# PAPA MATHS

LIVRE 1

# ARITHMÉTIQUE DANS $\mathbb{Z}$

# CONGRUENCES ET DIVISIBILITÉ

# STRUCTURES ALGÉBRIQUES




Rémy Trotabas

Pour LAETICIA chérie.

*La physique, ce sont les règles que Dieu a inventées.*
*Les maths, ce sont les lois qu'il a dû suivre.*

*Jean-Pierre Serre*

**Version électronique 1.0**

ISBN 978-3-9824279-1-1

Site officiel : https://papamaths.org

© 2022-2026 Rémy Trotabas
Röttenbach – Bayern – Deutschland

Licence :
Creative Commons Attribution 4.0 International (CC BY-NC-ND 4.0)
– Pas d'utilisation commerciale
– Pas de modification

*La diffusion libre et gratuite auprès des élèves, étudiants, enseignants et clubs de mathématiques est encouragée.*

**Pourquoi ce livre ?**

La théorie des nombres est le sujet préféré des olympiades de maths, alors que complètement opaque sans introduction initiale.
Elle est l'ouverture de la partie la plus difficile du programme de Math Sup et demande du temps pour être assimilée. Elle est déconcertante à prime abord, mais les bases mathématiques sur lesquelles elle s'appuie sont connues dès la 4ème / 8 Klasse.
Une fois acquise la langue des modulos, s'ouvre un paysage d'une beauté certaine. On plane. Et ce sans substance illicite.

Je me suis alors lancé le défi d'enseigner ce chapitre de Math Sup à mon élève de 4ème préférée.
Pour ce faire j'ai analysé (au sens premier : réduit en particules élémentaires) et synthétisé cinq livres qui se distinguent tantôt par l'ennui absolu de leur approche, tantôt par la compacité insupportablement excessive des démonstrations - à se demander si certains souffrent d'une pénurie de papier ou si écrire les étapes intermédiaires serait une atteinte à leur gloire. Sans parler d'une mise en page qui semble particulièrement étudiée pour décupler le temps de compréhension.

Certains problèmes venant de livres en allemand ou en anglais, je ne les ai pas traduits. Comme ça on se familiarise avec l'expression mathématique dans ces langues – c'est le double effet kisscool.

# ARITHMÉTIQUE DANS $\mathbb{Z}$

# CONGRUENCES ET DIVISIBILITÉ

La théorie des nombres est une des formes les plus pures des mathématiques.
Les concepts à acquérir sont en quantité très finie : ils sont tous présentés dans les deux pages qui suivent.
Les stratégies quant à elles sont acquises par un travail **massif** de résolution d'exercices.

Sur le sujet de l'arithmétique dans $\mathbb{Z}$ ce chapitre couvre tout ce qu'il y a à connaitre pour résoudre les problèmes d'Olympiades de Mathématique, ainsi que tout le programme de Math Sup.

D'un point de vue historique, cela couvre les connaissances de l'humanité sur la théorie des nombres environ jusqu'à l'année 1800. L'extension naturelle de ce chapitre sera la théorie des groupes, anneaux et corps… qui nous mènera à 1900.

LA THÉORIE DES NOMBRES EN DEUX PAGES 3
QUELQUES DÉMONSTRATIONS 5
RÈGLES DE DIVISIBILITÉ 8
MÉTHODE POUR CALCULER UN RESTE À L'AIDE DE CONGRUENCES 10
PETIT THÉORÈME DE FERMAT 11
NOMBRES SPÉCIAUX 12
BASE 10, BASE B 13
PROPRIÉTÉS DES CARRÉS 13
ENTIER SOMME DE DEUX CARRÉS 14
ENTIER SOMME DE TROIS CARRÉS 15
ENTIER SOMME DE QUATRE CARRÉS 15
RESTES CHINOIS 16
ON VA PLUS LOIN ? 17
IDENTITÉS REMARQUABLES 18
MA BOITE À OUTILS 19
PROBLÈMES CLASSÉS 20
RESTE & DIVISIBILITÉ 20
NOMBRES PREMIERS 25
REPRÉSENTATION DES NOMBRES 27
RESTKLASSEN 28
CARRÉ OU PAS CARRÉ ? 29
EQUATIONS DIOPHANTIENNES 31
COEFFICIENTS DE BEZOUT 34
GESCHICHTE DER ZAHLENTHEORIE 35
GRAND THÉORÈME DE FERMAT 37
APPLICATIONS DANS LA VIE MODERNE 38

ENSEMBLES 43
FONCTIONS 44
NOMBRE DE SOUS-ENSEMBLES D'UN ENSEMBLE FINI 47
NOMBRE DE PARTIES A K ELEMENTS D'UN ENSEMBLE A N ELEMENTS 47
BINÔME DE NEWTON 49
RELATIONS 50
GROUPES 51
MORPHISME DE GROUPE 52
GROUPE CYCLIQUE 52
ANNEAUX 53
CORPS 54
ESPACES VECTORIELS – EXTENSIONS DE CORPS 55
GROUPES, ANNEAUX & CORPS 56
UN PEU D'HISTOIRE 58

# LA THÉORIE DES NOMBRES en deux pages

1. Étant donné deux entiers relatifs a et b, on dit que b **divise** a et on écrit **b | a** si $\exists$ k $\in \mathbb{Z}$ tel que a = k.b
   On dit que b est un **diviseur** de a, ou que a est un **multiple** de b. Nous avons $|a| \geq |b|$
   L'ensemble des diviseurs de a est noté $\mathcal{D}(a)$. *Exemple :* $\mathcal{D}(6)= \{1, 2, 3, 6\}$
   L'ensemble des multiples de b est $b\mathbb{Z} = \{bq ; q \in \mathbb{Z}\}$

2. Propriétés fondamentales de la divisibilité
   *Propriété 1* a, b $\in \mathbb{Z}$ $a|b, b|c \Rightarrow a|c$ *Exemple :* $2|6$ et $6|18 \Rightarrow 2|18$
   *Propriété 2* a, b, u, v $\in \mathbb{Z}$ $d|a, d|b \Rightarrow d|au+bv$ *En particulier :* d | a+b et d | a-b
   En français : si a et b sont des multiples de d, alors d divise a+b, d divise a-b, d divise au+bv

3. **Division euclidienne**
   Soit a $\in \mathbb{Z}$ et b $\in \mathbb{N}^*$. Il existe un unique couple (q, r) $\in \mathbb{Z}^2$ tel que a = b.q + r et $0 \leq r < b$
   q et r sont appelés respectivement **quotient** et **reste de la division euclidienne** de a par b
   *En particulier :* b | a *ssi* le reste (de la division euclidienne de a par b) est nul. *ssi* = si et seulement si

4. **PGCD** a,b $\in \mathbb{N}^*$
   PGCD (a,b) = Plus Grand Commun Diviseur positif de a et b = **$a \wedge b$**
   *ggT (a,b) = der größte gemeinsame Teiler* *gcd (a,b) = greatest common divisor*

**Propriétés**

$a \wedge b = b \wedge a-b$ → méthode simple mais lente pour calculer $a \wedge b$ $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(b)\cap\mathcal{D}(a-b)$

**$a = bq+r \Rightarrow a \wedge b = b \wedge r$** → **Algorithme d'Euclide** pour calculer $a \wedge b$ $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(b)\cap\mathcal{D}(r)$

$kc \wedge kb = k.(a \wedge b)$

$a \wedge 1 = 1$ $a \wedge a = a$ $a \wedge 0 = a$ $a \wedge b = b \wedge a$ $0 \wedge 0 = 0$ (convention)

5. Un entier positif est appelé **premier** si il a exactement 2 diviseurs positifs : 1 et lui-même (1 n'est pas premier)
   Si un entier est non premier, il est dit **composé.**
   a et b $\in \mathbb{Z}$ sont dits étrangers ou **premiers entre eux** (*coprime* en anglais) si $a \wedge b = 1$.
   Si $a \wedge b = 1$, tout diviseur de a est premier avec tout diviseur de b.
   a, b, c $\in \mathbb{Z}$. Si $a \wedge c = 1$ et $b \wedge c = 1$ alors $ab \wedge c = 1$
   *Un produit est premier avec un entier c ssi chacun des facteurs du produit est premier avec c.*
   a, b $\in \mathbb{Z}$. Si $a \wedge b = 1$ alors $\forall (m,n) \in \mathbb{N}^2$ $a^m \wedge b^n = 1$

**Forme irréductible** d'un nombre rationnel r $\in \mathbb{Q}$: $\exists$ un couple unique (u,v) $\in \mathbb{Z}$x $\mathbb{N}^*$ tel que $r = \frac{u}{v}$ et $u \wedge v = 1$

6. **Lemme de Bézout** *Etienne Bézout 1730-1783*
   Le PGCD de 2 entiers a et b peut être représenté comme une combinaison linéaire
   de a et b avec des coefficients entiers. $\forall$ a,b $\in \mathbb{Z}$, $\exists$ u,v $\in \mathbb{Z}$ : **$a \wedge b = a.u + b.v$**
   Un tel (u,v) est appelé couple de **coefficients de Bézout** de a et b. Il n'y a pas unicité d'un tel couple.
   En particulier si a et b sont premiers entre eux : pour (a,b) $\in \mathbb{Z}^2$ $a \wedge b = 1 \Leftrightarrow \exists$ (u,v) $\in \mathbb{Z}^2$, au + bv = 1
   Autre formulation : si $a \wedge b = 1$, alors l'équation au + bv = 1 a au moins une solution entière.

7. **Lemme d'Euclide** Si p est premier, $p|ab \Rightarrow p|a$ ou $p|b$ (ou non exclusif : p peut diviser a et b)
   **Lemme de Gauss** a, b, c $\in \mathbb{Z}$. Si a | bc et $a \wedge b = 1$, alors a | c
   Si a|c, b|c et $a \wedge b = 1 \Rightarrow ab|c$
   Un nombre premier divise un produit *ssi* il divise (au moins) l'un de ses facteurs.
   Attention ! Ce n'est pas vrai si le nombre n'est pas premier : 6 divise 2x3 mais ne divise ni 2, ni 3.



8. **PPCM** a,b $\in \mathbb{N}^*$
   PPCM (a,b) = Plus Petit Commun Multiple positif = **$a \vee b$**
   *kgV (a,b) = das kleinste gemeinsame Vielfache* *lcm (a,b) = least common multiple*
   $ac \vee bc = (a \vee b).c$

9. **Théorème fondamental de l'arithmétique**
**Tout entier positif peut être représenté comme un produit de nombres premiers - ses facteurs premiers.**
Cette décomposition est unique.

Soit (a,b) $\in \mathbb{N}^2$ $a = p_1^{\alpha_1}$ x $p_2^{\alpha_2}$ x … x $p_n^{\alpha_n}$ $b = p_1^{\beta_1}$ x $p_2^{\beta_2}$ x … x $p_n^{\beta_n}$

Les $\alpha_i$ sont les **valuations $p_i$-adique** de a Les $\beta_i$ sont les valuations $p_i$-adique de b

$a \wedge b = p_1^{\min(\alpha_1,\beta_1)}$ x $p_2^{\min(\alpha_2,\beta_2)}$ x … x $p_n^{\min(\alpha_n,\beta_n)}$ min (a,b) est le plus petit des nombres a et b

$a \vee b = p_1^{\max(\alpha_1,\beta_1)}$ x $p_2^{\max(\alpha_2,\beta_2)}$ x … x $p_n^{\max(\alpha_n,\beta_n)}$ max (a,b) est le plus grand des nombres a et b

10. **$(a \wedge b) . (a \vee b) = a.b$** Valuations p-adiques : $\forall i,j$ max(i,j) + min(i,j) = i+j

11. **Propriétés des nombres premiers** k entier, p premier

$\forall$ k $\in$ [1;p-1], k $\wedge$ p = 1 p est premier avec tous les nombres plus petits que lui, donc avec le produit de ces nombres : **(p-1)! $\wedge$ p = 1**

Il existe une infinité de nombres premiers.

On peut construire un intervalle de n'importe quelle taille ne contenant aucun nombre premier :
n!+2 *(divisible par 2)*, n!+3 *(divisible par 3)*, … , n!+n *(divisible par n)* sont (n-1) entiers consécutifs non premiers.

Le plus grand facteur premier d'un nombre non premier n est $\leq \sqrt{n}$
→ Pour que n <121 = $11^2$ soit premier, il suffit qu'il soit premier avec 2, 3, 5 et 7. Pas besoin de voir plus loin.

Tous les nombres premiers p>3 sont de la forme $6k \pm 1$

12. **CONGRUENCES**

**Définition**

On dit que a et b $\in \mathbb{Z}$ sont congrus modulo n ($n \in \mathbb{N}^*$) et l'on écrit a ≡ b [n] ou a ≡ b (mod n)
si et seulement si a et b ont le même reste dans la division euclidienne par n.

**Propriétés** Soient quatre entiers relatifs a, b, c, d

a ≡ b [n] si et seulement si n divise a−b
En particulier **a ≡ 0 [n] si et seulement si n divise a**.

**Si a ≡ b [n] et b ≡ c [n], alors a ≡ c [n]**

Démonstration :

**Si a ≡ b [n] alors a+c ≡ b+d [n]** a ≡ b [n] $\Rightarrow \exists \lambda \in \mathbb{Z}$ (b-a) = λn c ≡ d [n] $\Rightarrow \exists \mu \in \mathbb{Z}$ (d-c) = μ n

**et c ≡ d [n]** **a−c ≡ b−d [n]** (b+d) – (a+c) = (b-a) + (d-c) = (λ +μ) n ⇒ (a+c) ≡ (b+d) [n]

**ac ≡ bd [n]** bd-ac = (a+ λn)(c+ μn) – ac = (λc + μa + λμn)n ⇒ ac ≡ bd [n]

**Si a ≡ b [n], alors ka ≡ kb [n] pour tout entier relatif k**

**$a^m \equiv b^m$ [n] pour tout entier naturel m**

**f(a) ≡ f(b) [n] pour toute fonction polynomiale $f(x) = a_n x^n + … + a_1 x + a_0$ $a_i \in \mathbb{Z}$**

**a ≡ b [d] pour d divisant n**

**Attention ! On ne peut diviser que si c $\wedge$ n = 1, alors ca ≡ cb [n] ⇒ a ≡ b [n]**

13. Pour tout (a,b) $\in \mathbb{Z}^2$ et p premier on a **$(a+b)^p \equiv a^p + b^p$ [p]**

Démonstration : binôme de Newton $(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k . b^{p-k} + b^p$ *et* $\binom{p}{k} = p!/(k!.(p-k)!) \equiv 0\ [p]$ $\forall$ k $\in [1, p-1]$

14. **Petit théorème de Fermat - 1640** *Pierre de Fermat 1607 – 1665*

Pour n entier relatif et p premier **$n^p \equiv n$ [p]**

Si en plus n et p sont premiers entre eux **$n^{p-1} \equiv 1$ [p]**

15. **Théorème de Wilson** **p est premier *ssi* (p-1)! ≡ -1 [p]**

# QUELQUES DÉMONSTRATIONS

**PGCD de deux entiers naturels**

Soient a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs à a et b admet un plus grand élément D,
appelé plus grand commun diviseur. On note : D = pgcd(a, b) = a $\wedge$ b

*Démonstration de l'existence du PGCD*
Posons $\mathcal{D}(a)$ = {ensemble des diviseurs entiers naturels de a}
$\mathcal{D}$ (b) = {ensemble des diviseurs entiers naturels de b}

On peut faire 3 remarques :
- $\mathcal{D}(a) \cap \mathcal{D}(b) \neq \varnothing$ En effet : $1 \in \mathcal{D}(a) \cap \mathcal{D}(b)$
- $\mathcal{D}(a) \cap \mathcal{D}(b) \subset \mathbb{N}$
- $\mathcal{D}(a) \cap \mathcal{D}(b)$ est majoré par a.b

Donc $\mathcal{D}(a) \cap \mathcal{D}(b)$ possède un plus grand élément.

$\mathcal{D}(a) \cap \mathcal{D}(b)$ peut se noter $\mathcal{D}(a;b)$

**Propriétés**
Soient a et b deux entiers naturels non nuls. On pose d = a $\wedge$ b

| |
|---|
| $\mathcal{D}(a;b) = \mathcal{D}(a - b;b) = \mathcal{D}(a - kb;b)$, pour $k \in \mathbb{N}$ |
| Si $k \in \mathbb{N}$, $ka \wedge kb = k.(a \wedge b)$ |
| Si $k \in \mathbb{Z}$, $ka \wedge kb = \lvert k \rvert . (a \wedge b)$ |
| $n \wedge 0 = n$ |
| $\exists$ a' et b' $\in \mathbb{N}$ tels que a = da' b = db' a' $\wedge$ b' = 1 |

*Démonstration par double inclusion que $\mathcal{D}(a;b) = \mathcal{D}(a - kb;b)$*

$\subseteq$ : Soit $x \in \mathcal{D}(a;b)$, alors x|a et x|b D'où : x | a - kb , pour $k \in \mathbb{N}$
Donc $x \in \mathcal{D}(a - kb ; b)$

$\supseteq$ : Soit $x \in \mathcal{D}(a - kb ;b)$, alors x | a - kb et x | b D'où : x | a - kb + kb = a
Donc $x \in \mathcal{D}(a;b)$

Donc $\mathcal{D}(a;b) = \mathcal{D}(a - kb ; b)$
Les 2 ensembles étant identiques, le plus grand élément de chacun est le même :
a $\wedge$ b = (a - kb) $\wedge$ b, pour $k \in \mathbb{N}$

| |
|---|
| **Définition** On dit que a et b sont **premiers entre eux** ssi a $\wedge$ b = 1 |

**Relation de Bézout**

Soit a,b ∈ ℕ et soit D = a ∧ b
Alors il existe au moins un couple (u,v) ∈ $\mathbb{Z}^2$ tel que au + bv = D

***Démonstration***

Si a ou b sont nuls on a les cas triviaux :
- Si a = 0 alors D = 0 ∧ b = b : v = 1, u peut être n'importe quel entier
- Si b = 0 alors D = a ∧ 0 = a : u = 1, v peut être n'importe quel entier
- Si a = 0 et b = 0 alors D = 0 : u et v peuvent être n'importe quels entiers.

On considère par la suite a,b ∈ ℕ*

Pour a,b ∈ ℕ* donnés, on considère l'ensemble E = {n = a.u + b.v ∈ ℕ*, avec u,v ∈ ℤ}
E est l'ensemble des entiers positifs NON NULS pouvant s'écrire sous la forme au + bv.

E ≠ ∅ En prenant u = 1 et v = 0 : a.1 + b.0 = a donc a ∈ E.
E étant une partie non vide de ℕ, E possède un plus petit élément. Notons le d.
Par définition de E, il existe donc u,v ∈ ℤ tels que d = au + bv

**Montrons *(par double inégalité)* que d = D**

***Inégalité D ≤ d***
Comme D est le plus grand diviseur de a et b, D divise a. Il divise alors aussi a.u : ∃ k ∈ ℕ, a.u = k.D
Comme D est le plus grand diviseur de a et b, D divise b. Il divise alors aussi b.v : ∃ k' ∈ ℕ, b.v = k'.D
au + bv = k.D + k'D = (k + k')D donc D divise au+bv = d
Donc D | d
**Donc D ≤ d [1]**

***Inégalité d ≤ D***
Effectuons la division euclidienne de a par d : il existe (q,r) ∈ ℤ×ℕ, a = dq + r, avec 0 ≤ r < d

*Supposons que r ≠ 0*
r = a - dq = a - (a.u + b.v).q = a.(1 - u) + b.(- b)q ≥ 0 d'où : r ∈ E
r < d et d est le plus petit élément de E
Il y a contradiction. Donc r = 0

Donc a = dq Donc d | a

De même en effectuant la division euclidienne de b par d on obtient d | b
Donc d ∈ Ɗ(a;b)
Or D est le plus grand diviseur commun à a et b.
**Donc d ≤ D [2]**

De [1] et [2] on déduit D = d CQFD

**D'après la relation de Bézout, dans le cas particulier où a et b sont premiers entre eux, a ∧ b = 1**
**Alors il existe au moins un couple (u,v) ∈ $\mathbb{Z}^2$ tel que au + bv = 1**

**Théorème de Bézout**

a et b sont premiers entre eux ⇔ il existe (u,v) entiers relatifs tels que au + bv = 1

## Il existe une infinité de nombres premiers

Supposons qu'il n'existe qu'un nombre fini de nombres premiers $\{p_1, p_2, \dots, p_n\}$

Soit p le produit de ces nombres augmenté de 1, c'est-à-dire $p = p_1.p_2. \dots .p_n + 1$

Le reste de la division de p par $p_1$ est 1;
le reste de la division de p par $p_2$ est 1; ... ;
le reste de la division de p par $p_n$ est 1.
Puisque p n'est divisible par aucun nombre premier, p est premier.

Ce qui contredit l'hypothèse que la liste $\{p_1, p_2, \dots, p_n\}$ contient tous les nombres premiers.

*QED*

*Attention ! La proposition suivante est fausse :*
*Considérons la liste des n premiers nombres premiers $\{p_1, p_2, \dots, p_n\}$.*
*Alors $p = p_1.p_2. \dots .p_n + 1$, est un nombre premier.*

Voici un contre-exemple. Pour n = 6, la liste des nombres premiers est {2, 3, 5, 7, 11, 13} et le nombre $p = 2\times3\times5\times7\times11\times13 + 1 = 30031 = 59\times509$ n'est pas premier!

# RÈGLES DE DIVISIBILITÉ

**Teilbarkeit durch 3**

$10 \equiv 1$ [3] also gilt es $10^i \equiv 1^i \equiv 1$ [3] d.h. bei Division durch 3 läßt jede Zehnerpotenz den Rest 1.
Damit gilt auch:
$z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1.10 + a_0$
$z \equiv a_n \cdot 1 + a_{n-1} \cdot 1 + ... + a_0 \cdot 1$ [3]
$z \equiv a_n + a_{n-1} + ... + a_0$ [3]
$z \equiv Q(z)$ [3]
Also läßt z bei Division durch 3 denselben Rest wie die Quersumme von z.
Dies gilt insbesondere für den Rest 0, also die Teilbarkeit durch 3.
**Eine ganze Zahl ist durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist, d.h. $3|z \Leftrightarrow 3|Q(z)$**

**Règle de divisibilité par 9**

De même $10^i \equiv 1^i \equiv 1$ [9] et donc $z \equiv Q(z)$ [9]
D'où : *Un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9.*
*C'est la théorie derrière la **preuve par 9** : ab[9]=a[9] b[9] → Q(ab)=Q(a).Q(b)*

**Règle de divisibilité par 2 et 5**

$z = 10.b + a_0 = 2.5.b + a_0$ donc $z \equiv a_0$ [2] et $z \equiv a_0$ [5]
D'où : *Un nombre est divisible par 2 si son chiffre des unités est divisible par 2.*
*Un nombre est divisible par 5 si son chiffre des unités est divisible par 5.*

**Règle de divisibilité par 4**

$z = 100k + 10\,a_1 + a_0 \equiv 10\,a_1 + a_0$ [4] ou $\equiv 2\,a_1 + a_0$ [4]
*Un nombre est divisible par 4 si le nombre constitué de ses 2 derniers chiffres est divisible par 4.*

**Règle de divisibilité par 8**

$z = 1000k + 100\,a_2 + 10\,a_1 + a_0 \equiv 100a_2 + 10\,a_1 + a_0$ [8] ou $\equiv 4\,a_2 + 2\,a_1 + a_0$ [8]
*Un nombre est divisible par 8 si le nombre constitué de ses 3 derniers chiffres est divisible par 8.*

**Notations utiles - alternierende und nichtalternierende k-Quersummen**

On peut écrire tout entier z sous la forme d'une somme de puissances de 10 :

$$z = \sum_{i=0}^{n} a_i.10^i$$

**Quersumme Q(z)** ist die Summe aller Ziffern einer Zahl.

$$Q(z) = \sum_{i=0}^{n} a_i$$

**Alternierende Quersumme AQ(z)** erhält man, indem man bei einer Zahl, beginnend ganz rechts, die Ziffernwerte abwechselnd subtrahiert und addiert.

$$AQ(z) = \sum_{i=0}^{n} (-1)^i . a_i$$

**k-Quersumme $Q_k(z)$** ist die Summe der k -stelligen Zahlen, die rechts beginnend aus z gebildet werden
*Beispiel:* $Q_2(12\,345\,678) = 78 + 56 + 34 + 12$

$$Q_k(z) = \sum_{l=0}^{\frac{n}{k}-1} \sum_{i=0}^{k-1} 10^i . a_{i+kl} = \overline{a_{k-1} \dots a_1 a_0} + \overline{a_{2k-1} \dots a_k} + \cdots$$

**Alternierende k-Quersumme $AQ_k(z)$** wird analog zu $Q_k(z)$ gebildet, jedoch mit wechselnden Vorzeichen bei der Summierung der Zahlen, beginnend bei einem Plus bzgl. der am weitesten rechts stehenden Zahl.
*Beispiel:* $AQ_3(12\,345\,678) = 678 - 345 + 12$

$$AQ_k(z) = \sum_{l=0}^{\frac{n}{k}-1} (-1)^l \sum_{i=0}^{k-1} 10^i . a_{i+kl} = \overline{a_{k-1} \dots a_1 a_0} - \overline{a_{2k-1} \dots a_k} + \cdots$$

## Teilbarkeit - Nutzung alternierender und nichtalternierender k-Quersummen

$$z = \sum_{i=0}^{n} a_i . 10^i$$

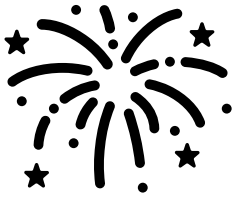


***Wir teilen die Monomen von z in k-er Gruppen. Es gilt folgende Schreibweise:***

$$z = \sum_{l=0}^{\frac{n}{k}-1} (10)^{k.l} . \sum_{i=0}^{k-1} 10^i . a_{i+kl}$$

***Nehmen wir an, es gelte m.x = $10^k$ - 1*** dann folgt $10^k$ -1 ≡ 0 [x] und $10^k$ ≡ 1 [x]

$$z \equiv \sum_{l=0}^{\frac{n}{k}-1} (1)^{l} . \sum_{i=0}^{k-1} 10^i . a_{i+kl} \ [x]$$



$$z \equiv \sum_{l=0}^{\frac{n}{k}-1} \sum_{i=0}^{k-1} 10^i . a_{i+kl} \ [x] = \ Q_k(z) \ [x]$$

Verbal ausgedrückt:

- Eine Zahl z ist genau dann durch x teilbar, wenn die nichtalternierende k-Quersumme durch x teilbar ist und es eine Zahl m gibt, für die m.x = $10^k$ −1 gilt ODER
- Für alle **Teiler von $10^k$–1** ist die k-Quersumme ein Teilbarkeitskriterium.

*k=2 : für alle Teiler von 99, also*
**für 3, 9, 11, 33 und 99, ist die 2er-Quersumme ein Teilbarkeitskriterium.**

*k=3 : für alle Teiler von 999, also*
**für 3, 9, 27, 37, 111, 333 und 999, ist die 3er-Quersumme ein Teilbarkeitskriterium**

***Nehmen wir an, es gelte m.x = $10^k$ + 1*** dann folgt $10^k$ +1 ≡ 0 [x] und $10^k$ ≡ -1 [x]

$$z \equiv \sum_{l=0}^{\frac{n}{k}-1} (-1)^{l} . \sum_{i=0}^{k-1} 10^i . a_{i+kl} \ [x] = \ AQ_k(z) \ [x]$$

Verbal ausgedrückt:

- Eine Zahl z genau dann durch x teilbar ist, wenn die alternierende k-Quersumme durch x teilbar ist und es eine Zahl m gibt, für die m.x = $10^k$ +1 gilt ODER
- Für alle **Teiler von $10^k$+1** ist die alternierende k-Quersumme ein Teilbarkeitskriterium.

*k=1 Teilbarkeit durch 11*
**z ist durch 11 teilbar, wenn die alternierende Quersumme $AQ_1(z)$ durch 11 teilbar ist.**

*k=2 Teilbarkeit durch 101*
**z ist durch 101 teilbar, wenn die alternierende 2er-Quersumme $AQ_2(z)$ durch 101 teilbar ist.**

*k=3 Teilbarkeit durch 7, 11, 13, 1001* **1001 = 7 . 11 . 13. (nombre remarquable)**
**z ist durch 7, 11 bzw. 13 teilbar, wenn die alternierende 3er-Quersumme $AQ_3(z)$ durch 7, 11 bzw. 13 teilbar ist.**

## Perioden der gewichteten Quersummen

Untersuchungen bzgl. Rest 7
Wir betrachten die Reste der 10-er Potenzen bei der Division durch 7.
1 ≡ 1 [7] 10 ≡ 3 [7] 100 ≡ 2 [7]
1000 ≡ −1 [7] 10000 ≡ −3 [7] 100000 ≡ −2 [7]
1000000 ≡ 1 [7] Nun wiederholen sich die Reste.
**$z \equiv a_0 + 3\,a_1 + 2\,a_2 - a_4 - 3a_5 - 2\,a_6 + a_7 + \ldots$ [7]**

# MÉTHODE POUR CALCULER UN RESTE À L'AIDE DE CONGRUENCES

On cherche à déterminer le **reste de la division euclidienne** d'un très grand entier par un autre très grand entier. Les nombres sont trop grands pour un ordinateur ☹, mais on peut résoudre en utilisant les congruences ☺.

Pour trouver le reste de la division de $a^b$ par n on remplace a et b par 2 entiers plus petits u et v tels que $a^b \equiv u^v[n]$

1. On remplace a par son reste u par la division par n : **$a \equiv u\ [n]$** $\Rightarrow a^b \equiv u^b\ [n]$
2. On calcule les puissances successives de u ($u, u^2, u^3, \ldots$) en cherchant le premier entier k tel que $u^k \equiv 1[n]$

(un tel entier existe si u et n sont premiers entre eux; l'exemple 2 traite des autres cas)

On effectue la division euclidienne de b par k : $b=kq+v$ **$b \equiv v\ [k]$**

on obtient : $u^b = u^{kq+v} = u^{kq} \times u^v = [u^k]^q \times u^v$

$u^b \equiv [u^k]^q \times u^v \equiv 1^q \times u^v \equiv u^v\ [n]$

3. On peut conclure : **$a^b \equiv u^b \equiv u^v\ [n]$**

Donc $a^b$ et $u^v$ ont le même reste dans la division par n. Ce reste est facile à calculer car u et v sont "petits".

**Exemple 1 : Quel est le reste de la division euclidienne de $12345^{2000}$ par 7 ?** ★★☆

1. On effectue la division euclidienne de 12345 par 7. Le quotient est 1763 et le reste est 4.

Donc $12345 \equiv 4\ [7]$ et $12345^{2000} \equiv 4^{2000}\ [7]$

2. $4^2 = 16 \equiv 2\ [7]$ Inutilisable, on continue: $4^3 = 64 \equiv 1\ [7]$ Parfait : k=3.

On effectue la division euclidienne de 2000 par 3 : $2000 = 666 \times 3 + 2$

$4^{2000} = 4^{666\times3+2} = (4^3)^{666} \times 4^2 \equiv 1^{666} \times 4^2 \equiv 16\ [7] \equiv 2\ [7]$

*Le reste de la division euclidienne de $12345^{2000}$ par 7 est donc 2.*

**Exemple 2 : Quel est le reste de la division euclidienne de $12344^{2000}$ par 6 ?**

1. On effectue la division euclidienne de 12344 par 6. Le quotient est 2057 et le reste est 2.

Donc $12344 \equiv 2\ [6]$ et $12344^{2000} \equiv 2^{2000}\ [6]$

2. $2^2 \equiv 4\ [6]$ $2^3 = 8 \equiv 2\ [6]$ $2^4 = 16 \equiv 4\ [6]$ etc…

Ici on ne peut pas trouver d'entier k tel que $2^k \equiv 1[6]$ mais on remarque que $2^k \equiv 2[6]$ si k est impair et $2^k \equiv 4[6]$ si k est pair (cette propriété se démontre facilement par récurrence – sa généralisation ci-dessous).

Donc $2^{2000} \equiv 4[6]$

*Le reste de la division euclidienne de $12344^{2000}$ par 6 est donc 4.*

**Montrons que pour $a \in \mathbb{Z}$, n entier > 2 et $a \wedge n = 1$ $\forall k \in \mathbb{N}$ les $r_k$ tels que $a^k \equiv r_k\ [n]$ sont périodiques**

$r_k$ ne peut prendre que une quantité limitée de valeurs : 0 à n-1

Il existe $k1 < k2$ tels que $r_{k1} = r_{k2} = r$

Posons $T = k2 - k1$ et montrons que $(r_k)\ k \in \mathbb{N}$ est T-périodique i.e. $a^{k+T}\ [n] = a^k\ [n]$

On a $a^k \equiv r\ [n]$ et $a^{k+T} \equiv r\ [n]$

(A) $a^k - r \equiv 0\ [n]$

$a^T a^k - r \equiv 0\ [n]$

$a^T a^k - r - r a^T + r a^T \equiv 0\ [n]$

$a^T (a^k - r) - r (1 - a^T) \equiv 0\ [n]$

(A) donc $0 - r (1 - a^T) \equiv 0\ [n]$

$r (a^T - 1) \equiv 0\ [n]$ (B)

or $a \wedge n = 1 \rightarrow a^k \wedge n = 1$ donc $a^k\ [n] \wedge n = 1$ c.-à-d. $r \wedge n = 1$

et donc d'après le Lemme de Gauss on peut affirmer que des deux facteurs dans B c'est $(a^T - 1) \equiv 0\ [n]$

$a^T \equiv 1\ [n]$

Donc $a^{k+T} = a^k a^T \equiv a^k . 1\ [n] \equiv a^k\ [n]$

Donc $\forall n \in \mathbb{N}$ $a^{k+T}$ et $a^k$ ont le même reste : $(r_k)\ k \in \mathbb{N}$ est T-périodique.

# PETIT THÉORÈME DE FERMAT

**PTF** - énoncé par Pierre de Fermat en 1640, prouvé par Leonhard Euler en 1736



**Pour p premier $n^p \equiv n$ [p]**

***ou***

**Pour p premier ne divisant pas n $n^{p-1} \equiv 1$ [p]**

**Preuve 1 – par récurrence**

- Pour n =1 $n^{1-1} = n^0 \equiv 1$ [p]
- Si $n^p - n \equiv 0$ [p] alors $(n+1)^p - (n+1) = n^p + \sum_{i=1}^{p-1}\binom{p}{i} n^{p-i} + 1 - (n+1) = n^p - n + \sum_{i=1}^{p-1}\binom{p}{i} n^{p-i}$

**Comme** $p|\binom{p}{i}$ pour 0<i<p **et** $p|n^p - n$ **on a** : $p|(n+1)^p - (n+1)$

**Preuve 2 – par les congruences**

On considère les ensembles de nombres E = {n, 2n, 3n, … , (p-1).n} E possède (p-1) éléments
F = { 1, 2, 3, … , p-1} F possède (p-1) éléments

Si $i \wedge p = 1$ et $n \wedge p = 1$ alors $i.n \wedge p = 1$ *(voir Théorie des Nombres § 5)*
Les éléments de E qui s'écrivent tous sous la forme i.n sont donc tous premiers avec p.
Selon le principe des tiroirs, chaque élément de E est congru modulo p à exactement un élément de F.
Alors le produit de tous les membres de E est congru modulo p au produit de tous les membres de F :
n.2n. … .(p-1)n ≡ 1.2. .(p-1) [p]
Par ailleurs n.2n. … .(p-1)n = $n^{p-1}$.1.2. … .(p-1) = $n^{p-1}$.(p-1)! et 1.2. .(p-1) = (p-1)! [p]
Donc $n^{p-1}$.(p-1)! ≡ (p-1)! [p]
Comme $(p-1)! \wedge p = 1$ *(voir TN § 11)* on peut simplifier par (p-1)! *(voir TN § 12)* et on obtient $n^{p-1} \equiv 1$ [p] □

**Preuve 3 – par les dénombrements**

On a des perles de n couleurs différentes. On prépare un collier en enfilant p perles (p premier).
On a alors $n^p$ possibilités différentes d'enfiler les perles.
On ne considère pas les colliers dont toutes les perles ont la même couleur. Comme on a n couleurs, il y en a n.
Il reste $n^p - n$ possibilités d'enfiler les perles.
On ferme le collier de façon à ne pas voir le nœud.
Des colliers qui ne diffèrent que par une permutation cyclique ne sont pas distinguables.
*(Pour p premier ?) Il y a p permutations cycliques de p perles.*
Le nombre de colliers non distinguables est donc $(n^p - n)/p$ ; qui est nécessairement un nombre entier puisque c'est un dénombrement de colliers. p est donc un diviseur de $n^p - n$, ce qui s'écrit $n^p \equiv n$ [p]

**L'inverse du théorème de Fermat n'est pas vrai.**

**Quel est le reste de la division de $2^{40}$ par 37 ?**
$2^{40} = 2^{36}.2^4 \equiv 1.2^4$ [37] (PTF)
$2^{40} = 16$ [37]

**Quel est le reste de la division de $2^{70}$ par 37 ?**
$2^{70} = 2^{36}.2^{34} \equiv 1.2^{34}$ [37] (PTF)
$2^8 = 256 \equiv 34 \equiv -3$ [37] donc $2^{34} = 4(2^8)^4 \equiv 4(-3)^4 \equiv 28$ [37]
$2^{70} \equiv 28$ [37] *Il ne faut pas hésiter à brutaliser si nécessaire …*

## Divisibilité de $n^k - n$

**$n^5 - n$ est divisible par 30** On utilise le PTF en cascade pour p=2 : $n^2 \equiv n$ [2]
$n^5 = n(n^2)^2 \equiv n(n^2) \equiv n.n = n^2 \equiv n$ [2] → $n^5$-n est divisible par 2

On utilise le PTF en cascade pour p=3 : $n^3 \equiv n$ [3]
$n^5 = n^2.n^3 \equiv n^2.n \equiv n^3 \equiv n$ [3] → $n^5$-n est divisible par 3

PTF pour p=5 : $n^5 \equiv n$ [5] → $n^5$-n est divisible par 5

**$n^7 - n$ est divisible par 42** On utilise le PTF en cascade pour p=2 : $n^2 \equiv n$ [2]
$n^7 = n(n^2)^3 \equiv n(n)^3 = (n^2)^2 \equiv n^2 \equiv n$ [2] → $n^7$-n est divisible par 2

On utilise le PTF en cascade pour p=3 : $n^3 \equiv n$ [3]
$n^7 = n(n^2)^3 \equiv n.n^2 = n^3 \equiv n$ [3] → $n^7$-n est divisible par 3

On utilise le PTF en cascade pour p=5 : $n^3 \equiv n$ [3]
$n^7 = n^2.n^5 \equiv n^2.n = n^3$ [5]. *marche pas*→ $n^5$-n n'est **pas** divisible par 5

PTF pour p=7 : $n^7 \equiv n$ [7] → $n^7$-n est divisible par 7

*De même :* $n^{11}$ - n est divisible par 2.3.11=66 $n^{13}$ - n est divisible par 2.3.5.7.13=2730 …

# NOMBRES SPÉCIAUX

On a donné à certains nombres des noms spéciaux.
Démystifions ça tout de suite.

### Nombres de Mersenne $M_n = 2^n - 1$

***Père Marin Mersenne 1588-1648***

Correspond avec Fermat, Descartes, Huygens, Hobbes, le père de Pascal
Traité d'acoustique : rapport des fréquences des notes de la gamme, mesure la vitesse du son (1636)
Crée un foyer de réflexion qui donnera naissance à l'Académie des Sciences en 1666

- Si on connait un nombre de Mersenne premier $M_n = 2^n - 1$ alors on connait un nombre parfait plus grand : $2^{n-1}(2^n - 1)$
- **Si un nombre de Mersenne $M_n = 2^n - 1$ est premier alors n est premier.**

Soit d un diviseur de n alors il existe $k \in \mathbb{N}$ tel que $n = kd$ et
$2^{kd} - 1 = (2^d)^k - 1 = (2^d - 1)(1 + 2^d + 2^{2d} + \dots + 2^{(k-1)d})$
$2^d - 1$ divise donc $2^n - 1$ donc $d = 1$ ou $d = n$ c.-à-d. n est premier.

- La réciproque est fausse.

Pour n = 11, $2^{11} - 1 = 2047 = 23 \times 89$

- Si p est composé alors $M_p$ est composé.
- $N = a^n - 1$ n'est premier que si a=2 et n est premier – c'est justement un nombre de Mersenne.

Liste des nombres de Mersenne : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 257, 521

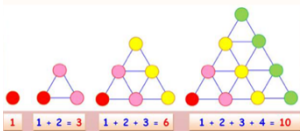
**Pour $m \in \mathbb{N}$ tel que $2^m + 1$ soit premier, montrer que m est de la forme $2^n$, $n \in \mathbb{N}$**

### Nombres de Fermat $Fn = 2^{2^n} + 1$

Fermat pensait que tous ces nombres sont premiers. En fait seulement $F_0$ à $F_4$ sont premiers, tous les autres non.
$F_0 = 3$ $F_1 = 5$ $F_2 = 17$ $F_3 = 257$ $F_4 = 65537$
Mais F5 = 4 294 967 297 = 641 x 6 700 417
*Un polygone régulier ne peut être dessiné à la règle (non graduée) et au compas que si il a un nombre de cotés égal à un nombre de Fermat premier (ou une combinaison linéaire de ceux-ci et/ou $x2^k$)*
Relation entre 2 voisins $F_{n+1} = (F_n - 1)^2 + 1$
Relation avec tous les précédents $F_n = F_0F_1F_2\dots F_{n-1} + 2$

### Nombres géométriques : triangulaires, carrés, pentagonaux…

Les nombres triangulaires sont de la forme somme des entiers de 1 à n = n(n+1)/2




| n | Triangulaires | Carrés | Pentagonaux | Hexagonaux |
|---|---|---|---|---|
| 1 | 1 = 1 | 1 = 1 | 1 = 1 | 1 = 1 |
| 2 | 1+2 = 3 | 1+3 = 4 | 1+4 = 5 | 1+5 = 6 |
| 3 | 1+2+3 = 6 | 1+3+5 = 9 | 1+4+7 = 12 | 1+5+9 = 15 |
| 4 | 1+2+3+4 = 10 | 1+3+5+7 = 16 | 1+4+7+10 = 22 | 1+5+9+13 = 28 |
| 5 | 1+2+3+4+5 = 15 | 1+3+5+7+9 = 25 | 1+4+7+10+13 = 35 | 1+5+9+13+17 = 45 |

| | |
|---|---|
| Triangulaires | $P_{3,n} = \frac{n^2 + n}{2} = \frac{1}{2}n(n+1)$ |
| Carrés | $P_{4,n} = \frac{2n^2}{2} = n^2$ |
| Pentagonaux | $P_{5,n} = \frac{3n^2 - n}{2} = \frac{1}{2}n(3n-1)$ |
| Hexagonaux | $P_{6,n} = \frac{4n^2 - 2n}{2} = 2n(n-1)$ |
| Heptagonaux | $P_{7,n} = \frac{5n^2 - 3n}{2}$ |
| **(k + 2)-gonaux** | $P_{k+2,n} = \frac{kn^2 - (k-2)n}{2}$ |
| **k-gonaux** | $P_{k,n} = \frac{(k-2)n^2 - (k-4)n}{2}$ |

# BASE 10, BASE B

Tout nombre entier naturel N s'écrit de manière **unique** comme :

- somme de puissances de 10 en base 10, c.-à-d. pour les nombres décimaux.
**$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 . 10 + a_0$**

- somme de puissances de B pour toute **base B**
**$N = b_n \cdot B^n + b_{n-1} \cdot B^{n-1} + \ldots + b_1 . B + b_0$**
N est unique.
Les coefficients $a_i$ sont compris entre 0 et B-1. Les $a_i$ sont les restes de la division euclidienne de N par B, puis les restes des divisions successives des quotients par B jusqu'à ce que le quotient soit nul.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 987 /10 | = 98 reste 7 | $a_0 = 7$ | 987 / 8 | = 123 reste 3 | $a_0 = 3$ | 987 / 16 = 61 reste 11 | $a_0 = B$ |
| 98 / 10 | = 9 reste 8 | $a_1 = 8$ | 123 / 8 | = 15 reste 3 | $a_1 = 3$ | 61 / 16 = 3 reste 13 | $a_1 = D$ |
| 9 / 10 | = 0 reste 9 | $a_2 = 9$ | 15 / 8 | = 1 reste 7 | $a_2 = 7$ | 3/16 = 0 reste 3 | $a_2 = 3$ |
| | | | 1 / 8 | = 0 reste 1 | $a_3 = 1$ | | |

987 s'écrit 987 en base 10 (pas de grosse surprise)
1733 en base 8
3DB en base 16.

# PROPRIÉTÉS DES CARRÉS

Si $n = a^2$ alors $n = p_1^{2\alpha_1} \times p_2^{2\alpha_2} \times \ldots \times p_n^{2\alpha_n}$

→ **Dans la décomposition en facteurs premiers d'un carré, tous les exposants sont pairs.**

Autrement dit - un nombre carré n'est jamais le produit de 2 nombres premiers distincts
- si le produit de deux entiers premiers entre eux est un carré, chacun d'eux est un carré

- Un carré est la somme de deux nombres triangulaire successifs.
- Le carré de n est égal au produit des 2 nombres qui l'encadrent plus 1 : $n^2 = (n+1)(n-1) + 1$
- Le carré de n est égal à la somme des nombres impairs de 1 à n
- **Tous les carrés sont de la forme 3k ou 3k+1 mais jamais 3k+2**

Tout nombre peut s'écrire $n=3q+r$ avec $r = \{0, 1, 2\}$
$n^2 = 9q^2 + 6qr + r^2$ avec $r^2 = \{0, 1, 4\} \equiv \{0, 1\}$ [3]

Si n est impair alors $n = 2k+1$ et $n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$
Comme k et k+1 sont consécutifs, l'un d'eux est pair. Alors $4.k(k+1) \equiv 0$ [8] et $n^2 \equiv 1$ [8]

**Le carré d'un nombre impair est ≡ 1 [8]**
**Il s'écrit sous la forme 8k+1**

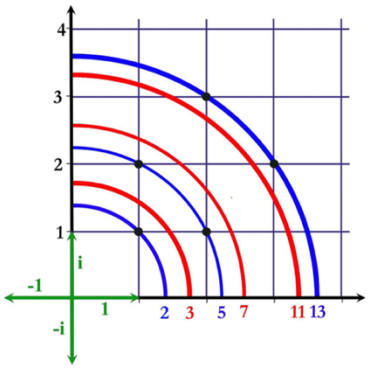
**Le carré d'un nombre pair est ≡ 0 [4]**
**Il s'écrit sous la forme 4k**

# ENTIER SOMME DE DEUX CARRÉS

Un **carré** somme de deux carrés est un triplet de Pythagore : $c^2 = a^2 + b^2$ $\quad 3^2 + 4^2 = 5^2$
Ils vérifient tous a.b.c ≡ 0 [60] $\quad$ Il y en a une infinité.

**La question plus générale : quel sont les nombres n qui sont une somme de deux carrés ($n = a^2 + b^2$) ?**
**Autrement dit : on cherche à caractériser l'ensemble $\Sigma = \{n \in \mathbb{N} / n = a^2 + b^2 ; a,b \in \mathbb{N}\}$**

**Analogie :**
Trouver si un nombre est somme de deux carrés,
c'est chercher si il existe un point de coordonnées entières
sur le cercle de rayon $\sqrt{n}$




**Attention : on accepte a = 0 ou b = 0**

**Théorème des deux carrés de Fermat - nombres premiers**
**Un nombre premier est somme de 2 carrés *ssi* il est de la forme 4n+1 i.e. ≡ 1 [4]**
Cette somme quand elle existe est toujours unique.

**Théorème des deux carrés de Fermat - nombres quelconques**
**Un entier est somme de 2 carrés *ssi* chacun de ses facteurs premiers ≡ 3 [4] est à une puissance paire.**
Cette somme est unique si aucun facteur n'est ≡ 1 [4] ou alors s'il n'y en a que 1 et qu'il est puissance 1.

Si a est pair alors a = 2k et $a^2 = 4k^2 \equiv 0$ [4]
Si a est impair alors a = 2k+1 et $a^2 = 4k^2 + 4k + 1 \equiv 1$ [4]
Donc quels que soient a et b, $a^2 + b^2 \equiv 0$ [4] ou ≡ 1 [4] ou ≡ 2 [4] mais jamais ≡ 3 [4]
**→ Si n ≡ 3 [4] alors n ne peut pas être la somme de deux carrés ($n \notin \Sigma$)**
**→ Tous les nombres impairs qui sont somme de deux carrés sont ≡ 1 [4] donc de la forme 4k+1**

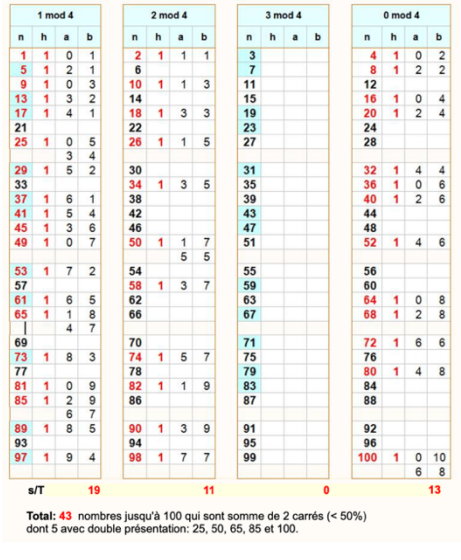
Tout entier positif peut être représenté de façon unique sous sa **forme canonique**, c'est-à-dire comme un produit de ses facteurs premiers : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n}$

$$n = \prod_{i=1}^{n} p_i^{\alpha_i}$$

Les nombres premiers étant… premiers, à part 2, tous les autres sont impairs.
Donc soit $p_i = 2$ soit $p_i \equiv \{1,3\}$ [4] $\quad$ On peut alors transformer la forme canonique sous la forme suivante :

$$n = 2^{\alpha} . \prod_{p_i \equiv 1[4]} p_i^{\beta_i} . \prod_{p_i \equiv 3[4]} p_i^{\gamma_i}$$

**Un nombre est somme de deux carrés *ssi* tous les $\gamma_i$ sont pairs**




Une autre notation avec les valuations p-adiques :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

**$n \in \Sigma \Leftrightarrow v_p(n)$ est pair quand $p \equiv 3$ [4]**

**Produit de deux nombres somme de deux carrés**
Le produit de deux nombres somme de deux carrés est aussi une somme de deux carrés
$n = a^2 + b^2$ $m = c^2 + d^2$ $n.m = \mathbf{(a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2}$ ***Identité de Lagrange***

**Équation diophantienne** $\mathbf{a^2 + 2b^2 = n}$ (n>2 pour éviter les cas triviaux)

**On cherche à caractériser l'ensemble $\Sigma = \{n \in \mathbb{N} / n = a^2 + 2b^2 ; a,b \in \mathbb{N}\}$**

**Pour p premier, $p \in \Sigma \Leftrightarrow p \equiv 1$ ou 3 [8]**

**Pour n entier, $n \in \Sigma \Leftrightarrow v_p(n)$ est pair quand $p \equiv -1$ ou -3 [8]**

Démonstration : une fois qu'on aura vu les anneaux et les complexes.

# ENTIER SOMME DE TROIS CARRÉS

**Tout nombre $n \equiv 7$ [8] ( forme 8k-1 ou 8k+7 ) n'est pas somme de trois carrés**

*Conjecturé par Fermat en 1636* *Prouvé par Descartes en 1639*

*Démonstration*
Si $n \equiv 7$ [8] alors n est impair.
Cas possibles pour la somme de 3 nombres, pairs ou impairs : P+P+P=P P+P+I=I P+I+I=P I+I+I=I
Si n est impair et somme de 3 nombres, alors - au moins l'un des trois est impair
- les 2 autres sont soit tous les 2 pairs, soit tous les 2 impairs
Disons que a est le nombre qu'on sait être impair.

- *Si a, b et c sont impairs*

Comme on a vu ci-dessus, pour tout nombre impair n, $n^2 \equiv 1$ [8]
Donc $a^2 + b^2 + c^2 \equiv 1 + 1 + 1 \equiv 3$ [8] → $\equiv 7$ [8] n'est pas possible

- *Si a est impair, b et c sont pairs*

$a^2 \equiv 1$ [8]
Pour tout nombre pair $n = 2k$ on a $n^2 = 4k^2 \equiv 0$ [8] ou $\equiv 4$ [8]
Donc $b^2 + c^2 \equiv 0$ ou 4 [8] et $a^2 + b^2 + c^2 \equiv 1$ ou 5 [8] → $\equiv 7$ [8] n'est pas possible

**Un nombre est somme de trois carrés *ssi* il n'est PAS de la forme $4^h(8k+7)$** **h, k entiers positifs**

*Prouvé par Legendre en 1798, Gauss en 1801 et Dirichlet en 1837* *Démonstration hors cadre.*

Exemples $5 = 2^2 + 1^2 + 0^2$ $6 = 2^2 + 1^2 + 1^2$ mais $7 = 2^2 + 1^2 + 1^2 + 1^2$
**Carré somme de trois carrés** 81 est le plus petit : $81 = 1^2 + 4^2 + 8^2$

Nombres de la forme $n = 4^h (8k + 7)$

| | h = 0 | 1 | 2 |
|---|---|---|---|
| k = 0 | 7 | 28 | 112 |
| 1 | 15 | 60 | 240 |
| 2 | 23 | 92 | 368 |
| 3 | 31 | 124 | 496 |
| 4 | 39 | 156 | 624 |
| 5 | 47 | 188 | 752 |
| 6 | 55 | 220 | 880 |
| 7 | 63 | 252 | 1008 |
| 8 | 71 | 284 | 1136 |
| 9 | 79 | 316 | 1264 |
| 10 | 87 | 348 | 1392 |
| 11 | 95 | 380 | 1520 |
| 12 | 103 | 412 | 1648 |

# ENTIER SOMME DE QUATRE CARRÉS

**Théorème de Lagrange**

**Tout entier naturel est décomposable en somme de quatre carrés, au plus.**

# RESTES CHINOIS

**Problème de Sun Zi**




Combien l'armé a-t-elle de soldats si,
rangés par 3 colonnes il en reste 1
rangés par 5 colonnes il en reste 2
rangés par 7 colonnes il en reste 3

**Liste de congruences**

On liste les valeurs successives modulo 3, 5 et 7
Et on cherche la concordance.
X [3] =1 → X = {…, 31, 34, 37, 40, 43, 46, 49, **52**, …}
X [5] = 2 → X = {2, 7, 12, 17, 22, 27, 32, 37, 42, 47, **52**, …}
X [7] = 3 → X = {10, 17, 24, 31, 38, 45, **52**, …}

**Restes de congruences**

On liste les valeurs successives modulo le plus grand facteur.
Puis on calcule les restes de ces nombres avec les autres modulos, jusqu'à trouver les restes désirés.
X [7] = 3 → X = {10, 17, 24, 31, 38, 45, **52**, …}

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| X [3] | 1 | 2 | 0 | 1 | 2 | 0 | **1** |
| X [5] | 0 | 2 | 4 | 1 | 3 | 0 | **2** |

**Théorème des restes chinois**

Pour tous (a, b) et (m, n) avec $m \wedge n = 1$, il existe un nombre unique X tel que $m_n^{-1}$ est l'inverse de m modulo n
$X \equiv a\ [m]$ et $X \equiv b\ [n]$
**$X \equiv b.\ m.\ m_n^{-1} + a.n.\ n_m^{-1}\ [m.n]$**

On calcule le produit des modulos N = 3.5.7= 105
Pour chaque modulo on calcule le produit des autres modulos.
Pour ceux-ci on cherche un multiple dont le reste est 1 dans son modulo

| | | |
|---|---|---|
| $X \equiv 1\ [3]$ | $N_3 = 5.7 = 35$ | $2\ N_3 = 70 \equiv 1\ [3]$ |
| $X \equiv 2\ [5]$ | $N_5 = 3.7 = 21$ | $2\ N_5 = 42 \equiv 2\ [5]$ |
| $X \equiv 3\ [7]$ | $N_7 = 3.5 = 15$ | $3\ N_7 = 45 \equiv 3\ [7]$ |

$X = 2\ N_3 + 2\ N_5 + 3\ N_7 =$ **157 = 52** +105k

**Les 17 pirates**

17 pirates ont amassé un trésor en pièces d'or égales. Partagé en parts égales il reste 3 pièces pour le cuisinier.
Lors d'une bataille 6 pirates sont tués. Partagé en parts égales, il resterait alors 4 pièces pour le cuisinier.
Après une terrible tempête il ne reste plus que six pirates - qui décident de changer de carrière. Ils distribuent le trésor et laissent 5 pièces au cuisinier. Combien y a-t'il au minimum de pièces dans le trésor ?

| | | |
|---|---|---|
| $X \equiv 3\ [17]$ | $N_{17} = 6.11 = 66$ | $3\ N_{17} = 198 \equiv 1\ [17]$ |
| $X \equiv 4\ [11]$ | $N_{11} = 6.17 = 102$ | $4\ N_{11} = 408 \equiv 1\ [11]$ |
| $X \equiv 5\ [6]$ | $N_6 = 11.17 = 187$ | $1\ N_6 = 187 \equiv 1\ [6]$ |

N = 6.11.17= 1122

$X = 3\ N_{17} + 4\ N_{11} + 1\ N_6 =$ **793** + 1122k

# ON VA PLUS LOIN ?

Trois théorèmes qui dépassent le cadre de ce livre …

**Le théorème de Fermat-Euler**
La fonction d'Euler est définie comme $\phi(n)$= nombre d'éléments dans {1, 2, ..., n-1} qui sont premiers avec n.

**a ∧ n = 1 ⟹ $a^{\phi(n)} \equiv 1$ [n]**

$\phi(n)$ est une fonction qui tend vers l'infini, mais n'est pas strictement croissante.
On l'appelle aussi totient.

Pour p premier $\phi(p) = p - 1$ (easy : un nombre est premier *ssi* il est premier avec tous les nombres plus petits que lui)
$\phi(p^n) = p^{n-1}(p-1)$
Si a ∧ b = 1 $\phi(ab) = \phi(a).\phi(b)$
Si a ∧ b = d $\phi(ab) = d.\phi(a).\phi(b)/\phi(d)$
$\phi(\boldsymbol{n}) = \boldsymbol{n}.\left(\mathbf{1}-\frac{\mathbf{1}}{\boldsymbol{p_1}}\right)\left(\mathbf{1}-\frac{\mathbf{1}}{\boldsymbol{p_2}}\right)\ldots\left(\mathbf{1}-\frac{\mathbf{1}}{\boldsymbol{p_r}}\right)$ *avec la décomposition en facteurs premiers* $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_r^{\alpha_r}$
Si n = p.q $\phi(n) = (p-1)(q-1)$ $\phi(n)$ = n.(1-1/p)(1-1/q) = n (p-1)(q-1)/pq = (p-1)(q-1)

**Grand théorème de Fermat**
Aussi appelé Dernier Théorème de Fermat ou Théorème de **FERMAT-WILES**

**Pour x, y, z entiers $z^n = x^n + y^n$ est impossible**
sauf pour les carrés (n=2) pour lesquels il y a une infinité de triplets de Pythagore comme $3^2 + 4^2 = 5^2$

**Une puissance (cubique ou plus) ne peut pas être la somme de 2 puissances du même ordre.**

Un des plus grands problèmes mathématiques de tous les temps. Démontré en 1994 après 350 ans d'efforts.
Voir plus loin pour un synoptique historique de la démonstration.

**La loi de la réciprocité quadratique (Gauss)**
***Karl Friedrich Gauss 1777 - 1855***
Considérant les équations **$x^2 \equiv q$ [p] et $x^2 \equiv p$ [q]**
- Si p et q sont de la forme 4k + 3, l'une des équations a des solutions et l'autre non ;
- Dans tous les autres cas, soit elles sont toutes les deux avec solutions ou alors toutes les deux sans.

Il s'agit de chercher si l'équation $x^2 \equiv q$ [p] a des solutions, sachant que p et q sont des nombres premiers impairs distincts.

Cette loi permet de contourner certains problèmes en les ramenant à des questions plus simples à résoudre.

Exemple $x^2 \equiv 5$ [103] n'a pas de solution, car :
- 5 n'est pas de la forme 4k + 3, et, conséquence de cette loi :
- $x^2 \equiv 103$ [5] $\equiv 3$ [5] n'a pas de solution.

# IDENTITÉS REMARQUABLES

Pour tout n **$a - b \mid a^n - b^n$** car $\forall n$ **$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$**

Pour tout n impair $a + b \mid a^n + b^n$ (c'est la même chose que la première identité en remplaçant b par -b)

Une somme de 2 carrés $a^2 + b^2$ est factorisable si 2ab est un carré :

$a^2 + b^2 = a^2 + b^2 + 2ab - 2ab$ on ajoute et on soustrait 2ab, l'élément manquant de la formule binomiale

$= (a^2 + 2ab + b^2) - 2ab$ on reconnait la formule binomiale

$= (a + b)^2 - 2ab$ si 2ab est un carré : $2ab = c^2$

$= (a + b)^2 - c^2$ on reconnait une formule binomiale du type $u^2 - v^2 = (u-v).(u+v)$

$= (a + b - c)(a + b + c)$ Et voilà ! On a transformé une somme de 2 carrés en un produit de deux facteurs : on dit qu'on a ***factorisé***.

La même technique est utilisée dans l'exemple le plus connu - l'***Identité de Sophie Germain***

**$\forall$ a,b $\in \mathbb{Z}$ $a^4 + 4b^4$ est factorisable en facteurs entiers**

$a^4 + 4b^4 = a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2$ on remarque que $a^4 = (a^2)^2$ et $4b^4 = (2b^2)^2$ donc on +/- $2.(a^2).(2b^2) = 4a^2b^2$

$= (a^4 + 4a^2b^2 + 4b^4) - 4a^2b^2$ on reconnait une formule binomiale du type $(u^2 + 2uv + v^2) = (u+v)^2$

$= (a^2 + 2b^2)^2 - 4a^2b^2$ quelle chance ! $4a^2b^2 = (2ab)^2$ est un carré

$= (a^2 + 2b^2)^2 - (2ab)^2$ on reconnait une formule binomiale du type $u^2 - v^2 = (u-v).(u+v)$

$= (a^2 + 2b^2 - 2ab).(a^2 + 2b^2 + 2ab)$ Booom ! Factorisé !



Autre exemple : $x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2$

$= (x^2 + 1)^2 - x^2$

$= (x^2 + 1 - x)(x^2 + 1 + x)$

*Identité de Sophie Germain – Exemple #1*

**Montrer que $n>1 \Rightarrow N = n^4 + 4^n$ n'est jamais premier**

- Si n est pair, N est pair et N>2 donc N n'est pas premier.
- Si n est impair $\exists$ k entier naturel tel que $n = 2k+1$

Alors $N = n^4 + 4^{2k+1} = n^4 + 4.4^{2k} = n^4 + 4.(2^2)^{2k} = n^4 + 4.(2^k)^4$

Donc N est de la forme $a^4 + 4b^4$, l'identité de Sophie Germain, qui est factorisable

Donc N n'est pas premier.

*Identité de Sophie Germain – Exemple #2*

**Est-ce que $4^{545} + 545^4$ est premier ?**

$4^{545} + 545^4 = 545^4 + 4.4^{544} = 545^4 + 4.4^{4.136} = 545^4 + 4.(4^{136})^4$

On a trouvé une identité de Sophie Germain $a^4 + 4b^4$ avec $a = 545$ et $b = 4^{136}$

Ce nombre est donc factorisable et donc non premier.

**Autre méthode de factorisation**

**Montrer que pour n >1 $f(n) = n^5 + n^4 + 1$ n'est pas premier**

Clairement ça veut dire que f(n) doit être factorisable.

Comment arriver au 5ème degré ?

Si il y avait un facteur linéaire ce serait (n-1) ou (n+1) mais $f(1) \neq 0$ et $f(-1) \neq 0$ donc il n'y en a pas.

Autre possibilité : un facteur quadratique multiplié par un facteur cubique.

Alors soit $f(n) = (n^2 + an + 1) . (n^3 + bn^2 + cn + 1)$

soit $f(n) = (n^2 + an - 1) . (n^3 + bn^2 + cn - 1)$

On développe la première forme $f(n) = n^5 + (a+b)n^4 + (ab+c+1)n^3 + (ac+b+1)n^2 + (a+c)n + 1$

On obtient 4 équations à 3 inconnues : $a+b=1$ $ab+c+1=0$ $ac+b+1=0$ $a+c=0$

On obtient $b=0$ $a=1$ $c=-1$

d'où $f(n) = (n^2 + n + 1) . (n^3 - n + 1)$

Donc f(n) est factorisable et n'est pas un nombre premier.

On n'a pas besoin de résoudre pour la seconde forme - qui d'ailleurs n'a pas de solution. Une factorisation suffit pour prouver que f(n) n'est pas premier - peu importe s'il en existe une, plusieurs ou aucune autre.

# MA BOITE À OUTILS




| **Je lis** | **n est pair** | **Je traduis automatiquement** | **Il existe k tel que n = 2k** |
|---|---|---|---|
| | **n est impair** | | **Il existe k tel que n = 2k +1** |



**Règles de divisibilité**

$z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1.10 + a_0$ **R**

$z = \sum_{i=0}^{n} a_i . 10^i$ **Quersumme** $Q(z) = \sum_{i=0}^{n} a_i$ **Alternierende Quersumme** $AQ(z) = \sum_{i=0}^{n} (-1)^i . a_i$

**Par 3** $10^i \equiv 1^i \equiv 1$ [3] $z \equiv Q(z)$ [3] **Par 9** $10^i \equiv 1^i \equiv 1$ [9] $z \equiv Q(z)$ [9]
**Par 5** $z = 10.b + a_0$ $z \equiv a_0$ [5]
**Par 2** $z = 10.b + a_0$ $z \equiv a_0$ [2] **Par 4** $z = 100k + 10\,a_1 + a_0 \equiv 10\,a_1 + a_0$ [4]
**Par 8** $z = 1000k + 100\,a_2 + 10\,a_1 + a_0 \equiv 100a_2 + 10\,a_1 + a_0$ [8]
**Par 11** $z \equiv Q[z]$ [11] **Par 7** $z \equiv AQ_3[z]$ [7] **Par 13** $z \equiv AQ_3(z)$ [13]

**Méthode pour calculer le reste de la division euclidienne de $a^b$ par n (a, b très grands)**
On remplace a par son reste u par la division par n : **$a \equiv u$ [n]** $\Rightarrow a^b \equiv u^b$ [n]
On calcule les puissances successives de u ($u, u^2, u^3, ...$) en cherchant le premier entier k tel que $u^k \equiv 1$[n] ou -1[n]
(un tel entier existe si u et n sont premiers entre eux; sinon les restes reviennent en boucle périodique)
En effectuant la division euclidienne de b par k : $b = kq + v$ **$b \equiv v$ [k]**
on obtient : $u^b = u^{kq+v} = u^{kq} \times u^v = [u^k]^q \times u^v$ $u^b \equiv [u^k]^q \times u^v \equiv 1^q \times u^v \equiv u^v$ [n] **$a^b \equiv u^b \equiv u^v$ [n]**

**Congruences**
Si $a \equiv b$ [n] et $b \equiv c$ [n], alors $a \equiv c$ [n]

Si $a \equiv b$ [n] alors $a+c \equiv b+d$ [n] $a-c \equiv b-d$ [n] $ac \equiv bd$ [n]
et $c \equiv d$ [n] ka ≡ kb [n] pour k entier relatif $a^m \equiv b^m$ [n] pour m entier naturel
f(a) ≡ f(b) [n] pour toute fonction polynomiale $f(x) = a_n x^n + ... + a_1 x + a_0$ $a_i \in \mathbb{Z}$
$a \equiv b$ [d] pour d divisant n
Attention ! $ca \equiv cb$ [n] $\Rightarrow a \equiv b$ [n] seulement si $c \wedge n = 1$
$(a+b)^p \equiv a^p + b^p$ [p]

Binôme de Newton $(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k . b^{p-k} + b^p$ *et* p divise $\binom{p}{k}$ pour tout k $\in [1, p-1]$

Si $a \equiv 1$ [n] et $a \equiv 1$ [m] alors $a \equiv 1$ [n.m] si $n \wedge m = 1$

**Petit théorème de Fermat**
Pour n entier relatif et p premier **$n^p \equiv n$ [p]**
Si en plus $n \wedge p = 1$ **$n^{p-1} \equiv 1$ [p]**

**Le carré d'un nombre impair est ≡ 1 [8]** **Il s'écrit sous la forme 8k+1**
**Le carré d'un nombre pair est ≡ 0 [4]** **Il s'écrit sous la forme 4k**

**Théorème des deux carrés de Fermat**
Un nombre premier est somme (unique) de 2 carrés *ssi* il est de la forme 4n+1 i.e. ≡ 1 [4]
Un entier est somme de 2 carrés *ssi* chacun de ses facteurs premiers ≡ 3 [4] est à une puissance paire.

**Tout nombre n ≡ 7 [8] ( forme 8k-1 ou 8k+7 ) n'est pas somme de trois carrés**

**Factorisation et identités remarquables**

# PROBLÈMES CLASSÉS

## RESTE & DIVISIBILITÉ

**Si le reste de la division euclidienne d'un entier naturel n par 12 est 7, quel est le reste de la division euclidienne de n par 3 ? Par 4 ?**

Puisque le reste de la division euclidienne de n par 12 est 7, il existe un entier naturel q tel que n=12q+7
C'est à dire : n=3×4q+7
Toutefois on ne peut pas en déduire que le reste de la division de n par 3 est 7 puisque 7 est plus grand que 3.
Mais 7 = 3×2+1 donc n = 3×4q+3×2+1 = 3(4q+2)+1
On a ainsi obtenu une formule du type n=bq'+r' avec q'=4q+2 et r'=1<3.
*Le reste de la division euclidienne de n par 3 est donc 1.*

De même : n = 4×3q+7 = 4×3q+4×1+3 = 4(3q+1)+3 ≡ 3 [4]
*Le reste de la division euclidienne de n par 4 est donc 3.*

**Si le reste de la division euclidienne d'un entier naturel n par 4 est 3, quels sont les restes possibles de la division euclidienne de n par 12 ?**

Le reste de la division euclidienne de n par 4 étant3, il existe un entier naturel k tel que : n=4k+3
On voudrait obtenir une expression de la forme n=12q+r
Pour cela on remplace k par 3q+r en analysant les 3 seuls cas possibles pour r :

- Si k ≡ 0 [3] i.e. k=3q n=4×3q+3=12q+3 n ≡ 3 [12]
- Si k ≡ 1 [3] i.e. k=3q+1 n=4×(3q+1)+3=12q+7 n ≡ 7 [12]
- Si k ≡ 2 [3] i.e. k=3q+2 n=4×(3q+2)+3=12q+11 n ≡ 11 [12]

*Le reste de la division euclidienne de n par 12 est donc soit 3, soit 7, soit 11.*

**Montrer que pour tout entier naturel n : $2^{n+4}+3^{3n+2}$ est divisible par 25.**

*L'astuce est de remarquer que $3^3 = 27 \equiv 2$ [25] et à factoriser $2^n$.* ★★☆

$3^3 \equiv 2$ [25]
On élève chaque membre à la puissance n : $(3^3)^n \equiv 2^n$ [25]
On multiplie par $3^2$ : $3^{3n} \times 3^2 \equiv 2^n \times 3^2$ [25]
$3^{3n+2} \equiv 9 \times 2^n$ [25]
On ajoute $2^{n+4}$ à chaque membre : $2^{n+4} + 3^{3n+2} \equiv 9 \times 2^n + 2^{n+4}$ [25]
On factorise $2^n$ : $2^{n+4} + 3^{3n+2} \equiv 9 \times 2^n + 2^4 \times 2^n$ [25]
$2^{n+4} + 3^{3n+2} \equiv 9 \times 2^n + 16 \times 2^n$ [25]
$2^{n+4} + 3^{3n+2} \equiv 25 \times 2^n$ [25]
$2^{n+4} + 3^{3n+2} \equiv 0$ [25]
*donc $2^{n+4}+3^{3n+2}$ est divisible par 25.*

**Montrer que pour tout entier naturel n : $16x7^{2n} – 28x3^{2n+3}$ est divisible par 5**

*On exprime chaque nombre modulo 5 :*

$16 \equiv 1$ [5] $7^2=49 \equiv -1$ [5] $28 \equiv 3$ [5] $\equiv -2$ [5] $3^2=9 \equiv -1$ [5] $3^3=27 \equiv 2$ [5]
$16x7^{2n} – 28x3^{2n+3} = 16 \times (7^2)^n – 28 \times (3^2)^n \times 3^3 \equiv 1 \times (-1)^n + 2 \times (-1)^n \times 2 \equiv 5(-1)^n \equiv 0$ [5]

**Déterminer en fonction de n le reste de la division euclidienne de $2^n$ par 3**

Puisqu'on observe la division par 3, on va travailler modulo 3.
On calcule les premières puissances de 2 jusqu'à en trouver une de reste 1 modulo 3 :
$2 \equiv 2$ [3] Ça ne marche pas, on continue.
$2^2 = 4 \equiv 1$ [3] Trouvé.
Pour les nombres pairs, s'écrivant sous la forme n=2k, on a $2^{2k} = (2^2)^k \equiv 1^k \equiv 1$ [3]
Pour les nombres impairs, s'écrivant sous la forme n=2k+1, on a $2^{2k+1} = 2(2^2)^k \equiv 2(1)^k \equiv 2$ [3]
*Le reste de la division euclidienne de $2^n$ par 3 est donc 1 si n est pair ou 2 si n est impair.*

**Montrer que $5^{2n}-7^m$ est divisible par 3**
$5^{2n} - 7^m \equiv (-1)^{2n} - 1^m\ [3] \equiv 1-1\ [3] \equiv 0\ [3]$

**Montrer que $(3a-1)^{2n} - (3b+1)^m$ est divisible par 3**
$(3a-1)^{2n} - (3b+1)^m \equiv (-1)^{2n} - 1^m\ [3] \equiv 0\ [3]$

**Montrer que $N = n^7-n$ est divisible par 42**

★★☆

*42 = 2.3.7 Il faut montrer la divisibilité par 2, par 3 et par 7.*



- *Divisibilité par 2*

Si n est pair, $n^7$ est pair, et N est pair
Si n est impair, $n^7$ est impair, et N est pair

- *Divisibilité par 3*

Si $n \equiv 0\ [3]$, $N= n^7-n \equiv 0-0 \equiv 0\ [3]$
Si $n \equiv 1\ [3]$, $N= n^7-n \equiv 1^7-1 \equiv 0\ [3]$
Si $n \equiv -1\ [3]$, $N= n^7-n \equiv (-1)^7-(-1) \equiv 0\ [3]$

- *Divisibilité par 7*

C'est le petit théorème de Fermat pour p=7 : $n^7-n \equiv 0\ [7]$

On peut aussi observer $n^7-n = (n+1).n.(n+1).(n^4+n^2+1)$
Si n est impair : n+1, n et n+1 sont trois nombres consécutifs dont 2 pairs consécutifs,
donc (n+1).n.(n+1) est divisible par 2, 3 et 4
**Si n est impair N est alors divisible par 2.3.4.7 = 168**

**Montrer que $N = 5^{96} - 7^{112}$ est divisible par 66**

*66 = 2.3.11 Il faut montrer la divisibilité par 2, par 3 et par 11.*

- *Divisibilité par 2*

5 est impair donc $5^{96}$ est impair ; 7 est impair donc $7^{112}$ est impair. La différence de 2 nombres impairs est paire.

- *Divisibilité par 3*

$N = 5^{96} - 7^{112} \equiv (-1)^{96} - 1^{112}\ [3] \equiv 1-1 \equiv 0\ [3]$

- *Divisibilité par 11*

Avec le petit théorème de Fermat :
$5^{10} \equiv 1\ [11]$ et $5^{96} \equiv 5^6\ [11] \equiv 25^3\ [11] \equiv 3^3\ [11] \equiv 27\ [11] \equiv 5\ [11]$
$7^{10} \equiv 1\ [11]$ et $7^{112} \equiv 7^2\ [11] \equiv 49\ [11] \equiv 5\ [11]$
Donc $N \equiv 5-5\ [11] \equiv 0\ [11]$

**Montrer que $N = n^4 + n^2 + 2n$ est divisible par 4**

★☆☆

- *Si n est pair*

n= 2k $N = (2k)^4 + (2k)^2 + 4k = 16k^4 + 4k^2 + 4k \equiv 0[4]$

- *Si n est impair*

$n= 2k+1 \equiv 1$ ou $-1\ [4]$ Dans tous les cas $(2k+1)^4 \equiv 1\ [4]$ et $(2k+1)^2 \equiv 1\ [4]$
$N = (2k+1)^4 + (2k+1)^2 + 4k+2 \equiv 1 + 1+ 0 + 2 \equiv 0[4]$

**Montrer que $n^2 - n$ est divisible par 2**
$n^2 - n = n(n-1)$
Produit de 2 nombres successifs, l'un est forcément pair, le produit est pair.

**Montrer que $n^3 - n$ est divisible par 6**
$n^3 - n = (n-1)n(n+1)$
Produit de 3 nombres successifs, au moins un est pair, au moins un est divisible par 3.

## Divisibilité par 504

*504 = 7 x 8 x 9  La divisibilité par 504 revient à démonter la divisibilité par 7, par 8 et par 9.*

★★☆

**Montrer que pour tout entier naturel n>1 : $N = (n^3-1).n^3.(n^3+1)$ est divisible par 504**

- *Divisibilité par 7*

$N = (n^3-1).n^3.(n^3+1) = n^3(n^6-1) = n^2(n^7-n)$
$n^7 \equiv n\ [7]$ (petit théorème de Fermat)
$n^7 - n \equiv 0\ [7]$
$N = n^2(n^7 - n) \equiv 0.n^2\ [7] = 0\ [7]$

- *Divisibilité par 8*

- Si n est pair, $n^3$ est divisible par 8.
- Si n est impair, $n^3$ est impair, ses 2 voisins sont pairs consécutifs donc l'un d'eux divisible par 4, donc N est divisible par 8.

- *Divisibilité par 9*

- Si $n \equiv 0\ [3]$, $n^3$ est divisible par $3^3=27$ et a fortiori par 9 : $N \equiv 0[9]$
- Si $n \equiv 1\ [3]$, on remarque que $n^3-1 = (n-1)(n^2+n+1)$.

$n - 1 \equiv 0\ [3]$ et $n^2+n+1 \equiv 1+1+1\ [3] \equiv 0\ [3]$ donc $n^3-1 \equiv 0[9]$ et $N \equiv 0[9]$

- Si $n \equiv -1\ [3]$, on remarque que $n^3+1 = (n+1)(n^2-n+1)$.

$n + 1 \equiv 0\ [3]$ et $n^2-n+1 \equiv (-1)^2-(-1)+1\ [3] \equiv 3\ [3] \equiv 0\ [3]$ donc $n^3+1 \equiv 0[9]$ et $N \equiv 0[9]$

**Montrer que pour tout p premier >7 : $M = p^6 - 1$ est divisible par 504**

On remarque que $M = (p^3-1).(p^3+1)$

- *Divisibilité par 7*

$p^7 \equiv p\ [7]$ (petit théorème de Fermat)
$p^7 - p = M.p \equiv 0\ [7]$
M.p est divisible par 7 et p est premier >7, donc M est divisible par 7.

- *Divisibilité par 8*

$M = p^6-1 = (p^3-1).(p^3+1)$
p est premier >7 donc impair.
$p^3$ est impair ; $p^3-1$ est pair ; $p^3+1$ est pair.
De plus $p^3-1$ et $p^3+1$ sont des nombres pairs consécutifs, donc l'un des deux est multiple de 4.
M est donc un multiple de 8.  $M \equiv 0\ [8]$

- *Divisibilité par 9*

- $p \equiv 0\ [3]$ n'est pas possible car p est premier
- Si $p \equiv 1\ [3]$, on remarque que $p^3-1 = (p-1)(p^2+p+1)$.

$p - 1 \equiv 0\ [3]$ et $p^2+p+1 \equiv 1+1+1\ [3] \equiv 0\ [3]$ donc $p^3-1 \equiv 0[9]$ et $M = (p^3-1).(p^3+1) \equiv 0[9]$

- Si $p \equiv -1\ [3]$, on remarque que $p^3+1 = (p+1)(p^2-p+1)$.

$p + 1 \equiv 0\ [3]$ et $p^2-p+1 \equiv (-1)^2-(-1)+1\ [3] \equiv 3\ [3] \equiv 0\ [3]$ donc $p^3+1 \equiv 0[9]$ et $M \equiv 0[9]$

**a-c | ab+cd ⇒ a-c | ad+bc**

ab + cd – (ad + bc) = a(b-d) – c (b-d) = (a-c)(b-d) ⇒ (ab + cd) = (ad + bc) + (a-c)(b-d)

a-c | ab+cd ⇒ il existe k tel que k(a-c)= ab + cd = (ad + bc) + (a-c)(b-d)

⇒ ad+bc = k(a-c) - (a-c)(b-d) = (a-c)(k-b+d)

⇒ a-c | ad+bc

**a ≡ b ≡ 1 [2 ] ⇒ $a^2 + b^2$ n'est pas un carré**

a, b impairs ⇒ $a^2$, $b^2$ impairs ⇒ $a^2 + b^2$ pair

Si $a^2 + b^2$ qui est pair était un carré, il devrait être multiple de 4 i.e. **≡ 0 [4]**

Mais a ≡ 1 [2] ⇒ a ≡ 1 ou -1 [4] ⇒ $a^2$ ≡ 1 [4]

De même $b^2$ ≡ 1 [4] et $a^2 + b^2$ ≡ 1+1 **≡ 2 [4]**

Contradiction.

**6 | $n^3 + 5n$**

PTF : $n^3$ ≡ n [3] $n^3$ +5n ≡ n+5n = 6n ≡ 0[3]

Si n pair, $n^3 + 5n$ pair Si n impair, $n^3 + 5n$ pair donc $n^3$ +5n ≡ 0[2]

Donc 6 | $n^3 + 5n$

**30 | $n^5$ -n**

PTF : $n^5$ ≡ n [5] $n^5$ - n ≡ n-n ≡ 0[5] ⇒ 5 | $n^5$ -n

$n^5$ -n = n($n^4$ -1) = n($n^2$ - 1)($n^2$ + 1) = n(n - 1)(n + 1)($n^2$ + 1) = (n - 1)n(n + 1)($n^2$ + 1)

n-1, n et n+1 sont 3 entiers successifs, donc l'un d'eux est multiple de 3 ⇒ 3 | $n^5$ -n

De même au moins l'un d'eux est multiple de 2 ⇒ 2 | $n^5$ -n

$n^5$ -n est divisible par 2, 3 et 5, donc par 30

**Si n impair**, on a n-1 et n+1 entiers pairs consécutifs, donc n-1 ou n+1 ≡ 0[4] et donc **120 | $n^5$ -n**

**3 | a, 3 | b ⇔ 3 | $a^2 + b^2$**

⇒ a ≡ 0 [3] alors $a^2$ ≡ 0 [3] b ≡ 0 [3] alors $b^2$ ≡ 0 [3] Donc $a^2 + b^2$ ≡ 0 [3]

⇐ a ≡ 0, 1 ou -1 [3] $a^2$ ≡ 0 ou 1 [3] Donc $a^2 + b^2$ ≡ 0 [3] implique $a^2$ ≡ 0 [3] et $b^2$ ≡ 0 [3]

**7 | a, 7 | b ⇔ 7 | $a^2 + b^2$**

⇒ a ≡ 0 [7] alors $a^2$ ≡ 0 [7] b ≡ 0 [7] alors $b^2$ ≡ 0 [7] Donc $a^2 + b^2$ ≡ 0 [7]

⇐ Si a pair a = 2k, $a^2 = 4k^2$ ≡ 0 ou 4 [7]

Si a impair a = 2k+1, $a^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$ ≡ 1 [7] car k ou k+1 est pair

Donc quel que soit a, **$a^2$ ≡ 0, 1 ou 4 [7]** Donc $a^2 + b^2$ ≡ 0 [7] implique $a^2$ ≡ 0 [7] et $b^2$ ≡ 0 [7]

**21 | $a^2 + b^2$ ⇒ 441 | $a^2 + b^2$**

21 | $a^2 + b^2$ ⇒ 3 | $a^2 + b^2$ ⇒ 3 | a, 3 | b

et 7 | $a^2 + b^2$ ⇒ 7 | a, 7 | b ⇒ 21 | a, 21 | b ⇒ 441 | $a^2$, 441 | $b^2$ ⇒ 441 | $a^2 + b^2$

**6 | a + b + c ⇔ 6 | $a^3 + b^3 + c^3$**

($a^3$+$b^3$+$c^3$) – (a + b + c) = $a^3$ – a + $b^3$ - b + $c^3$ – c = a($a^2$-1) + b($b^2$-1) + c($c^2$-1) = (a-1)a(a+1) + (b-1)b(b+1) + (c-1)c(c+1)

On a déjà vu plusieurs fois maintenant que le produit de 3 nombres successifs est divisible par 6.

Donc il existe k entier tel que ($a^3$+$b^3$+$c^3$) = (a + b + c) + 6k

Donc si ($a^3$+$b^3$+$c^3$) ≡ 0 [6] alors (a + b + c) ≡ 0 [6], et inversement.

**Critère de divisibilité par 9**

10 ≡ 1 [9] ⇒ pour tout i, $10^i$ ≡ 1 [9]

$$n = \sum_i a_i 10^i \equiv \sum_i a_i \ [9] = Quersumme(n)$$

**Critère de divisibilité par 11**

10 ≡ -1 [11] ⇒ pour tout i, $10^i$ ≡ $(-1)^i$ [9]

$$n = \sum_i a_i 10^i \equiv \sum_i (-1)^i a_i \ [11] = Alternierende\ Quersumme(n)$$

**A = $3^{105} + 4^{105}$  A ≡ ? [7], [11], [13]**
A ≡ $3^3(3^6)^{17} + 4^3(4^6)^{17}$ ≡ $27(1)^{17} + 64(1)^{17}$ ≡ -1 + 1 ≡ 0 [7]
A ≡ $(3^5)^{21} + (4^5)^{21}$ ≡ $(1)^{21} + (1)^{21}$ ≡ 2 [11]
A ≡ $(3^3)^{35} + 4^3(4^6)^{17}$ ≡ $(1)^{35} + 64(1)^{21}$ ≡ 65 ≡ 0 [13]

**Montrer que 641 | $2^{32} + 1$**
641 n'est pas divisible par 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 et $29^2$> 641 donc 641 est premier.

*On remarque d'une part que*
641 = 640 + 1 = 64.10 + 1 = $2^6$.10 +1 = $2^7$.5 + 1
$2^7$.5 = 641 -1 ≡ -1 [641]
A = $(2^7.5)^4$ = $2^{28}.5^4$ ≡ 1 [641]

★★★

*On remarque d'autre part que*
641 = 16 + 625 = $2^4 + 5^4$  *( Mouais… )*
$2^4 + 5^4$ ≡ 0 [641]
$2^{28}(2^4 + 5^4)$ = $2^{32} + 2^{28}.5^4$ = $2^{32}$ + A ≡ 0 [641]
⇒ $2^{32}$ + 1 ≡ 0 [641]

**Sei X= $4444^{4444}$ und Q(X) = A ihre Quersumme. Sei B = Q(A). Bestimme C = Q(B).**
Wir machen zuerst eine sehr grobe Abschätzung:

★★★

X ⩽ $10000^{10000}$ = $(10^4)^{10000}$ = $10^{40000}$
Da die 40000 Ziffern all höchstens 9 sein können, gilt A ⩽ 40000 . 9 = 360 000
Die höchste Quersumme wäre die von 299 999, also B ⩽ 5.9+2 = 47
Damit ist C ⩽ 3 + 9 = 12

Da der Rest Modulo 9 bei einer Quersumme der gleiche ist wie bei der Ausgangszahl (Regel Teilbarkeit bei 9), wenn wir den Rest von X bestimmen, kennen wir also auch den Rest von C.
4444 = 493.9+7 ≡ 7 [9] also $4444^{4443}$ ≡ $7^{4443}$ [9] = $(7^3)^{1481}$ [9]
Da $7^3$ = 38.9+1 ≡ 1 [9]  $(7^3)^{1481}$ [9] ≡ $1^{1481}$ [9] = 1 [9]
Also $4444^{4444}$ ≡ $7^{4444}$ [9] = $7.7^{4443}$ [9] ≡ 7.1 [9] ≡ 7 [9]
Also der Rest beim Teilen von C durch 9 ist auch 7.
Da C ⩽ 12, C kann nur 7 sein.  C = 7

**Reste en utilisant le théorème de Fermat-Euler  a ∧ n = 1 ⇒ $a^{\phi(n)}$ ≡ 1 [n]**
**Quels sont les trois derniers chiffres de $7^{9999}$ ?**

★★★

On cherche n ≡ $7^{9999}$ [1000] ou 7n ≡ $7^{10000}$ [1000]
On utilise la formule
$\phi(n) = n.\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)$ *avec la décomposition en facteurs premiers* $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_r^{\alpha_r}$
1000 = $10^3$ = $2^3.5^3$ donc $\phi(1000) = 1000.\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400$
Le théorème de Fermat-Euler dit que comme 7 ∧ 1000 = 1 ⇒ $7^{\phi(1000)}$ = $7^{400}$ ≡ 1 [1000]
Alors $7^{10000}$ = $7^{400.25}$ ≡ $1^{25}$ = 1 [1000]
On cherche donc 7n ≡ 1 [1000]
On pourrait résoudre de façon systématique avec l'algorithme d'Euclide 7n+1000m = 1
Mais on peut reconnaitre ici un produit spécial.
Avec m = -1 on a 7n = 1001 = 7.11.13 donc n = 11.13 = **143**

## NOMBRES PREMIERS

**Déterminer tous les nombres premiers p tels que p−10 et p+10 soient aussi premiers.**

On décale le problème : q=p-10 et on cherche q tel que q, q+10 et q+20 soient premiers.
Si $q \equiv 1$ [3], alors $q + 20 \equiv 3 \equiv 0$ [3] donc q+20 est divisible par 3. q+20 > 3 ne peut alors pas être premier.
Si $q \equiv 2$ [3], alors $q + 10 \equiv 3 \equiv 0$ [3] donc q+10 est divisible par 3. q+10 > 3 ne peut alors pas être premier.
Si $q \equiv 0$ [3], le seul multiple de 3 premier est 3. q = 3.
Donc q = 3. q+10 = 13 est premier et q+20 = 23 est aussi premier.
Pour répondre à la question initiale : p=13 est la solution unique.

**Montrer que si n a un diviseur impair, alors 2n + 1 n'est pas premier**

$a + b \mid a^n + b^n$ pour n impair.
Donc $2 + 1 = 3 \mid 2^n + 1$ et $2^n + 1$ n'est pas premier pour n impair

**Déterminer tous les nombres p tels que p, p+10 et p+14 soient premiers.**

p, p+10 et p+14 ont des restes différents [3] – ils appartiennent à des classes de reste distinctes modulo 3.
L'un d'eux est divisible par 3. Si ils sont tous premiers, ce n'est possible que pour p=3 (le seul nombre premier divisible par 3 est 3).
13 et 17 sont bien premiers.

**Déterminer tous les nombres p tels que p, 2p+1 et 4p+1 soient premiers.**

Si $p \equiv 1$ [3] alors $2p+1 \equiv 0$ [3] qui n'est possible pour un nombre premier que si 2p+1 = 3.
Mais alors on aurait p =1 qui n'est pas premier.
Si $p \equiv 2$ [3] alors $4p+1 \equiv 0$ [3] qui n'est possible pour un nombre premier que si 4p+1 = 3 ce qui n'est pas possible pour p entier.
Si $p \equiv 0$ [3] alors p premier n'est possible que si p = 3. 2p+1 = 7 et 4p+1 = 13 sont premiers. Solution unique

**Déterminer tous les nombres p tels que p et $8p^2 + 1$ soient premiers.**

Si $p \equiv 1$ [3] alors $8p^2 + 1 \equiv -p^2 + 1$ [3] $\equiv 0$ [3] si il doit être premier, cela implique $8p^2 + 1 = 3$ – pas possible.
Si $p \equiv 2$ [3] alors $8p^2 + 1 \equiv -p^2 + 1$ [3] $\equiv 0$ [3] si il doit être premier, cela implique $8p^2 + 1 = 3$ – pas possible.
Si $p \equiv 0$ [3] alors p premier n'est possible que si p = 3. $8p^2 + 1 = 73$ est premier. Qui est alors la solution unique.

**Trouver tous les couples (p,q) de nombres premiers tels que $p^q + q^p$ soit premier.**

Si un couple (p,q) satisfait cette condition, le couple (q,p) la satisfait également.

Si p et q sont tous deux impairs, alors $p^q$ est impair, $q^p$ est impair et $p^q + q^p$ est pair.
Mais p > 2, q >2 donc $p^q + q^p > 8$ or le seul nombre pair et premier est 2.
Il y a donc contradiction et il n'est pas possible que p et q soient tous deux impairs.

Si p et q sont tous deux pairs, alors $p \geq 2$, $q \geq 2$ donc $p^q + q^p \geq 8$ or le seul nombre pair et premier est 2.
Seul un des deux nombres est donc pair. Comme il doit être premier, il ne peut qu'être égal à 2 (CN).

On a ramené le problème à la recherche des nombres premiers p tels que $2^p + p^2$ soit premier.

Si $p \equiv 1$ ou $p \equiv -1$ [3] alors
$p^2 \equiv 1$ [3]
p étant impair il s'écrit sous la forme 2k+1 et $2^p = 2^{2k+1} = (2^2)^k \cdot 2 \equiv 1^k.2 \equiv 2$ [3]
Alors $2^p + p^2 \equiv 1 + 2 \equiv 0$ [3] qui doit aussi être premier donc $2^p + p^2 = 3$ - ce qui n'est pas possible car $p \geq 3$
Donc on a nécessairement $p \equiv 0$ [3] qui n'est premier que si p = 3 (CN).

$2^3 + 3^2 = 17$ est premier. Les solutions sont donc (2,3) et (3,2).

**Trouver tous les couples (p,q) de nombres premiers tels que $p^2 - 3q - 1$ soit premier.**

*Cas 1 : Si p pair et q est pair*
p = 2 et q = 2 car 2 est le seul nombre premier pair
$p^2 – 3q – 1 = -3$ mais -3 n'est pas premier.
Ce cas n'a pas de solution.

*Cas 2 : Si p pair et q impair*
p = 2 car 2 est le seul nombre premier pair
$p^2 – 3q – 1 = 3 – 3q = 3.(1-q)$ ce qui ne peut être premier que si 1-q=1 soit q=0 – mais 0 n'est pas impair.
Ce cas n'a pas de solution.

*Cas 3 : Si p impair et q pair*
q = 2 car 2 est le seul nombre premier pair
$p^2 – 3q – 1 = p^2 – 7$ est pair, donc nécessairement =2 pour être premier
On a donc $p^2 – 7 = 2$ $p^2 = 9$ p = 3 (CN)
$3^2 – 3.2 – 1 = 9 – 6 – 1 = 2$ qui est bien premier (CS)
**(3,2) est la seule solution de ce cas.**

*Cas 4 : Si p impair et q impair*
Si $p \equiv 0$ [3] alors p = 3 car 3 est le seul nombre premier multiple de 3.
$p^2 – 3q – 1 = 9 – 3q – 1 = 8 - 3q$ qui n'est premier que pour q = 2 ou 1, qui ne sont pas impair et premier.

Donc $p \equiv \{-1 ; 1\}$ [3] On a alors $p^2 – 3q - 1 \equiv 0$ [3]
Comme $p^2 – 3q - 1$ doit être premier c'est que $p^2 - 3q - 1 = 3$
$p^2 - 4 = 3q$
**$(p-2).(p+2) = 3q$**
Si q = 3 $p^2 – 4 = 9$ $p^2 = 13$ n'a pas de solution entière
Donc q > 3, ce qui implique que 3q est le produit de 2 nombres premiers distincts.
p est impair, premier, non multiple de 3, donc p >3, donc $(p-2) \neq 1$ et $(p+2) \neq 1$
De par l'unicité de la décomposition en facteurs premiers, comme q > 3,
c'est que p-2 et p+2 sont des nombres premiers
et que p-2 = 3 et p+2 = q
Donc p = 5 et q = 7 (CN)
$5^2 – 3.7 – 1 = 25 – 21 – 1 = 3$ qui est bien premier (CS)
**(5,7) est la seule solution de ce cas.**

Les 4 cas sont exhaustifs. **Les seules solutions sont donc (3,2) et (5,7).**

**Pour un entier naturel n on note QP(n) le produit de ses chiffres et QS(n) la somme de ses chiffres.** ***580846***
**Montrer que tout entier naturel à 6 chiffres en base décimale satisfaisant QS(n) = QP(n) est divisible par 3.**

*Supposons qu'un entier n à 6 chiffres satisfaisant QP(n) = QS(n) ne soit pas divisible par 3.*
La règle de divisibilité par 3 nous indique qu'alors QS(n) n'est pas divisible par 3, donc QP(n) = QS(n) n'est pas divisible par 3. Alors aucun des chiffres de n n'est divisible par 3 et chacun des chiffres de n $\in \{1, 2, 4, 5, 7, 8\}$
Chacun des chiffres de n est $\equiv 1$ [3] ou est $\equiv 2$ [3]
Soit a le nombre de chiffres de n $\equiv 2$ [3] $a \in \{0, 1, 2, 3, 4, 5, 6\}$
n contient alors 6-a chiffres $\equiv 1$ [3]
$QP(n) \equiv 1^{6-a} . 2^a \equiv 2^a$ [3] et $QS(n) \equiv a.2 + (6-a).1 = a + 6 \equiv a$ [3] donc **$2^a \equiv a$ [3]** (CN)

| a | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| a [3] | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| $2^a$ [3] | 1 | 2 | 1 | 2 | 1 | 2 | 1 |

La CN n'est vérifiée que pour a=4 et a=5
n a donc au maximum 2 chiffres $\equiv 1$ [3].
Donc n contient au maximum 2 fois le chiffre 1 parmi ses 6 chiffres.
Soit g le plus grand des chiffres de n. Au moins 4 des chiffres de n, dont g, sont $\geq 2$
Alors $QS(n) \leq 6g$ et $QP(n) \geq 1.1.2^3.g = 8g$
Le nombre QS(n) = QP(n) ne peut pas simultanément être $\leq 6g$ et $\geq 8g$
La supposition de départ est donc fausse.

Tout entier n à 6 chiffres satisfaisant QP(n) = QS(n) est donc divisible par 3.

## REPRÉSENTATION DES NOMBRES

**Montrer qu'il n'y a pas de fonction polynomiale f(x) avec coefficients entiers tel que f(7)=11 et f(11)=13.**
Pour rappel, on a :
Si $a \equiv b\ [n]$, $f(a) \equiv f(b)\ [n]$ pour toute fonction polynomiale $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \quad a_i \in \mathbb{Z}$
Donc si $a - b \equiv 0\ [n]$, on doit avoir $f(a) - f(b) \equiv 0\ [n]$
$11-7 = 4 \equiv 0\ [4]$ mais $f(11)-f(7) = 13-11 = 2 \equiv 2\ [4]$ Contradiction.

**Quels nombres entiers peuvent s'écrire sous la forme $(a^2 + b^2) – (c^2 + d^2)$ avec a, b, c, d entiers ?**
Tous :
**Si n est impair** il existe k entier tel que n = 2k+1
Avec a = k+1 b = 1 c = k d = 1
nous avons $(a^2 + b^2) – (c^2 + d^2) = (k^2 + 2k + 1 + 1 ) – (k^2 + 1) = 2k + 1 = n$

**Si n est pair** il existe k entier tel que = 2k
Avec a = k+1 b = 0 c = k d = 1
nous avons $(a^2 + b^2) – (c^2 + d^2) = (k^2 + 2k + 1 + 0 ) – (k^2 + 1) = 2k = n$

**Combien a-t-on de zéros à la fin de 1000!**
Comme il y a beaucoup plus de 2 que de 5 dans une factorielle,
Chaque multiple de 5 apporte un zéro Il y en a 200
Chaque multiple de 25 apporte un zéro supplémentaire Il y en a 40
Chaque multiple de 125 apporte un zéro supplémentaire Il y en a 8
Chaque multiple de 625 apporte un zéro supplémentaire Il y en a 1
Soit au total 249 zéros

**On cherche les 2 derniers chiffres de 1! + 2! + 3! + … + 100!**
Pour $n \geq 10$ n! se termine par 2 zéros apportés par 2.5 et 10.
Donc les 2 derniers chiffres de 1! + 2! + 3! + … + 100! sont les mêmes que ceux de 1! + 2! + 3! + … + 9!
Les 6 premiers sont faciles à calculer de tête : 1 2 6 24 120 720
$7! = 7.720 \equiv 7.20 = 140 \equiv 40\ [100]$ $8! \equiv 8.40 = 320 \equiv 20\ [100]$ $9! \equiv 9.20 = 180 \equiv 80\ [100]$
Les deux derniers chiffres sont $\equiv 1 + 2 + 6 + 24 + 20 + 20 + 40 + 20 + 80 \equiv 13\ [100]$

*Pour les 3 derniers chiffres il faut aller jusqu'à 14!*
*Pour les 4 derniers chiffres il faut aller jusqu'à 19!*
*En allant jusqu'à 24! on a les 6 derniers chiffres – car $25 = 5^2$ nous donne 2 zéros d'un coup.*

**On cherche le reste de la division euclidienne de 1! + 2! + 3! + … + 100! par 7**
Pour tout $n \geq 7$, n ! est un multiple de 7 donc $n! \equiv 0[7]$
Donc $1! + 2! + 3! + \dots + 100! \equiv 1! + 2! + \dots + 6! = 873 \equiv 5\ [7]$

## RESTKLASSEN

**In jeder Menge von 5 natürlichen Zahlen gibt es zwei, deren Summe oder Differenz durch 7 teilbar ist.**
Es gibt 7 Restklassen. Wir ordnen paarweise ($R_1$, $R_6$), ($R_2$, $R_5$), ($R_3$, $R_4$). ★★★
Die Summe der Restklassen eines Paares ist $R_0$.
Wenn 2 der 5 Zahlen derselben Restklasse modulo 7 angehören, ist ihre Differenz durch 7 teilbar.
Wenn das nicht der Fall ist, gehören sie 5 verschiedenen Restklassen an. Eine davon könnte $R_0$ sein.
Es bleiben also mindestens 4 verschiede Restklassen ungleich $R_0$ übrig, die in den 3 Paaren vorkommen.
Mindestens 2 davon bilden ein Paar. Ihre Summe ist $R_0$.
Die beiden Zahlen aus diesen beiden Restklassen haben also eine Summe, die durch 7 teilbar ist.

*Das gilt für 4 Zahlen nicht: sie könnten den Restklassen $R_0$, $R_1$, $R_2$ und $R_3$ angehören.*

**Among 5 integers, there are always 3 with sum divisible by 3.** ★★☆
We consider three boxes 0, 1, 2.
We put a number n in box b so that $n \equiv b\ [3]$.
One of the following 2 configurations must be true:
a) There are 3 numbers in one box. Their sum is $\equiv 3b \equiv 0\ [3]$.
b) There is 1 number in each box. Their sum is $\equiv 0 + 1 + 2 \equiv 0\ [3]$.

**On cherche le plus petit $n \in \mathbb{N}$ tel que $n \equiv 9\ [10]$ ; $n \equiv 8\ [9]$ ; $n \equiv 7\ [8]$ ; … ; $n \equiv 1\ [2]$** ★★☆

$n \equiv 9\ [10]$ ; $n \equiv 8\ [9]$; $n \equiv 7\ [8]$; $n \equiv 6\ [7]$; $n \equiv 5\ [6]$; $n \equiv 4\ [5]$; $n \equiv 3\ [4]$; $n \equiv 2\ [3]$; $n \equiv 1\ [2]$
est équivalent à
$n \equiv -1\ [10]$ ; $n \equiv -1\ [9]$; $n \equiv -1\ [8]$; $n \equiv -1\ [7]$; $n \equiv -1\ [6]$; $n \equiv -1\ [5]$; $n \equiv -1\ [4]$; $n \equiv -1\ [3]$; $n \equiv -1\ [2]$

Quand $n \equiv -1\ [8]$ on a automatiquement $n \equiv -1\ [4]$ et $n \equiv -1\ [2]$ car $n = 8k - 1 = 4(2k) - 1 = 2(4k) - 1$
Quand $n \equiv -1\ [9]$ on a automatiquement $n \equiv -1\ [3]$ car $n = 9k - 1 = 3(3k) - 1$
**Plus généralement si $n \equiv -1$ [une puissance de p] alors $n \equiv -1$ [toutes les puissances plus petites de p]**

Pour un entier n si $n \equiv k\ [p]$, $n \equiv k\ [q]$ et $p \wedge q = 1$, alors $n \equiv k\ [p.q]$
En particulier si $n \equiv -1\ [p]$, $n \equiv -1\ [q]$ et $p \wedge q = 1$, alors $n \equiv -1\ [p.q]$
Donc - Quand $n \equiv -1\ [2]$ et $n \equiv -1\ [3]$ on a automatiquement $n \equiv -1\ [6]$
- Quand $n \equiv -1\ [2]$ et $n \equiv -1\ [5]$ on a automatiquement $n \equiv -1\ [10]$

Donc n a seulement besoin de remplir les conditions $n \equiv -1\ [9]$; $n \equiv -1\ [8]$; $n \equiv -1\ [7]$; $n \equiv -1\ [5]$
Soit $n \equiv -1\ [5.7.8.9]$
**$n \equiv -1\ [2520]$**
**Le plus petit est n = 2519**
n= ppcm(2, 3, …, 10) - 1 = 2.3.2.5.7.2.3 – 1 = 2519

**Jede positive ganze Zahl k besitzt ein positives Vielfaches der Form 9999..99000..00**
Für ein gegebenes k, wir betrachten den Rest der Division der 10i ($i \in \mathbb{N}$) durch k.
$\forall\ i \in \mathbb{N}$ es gibt maximal k verschiedene Resten.
In einer Menge von mindestens 2k unterschiedliche Zehnerpotenzen gibt es also mindestens zwei mit dem gleichen Rest in der Division durch k.
Die Differenz dieser zwei Zehnerpotenzen ist dann durch k teilbar.
Zum Beispiel, die Menge $\{10^k, 10k^{+1}, \ldots, 10^{3k}\}$ beinhaltet 2k+1 unterschiedliche Zehnerpotenzen.
Somit hat man bewiesen: $\forall\ k \in \mathbb{N}, \exists\ r,t \in \mathbb{N},\ k \leq r < r+t \leq 3k$ und $10^{r+t} - 10^r$ ist ein Vielfaches von k.
$10^{r+t} - 10^r$ est de la forme 99…9900…00
*t* *r*

## CARRÉ OU PAS CARRÉ ?

**Un nombre A ayant 666 fois le nombre 6 suivis de plusieurs 0 peut-il être un carré ?**
Pour commencer, si un nombre se termine par 0, son carré se termine par 00.
Si un nombre se termine par n zéros, son carré se termine par 2n zéros.
**Plus généralement, si un carré se termine par des zéros, ce nombre de zéros est pair.**
Donc si A a un nombre impair de zéros après les six il n'est pas un carré.
Assumons un nombre pair de zéros.
Considérons le nombre A' qui est A sans les zéros. $A=A'.10^{2n} = A'.(10^n)^2$ alors A est un carré si A' est un carré.
A' a 666 fois le nombre six.
Soit B tel que A'=2B. B a 666 fois le nombre trois.
B est donc impair et A' = 2 fois un nombre impair n'a le facteur 2 qu'une seule fois : il ne peut pas être un carré.

Évidemment 666 fois le nombre six c'était pour rigoler. Quel que soit le nombre de six, 66666… n'est pas un carré.
Par le même raisonnement 222222… 10101010… 14141414… 18181818… n'est pas un carré.

**Un nombre à 9 chiffres contenant tous les chiffres sauf 0 et se terminant par 5 peut-il être un carré ?**
Si le nombre a 9 chiffres et que les chiffres de 1 à 9 sont tous représentés c'est que chacun est représenté une et une seule fois. Soit D un tel nombre. $D=A^2$
On peut écrire A=10a+5 $D = A^2 = 100a^2 + 100a + 25 = 100a(a+1) + 25$
Les deux derniers chiffres de D doivent donc être 2 et 5.

Le chiffre des milliers de D (le 3eme chiffre de D en partant de la droite) est le chiffre des unités de a(a+1)

| a [10] | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| a(a+1) [10] | 0 | 2 | 6 | 2 | 0 | 0 | 2 | 6 | 2 | 0 |

Les seules possibilités sont 0, 2 ou 6. Mais D ne contient pas 0 et 2 est utilisé pour le chiffre des dizaines de D donc le chiffre des milliers est 6.

On peut écrire $D = 1000b+625 = 125(8b+5) = 5^3(8b+5)$ donc $5^3 \mid D$ mais comme D est un carré on doit avoir $5^4 \mid D$
Donc 5 doit diviser 8b+5. Le chiffre des unités de b qui est le $4^{ème}$ chiffre de D depuis la droite doit donc être 0 ou 5.
Mais D ne contient pas 0 et 5 est déjà utilisé pour le chiffre des unités de D.
Donc ce n'est pas possible et un tel nombre D ne peut pas être un carré.

**Pourquoi un carré ne se termine jamais par 2, par 3, par 7, ni par 8 ?**
Si un nombre se termine par x son carré se termine par y
(x ; y) (0 ; 0) (1 ;1) (2 ;4) (3 ;9) (4 ;6) (5 ;5) (6 ;6) (7 ;9) (8 ;4) (9 ;1)
Donc un carré ne se termine jamais par 2, jamais par 3, jamais par 7 et jamais par 8.

**Les puissances de 2 peuvent se terminer seulement par 0, 1, 4, 5, 6 ou 9.**

**Les puissances de 3 peuvent se terminer par n'importe quel chiffre !**

**Les puissances de 4 peuvent se terminer seulement par 0, 1, 5 ou 6.**

| Nombre (n) \ Puissance (p) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 6 | 2 | 4 | 8 | 6 | 2 | 4 |
| 3 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 | 9 |
| 4 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 | 7 | 9 |
| 8 | 8 | 4 | 2 | 6 | 8 | 4 | 2 | 6 | 8 | 4 |
| 9 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Somme | 45 | 45 | 45 | 33 | 45 | 45 | 45 | 33 | 45 | 45 |

**Montrer que le carré d'un nombre impair est un multiple de 8 plus 1.**
*Autre formulation*
**$n \equiv 1\ [2] \Rightarrow n^2 \equiv 1\ [8]$**

Pout tout nombre impair $z \equiv \{1, 3, 5, 7\}\ [8]$ $z^2 \equiv \{1^2, 3^2, 5^2, 7^2\}\ [8]$
$z^2 \equiv \{1, 9, 25, 49\}\ [8]$ $z^2 \equiv \{1, 1, 1, 1\}\ [8]$
$z^2 \equiv 1\ [8]$
*Donc le carré d'un nombre impair est un multiple de 8 plus 1* **C'est une identité remarquable**

*Autre démonstration :*
Si $n \equiv 1\ [2]$ alors il existe k tel que $n= 2k+1$ et $n^2 = 4k^2 + 4k + 1 = 4.k.(k+1) + 1$
Comme k et k+1 sont consécutifs, l'un d'eux est pair.
Alors $4.k(k+1) \equiv 0\ [8]$ et $n^2 = 4.k.(k+1) + 1 \equiv 1\ [8]$

★★☆

**De 9, 99, 999, 9999… lesquels sont des carrés ?**
9 est un carré 99 = 9.11 n'est pas un carré
Tous les autres : 999 = 1000-1 = 8.125 -1 ≡ -1 [8] 9999 = 1000-1 = 8.1250 -1 ≡ -1 [8] 9999… ≡ -1 [8]
sont de la forme 8k-1 et ne sont donc pas des carrés (il faudrait qu'ils soient de la forme 8k+1).

**Montrer que 3n-1, 5n+2, 5n-2, 7n-1, 7n-2 et 7n+3 ne sont pas des carrés**
$3n-1 \equiv -1\ [3]$ mais pour tout a, $a^2 \equiv 0$ ou $1\ [3]$ *donc 3n-1 ne peut pas être un carré*.

$5n+2 \equiv 2\ [5]$ mais pour tout $a=10u+v$ $(v<10)$, $a^2 \equiv 100u^2+20uv+v^2 \equiv v^2\ [5]$
On considère les paires $(v,v^2)$ :
(0 ; 0) (1 ;1) (2 ;4) (3 ;9) (4 ;16) (5 ;25) (6 ;36) (7 ;49) (8 ;64) (9 ;81)
Et $v^2 \equiv 0$, 1 ou -1 [5] mais jamais 2 [5]

Pareil pour 5n-2 : on n'a jamais $v^2 \equiv -2\ [5]$

De même $v^2 \equiv 0, 1, 4, 2, 2, 1, -1, 0, -1, 4$ donc 0, 1, 2, 4 ou -1 [7] mais on n'a jamais $v^2 \equiv 3\ [7]$ ou $5=-2\ [7]$ ou -1 [7]
*Donc 7n-1, 7n-2 et 7n+3 ne sont pas des carrés*

**Montrer que pour p premier >3, $p^2 \equiv 1\ [24]$**
p étant premier >3, il est impair et on a vu ci-dessus que $p^2 \equiv 1\ [8]$
On a aussi p non multiple de 3 donc $p \equiv -1$ ou $1\ [3]$ et $p^2 \equiv 1\ [3]$
Donc $p^2 \equiv 1\ [24]$

# ÉQUATIONS DIOPHANTIENNES

## TRIPLETS DE PYTHAGORE

Un carré somme de deux carrés satisfaisant $a^2 + b^2 = c^2$ est un triplet de Pythagore car il existe alors un triangle rectangle dont les côtés sont de longueur a, b et c.

**Il y a une infinité de triplets de Pythagore**

(3,4,5) est le plus petit. Mais on a aussi (5,12,13) ;(7,24,25) ; (8,15,17) ; (9,40,41) ; (11,60,61)…

Pour un triplet donné (a,b,c), tous les triplets (ka, kb, kc) fonctionnent aussi : quand on en a un, on peut en construire une infinité d'autres.

On peut aussi construire un triplet à partir de 2 nombres quelconques u et v : $(a,b,c) = (u^2 - v^2, 2uv, u^2 + v^2)$

**Montrer que pour tout triplet de Pythagore (tel que $a^2 + b^2 = c^2$) : $a.b.c \equiv 0\ [60]$** ★★☆

On va montrer que $a.b.c \equiv 0\ [3]$, $a.b.c \equiv 0\ [4]$ et $a.b.c \equiv 0\ [5]$

*[4]*

- Si $a^2$ et $b^2$ sont impairs, la somme de 2 impairs est paire donc $c^2$ ne peut pas être impair.

*Donc a, b et c ne sont pas tous impairs.*

- Si $a^2$ et $b^2$ sont impairs et $c^2$ est pair on aurait $a^2 + b^2 \equiv 1 + 1 \equiv 2\ [4]$ et $c^2 \equiv 0[4]$ Cas impossible

*Donc a et b impairs est impossible, quelle que soit la parité de c.*

- Si $a^2$ et $b^2$ sont pairs, $c^2$ est pair : a, b et c sont tous pairs, $abc \equiv 0\ [8]$ et à fortiori **$a.b.c \equiv 0\ [4]$**
- Si $a^2$ est pair et $b^2$ est impair ou vice versa, alors $c^2$ est impair. Disons que a est le nombre pair ; b et c impairs.

$a = 2k$ $b = 2m + 1$ $c = 2n + 1$ $a^2 = c^2 - b^2$

$4k^2 = 4n^2 + 4n + 1 – 4m^2 -4m -1$

$4k^2 = 4(n^2 + n – m^2 -m)$

$k^2 = n^2 + n – m^2 -m$

$k^2 = n(n+1) – m(m+1)$

Comme n et n+1 se suivent n(n+1) est pair ; de même m(m+1) est pair

Donc $k^2$ est pair et k est pair.

Comme a = 2k et k est pair alors **$a \equiv 0\ [4]$** et **$a.b.c \equiv 0\ [4]$**

*[3]*

Si un nombre m ne divise pas 3, alors $m \equiv \pm 1\ [3]$ et $m^2 \equiv 1\ [3]$

Donc si ni a, ni b, ni c ne divisent 3 on aurait $a^2 + b^2 \equiv 2\ [3]$ et $c^2 \equiv 1\ [3]$

Contradiction. L'un d'eux doit diviser 3 et donc **$a.b.c \equiv 0\ [3]$**

*[5]*

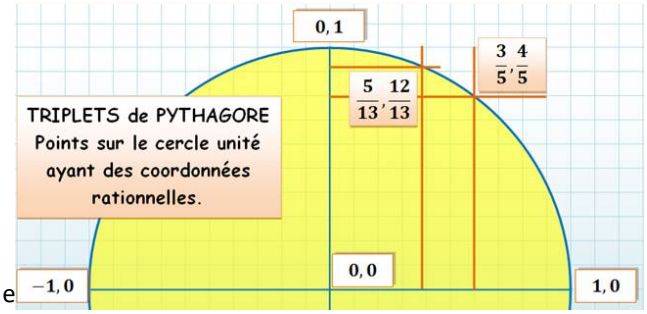
Si un nombre m ne divise pas 5, soit $m \equiv \pm 1\ [5]$ ; soit $m \equiv \pm 2\ [5]$

donc soit $m^2 \equiv 1\ [5]$ ; soit $m^2 \equiv 4 \equiv -1\ [5]$

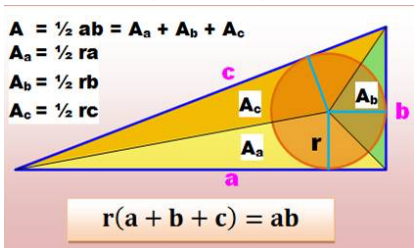
ce qui s'écrit $m^2 \equiv \pm 1\ [5]$

Donc si ni a, ni b, ni c ne divisent 5 on aurait $a^2 + b^2 \equiv 0, 2$ ou $-2\ [5]$ et $c^2 \equiv 1$ ou $-1\ [5]$

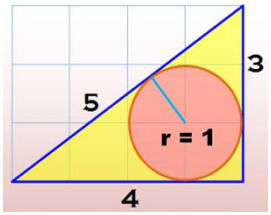
Contradiction. L'un d'eux doit diviser 5 et donc **$a.b.c \equiv 0\ [5]$**




Dans un triangle rectangle




Pour le triplet (3,4,5), le cercle inscrit



## Équations diophantiennes ax + by = c

Considérons l'équation (E) $ax + by = c$ où $a, b, c \in \mathbb{Z}$

1. L'équation (E) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $a \wedge b \mid c$

2. Si $a \wedge b \mid c$ alors il existe une infinité de solutions entières. Elles s'écrivent sous la forme $(x, y) = (x_0 + \alpha k, y_0 + \beta k)$ avec $x_0, y_0, \alpha, \beta \in \mathbb{Z}$ fixés et k parcourant $\mathbb{Z}$.

Le premier point est une conséquence du théorème de Bézout.
Voyons sur un exemple comment prouver le second point et calculer explicitement les solutions :

**Trouver les solutions entières de 161x + 368y = 115**

• ***Première étape : y a-t-il des solutions ?***

On effectue **l'algorithme d'Euclide** pour calculer le pgcd de a = 161 et b = 368.

$368 = 161 \times 2 + 46$
$161 = 46 \times 3 + 23$
$46 = 23 \times 2 + 0$

Donc $368 \wedge 161 = 23$. Comme $115 = 5 \times 23$ on a bien $368 \wedge 161 \mid 115$.

Le théorème de Bézout nous dit que l'équation (E) admet des solutions entières.

• ***Deuxième étape : trouver une solution particulière***

On effectue la **remontée de l'algorithme d'Euclide** pour calculer les coefficients de Bézout.

$368 = 161 \times 2 + 46$
$161 = 46 \times 3 + 23$
$46 = 23 \times 2 + 0$

$23 = 161 \times 7 + 368 \times (-3)$
$23 = 161 - 3\,(368 - 2 \times 161)$
$23 = 161 - 3 \times 46$

On a trouvé $161.7 + 368.(-3) = 23$.

Comme $115 = 5.23$ on obtient en multipliant par 5 : $161.35 + 368.(-15) = 115$

Ainsi $(x_0, y_0) = (35, -15)$ est une solution particulière de (E).

• ***Troisième étape : recherche de toutes les solutions***

Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E). Nous savons que $(x_0, y_0)$ est aussi solution. Ainsi :

$161\,x + 368\,y = 115$
$-\quad 161\,x_0 + 368\,y_0 = 115$

$161.(x - x_0) + 368.(y - y_0) = 0$ >> Ne pas remplacer $x_0$ et $y_0$ par leurs valeurs

$23.7.(x - x_0) + 23.16.(y - y_0) = 0$ >> On simplifie par $23 = 161 \wedge 368$

$7(x - x_0) = -16(y - y_0)$ $(*)$ Attention : cette simplification est nécessaire, sinon la suite est fausse

Donc $7 \mid 16(y - y_0)$. Par ailleurs $7 \wedge 16 = 1$ donc par le lemme de Gauss $7 \mid y - y_0$.

Il existe donc $k \in \mathbb{Z}$ tel que $y - y_0 = 7k$

On insère ce résultat dans $(*)$ : $7(x - x_0) = -16.7k$

$x - x_0 = -16k$ (c'est le même k pour x et pour y)

Nous avons donc $(x, y) = (x_0 - 16k, y_0 + 7k)$

Tout couple de cette forme est solution de (E).

On substitue $(x_0, y_0)$ par sa valeur et nous obtenons :

Les solutions entières de $161\,x + 368\,y = 115$ sont les $(x, y) = (35 - 16k, -15 + 7k)$, $k \in \mathbb{Z}$.

**Montrer que l'équation $a^2 + b^2 + c^2 = 2abc$ n'a pas de solution entière autre que (0,0,0).**

***Première solution***

Soit $k \geq 0$ tel que $2^k$ soit la plus grande puissance de 2 qui divise a, b et c.
Alors $a = 2^k u$ $b= 2^k v$ $c = 2^k w$ et l'équation s'écrit $2^{2k}u^2 + 2^{2k}v^2 + 2^{2k}w^2 = 2^{3k+1}uvw$
On simplifie par $2^{2k}$ $u^2 + v^2 + w^2= 2^{k+1} uvw$
$2^{k+1}uvw$ est pair donc $u^2 + v^2 + w^2$ doit aussi l'être.
k est défini de telle sorte que $u^2$, $v^2$ et $w^2$ ne peuvent pas être tous pair. Au moins un d'eux doit être impair.
Comme la somme des trois carrés doit être paire, cela implique qu'exactement deux des 3 carrés sont impairs.
Disons que $u^2$et $v^2$ sont impairs et que $w^2$ est pair. Il doit alors exister z tel que w=2z.
$u^2 + v^2 + w^2= 2^{k+1} uvw$ devient
$u^2 + v^2 = -w^2+ 2^{k+1} uvw = -4z^2 + 2^{k+2}uvz = -4z^2 + 4.2^kuvz \equiv 0$ [4] (@)
Mais $u^2$ et $v^2$ impairs implique u impair et v impair.
Pour tout nombre impair $u \equiv \{1, 3\}$ [4]
$u \equiv \{1, -1\}$ [4]
$u^2 \equiv \{1^2, (-1)^2\}$ [4]
$u^2 \equiv 1$ [4]
Donc $u^2 + v^2 \equiv 2$ [4] → contradiction avec (@) : $u^2 + v^2 \equiv 0$ [4]
L'équation n'a donc pas de solution entière.

***Deuxième solution – MÉTHODE DE DESCENTE INFINIE (type de raisonnement formalisée par Fermat, un peu entre le raisonnement par récurrence et le raisonnement par l'absurde)***

Dans $a^2 + b^2 + c^2$ soit 1 terme est pair soit chacun des 3 termes est pair.
Si un seul terme est pair, alors 2abc est divisible par 4, mais $a^2 + b^2 + c^2$ est seulement divisible par 2. Contradiction.
Donc chacun des 3 carrés doit être pair.
Alors $a=2a_1$ $b=2b_1$ $c=2c_1$ et $a_1^2 + b_1^2 + c_1^2 = 4a_1b_1c_1$
De même $a_1=2a_2$ $b_1=2b_2$ $c_1=2c_2$ et $a_2^2 + b_2^2 + c_2^2 = 8a_2b_2c_2$
$a = 2a_1 = 2^2a_2 = \dots = 2^na_n$
$b = 2b_1 = 2^2b_2 = \dots = 2^nb_n$
$c = 2c_1 = 2^2c_2 = \dots = 2^nc_n$
Donc si (a,b,c) est solution, alors a, b et c sont chacun divisibles par $2^n$ quel que soit n. Pas possible.

**Trouver tous les nombres premiers p, q tels que $p^2 - 2q^2 = 1$**

p ne peut pas être nul. Prenons p > q
$-2q^2$ est pair donc $p^2$ est impair et p est impair.

Il existe une solution : (1 ; 0) à rejeter car 1 n'est pas premier
(3 ; 2) fonctionne
(5 ; q) ne fonctionne pas
Pour p premier > 5 on aura $q^2 > 12$ et donc q > 3
Pour p,q > 3 p est impair . Comme q doit être premier et >3, q est aussi impair : $p, q \equiv 1$ ou -1 [3]
Alors $p^2 - 2q^2 \equiv 1 - 2 = -1$ [3]
$1 \equiv -1$ [3] : contradiction avec l'égalité recherchée.
Il n'y a donc aucune solution pour p,q > 3 et la seule solution est (3 ; 2).

**Pour (a, b) $\in \mathbb{N}^2$, p premier, quelle forme ont a et b en fonction de p pour satisfaire $\frac{1}{a}+\frac{1}{b}=\frac{1}{p}$**

1/a < 1/p donc a > p et 1/b < 1/p donc b > p
On peut alors écrire a= p + r et b = p + s avec r et s entiers positifs.

$$\frac{1}{a}+\frac{1}{b}=\frac{1}{p} \Leftrightarrow \frac{1}{p+r}+\frac{1}{p+s}=\frac{1}{p} \Leftrightarrow \frac{p(p+s)}{p(p+r)(p+s)}+\frac{p(p+r)}{p(p+r)(p+s)}=\frac{(p+r)(p+s)}{p(p+r)(p+s)}$$
$$\Rightarrow p^2+ps+p^2+pr=p^2+pr+ps+rs \Rightarrow p^2=rs$$

Comme p est premier, les seules solutions possibles pour (r,s) sont $(1,p^2)$ ; (p,p) ou $(p^2,1)$
Les seules solutions pour (a,b) = (p+r, p+s) sont $(p+1, p+p^2)$ ; (2p, 2p) ou $(p+p^2, p+1)$

## COEFFICIENTS DE BEZOUT

**Montrer pourquoi a = bq+r $\Rightarrow$ a $\wedge$ b = b $\wedge$ r** (la base de l'algorithme d'Euclide pour calculer a $\wedge$ b)

- Si b et r sont divisibles par c alors b ≡ 0 [c] donc bq ≡ 0 [c] et r ≡ 0 [c] $\Rightarrow$ bq + r = a ≡ 0 [c]
  Donc si un nombre est diviseur de b et de r, il est aussi diviseur de a (et de b)
- Si a et b sont divisibles par d alors b ≡ 0 [d] donc -bq ≡ 0 [d] et a ≡ 0 [d] $\Rightarrow$ -bq + a = r ≡ 0 [d]
  Donc si un nombre est diviseur de a et de b, il est aussi diviseur de r (et de b)

  $\mathcal{D}$(a)$\cap\mathcal{D}$(b) = $\mathcal{D}$(b)$\cap\mathcal{D}$(r) $\Rightarrow$ max ($\mathcal{D}$(a)$\cap\mathcal{D}$(b)) =max ($\mathcal{D}$(b)$\cap\mathcal{D}$(a-b)) $\Rightarrow$ a $\wedge$ b = b $\wedge$ r

CALCUL DES COEFFICIENTS DE BEZOUT PAR L'ALGORITHME D'EUCLIDE

Comme on a vu : a = bq+r $\Rightarrow$ a $\wedge$ b = b $\wedge$ r

| **Exemple** | **a = 19** | **b = 7** | | |
|---|---|---|---|---|
| $a = bq_1 + c$ | $19 = 7.2 + 5$ | $q_1 = 2$ | $c = 5$ | $c = a - 2b$ |
| $b = cq_2 + d$ | $7 = 5.1 + 2$ | $q_2 = 1$ | $d = 2$ | $d = b - c$ |
| $c = dq_3 + e$ | $5 = 2.2 + 1$ | $q_3 = 2$ | $e = 1$ | $1 = c - 2d$ |



donc 1=-2b+3(a-2b)=3a-8b : 1= 3.19 – 8.7
donc 1 = c-2(b-c) = -2b+3c

# GESCHICHTE DER ZAHLENTHEORIE

### Zahlentheorie in der Antike und im Mittelalter

Die ersten schriftlichen Nachweise der Zahlentheorie reichen bis ca. 2000 v. Chr. zurück. Die Babylonier und Ägypter kannten in dieser Zeit bereits die Zahlen kleiner als eine Million, die Quadratzahlen und einige pythagoreische Tripel.

Die systematische Entwicklung der Zahlentheorie begann jedoch erst im ersten Jahrtausend v. Chr. im antiken Griechenland. Herausragendster Vertreter ist **Euklid** (ca. 300 v. Chr.), der die von Pythagoras erfundene Methode des mathematischen Beweises in die Zahlentheorie einführte. Sein berühmtestes Werk, Euklids Elemente - bis in das 18te Jahrhundert als Standardlehrbuch für Geometrie und Zahlentheorie verwendet - beschäftigt sich unter anderem mit der Definition der Primzahl, einem Verfahren zur Berechnung des größten gemeinsamen Teilers (Euklidischer Algorithmus) und dem Beweis der Existenz unendlich vieler Primzahlen (Satz von Euklid).

Im dritten Jahrhundert beschäftigte sich als Erster der griechische Mathematiker **Diophantos von Alexandria** mit den nach ihm später benannten Gleichungen, die er mit linearen Substitutionen auf bekannte Fälle zu reduzieren versuchte. Diophants Hauptwerk sind die Arithmetika.

Die Griechen warfen viele wichtige arithmetische Fragestellungen auf, die zum Teil bis heute ungelöst sind, wie z.B. das Problem der Primzahlzwillinge und das der vollkommenen Zahlen, oder deren Lösungen viele Jahrhunderte in Anspruch nahmen.

Mit dem Untergang der griechischen Staaten erlosch auch die Blütezeit der Zahlentheorie in Europa. Aus dieser Zeit ist nur der Name des Leonardo di Pisa (**Fibonacci**, ~ 1200) nennenswert, der sich neben Zahlenfolgen und der Auflösung von Gleichungen durch Radikale auch mit diophantischen Gleichungen befasste.

#### Zahlentheorie in der frühen Neuzeit

Der erste wichtige Vertreter der Zahlentheorie der Neuzeit war **Pierre de Fermat** (1607–1665). Er stellte den **kleinen Satz von Fermat** auf, untersuchte die Darstellbarkeit einer Zahl als **Summe zweier Quadrate** und erfand die **Methode des unendlichen Abstiegs**, mit der er den von ihm aufgestellten **großen Satz von Fermat** im Fall n=4 lösen konnte. Der Versuch einer allgemeinen Lösung des großen Satzes inspirierte die Methoden der Zahlentheorie bis in die Moderne.

Das 18. Jahrhundert der Zahlentheorie wird vor allem von drei Mathematikern beherrscht: **Leonhard Euler** (1707–1783), **Joseph-Louis Lagrange** (1736–1813) und **Adrien-Marie Legendre** (1752–1833).

**Eulers** Gesamtwerk ist sehr umfangreich. Er führte die analytischen Methoden in die Zahlentheorie ein und fand einen neuen Beweis für die Unendlichkeit der Menge der Primzahlen. Er erfand die zahlentheoretischen Funktionen, insbesondere die Eulersche **ϕ-Funktion**, untersuchte Partitionen und betrachtete bereits 100 Jahre vor Bernhard Riemann die Riemannsche **Zeta-Funktion**. Er entdeckte das **quadratische Reziprozitätsgesetz**, zeigte, dass die **eulersche Zahl e** irrational ist und löste den großen Satz von Fermat im Fall n=3.

**Lagrange** bewies den **Satz von Wilson**, begründete die systematische Theorie der **Pellschen Gleichung** und die Theorie der quadratischen Formen, die erst in der ersten Hälfte des 20. Jahrhunderts ihren Abschluss fand.

**Legendre** führte das Legendre-Symbol in die Zahlentheorie ein und formuliert das quadratische Reziprozitätsgesetz in seiner heutigen Form. Sein Beweis verwendet allerdings die Unendlichkeit der Menge der Primzahlen in arithmetischen Progressionen, die erst im Jahre 1832 von Lejeune Dirichlet bewiesen wurde.

Die nächste große Zäsur in der Geschichte der Zahlentheorie wird durch das Wirken von **Carl Friedrich Gauß** (1777–1855) bestimmt. Gauß gab als Erster (sechs verschiedene) vollständige Beweise für das quadratische Reziprozitätsgesetz. Er entwickelte Legendres Theorie der quadratischen Formen weiter und baute sie zu einer vollständigen Theorie aus. Er schuf die Arithmetik der quadratischen Zahlkörper. Auf diese Weise fand er das Zerlegungsgesetz der Primzahlen in Z[i], den gaußschen Zahlen. Ebenso untersuchte er zuerst die **Kreisteilungskörper**, d. h. die Lösungen der Gleichung $x^{p-1}=1$, und entwickelte den Kalkül der Gaußschen Summen. Er entdeckte den gaußschen Primzahlsatz. Die Zahlentheorie ist erst durch Gauß eine selbständige und systematisch geordnete Disziplin geworden.

#### Das 19. Jahrhundert

Das 19. Jahrhundert ist eine Blütezeit der analytischen Zahlentheorie. Unter Niels Henrik **Abel** (1802–1829), Carl Gustav **Jacobi** (1804–1851), Gotthold **Eisenstein** (1823–1852) und Peter Gustav **Lejeune Dirichlet** (1805–1859) wird die Theorie der **elliptischen Funktionen** entwickelt. Dirichlet erfindet den Begriff der **L-Reihe** und beweist damit den Primzahlsatz in arithmetischen Progressionen. Dirichlet und Eisenstein verwenden die Theorie der Modulformen, um die Anzahl der Darstellungen einer Zahl als Summe von vier bzw. fünf Quadraten zu untersuchen. Der **Einheitensatz** von Dirichlet ist heute einer der Grundpfeiler der algebraischen Zahlentheorie.

Bernhard **Riemann** (1826–1866) entdeckte und bewies die Funktionalgleichung der Riemannschen **Zeta-Funktion** und stellte tiefgreifende Vermutungen auf, die die analytische Eigenschaften dieser Funktion mit der Arithmetik in Verbindung brachten.

Sehr bedeutsam für die gesamte Mathematik war das kurze Wirken von Évariste **Galois** (1811–1832), der die **Galoistheorie** entwickelte und damit viele alte Fragen, wie die Quadratur des Kreises, die Konstruktion von n-Ecken mittels Zirkel und Lineal und die Auflösbarkeit von Polynomgleichungen durch Wurzelausdrücke klärte. Die Galoistheorie spielt heute in der Zahlentheorie eine exponierte Rolle.

In der algebraischen Schule des 19. Jahrhunderts sind vor allem Ernst Eduard **Kummer** (1810–1893), Leopold **Kronecker** (1823–1891) und Richard **Dedekind** (1831–1916) zu nennen. Diese begründeten zusammen die Eckpfeiler der modernen strukturellen Auffassung der Algebra, insbesondere die **Theorie der Gruppen, Ringe, Ideale und der algebraischen Zahlkörper**. Kronecker führte den Begriff eines Divisors ein und entdeckte die heute als **Satz von Kronecker-Weber** genannten Formel, wonach jede abelsche Erweiterung des rationalen Zahlkörpers in einem Kreisteilungskörper enthalten ist. Kummer bewies den großen Satz von Fermat für alle regulären Primzahlen, und Dedekind zeigte die Existenz von Ganzheitsbasen in Zahlkörpern.

**Das 20. Jahrhundert und die Moderne**

Das 20. Jahrhundert brachte der Zahlentheorie endlich einige Lösungen, nach denen so lange geforscht wurde:

- Die komplette Lösung der zu einer quadratischen Form gehörenden Diophantischen Gleichung.
- Mit Klassenkörpertheorie und Iwasawatheorie eine keineswegs vollständige, aber strukturell befriedigende Beschreibung der abelschen und zyklischen Zahlkörper, die zu einem allgemeinen Reziprozitätsgesetz für beliebige Potenzreste führte, dem **Artinschen Reziprozitätsgesetz**.
- Die noch unbewiesene Lösung der zu elliptischen Kurven gehörenden Diophantischen Gleichung.

Bahnbrechend war die Entdeckung der p-adischen Zahlen durch Kurt **Hensel**. Aufbauend auf seinen Arbeiten konnten Hermann **Minkowski** und Helmut **Hasse** das Problem der quadratischen Formen lösen: eine quadratische Form hat genau dann eine rationale Nullstelle, wenn sie eine Nullstelle in jedem Körper Q besitzt. Der **Satz von Hasse-Minkowski** liefert ein erstes Beispiel für ein Lokal-Global-Prinzip.

Aufbauend auf den Arbeiten von Kummer wurde die Klassenkörpertheorie am Anfang des 20. Jahrhunderts von einer Reihe von Mathematikern entwickelt, vor allem David **Hilbert**, Helmut Hasse, Philipp **Furtwängler**, Teiji **Takagi** und Emil **Artin**, wobei Takagi den Existenzsatz bewies, aus dem **Artin** sein Reziprozitätsgesetz ableitete. Eine komplette Berechnung des Hilbertsymbols und damit die praktische Anwendung des Reziprozitätsgesetzes, gab erst Helmut **Brückner** in der zweiten Hälfte des 20 Jahrhunderts. In die moderne Sprache der **Gruppenkohomologie**, abstrakten harmonischen Analysis und Darstellungstheorie wurde die **Klassenkörpertheorie** von John **Tate** und Robert **Langlands** übersetzt. Langlands vermutete weitgehende Verallgemeinerungen der Klassenkörpertheorie und legte so den Grundstein für das Langlands-Programm.

Für die bessere Erklärung **zyklotomische Körper** (Kreisteilungskörper) entwickelte Kenkichi **Iwasawa** die Iwasawa-Theorie. Mit diesen Körpern werden gewisse p-adische L-Reihen verknüpft. Die Hauptvermutung der Iwasawatheorie, die die verschiedenen Möglichkeiten diese L-Reihen zu definieren für äquivalent erklärt, wurde für total-reelle Zahlkörper von Barry **Mazur** und Andrew **Wiles** am Ende der 1980er Jahren bewiesen.

Louis **Mordell** vermutete, dass für Kurven des Geschlechts >1 die Menge der rationalen Punkte immer endlich ist. Dies bewies Gerd **Faltings**, wofür er 1986 die Fields-Medaille bekam. Damit war gezeigt, dass die Gleichung des großen Satzes von Fermat höchstens endlich viele Lösungen haben konnte (der Satz sagt, dass es gar keine gibt).

Der **Modularitätssatz** wurde 1995 durch Andrew Wiles für die meisten elliptischen Kurven bewiesen. Daraus geht insbesondere hervor, dass der große Satz von Fermat wahr ist.

Der Modularitätssatz wurde 2001 durch Christophe Breuil, Brian Conrad, Fred Diamond und Richard Taylor bewiesen.

# GRAND THÉORÈME DE FERMAT

***aka*** **Dernier Théorème de Fermat**

***aka*** **THÉORÈME DE FERMAT-WILES**

**$Z^n = X^n + Y^n$ IMPOSSIBLE sauf pour n=2**

## HISTORIQUE – Chronologie

| | | |
|---|---|---|
| 1637 | **Pierre de Fermat** | • Il annote l'Arithmetica de Diophante , traduction de Bachet.<br>• pas de cubes, pas plus que de puissances quelconques qui satisfassent l'équation.<br>• j'ai une démonstration merveilleuse, mais la marge est trop étroite pour la contenir. |
| 1670 | **Clément Samuel fils de Fermat** | • Publication de l'Arithmetica de Diophante avec les observations de Fermat. |
| 1753 | **Euler** | • Preuve pour n = 3, avec une erreur récupérable en lisant d'autres démonstrations d'Euler. |
| vers 1800 | **Sophie Germain Legendre** | • Pas de solution jusqu'à x, y et z divisibles par n jusqu'à 100.<br>• Extension jusqu'à 197. |
| 1825<br>1832 | **Dirichlet** | • Prouve le cas n = 5.<br>• Prouve le cas n = 14. |
| 1839<br>1847 | **Gabriel Lamé** | • Prouve le cas n = 7.<br>• Prétend avoir trouvé la solution complète. |
| 1908 | **l'Université de Göttingen en Allemagne** | • Offre un prix de 100 000 marks à qui trouvera la démonstration avant 2007. |
| 1968 | **Shimura- Taniyama -Weil** | • Conjecture STW: toute courbe elliptique provient d'une forme modulaire. |
| 1970 | **Serres** | • Conjecture qui concerne les formes modulaires. |
| 1983 | **Gerd Faltings** | • Nombre fini de premiers entre eux qui seraient solution de l'équation. |
| 1985 | **Frey & Ribet** | • Conjecture de Frey démontrée par Ribet en 1986: si des courbes vérifient la conjecture STW, elles vérifient aussi la conjecture de Serre. |
| 23 juin<br>1993 | **Andrew Wiles** | • Conférence annonçant la démonstration du théorème de Fermat. |
| Nov.1993 | | • Rumeur concernant une défaillance dans la démonstration. |
| 3 avril 1994 | **Noam Elkies** | • Il annonce avoir trouvé un contre-exemple à la conjecture de Fermat ou presque >>> |
| 25<br>Oct.1994 | **Andrew Wiles<br>Richard Taylor** | • Mise à jour de la démonstration du Dernier théorème de Fermat : preuve finale. |
| Mai 1995 | **Andrew Wiles** | • Publication dans les Annals of Mathematics. |
| 27 juin<br>1997 | **Andrew Wiles** | • Attribution du prix Wolfskehl de 50 000 $. |
| 1999 | **Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor** | • Conjecture de Taniyama–Shimura complètement démontrée.<br>**La partie suffisante pour en déduire le dernier théorème de Fermat a été démontrée par Andrew Wiles. Ces mathématiciens ont traité les cas restants en s'inspirant des travaux de Wiles.** |

## DÉMONSTRATION – Principe

- Cette preuve est fondée sur les propriétés des ***courbes elliptiques*** pour lesquelles Gerhard Frey, une dizaine d'années auparavant, avait montré la connexion avec le théorème de Fermat.
- Il avait montré que les solutions de l'équation pour n > 2 engendraient une étrange classe de courbes elliptiques semi - stables, qui infirmaient une autre conjecture fameuse, la conjecture de **Shimura – Taniyama – Weil (STW)**.
- En 1986, Kenneth Ribe de l'université de Californie, prouva que si cette conjecture était vraie, au moins pour les courbes elliptiques semi - stables, alors le théorème de Fermat en découlait.
- Lors de la première tentative, A. Wiles avait eu une approche " directe ", mais commettait une généralisation abusive.
- Ce qu'il a corrigé en trouvant une voie détournée.
- La démonstration suppose la consistance du système formel Zermelo-Fraenkel.

**Pour information**: une démonstration ultrasimple découlerait de la résolution de la conjecture ABC (annoncée en 2013).

### Historique:

- Les démonstrations pour prouver cette relation jusqu'à n < 269 existaient en 1961.
- Fermat, dans la marge du livre " Arithmétique " de Diophante, avait noté en 1637 qu'il avait découvert la démonstration mais n'avait pas la place de la noter.
- Fermat avait sans doute vu des cas particuliers non évidents, ou autres, mais il est peu probable qu'il ait eu la solution complète.
- La preuve a résisté à 350 ans d'efforts.

### Découverte:

- En 1993, Andrew Wiles publiait la démonstration générale en 151 pages.
- Il reconnu immédiatement qu'il y avait une erreur.
- Il a fallu 10 mois à **A. Wiles et R. Taylor** pour présenter une version améliorée, que les experts estiment correcte.
- Seuls 200 mathématiciens au maximum au monde sont capables de saisir tous les détails de la démonstration.
- La démonstration fait un long détour par la théorie des nombres et la géométrie algébrique pour se terminer par la preuve du théorème de Fermat.
- Au passage, la démonstration laisse des démonstrations générales plus fortes et plus importantes dans ses applications.
- C'est probablement la démonstration la plus épluchée de l'histoire des mathématiques.

### Contributeurs

- Quatre mathématiciens sont à l'origine de la réussite de Wiles
  - Gerhard Frey,
  - Jean-Pierre Serre,
  - Ken Ribet,
  - Richard Taylor.

## Fermat et les SIMPSONS: $1\,782^{12} + 1\,841^{12} = 1\,922^{12}$

**Curiosité**

Une égalité qui contredit le théorème de Fermat proposée par les Simpsons.
Où est la supercherie?

**Calcul – C'est pourtant vrai ...**

Prendre votre calculette avec dix chiffres significatifs et faites:

$A + B = 1\,782^{12} + 1\,841^{12}$ et $S = 1\,922^{12}$

$A = 1{,}025397835\ e{+}39$ (e+39 veut dire $10^{39}$)

$B = 1{,}5158124229\ e{+}39$

$A + B = 2{,}541210259\ e{+}39$

$S = 2{,}541210259\ e{+}39$

Ainsi: $1\,782^{12} + 1\,841^{12} = 1\,922^{12}$

**Explications – Finalement non!**

Avec la calculette de votre ordinateur (ou même sur Google: tapez simplement 1782^12 dans la fenêtre de recherche et vous aurez le résultat immédiat).

A = 1,025397835622633634807550462948 2e+39
B = 1,515812422991955541481119495194 2e+39
A + B = 2,541210258614589176288669958142 4e+39
S = 2,541210259314801410819278649643 7e+39
S - (A+B) = 0, 700 212 234 530 608 691 501 223 040 959e+30

La somme est presque juste. La différence est pourtant un nombre comportant 30 chiffres.
L'égalité est en fait:

$1\,782^{12} + 1\,841^{12} = 1921{,}9999999586\ldots^{12}$

Pour information A + B compte six facteurs:

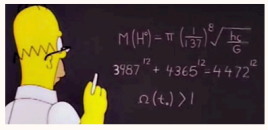
A + B = 409 x 4793 x 7793 x 577513 x 17960641 x 16036943149450969

**Un autre exemple des Simpsons tout aussi faux**

$3\,987^{12} + 4\,365^{12} = 4\,472^{12}$

cette somme vaut en fait:

$4472{,}000000007059290\ldots^{12}$




**Supercherie révélée immédiatement avec la théorie des nombres**

Explication 1: la parité d'un nombre élevé à une puissance est conservée.

- Dans le premier cas: $1\,782^{12} + 1\,841^{12} = 1\,922^{12}$ on a P + I = P ce qui est impossible.
- Dans le second cas: $3\,987^{12} + 4\,365^{12} = 4\,472^{12}$ on a I + I = P ce qui est possible.

Explication 2: divisibilité par 3 (qui est conservée lorsqu'on élève à une puissance).
Pour le deuxième exemple, les deux premiers termes sont divisibles par 3 alors que celui de la somme ne l'est pas. L'égalité ne peut pas tenir.

# APPLICATIONS DANS LA VIE MODERNE

## LE CODE D'AUTHENTICITÉ DES CARTES BANCAIRES

| | |
|---|---|
| Le code à 16 chiffres comporte quatre nombres particuliers. | **Signification du code de la carte bancaire**<br><br>*Source:* Exemple pris sur le site en référence<br>Le numéro est totalement imaginaire. |
| **Identifiant industrie** | 1. Compagnies aériennes;<br>2. idem<br>3. Voyages et loisirs;<br>4. Banques et finances;<br>5. idem<br>6. Merchandising;<br>7. Pétrole<br>8. Télécommunicatiosn; et<br>9. Supports nationaux. |
| **N° établissement** | Identifaint de l'organisme.<br>Les cartes Visa commencent par 4, Mastercard par 51 ou 55, Amex par 34 ou 37, etc. |
| **N° de la carte** | Rang de la carte dans l'établissement<br>Avec neuf chiffres: $10^9$ = 1 milliard de possibilités<br>Avec une extension possible à douze chiffres: $10^{12}$ = mille milliards de possibilités. |
| **Code authenticité** | Associé aux 15 autre chiffres, il permet d'en déterminer l'authenticité à travers l'algorithme de Luhn. |

### ALGORITHME DE LUHN ou algorithme du modulo 10

Hans Peter Luhn, ingénieur allemand chez IBM – 1960

L'algorithme de Luhn est une formule de validation de nombres utilisée pour
- Les cartes bancaires
- Les numéros administratifs (SIRET, SIREN…)

Pour chacune des 8 paires de chiffres :
On double le chiffre de rang impair, on garde le chiffre de rang pair.
On fait la somme des chiffres des 2 nombres ainsi obtenus. Par exemple : 14 & 8 → 1+4+8=13
Si la somme des 8 sommes ainsi obtenues est divisible par 10, le numéro de la carte est possible (« validé »).
En fait le 16ème chiffre est calculé pour valider les 15 premiers selon cet algorithme.

*Exemple :*

| Carte | 4 | 4 | 1 | 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 1 | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *1 sur 2* | 4 | | 1 | | 1 | | 3 | | 5 | | 7 | | 9 | | 1 | |
| *x 2* | 8 | | 2 | | 2 | | 6 | | 10 | | 14 | | 18 | | 2 | |
| *Les autres* | | 4 | | 7 | | 2 | | 4 | | 6 | | 8 | | 1 | | 3 |
| *Somme Chiffres* | 12 | | 9 | | 4 | | 10 | | 7 | | 13 | | 10 | | 5 | |
| *Cumul* | | | 21 | | 25 | | 35 | | 42 | | 55 | | 65 | | 70 | |
| *Divisible par 10?* | | | | | | | | | | | | | | | oui! | |

## IBAN

IBAN stands for "International Bank Account Number". It uniquely identifies an account and a bank.

IBAN was introduced to standardize and simplify payment transactions between countries.

Its use within the Single Euro Payments Area (SEPA) is mandatory since 2016.

IBANs have 2 check digits.

Check digits are used to recognize input errors. They enable a plausibility check of the account number information before it is transmitted, limiting the need to resolve errors and accelerating the transfer of funds.

**How is an IBAN structured?**

An IBAN is an alphanumeric string of characters.

It contains a country code, check digits, a bank identification number and an account number.

IBAN length is fixed within a country but varies by country, from 15 in Norway to 31 in Malta.

| | |
|---|---|
| German IBANs have 22 characters: | DE29 1001 0010 0987 6543 21 |
| • 2-digit country code (DE) | DE Länderkennzeichen |
| • 2-digit check digit | 29 Prüfziffern |
| • 8-digit bank code (BLZ) | 1001 0010 Bankleitzahl |
| • 10-digit account number | 0987 6543 21 Kontonummer |

**Calculation of the check digits**

They are calculated using the following procedure:

*Example using bank code 1001 0010 and account number 987654321.*

| | |
|---|---|
| 1. If the account number has less than 10 digits, it is filled with leading zeros | 0987 6543 21 |
| 2. The 8-digit bank code and the account number are merged to form the BBAN | 1001 0010 0987 6543 21 |
| 3. The country code and two check digits set to 00 are placed after the BBAN | 1001 0010 0987 6543 21 DE00 |
| 4. Letters are replaced by numbers: A = 10, B = 11 etc. DE becomes 13 14 | 1001 0010 0987 6543 21 131400 |
| 5. The rest of that number divided by 97 (modulo 97) is calculated | ≡ 69 [97] |
| 6. That rest is subtracted from 98. This yields the check digits: | 98 - 69 = 29 |
| 7. IBAN | DE29 1001 0010 0987 6543 21 |

*Algorithme du Modulo 97*

*Lemme de Laeticia : $02 \leq$ IBAN check digits $\leq 98$*

## CRYPTAGE RSA

Les nombres RSA sont un produit de deux facteurs premiers (nombres dits semi-premiers).

Alors qu'il est très facile de calculer N = p.q il est très difficile de trouver p et q connaissant N.

Prendre N suffisamment grand sert au chiffrement des communications.

RSA Security a offert des prix à ceux qui ont réussi à factoriser certains de ces nombres.

| Le nombre | contenant | a été factorisé en |
|---|---|---|
| RSA-100 | 100 chiffres, soit 330 bits | 1991 |
| RSA-200 | 200 chiffres, soit 663 bits | 2005 |
| RSA-220 | 768 bits | 2016 |
| RSA-240 | 795 bits | 2019 |
| RSA-250 | 829 bits | 2020 |

RSA 617 chiffres / 2048 bits est utilisé commercialement.

### L'idée générale du cryptage :

| | | |
|---|---|---|
| • Deux nombres premiers tenus secrets | **p et q** | 3 et 7 |
| • Son produit **n** est diffusé | **n = p.q** | n = 21 |
| • On calcule **f** | **f = (p – 1) (q – 1)** | f = 2x6 = 12 |
| • Un nombre **e** est, lui aussi, diffusé | **e premier avec f** | e = 5 |
| • Je calcule **d**, inverse de **e mod f** | **e.d = 1 mod f** | 5d = 1 mod 12<br>5x5 = 1 mod 12<br>d = 5 |
| **Préparation du message** | | |
| • Le message est converti en chiffres<br>• On va coder chaque chiffre | **$x_1$ … $x_i$ …**<br>**avec $x_i$ < n** | x = **2**, par exemple |
| **Codage du message** | | |
| • Chaque **x** est codé par **y** | **$y = x^e \bmod n$** | $y = 2^5 \bmod 21$<br>y = 32 mod 21<br>y = 11 |
| • Les valeurs de **y** sont transmises | **y est transmis** | 11 est transmis |
| **Déchiffrage** | | |
| • Je calcule **z** | **$z = y^d \bmod n$** | $z = 11^5 \bmod 21$<br>z = 11 x121x121 mod 21<br>z = 11 x 16 x 16 mod 21<br>z = 11 x 256 mod 21<br>z = 11 x 4 mod 21<br>z = 44 mod 21<br>z = **2** mod 21 |
| • Car en fait | **z = x mod n** | z = **2** mod 21 |

**Références**

Je voudrais recommander ici le travail encyclopédique de Gérard Villemin :
http://villemin.gerard.free.fr
Ce site offre une approche très efficace à la découverte de nouvelles notions mathématiques…
une fois habitué à la navigation.

Nombres : curiosités – théorie – usage

Problem Solving Strategies de Arthur Engel – chapitre 6 *(Springer)*

Mathe ist Cool ! *(Cornelsen)*

1001 problèmes de théorie classique des nombres – Jean Marie De Koninck et Armel Mercier *(Ellipses)*

Maths MPSI Tout-en-un – Claude Deschamps et François Moulin - Chapitre 15 *(Dunod)*

Maths MPSI – Nicolas Nguyen - Chapitre 13 *(Ellipses)*

# ENSEMBLES

# FONCTIONS

# STRUCTURES ALGÉBRIQUES : GROUPES, ANNEAUX & CORPS

Les structures algébriques sont les bases fondamentales de… l'algèbre.
Qui l'eut cru ?

Quand on construit ces structures, c'est comme si on construisait un vaisseau spatial.
Avec ça on peut partir explorer de nouvelles galaxies : probabilités, arithmétique, géométrie…

Ce chapitre veut intentionnellement rester très simple.
Mais il contient beaucoup, beaucoup de vocabulaire nouveau et de définitions.
L'objectif premier est de se familiariser avec ces noms et ces concepts.

Et là il faut lire, relire jusqu'à ce que les concepts et définitions soient compris et appris par cœur.

# ENSEMBLES

Un **ensemble** (*Menge*) est une collection d'éléments.

Exemples : {0, 1} {rouge, noir} {0, 1, 2, 3,…} = N

Un ensemble particulier est l'**ensemble vide** (*leere Menge*), noté ∅ qui est l'ensemble ne contenant aucun élément.

On note **x ∈ E** si x est un élément de E **x ∉ E** dans le cas contraire.

On peut aussi définir un ensemble comme collection d'éléments qui vérifient une propriété.

Exemples : $\{x \in \mathbb{R} \mid |x-2| < 1\}$ $\{z \in \mathbb{C} \mid z^5 = 1\}$ $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\} = [0,1]$.

F est un **sous-ensemble** (*Teilmenge*) de E ou une **partie** de E si ∀x ∈ F (x∈ E) F est **inclus** dans E : F ⊂ E

**Égalité** ssi F ⊂ E et E ⊂ F

On note **$\mathcal{P}$(E) l'ensemble des parties** de E. (*Potenzmenge*)

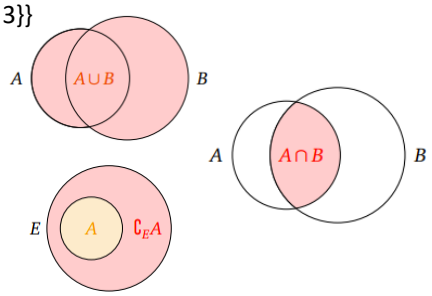
Pour un ensemble de n éléments il y a $2^n$ parties.

Par exemple si E = {1, 2,3} : $\mathcal{P}$(E) = { ∅ ,{1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}

Pour A, B ⊂ E **Union** A ∪ B = {x ∈ E | x ∈ A ou x ∈ B}

**Intersection** A ∩ B = {x ∈ E | x ∈ A et x ∈ B}

**Complémentaire** E\A ou $\mathcal{C}A$ = {x ∈ E | x ∉ A}




*Vereinigung - Durchschnitt - Komplementär von A in E*

### Règles de calcul

Soient A, B, C des parties d'un ensemble E :

A ∩ B = B ∩ A

A ∩ (B∩C) = (A∩B) ∩C on peut donc écrire A∩B∩C sans ambigüité

A ∩ ∅ = ∅ A ∩ A = A A ⊂ B ⇔ A∩B = A

A ∪ B = B ∪A

A ∪ (B∪C) = (A∪B) ∪ C on peut donc écrire A∪B∪C sans ambiguïté

A ∪ ∅= A A ∪ A = A A ⊂ B ⇔ A∪B = B

A ∩ (B∪C) = (A∩B) ∪ (A∩C)
A ∪ (B∩C) = (A∪B) ∩ (A∪C)

$\mathcal{C}(\mathcal{C}A)$ = A $\mathcal{C}$(A∩B) = $\mathcal{C}$A ∪ $\mathcal{C}$B $\mathcal{C}$(A∪B) = $\mathcal{C}$A ∩ $\mathcal{C}$B

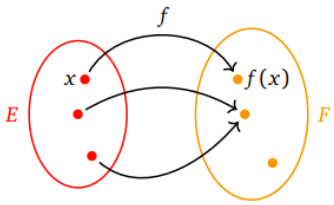
Soient E et F deux ensembles :

Le **produit cartésien** (*kartesisches Produkt*),noté **E × F**, est l'ensemble des couples (x, y) où x ∈ E et y ∈ F.

Exemple $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\} = \mathbb{C}$

# FONCTIONS

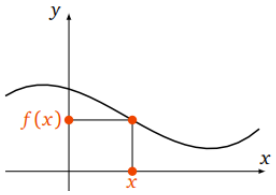
Une **application** (*Abbildung*) ou une **fonction** (*Vorschrift*) f : E → F c'est la donnée pour chaque élément x de E d'un ***unique*** élément de F noté f(x).



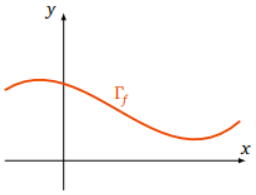

Nous représenterons les applications par deux types d'illustrations :

***Les ensembles « patates »***
L'ensemble de départ et celui d'arrivée sont schématisés par un ovale ;
leurs éléments par des points.
L'association x ⟼ f (x) est représentée par une flèche.

***Représentation des fonctions continues de ℝ dans ℝ (ou des sous-ensembles de ℝ)***
L'ensemble de départ est représenté par l'axe des abscisses,
celui d'arrivée par l'axe des ordonnées.
L'association x ⟼ f (x) est représentée par le point (x, f (x)).

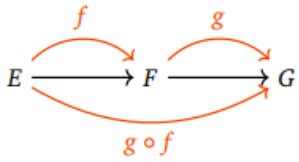



**Le graphe** de f : E → F est $\Gamma_f = \{(x, f(x)) \in E \times F \mid x \in E\}$
De par la définition des fonctions :
le graphe d'une fonction ne « revient jamais en arrière ».
Il n'a jamais non plus 2 sections de courbe l'une au-dessus de l'autre.



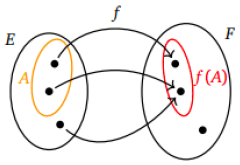

Deux applications *f*, *g* : E → F sont **égales** ssi ∀x ∈ E, *f* (x) = *g*(x) On note alors *f* = *g*

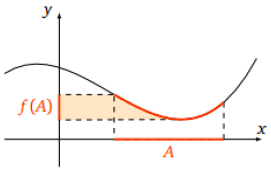
Soient *f* : E → F et *g* : F → G alors ***g* o *f*** : E → G est l'application **composée**
définie par ***g* o *f* (x) = *g*(*f*(x))** Exemple : si f(x) = 2x et g(x) = x³ alors *g* o *f* (x) = *g*(2*x*)=(2x)³



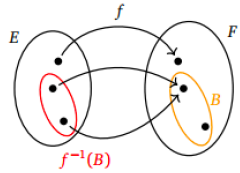

L'**identité** $id_E$ : E → E est simplement définie par x ⟼ x

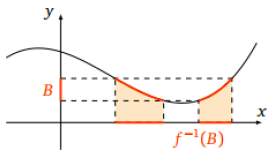
Soit A ⊂ E et *f* : E → F l'**image directe** de A par *f* est l'ensemble *f*(A) = {*f*(x) | x ∈ A}



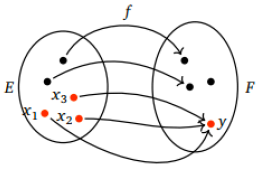

Soit B ⊂ F et *f* : E → F l'**image réciproque** de B par *f* est l'ensemble $f^{-1}$(B) = {x ∈ E | *f*(x) ∈ B}

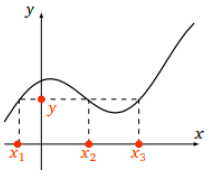



L'image réciproque est un sous-ensemble de E. Elle existe quelle que soit la fonction, bijective ou pas.
L'image directe d'un singleton est un singleton.
Par contre l'image réciproque d'un singleton peut être un singleton, un ensemble de plusieurs éléments de E, l'ensemble E entier, ou l'ensemble vide.

Pour y ∈ F, tout élément x ∈ E
tel que *f* (x) = y est un **antécédent** de y.



Soient E et F deux ensembles et $f : E \to F$ une application

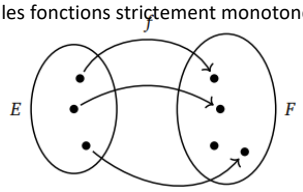
**$f$ est injective si** $\forall x, x' \in E \ ( f(x) = f(x') \Longrightarrow x = x' )$

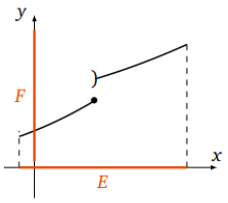
$f$ est injective ssi tout élément de F a ***au plus*** un antécédent

Exemples de fonctions injectives

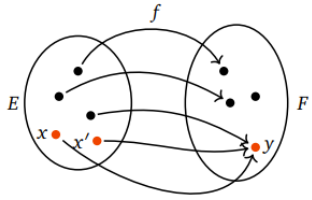
Parmi les fonctions numériques :

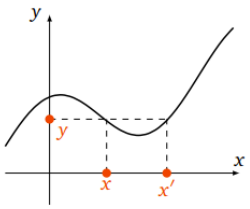
les fonctions strictement monotones




Exemples de fonctions NON injectives :



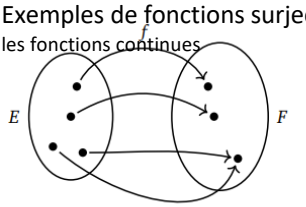

**$f$ est surjective si** $\forall y \in F \ \exists x \in E \ ( y = f(x) )$

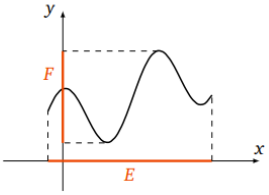
$f$ est surjective ssi tout élément de F a ***au moins*** un antécédent

Exemples de fonctions surjectives :

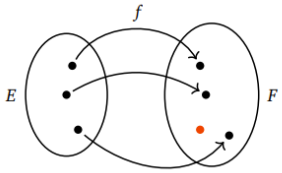
Parmi les fonctions numériques :

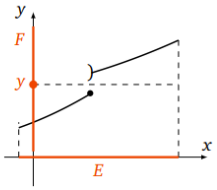
les fonctions continues




Exemples de fonctions NON surjectives :



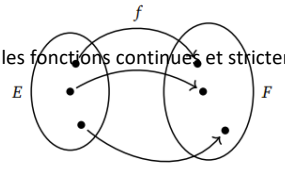

**$f$ est bijective si** $\forall y \in F \ \exists! x \in E \ ( y = f(x) )$

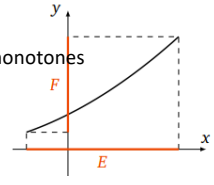
$f$ est bijective si elle est injective et surjective.

$f$ est bijective si tout élément de F a un antécédent unique par $f$.

Parmi les fonctions numériques :

les fonctions continues et strictement monotones




Remarque : il existe des fonctions qui ne sont ni injectives, ni surjectives.

L'application $f$ est **bijective ssi** il existe une application $g : F \to E$ telle que $f \circ g = id_F$ et $g \circ f = id_E$.
*Satz über die Invertierbarkeit bijektiver Abbildungen*

Si $f$ est bijective alors l'application $g$ est unique et elle aussi est bijective.
L'application $g$ s'appelle la **bijection réciproque** de $f$ et est notée $f^{-1}$. De plus $(f^{-1})^{-1} = f$
*Eindeutigkeit der inversen Abbildung*

Soient $f : E \to F$ et $g : F \to G$ deux applications bijectives.
L'application $g \circ f$ est bijective et sa **bijection réciproque** est $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Un ensemble E est **fini** (*endlich*) s'il existe un entier n et une bijection de E vers {1,2, .. ., n}
*a fancy way of saying* : on peut compter les éléments de E

Cet entier n est unique et s'appelle le **cardinal** de E, ou le **nombre d'éléments** de E, et est noté **Card E** ou |E|

| | |
|---|---|
| $Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$ | $\|A \cup B\| = \|A\| + \|B\| - \|A \cap B\|$ |

Soit E, F deux ensembles finis et $f : E \to F$ une application.

- Si f est injective Card E $\leq$ Card F
- Si f est surjective Card E $\geq$ Card F
- Si f est bijective Card E = Card F

**Principe des tiroirs :** Si l'on range dans k tiroirs, n > k paires de chaussettes
alors il existe (au moins) un tiroir contenant (au moins) deux paires de chaussettes.

Soient E, F des ensembles **finis**, non vides. On note Card E = n et Card F = p.

**Le nombre d'applications** différentes de E dans F est : $\mathbf{p^n = (Card\ F)^{Card\ E}}$

**Le nombre d'injections** (donc n<p) de E dans F est : $p \times (p-1) \times \cdots \times (p-(n-1)) = \frac{\mathbf{p!}}{\mathbf{(p-n)!}}$

C'est le nombre d'**arrangements**.

**Le nombre de bijections** d'un ensemble E de cardinal n dans lui-même est : **n!**
C'est le nombre de **permutations** de E. C'est aussi le cas particulier des injections avec p = n.

**Gleichmächtigkeit**

Zwei Mengen E und F sind **gleichmächtig**, wenn es eine bijektive Abbildung von E nach F gibt.

Seien E und F endliche Mengen. E und F sind genau dann gleichmächtig, wenn Card E= Card F.

**Was ist mit unendlichen Mengen?**

$\mathbb{Z}$ und $2\mathbb{Z}$ sind gleichmächtig
N und $\mathbb{Z}$ sind gleichmächtig

*Dedekindsche Beschreibung unendlicher Mengen*
Jede unendliche Menge enthält eine echte Teilmenge derselben Mächtigkeit.

*Satz von der Potenzmenge* (die Menge aller Teilmengen)
Für jede nichtleere Menge E, die Potenzmenge P(E) hat eine größere Mächtigkeit als E.

# NOMBRE DE SOUS-ENSEMBLES D'UN ENSEMBLE FINI

Soit E un ensemble fini de cardinal n.
**Il y a $2^n$ sous-ensembles de E** Card $\mathcal{P}$ (E) = $2^n$

*Exemple*
Si E = {1, 2, 3, 4,} alors $\mathcal{P}$ (E) a $2^4 = 16$ parties :
L'ensemble vide : ∅
4 singletons : {1}, {2}, {3}, {4},
6 paires : {1,2}; {1,3}; {1,4}; {2,3}; {2,4}; {3,4}
4 triplets : {1,2,3}, {1,2,4}, {1,3,4}, {2,3,4}
E tout entier : {1, 2, 3, 4}

*Démonstration*
Par récurrence sur n = Card E.

• Si n = 1, E = {a} est un singleton, les deux sous-ensembles sont : ∅ et E.

• Supposons que la proposition soit vraie pour n > 1 fixé. Soit E un ensemble à n + 1 éléments.
On fixe a ∈ E. Il y a deux sortes de sous-ensembles de E :
- Les sous-ensembles A qui ne contiennent pas a : ce sont les sous-ensembles A ⊂ E\{a}.
  Par l'hypothèse de récurrence il y en a $2^n$.
- Les sous-ensembles A qui contiennent a : ils sont de la forme A = {a} ∪ A' avec A' ⊂ E\{a}.
  Par l'hyp. de récurrence il y a $2^n$ sous-ensembles A' possibles et donc aussi $2^n$ sous-ensembles A.
Il y a donc $2^n + 2^n = 2^{n+1}$ parties A ⊂ E. *QED*

• Par le principe de récurrence, nous avons prouvé que si Card E = n alors Card $\mathcal{P}$ (E) = $2^n$

# NOMBRE DE PARTIES à k éléments d'un ensemble à n éléments

**Le nombre de parties à k éléments d'un ensemble à n éléments est noté $\binom{n}{k}$**

*Exemple* Nous avons compté ci-dessus les parties de {1,2,3,4} par nombre d'éléments :
$\binom{4}{0} = 1$ La seule partie n'ayant aucun élément est l'ensemble vide
$\binom{4}{1} = 4$ Il y a 4 singletons $\binom{4}{2} = 6$ Il y a 6 paires $\binom{4}{3} = 4$ Il y a 4 triplets
$\binom{4}{4} = 1$ La seule partie ayant 4 éléments est l'ensemble tout entier

Pour un ensemble à n éléments on a les propriétés suivantes :

**$\binom{n}{0} = 1$** La seule partie n'ayant aucun élément est l'ensemble vide

**$\binom{n}{n} = 1$** La seule partie ayant n éléments est l'ensemble tout entier

**$\binom{n}{1} = n$** Il y a n singletons

**$\binom{n}{k} = \binom{n}{n-k}$**
*Démonstration* Compter le nombre de parties A ⊂ E ayant k éléments est la même chose que compter les complémentaires de A (qui ont donc n − k éléments)



**$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k} + \ldots + \binom{n}{n} = 2^n$**
*Démonstration* Compter toutes les parties de E c'est faire la somme du nombre de parties à 0, à 1, …, et à n éléments.

$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ $\quad 0 < k < n$

*Les formules associées à ce pictogramme sont à mémoriser jusqu'à vos derniers jours*

*Démonstration*

Soit E un ensemble à n éléments. Soit a un élément de E. Soit E' = E \ {a} Card (E') = n−1
On dénombre les sous-ensembles A ⊂ E ayant k éléments. Il y en a de deux sortes disjointes :
- Ceux qui ne contiennent pas a : ce sont des parties à k éléments dans l'ensemble E'.
Comme Card (E') = n−1, il y en a $\binom{n-1}{k}$.
- Ceux qui contiennent a : ils sont de la forme A = {a} ∪ A' avec A' une partie à k-1 éléments dans E'.
Il y a donc autant d'ensembles de ce type que d'ensembles A' qui sont au nombre de $\binom{n-1}{k-1}$.
D'autre part, le nombre de sous-ensembles A est par définition $\binom{n}{k}$. *QED*

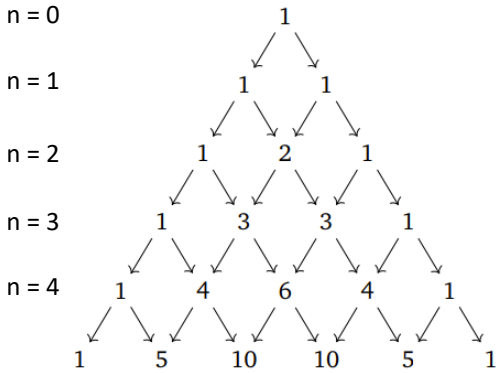
Cette formule peut se représenter ainsi :

$\binom{n-1}{k-1}$ $\quad$ $\binom{n-1}{k}$

$\binom{n}{k}$

Les flèches représentent les Summanden

On peut utiliser cette représentation pour construire une pyramide appelée ***triangle de Pascal*** (l'ami Blaise) qui permet de calculer tous les $\binom{n}{k}$.
On part en haut de $\binom{0}{0} = 1$ et on construit chaque ligne successive.
Chaque élément de la nouvelle ligne est obtenu en ajoutant les deux nombres qui lui sont au-dessus à droite et au-dessus à gauche.
Les nombres les plus à droite et les plus à gauche valent 1.




Cette méthode est très pratique pour calculer rapidement une ligne entière pour n assez petit.
Mais on a plus fort : pour $0 \le k \le n$ k, n$\in \mathbb{N}$

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

*Démonstration*

Par récurrence sur n. Soit ($P_n$) l'assertion $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ pour tout entier k tel que $0 \le k \le n$

• $P_1$ est vraie : si n = 1 alors k = 0 ou k = 1. Si k = 0 on doit avoir $\binom{1}{0} = 1$ et on a bien $\frac{1!}{0!\,(1-0)!} = 1$
(par convention 0! = 1) Si k = 1 on doit avoir $\binom{1}{1} = 1$ et on a bien $\frac{1!}{1!\,(1-1)!} = 1$

• Supposons que l'hypothèse de récurrence soit vraie au rang n-1 et montrons qu'elle est vraie au rang n.
Nous pouvons utiliser la formule déjà prouvée $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ à n'importe quel rang, en particulier au rang n.
On y remplace les 2 termes $\binom{n-1}{k}$ et $\binom{n-1}{k-1}$ qui sont de rang n-1 par leur équivalent tel qu'exprimé par l'hypothèse de récurrence, ce que l'on peut faire car l'hypothèse de récurrence est admise au rang n-1 :

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!}$$
$$= \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \left(\frac{1}{n-k} + \frac{1}{k}\right) = \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \frac{n}{k(n-k)}$$
$$= \frac{n!}{k!(n-k)!}$$ $P_n$ est vérifiée.

Et on a même carrément encore plus fort : pour a, b $\in \mathbb{R}$ et n $\in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

C'est la formule du **binôme de Newton.**

# BINÔME DE NEWTON

**On répète la formule du binôme :** $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

Autrement dit :

$(a+b)^n = \binom{n}{0} a^n.b^0 + \binom{n}{1} a^{n-1}.b^1 + \cdots + \binom{n}{k} a^{n-k}.b^k + \ldots + \binom{n}{n} a^0.b^n$

*Exemples*

Pour n = 2 on retrouve la formule archi-connue : $(a+b)^2 = a^2 + 2ab + b^2$

Pour n = 3 on a une autre formule à connaître : $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
Si on l'a oubliée, on utilise *rapidos* le triangle de Pascal pour retrouver les coefficients.

Pour a = 1 et b = 1 on retrouve la formule $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k} + \ldots + \binom{n}{n} = 2^n$

Et maintenant, comme on est super balaise Blaise, on va démontrer ici-même
la formule du binôme de Newton :

Démonstration par récurrence sur n.
Soit ($P_n$) l'assertion : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

• *Initialisation*. Pour n = 1, $(a+b)^1 = \binom{1}{0} a^1.b^0 + \binom{1}{1} a^0.b^1$. Ainsi $P_1$ est vraie.



• *Hérédité*. Fixons $n \geq 2$ et supposons que $P_{n-1}$ est vraie.

$$\begin{aligned}
(a+b)^n &= (a+b)\cdot(a+b)^{n-1} \\
&= a\left(a^{n-1} + \cdots + \binom{n-1}{k} a^{n-1-k}b^k + \cdots + b^{n-1}\right) \\
&\quad + b\left(a^{n-1} + \cdots + \binom{n-1}{k-1} a^{n-1-(k-1)}b^{k-1} + \cdots + b^{n-1}\right) \\
&= \cdots + \left(\binom{n-1}{k} + \binom{n-1}{k-1}\right) a^{n-k}b^k + \cdots \\
&= \cdots + \binom{n}{k} a^{n-k}b^k + \cdots \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k}\cdot b^k
\end{aligned}$$



Ainsi $P_n$ est vérifiée.

• *Conclusion*. Par le principe de récurrence $P_n$ est vraie, pour tout $n \geq 1$.

**Les multiples noms de $\binom{n}{k}$**

Revenons un peu en arrière et rappelons-nous comment on a défini $\binom{n}{k}$ :
c'est le nombre de parties à k éléments d'un ensemble à n éléments.
On l'appelle le nombre de **k combinaisons dans n**.
D'où l'ancienne notation $C_k^n$ … et la prononciation « C N K ».
Ce sont aussi les coefficients d'un polynôme dans la formule du binôme.
C'est pourquoi on les appelle aussi **coefficients binomiaux**– ou **coefficients du binôme** de Newton.

Un scoop en avant-première : en fait la formule du binôme de Newton est vraie dans n'importe quel anneau commutatif. Donc **aussi avec les nombres complexes et les polynômes**. *Yeah !*

*Il s'est passé quelque chose : en faisant avec des ensembles-patate des « maths avec les mains » comme des élèves de maternelle jouent à la pâte à modeler, on a montré en 3 pages l'essentiel de ce qu'il y a à savoir sur les probabilités. Dans l'empire des mille planètes notre vaisseau algébrique a fait un saut spatio-temporel. Nous voilà équipés à explorer la galaxie des probabilités !*

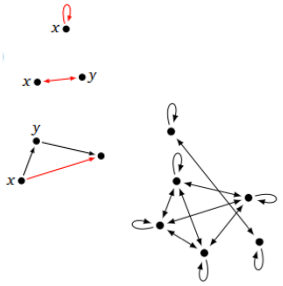
# RELATIONS

Une relation sur un ensemble E, c'est la donnée pour tout couple (x, y) ∈ E × E
de « Vrai » s'ils sont en relation, ou de « Faux » sinon.

Nous schématisons une relation ainsi : les éléments de E sont des points, une flèche de x vers y signifie que
x est en relation avec y, c'est-à-dire que l'on associe « Vrai » au couple (x, y).

Une relation $\mathcal{R}$ sur un ensemble E est une **relation d'équivalence** si elle est réflexive, symétrique et transitive.

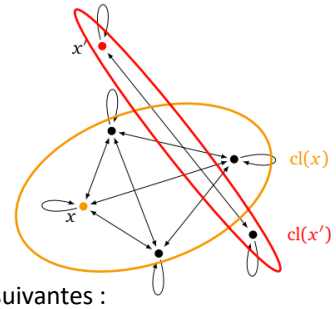
- ∀x ∈ E, x $\mathcal{R}$ x (**réflexivité**)
- ∀x, y ∈ E, x $\mathcal{R}$ y ⟹ y $\mathcal{R}$ x (**symétrie**)
- ∀x, y, z ∈ E, x $\mathcal{R}$ y et y $\mathcal{R}$ z ⟹ x $\mathcal{R}$ z (**transitivité**)



Exemple de relation d'équivalence :

Exemples :
La relation « être parallèle » est une relation d'équivalence pour l'ensemble des droites affines du plan.
La relation « être du même âge » est une relation d'équivalence pour l'ensemble des élèves du lycée.
La relation « être perpendiculaire » n'est pas une relation d'équivalence : ni réflexive, ni transitive.
La relation ≤ (sur E = ℝ par exemple) n'est pas une relation d'équivalence : pas symétrique.

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.
Soit x ∈ E, la **classe d'équivalence** de x est **cl(x) = {y ∈ E | y $\mathcal{R}$ x}**

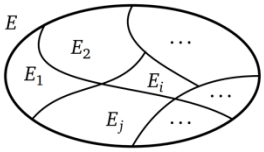



cl(x) est donc un sous-ensemble de E. On le note aussi $\bar{x}$.
Si y ∈ cl(x), on dit que y un **représentant** de cl(x).

Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence. On a les propriétés suivantes :

1. cl(x) = cl(y) ⇔ x $\mathcal{R}$ y
2. Pour tout x, y ∈ E, cl(x) = cl(y) ou cl(x) ∩ cl(y) = ∅ *Zwei Äquivalenzklassen sind gleich oder disjunkt*
3. Soit C un ensemble de représentants de toutes les classes alors {cl(x) | x ∈ C} constitue une partition de E.

Une **partition** de E est un ensemble {$E_i$} de parties de E tel que E = $\bigcup_i E_i$ et Ei ∩ Ej = ∅ (si i ≠ j).




**Construction de l'ensemble ℚ**
Définissons sur ℤ × ℕ* la relation $\mathcal{R}$ par (p,q) $\mathcal{R}$ (p',q') ⇔ pq' = p'q  $\mathcal{R}$ est une relation d'équivalence.
Nous allons noter p/q = cl(p, q) la classe d'équivalence d'un élément (p, q) ∈ ℤ × ℕ*
Par exemple, comme (2,3) $\mathcal{R}$ (4,6) (car 2 × 6 = 3 × 4) alors les classes de (2,3) et (4,6) sont égales.
Avec notre notation cela s'écrit : 2/3 = 4/6. C'est ainsi que l'on définit l'ensemble des rationnels :
ℚ est l'ensemble des classes d'équivalence de la relation $\mathcal{R}$ ! *(ici ! est un point d'exclamation comme dans oh ! ah ! woua !*
*Il convient de faire une pause pour méditer la puissance de la chose : on a construit ℚ sans jamais avoir prononcé le mot fraction ou division).*

**L'ensemble $\mathbb{Z}/n\mathbb{Z}$**
Définissons sur ℤ la relation a ≡ b [n] ⇔ a − b est un multiple de n  (pour un entier n ≥ 2 fixé).
L'ensemble des classes d'équivalence de ℤ est l'ensemble $\mathbb{Z}/n\mathbb{Z}$ = {$\bar{0}$, $\bar{1}$, $\bar{2}$, ..., $\overline{n-1}$ }
Exemple : $\mathbb{Z}/3\mathbb{Z}$ = {$\bar{0}$, $\bar{1}$, $\bar{2}$} possède 3 éléments.

# GROUPES

Un **groupe (G,*)** est un ensemble G muni d'une opération * (la **loi de composition**)
vérifiant les propriétés suivantes :

| | | |
|---|---|---|
| 1. | $\forall x, y \in G, x * y \in G$ | * est une **loi de composition interne** sur G |
| 2. | $\forall x, y, z \in G, (x * y) * z = x * (y * z)$ | la loi * est **associative** |
| 3. | $\exists e \in G$ tel que $\forall x \in G, x * e = x$ et $e * x = x$ | il existe un **élément neutre e** dans G |
| 4. | $\forall x \in G$ il existe $x' \in G$ tel que $x * x' = x' * x = e$ | tout élément de G possède un **symétrique** dans G |

Si de plus l'opération vérifie $\forall x, y \in G, x * y = y * x$, on dit que G est un groupe **commutatif** (ou **abélien**).

Remarques :
- L'élément neutre e est unique.
- L'inverse de l'élément neutre est lui-même.
- S'il y a plusieurs groupes, on peut noter $e_G$ l'élément neutre du groupe G.
- Un élément $x \in G$ ne possède qu'un seul inverse.

Exemples d'ensembles bien connus pour lesquels l'opération donnée définit une structure de groupe :

$(\mathbb{Z},+)$ est un groupe commutatif. Ici + est l'addition habituelle.
*Démonstration :*
1. Si $x, y \in \mathbb{Z}$ alors $x + y \in \mathbb{Z}$
2. Pour tout $x, y, z \in \mathbb{Z}$ alors $x + (y + z) = (x + y) + z$
3. 0 est l'élément neutre pour l'addition : $\forall x \in \mathbb{Z}$ $0 + x = x$ et $x + 0 = x$
4. L'inverse d'un élément $x \in \mathbb{Z}$ est $x' = -x$ car $x + (-x) = 0$ est bien l'élément neutre 0.
Quand la loi de groupe est + l'inverse s'appelle plus couramment **l'opposé**.
5. Enfin $x + y = y + x$, et donc $(\mathbb{Z},+)$ est un groupe commutatif.

$(\mathbb{R},+)$ $(\mathbb{Q},+)$ $(\mathbb{C},+)$ sont des groupes commutatifs, + est l'addition habituelle.
$(\mathbb{R}^*,\times)$ $(\mathbb{Q}^*,\times)$ $(\mathbb{C}^*,\times)$ sont des groupes commutatifs, × est la multiplication habituelle.

Mais :
$(\mathbb{Z}^*,\times)$ n'est pas un groupe.
En effet l'inverse de 2 pour × devrait être ½ mais $\frac{1}{2} \notin \mathbb{Z}$

$(\mathbb{N},+)$ n'est pas un groupe.
En effet l'inverse de 3 pour + devrait être -3 mais $-3 \notin \mathbb{N}$

$(\mathbb{R},x)$ n'est pas un groupe car 0 n'est pas inversible.

| | |
|---|---|
| $\mathbb{Z}/n\mathbb{Z}$ **est un groupe** | $\mathbb{Z}/n\mathbb{Z}$ c'est $\mathbb{Z}$ muni de la loi de congruence modulo n : ($\mathbb{Z}$, ≡ [n]) |

# MORPHISME DE GROUPE

Soient (G,*) et (H,$\bullet$) deux groupes.

Une application f : G $\to$ H est un **morphisme de groupes** si $\forall$ x, y $\in$ G  f(x * y) = f (x) $\bullet$ f (y)

Un morphisme bijectif est un **isomorphisme**.

Deux groupes G, H sont **isomorphes** s'il existe un morphisme bijectif f : G $\to$ H

Soit f : G $\to$H un morphisme de groupes.

Le **noyau** de f est  **Ker f** = {x $\in$ G | f (x) = $e_H$}

L'**image** de f est  **Im f** = {f (x) | x $\in$ G}

# GROUPE CYCLIQUE

Un groupe (G,*) est un **groupe cyclique** s'il existe un élément a $\in$ G tel que : $\forall$x $\in$ G, $\exists$ k $\in \mathbb{Z}$ tel que x = $a^k$

L'ensemble des permutations de E muni de la loi o  (P(E), o) est un groupe.

L'étude des groupes requiert à elle seule de multiples chapitres.
Dans ce chapitre on s'arrêtera là.
L'objectif ici est de se rappeler de la définition comme on respire et de mémoriser avec la même aisance les différences avec anneaux et corps – dont l'étude est aussi une science en soi.

# ANNEAUX

Un **anneau (A, ⊕,⊗)** est un ensemble A auquel est associé deux opérations ⊕ et ⊗ vérifiant :

| | | |
|---|---|---|
| 1. | ⊕ et ⊗ sont des **lois de composition interne** | ∀ x, y ∈ A, x ⊕ y ∈ A et x ⊗ y ∈ A |
| 2. | (A, ⊕) est un groupe commutatif : | |
| | la loi ⊕ est **associative** | ∀ x, y, z ∈ A, (x ⊕ y) ⊕ z = x ⊕ (y ⊕ z) |
| | A possède un **élément neutre 0** pour la loi ⊕ | ∃ 0 ∈ A tel que ∀ x ∈ A, x ⊕ 0 = x et 0 ⊕ x = x |
| | il existe un **inverse -x** dans A pour la loi ⊕ | ∀ x ∈ A ∃-x ∈ A tel que x ⊕ (-x) = 0 |
| | la loi ⊕ est **commutative** | ∀ x, y ∈ A, x ⊕ y = y ⊕ x |
| 3. | la loi ⊗ est **associative** | ∀ x, y, z ∈ K, (x ⊗ y) ⊗ z = x ⊗ (y ⊗ z) |
| 4. | A possède un **élément neutre 1** pour la loi ⊗ | ∃ 1 ∈ A tel que ∀ x ∈ K, x ⊗ 1 = x et 1 ⊗ x = x |
| 5. | ⊗ est **distributive** sur ⊕ | ∀ x, y, z ∈ A, x⊗ (y ⊕ z) = x⊗y ⊕ x⊗z |
| | Si de plus ⊗ est commutative l'anneau est **commutatif** | ∀ x, y ∈ A, x ⊗ y = y ⊗ x |

C'est un total de 9 conditions (en comptant les lci pour 2).

On a fait les gros malins super généralisateurs en utilisant les notation ⊕ et ⊗ pour montrer que les lois dans un anneau ne sont pas limitées aux lois connues d'addition et de multiplication. Mais en pratique on va souvent utiliser l'addition classique + comme exemple de ⊕ et la multiplication classique x comme exemple de ⊗.

Le nom « anneau » est une traduction de l'allemand et il n'y a *aucune relation* avec la forme géométrique ou l'objet que l'on connait sous le nom d'anneau.

Exemples :

$(\mathbb{Z},+,x)$ $(\mathbb{Q},+,x)$ $(\mathbb{R},+,x)$ sont des anneaux commutatifs avec + et x représentant l'addition et la multiplication usuelle.

Jusque-là rien de renversant. Là où ça devient intéressant :

La formule du binôme de Newton est valable dans n'importe quel anneau **commutatif**.
Le théorème du capitaine d'artillerie Bézout l'est aussi.

Et : (l'ensemble des polynômes, +, x) est un anneau commutatif !

**Construction de l'ensemble $\mathbb{C}$**

On définit dans $\mathbb{R}^2$ deux lois de composition interne notées ⊕ et ⊗ :

$\forall$ x, x', y, y' $\in \mathbb{R}$ $\quad (x,y) \oplus (x',y') = (x+x',y+y')$

$\quad (x,y) \otimes (x',y') = (xx'-yy',xy'+x'y)$

$\mathbb{C}$ est défini comme l'anneau commutatif $(\mathbb{R}^2, \oplus, \otimes)$ dont les éléments sont appelés nombres complexes.

# CORPS

Un **corps ($\mathbb{K}$,+,*)** est un ensemble $\mathbb{K}$ auquel est associé deux opérations + et * vérifiant :

| | | |
|---|---|---|
| 1. | + et * sont des **lois de composition interne** | $\forall x, y \in \mathbb{K}$, $x + y \in \mathbb{K}$ et $x * y \in \mathbb{K}$ |
| 2. | ($\mathbb{K}$,+) est un groupe commutatif : | |
| | la loi + est **associative** | $\forall x, y, z \in \mathbb{K}$, $(x + y) + z = x + (y + z)$ |
| | $\mathbb{K}$ possède un **élément neutre 0** pour la loi + | $\exists\, 0 \in \mathbb{K}$ tel que $\forall x \in \mathbb{K}$, $x + 0 = x$ et $0 + x = x$ |
| | il existe un **inverse** -x dans $\mathbb{K}$ pour la loi + | $\forall x \in \mathbb{K}\ \exists -x \in \mathbb{K}$ tel que $x + (-x) = 0$ |
| | la loi + est **commutative** | $\forall x, y \in \mathbb{K}$, $x + y = y + x$ |
| 3. | ($\mathbb{K} \setminus \{0\}$,*) est un groupe commutatif : | |
| | la loi * est **associative** | $\forall x, y, z \in \mathbb{K}$, $(x * y) * z = x * (y * z)$ |
| | $\mathbb{K}$ possède un **élément neutre 1** pour la loi * | $\exists\, 1 \in \mathbb{K} \setminus \{0\}$ tel que $\forall x \in \mathbb{K}$, $x * 1 = x$ et $1 * x = x$ |
| | il existe un **inverse** $x^{-1}$ dans $\mathbb{K}$ pour la loi * | $\forall x \in \mathbb{K} \setminus \{0\}\ \exists x^{-1} \in \mathbb{K}$ tel que $x * x^{-1} = x^{-1} * x = 1$ |
| | la loi * est **commutative** | $\forall x, y \in \mathbb{K}$, $x * y = y * x$ |
| 4. | * est **distributive** sur + | $\forall x, y, z \in \mathbb{K}$, $x*(y + z) = x*y + x*z$ |

C'est un total de 11 conditions : celles de l'anneau plus commutativité et inverse pour *

Version courte :

Un **corps ($\mathbb{K}$,+,*)** est un anneau commutatif non réduit à {0} dont tous les membres non nuls sont inversibles.

Exemples classiques :

($\mathbb{Q}$,+,x) ($\mathbb{R}$,+,x) ($\mathbb{C}$,+,x) sont des corps avec + et x représentant l'addition et la multiplication usuelle

Mais ($\mathbb{Z}$,+,x) n'est pas un corps car seuls 1 et -1 sont inversibles.

Exemples nouveaux :

($\mathbb{Q}$,$\sqrt{2}$) = {a+b$\sqrt{2}$ | a, b $\in \mathbb{Q}$} est un corps

($\mathbb{Q}$,i) = {a+ib | a, b $\in \mathbb{Q}$} est un corps avec l'addition et la multiplication usuelle des nombres complexes

Mais {a+b$\pi$ | a, b $\in \mathbb{Q}$} n'est pas un corps.

Ha !

L'ensemble des nombres réels constructibles ($C_{\mathbb{R}}$,+,x) est un corps inclus dans $\mathbb{R}$.

L'ensemble des nombres complexes constructibles ($C_{\mathbb{C}}$,+,x) est un corps inclus dans $\mathbb{C}$.

Ha ! Ha !

# ESPACES VECTORIELS – EXTENSIONS DE CORPS

On cherche à regarder ce qui se passe quand un corps est inclus dans un autre.

Soit $\mathbb{K}$ un corps. On appelle **espace vectoriel sur** $\mathbb{K}$, ou **$\mathbb{K}$-espace vectoriel**, tout ensemble E muni :

- D'une loi interne + telle que (E,+) soit un groupe commutatif
- D'une loi externe de $\mathbb{K}$ sur E vérifiant les 4 propriétés :

| | | |
|---|---|---|
| $\forall x \in E$ | | $1_K.x = x$ |
| $\forall x \in E$ | $\forall \lambda,\mu \in \mathbb{K}^2$ | $(\lambda+\mu).x = \lambda.x + \mu.x$ |
| $\forall (x,y) \in E^2$ | $\forall \lambda \in \mathbb{K}$ | $\lambda.(x+y) = \lambda.x + \lambda.y$ |
| $\forall x \in E$ | $\forall \lambda,\mu \in \mathbb{K}^2$ | $(\lambda\mu).x = \lambda.(\mu.x)$ |

Si E est un $\mathbb{K}$ -espace vectoriel, on appelle **vecteurs** les éléments de E et **scalaires** les éléments de $\mathbb{K}$.

Soient $\mathbb{K}$, $\mathbb{M}$ deux corps avec $\mathbb{K} \subset \mathbb{M}$ Alors $\mathbb{M}$ est un espace vectoriel sur $\mathbb{K}$.

$\mathbb{M}$ est appelé une **extension** de $\mathbb{K}$.
Si la dimension de cet espace vectoriel est finie, alors on appelle le **degré** de l'extension : $[\mathbb{M} : \mathbb{K}] = \dim_K \mathbb{M}$
Si ce degré vaut 2, nous parlons d'**extension quadratique**.

# GROUPES, ANNEAUX & CORPS

On ne saurait trop répéter :

Un **groupe (G,*)** est un ensemble G muni d'une opération * (la **loi de composition**)
vérifiant les propriétés suivantes :

| | | |
|---|---|---|
| 1. | $\forall x, y \in G, x * y \in G$ | * est une **loi de composition interne** sur G |
| 2. | $\forall x, y, z \in G, (x * y) * z = x * (y * z)$ | la loi * est **associative** |
| 3. | $\exists e \in G$ tel que $\forall x \in G, x * e = x$ et $e * x = x$ | il existe un **élément neutre e** dans G |
| 4. | $\forall x \in G$ il existe $x' \in G$ tel que $x * x' = x' * x = e$ | tout élément de G possède un **symétrique** dans G |

Si de plus l'opération vérifie $\forall x, y \in G, x * y = y * x$, on dit que G est un groupe **commutatif** (ou **abélien**).

Un **anneau (A, $\oplus$,$\otimes$)** est un ensemble A auquel est associé deux opérations $\oplus$ et $\otimes$ vérifiant :

| | | |
|---|---|---|
| 1. | $\oplus$ et $\otimes$ sont des **lois de composition interne** | $\forall x, y \in A, x \oplus y \in A$ et $x \otimes y \in A$ |
| 2. | (A, $\oplus$) est un groupe commutatif : | |
| | la loi $\oplus$ est **associative** | $\forall x, y, z \in A, (x \oplus y) \oplus z = x \oplus (y \oplus z)$ |
| | A possède un **élément neutre 0** pour la loi $\oplus$ | $\exists 0 \in A$ tel que $\forall x \in A, x \oplus 0 = x$ et $0 \oplus x = x$ |
| | il existe un **inverse -x** dans A pour la loi $\oplus$ | $\forall x \in A \exists -x \in A$ tel que $x \oplus (-x) = 0$ |
| | la loi $\oplus$ est **commutative** | $\forall x, y \in A, x \oplus y = y \oplus x$ |
| 3. | la loi $\otimes$ est **associative** | $\forall x, y, z \in K, (x \otimes y) \otimes z = x \otimes (y \otimes z)$ |
| 4. | A possède un **élément neutre 1** pour la loi $\otimes$ | $\exists 1 \in A$ tel que $\forall x \in K, x \otimes 1 = x$ et $1 \otimes x = x$ |
| 5. | $\otimes$ est **distributive** sur $\oplus$ | $\forall x, y, z \in A, x\otimes (y \oplus z) = x\otimes y \oplus x\otimes z$ |
| | Si de plus $\otimes$ est commutative l'anneau est **commutatif** | $\forall x, y \in A, x \otimes y = y \otimes x$ |

Un **corps ($\mathbb{K}$,+,*)** est un ensemble $\mathbb{K}$ auquel est associé deux opérations + et * vérifiant :

| | | |
|---|---|---|
| 1. | + et * sont des **lois de composition interne** | $\forall x, y \in \mathbb{K}, x + y \in \mathbb{K}$ et $x * y \in \mathbb{K}$ |
| 2. | ($\mathbb{K}$,+) est un groupe commutatif : | |
| | la loi + est **associative** | $\forall x, y, z \in \mathbb{K}, (x + y) + z = x + (y + z)$ |
| | $\mathbb{K}$ possède un **élément neutre 0** pour la loi + | $\exists 0 \in \mathbb{K}$ tel que $\forall x \in \mathbb{K}, x + 0 = x$ et $0 + x = x$ |
| | il existe un **inverse** -x dans $\mathbb{K}$ pour la loi + | $\forall x \in \mathbb{K} \exists -x \in \mathbb{K}$ tel que $x + (-x) = 0$ |
| | la loi + est **commutative** | $\forall x, y \in \mathbb{K}, x + y = y + x$ |
| 3. | ($\mathbb{K} \setminus \{0\}$,*) est un groupe commutatif : | |
| | la loi * est **associative** | $\forall x, y, z \in \mathbb{K}, (x * y) * z = x * (y * z)$ |
| | $\mathbb{K}$ possède un **élément neutre 1** pour la loi * | $\exists 1 \in \mathbb{K} \setminus \{0\}$ tel que $\forall x \in \mathbb{K}, x * 1 = x$ et $1 * x = x$ |
| | il existe un **inverse** $x^{-1}$ dans $\mathbb{K}$ pour la loi * | $\forall x \in \mathbb{K} \setminus \{0\} \exists x^{-1} \in \mathbb{K}$ tel que $x * x^{-1} = x^{-1} * x = 1$ |
| | la loi * est **commutative** | $\forall x, y \in \mathbb{K}, x * y = y * x$ |
| 4. | * est **distributive** sur + | $\forall x, y, z \in \mathbb{K}, x*(y + z) = x*y + x*z$ |

# L'ANNEAU $\mathbb{Z}/n\mathbb{Z}$

Pour $n \in \mathbb{N}$ $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalences de la relation de congruence modulo n.
$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \ldots, \dot{n-1}\}$ ou $\dot{a}$ est l'ensemble des entiers $\equiv a\ [n]$

On a déjà montré que $\equiv$ est une relation d'équivalence.

| | | |
|---|---|---|
| $\forall\ \dot{a}, \dot{b}, \dot{c} \in \mathbb{Z}/n\mathbb{Z}$ | $a + (b + c) = (a + b) + c$ | l'addition est associative |
| $\forall\ a \in \mathbb{Z}/n\mathbb{Z}$ | $a = a + 0 = 0 + a = a$ | 0 est l'élément neutre |
| $\forall\ a \in \mathbb{Z}/n\mathbb{Z}\ ,\ \exists\ b \in \mathbb{Z}/n\mathbb{Z}$ | $a + b = 0\ \ (b = n - a)$ | tout élément possède un opposé |
| $\forall\ a, b \in \mathbb{Z}/n\mathbb{Z}$ | $a + b = b + a$ | l'addition est commutative |

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

| | | |
|---|---|---|
| $\forall\ a, b, c \in \mathbb{Z}/n\mathbb{Z}$ | $a\ .\ (b\ .\ c) = (a\ .\ b)\ .\ c$ | la multiplication est associative |
| $\forall\ a,b \in \mathbb{Z}/n\mathbb{Z}$ | $a\ .\ b = b\ .\ a$ | la multiplication est commutative |
| $\forall\ a, b, c \in \mathbb{Z}/n\mathbb{Z}$ | $a\ .\ (b + c) = (a\ .\ b) + (b\ .\ c)$ | la multiplication est distributive sur l'addition |
| $\forall\ a \in \mathbb{Z}/n\mathbb{Z}$ | $a = a\ .\ 1 = 1\ .\ a = a$ | 1 est l'élément neutre |

**$(\mathbb{Z}/n\mathbb{Z}, +, x)$ est un anneau commutatif.**

Dans $\mathbb{Z}/10\mathbb{Z}$ : $2\ .\ 5 = 0$ $5\ .\ 5 = 0$ $9\ .\ 9 = 1$ $3^{100} = (3^2)^{50} = (-1)^{50} = 1$

Tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ ont un opposé, mais pas forcément un inverse.

Pour $a \in \mathbb{Z}/n\mathbb{Z}$ on dit que **a est inversible** *SSI* $\exists\ b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a\ .\ b = 1$
On appelle b **l'inverse** de a et on le note $\mathbf{a^{-1}}$
L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $\mathbf{(\mathbb{Z}/n\mathbb{Z})^*}$

Pour $a \in \mathbb{Z}/n\mathbb{Z}$ on dit que a est un **diviseur de 0** *SSI*
$a \neq 0$ et
$\exists\ b \in \mathbb{Z}/n\mathbb{Z},\ b \neq 0$ et $a\ .\ b = 0$

Dans $\mathbb{Z}/20\mathbb{Z}$ :

| | | | |
|---|---|---|---|
| $3x = 9$ | $7\ .\ 3y = 7\ .\ 9$ | $21\ x = 63$ | $x = 3$ |
| $3x = 4$ | $7\ .\ 3y = 7\ .\ 4$ | $21\ x = 28$ | $x = 8$ |
| $3x = 9$ | $7\ .\ 3y = 7\ .\ 9$ | $21\ x = 63$ | $x = 3$ |
| $4x = 3$ | 0, 4, 8, 12, 16, 0, 4… | | Il n'y a pas de solution |
| $4x = 8$ | $4x = 8 + 20n$ | $x = 2 + 5n$ | $x \in \{2, 7, 12, 17\}$ |

# UN PEU D'HISTOIRE

Die Lösung linearer und quadratischer Gleichungen wurde in Italien in der Renaissance (16. JH) auf kubische und quartische Gleichungen erweitert (Scipione dal Ferro, Niccolò Tartaglia, Lodovico Ferrari, Gerolamo Cardano).

François Viète ist ein wichtiger Begründer der Algebra und deren Anwendung auf die Geometrie mit konsequenter Verwendung von Variablen und Gleichungen zwischen diesen.

Die Theorie der Gleichungen wurde im 18. Jahrhundert weiter ausgebaut (Leonhard Euler, Joseph-Louis Lagrange) und die Lösung im Komplexen mit einbezogen. 1799 bewies Carl Friedrich Gauß den Fundamentalsatz der Algebra.

Algebra war damals weitgehend Untersuchung algebraischer Gleichungen der Form $a_n x^n+a_{n-1}\,x^{n-1}+\cdots+a_1 x+a_0=0$.

Um 1830 entwickelte Évariste Galois (1811–1832) die Galoistheorie. Diese kann als der Beginn der *modernen Algebra* verstanden werden. Galois und unabhängig Niels Henrik Abel lösten das lange offene Problem der Lösung algebraischer Gleichungen von höherem als viertem Grad, wobei man unter Lösung damals die Darstellung durch die üblichen Rechenoperationen und Wurzelausdrücke („Radikale" genannt) verstand, indem sie zeigten, dass dies ab dem fünften Grad im Allgemeinen nicht mehr möglich ist (Satz von Abel-Ruffini). Von Galois stammen in diesem Zusammenhang die Anfänge der Gruppentheorie (Permutationsgruppen, den abstrakten Gruppenbegriff führte später Arthur Cayley ein) und Körpertheorie (endliche Körper, auch Galois-Felder genannt, Körpererweiterungen). Die Gruppentheorie von Galois wurde insbesondere von Camille Jordan im 19. Jahrhundert ausgebaut mit Beiträgen von Otto Hölder (Satz von Jordan-Hölder) und anderen. Die Theorie kontinuierlicher Gruppen (Lie-Gruppen) wurde von Sophus Lie im 19. Jahrhundert begründet, mit Struktursätzen und Theorie der Lie-Algebren von Wilhelm Killing und Élie Cartan gegen Ende des 19. JH.

Weitere algebraische Strukturen kamen hinzu, wobei verschiedene *Algebren* teilweise geometrisch motiviert waren (Hermann Grassmann mit dem Vektor-Konzept und Grassmann-Algebra als Basis der Differentialformen von Élie Cartan, Quaternionenvon William Rowan Hamilton, Clifford-Algebra nach William Kingdon Clifford, die auch erst viel später mit dem Spinorkonzept Bedeutung in den Anwendungen erlangte) oder aus der Logik kamen (Boolesche Algebra), teilweise auch einfach aus der Frage der Erweiterung der komplexen Zahlen (hyperkomplexe Zahlen, Divisionsalgebren, zu denen auch die Quaternionen gehören). Wichtige Klassifikationssätze zu Algebren waren der Satz von Wedderburn und der Satz von Frobenius.

Die Lineare Algebra entstand aus der Theorie der Matrizen und Determinanten (Augustin-Louis Cauchy, Cayley, James Joseph Sylvester). Die Erweiterung zur multilinearen Algebra (Tensorkonzept) begann Ende des 19. Jahrhunderts in der Differentialgeometrie (Gregorio Ricci-Curbastro, Tullio Levi-Civita) und Physik.

Die Darstellungstheorie insbesondere von Gruppen entwickelte sich ebenfalls ab Ende des 19. JH (Ferdinand Georg Frobenius, Issai Schur). Sie ist besonders für die Anwendungen der Gruppentheorie in den Naturwissenschaften wichtig, sowohl was endliche Gruppen betrifft, als auch was Lie-Gruppen betrifft (Darstellungstheorie von Elie Cartan mit dem Spinorkonzept, Hermann Weyl und anderen).

Die Idealtheorie wurde im 19. JH von Richard Dedekind und Leopold Kronecker begründet (mit Anwendungen auf die Algebraische Zahlentheorie und Funktionenkörper). Von Dedekind stammen auch weitere wichtige Prinzipien der abstrakten Algebra (so die Auffassung der Galoisgruppe als Automorphismengruppe von Körpern, Konzepte von Ring und Modul). In der Schule von David Hilbert wurde die Theorie der Polynomideale (kommutative Ringe im Rahmen der kommutativen Algebra) begründet, mit wichtigen Beiträgen von Emmy Noether, Emanuel Lasker, Francis Macaulay und später weiter entwickelt von Wolfgang Krull. Von Ernst Steinitz wurde um 1909 die algebraische Theorie der Körper entwickelt. Von zentraler Bedeutung für die Entwicklung der modernen Algebra war die Schule von Emmy Noether in Göttingen, aus der das Standards setztende Lehrbuch *Moderne Algebra* von van der Waerden hervorging. Von hier aus gingen auch Anwendungen auf andere Gebiete aus wie die Topologie (algebraische Topologie) und die kommutative Algebra wurde zur Grundlage der algebraischen Geometrie. Weitere wichtige Vertreter der Algebra waren damals in Deutschland Emil Artin und Helmut Hasse.

Nach dem Zweiten Weltkrieg begann der Siegeszug einer weiteren Abstraktionsstufe (homologische Algebra, Kategorientheorie), sowohl in algebraischer Topologie (Samuel Eilenberg, Norman Steenrod, Saunders MacLane) als auch in algebraischer Geometrie (Alexander Grothendieck).

Ein Höhepunkt der Gruppentheorie war im 20. Jahrhundert die Vollendung der Klassifikation der endlichen einfachen Gruppen und die Entwicklung der Theorie unendlichdimensionaler Darstellungen zum Beispiel von Lie-Gruppen (Harish Chandra, Anwendung in der Quantentheorie und im Langlands-Programm).