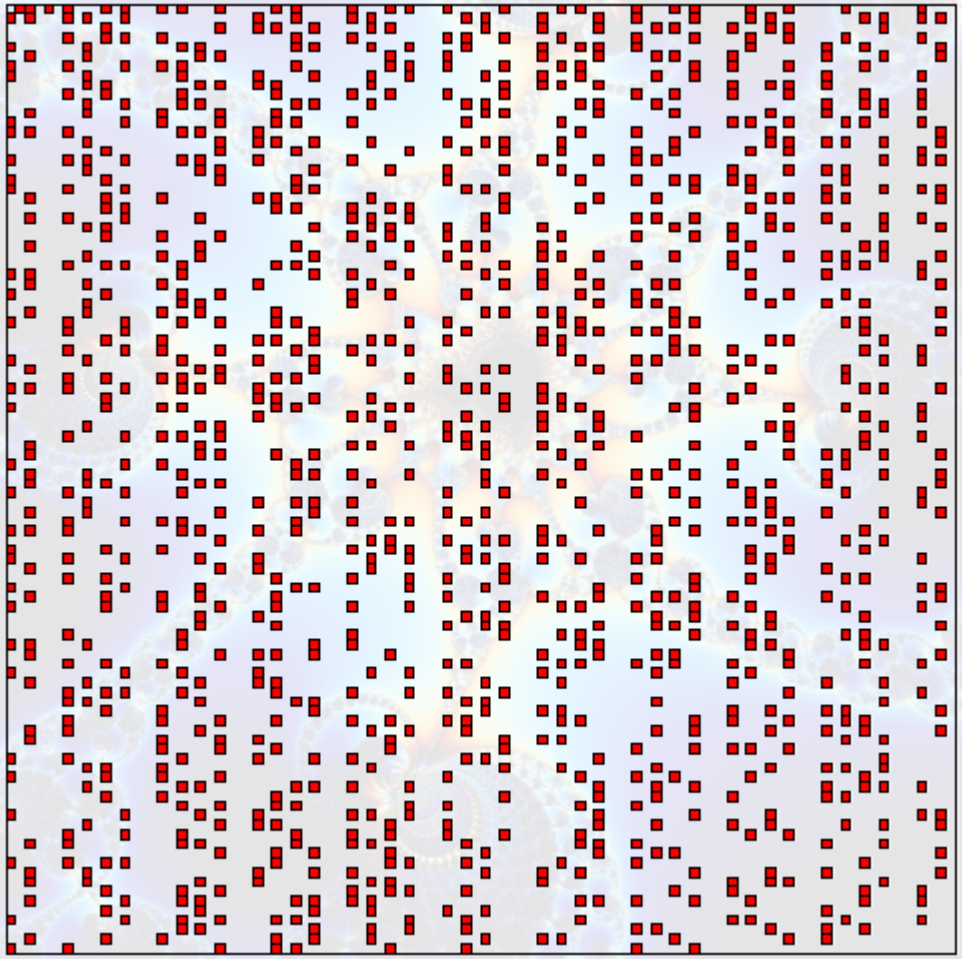
Questions

- Quel est la proportion de nombres premiers ?
- Comment sont-ils répartis dans $\mathbb{N}$?
- Existe-t-il une formule pour p_n ?

Répartition des nombres premiers inférieurs à 10 x 10 = 100



Répartition des nombres premiers inférieurs à 100 x 100 = 10 000



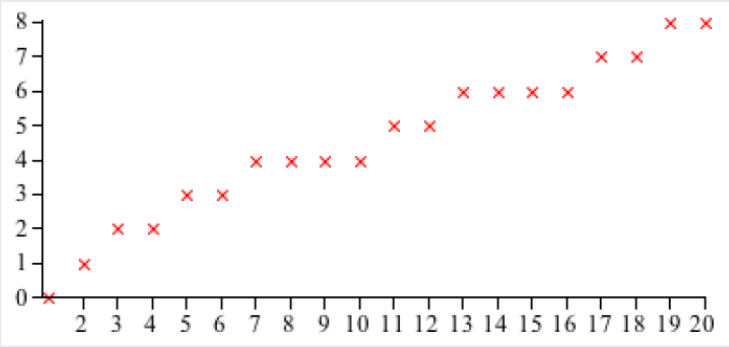
Répartition des nombres premiers inférieurs à 1000 x 1000 = 1 000 000

A 15 ans, Karl Friedrich Gauss (1777-1855) collectionne les nombres premiers au dos de ses tables de logarithmes.

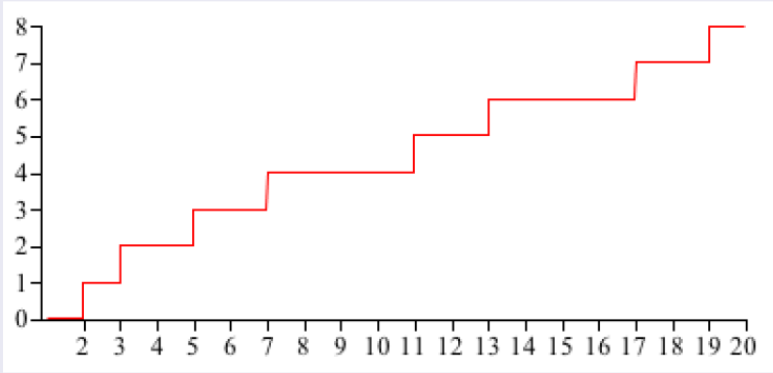
Ni	Combien de nombres premiers dans Ni ?	Combien de nombres en moyenne faut-il tester dans Ni avant de rencontrer un nombre premier ?
10	4	2,5
100	25	4,0
1 000	168	6,0
10 000	1 229	8,0
100 000	9 592	10,4
1 000 000	78 498	12,7
10 000 000	664 579	15,0
100 000 000	5 761 455	17,4
1 000 000 000	50 847 534	19,7
10 000 000 000	455 052 511	22,0

Pouvons-nous les compter ?

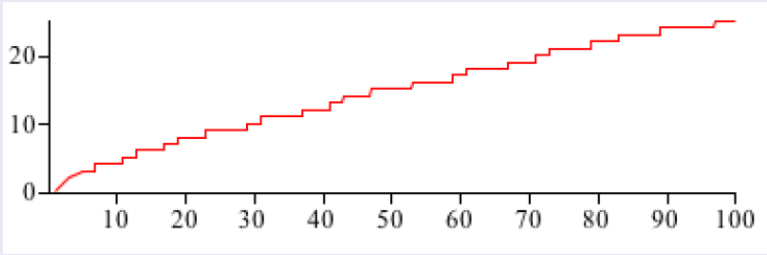
$$\pi : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto \pi(n) = \text{nombre de } p \in \mathcal{P} \text{ tel que } p \leqslant n$$



$$\pi : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto \pi(x) = \text{nombre de } p \in \mathcal{P} \text{ tel que } p \leqslant x$$

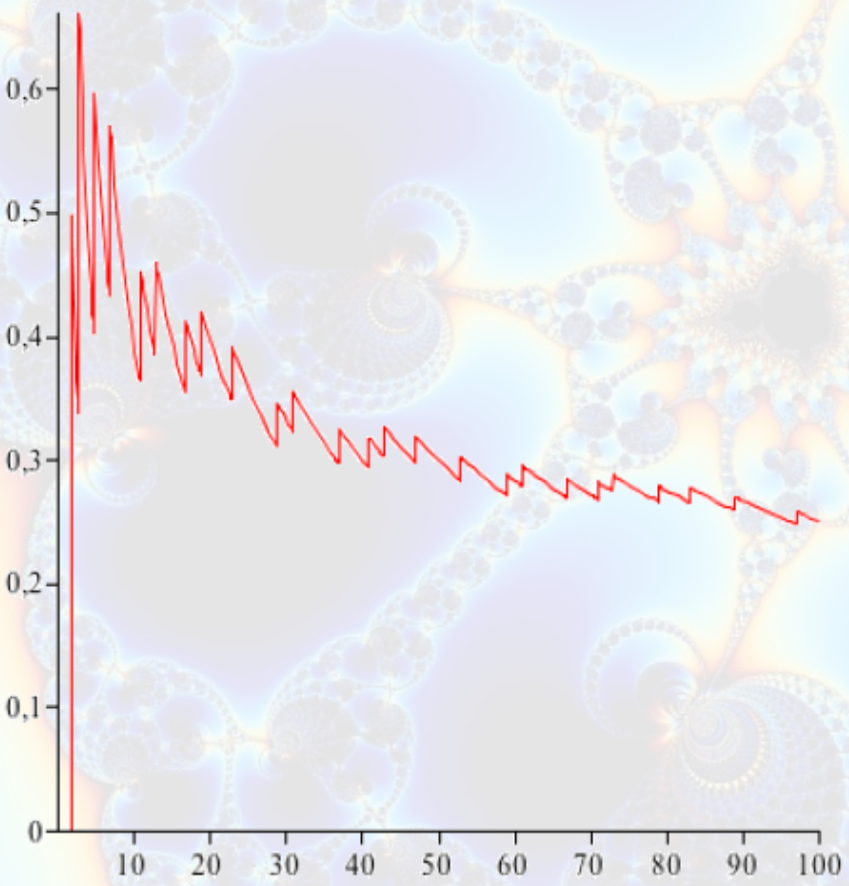


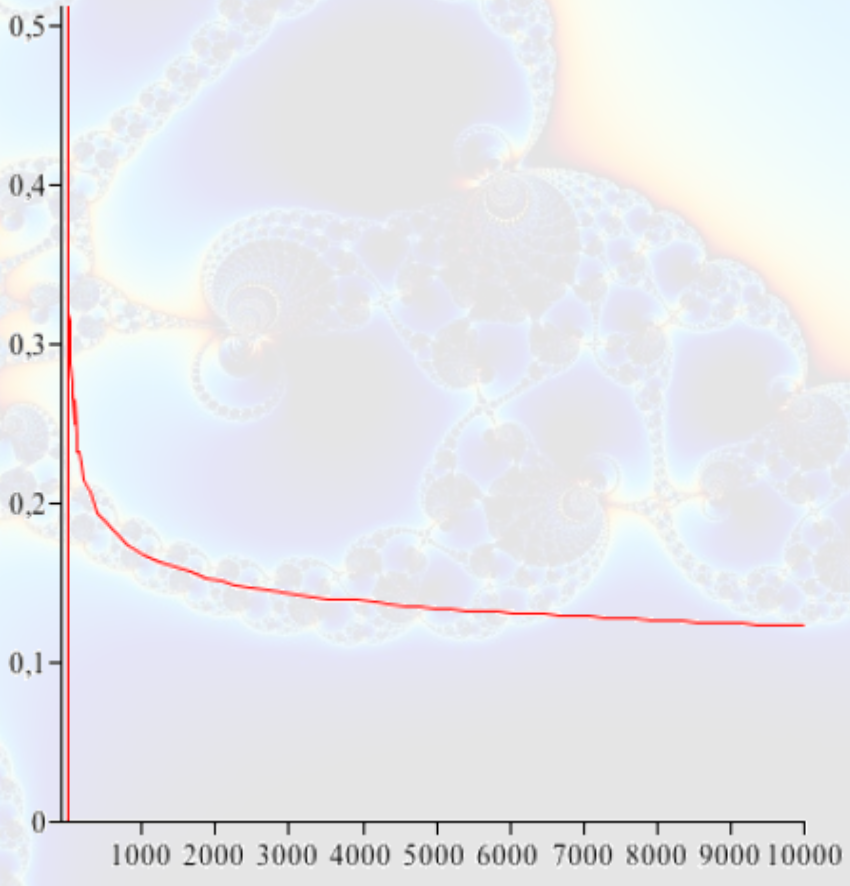
$$\pi : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto \pi(x) = \text{nombre de } p \in \mathcal{P} \text{ tel que } p \leqslant x$$



Comment évolue la proportion ?

$$x \mapsto \frac{\pi(x)}{x} = \text{proportion de } p \in \mathcal{P} \text{ tel que } p \leqslant x$$





Conjecture de Gauss (1792) et Legendre (1798)

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln(x)} \text{ lorsque } x \to +\infty$$

Théorème des nombres premiers (1896)

$$\frac{\pi(x)}{x} \underset{x\to+\infty}{\sim} \frac{1}{\ln(x)} \quad \textbf{(TNP)}$$

En particulier, la proportion des nombres premiers est infiniment petite.

Idées – Formes - Modèles

Beauté

Luxe Commerce

Niko (Nicole Mathieu)
2022
Galerie Bartoux à Megève
Prix = 28 800 €

Monde sensible - Expérimentation

Commerce
1977 : chiffrement RSA

Chiffrement asymétrique = Public-Key Cryptography

Je donne à un tiers la possibilité de chiffrer avec ma clé publique un message que moi seul pourrai déchiffrer avec ma clé privée

RSA might have been called CCC

Clifford Christopher Cocks

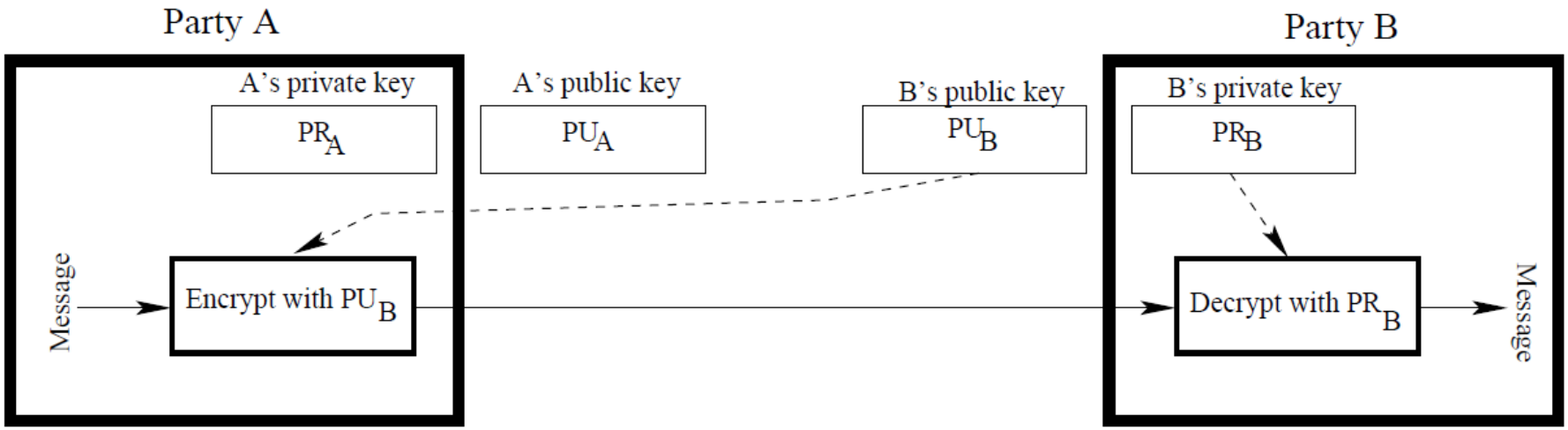
(born 28 December 1950) is a British mathematician and cryptographer.

In 1973, while working at the United Kingdom Government Communications Headquarters, he invented a public-key cryptography algorithm equivalent to what would become (in 1977) the RSA algorithm.

The idea was classified information and his insight remained hidden for 24 years

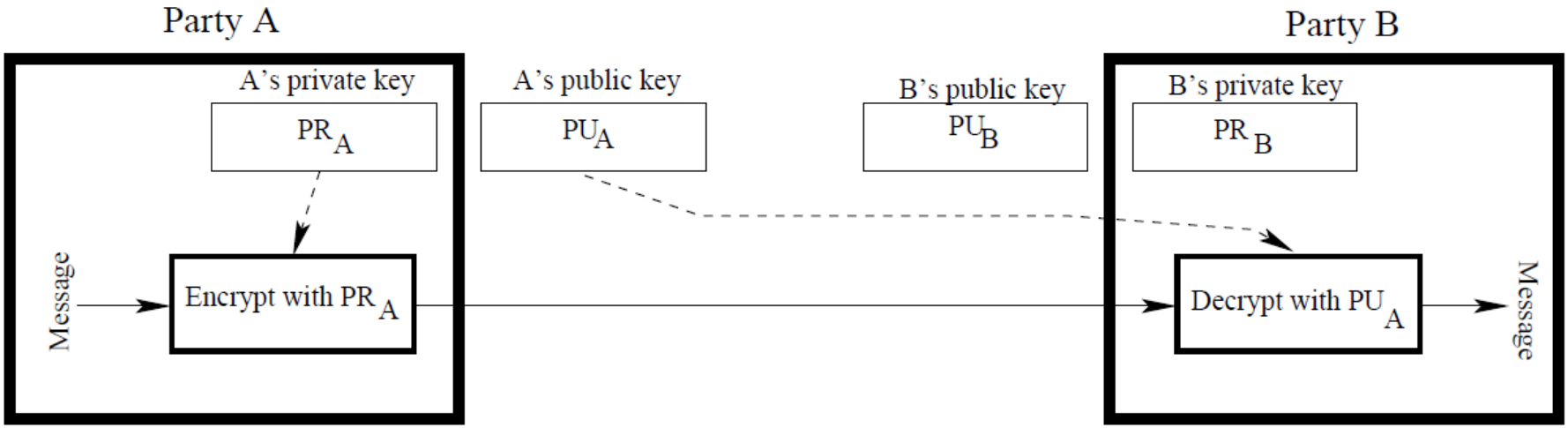
Public-Key Cryptography

When only confidentiality is needed:



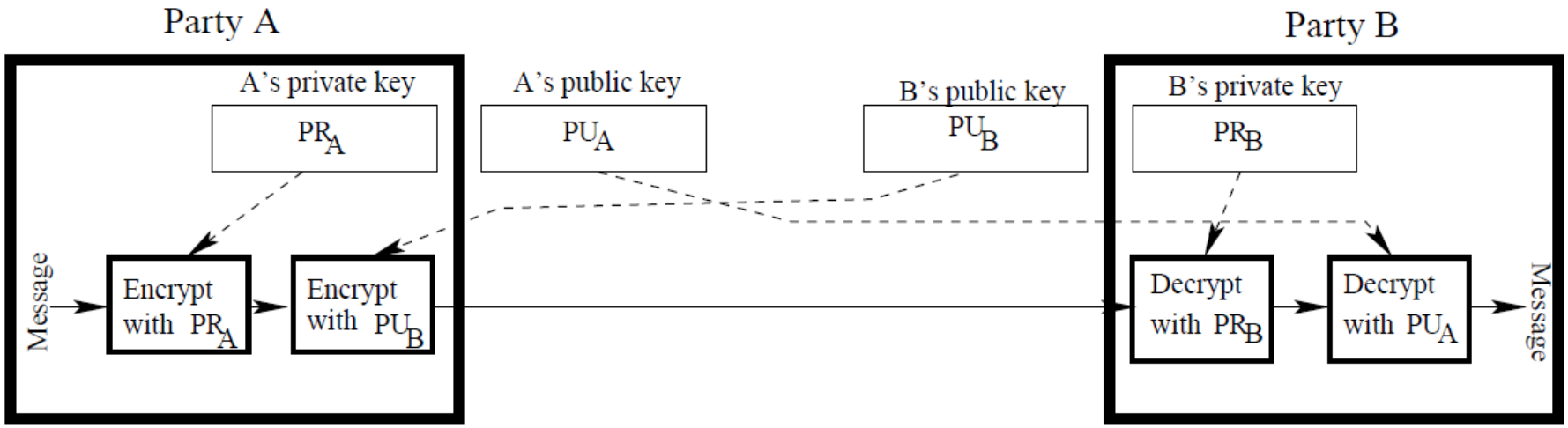
Public-Key Cryptography

When only authentication is needed:



Public-Key Cryptography

When both confidentiality and authentication are needed:



Lectures from
Avinash Kak
India

Euler's Totient function $\Phi(n)$

$\Phi(n)$ is the number of positive integers $\leq n$ that are coprime to n.

ints:	1	2	3	4	5	6	7	8	9	10	11	12
totients:	1	1	2	2	4	2	6	4	6	4	10	4

Suppose a number n is a product of two primes p and q, that is $n = p \times q$, then $\phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$

Very useful for RSA !

The basic idea of RSA

M is an integer representing the message

$n \geq M$

We suppose (e, d) *such that:* $M^{e \times d} = M \pmod{n}$

The ciphertext C results from the exponentiation : $C = M^{e} \pmod{n}$

We recover back M from C by the operation : $M = C^{d} \pmod{n}$


Ronald Rivest


Adi Shamir


Leonard Adleman

How to compute the RSA keys

1. Generate two different primes p and q
2. Calculate the modulus $n = p \times q$
3. Calculate the totient $\Phi(n) = (p - 1) \times (q - 1)$
4. Select for public exponent an integer e such that
$$1 < e < \Phi(n) \text{ and } \gcd(\Phi(n), e) = 1$$
5. Calculate for the private exponent a value for d such that
$$d = e^{-1} \bmod \Phi(n)$$
6. Public Key = [e, n]
7. Private Key = [d, n]

4 . Les limites du contrôle, cailloux dans la chaussure

Deux petits cailloux dans le RSA

Le RSA repose sur deux conjectures :

- *Conjecture 1* : « casser » RSA par la force brute nécessite la factorisation du nombre *n* en le produit initial des nombres *p* et *q*
- *Conjecture 2* : avec les algorithmes classiques, le temps que prend cette factorisation croît exponentiellement avec la longueur de la clé *n*

Le 2 décembre 2019, le plus grand *n* cassé était long de 795 bits.

$\Rightarrow$ il est recommandé de choisir *n >= 2 048 bits*

L'algorithme de Shor permet théoriquement aux ordinateurs quantiques de casser le RSA par la force brute, mais actuellement ces ordinateurs génèrent des erreurs aléatoires qui les rendent inefficaces.

Un gros caillou dans l'arithmétique

Pour régler la question des fondements, **Hilbert** conçoit un programme dont il établit les prémisses en 1900 dans l'introduction à sa célèbre liste de problèmes, le second problème étant celui de la cohérence de l'arithmétique.

En 1930, **Gödel** expose ses deux théorèmes d'incomplétude, qui seront publiés en 1931 et mettront fin aux espoirs fondés par Hilbert.

Théorie cohérente : on ne peut pas y démontrer à la fois un énoncé et son contraire

Théorie complète : tous les énoncés vrais sont démontrables

Les théorèmes d'incomplétude de Gödel

Définition : Une théorie récursivement axiomatisable est une théorie telle qu'on peut reconnaître de façon purement mécanique les axiomes parmi les énoncés du langage de la théorie. C'est le cas des théories utilisées pour formaliser tout ou partie des mathématiques usuelles, comme l'arithmétique de Peano ou la théorie des ensembles de Zermelo-Fraenkel.

Théorème 1 : Dans n'importe quelle théorie récursivement axiomatisable, cohérente et capable de « formaliser l'arithmétique », on peut construire un énoncé arithmétique qui ne peut être ni démontré ni réfuté dans cette théorie.

Théorème 2 : Si T est une théorie cohérente récursivement axiomatisable, cohérente et capable de « formaliser l'arithmétique », la cohérence de T, qui peut s'exprimer dans la théorie T, n'est pas démontrable dans T.

il faut un « niveau de complexité » minimum

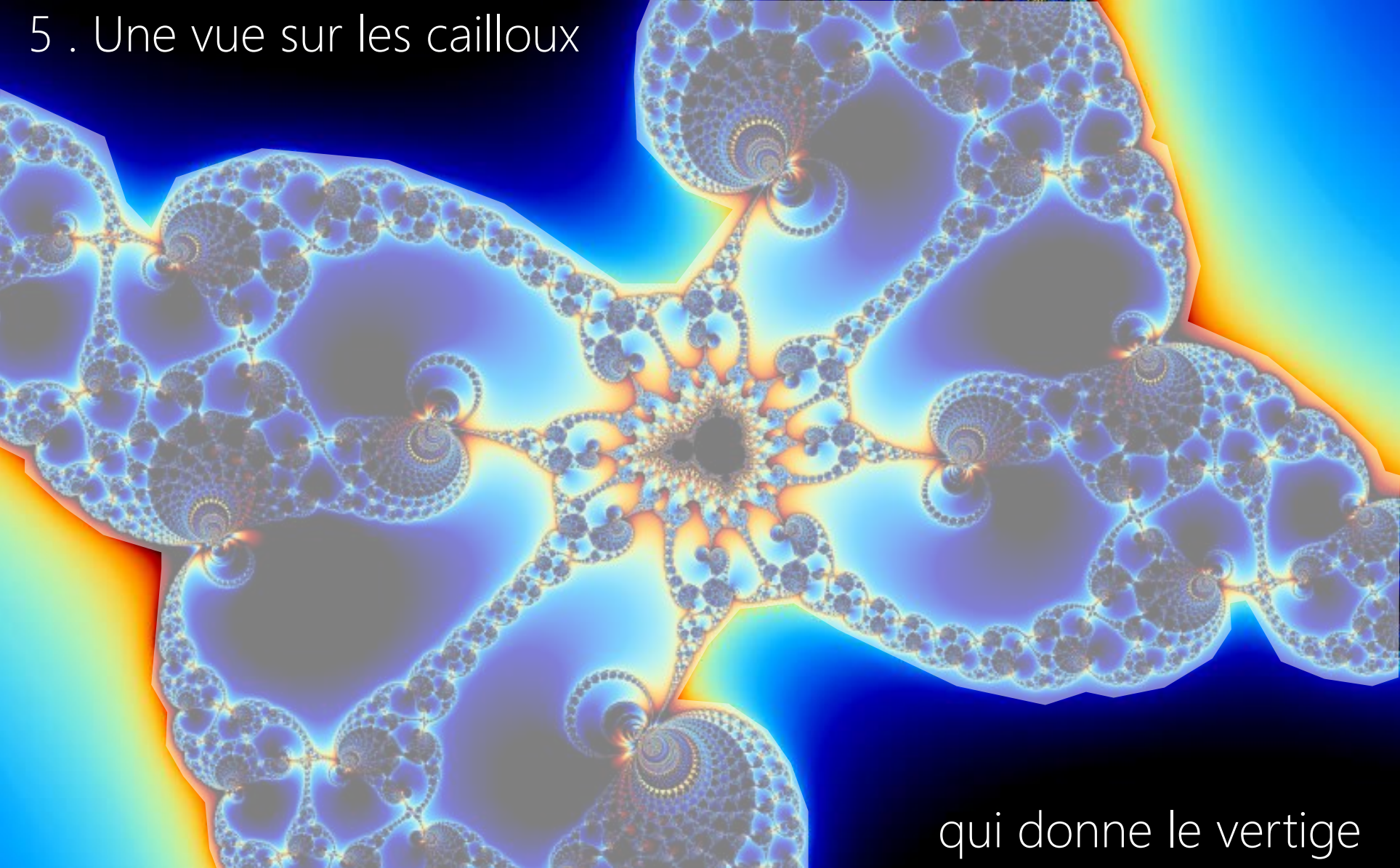
La démonstration de Gödel

https://scienceetonnante.com/2016/12/09/theoreme-godel/

G = « la proposition G n'est pas démontrable à partir des axiomes de la théorie »

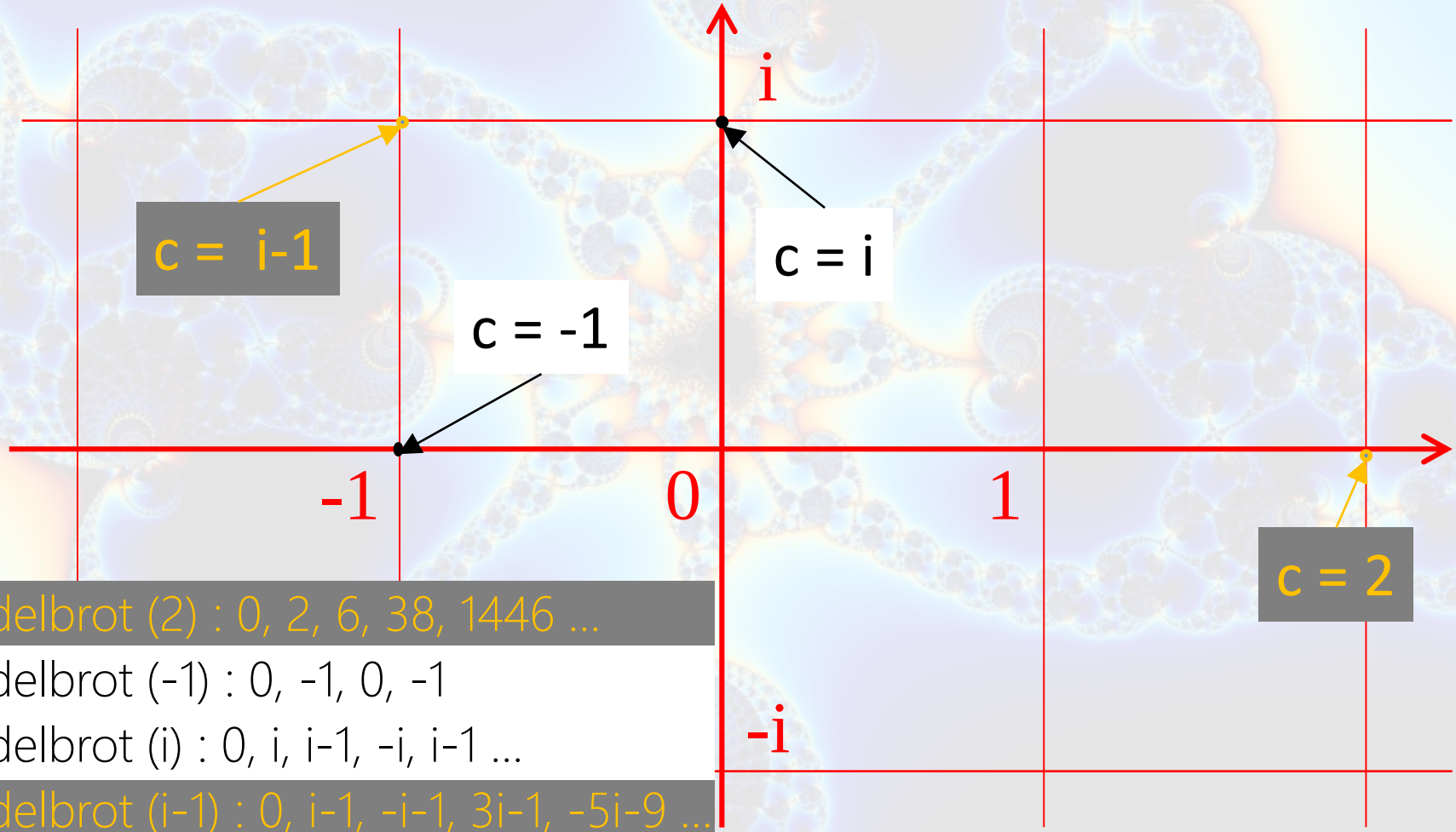
- Toute proposition mathématique peut s'écrire comme une suite finie de symboles, respectant certaines règles. Il est alors possible, par exemple en utilisant astucieusement les nombres premiers, de coder chaque proposition mathématique sous forme d'un **nombre**.
- Toute démonstration est une suite de formules, et peut également être codée par un nombre "codé de Gödel". La validité des étapes de la démonstration se traduit par le respect de certaines **propriétés arithmétiques sur ce nombre**. On peut alors construire la proposition purement arithmétique C(y) vraie si et seulement si la proposition codée par le nombre y est démontrable.
- Grâce à une astuce de diagonalisation, Gödel exhibe UNE proposition G, codée par le nombre de Gödel g, telle que C(g) soit la négation de G. Cela signifie que G est démontrable si et seulement si elle est fausse.

5 . Une vue sur les cailloux



qui donne le vertige

Mandelbrot (c) : $x_0 = 0$; $x_n = x_{n-1}^2 + c$



Mandelbrot (2) : 0, 2, 6, 38, 1446 ...

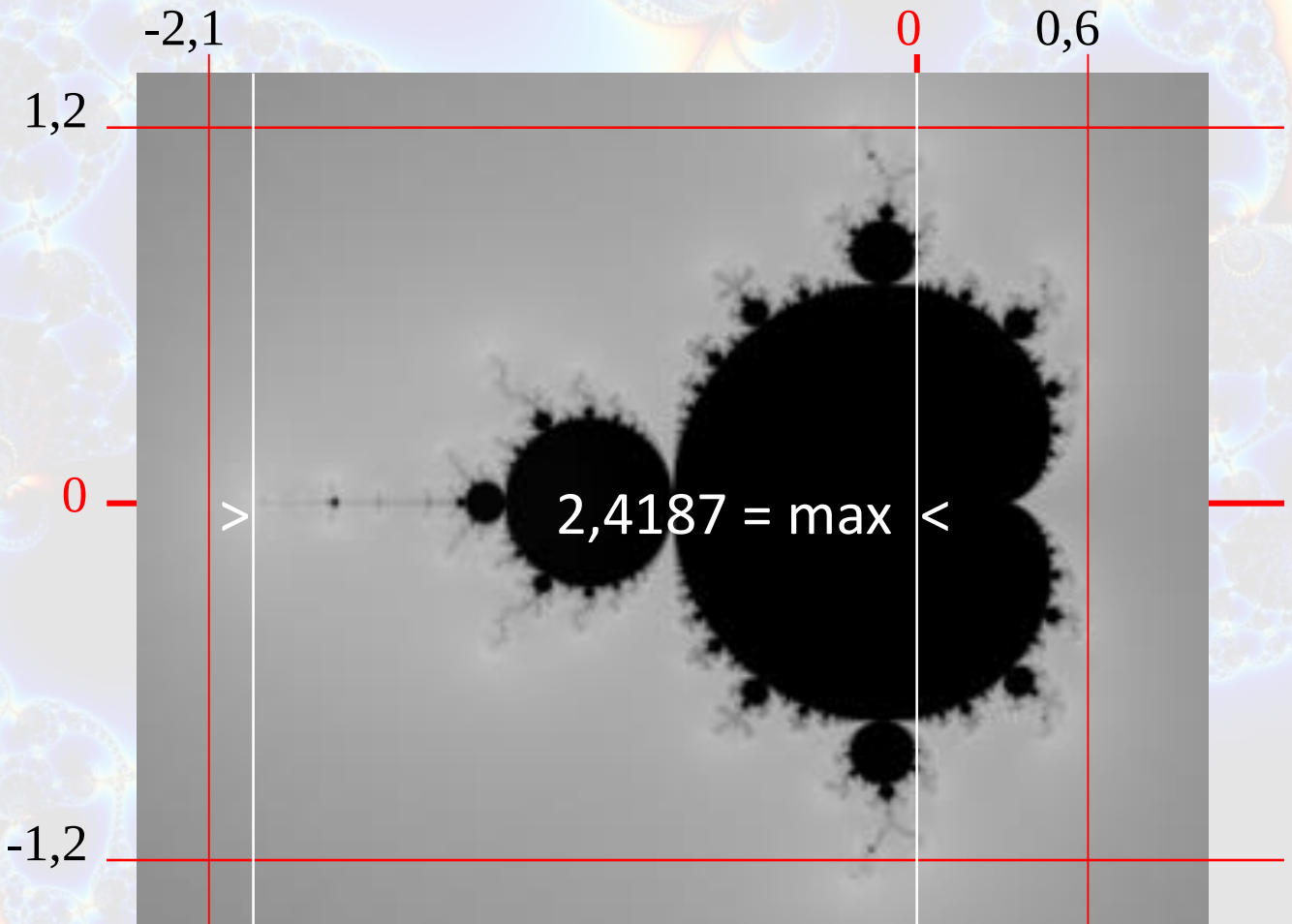
Mandelbrot (-1) : 0, -1, 0, -1

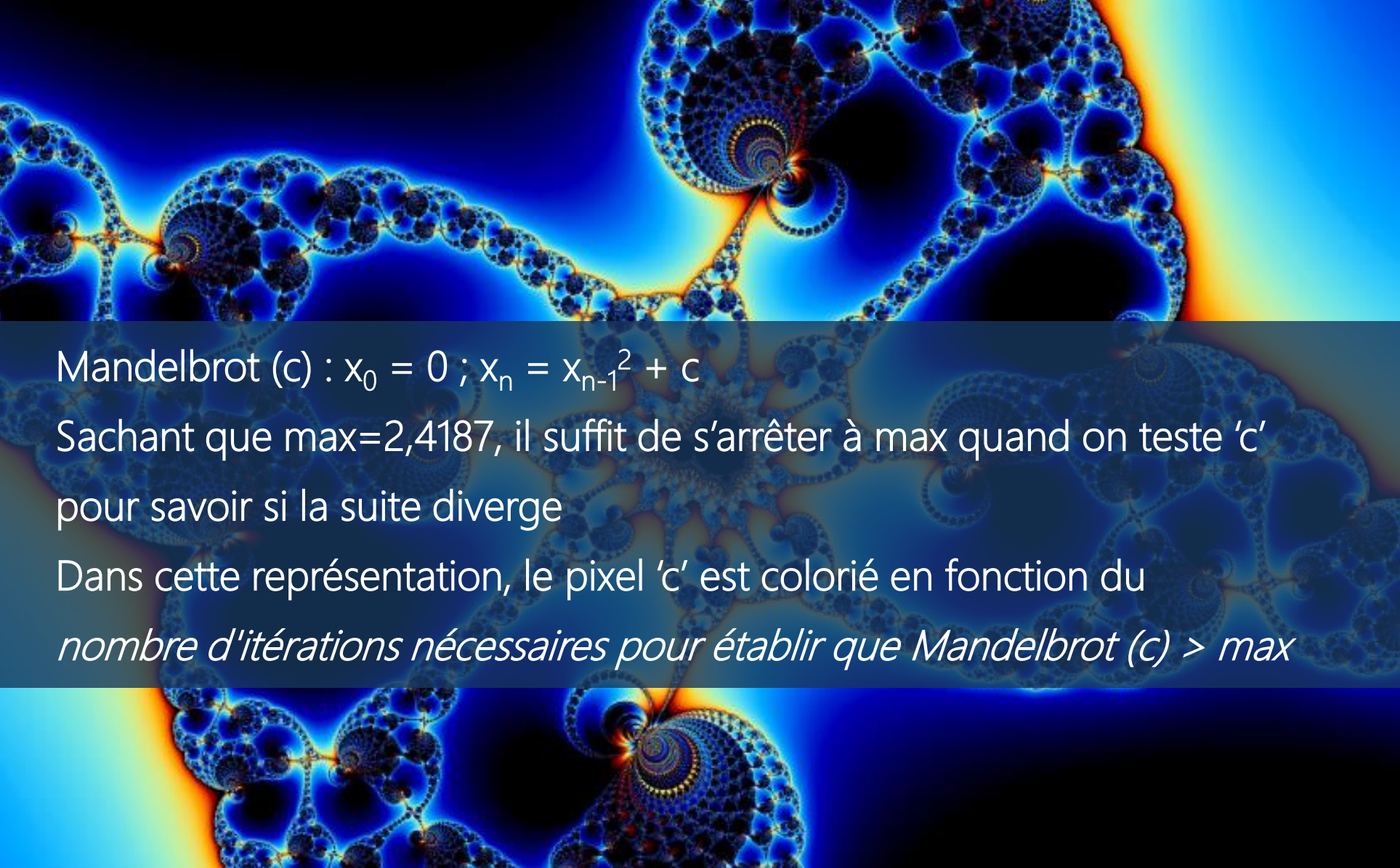
Mandelbrot (i) : 0, i, i-1, -i, i-1 ...

Mandelbrot (i-1) : 0, i-1, -i-1, 3i-1, -5i-9 ...

Mandelbrot (c) : $x_0 = 0$; $x_n = x_{n-1}^2 + c$

Les pixels '**c**' qui génèrent des suites bornées apparaissent en noir.



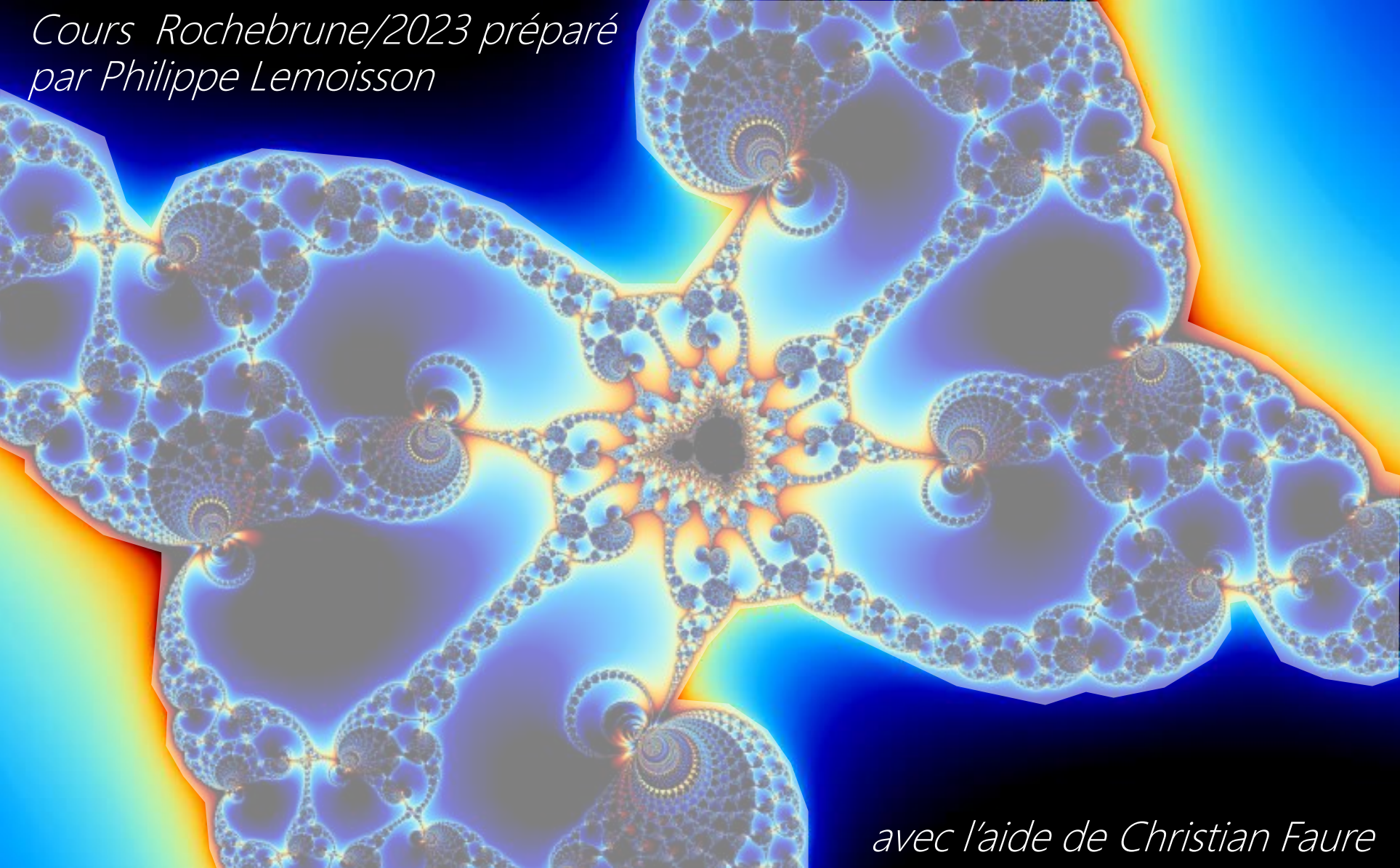


Mandelbrot (c) : $x_0 = 0$; $x_n = x_{n-1}^2 + c$

Sachant que max=2,4187, il suffit de s'arrêter à max quand on teste 'c' pour savoir si la suite diverge

Dans cette représentation, le pixel 'c' est colorié en fonction du *nombre d'itérations nécessaires pour établir que Mandelbrot (c) > max*

Cours Rochebrune/2023 préparé par Philippe Lemoisson



avec l'aide de Christian Faure