Chapitre 7. Nombres Premiers

Boulanger Yann

25 juin 2025

Table des matières

1 Introduction

Une motivation : l'arithmétique est au cœur du cryptage des communications.
Pour crypter un message on commence par le transformer en un (ou plusieurs) nombre(s).
Le processus de codage et décodage fait appel à plusieurs notions de ce chapitre :

— Choix de deux nombres premiers p et q que l'on garde secrets, on pose $n = p \times q$.
— La clé secrète et la clé publique se calculent à l'aide de l'algorithme d'Euclide et des coefficients de Bézout.
— Les calculs de cryptage se font modulo n.
— Le décodage fonctionne grâce à une variante du petit théorème de Fermat.

2 Vers une infinité de nombres premiers

2.1 Nombres premiers

Définition 1
Un entier n est dit *premier* s'il est strictement supérieur à 1 et que ses seuls diviseurs sont 1 et n.

Lemme 1
Tout entier $n \geq 2$ admet un diviseur premier.

Démonstration Par récurrence. Le résultat est évident pour $n = 2$. Supposons-le vrai jusqu'à $n - 1$.
Si n est premier, c'est terminé. Sinon, il existe a tel que $1 < a < n$ et $a \mid n$.
D'après l'hypothèse de récurrence, a admet un diviseur premier p, qui divise alors n.

Théorème 1
Tout entier $n \geq 2$ se décompose de manière unique comme produit de nombres premiers.

Démonstration

— Existence
On procède par récurrence sur $n \geq 2$.
Initialisation
Pour $n = 2$, 2 est un nombre premier, donc la propriété est vraie.
Hérédité
Supposons que tout entier k tel que $2 \leq k < n$ se décompose en produit de nombres premiers.
Considérons n.
  — Si n est premier, alors n est déjà un produit de nombres premiers (lui-même).
  — Sinon, n n'est pas premier, donc il existe a, b tels que $2 \leq a \leq b < n$ et $n = a \times b$.
Par hypothèse de récurrence, a et b se décomposent en produits de nombres premiers.
Donc $n = a \times b$ est aussi un produit de nombres premiers.
Par récurrence, tout entier $n \geq 2$ se décompose en produit de nombres premiers.

— Unicité

Supposons que $n \geq 2$ admette deux décompositions en produit de nombres premiers :

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

où les p_i et q_j sont des nombres premiers.

On veut montrer que $r = s$ et, à réarrangement près, $p_i = q_i$ pour tout i.

On procède par récurrence sur n.

Initialisation :

Pour $n = 2$, la seule décomposition est 2 lui-même.

Hérédité :

Supposons l'unicité vraie pour tout entier strictement inférieur à n.

Considérons les deux décompositions de n ci-dessus.

— p_1 divise n, donc p_1 divise $q_1 q_2 \cdots q_s$.

— Or, p_1 est premier, donc il divise l'un des q_j (propriété fondamentale des nombres premiers).

— Supposons que p_1 divise q_1. Mais q_1 est premier, donc $p_1 = q_1$.

On peut alors simplifier :

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$$

Par hypothèse de récurrence, les deux produits restants sont égaux à l'ordre près.

Par récurrence, la décomposition en produit de nombres premiers est unique à l'ordre près.

Conclusion :

Tout entier $n \geq 2$ se décompose de manière unique (à l'ordre près) comme produit de nombres premiers.

2.2 Infinité des nombres premiers

Théorème 2

Il existe une infinité de nombres premiers.

Démonstration (par l'absurde)

Supposons qu'il n'en existe qu'un nombre fini, disons $p_1, \ldots, p_n$.

Considérons $N = p_1 \ldots p_n + 1$. Alors N n'est divisible par aucun des p_i.

Il est donc premier ou possède un diviseur premier distinct des p_i.

3 Crible d'Ératosthène et Euclide

Crible d'Ératosthène

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Méthode classique pour déterminer tous les nombres premiers jusqu'à un entier donné N :

1) Écrire tous les entiers de 2 à N.
2) Entourer le premier nombre non barré p.
3) Rayer tous les multiples de p.
4) Recommencer à l'étape 2 tant qu'il reste des entiers non barrés.

Proposition 1 (Lemme d'Euclide)
Soit p un nombre premier. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Démonstration
Si p ne divise pas a alors p et a sont premiers entre eux -en effet les diviseurs de p sont 1 et p, mais seul 1 divise aussi a, $a \wedge p = 1$). Ainsi par le lemme de Gauss $p \mid b$.

4 Pour aller plus loin

4.1 Petit théorème de Fermat

Théorème 3 Petit théorème de Fermat
Si p est un nombre premier et n un entier premier avec p, alors $n^{p-1} \equiv 1[p]$.

Démonstration
Par récurrence sur n. L'énoncé est trivial si $n = 0$ ou $n = 1$.
On suppose donc que $n^p \equiv n \mod p$. Alors

$$(n+1)^p = 1 + \sum_{k=1}^{p-1} \binom{p}{k} n^k + n^p \equiv 1 + n^p \equiv 1 + n = n + 1 \mod p,$$

où la deuxième équivalence est l'hypothèse de récurrence.
Ainsi $n^p \equiv n \mod p$ pour tout $n \in \mathbb{N}$.
Si de plus $\text{pgcd}(n, p) = 1$, alors comme p divise $n^p - n = n(n^{p-1} - 1)$,
d'après le lemme de Gauss p
divise $n^{p-1} - 1$, et $n^{p-1} \equiv 1 \mod p$.

4.2 Fonction indicatrice d'Euler

Définition 2
Pour tout entier $n \geq 1$, on note $\varphi(n)$ le nombre d'entiers k entre 1 et n tels que $k \wedge n = 1$.

Proposition 2
Si p est un nombre premier, alors $\varphi(p) = p - 1$.
Plus généralement, si p est premier et $k \geq 1$, alors $\varphi(p^k) = p^k - p^{k-1}$.

Démonstration
Cas 1 : $n = p$ (premier).
Pour tout entier m tel que $1 \leq m < p$, p ne divise pas m (car p est premier et $m < p$),
donc $m \wedge p = 1$.
Le seul entier dans $\{1, 2, \ldots, p\}$ qui n'est pas premier avec p est p lui-même ($p \wedge p = p$).
Ainsi,

$$\varphi(p) = p - 1$$

Cas 2 : $n = p^k$, $k \geq 1$.
On cherche à déterminer le nombre d'entiers m avec $1 \leq m \leq p^k$ tels que $m \wedge p^k = 1$.
Observation clé : Un entier m est premier avec p^k si et seulement si p ne divise pas m.
Justification :

— Si $p \mid m$, alors $p \mid p^k$, donc $m \wedge p^k \geq p > 1$.

— Si $p \nmid m$, alors m et p^k n'ont aucun facteur premier commun, donc $m \wedge p^k) = 1$.

Comptage :
Il y a p^k entiers dans $\{1, 2, \ldots, p^k\}$.
Parmi eux, combien sont divisibles par p ? Ce sont les entiers de la forme $m = p \cdot t$, avec $1 \leq t \leq p^{k-1}$.
Il y a donc exactement p^{k-1} multiples de p dans $\{1, 2, \ldots, p^k\}$.
Conclusion :
Le nombre d'entiers m premiers avec p^k est donc :

$$\varphi(p^k) = p^k - p^{k-1}$$

Proposition 3
Si a et b sont premiers entre eux, alors $\varphi(ab) = \varphi(a)\varphi(b)$.

Corollaire 1
Pour tout $n \geq 1$, si $n = \prod_i p_i^{\alpha_i}$ est la décomposition en facteurs premiers de n, alors :

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

Démonstration

— La fonction d'Euler $\varphi(n)$ compte le nombre d'entiers k tels que $1 \leq k \leq n$ et $\gcd(k, n) = 1$.

— Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, où les p_i sont des nombres premiers distincts.

— Un entier k entre 1 et n n'est **pas** premier avec n s'il est divisible par au moins un des p_i.

— Le nombre d'entiers entre 1 et n divisibles par p_i est $\frac{n}{p_i}$.

— Par le principe d'inclusion-exclusion, le nombre d'entiers entre 1 et n **non premiers** avec n est :

$$\sum_i \frac{n}{p_i} - \sum_{i<j} \frac{n}{p_i p_j} + \sum_{i<j<k} \frac{n}{p_i p_j p_k} - \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r}$$

— Donc, le nombre d'entiers **premiers** avec n est :

$$\varphi(n) = n - \left[\sum_i \frac{n}{p_i} - \sum_{i<j} \frac{n}{p_i p_j} + \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r}\right]$$

— On factorise n :

$$\varphi(n) = n\left[1 - \sum_i \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}\right]$$

— Cette somme est exactement le développement du produit :

$$\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

En effet, en développant ce produit, on retrouve la somme précédente.

Conclusion :

$$\varphi(n) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

Remarque
Cette formule découle aussi du fait que φ est multiplicative et que pour une puissance d'un nombre premier p^α, on a : $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$ et donc on retrouve la formule générale.

4.3 Nombres premiers jumeaux

Définition 3
On appelle *nombres premiers jumeaux* deux nombres premiers qui diffèrent de 2, comme $(11, 13)$.

Remarque 1
On ignore s'il existe une infinité de couples de nombres premiers jumeaux.

4.4 Nombres premiers de Fermat

Définis comme les entiers $F_n = 2^{2^n} + 1$. On connaît très peu de tels nombres qui soient premiers. Les cinq premiers, de F_0 à F_4, sont premiers. Ensuite, on a :

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417.$$

Remarque 2
On ignore s'il existe une infinité de nombres premiers de Fermat.

Fin de chapitre