Nombres premiers

Arithmétique et cryptographie

SUPINFO

Sommaire

1. Ensemble des nombres premiers.

1. Ensemble des nombres premiers.

Nombre premier : définition

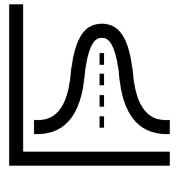
- Un entier naturel est dit **premier** s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

1. Ensemble des nombres premiers.

Nombre premier : exemple

- Quelques nombres premiers : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,\ldots$

- Quelques nombres non premiers : $0, 1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18,\ldots$



1. Ensemble des nombres premiers.

Nombre premier : culture générale

- Le concept de nombre premier semble être connue depuis plus de 25000 ans, bien avant l'apparition de l'écriture.

- Ces nombres ont de tout temps fasciné les mathématiciens et même le grand public.

- La découverte du nouveau plus grand nombre premier connu a par exemple toujours eu un écho considérable, même dans les médias généralistes.

- Actuellement il s'agit de $2^{82\,589\,933}-1$ qui comporte presque 25 millions de chiffres.

1. Ensemble des nombres premiers.

Théorème d'Euclide : énoncé

- Soit a,b élément de $\mathbb{Z}^*$ et p un nombre premier.
- Si $p|ab$ alors $p|a$ ou $p|b$.
- Autrement dit (formulation originelle d'Euclide) : si deux nombres se multipliant l'un l'autre produisent un certain nombre et si un nombre premier mesure leur produit, il mesurera aussi l'un des nombres initiaux.

1. Ensemble des nombres premiers.

Théorème d'Euclide : démonstration

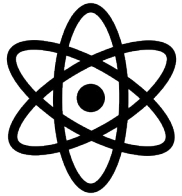
- Si $p|a$ il n'y a rien d'autre à prouver.

- Sinon, puisque p est premier, on a nécessairement $\mathrm{PGCD}\,(a,p) = 1$. D'après le théorème de Gauss, on aura alors $p|b$.

1. Ensemble des nombres premiers.

Théorème d'existence d'un diviseur premier : énoncé

- Tout entier naturel n supérieur ou égal à 2 admet au moins un diviseur premier.



1. Ensemble des nombres premiers.

Théorème d'existence d'un diviseur premier : démonstration

- Si n est premier, comme il se divise lui-même, le résultat est prouvé.
- Sinon, n admet des diviseurs différents de 1 et n. Soit p le plus petit d'entre eux. Il existe alors un entier q tel que $n = pq$.
- Montrons que p est nécessairement premier. Dans le cas contraire, il admettrait un diviseur m tel que $1 < m < p$. Il existerait donc un entier r tel que $p = mr$. En remplaçant cette expression de p dans celle de n on obtient $n = mrq$. Ceci est absurde car m serait alors un diviseur de n strictement plus petit que p. Q.E.D.

1. Ensemble des nombres premiers.

Corollaire : énoncé

- L’ensemble des nombres premiers est infini.

- Il n’existe donc pas de nombre premier plus grand que les autres.

1. Ensemble des nombres premiers.

Corollaire : démonstration

- On raisonne par l'absurde en supposant qu'il existe un nombre fini de nombres premiers : $p_1, p_2, \ldots, p_n$.
- On pose alors $N = p_1 p_2 \ldots p_n + 1$.
- D'après le théorème précédent, N admet un diviseur premier.
- Ainsi il existe $i, 1 \leq i \leq n$ tel que $p_i | N$.

1. Ensemble des nombres premiers.

Corollaire : démonstration

- D'autre part il est clair que $p_i | p_1 p_2 \ldots p_n$.

- On en déduit alors que $p_i | (N - p_1 p_2 \ldots p_n)$, *i.e.* $p_i | 1$ ce qui est absurde. Q.E.D.

1. Ensemble des nombres premiers.

Test naïf de primalité : principe

- D'après la définition même, pour tester le fait qu'un nombre n soit premier ou non, il suffit de prendre tous les entiers de 2 à $n-1$ et regarder s'ils divisent n.

- Si l'on trouve un diviseur parmi eux, cela signifie que n n'est pas premier. Sinon, il l'est.

1. Ensemble des nombres premiers.

Test naïf de primalité : principe

- On peut améliorer un peu cette recherche de diviseurs en se limitant aux entiers entre 2 et $\sqrt{n}$.

- En effet, si n se décompose en $n = pq$, nécessairement l'un des deux entiers p ou q sera inférieur ou égal à $\sqrt{n}$.

- Si ce n'était pas le cas, *i.e.* si les deux entiers p et q étaient tous deux strictement supérieurs à $\sqrt{n}$, pq serait strictement supérieur à n, ce qui est absurde car
  $pq = n$.

1. Ensemble des nombres premiers.

Test naïf de primalité : implémentation

```
def prime(n):
    if n == 1:
        return False
    m=2
    while m*m <= n:
        if n % m == 0:
            return False
        m += 1
    return True
```

1. Ensemble des nombres premiers.

Test naïf de primalité : performance

- L'algorithme précédent se révèle inefficace pour de grands nombres car il est très lent.

- Si l'on dispose d'une table de nombres premiers, il suffit de tester la divisibilité de a par ceux-ci. Le gain de temps est appréciable. Par exemple si on connaît tous les nombres premiers inférieurs à 100, on testera la primalité de tous les nombres inférieurs à $100^2 = 10000$.

1. Ensemble des nombres premiers.

Crible d'Erathostène

- Méthode élémentaire pour dresser une table de nombres premiers.

- Si l'on veut par exemple obtenir tous les nombres premiers inférieurs à 100, on commence par écrire dans un tableau tous les nombres de 2 à 100.

1. Ensemble des nombres premiers.

Crible d'Erathostène

	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

1. Ensemble des nombres premiers.

Crible d'Erathostène

- On marque ensuite (ici en rouge) tous les multiples de 2, excepté 2 lui-même.
- Puis on marque (ici en vert) tous les multiples de 3 non encore marqués, sauf 3.
- On procède de même avec 5 (en bleu).

- Plus généralement, après un marquage, on prend le premier entier non marqué qui le suit, et on marque ses multiples à l'exception de lui-même.

- On s'arrête ici à 10 car $10 = \sqrt{100}$.

- Les nombres non marqués ne sont multiples d'aucun autre et sont donc premiers.

1. Ensemble des nombres premiers.

Crible d'Erathostène

	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

1. Ensemble des nombres premiers.

Crible d'Erathostène : implémentation

```
def eratosthene(n):
    L = [True for i in range(n+1)]
    L[0] = L[1] = False
    for i in range(2,n+1):
        if L[i]:
            for j in range(2*i,n+1,i):
                L[j] = False
    return [i for i in range(n+1) if L[i]]
```

1. Ensemble des nombres premiers.

2. Petit théorème de Fermat.

2. Petit théorème de Fermat.

Petit théorème de Fermat : énoncé

- Soit p un nombre premier et a un entier naturel non divisible par p.

- Alors

$$a^{p-1} \equiv 1\,[p]$$

2. Petit théorème de Fermat.

Petit théorème de Fermat : exemple

- Montrons que le reste de la division euclidienne de 2^{100} par 101 est égal à 1.
- En effet, 101 étant un nombre premier et 2 n'étant pas divisible par 101, le petit théorème de Fermat implique que

$$2^{101-1} \equiv 1\,[101]$$

- C'est-à-dire

$$2^{100} \equiv 1\,[101]$$

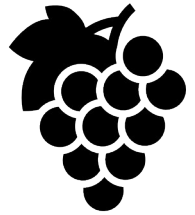
2. Petit théorème de Fermat.

Petit théorème de Fermat : formulation équivalente

- Soit p un nombre premier et a un entier naturel quelconque.

- Alors

$$a^p \equiv a\,[p]$$



2. Petit théorème de Fermat.

Petit théorème de Fermat : équivalence des deux formulations

- Supposons la première formulation vérifiée.
- Soit p un nombre premier et a un entier naturel quelconque.
- Deux cas de figure selon que p divise ou non a :
  - Si $p|a$, alors $p|a^p$. D'où $a \equiv 0\,[p]$ et $a^p \equiv 0\,[p]$. Ainsi $a^p \equiv a\,[p]$.
  - Si p ne divise pas a, la première formulation s'applique et on a $a^{p-1} \equiv 1\,[p]$. Après multiplication par a on obtient bien $a^p \equiv a\,[p]$.

2. Petit théorème de Fermat.

Petit théorème de Fermat : équivalence des deux formulations

- Réciproquement, supposons maintenant que la seconde formulation soit vérifiée.
- Soit p un nombre premier et a un entier naturel non divisible par p.
- Par hypothèse $p|\,(a^p - a)$, ce qui peut se réécrire $p|a\left(a^{p-1} - 1\right)$.
- Puisque p ne divise pas a, le théorème d'Euclide implique que $p|\left(a^{p-1} - 1\right)$.
- D'où $a^{p-1} \equiv 1\,[p]$.

2. Petit théorème de Fermat.

Petit théorème de Fermat : démonstration de la première formulation

- On considère p un nombre premier et a un entier naturel non divisible par p.
- On commence par montrer que pour tout entier p tel que $1 \leq k \leq p-1$, le reste de la division euclidienne de ka par p est non nul.
- Raisonnons par l'absurde : supposons que ce reste soit nul, *i.e.* que $p|ka$ pour un k tel que $1 \leq k \leq p-1$. Comme p ne divise pas a , le théorème d'Euclide implique que $p|k$. Ce qui est impossible car k est inférieur à p.

2. Petit théorème de Fermat.

Petit théorème de Fermat : démonstration de la première formulation

- On montre ensuite que les restes des divisions euclidiennes de ka et $k'a$ par p sont différents, pour k,k' tels que $1 \leq k,k' \leq p-1$ et $k \neq k'$.

- Raisonnons là aussi par l'absurde : supposons que $ka \equiv k'a\,[p]$ pour k,k' tels que $1 \leq k,k' \leq p-1$ et $k \neq k'$.

- Cela implique que $(k-k')\,a \equiv 0\,[p]$. Ainsi $p|\,(k-k')\,a$. Comme p ne divise pas a, le théorème d'Euclide implique que $p|\,(k-k')$.

- Ce qui est impossible car $k-k'$ est inférieur (en valeur absolue) à $p-2$ (puisque $1 \leq k,k' \leq p-1$).

2. Petit théorème de Fermat.

Petit théorème de Fermat : démonstration de la première formulation

- Les deux points précédents impliquent que les nombres $a, 2a, 3a, \ldots, (p-1)a$ ont après division Euclidienne par p des restes tous différents et non nuls.

- Ces restes valent donc (dans le désordre) $1, 2, \ldots, p-1$.

- On a alors

$$a \times 2a \times \ldots \times (p-1)a \equiv 1 \times 2 \times \ldots \times (p-1) \, [p]$$

- Ce qui peut se réécrire $a^{p-1}(p-1)! \equiv (p-1)! \, [p]$, ou encore après factorisation $\left(a^{p-1}-1\right)(p-1)! \equiv 0 \, [p]$.

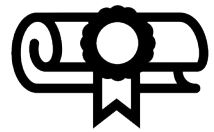
2. Petit théorème de Fermat.

Petit théorème de Fermat : démonstration de la première formulation

- Ainsi $p|\left(a^{p-1}-1\right)(p-1)!$

- Or p est premier avec $(p-1)!$ (aucun diviseur commun ne peut exister) donc d'après le théorème de Gauss $p|\left(a^{p-1}-1\right)$.

- Ce qui signifie bien sûr que $a^{p-1} \equiv 1\,[p]$. Q.E.D.



2. Petit théorème de Fermat.

3. Factorisation en nombre premiers.

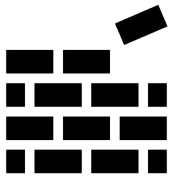
3. Factorisation en nombres premiers.

Théorème de factorisation

- Le but de ce théorème est d'écrire tout nombre entier à l'aide uniquement de nombres premiers.

- Ces derniers apparaîtront alors comme des briques permettant de reconstituer tous les nombres entiers.

- Ce théorème est parfois appelé **théorème fondamental de l'arithmétique**.



3. Factorisation en nombres premiers.

Théorème de factorisation : énoncé

- Tout entier naturel $a \geq 2$ se décompose de manière unique (à l'ordre des facteurs près) sous la forme d'un produit de nombres premiers, *i.e.*

$$a = \prod_{i=1}^{r} {p_i}^{\alpha_i} = {p_1}^{\alpha_1} \times {p_2}^{\alpha_2} \times \ldots \times {p_r}^{\alpha_r}$$

- Où les p_i sont des nombres premiers deux à deux distincts et les α_i des entiers naturels non nuls.

3. Factorisation en nombres premiers.

Théorème de factorisation : remarque

- La détermination pratique d'une telle décomposition est en général très difficile à obtenir.

- C'est d'ailleurs à cause de cette difficulté que certains systèmes de cryptographie tels que le R.S.A. sont si efficaces (voir dernier chapitre du cours).

- Une méthode naïve pour obtenir la décomposition d'un entier est de chercher à le diviser successivement par les nombres premiers qui lui sont inférieurs, et ce jusqu'à obtenir un nombre premier.

3. Factorisation en nombres premiers.

Théorème de factorisation : exemple avec 1400

- On commence par diviser 1400 par 2 autant de fois que possible : on a $1400 = 2 \times 700$, puis $700 = 2 \times 350$ et enfin $350 = 2 \times 175$.
- On constate ensuite que 175 n'est pas divisible par 3.
- Il est par contre divisible deux fois par 5 : $175 = 5 \times 35$ et $35 = 5 \times 7$.
- Le nombre 7 étant premier, la décomposition est terminée

$$1400 = 2^3 \times 5^2 \times 7$$

3. Factorisation en nombres premiers.

Algorithme de factorisation

```
def factorisation(n):
    L = []
    while n % 2 == 0:
        L.append(2)
        n //= 2
    m=3
    while m*m <= n:
        if n % m == 0:
            L.append(m)
            n //= m
        else:
            m += 2
    if n > 1:
        L.append(n)
    return L
```

3. Factorisation en nombres premiers.

Condition de divisibilité

- Si la décomposition d'un entier naturel a en produit de nombres premiers est

$$a = \prod_{i=1}^{r} {p_i}^{\alpha_i}$$

- Alors un entier b divise a si et seulement si

$$b = \prod_{i=1}^{r} {p_i}^{\beta_i}$$

- Où chaque exposant β_i vérifie $\beta_i \leq \alpha_i$.

3. Factorisation en nombres premiers.

Nombre de diviseur d'un entier naturel

- Si la décomposition d'un entier naturel a en produit de nombres premiers est

$$a = \prod_{i=1}^{r} {p_i}^{\alpha_i}$$

- Alors le nombre n de diviseurs de l'entier a dans $\mathbb{N}$ est

$$n = \prod_{i=1}^{r} (\alpha_i + 1)$$

3. Factorisation en nombres premiers.

Nombre de diviseur d'un entier naturel : exemple avec 1400

- On avait obtenu $1400 = 2^3 \times 5^2 \times 7$ donc 1400 possède $4 \times 3 \times 2 = 24$ diviseurs.

- De plus, ceux-ci seront de la forme $2^m \times 5^n \times 7^p$, avec $0 \leq m \leq 3$, $0 \leq n \leq 2$, et $0 \leq p \leq 1$.

- On trouve alors $1, 2, 4, 5, 7, 8, 10, 14, 20, 25, 28, 35, 40, 50, 56, 70, 100, 140, 175, 200, 280, 350, 700, 1400$.

3. Factorisation en nombres premiers.

Théorème sur le calcul du PGCD : énoncé

- Si la décomposition de deux entiers naturels a et b en produit de nombres premiers est

$$a = \prod_{i=1}^{r} {p_i}^{\alpha_i} \quad \text{et} \quad b = \prod_{i=1}^{r} {p_i}^{\beta_i}$$

- Avec α_i, β_i éventuellement nuls, alors

$$\text{PGCD}\,(a,b) = \prod_{i=1}^{r} {p_i}^{\min(\alpha_i,\beta_i)}$$

3. Factorisation en nombres premiers.

Théorème sur le calcul du PGCD : exemple avec 1400 et 2250

- On a

$$1400 = 2^3 \times 5^2 \times 7 \quad \text{et} \quad 2250 = 2 \times 3^2 \times 5^3$$

- Ce qui peut se réécrire

$$1400 = 2^3 \times 3^0 \times 5^2 \times 7^1 \quad \text{et} \quad 2250 = 2^1 \times 3^2 \times 5^3 \times 7^0$$

- D'où

$$\text{PGCD}\,(1400,2250) = 2^1 \times 3^0 \times 5^2 \times 7^0 = 2 \times 5^2 = 50$$

3. Factorisation en nombres premiers.