Nombres premiers et petit théorème de Fermat

Introduction :

Dans l'ensemble $\mathbb{N}$, une place particulière est faite, depuis l'Antiquité, à l'étude des nombres premiers. Ces nombres, qui d'après leur définition ne sont divisibles que par 1 et eux-mêmes, permettent d'obtenir par multiplication tous les nombres entiers.
De nos jours, une grande part de la recherche mathématique s'intéresse à eux, à leur obtention et à leur utilisation, notamment dans le numérique et le codage des données.

Dans une première partie, nous définirons les nombres premiers, et nous apprendrons comment reconnaître qu'un nombre est premier ou non.
Nous verrons, dans une deuxième partie, que tout nombre entier peut être « généré » à partir de nombres premiers.
Dans la dernière partie de ce cours, nous nous intéresserons à un résultat de l'arithmétique, le petit théorème de Fermat, qui a de nombreuses applications.

→ Dans tout ce chapitre, nous travaillerons dans l'ensemble $\mathbb{N}$.

1 Nombres premiers

Nous avons déjà abordé les nombres premiers en classe de seconde ; nous allons rappeler les définitions et les premières propriétés de ces nombres.

a. Définition et exemples

Définition

Nombre premier :

Soit $n \in \mathbb{N}$.
n est un nombre premier lorsqu'il a exactement deux diviseurs entiers naturels distincts : 1 et lui-même.

 Exemple

- 13 est un nombre premier ; en effet, ses seuls diviseurs sont 1 et 13.
- L'ensemble des diviseurs positifs de 35 est : $\mathrm{D}(35) = \{1,\ 5,\ 7,\ 35\}$: 35 n'est pas un nombre premier.

Donnons quelques conséquences :

- 0 n'est pas premier, car il a une infinité de diviseurs.
- Le nombre 1 n'est pas un nombre premier, puisqu'il n'a qu'un diviseur : 1.
- 2 est un nombre premier, car il a exactement deux diviseurs : 1 et 2.
- Aucun nombre pair strictement supérieur à 2 n'est un nombre premier.

→ En effet, si n est un nombre pair strictement supérieur à 2, alors il a au moins trois diviseurs : 1, 2 et n.

Illustrons comment prouver qu'un nombre est premier ou non en recherchant la liste de ses diviseurs.

 Exemple

Soit $n \in \mathbb{N}$, avec $n \geq 2$.
Nous cherchons à savoir si le nombre entier $n^2 + 4n - 5$ peut être un nombre premier.

 À retenir

Méthodologie :

Pour montrer qu'un nombre n n'est pas premier, il suffit de trouver un diviseur de n différent de 1 et de lui-même.

→ Pour ce faire, on essaiera d'écrire n comme un produit de nombres entiers.

Pour trouver d'éventuels diviseurs de n^2+4n-5, essayons de factoriser cette expression en utilisant la forme canonique d'un polynôme du second degré.

→ Le polynôme s'écrit sous la forme an^2+bn+c, avec $a=1$, $b=4$, $c=-5$.

$$\begin{aligned} n^2+4n-5 &= an^2+bn+c \\ &= (n-\alpha)^2+\beta \ [\text{où } \alpha=-\tfrac{b}{2a} \text{ et } \beta=a\alpha^2+b\alpha+c] \\ &= (n+2)^2+4-8-5 \\ &= (n+2)^2-9 \\ &= (n+2)^2-3^2 \\ &= (n+2+3)(n+2-3) \\ &= (n+5)(n-1) \end{aligned}$$

Comme $n \geq 2$, on a : $n+5 > n-1 \geq 1$.

Nous envisageons donc les deux cas suivants :

1. $n-1=1$, c'est-à-dire $n=2$.

→ Dans ce cas, $n^2+4n-5=7\times 1$ est un nombre premier.

2. $n-1>1$, c'est-à-dire $n>2$.

Les nombres entiers $(n+5)$ et $(n-1)$ sont des diviseurs de n^2+4n-5 et sont tous les deux strictement supérieurs à 1.

→ Dans ce cas, n^2+4n-5 n'est pas premier.

C. En conclusion, n^2+4n-5 est un nombre premier si et seulement si $n=2$.

Dans cet exemple, nous avons déterminé si un entier pouvait être un nombre premier en recherchant ses diviseurs. Parfois, il n'est pas évident de trouver ces diviseurs.
Dans le paragraphe suivant, nous allons donc utiliser un algorithme pour déterminer si un nombre est premier.

b. Reconnaître si un nombre est premier

Ce critère de reconnaissance d'un nombre premier a été trouvé dans les travaux d'un mathématicien du XIII^{e} siècle, Léonard de Pise, connu sous le nom de Fibonacci.

Propriété

Prenons $n \in \mathbb{N}$, avec $n \geq 4$.
Si n n'est pas un nombre premier, alors n admet au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Nous allons démontrer cette propriété.

Démonstration

Soit $n \geq 4$, un nombre entier qui n'est pas premier.

1. L'ensemble $\mathrm{D}(n)$ n'est pas vide, donc il admet un plus petit élément : notons alors p le plus petit diviseur de n tel que :

$$\begin{cases} p \neq n \\ p \geq 2 \end{cases}$$

2. Supposons **par l'absurde** que p n'est pas premier : il a lui-même un diviseur d différent de 1 et de p selon la définition d'un nombre premier.

p a donc un diviseur d tel que $2 \leq d < p$.
Comme d divise p et p divise n, alors, par transitivité, d divise n.

d est donc un diviseur de n plus petit que p et supérieur à 2, ce qui contredit la définition de p.

→ p est donc premier.

3. p divise n, donc il existe $q \in \mathbb{N}$ tel que : $n = pq$, avec $p \leq q$. Ainsi :

$$p \times p \leq p \times q$$
$$\text{Soit : } p^2 \leq n$$
$$\text{On en déduit : } p \leq \sqrt{n}$$

Astuce

Nous utiliserons souvent cette propriété dans sa forme contraposée.

Propriété

Si n n'admet aucun diviseur premier inférieur à $\sqrt{n}$, alors n est un nombre premier.

Prenons un exemple pour illustrer l'utilisation de cette propriété.

Exemple

Nous voulons savoir si le nombre 127 est premier.
Nous testons alors la divisibilité de 127 par tous les nombres premiers inférieurs à $\sqrt{127} \approx 11,3$.

1. En utilisant les critères de divisibilité, nous prouvons que 127 n'est divisible ni par 2, ni par 3, ni par 5.
2. Testons la divisibilité par 7 : la division euclidienne de 127 par 7 donne :

$$127 = 7 \times 18 + 1$$

→ Donc 127 n'est pas divisible par 7.

3. Testons la divisibilité par 11 :

$$127 = 11 \times 11 + 6$$

→ Donc 127 n'est pas divisible par 11.

C. Ainsi, 127 n'est divisible par aucun des nombres premiers inférieurs à $\sqrt{127}$.

→ En utilisant la contraposée ci-dessus, nous avons donc prouvé que 127 est un nombre premier.

Toujours en utilisant cette propriété, nous pouvons également établir la liste des nombres premiers inférieurs à un entier n.
Pour déterminer cette liste, on utilise le **crible** (ou **critère**) **d'Ératosthène**, un savant de l'Antiquité, qui a vécu au III^{e} s. av. J.-C.
Sa méthode part d'un tableau où sont écrits les n premiers nombres entiers supérieurs ou égaux à 1.

Nous allons illustrer cette méthode avec $n = 119$ et déterminer les nombres premiers compris entre 1 et 119. Ils nous seront utiles plus tard quand nous décomposerons un nombre entier en facteurs premiers.
Nous allons mettre en gris tous les nombres entiers qui ne sont pas premiers ; et encadrer les nombres premiers au fur et à mesure que nous les trouverons.

1. Nous commençons par griser 1 et, excepté 2, tous les nombres pairs, qui ne sont pas des nombres premiers.

	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	101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118	119

2. Puis, nous entourons 3, qui est premier, et barrons tous les multiples de 3.

Pour les reconnaître, nous utilisons le critère de divisibilité : « Un entier est divisible par 3 si et seulement si la somme de ses chiffres est un multiple de 3 ».

3. De la même manière, nous entourons 5, qui est premier, et barrons tous les multiples de 5, c'est-à-dire ceux qui se terminent par 0 ou 5.

4. Le nombre premier suivant est 7. Nous l'entourons et barrons ensuite tous les multiples de 7.

	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	101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118	119

C En utilisant la propriété ci-dessus, nous savons que, si $4 \leq n \leq 119$ et qu'il n'est pas premier, alors il admet un diviseur premier inférieur à $\sqrt{119} \approx 10,91$, donc inférieur ou égal à 10.

Nous avons grisé les multiples des nombres premiers inférieurs ou égaux à 10 ; donc nous avons trouvé tous les nombres de la grille qui ne sont pas premiers.

→ Les nombres sur fond blanc sont donc les nombres premiers inférieurs à 119.

À retenir

En particulier, 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	97

Nous avons déterminé l'ensemble des nombres premiers strictement inférieurs à 119 et il ne semble pas y avoir de « schéma » ou de relation évidente entre eux.
Quels sont les autres nombres premiers ? Pouvons-nous tous les déterminer ou déterminer leur place dans $\mathbb{N}$? Nous allons nous intéresser à leur ensemble.

c. Ensemble des nombres premiers

Propriété

Il y a une infinité de nombres premiers.

Nous allons démontrer cette propriété ; l'idée de cette démonstration vient d'un autre mathématicien de l'Antiquité, Euclide, dont nous connaissons déjà des travaux en arithmétique, comme l'utilisation des divisions euclidiennes et l'algorithme de recherche d'un PGCD.

Démonstration

1. On suppose **par l'absurde** qu'il y a un nombre fini l de nombres premiers dans $\mathbb{N}$.

   Leur ensemble, classé par ordre coissant, est $\{p_1, p_2, \ldots, p_{l-1}, p_l\}$.

   → Ils sont tous strictement supérieurs à 1.

2. Soit n le nombre entier : $n = p_1 \times p_2 \times \ldots \times p_l + 1$.

   n est strictement supérieur à tous les p_i de l'ensemble $\{p_1, p_2, \ldots, p_{l-1}, p_l\}$ des nombres premiers.

   → D'après notre hypothèse, puisque p_l est le plus grand nombre premier, n n'est pas premier.

3. D'après la propriété que nous avons vue au point précédent, il existe donc un nombre premier inférieur à $\sqrt{n}$ qui le divise.

   On note p_k ce nombre premier :

   $$p_k \in \{p_1, p_2, \ldots, p_{l-1}, p_l\}$$

   p_k divise n et p_k divise $p_1 \times p_2 \times \ldots \times p_l$.

   → Donc p_k divise $(n - p_1 \times p_2 \times \ldots \times p_l)$.

4. Or, $n = p_1 \times p_2 \times \ldots \times p_l + 1$, donc :

   $$n - p_1 \times p_2 \times \ldots \times p_l = 1$$

   → Cela signifie que p_k divise 1, et donc que $p_k = 1$ n'est pas premier, ce qui est contradictoire.

c. En conclusion, l'hypothèse de départ : « Il y a un nombre fini de nombres premiers », est fausse, et nous avons démontré la propriété.

Nous ne connaissons donc pas tous les nombres premiers ni comment les obtenir. Des études sont menées sur ces derniers, car leur connaissance permet d'obtenir des méthodes de codage et de chiffrement des données. Pour le comprendre, nous devons d'abord nous intéresser au lien entre les nombres premiers et les autres nombres entiers.

2 | Décomposition d'un nombre entier en facteurs premiers

En seconde, nous avons déjà vu qu'un nombre entier non premier pouvait s'écrire comme un produit de nombres premiers.
Par exemple, si nous considérons le nombre 280, il peut s'écrire ainsi :

$$\begin{aligned} 280 &= 10 \times 28 \\ &= (2 \times 5) \times (7 \times 4) \\ &= 2 \times 5 \times 7 \times 2 \times 2 \end{aligned}$$

C'est un produit des nombres premiers 2, 5 et 7.

→ Nous pouvons l'écrire : $280 = 2^3 \times 5 \times 7$.

Cette décomposition est possible pour chacun des nombres entiers non premiers. C'est ce que nous allons voir avec les propriétés ci-dessous.

a. Existence et unicité de la décomposition

Propriété

Soit $n > 2$, un nombre entier **non premier**.
n est le produit de nombres premiers.

→ Autrement dit :

Il existe des nombres premiers p_1, p_2, ..., p_k distincts et des entiers a_1, a_2, ..., a_k appartenant à $\mathbb{N}^*$ tels que :

$$n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_{k-1}^{a_{k-1}} \times p_k^{a_k}$$

Cette décomposition de n en produit de facteurs premiers est **unique**.

Dans l'exemple ci-dessus, $280 = 2^3 \times 5 \times 7$, les nombres premiers sont $p_1 = 2$, $p_2 = 5$ et $p_3 = 7$, et les nombres a_1, a_2, a_3 valent respectivement 3, 1 et 1.

Définition

Décomposition en produit de facteurs premiers :

Soit n un nombre entier naturel non premier.

L'écriture :
$n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_{k-1}^{a_{k-1}} \times p_k^{a_k}$
avec, pour tout $i \in \{1, \ldots, k\}$: $\begin{cases} p_i \text{ est un nombre premier} \\ a_i \in \mathbb{N}^* \end{cases}$
s'appelle la décomposition de n en produit de facteurs premiers.

→ On dit aussi qu'on a décomposé n en produit de facteurs premiers.

Nous allons démontrer l'existence de la décomposition en facteurs premiers. Le premier à avoir démontré cette propriété est Euclide.

Démonstration

Soit $n > 2$, un nombre entier non premier.

1. Nous savons que son plus petit diviseur est un nombre premier p_1 tel que :

$$2 \leq p_1 \leq \sqrt{n} < n$$

2. Ainsi, nous pouvons écrire :

$$n = p_1 \times q_1 \text{ où } \begin{cases} q_1 \in \mathbb{N} \\ 2 \leq p_1 < q_1 < n \end{cases}$$

→ Si q_1 est premier, nous avons démontré la propriété : $n = p_1 \times q_1$, où p_1 et q_1 sont des nombres premiers.

3. Si q_1 n'est pas premier, alors nous pouvons lui appliquer le même raisonnement que nous avons mené pour n.

q_1 n'est pas premier, donc il admet un plus petit diviseur premier p_2 et on peut écrire :

$$q_1 = p_2 \times q_2 \text{ où } \begin{cases} q_2 \in \mathbb{N} \\ 2 \leq q_2 < q_1 < n \end{cases}$$
$$\text{et : } n = p_1 \times p_2 \times q_2$$

4. Nous pouvons mener de nouveau ce raisonnement avec le nombre q_2.

5. Et ainsi de suite.

6. Nous allons donc obtenir une suite décroissante d'entiers naturels q_i, tous supérieurs ou égaux à 2.

→ Cette suite sera donc composée d'un nombre fini de nombres entiers.

Cela signifie que la décomposition s'arrête et nous arrivons à :

$$2 \leq q_{l-1} < \ldots < q_1$$
$$\text{et : } n = p_1 \times p_2 \times \ldots \times p_{l-1} \times q_{l-1}$$

Au dernier q_{l-1}, on ne peut trouver un diviseur premier strictement inférieur, car sinon il ne serait pas le dernier.

→ Donc q_{l-1} est premier. On peut le noter p_l.

Cela donne donc la décomposition :

$$n = p_1 \times p_2 \times \ldots \times p_{l-1} \times p_l$$
$$\text{où les } p_i \text{ sont des nombres premiers}$$

C. En regroupant les valeurs égales de certains nombres premiers, nous obtenons la forme :

$$n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_{k-1}^{a_{k-1}} \times p_k^{a_k}$$

→ Nous admettrons que cette décomposition est unique.

Remarque :
Si $n$est un nombre premier, il ne peut pas être décomposé de la sorte.

À retenir

Ainsi, si $n > 2$:

- soit il est premier ;
- soit il peut être décomposé en produit de facteurs premiers.

Astuce

Ces deux propriétés – existence et unicité – de la décomposition en produit de facteurs premiers sont connues comme le **théorème fondamental de l'arithmétique**.
Il stipule en effet que les nombres premiers « génèrent » par produit l'ensemble des nombres entiers naturels.

Pour trouver la décomposition en facteurs premiers de n,nous allons rappeler la méthode vue en seconde, et qui sera utilisée quand n est relativement grand.

À retenir

Méthodologie :

1. On teste la divisibilité de n par les nombres premiers dans l'ordre croissant.

   Pour cela, nous pouvons nous aider des critères de divisibilité et de la liste des diviseurs premiers inférieurs à 100.

2. Soit p le plus petit nombre premier qui divise n.

   → On trouve le quotient q de n par p : $n = qp$.

3. On teste de nouveau la divisibilité de q par p :
   - → si q est divisible par p, on procède comme ci-dessus, on trouve son quotient et on teste sa divisibilité par p ;
   - → sinon, on teste la divisibilité de q par le nombre premier immédiatement supérieur à p.
4. On continue ce procédé jusqu'à obtenir un quotient égal à 1.

Prenons un exemple pour illustrer cette méthode, qui est un algorithme que nous pourrions programmer.

Exemple

Nous voulons décomposer $5\,355$ en produit de facteurs premiers.

1. L'utilisation des critères de divisibilité que nous connaissons prouve que $5\,355$ n'est pas divisible par 2, mais qu'il est divisible par 3 (puisque $5+3+5+5=18$ est un multiple de 3).
   - → Nous avons : $5\,355 = 3 \times 1\,785$.
2. Le quotient de cette division euclidienne est $1\,785$. Testons de nouveau la divisibilité de $1\,785$ par 3.
   - → $1\,785 = 3 \times 595$
3. Ensuite, 595 n'est pas divisible par 3, mais il est divisible par le nombre premier suivant...
4. On continue ainsi par des divisions successives jusqu'à obtenir le quotient 1.

Pour schématiser ces divisions successives, nous pouvons les noter dans un tableau.

Quotient	Division par
$5\,355$	3

$1\,785$	3
595	5
119	7
17	17
1	

c. Nous lisons donc dans la colonne de droite la décomposition de $5\,355$ en produit de facteurs premiers :

$$5\,355 = 3^2 \times 5 \times 7 \times 17$$

→ Cette décomposition est unique selon la propriété ci-dessus.

Nous allons maintenant nous intéresser à l'ensemble des diviseurs d'un nombre entier, à partir de cette décomposition.

b. Diviseurs d'un nombre entier naturel

Reprenons l'exemple de la décomposition de $5\,355$.

→ Nous cherchons comment obtenir tous les diviseurs de $5\,355$ et leur nombre.

Si d est un diviseur de $5\,355$, alors d divise $3^2 \times 5 \times 7 \times 17$.

- Si d est premier, alors d est nécessairement 3, 5, 7 ou 17.
- Sinon, soit p^a un facteur de la décomposition en facteurs premiers de d.

p^a divise d et d divise $3^2 \times 5 \times 7 \times 17$.

→ Donc, par transitivité, p^a divise $3^2 \times 5 \times 7 \times 17$.

Comme la décomposition de $5\,355$ en produit de facteurs premiers est unique, cela signifie que p^a doit nécessairement être un facteur de la décomposition de $5\,355$.

→ On en déduit que la forme des diviseurs de $5\,355$ est :

$$3^{a_1} \times 5^{a_2} \times 7^{a_3} \times 17^{a_4}$$

$$\text{avec : } \begin{cases} 0 \leq a_1 \leq 2 \\ 0 \leq a_2 \leq 1 \\ 0 \leq a_3 \leq 1 \\ 0 \leq a_4 \leq 1 \end{cases}$$

Il y a 3 valeurs possibles pour a_1, 2 valeurs possibles pour a_2, ainsi que pour a_3 et a_4.

→ Il y a donc $3 \times 2 \times 2 \times 2 = 24$ diviseurs de $5\,355$.

En nous appuyant sur cet exemple, nous en déduisons la forme des diviseurs d'un nombre n non premier.

Propriété

Soit n un nombre entier naturel **non premier** dont la décomposition en facteurs premiers est :

$$n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_{k-1}^{a_{k-1}} \times p_k^{a_k}$$

Les diviseurs positifs de n sont les nombres entiers naturels de la forme :

$$p_1^{b_1} \times p_2^{b_2} \times \ldots \times p_{k-1}^{b_{k-1}} \times p_k^{b_k}$$

où $b_i \in \mathbb{N}^*$ et $0 \leq b_i \leq a_i$ pour tout entier naturel i entre 1 et k

Prenons un exemple pour illustrer cette propriété.

Exemple

Nous avons vu que $280 = 2^3 \times 5 \times 7$.
Les diviseurs de 280 sont donc les nombres entiers :

$$2^{a_1} \times 5^{a_2} \times 7^{a_3}$$

$$\text{où } \begin{cases} a_1 \text{ peut valoir } 0, 1, 2 \text{ ou } 3 \\ a_2 \text{ et } a_3 \text{ peuvent valoir } 0 \text{ ou } 1 \end{cases}$$

→ $4 \times 5 = 20$ est donc un diviseur de 280 ; $2 \times 5 \times 7 = 70$ également.

→ 2×5^2 n'est pas un diviseur de 280 ; non plus que $2 \times 5 \times 11$.

Cette propriété va nous permettre également de résoudre certaines équations comme dans l'exemple ci-dessous.

Exemple

Nous voulons résoudre dans $\mathbb{N}$, l'équation $(E) : x(x^2 + 5x - 24) = 130$.

→ Pour résoudre cette équation de degré 3 dans $\mathbb{N}$, nous allons factoriser l'expression polynomiale et nous servir de la décomposition en facteurs premiers de 130.

- D'une part, nous factorisons en utilisant la forme canonique ou le calcul du discriminant :

$$x^2 + 5x - 24 = (x - 3)(x + 8)$$

- D'autre part, on décompose 130 en produit de facteurs premiers :

$$\begin{aligned} 130 &= 10 \times 13 \\ &= 2 \times 5 \times 13 \end{aligned}$$

→ Nous avons ainsi :

$$(E) \Leftrightarrow x(x - 3)(x + 8) = 2 \times 5 \times 13$$

Les nombres entiers x, $x - 3$ et $x + 8$ sont des diviseurs de 130 et cela implique que les trois nombres sont strictement positifs.

→ x, $x - 3$ et $x + 8$ appartiennent donc à l'ensemble :

$$\{1, 2, 5, 2 \times 5, 13, 2 \times 13, 5 \times 13, 130\} = \{1, 2, 5, 10, 13, 26, 65, 130$$

Nous cherchons dans cette liste un entier x tel que $x-3$ et $x+8$ y soient aussi. La seule solution est $x=5$.

→ Ainsi, dans $\mathbb{N}$, $(E) \Leftrightarrow x=5$.

Enfin, une des applications du théorème fondamental de l'arithmétique est de trouver le PGCD de deux nombres entiers naturels.

c. Application : PGCD de deux nombres de $\mathbb{N}^*$

Nous retrouvons la propriété sur le PGCD de deux nombres que nous avons vue dans le cours précédent.

Propriété

Soit a et b deux nombres de $\mathbb{N} \setminus \{0,\ 1\}$ non premiers entre eux. $\mathrm{PGCD}(a\ ;\ b)$ est le produit des nombres premiers communs à leur décomposition en facteurs premiers, affectés du plus petit exposant.

Exemple

Nous cherchons $\mathrm{PGCD}(1960\ ;\ 5\,355)$.
Nous avons établi que :

$$\begin{aligned} 5\,355 &= 3^2 \times 5 \times 7 \times 17 \\ \text{et : } 1\,960 &= 280 \times 7 \\ &= 2^3 \times 5 \times 7^2 \end{aligned}$$

Les facteurs premiers communs aux deux décompositions sont 5 et 7.

- Dans la première décomposition, l'exposant de 5 est 1, comme dans la deuxième.
- Dans la première décomposition, l'exposant de 7 est 1 ; il est égal à 2 dans la deuxième.

→ Nous en déduisons :

$$\begin{aligned}\text{PGCD}(1\,960\ ;\ 5\,355) &= 5 \times 7 \\ &= 35\end{aligned}$$

Nous nous sommes intéressés à la décomposition des nombres entiers en facteurs de nombres premiers. Ces algorithmes deviennent ardus quand le nombre entier est très grand, même avec les ordinateurs d'aujourd'hui. Nous allons maintenant examiner un théorème important de l'arithmétique qui permet notamment de déterminer la divisibilité de très grands nombres par des nombres premiers.

3 Petit théorème de Fermat

Pierre de Fermat est un mathématicien français qui vécut au XVII^{e}siècle et travailla surtout sur les nombres. Il écrivit de nombreuses propriétés arithmétiques, mais ne fournit pas toujours de démonstrations écrites. Certaines conjectures sont en en cours d'analyse de nos jours, certaines ont été prouvées ou contredites plusieurs siècles plus tard. Le petit théorème de Fermat a notamment été démontré par le mathématicien Léonard Euler, qui vécut au XVIII^{e} siècle.

a. Petit théorème de Fermat

Nous admettons le résultat suivant.

Théorème

Soit $n \in \mathbb{N}^*$ et p est un nombre premier qui ne divise pas n.
Alors p divise $n^{p-1} - 1$, c'est-à-dire :

$$n^{p-1} \equiv 1\ [p]$$

Prenons un exemple d'application directe de ce théorème.

Exemple

Nous cherchons le reste dans la division euclidienne de 12^6 par 7.
7 est un nombre premier qui ne divise pas 12.
Nous pouvons donc appliquer le petit théorème de Fermat et déduire que :

$$12^{7-1} \equiv 1[7] \text{ donc : } 12^6 \equiv 1\,[7]$$

→ Ainsi, le reste dans la division euclidienne de 12^6 par 7 est 1.

Ce théorème permet de résoudre des équations à congruence avec de grands nombres. Pour nous en convaincre, prenons un autre exemple.

Exemple

Nous voulons résoudre l'équation (E) : $x^{62} \equiv 3\,[11]$ dans $\mathbb{N}$.

1. 11 est un nombre premier. Nous n'avons pas x^{11-1}, soit x^{10}, dans cette équation, ce qui pourrait faire penser directement au petit théorème de Fermat ; nous allons donc le faire apparaître !

Nous effectuons la division euclidienne de 62 par 10 : $62 = 10 \times 6 + 2$.

→ Ainsi : $(E) \Leftrightarrow \left(x^6\right)^{10} x^2 \equiv 3\,[11]$.

2. Repérons deux cas.

   - Si 11 divise x, alors 11 divise x^{62}.

→ Les multiples de 11 ne sont pas solutions de (E), car alors :

$$x^{62} \equiv 0\,[11]$$

   - Si 11 ne divise pas x, comme 11 est premier avec x, il ne divise pas x^6 non plus.

Ainsi, nous pouvons appliquer le petit théorème de Fermat à x^6, avec $p = 11$.

Nous avons donc :

$$(x^6)^{10} \equiv 1\,[11]$$

→ La congruence est compatible avec la multiplication, donc, si 11 ne divise pas x , nous avons :

$$(E) \Leftrightarrow x^2 \equiv 3\,[11]$$

3 Intéressons-nous maintenant au reste de la division euclidienne de x^2 par 11.

Nous utilisons, comme dans le cours sur la divisibilité dans $\mathbb{Z}$, la propriété suivante.

Rappel

> Si $a \equiv b[n]$, alors $a^p \equiv b^p[n]$.

Nous allons maintenant procéder comme nous l'avons appris dans le cours sur la congruence.

- Si $x \equiv 0\ [11]$, nous avons :

$$x^2 \equiv 0\ [11]$$

- Si $x \equiv 1\,[11]$, nous avons :

$$x^2 \equiv 1\,[11]$$

- Si $x \equiv 2\,[11]$, nous avons :

$$x^2 \equiv 4\,[11]$$

- Si $x \equiv 3\,[11]$, nous avons :

$$x^2 \equiv 9\,[11]$$

- Si $x \equiv 4\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 16\,[11] \\ &\equiv 5\,[11] \end{aligned}$$

- Si $x \equiv 5\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 25\,[11] \\ &\equiv 3\,[11] \end{aligned}$$

- Si $x \equiv 6\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 36\,[11] \\ &\equiv 3\,[11] \end{aligned}$$

- Si $x \equiv 7\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 49\,[11] \\ &\equiv 5\,[11] \end{aligned}$$

- Si $x \equiv 8\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 64\,[11] \\ &\equiv 9\,[11] \end{aligned}$$

- Si $x \equiv 9\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 81\,[11] \\ &\equiv 4\,[11] \end{aligned}$$

- Si $x \equiv 10\,[11]$, nous avons :

$$\begin{aligned} x^2 &\equiv 100\,[11] \\ &\equiv 1\,[11] \end{aligned}$$

→ Nous obtenons le tableau :

x modulo 11	0	1	2	3	4	5	6	7	8	9	10

x^2 modulo 11	0	1	4	9	5	3	3	5	9	4	1

C En conclusion :

$$x^2 \equiv 3[11] \Leftrightarrow x \equiv 5\,[11] \text{ ou } x \equiv 6\,[11]$$

→ Les solutions de l'équation (E) dans $\mathbb{N}$ sont donc :

$$\{11k+5,\ 11k+6\ ;\ k \in \mathbb{N}\}$$

Ces exemples illustrent le cas où le nombre premier p ne divise pas n. Nous disposons également d'un corollaire qui s'applique à n'importe quel entier naturel n.

b. Corollaire du petit théorème de Fermat

Propriété

Soit p un nombre premier et $n \in \mathbb{N}$.
Alors p divise $n^p - n$, c'est-à-dire :

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

Démonstration

Soit $n \in \mathbb{N}$ et p un nombre premier :

$$n^p - n = n(n^{p-1} - 1)$$

1. Si p divise n, alors p divise $n(n^{p-1} - 1)$.
2. Sinon, le petit théorème de Fermat nous assure que $n^{p-1} \equiv 1\,[p]$.

   → Donc p divise $n^{p-1} - 1$.

C Dans les deux cas, p divise $n(n^{p-1} - 1)$, ce qui donne la relation : p divise $n^p - n$.

→ Nous avons donc :

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

Astuce

L'intérêt de ce corollaire peut être énoncé ainsi : un entier n élevé à la puissance du nombre premier p a le même reste dans la division euclidienne par p que n.

Prenons un exemple d'application de cette propriété.

Exemple

Nous cherchons à montrer que 13 divise $11^{13} + 15^{13}$.

13 est un nombre premier, donc on peut appliquer le corollaire ci-dessus :

$$11^{13} \equiv 11\,[13]$$
$$15^{13} \equiv 15\,[13]$$

La congruence est compatible avec l'addition, donc :

$$\begin{aligned} 11^{13} + 15^{13} &\equiv 11 + 15\,[13] \\ &\equiv 26\,[13] \\ &\equiv 0\,[13] \end{aligned}$$

→ Nous en déduisons que 13 divise $11^{13} + 15^{13}$.

Cet exemple prouve l'efficacité du petit théorème de Fermat et de son corollaire quand il s'agit de déterminer la divisibilité ou la congruence de très grands nombres par des nombres premiers.

Conclusion :

Dans ce cours, nous avons abordé quelques notions du vaste champ d'étude des nombres premiers : leur définition, quelques algorithmes pour les reconnaître et quelques propriétés fondamentales.

Des applications nombreuses et actuelles utilisent les grands nombres premiers, qui ne sont pas encore très connus, pour chiffrer ou déchiffrer des données, notamment dans le commerce électronique ou la cryptographie ; c'est pourquoi l'arithmétique reste une branche active de la recherche en mathématiques.