

Chapitre 7 – Nombres premiers

1. Premières propriétés

1a. Définition

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

Remarques :

- 1 n'est pas premier car il n'a qu'un seul diviseur : lui-même. Ainsi, tout nombre premier p vérifie $p \geq 2$.
- A part 2, tous les nombres premiers sont impairs.
- Un entier naturel non premier supérieur à 1 est appelé **nombre composé**.
Il existe alors deux nombres a et b supérieurs ou égaux à 2 tels que $n = ab$.
- Il y a vingt-cinq nombres premiers inférieurs à 100, qui sont :

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; 53 ; 59 ; 61 ; 67 ; 71 ; 73 ; 79 ; 83 ; 97 et 97.

1b. Test de primalité

Propriété : Tout entier naturel $n \geq 2$ est divisible par un nombre premier.

Démonstration : Par récurrence sur n .

Initialisation : $n = 2$ est divisible par 2, qui est premier.

Hérédité : Soit $n \in \mathbb{N}$. Supposons que tout entier inférieur ou égal à n est divisible par un nombre premier.

On considère alors $n + 1$.

- si $n + 1$ est premier, alors il est divisible par lui-même, qui est premier.
- sinon, il existe deux entiers a et b inférieurs ou égaux à n tels que $n + 1 = ab$.
Or $a \leq n$, donc par hypothèse de récurrence, il existe un nombre premier p tel que $a = kp$. Donc $n + 1 = kpb$ et $n + 1$ est divisible par le nombre premier p .
Dans tous les cas, $n + 1$ est divisible par un nombre premier, ce qui montre l'hérédité.

Propriété : Si $n \geq 2$ n'est pas premier, alors il admet un diviseur premier p tel que $1 < p \leq \sqrt{n}$.

Démonstration : Si n n'est pas premier, alors il existe a et b entiers tels que $n = ab$.

Par l'absurde, supposons que a et b sont tous les deux strictement supérieurs à

$\sqrt{n}$. On a alors $a > \sqrt{n}$ et $b > \sqrt{n}$, ainsi $ab > \sqrt{n}^2$ et donc $ab > n$, ce qui est absurde car $ab = n$.

Ainsi, soit a , soit b est inférieur à $\sqrt{n}$. Supposons que ce soit le cas pour a . D'après la propriété précédente, il est divisible par un nombre premier, qui est donc également inférieur ou égal à $\sqrt{n}$.

Ainsi, $n = ab$ est divisible par un nombre premier inférieur ou égal à $\sqrt{n}$.

Exemple 1

Pour chacun des nombres suivants, indiquer s'il est premier ou non : 143 ; 317 ; 437 ; 1053 en utilisant le critère d'arrêt.

Exemple 2

Montrer que pour tout entier n supérieur ou égal à 3, l'entier $n^2 - 1$ n'est pas premier.

Cette propriété est-elle vraie pour $n = 2$?

Exemple 3

a. Prouver que, pour tout entier naturel n , l'un des trois entiers n , $n + 10$ et $n + 20$ est un multiple de 3.

b. À quelle condition les entiers n , $n + 10$ et $n + 20$ sont tous les trois des nombres premiers ?

Exemple 1 *Le critère d'arrêt, c'est le fait de s'arrêter de tester les diviseurs premiers supérieurs à $\sqrt{n}$.*

- $\sqrt{143} \approx 12$.

2, 3, 5, 7 ne divisent pas 143, mais $143 = 11 \times 13$. Il n'est donc **pas premier**.

- $\sqrt{317} \approx 18$. Or 2, 3, 5, 7, 11, 13 et 17 ne divisent pas 317. Il est donc **premier**.

- $\sqrt{437} \approx 21$. Or 2, 3, 5, 7, 11, 13 et 17 ne divisent pas 437, mais $437 = 19 \times 23$. Il n'est donc **pas premier**.

- $\sqrt{1\,053} \approx 32$.

Heureusement, on trouve assez vite que c'est un **multiple de 3** : $1\,053 = 3 \times 351$.

Exemple 2 On sait que $n^2 - 1 = (n + 1)(n - 1)$.

Or pour $n \geq 3$, $(n - 1)$ est supérieur ou égal à 2, donc $n^2 - 1$ **est composé**.

Pour $n = 2$, on a $n^2 - 1 = 3$, qui est bien premier. D'ailleurs, $(n - 1)$ est égal à 1.

Exemple 3

a. On utilise les congruences : $n + 10 \equiv n + 9 + 1 \equiv n + 1[3]$

et $n + 20 \equiv n + 18 + 2 \equiv n + 2[3]$.

Or l'un des trois entiers n , $n + 1$ et $n + 2$ est un multiple de 3, donc c'est le cas pour l'un des trois entiers n , $n + 10$ et $n + 20$.

b. Si $n = 3$, on a bien 3, 13 et 23 qui sont tous premiers. Sinon, l'un des trois entiers n , $n + 10$ et $n + 20$ est un multiple de 3 sans être égal à 3. Cet entier n'est donc pas premier. Ainsi, n , $n + 10$ et $n + 20$ ne peuvent être tous premiers que si $n = 3$.

1c. Application du théorème de Gauss

Propriété : Soit a et b deux entiers non nuls.

- Si un nombre premier p divise le produit ab , alors p divise a ou p divise b .
- Si p premier divise le produit a^k , alors p divise a .

Exemple 1 Soit un entier relatif n tel que $n^2 = 29p + 1$, où p est un nombre premier.

1. Factoriser $29p$.
2. Montrer alors que n est de la forme $(29k + 1)$ ou $(29k - 1)$ avec $k \in \mathbb{Z}$.
3. Déterminer alors les valeurs de n et p qui conviennent au problème.

Exemple 2 Soit p un nombre premier supérieur ou égal à 5.

Montrer que $p^2 - 1$ est divisible par 3 et 8. En déduire qu'il est divisible par 24.

Exemple 1

1. $n^2 = 29p + 1 \Leftrightarrow 29p = n^2 - 1 = (n + 1)(n - 1)$

2. Le nombre 29 divise le produit $(n + 1)(n - 1)$.

D'après le théorème de Gauss, il divise alors $(n + 1)$ ou $(n - 1)$.

Alors il existe $k \in \mathbb{Z}$ tel que $n + 1 = 29k$ d'où $n = 29k - 1$

ou alors il existe $k \in \mathbb{Z}$ tel que $n = 29k + 1$.

3. Si $n = 29k + 1$:

$$(29k + 1)^2 = 29p + 1$$

$$\Leftrightarrow (29k)^2 + 2 \times 29k + 1 = 29p + 1$$

$$\Leftrightarrow 29k(29k + 2) = 29p$$

$$\Leftrightarrow k(29k + 2) = p$$

La seule possibilité pour que p soit premier est que $k = 1$, donc $p = 31$.

On a alors $n^2 = 29 \times 31 + 1 = 900$, et ainsi $n = 30$.

Si $n = 29k - 1$, on aboutit à $k(29k - 2) = p$. On doit alors avoir $k = 1$, mais alors $p = 27$, qui n'est pas premier. Le cas $n = 29k - 1$ est donc impossible.

Exemple 2

• p étant supérieur ou égal à 5, il n'est pas multiple de 3. Ainsi :

soit $p \equiv 1[3]$ et alors $p^2 \equiv 1[3]$ donc $p^2 - 1 \equiv 0[3]$

soit $p \equiv 2[3]$ et alors $p^2 \equiv 8 \equiv 2[3]$ donc $p^2 - 1 \equiv 2^2 - 1 \equiv 3 \equiv 0[3]$

Dans tous les cas, $p^2 - 1$ est multiple de 3.

• $p^2 - 1 = (p + 1)(p - 1)$

p étant supérieur ou égal à 5, il est impair. Ainsi, $(p + 1)$ et $(p - 1)$ sont deux nombres pairs consécutifs, donc l'un d'entre eux est multiple de 4. Ainsi, $p^2 - 1$ est multiple de $2 \times 4 = 8$.

• $p^2 - 1$ est un multiple de 3 et de 8, qui sont premiers entre eux. Donc $p^2 - 1$ est multiple de $3 \times 8 = 24$.

1d. Infinité des nombres premiers

Propriété : Il existe une infinité de nombres premiers.

Démonstration : Par l'absurde, supposons qu'il y ait un nombre fini de nombres premiers. On les note alors $p_1; p_2; \dots; p_n$.

- Soit $N = p_1 \times p_2 \times \dots \times p_n + 1$.

Par construction, $N \geq p_n$, donc N n'est pas premier.

- N admet alors un diviseur premier parmi $p_1; p_2; \dots; p_n$. Notons-le p_k .
 p_k divise donc N , mais il divise aussi le produit $P = p_1 \times p_2 \times \dots \times p_n$.

Il divise donc leur différence $N - P = 1$.

- p_k est positif et divise 1, il est forcément égal à 1.

C'est une contradiction car p_k est un nombre premier.

Ainsi, il y a une infinité de nombres premiers.

2. Décomposition en facteurs premiers

2a. Théorème fondamental de l'arithmétique

Propriété : Tout entier $n \geq 2$ peut se décomposer de façon unique en un produit de facteurs premiers, de la forme $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$.

Démonstration : On démontre seulement l'existence de la décomposition par récurrence sur n . L'unicité de cette décomposition est admise.

Initialisation : pour $n = 2$, n étant premier, il se décompose en lui-même.

Hérédité : soit $n \in \mathbb{N}$, supposons que tout entier inférieur ou égal à n se décompose en produit de facteurs premiers.

On s'intéresse à $n + 1$.

- si $n + 1$ est premier, il se décompose en lui-même.
- si $n + 1$ est composé, il admet alors deux diviseurs stricts a et b .

On a alors $n + 1 = ab$ avec $a \leq n$ et $b \leq n$.

Par hypothèse de récurrence, a et b se décomposent en produit de facteurs premiers. Ainsi, le produit ab , égal à $n + 1$ se décompose également.

Conclusion : tout entier $n \geq 2$ se décompose en produit de facteurs premiers.

Exemple 1 Décomposer 189 et 16 758 en produit de facteurs premiers, en commençant par les plus petits.

Exemple 2 A l'aide d'une décomposition en facteurs premiers, déterminer $PGCD(126; 735)$.

Exemple 3 A l'aide d'une décomposition en facteurs premiers, déterminer les réels a et b tels que :

$$\frac{a}{b} = \frac{5\,292}{5\,544} \text{ et } a + b = 903$$

Exemple 1 Pour trouver des décompositions, on teste avec les nombres premiers dans l'ordre croissant : d'abord 2, puis 3...

- 189 n'est pas divisible par 2, mais par 3.

$189 = 3 \times 63$, qui est lui-même divisible par 3.

$189 = 3^2 \times 21$, qui est encore divisible par 3.

$189 = 3^3 \times 7$ et ce produit ne contient que des facteurs premiers.

- 16 758

$$= 2 \times 8\,379$$

$$= 2 \times 3 \times 2\,793$$

$$= 2 \times 3^2 \times 931$$

$$= 2 \times 3^2 \times 7 \times 133$$

$$= 2 \times 3^2 \times 7^2 \times 19$$

Exemple 2 $126 = 2 \times 63 = 2 \times 3 \times 21 = 2 \times 3^2 \times 7$

$$735 = 3 \times 245 = 3 \times 5 \times 49 = 3 \times 5 \times 7^2$$

En prenant les plus grandes puissances figurant à la fois dans la décomposition des deux nombres, on trouve que $\text{pgcd}(126 ; 735) = 3 \times 7 = 21$

Exemple 3

$$5\,292 = 2^2 \times 1323 = 2^2 \times 3^3 \times 49 = 2^2 \times 3^3 \times 7^2$$

$$5\,544 = 2^3 \times 693 = 2^3 \times 3^2 \times 77 = 2^3 \times 3^2 \times 7 \times 11.$$

$$\text{Donc } \text{pgcd}(5\,292 ; 5\,544) = 2^2 \times 3^2 \times 7 = 252 \text{ et :}$$

$$\frac{5\,292}{5\,544} = \frac{21 \times 252}{22 \times 252} = \frac{21}{22}$$

On sait alors qu'il existe $k \in \mathbb{N}$ tel que $a = 21k$ et $b = 22k$.

$$\text{Donc } 21k + 22k = 903 \Leftrightarrow 43k = 903 \Leftrightarrow k = 21.$$

$$\text{Ainsi, } a = 21 \times 21 = \mathbf{441} \text{ et } b = 22 \times 21 = \mathbf{462}.$$

2b. Nombre de diviseurs

Propriété :

Soit $n \geq 2$ admettant pour décomposition $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$

- Le nombre de diviseurs de n est alors $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.
- Un entier est un carré parfait ssi il admet un nombre impair de diviseurs.
- Tout diviseur d de n admet une décomposition :

$$p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$$

où pour tout indice i , $0 \leq \beta_i \leq \alpha_i$

Exemple 1 Trouver le nombre de diviseurs de 120 et de 1 575.

Exemple 2 Un entier naturel n possède 15 diviseurs. On sait de plus que n est divisible par 6 mais pas par 8. Quel est cet entier ?

Exemple 1

- $120 = 2^3 \times 3 \times 5$.

Le nombre de diviseurs de 120 est donc $(3 + 1)(1 + 1)(1 + 1) = 4 \times 2 \times 2 = \mathbf{16}$.

- $1\,575 = 3^2 \times 175 = 3^2 \times 5^2 \times 7$

Le nombre de diviseurs de 1575 est $(2 + 1)(2 + 1)(1 + 1) = 3 \times 3 \times 2 = \mathbf{18}$.

Exemple 2

- n possède 15 diviseurs, et d'après la propriété, ce nombre de diviseurs est de la forme $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$: c'est un produit.

Deux décompositions sont possibles : on peut avoir :

$(\alpha_1 + 1) = 15$, soit $\alpha_1 = 14$

ou bien $(\alpha_1 + 1) = 3$ et $(\alpha_2 + 1) = 5$, soit $\alpha_1 = 2$ et $\alpha_2 = 4$.

- Comme n est divisible par 6, on sait que la décomposition fait intervenir les deux nombres premiers 2 et 3. Cela exclut donc le premier cas $\alpha_1 = 14$.

On sait donc que $n = 2^i \times 3^j$; avec $i = 2$ et $j = 4$, ou bien $i = 4$ et $j = 2$.

- Or de plus, n n'est pas divisible par 8, donc la puissance i ne peut pas être égale à 4 (sinon n serait même divisible par 16). Ainsi, on a $i = 2$ et $j = 4$.

Conclusion : $n = 2^2 \times 3^4 = 324$.

3. Petit théorème de Fermat

3a. Énoncé

Propriété :

- Soit p premier, et $a \in \mathbb{N}$ non multiple de p . Alors $a^{p-1} \equiv 1[p]$.
- De plus, si a est un entier naturel quelconque, $a^p \equiv a[p]$.

Exemple 1 Montrer que $4^{12} + 6$ est multiple de 7.

Exemple 2 Montrer que pour tout n entier naturel, $3^{6n} - 1$ est divisible par 7.

Exemple 3 Soit $n \in \mathbb{N}$ et $a = n^5 - n$.

a. Montrer que a est divisible par 5.

b. Montrer que $a = n(n^2 - 1)(n^2 + 1)$ puis que a est divisible par 2 et 3.

En déduire que a est divisible par 30.

Exemple 1 D'après le petit théorème de Fermat, $4^6 \equiv 1[7]$.

Ainsi, $4^{12} \equiv (4^6)^2 \equiv 1[7]$,

et $4^{12} + 6 \equiv 1 + 6 \equiv 0[7]$, donc $4^{12} + 6$ est multiple de 7.

Exemple 2 D'après le petit théorème de Fermat, $3^6 \equiv 1[7]$.

Donc pour tout n entier naturel, $3^{6n} \equiv (3^6)^n \equiv 1^n \equiv 1[7]$.

Ainsi, $3^{6n} - 1 \equiv 1 - 1 \equiv 0[7]$ et $3^{6n} - 1$ est multiple de 7.

Exemple 3

a. D'après le petit théorème de Fermat, $n^5 \equiv n[5]$, donc $n^5 - n \equiv 0[5]$.
 $n^5 - n$ est divisible par 5.

b. • On développe l'expression proposée :

$$n(n^2 - 1)(n^2 + 1) = (n^3 - n)(n^2 + 1) = n^5 + n^3 - n^3 - n = n^5 - n$$

• Si n est pair, alors a est pair.

Si n est impair, alors n^2 est impair, donc $(n^2 + 1)$ est pair. Ainsi, a est pair.

Dans les deux cas, a est divisible par 2.

• Si $n \equiv 0[3]$, alors a est divisible par 3.

Si $n \equiv 1[3]$, alors $n^2 - 1 \equiv 0[3]$, et ainsi a est divisible par 3.

Si $n \equiv 2[3]$, alors $n^2 - 1 \equiv 3 \equiv 0[3]$, et ainsi a est divisible par 3.

Dans tous les cas, a est divisible par 3.

• a est donc divisible par 2, 3 et 5, qui sont premiers entre eux. Donc a est divisible par 30.

3b. Chiffrement RSA

Le système RSA

Son nom provient des initiales de ses inventeurs en 1977 : Ronald Rivest, Adi Shamir et Leonard Adleman.

Soient p et q deux nombres premiers impairs distincts. On pose $n = pq$ et $m = (p - 1)(q - 1)$.

Soit e un entier tel que $1 < e < m$ avec e et m premiers entre eux.

On peut montrer qu'il existe alors un entier d unique, tel que $1 \leq d < m$ et $ed \equiv 1[m]$.

De plus pour tout a entier naturel, si b est le reste dans la division de a^e par n , alors $b^d \equiv a[n]$.

Envoi d'un message

Alice veut transmettre un message à Bob.

Pour cela, Bob choisit deux nombres p et q , détermine un nombre e .

a. Supposons que Bob ait choisi $p = 3$ et $q = 11$. Il a aussi $e = 7$. Déterminer n , m et enfin d (cf **partie A**).

Bob diffuse à tout le monde les nombres (n, e) , qui représentent sa *clé publique*.

Il garde pour lui les nombres (p, q) , qui représentent sa *clé privée*.

Alice veut transmettre à Bob le mot « SALUT ».

Elle utilise le tableau ci-contre pour coder chaque lettre du mot :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

b. Déterminer le codage de chaque lettre .

Ensuite, pour chaque lettre a , elle la transforme en b tel que $a^e \equiv b[n]$. Ce sont ces lettres qu'elle envoie à Bob.

c. Vérifier qu'Alice envoie les lettres suivantes : 6 – 0 – 11 – 26 – 13.

d. Comment Bob peut-il faire pour décoder le message ainsi reçu ?

e. Décoder cet autre message qu'Alice a envoyé à Bob : 13 – 26 – 21 – 0 – 6 – 1 – 2 – 16 – 7

a. On calcule $n = 3 \times 11 = 33$ et $m = 2 \times 10 = 20$.

On cherche alors d tel que $7d \equiv 1[20]$. $7 \times 3 = 21 \equiv 1[20]$. Ainsi, $d = 3$.

b. Le mot SALUT devient : 18 – 0 – 11 – 20 – 19.

c. Pour chaque chiffre a , Alice calcule a^7 puis le reste de la division de a^7 par 33.

Par exemple pour 18 : $18^7 = 612\,220\,032$,

or $612\,220\,032 = 18\,522\,122 \times 33 + 6$. Donc le 18 devient bien un 6.

Il en est de même pour les lettres suivantes.

d. D'après la propriété énoncée au début, $b^d \equiv a[n]$.

Ainsi, pour chaque a , Bob calcule a^3 puis le reste de la division de a^3 par 33.

Par exemple pour le 6 reçu : $6^3 = 216$ et $216 = 6 \times 33 + 18$. On retrouve 18.

Il en est de même pour les lettres suivantes.

e. On applique la même méthode pour chaque lettre.

Par exemple, $13^3 = 2\,197$ et $2\,197 = 66 \times 33 + 19$. La 1^{ère} lettre est 19, soit T.

On trouve dans l'ordre : 19 – 20 – 21 – 0 – 18 – 1 – 8 – 4 – 13.

c'est-à-dire TU VAS BIEN. Alice s'enquiert donc de l'état de Bob.