Les nombres premiers

Table des matières

1 Définition et propriétés immédiates

1.1 Définition

Définition 1 : Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même

Conséquence :
- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur)
- Un nombre premier p est un naturel supérieur ou égal à 2 soit : $p \geqslant 2$.
- Les nombres premiers inférieurs à 100 sont :
  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97

1.2 Critère d'arrêt

Théorème 1 : Tout entier naturel n, $n \geqslant 2$, admet un diviseur premier.
Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}$$

Démonstration :
- Si n est premier, il admet donc un diviseur premier : lui-même.
- Si n n'est pas premier, l'ensemble des diviseurs d de n tel que : $2 \leqslant d < n$ n'est pas vide. Il admet donc un plus petit élément p. Si p n'était pas premier, il admettrait un diviseur d' tel que $2 \leqslant d' < p$ qui diviserait n. Ceci est impossible car p est le plus petit. Donc p est premier.
- On a donc p premier et $n = p \times q$ avec $p \leqslant q$. En multipliant cette inégalité par p, on obtient :
$$p^2 \leqslant pq \quad \Leftrightarrow \quad p^2 \leqslant n \quad \text{soit} \quad p \leqslant \sqrt{n}$$

Exemple : Montrer que 109 est un nombre premier.

On a $10 < \sqrt{109} < 11$.
On teste tous les nombres premiers strictement inférieurs à 11, soit :
2, 3, 5 et 7.

Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
En effectuant la division euclidienne de 109 par 7, on obtient :

$$109 = 7 \times 15 + 4 \qquad 109 \text{ n'est donc pas divisible par } 7$$

Conclusion : comme 109 n'est pas divisible par 2, 3, 5, et 7, 109 est premier.

Algorithme : Un petit programme pour déterminer si un nombre N est premier. N'ayant pas à notre disposition la liste des nombres premiers, on teste si N est divisible par 2, puis on teste les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieur à $\sqrt{N}$.

On obtient alors :
- 527 est divisible par 17
- 719 est premier
- 11 111 est divisible par 41
- 37 589 est premier

Variables : N, I entiers
Entrées et initialisation
  Lire N
  $2 \to I$
Traitement
  si $E\left(\frac{N}{I}\right) = \frac{N}{I}$ **alors**
    Afficher N , "div. par :" , I
    Stop
  fin
  $I+1 \to I$
  tant que $I \leqslant \sqrt{N}$ **faire**
    si $E\left(\frac{N}{I}\right) = \frac{N}{I}$ **alors**
      Afficher N , "div. par :" , I
      Stop
    fin
    $I+2 \to I$
  fin
Sorties : Afficher N , "est premier"

1.3 Infinité des nombres premiers

Théorème 2 : Il existe une infinité de nombres premiers

ROC

Démonstration : Supposons qu'il existe un nombre fini de nombres premiers : p_1, p_2,..., p_i, ..., p_n. Posons $N = p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n + 1$

D'après le critère d'arrêt, N admet un diviseur premier.
Soit p_i ce diviseur premier. p_i divise donc $p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n$ et N.
Il divise donc la différence $N - (p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n) = 1$.
Ceci est impossible, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est absurde.

1.4 Crible d'Ératosthène

Pour dresser la liste des nombres premiers entre 2 et 150, la méthode du crible d'Ératosthène consiste à :
- écrire la liste des nombres entiers de 2 à 150 ;
- éliminer successivement les multiples propres [1] de 2, de 3... puis ceux de p, où p est le premier nombre non encore éliminé, etc

Les entiers éliminés (sur fond bleu dans le tableau ci après) sont les entiers non premiers entre 2 et 150. Les entiers restant (sur fond jaune) sont donc les nombres premiers inférieur à 150.

Remarque :

1) Pour éliminer les multiples propre de 7, commencer à 7^2, car les multiples inférieurs ont déjà été éliminés.

1. multiple propre de n : multiple de n distinct de n

2) Il est possible de savoir à l'avance « jusqu'où aller ». En effet grâce au critère d'arrêt, tout entier composé n admet un diviseur premier p tel que : $2 \leqslant p \leqslant \sqrt{n}$
Si $n \leqslant 150$, alors $\sqrt{n} \leqslant \sqrt{150}$, or $12 < \sqrt{150} < 13$ et donc tout entier non premier sera éliminés en tant que multiple propre de 2, 3, 5, 7 et 11.

	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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

On peut écrire l'algorithme suivant :

- Les entiers A correspondent aux nombres premiers de la liste des entiers de 2 à N
- Les entiers M correspondent aux multiples de A inférieurs à N
- Les entiers P correspondent aux rangs des nombres premiers A.
- Les entiers Q correspondent au nombre de multiples de A inférieurs à N
- La liste L_1 correspond à la liste des entiers de 2 à N
- La Liste L_2 correspond à la liste des nombres premiers inférieurs à N

À chaque fois que l'on trouve un nombre premier A, on le met dans la liste L_2 et l'on remplace tous les multiples de A dans la liste L_1 par un 0 (revient à rayer tous ces multiples)

On trouve le nombre premier suivant A, en prenant dans la liste L_1 le nombre suivant non nul
Avec la Ti, pour visualiser la liste L_2 faire : (stats) puis "edit"

Variables : N, I, A, M, P, Q entiers
L_1, L_2 listes
Entrées et initialisation
Lire N
Effacer liste L_1
Effacer liste L_2
pour I *de 2 à* N * **faire**
$I \to L_1(I)$
fin
$2 \to A$
$0 \to P$
Traitement
tant que $A \leqslant N$ **faire**
tant que $L_1(A) = 0$ **faire**
$A + 1 \to A$
fin
si $A \leqslant N$ **alors**
$P + 1 \to P$
$L_1(A) \to L_2(P)$
$\mathrm{E}\left(\frac{N}{A}\right) \to Q$
fin
pour I *de 1 à* Q **faire**
$A * I \to M$
$0 \to L_1(M)$
fin
fin
Sorties : Afficher P, L_2

* *Pour les TI faire :* I de 1 à $N + 1$.
De plus comme les listes sont limitées, rentrer un nombre N inférieur à 999

1.5 Nombres de Mersenne

On appelle nombres de Mersenne, les nombres M_n de la forme :

$$M_n = 2^n - 1 \qquad \text{avec } n \in \mathbb{N}^*$$

1) Calculons les 6 premiers nombres de Mersenne :

$$\begin{aligned} M_1 &= 2 - 1 = 1 \\ M_2 &= 4 - 1 = 3 \\ M_3 &= 8 - 1 = 7 \\ M_4 &= 16 - 1 = 15 \\ M_5 &= 32 - 1 = 31 \\ M_6 &= 64 - 1 = 63 \end{aligned}$$

On constate que pour les n égaux à 2, 3, 5, les nombres de Mersenne sont premiers. Est-ce que si n est premier, M_n est premier ? Cela permettrait de connaître un nombre premier aussi grand que l'on souhaite.

Remarque : Actuellement (janvier 2013) le plus grand nombre premier trouvé (nombre de Mersenne) est : $2^{57\,885\,161} - 1$ qui possède 17 425 170 chiffres !

2) Montrons que si n n'est pas premier alors M_n ne l'est pas non plus.

On rappelle la factorisation standard :

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

Si n n'est pas premier, alors il existe d, diviseur propre de n tel que :

$$n = dq \qquad \text{avec } q > 1$$

Factorisons alors M_n :

$$\begin{aligned} M_n &= 2^n - 1 \\ &= (2^d)^q - 1 \qquad \text{car } n = dq \\ &= (2^d - 1)[(2^d)^{q-1} + (2^d)^{q-2} + \cdots + 2^d + 1] \end{aligned}$$

donc $2^d - 1$ est un diviseur propre de M_n et donc M_n n'est pas premier.

Conclusion : Si n n'est pas premier alors M_n ne l'est pas non plus.
On peut aussi utiliser la contraposée :
Si M_n est premier alors n l'est également.

3) La réciproque est-elle vraie ?
Malheureusement la réciproque est fausse, ce qui met à mal une formule permettant de trouver un nombre premier aussi grand que l'on souhaite.
En effet si $n = 11$ alors $M_{11} = 2^{11} - 1 = 2\,047$ or $2\,047 = 23 \times 89$.
M_{11} n'est pas premier mais 11 l'est.

2 Divisibilité et nombres premiers

2.1 Théorème de Gauss et nombres premiers

Les résultats qui suivent ne sont que des reformulations du théorème de Gauss et de ses conséquences dans le cas particulier des nombres premiers.
Les démonstrations étant évidentes, elles sont laissées à l'entraînement du lecteur.

Théorème 3 : Un nombre premier divise un produit de facteurs si, et seulement si, il divise l'un de ces facteurs.

$$\text{Si } p \text{ divise } ab \quad \Leftrightarrow \quad p \text{ divise } a \text{ ou } p \text{ divise } b$$

En particulier, si p premier divise une puissance a^k, alors nécessairement p divise a, d'où découle que p^k divise a^k.

2.2 Conséquences

- Si un nombre premier p divise un produit de facteurs premiers, alors p est l'un de ces facteurs premiers
- Soit $p_1,p_2,\ldots,p_k$ des nombres premiers distincts et $\alpha_1,\alpha_2,\ldots,\alpha_k$ des entiers naturels non nuls. Si, pour tout $i \in \{1,2,\ldots,k\}$, $p_i^{\alpha_i}$ divise un entier n alors le produit $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ divise aussi l'entier n.

3 Décomposition, diviseurs d'un entier

3.1 Théorème fondamental de l'arithmétique

Théorème 4 : tout entier $n \geqslant 2$, peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers.

$$n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times \cdots \times p_m^{\alpha m}$$

Exemple : Décomposons 16 758 en produit de facteur premier

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

on a donc $16\,758 = 2 \times 3^2 \times 7^2 \times 19$

Algorithme : : On peut proposer l'algorithme suivant : Il faut donc chercher les facteurs premiers d'un entier $N \geqslant 2$. On teste si D est un diviseur de N en commençant par 2 puis les nombres impairs dans l'ordre croissant en appliquant le critère d'arrêt $D \leqslant \sqrt{N}$. On réinitialise N en prenant le quotient N/D. Le dernier nombre qui ne vérifie par le critère d'arrêt est alors premier et on le rajoute à la liste des diviseurs. On peut tester la programme avec :

16 758, on obtient $L_1 = \{2, 3, 3, 7, 7, 19\}$

87 616, on obtient $L_1 = \{2, 2, 2, 2, 2, 37, 37\}$

77 986 545, on obtient :
$L_1 = \{3, 5, 7, 13, 19, 31, 97\}$

Variables : N, D, I, C entiers
L_1 liste
Entrées et initialisation
Lire N
$2 \to D$
$1 \to I$
$1 \to C$
Traitement
tant que $D \leqslant \sqrt{N}$ **faire**
si $E\left(\frac{N}{D}\right) = \frac{N}{D}$ **alors**
$D \to L_1(I)$
$I + 1 \to I$
$\frac{N}{D} \to N$
sinon
$D + C \to D$
$2 \to C$
fin
fin
$N \to L_1(I)$
Sorties : Afficher L_1

Application : Soit à calculer pgcd$(126, 735)$ et ppcm$(126, 735)$

- Décomposons les deux nombres

126	2
63	3
21	3
7	7
1	

735	3
245	5
49	7
7	7
1	

On a donc :

$126 = 2 \times 3^2 \times 7$

$735 = 3 \times 5 \times 7^2$

- On détermine les facteurs communs pour le pgcd et les facteurs utilisés pour le ppcm.

$$\text{pgcd}(126; 735) = 3 \times 7 = 21 \quad \text{et} \quad \text{ppcm}(126, 735) = 2 \times 3^2 \times 5 \times 7^2 = 4410$$

3.2 Diviseurs d'un entier

Théorème 5 : Soit un nombre n ($n \geqslant 2$) dont la décomposition en facteurs premiers est :

$$n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times \cdots \times p_m^{\alpha m}$$

Alors tout diviseurs d de n a pour décomposition :

$$d = p_1^{\beta 1} \times p_2^{\beta 2} \times \cdots \times p_m^{\beta m}$$

$$\text{avec} \quad 0 \leqslant \beta_i \leqslant \alpha_i \quad \text{et} \quad i \in \{1, 2, \ldots, m\}$$

Le nombre de diviseurs N est alors :

$$N = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_m + 1)$$

Exemple : Trouver le nombre de diviseurs de 120 puis déterminer tous ces diviseurs.

- On décompose 120 en facteurs premiers : $120 = 2^3 \times 3 \times 5$

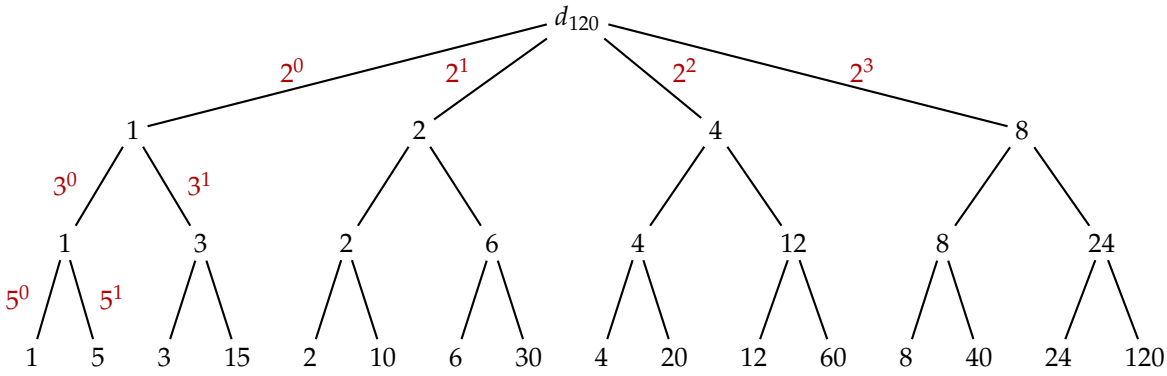
  On alors : $(3+1)(1+1)(1+1) = 4 \times 2 \times 2 = 16$

  Il y a donc 16 diviseurs pour 120.

- Pour déterminer tous ces diviseurs, on peut utiliser un tableau double entrée en séparant les puissance de 2 et les puissance de 3 et 5. On obtient alors :

$\times$	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

- On peut aussi utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles



- Les 16 diviseurs de 120 sont donc :

$$D_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$$

3.3 Problèmes

1) *Un entier naturel n a 15 diviseurs. on sait de plus que n est divisible par 6 mais pas par 8. Déterminer cet entier n.*

   L'entier n a 15 diviseurs. Il faut donc connaître toutes les décompositions de 15 en facteurs supérieurs à 1. Il n'y a que 2 décompositions soit en un seul facteur 15, soit en deux facteurs 3×5.
   On sait que n est divisible par 6, il est donc divisible par 2 et par 3. Donc n admet 2 facteurs premiers. Comme 15 ne peut se décomposer en plus de 2 facteurs, alors n ne peut admettre que 2 facteurs premiers 2 et 3. On a donc :

$$n = 2^\alpha 3^\beta$$

   Comme $15 = 3 \times 5$, on a alors : $(1+\alpha)(1+\beta) = 3 \times 5$
   On trouve alors deux solutions : $\alpha = 2$ et $\beta = 4$ ou $\alpha = 4$ et $\beta = 2$

   On sait de plus que n n'est pas divisible par $8 = 2^3$, donc α est inférieur à 3. n est donc :

$$n = 2^2 3^4 = 4 \times 81 = 324$$

2) *Déterminer le plus petit entier naturel possédant 28 diviseurs.*

Soit n l'entier cherché.

Trouvons toutes les décompositions de 28 en facteurs supérieurs à 1. On peut décomposer 28 en 1, 2 ou trois facteurs :

$$28 \quad \text{ou} \quad 2 \times 14 \quad \text{ou} \quad 4 \times 7 \quad \text{ou} \quad 2 \times 2 \times 7$$

- En 1 facteur.
  Le plus petit entier n est alors $n = 2^{\alpha}$ avec $\alpha + 1 = 27$ soit $\alpha = 27$

  $$n = 2^{27} = 134\,217\,728$$

- En deux facteurs : $28 = 2 \times 14$.
  Le plus petit entier n est alors :

  $$n = 2^{\alpha} \times 3^{\beta}$$

  $$\text{avec} \quad \alpha + 1 = 14 \quad \text{et} \quad \beta + 1 = 2$$

  On trouve alors :

  $$\alpha = 13 \quad \text{et} \quad \beta = 1$$

  donc

  $$n = 2^{13} \times 3 = 24\,576$$

- En deux facteurs : $28 = 4 \times 7$.
  Le plus petit entier n est alors :

  $$n = 2^{\alpha} \times 3^{\beta}$$

  $$\text{avec} \quad \alpha + 1 = 7 \quad \text{et} \quad \beta + 1 = 4$$

  On trouve alors :

  $$\alpha = 6 \quad \text{et} \quad \beta = 3$$

  donc

  $$n = 2^6 \times 3^3 = 1\,728$$

- En trois facteurs : $28 = 2 \times 2 \times 7$.
  Le plus petit entier n est alors :

  $$n = 2^{\alpha} \times 3^{\beta} \times 5^{\gamma}$$

  $$\text{avec} \quad \alpha + 1 = 7 \quad ; \quad \beta + 1 = 2 \quad \text{et} \quad \gamma + 1 = 2$$

  On trouve alors :

  $$\alpha = 6 \quad ; \quad \beta = 1 \quad \text{et} \quad \gamma = 1$$

  donc

  $$n = 2^6 \times 3 \times 5 = 960$$

Conclusion : Le plus petit entier naturel ayant 28 diviseurs est 960

4 Petit théorème de Fermat - Hors programme

4.1 Théorème, remarque et exemple

Théorème 6 : Soit un nombre premier p et un naturel a non multiple de p alors :

$$a^{p-1} \equiv 1 \mod p$$

Démonstration : Considérons les $p-1$ premiers multiples de a :

$$a, 2a, 3a, \ldots, (p-1)a$$

Considérons les restes de la division de ces multiples de a par p :

$$r_1, r_2, r_3, \ldots, r_{p-1}$$

- Ces restes sont deux à deux distinct. En effet s'il existait deux restes identiques soit r_i et r_j avec $i > j$, alors :

$$\begin{aligned} ia - ja &\equiv r_i - r_j \mod p \\ a(i-j) &\equiv 0 \mod p \end{aligned}$$

  donc $(i-j)a$ serait multiple de p ce qui est impossible.

- Si ces restes sont tous différents et qu'il y a $p-1$ multiples, on trouve tous les restes non nul possibles de la division par p. Donc

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times 3 \times \cdots \times (p-1) = (p-1)!$$

- Si l'on cherche le reste du produits de tous ces multiples, on obtient :

$$\begin{aligned} a \times 2a \times 3a \times \cdots \times (p-1)a &\equiv (p-1)! \mod p \\ (p-1)!\, a^{p-1} &\equiv p-1)! \mod p \\ (p-1)!\, (a^{p-1} - 1) &\equiv 0 \mod p \end{aligned}$$

  Comme $(p-1)!$ n'est pas un multiple de p car tous les facteurs sont inférieur à p, alors $a^{p-1} - 1$ est donc un multiple de p.

  On a donc : $a^{p-1} - 1 \equiv 0 \mod p$. Le théorème est donc vérifié.

Remarque : $\forall p$ premier et $\forall a \in \mathbb{N}$, on a : $a^p \equiv a \mod p$

En effet, si a n'est pas multiple de p, en multipliant l'équivalence du théorème de Fermat, on obtient l'équivalence ci-dessus. Si a est est un multiple de p, on a alors : $a \equiv 0 \mod p$ et donc $a^p \equiv 0 \mod p$

Exemple : Prouver que, pour tout entier n, 7 divise $3^{6n} - 1$

7 est premier et 3 n'est pas un multiple de 7, donc, d'après le petit théorème de Fermat, on a :

$$3^6 \equiv 1 \mod 7$$

Comme la congruence est compatible avec les puissances, on a :

$$3^{6n} \equiv 1 \mod 7$$

donc $3^{6n} - 1$ est divisible par 7 pour tout n.

4.2 Nombre de Poulet

Soit un entier $n(n \geqslant 1)$ un nombre impair tel que $2^{n-1} \not\equiv 1 \mod n$.

1) Montrer que n n'est pas premier.

2) Prouver que $2^{340} \equiv 1 \mod 341$, *mais que 341 n'est pas premier.*

1) Montrons que n est composé par la contraposée :

$$n \text{ est premier impair alors : } \quad 2^{n-1} \equiv 1 \mod n$$

Si n est premier et impair, alors 2 n'est pas un multiple de n, d'après le théorème de Fermat, on a :

$$2^{n-1} \equiv 1 \mod n$$

La contraposée est donc vérifiée.

2) On sait que $2^{10} = 1024$ et $1024 = 341 \times 3 + 1$, donc $1024 \equiv 1 \mod 341$

$$2^{340} = \left(2^{10}\right)^{34} \quad \text{et donc} \quad \left(2^{10}\right)^{34} \equiv 1 \mod 341$$

Or on a : $341 = 11 \times 31$ donc 341 n'est pas premier.
La réciproque de la contraposée est fausse.

Conclusion : un nombre de Poulet (mathématicien français du début du XX^{e} siècle) est un nombre n, non premier, tel que : $2^{n-1} \equiv 1 \mod n$. Le nombre 341 est un nombre de Poulet.