

Mid term

Nombre premier

Question

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

Solution

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


Groupe additif

Groupe

Définition (Groupe)


Un **groupe** (\mathbb{G}, \star) est un ensemble \mathbb{G} muni d'une opération \star qui vérifie les propriétés suivantes :

- Pour tous les éléments $a, b \in \mathbb{G}$, le résultat de $a \star b$ appartient également à \mathbb{G} (**Loi Interne**).
- Pour tous les éléments $a, b, c \in \mathbb{G}$, l'égalité $(a \star b) \star c = a \star (b \star c)$ est vraie (**Associativité**).
- Il existe un élément $e \in \mathbb{G}$ tel que pour tout $a \in \mathbb{G}$, on a $a \star e = e \star a = a$ (**Élément Neutre**).
- Pour tout élément $a \in \mathbb{G}$, il existe un élément $b \in \mathbb{G}$ tel que $a \star b = b \star a = e$ (**Élément Symétrique**).

 Un groupe (\mathbb{G}, \star) pour lequel $a \star b = b \star a$ pour tout $a, b \in \mathbb{G}$ est appelé **commutatif**, ou **abélien**.

Théorème (Groupe Abélien)

L'ensemble $\mathbb{Z}_m = \{0, 1, \dots, m-2, m-1\}$ muni de l'addition modulo m , où $m > 0$ est un entier naturel non-nul, est un groupe abélien.

 On appelle parfois l'élément symétrique d'un groupe additif, un **opposé** ou un **inverse additif**.

Inverse modulaire

Inverse Modulaire

Définition (Inverse Modulaire)

Un entier a est **inversible** modulo m si l'équation $ax \equiv 1 \pmod{m}$ possède une solution $x \in \mathbb{Z}$.

👉 $ax \equiv 1 \pmod{m}$ possède une solution $x \in \mathbb{Z}$ si l'équation $ax + ym = 1$ possède une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

👉 On note a^{-1} **l'inverse modulaire** (ou inverse multiplicatif) de a .

Théorème (Inverse Modulaire)

a est **inversible modulo** m si et seulement si $\text{pgcd}(a, m) = 1$.

- $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$.
- $ab \bmod m = (a \bmod m)(b \bmod m) \bmod m$.
- $a^b \bmod m = (a \bmod m)^b \bmod m$.

Indicatrice d'Euler

- Si p est un nombre premier, alors $\varphi(p) = p - 1$.
- Si p est premier et $k > 1$, $\varphi(p^k) = (p - 1)p^{k-1}$.
- Si $\text{pgcd}(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$
- 👉 Si $p \neq q$ sont des nombres premiers, alors $\varphi(pq) = (p - 1)(q - 1)$.

$$\varphi(n) = n \prod_{p \text{ premier divise } n} \left(1 - \frac{1}{p}\right)$$

- Par exemple :

$$\varphi(12) = 12 \cdot \prod_{p \in \{2,3\}} \left(1 - \frac{1}{p}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

Groupe multiplicatif

Théorème (Groupe Multiplicatif \mathbb{Z}_m^*)

L'ensemble $\mathbb{Z}_m^* = \{1 \leq a \leq m : \text{pgcd}(a, m) = 1\}$ muni de la multiplication modulo m , où $m > 0$ est un entier naturel non-nul, est un groupe abélien.

- 👉 L'addition n'a pas de sens dans un groupe multiplicatif !
- $2/5 \pmod{7} \equiv 2 \cdot (5^{-1}) \pmod{7} \equiv 2 \cdot 3 \pmod{7} \equiv 6 \pmod{7}$
- $5^3 \pmod{7} = 6$. Donc le logarithme discret en base 5 de 6 modulo 7 est 3.

L'ordre d'un élément (Théorème de Lagrange)

Théorème (Joseph-Louis Lagrange, 1771)

L'ordre $\text{ord}(a)$ d'un élément a d'un groupe fini divise l'ordre du groupe (le nombre d'éléments du groupe).

Théorème de Fermat-Euler

Le théorème suivant est appelé le **petit théorème de Fermat**.

Théorème (Pierre de Fermat, 1640)

Si p est un nombre premier, et si a est un entier non-divisible par p , alors

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

Il a été généralisé par le mathématicien bâlois Leonhard Euler :

Théorème (Leonhard Euler, 1761)

Si n est un entier naturel et a **un entier premier avec n** , alors

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

Anneaux et Corps

Un **anneau** $(\mathbb{A}, +, \times)$ est un ensemble \mathbb{A} muni de deux opérations $+$ et \times qui vérifient les propriétés suivantes :

- $(\mathbb{A}, +)$ est un groupe abélien.
- L'opération \times est une loi de composition interne et associative sur \mathbb{A} .
- L'opération \times est distributive à gauche et à droite par rapport à $+$.
- L'opération \times admet un élément neutre dans \mathbb{A} .
- Un anneau $(\mathbb{A}, +, \times)$ pour lequel \times est également commutatif s'appelle un **anneau commutatif**.
- 👉 On remarque que $(\mathbb{A} \setminus \{0\}, \times)$ forme **presque** un groupe : il ne lui manque que l'exigence d'inverse !
- 👉 Ainsi, $\{0, 1, \dots, m-1\}$ muni de l'addition et de la multiplication modulo m forme un anneau.

Théorème (Corps Fini)

- Si \mathbb{F} est un corps fini, alors \mathbb{F} contient p^m éléments, avec p premier et $m \geq 1$.
- Pour chaque puissance p^m d'un nombre premier, il existe un unique corps fini d'ordre p^m .

- 👉 Le corps à p^m éléments est noté $\text{GF}(p^m)$, en honneur du mathématicien français **Évariste Galois** (1811-1832).
- 👉 Le nombre p est appelé **caractéristique** du corps $\text{GF}(p^m)$.
- 👉 Le plus petit corps fini est $\text{GF}(2)$. Il ne comporte que les éléments 0 et 1.

Polynômes sur un corps

Définition (Anneau des Polynômes sur un Corps)

On note $\mathbb{Z}_p[x]$ **l'anneau** formé de l'ensemble des polynômes en x possédant des coefficients dans \mathbb{Z}_p .

- $x^5 + x^2 + x + 1 \in \mathbb{Z}_2[x]$,
- $3x^5 + 2x^2 + x \in \mathbb{Z}_5[x]$,
- 👉 On appelle $0 \in \mathbb{Z}_p[x]$ le **polynôme nul**.
- 👉 Un polynôme dont le monôme de plus haut degré possède un coefficient égal à 1 s'appelle un polynôme **unitaire**.
- 👉 Il est possible d'additionner et de multiplier des polynômes entre eux, le calcul sur les coefficients se faisant dans le corps sous-jacent.
- Un polynôme **de degré deux ou trois** est irréductible si et seulement si il n'a pas de racine.
- **Exemple** : $x^2 + 1$ est irréductible dans $\mathbb{Z}_3[x]$ mais pas dans $\mathbb{Z}_2[x]$.
- **Attention** : Contrairement à la factorisation des entiers, il existe des algorithmes efficaces pour factoriser un polynôme (algorithme de Cantor–Zassenhaus).
- A la main, pour des degrés $k > 2$, la solution la plus facile est de tester si le polynôme est divisible par tous les polynômes irréductible de degrés $\leq k/2$.

Définition (PGCD de Polynômes)

Le $\text{pgcd}(a(x), b(x))$, avec $a(x), b(x) \in \mathbb{Z}_p[x]$ est défini comme étant l'unique polynôme **unitaire** de degré maximal qui divise $a(x)$ et $b(x)$.

- Étant donné un corps \mathbb{F} et un polynôme $m(x) \in \mathbb{F}[x]$, on peut définir l'anneau $\mathbb{F}[x]/(m(x))$:
 - Les éléments de l'anneau sont les polynômes de degré inférieur à $m(x)$ possédant des coefficients dans \mathbb{F} .
 - Les deux opérations de l'anneau sont l'addition et la multiplication modulo $m(x)$, respectivement.
- Étant donné un anneau $\mathbb{F}[x]/(m(x))$, et en exigeant que $m(x)$ soit **irréductible** sur \mathbb{F} , on obtient une structure de **corps**.
- En effet, il est possible de calculer un inverse modulo $m(x)$ pour tout élément de l'anneau (à part 0) en utilisant l'algorithme d'Euclide étendu.
- Par exemple, $\mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x^2 + 1)$ forme un corps possédant 256 éléments, qui sont les polynômes de degré au plus 7 avec des coefficients égaux à 0 ou à 1.

Corps de Galois

Pour un corps de Galois **de type $\text{GF}(p^m)$** , avec p premier et $m > 1$:

- On choisit un polynôme $p(x)$ de degré m irréductible sur \mathbb{Z}_p .
- Les éléments de $\text{GF}(p^m)$ sont les polynômes de degrés au plus $m - 1$ possédant des coefficients dans \mathbb{Z}_p .
- Nous travaillons donc dans $\mathbb{Z}_p[x]$ et les multiplications sont faites modulo $p(x)$.