Les nombres premiers

Les nombres premiers sont en quelque sorte les atomes du monde des nombres. Ils jouent un rôle essentiel dans de nombreux domaines des mathématiques et sont très utilisés dans des applications comme la cryptographie.

1) Définition

Un nombre premier est un nombre entier naturel qui ne peut pas se diviser par un plus petit que lui mais qui n'est pas 1.

Une autre façon de le définir plus précisément, c'est de dire que c'est un nombre ayant exactement deux diviseurs distincts, ce qui exclut de ce fait 1.

Voyons ainsi lesquels des premiers nombres sont premiers, en faisant apparaître leurs décompositions en produit de deux facteurs excluant celles triviale où figure 1, faisant ainsi la liste de leurs diviseurs :

Nombres	décompositions	diviseurs	premier
1	-	1	non
2	-	1 ; 2	oui
3	-	1 ; 3	oui
4	2×2	1 ; 2 ; 4	non
5	-	1 ; 5	oui
6	2×3	1 ; 2 ; 3 ; 6	non
7		1 ; 7	oui
8	2×4	1 ; 2 ; 4 ; 8	non

2) Crible d'Erathostène

La méthode précédente est laborieuse, si nous souhaitons par exemple déterminer tous les nombres premiers inférieurs à 100, ou à un nombre quelconque. Il existe alors une technique efficace appelée **crible d'Eratosthène**. Présentons là.

Disposons pour cela tous les nombres en tableau (la disposition est essentielle pour une bonne efficacité visuelle, sinon la méthode peut être employée pour un traitement informatique).

La première étape consiste à éliminer 1 en le faisant apparaître en rouge et relever 2 en le faisant apparaître en vert.

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

La deuxième étape consiste à éliminer tous les multiples de 2. Notez que cela se visualise facilement car ce sont des colonnes, d'où l'importance de la disposition.

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

A ce stade, nous pouvons être assurés du fait que le nombre 3 suivant 2 est premier car il n'a pas été éliminé et donc il n'a pas de diviseur plus petit que lui.

La troisième étape consiste à relever ce nombre 3 en vert puis à éliminer tous ses multiples.

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

Notez là encore que, de par la disposition adoptée, les multiples de 3 s'éliminent en diagonales montantes.

Le premier nombre non éliminé qui suit 3 est 5. Il est donc premier car il ne peut pas avoir de diviseur strictement inférieur sinon il aurait été éliminé. Nous le relevons donc en vert et éliminons les multiples de 5, c'est-à-dire, la colonne du 5 car celle du 10 a déjà été éliminée.

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

Le nombre suivant 5 et non éliminé est 7. Il est donc premier. Nous le relevons en vert et éliminons ses multiples.

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

Le premier nombre non éliminé suivant 7 est 11. Il est donc premier et là on s'arrête. Pourquoi me direz-vous ? Parce que dans les multiples de 11, seuls sont à éliminer les multiples à partir de 11×11, car 2×11 a déjà été éliminé en tant que multiple de 2, 3×11 en tant que multiple de 3, 4×11 en tant que multiple de 2 car 4 est multiple de 2, etc jusqu'à 10×11.

Or $11 \times 11 = 121 > 100$, donc aucun des multiples de 11 n'est plus à éliminer dans le tableau.

Le premier nombre non éliminé suivant 11 est alors 13. Il est donc premier et le même raisonnement s'applique de proche en proche pour affirmer que tous les nombres non éliminés du tableau sont premiers.

Au final, les nombres relevés en vert forment l'ensemble des nombres premiers inférieurs à 100. Nous ne conseillons que trop au lecteur désireux de devenir un vrai scientifique de les apprendre par cœur au même titre que les tables de multiplication.

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

Cette méthode est employée avec des ordinateurs pour déterminer de très grands nombres premiers. Le plus grand connu à ce jour a 24 862 048 chiffres. La production de tels nombres est à la base de la cryptographie, branche des mathématiques qui a pour but le codage de données.

3) Décomposition d'un nombre entier naturel en produit de facteurs premiers

Tout nombre entier naturel non nul peut se décomposer de façon unique en un produit de facteurs premiers.

La preuve se trouve sur la page des mathématiques des classes préparatoires aux grandes écoles. Nous ne retiendrons ici que la technique permettant de faire cette décomposition efficacement en distinguant deux méthodes :

Première méthode :

On tente de diviser le plus possible par les premiers nombres premiers, 2,3,5, etc… en utilisant les critères de divisibilité et en s'arrêtant au nombre premier situé juste avant celui dont le carré est supérieur au nombre à décomposer.

Exemple : Décomposer 84

On note que le chiffre des unités de 84 est pair donc le nombre est divisible par 2 et que le quotient obtenu est encore divisible par 2 :

$$84 = 2 \times 42 = 2 \times (2 \times 21)$$

Le quotient final obtenu 21 est alors divisible par 3 car la somme de ses chiffres 2+1 l'est :

$$84 = 2 \times 2 \times 3 \times 7$$

Nous obtenons ainsi la décomposition souhaitée.

Cette méthode peut cependant s'avérer laborieuse pour de grands nombres.

Deuxième méthode :

On tente de décomposer le nombre en un produits de deux facteurs les plus grands possibles et on recommence pour ces facteurs.

Exemple 1 : Décomposer 84

Les chiffres de ce nombre se divisant pas 4 :

$$84 = 4 \times 21$$

On peut alors décomposer aisément les facteurs apparus puis ranger les facteurs premiers par ordre croissant :

$$84 = (2 \times 2) \times (7 \times 3) = 2 \times 2 \times 3 \times 7$$

Exemple 2 : Décomposer 749000

$$749000 = 749 \times 1000 = (7 \times 107) \times (10 \times 10 \times 10) = (7 \times 107) \times (2 \times 5) \times (2 \times 5) \times (2 \times 5)$$

$$= 2 \times 2 \times 2 \times 5 \times 5 \times 5 \times 7 \times 107$$

Il faut cependant encore s'assurer que 107 est un nombre premier, ce qui se fait en testant tous les nombres premiers inférieurs strictement à 11 (car $11 \times 11 = 121 > 107$) :

2 ne divise pas 107 car son chiffre des unités 7 est impair, 3 ne divise pas 107 car il ne divise pas la somme de ses chiffres 1+0+7, 5 ne divise pas 107 car son chiffre des unités n'est ni 0 ni 5, 7 ne divise pas 107 car le reste de la division entière de 107 par 7 n'est pas nul. Donc 107 est premier.

Toutefois, comme il y a un grand nombre de facteurs dans la décomposition, il sera avantageux d'utiliser une notation puissance :

$$749000 = 2^3 \times 5^3 \times 7 \times 107$$