# Arithmétique et cryptanalyse

---

## Codex

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

---

## Symboles & notations

$a \equiv_n b$ se prononce $a$ est congru à $b$ modulo $n$ et signifie que $b - a = nk$ pour un certain $k \in \mathbb{Z}$.

$a|b$ se prononce $a$ divise $b$ et signifie que $b = ak$ pour un certain $k \in \mathbb{Z}$.

$D(a)$ désigne l'ensemble des diviseurs positifs de l'entier $a$.

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des restes possible lors de la division d'entier par $n$.

$(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui possède un inverse modulo $n$.

$\mathrm{PGCD}(a, b)$ désigne le plus grand diviseur commun à $a$ et à $b$.

$\mathtt{det}(A)$ désigne le déterminant d'une matrice $A$.

$\mathbf{GL}_2(\mathbb{Z}/n\mathbb{Z})$ désigne l'ensemble des matrices $2 \times 2$ inversible modulo $n$.

$\mathcal{P}$ désigne l'ensemble des nombres premiers.

$\nu_p(n)$ désigne la valuation $p$-adique de l'entier $n$.

$x^p \equiv_p x$ pour un nombre premier $p$ est appelé le petit théorème de Fermat ou "le petit Fermat".

$n = (\cdots)_b$ est l'écriture de l'entier $n$ en base $b$.

---

## Fréquence d'apparition des caractères latin dans la langue française

| Caractère | a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fréquence (%) | 8.122 | 0.901 | 3.345 | 3.669 | 17.115 | 1.066 | 0.866 | 0.737 | 7.580 | 0.545 | 0.049 | 5.456 | 2.968 |

| Caractère | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fréquence (%) | 7.095 | 5.378 | 3.021 | 1.362 | 6.553 | 7.948 | 7.244 | 6.311 | 1.628 | 0.114 | 0.387 | 0.308 | 0.136 |