Algorithmique.
Rappels mathématiques.

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

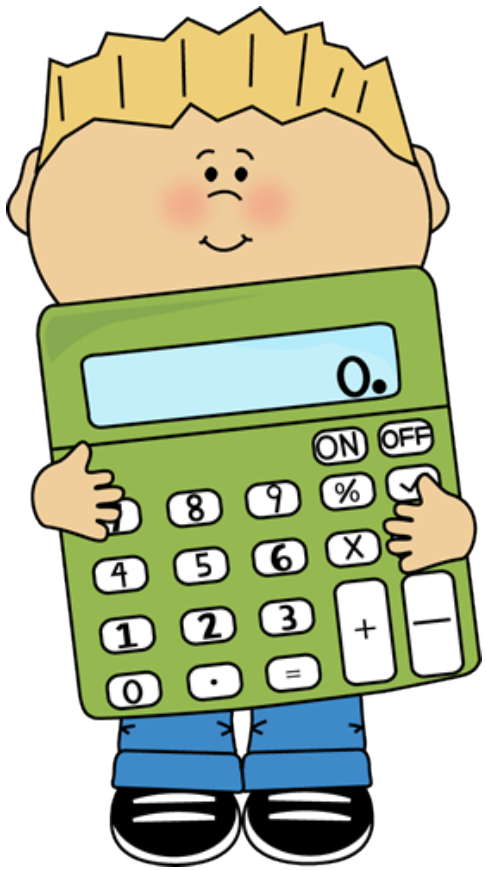
Cours 2

Algorithme

Définition

Algorithme = Suite finie d'opérations élémentaires constituant un schéma de calcul ou de résolution d'un problème

(Petit Larousse)



Mathématiques ≠ Informatique

Problèmes pratiques

La pratique = Ligne de séparation entre les maths et l'info :

- **Mathématiques :** on résout un problème en montrant l'existence d'une solution.
- **Informatique :** on cherche à construire cette solution en s'intéressant à l'effcacitè de la construction.

Un algorithme permet un traitement (informatique) automatisé si :

- la solution existe
- l'algorithme soit performant

Crypto

Algorithmes et cryptographie

- Représenter les tâches à accomplir, manipuler des objets mathématiques :
  - calculer un chiffrement
  - générer une signature
  - retrouver une clé
- Comparer les algorithmes :
  - effcacité des schémas cryptographiques
  - dificulté d'attaquer

Complexité

Mesurer un algorithme

La variable/le paramètre = la taille des données en entrée de l'algorithme

- **temps** = nombre d'opérations élémentaires
- **espace** = mémoire nécessaire à l'algorithme
- **comportement** = mesure aymptotique

Variantes : cas "moyen" ou "pire" des cas

Complexités élémentaires

Les opérations arithméthiques

- **Addition :** $\boxed{x+y}$ complexité $\mathcal{O}(\log x + \log y)$
- **Soustraction :** $\boxed{x-y}$ complexité $\mathcal{O}(\log x + \log y)$
- **Multiplication :** $\boxed{x \times y}$ complexité $\mathcal{O}(\log x \cdot \log y)$
- **Division :** $\boxed{x = q \times y + r}$ complexité $\mathcal{O}(\log q \cdot \log y)$
- **Exponentiation :** $\boxed{x^n}$ complexité ???

Exponentiation

Algorithme naïf

Calcul de $n-1$ multiplications successives :

$$x^n = x \cdot x \cdot x \ldots x$$

Optimisation

Pour $n = 2^k$

$$x^n = \left(\ldots \left(\left(x^2 \right)^2 \right)^2 \ldots \right)^2$$

k multiplications au lieu de $n = 2^k$

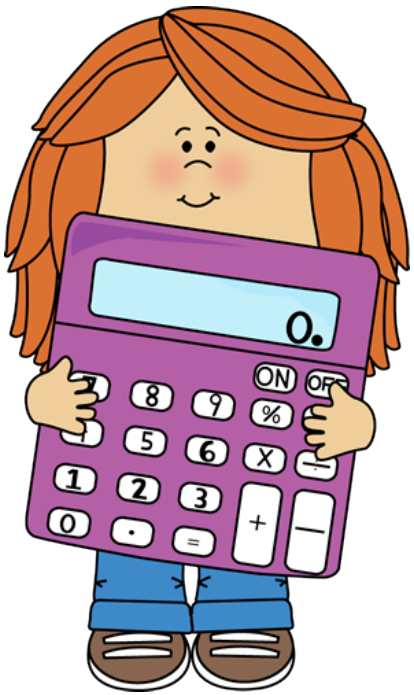
Comparaisons

Comparaison de fonctions

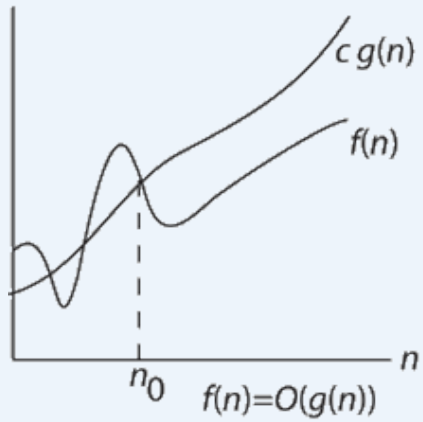
Soit f et g deux fonctions croissantes positives
$f, g : \mathbb{N} \to \mathbb{R}$

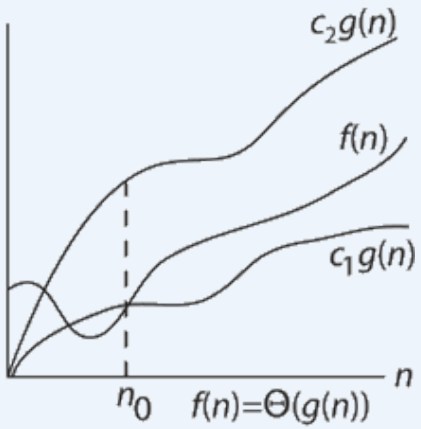
- $f = \mathcal{O}(g)$ si $\exists\ c > 0$ tel que : $f(n) < c \cdot g(n)$ pour $n \to \infty$
- $f = \Theta(g)$ si $f = \mathcal{O}(g)$ and $g = \mathcal{O}(f)$
- $f = \Omega(g)$ si $g = \mathcal{O}(f)$
- $f = o(g)$ si $\forall\ c > 0$ on a : $f(n) < c \cdot g(n)$ pour $n \to \infty$
- $f = \omega(g)$ si $g = o(f)$

Exemples de comparaisons



Fonctions





- $3n^2 + 3n + 1 = \Omega(9n^2) = \mathcal{O}(n^3/100)$
- $1000n^{512} = \mathcal{O}(1.01^n)$
- $2^n = \mathcal{O}(10^n) = \mathcal{O}(n!)$
- $\log n = o(n) = o(n \log n) = \mathcal{O}(n \log n)$

Exemple de complexité

Multiplication matricielle

Multiplier deux matrices carrées de dimension n :

- dénombrement des multiplications entre coeficients
- algorithme simple : $\mathcal{O}(n^3)$
- algorithme (très) complexe : $\mathcal{O}(n^{2,376})$

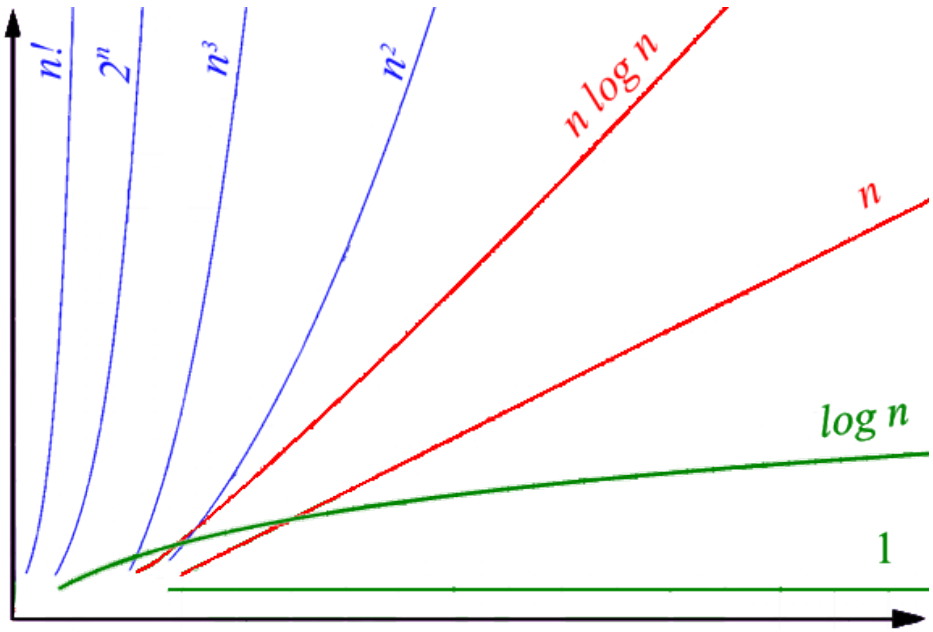
 $n = 5000$: algorithme 200 fois plus rapide.

 $n = 1$ million : algorithme 5000 fois plus rapide ! (ex :rapport de 1 heure à 200 jours)

Hiérarchie entre fonctions

Hiérarchie élémentaire

- f est **logarithmique** si $f(n) = \mathcal{O}(\log(n)^{\mathcal{O}(1)})$
- f est **polynomiale** si $f(n) = \mathcal{O}(n^{\mathcal{O}(1)})$
- f est **exponentielle** si $f(n) = \Omega(\exp(\Omega(n)))$



Hiérarchie entre fonctions

Hiérarchie intermédiaire

Pire que polynomiale ...

- f est **super-polynomiale** si $f(n) = \Omega(n^{\omega(1)})$
- f est **sous-exponentielle** si $f(n) = \mathcal{O}(\exp(o(n)))$

... moins pire qu'exponentielle

La fonction $L_x[\alpha, c] = \exp(c \cdot (x)^{\alpha}(\log x)^{1-\alpha})$

- **polynomiale** si $\alpha = 0$
- **exponentielle** si $\alpha = 1$
- **sous-exponentielle** et **super-polynomiale** sinon

Exemples

$$1 \lll \log\log x \lll (\log\log x)^n \lll \frac{\log x}{\log\log x} \lll$$

$$\log x \lll (\log x)^n \lll \sqrt[n]{x} \lll \frac{x}{\log x} \lll x \lll$$

$$x\log x \lll x^n \lll \underbrace{\exp((x)^{\alpha}(\log x)^{1-\alpha})}_{0\to\alpha\to 1}$$

$$\frac{exp(x)}{x^n} \lll \exp(x) \lll (exp(x))^n$$

$$\lll x! \lll x^x \lll (x!)^n \lll exp(x^n) \lll \ldots$$

Efficacité en pratique

En pratique

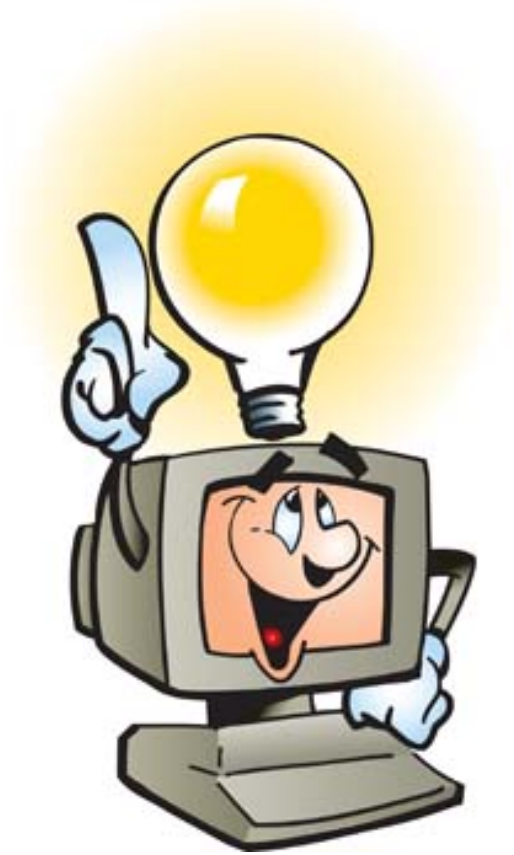

logarithmique : toujours facile


polynomial : facile (si l'exposant reste petit)


sous-exponentiel, **super-polynomial** : très difficile
possible jusqu'à une taille *critique*


exponentiel : extrêmement difficile
très vite impossible en pratique

Efficacité en pratique



Faisable = Polynomial

Pour être utilisable, un algorithme doit être

- **polynomial** en moyenne
- **super-polynomial** dans le pire des cas
- implémentable facilement
- efficace en pratique

Exemples de complexités

$k = \lvert x \rvert = \log_2(x)$	64	128	512	1024
k^2	2^{12}	2^{14}	2^{18}	2^{20}
k^3	2^{18}	2^{21}	2^{27}	2^{30}
$O\left(e^{k^{1/3}(\ln k)^{2/3}}\right)$	2^{30}	2^{41}	2^{78}	2^{105}
$2^{k/2}$, soit $\sqrt{x}$	2^{32}	2^{64}	2^{256}	2^{512}
2^k, soit x	2^{64}	2^{128}	2^{512}	2^{1024}

Exponentiation

Algorithme naïf

Calcul de $n-1$ multiplications successives :

$$x^n = x \cdot x \cdot x \ldots x$$

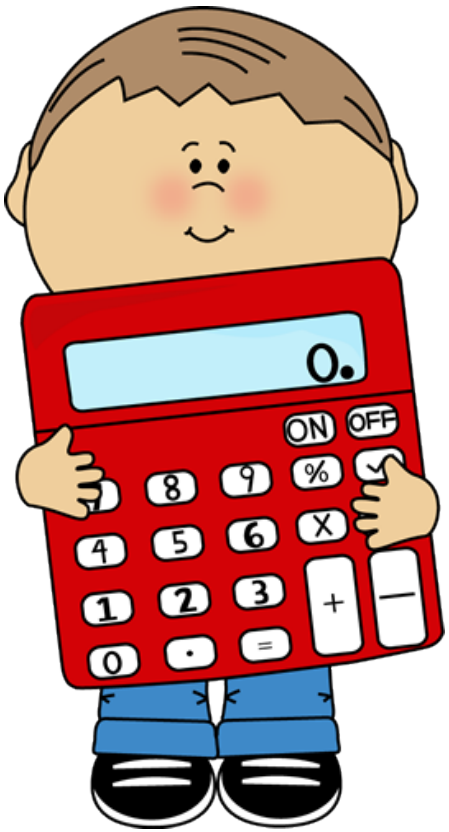
Idée

Décomposer len écriture binaire : $n = 16 = 2^4$

$$x^{16} = \left(\left(\left(x^2\right)^2\right)^2\right)^2$$

4 multiplications au lieu de $n = 2^4 = 16$

Exponentiation



Exemple

Pour calculer x^{11} :

- $11 = 8 + 2 + 1 = 2^3 + 2^1 + 2^0$
- Calcul de 1, x^2, $x^8 = \left(\left(x^2\right)^2\right)^2$
- $x^{11} = x^8 \cdot x^2 \cdot x$

Algorithme d'Euclide

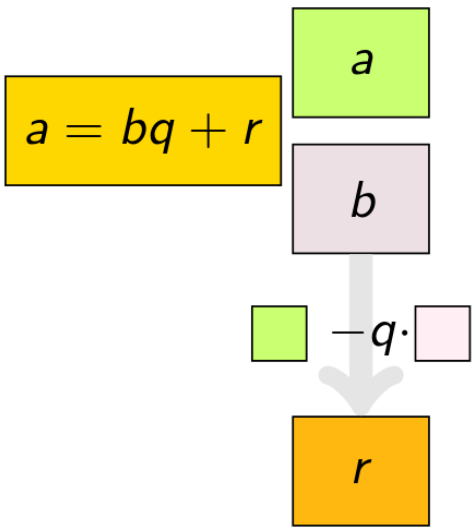
But

Algorithme de calcul du $d = \mathbf{pgcd}(a, b)$.

PGCD

- **Définition :** plus grand entier d divisant à la fois **a** et **b**
- **Propriétés :** si $a > b$ alors on a $\mathbf{a} = \mathbf{b}q + r$
  - les diviseurs communs à **a** et **b** sont les mêmes que les diviseurs communs à **b** et **r**
  - donc $\mathbf{pgcd}(a, b) = \mathbf{pgcd}(b, r)$

Algorithme d'Euclide : Exemple



a	b	q
546738492	6754024	
6754024	6416572	80
6416572	337452	1
337452	4984	19
4984	3524	67
3524	1460	1
1460	604	2
604	252	2
252	100	2
100	52	2
52	48	1
48	4	1
4	0	12

Algorithme d'Euclide étendu

But

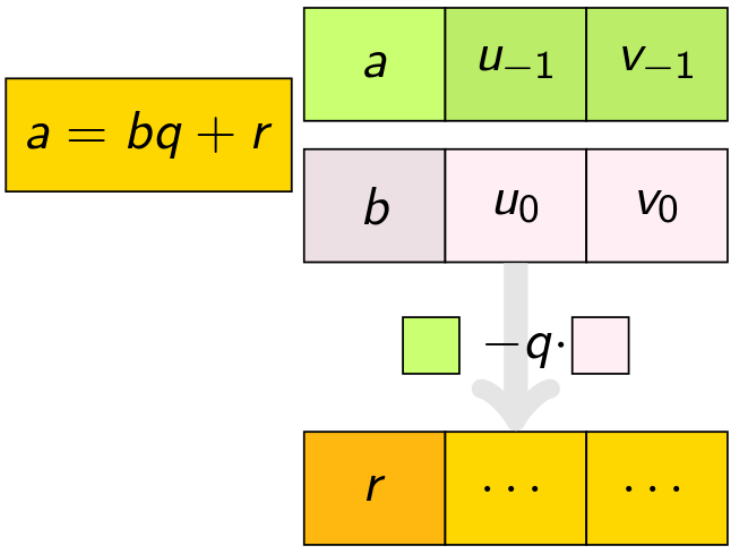
Agorithme de calcul des coeficients (u, v) tels que

$$\mathbf{a}u + \mathbf{b}v = d = \text{pgcd}(a, b)$$

Théorème de Bézout

- **Définition :** (u, v) sont les *coefficients de Bézout* pour les deux entiers naturels **a** et **b**
- **Propriétés :** **a** et **b** sont premiers entre eux si et seulement s'il existe deux entiers relatifs (u, v) tels que $au + bv = 1$.

Algorithme d'Euclide étendu : Exemple



a	u	v	q
4864	1	0	
3458	0	1	1
1406	1	−1	2
646	−2	3	2
114	5	−7	5
76	−27	38	1
38	32	−45	2
0	...	...	

$$38 = 32a - 45b = 32 \times 4864 - 45 \times 3458$$

Primalité

Définition

Un nombre p est premier si ses seuls diviseurs positifs sont p et 1.

Liste : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Propriétés

- Entre n et $2n$, il y a toujours un nombre premier.
- Un nombre pair est toujours la somme de 2 premiers.
- Un nombre impair (>5) est la somme de 3 premiers.

Théorème d'Euclide

Il existe une infinité de nombres premiers.

Décomposition en facteurs prémiers

Théorème fondamental de l'arithmétique

Tout entier **n** s'écrit de façon unique comme produit de puissances de nombres premiers :

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

PGCD

Si $a = \prod_i p_i^{\alpha_i}$ et $b = \prod_i p_i^{\beta_i}$, alors :

$$\text{pgcd}(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

Théorème Gauss

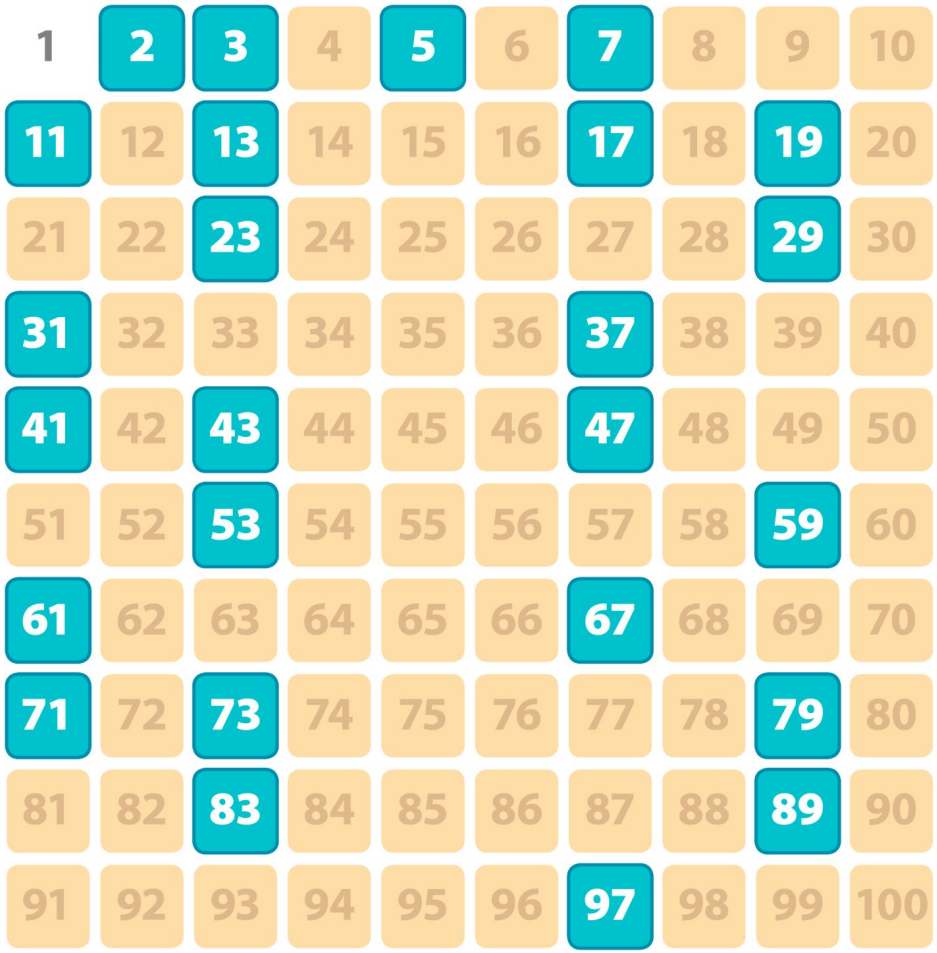
Si p est premier et $p|ab$ alors $p|a$ ou $p|b$.

Distribution des nombres premiers

Question

Il existe une infinité de nombres premiers. (Euclide)

Comment sont-ils *répartis* ? ? ?



Distribution des nombres premiers

Théorème des nombres premiers

Soit $\pi(n)$ le nombre de nombre premiers inférieurs ou égaux à n.

$$\pi(n) \sim \int_2^n \frac{dx}{\ln n} \sim \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2n}{(\ln n)^3} + \dots$$

Distribution des nombres premiers

En pratique

Le nombre de premiers inférieurs à n est de l'ordre de $n/\ln n$.

Conclusions :

- il y a environ 2^{1014} nombres premiers de 1024 bits
- la probabilité qu'un nombre x soit premier est proche de $1/\ln n$,
- probabilité de $1/710$ pour un entier de 1024 bits

Arithmétique modulaire

Le "groupe de l'horloge"

Heures :

- $2h + 5h = 7h$
- $9h + 4h = 1h \mod 12h$
- $8h + 12h = 8h$

Minutes :

- $45 + 25 = 10 \mod 60$ min
- $50 + 30 = 20 \mod 60$ min

Addition modulaire $\mathbb{Z}_7$

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $2 + 4 = 6$
- $4 + 5 = 9 = 7 + 2 = 2 \bmod 7$
- $3 + 4 = 0$

$\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Groupe additif $(\mathbb{Z}_n, +)$

$(\mathbb{Z}_n, +)$ forme un **groupe commutatif d'ordre** n.

Définition

Un groupe est un couple ensemble-loi de composition $(\mathbb{G}, \star)$ qui vérifie

- **associativité :** $\forall a, b, c, \in \mathbb{G}$: $(a \star b) \star c = a \star (b \star c)$
- **élement neutre :** $\exists e \in \mathbb{G}, \forall a \in \mathbb{G}$: $a \star e = e \star a = a$
- **inversion :** $\forall a \in \mathbb{G}, \exists b \in \mathbb{G}$: $a \star b = b \star a = e$

Propriétés

- **commutativité :** $\forall a, b, c, \in \mathbb{G}$: $a \star b = b \star a$
- **ordre de** $\mathbb{G}$ **:** nombre d'éléments du groupe $\mathbb{G}$

Multiplication modulaire $\mathbb{Z}_7$

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $3 \times 5 = 5 + 5 + 5 = 10 + 5$
  $= 3 + 5 = 8 = 7 + 1$
  $= 1 \bmod 7$
- $3 \times 5 = 15 = 2 \cdot 7 + 1$
  $= 1 \bmod 7$
- $6 \times 4 = 24 = 3 \cdot 7 + 3 = 3 \bmod 7$

$\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication modulaire $\mathbb{Z}_7$ et $\mathbb{Z}_8$

$\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$\mathbb{Z}_8$

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Anneau $(\mathbb{Z}_n, +, \cdot)$

$(\mathbb{Z}_n, +, \cdot)$ forme un **anneau commutatif**.

Définition

Un anneau est un triplet, ensemble et deux lois de composition, $(\mathbb{G}, +, \cdot)$ qui vérifie

- $(\mathbb{G}, +)$ est un groupe commutatif avec élement neutre 0
- **associativité :** $\forall a, b, c, \in \mathbb{G}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **élement neutre :** $\exists e \in \mathbb{G}, \forall a \in \mathbb{G}$: $a \cdot e = e \cdot a = a$
- **distributivité :** $\forall a, b, c \in \mathbb{G}$: $a \cdot (b + c) = a \cdot b + a \cdot c$

Propriétés

- **anneau commutatif :** $\forall a, b, c, \in \mathbb{G}$: $a \cdot b = b \cdot a$
- **élément inversible :** $a \neq 0$ est inversible par rapport à $\cdot$ si $\exists b \in \mathbb{G}$: $a \cdot b = b \cdot a = e$

Inverse modulaire $\mathbb{Z}_7$

Inverse de a modulo n :

entier $b = a^{-1}$ tel que

$$a \times b = 1 \mod n$$

- $\mathbb{Z}_7^\star = \{1, 2, 3, 4, 5, 6\}$
- $3^{-1} = 5 \mod 7$
- $4^{-1} = 2 \mod 7$
- $6^{-1} = 6 \mod 7$

$\mathbb{Z}_7^\star$

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Inverse modulaire $\mathbb{Z}_8$

- 2,4 et 6 sont *non-inversibles*
- 1,3,5 et 7 sont *inversibles* (et leur propre inverse !)
- attention aux écritures
  - éviter ~~$3 = 1/3$~~
  - proscrire ~~$\sqrt{1} = 3$~~
- écrire $3^{-1} = 3$

$\mathbb{Z}_8$

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Inverse modulaire $\mathbb{Z}_6$

Que faire avec $\mathbb{Z}_6$?

- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
- $5^{-1} = 5 \bmod 6$
- $4^{-1} =?? \bmod 6$

  L'inverse de 4 *n'est pas défini* modulo 6

$\mathbb{Z}_6$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Il « reste » $\{1, 5\}$: $\mathbb{Z}_6^\star$

$\times$	1	5
1	1	5
5	5	1

Éléments inversibles

Définition

$\mathbb{Z}_n^\star =$ l'ensemble des éléments inversibles modulo n.


Attention ! $\mathbb{Z}_n^\star \neq \mathbb{Z}_n \setminus \{0\}$

Exemples

- $\mathbb{Z}_7^\star = \{1,2,3,4,5,6\}$: tous les éléments sont inversibles
- $\mathbb{Z}_6^\star = \{1,5\}$: on a $Z_6^\star \neq \mathbb{Z}_6 \setminus \{0\}$

Groupe multiplicatif $\mathbb{Z}_n^\star$

$(\mathbb{Z}_n^\star, \cdot)$ forme un groupe multiplicatif.

Critère d'inversibilité

Question

Quels sont les entiers inversibles modulo n ?

Critère

$x \in \mathbb{Z}_n^\star$ est inversibles modulo n si et seulement si $\text{pgcd}(x, n) = 1$.
Preuve : T. Bézout.

Cas de $n = p$ premier : $\mathbb{Z}_p$

Les entiers inversibles modulo p :
Toutes les éléments non-nuls de $\mathbb{Z}_p$ sont premiers avec p

$$\mathbb{Z}_p^\star = \mathbb{Z}_p \setminus \{0\}$$

Calcul de l'inverse modulaire

Applications $x^{-1} \mod n$

- Il existe u et v tels que $xu + nv = \text{pgcd}(x, n) = 1$
- Trouver l'inverse d'un élément revient à calculer u.
- L'algorithme d'Euclid étendu calcule des coeficients (u, v)

Division modulaire $\mathbb{Z}_7^\star$

Division modulaire = Multiplication par l'inverse modulaire

- $\mathbb{Z}_7 = \{1, 2, 3, 4, 5, 6\}$
- $5 \div 3 = 5 \times 3^{-1} = 5 \times 5 = 25 = 4 \bmod 7$
- $4 \div 6 = 4 \times 6^{-1} = 4 \times 6 = 24 = 3 \bmod 7$
- $6 \div 6 = 6 \cdot 6^{-1} = 6 \times 6 = 1 \bmod 7$

$\mathbb{Z}_7^\star$

$\div$	1	2	3	4	5	6
1	1	4	5	2	3	6
2	2	1	3	4	6	5
3	3	5	1	6	2	4
4	4	2	6	1	5	3
5	5	6	4	3	1	2
6	6	3	2	5	4	1

Corps $(\mathbb{Z}_p, +, \cdot)$

$(\mathbb{Z}_p, +, \cdot)$ forme un **corps commutatif**.

Définition

Un corps est ensemble avec deux lois de composition, $(\mathbb{G}, +, \cdot)$ qui vérifient

- $(\mathbb{G}, +)$ est un groupe commutatif pour l'addition
- $(\mathbb{G} \setminus \{0\}, \cdot)$ est un groupe pour la multiplication
- **distributivité :** $\forall a, b, c \in \mathbb{G} :$ $a \cdot (b + c) = a \cdot b + a \cdot c$
- **corps commutatif :** $\forall a, b, c, \in \mathbb{G} :$ $a \cdot b = b \cdot a$

Théorème - Corps fini $\mathbb{F}_p$

$(\mathbb{Z}_p, +, \cdot)$ est un corps, noté $\mathbb{F}_p$, si et seulement si p est premier.

Récapitulatif sur $\mathbb{Z}_n$

A retenir

Deux cas distincts :

- $n = p$ est **premier** : $(\mathbb{Z}_p, +, \cdot)$ est un corps
  - tous les éléments sont inversibles (Euclide)
  - $\mathbb{Z}_p^\star$ coïncide avec $\mathbb{Z}_p \setminus \{0\}$

- n est **composé** : $(\mathbb{Z}_n, +, \cdot)$ est un anneau
  - seuls les éléments de $\mathbb{Z}_n^\star$ sont inversibles
  - $\mathbb{Z}_n^\star$ **n'est pas** $\mathbb{Z}_n \setminus \{0\}$

Ordre du groupe $\mathbb{Z}_n^\star$

n=p premier

Tous les éléments non-nuls sont premiers avec p :

$\mathbb{Z}_p^\star = \{1,\ 2,\ 3, \ldots,\ p-1\}$ ordre $|\mathbb{Z}_p^\star| = p-1$

n composé

Tous les éléments non-nuls premiers avec n sont dans $\mathbb{Z}_n^\star$
Leur nombre est donné par la **fonction d'Euler**.

Fonction d'Euler

Définition

- $\varphi(n)$ est le nombre d'entiers de $[1, n]$ qui sont premiers avec n.
- $\varphi(n)$ désigne l'ordre du groupe multiplicatif $\mathbb{Z}_n^\star$

Propriétés

si p est premier et q premier :

- $\varphi(p) = p - 1$
- $\varphi(p^e) = p^{e-1}(p-1)$
- $\varphi(pq) = \varphi(p)\varphi(q)$

Fonction d'Euler

Calcul de $\varphi(n)$

Formule générale pour $n = \prod_i p_i^{\alpha_i}$:

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p} \right)$$

Exponentiation modulaire

Théorème de Lagrange

Si $\mathbb{G}$ est un groupe multiplicatif d'ordre n, alors :

$$\forall g \in \mathbb{G} \quad g^n = e$$

Cas de $\mathbb{Z}_7^\star$

$$\begin{aligned} 3^6 &= 3 \times 3 \times 3 \times 3 \times 3 \times 3 \quad \mod 7 \\ &= 9 \times 9 \times 9 \quad \mod 7 \\ &= 2 \times 2 \times 2 \quad \mod 7 \\ &= 8 = 1 \quad \mod 7 \end{aligned}$$

L'ordre de $|\mathbb{Z}_7^\star| = \varphi(7) = 7 - 1 = 6$, d'où $3^6 = 1 \mod 7$

Exponentiation modulaire

Petit théorème de Fermat

Pour p premier et tout entier a on a

$$a^p = a \mod p$$

Preuve : $a^{\varphi(p)} = a^{(p-1)} = 1 \mod p$, donc $a^p = a \mod p$.

Théorème d'Euler

Pour tout entier n et tout $a \in \mathbb{Z}_n^\star$, on a

$$a^{\varphi(n)} = 1 \mod n$$

Exponentiation modulaire

En pratique

Règles :

- Dans une exponentiation modulaire (modulo un entier M), les exposants doivent être pris modulo $\varphi(M)$.
- Effectuer les réduction modulaires au fur et à mesure.

Théorème des restes chinois

Problème

Pour p et q premiers et a et b entiers on cherche x tel que :

$$x = a \mod p \quad \text{et} \quad x = b \mod q$$

Théorème CRT (Chinese Remainder Theorem)

La solution x est unique modulo pq et se calcule par l'algorithme de Gauss :

$$x = aq(q^{-1} \mod p) + bp(p^{-1} \mod q) \mod pq$$