Chapitre III

Nombres premiers et arithmétique

Table des matières

Partie A

Les nombres premiers

1. Définitions et premières propriétés

Définition 1. *Nombre premier*

Soit p un entier naturel. On dit que p est **premier** s'il possède **exactement deux diviseurs positifs distincts**.

Question 1.

Si p est un nombre premier, quels sont ses deux diviseurs positifs ?

Réponse : Comme tout nombre entier est divisible par 1 et lui-même, les diviseurs positifs de p sont donc 1 et p !

Exemple 1.

— 0 et 1 ne sont pas des nombres premiers.
— 2 ou 19 par exemple, sont des nombres premiers.

Activité d'introduction : le crible d'Ératosthène Math'x Problème 2 page 49.

Notation 1. *Ensemble des diviseurs positifs d'un nombre*

Soit n un entier relatif. On note $\mathcal{D}_n$ l'ensemble des diviseurs positifs de n i.e.

$$\mathcal{D}_n = \{k \in \mathbb{N} \mid k \text{ divise } n\}.$$

Exemple 2.

— $\mathcal{D}_1 = \{1\}$; $\mathcal{D}_2 = \{1, 2\}$; $\mathcal{D}_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$; $\mathcal{D}_{-6} = \{1, 2, 3, 6\}$.
— $\mathcal{D}_0 = \mathbb{N}$ - c'est le seul ensemble de diviseurs infini.
— Si p est un nombre premier, $\mathcal{D}_p = \{1, p\}$.

Proposition 1.

Soit n un nombre entier supérieur ou égal à 2. Alors n possède un diviseur premier.
Plus précisément, le plus petit diviseur positif, différent de 1, de n est un nombre premier.

Démonstration.

Soit n un entier supérieur ou égal à 2. On procède par disjonction de cas :

- *1er cas :* n est un nombre premier. Alors n divise n donc n possède un diviseur premier.
- *2eme cas :* n est n'est pas un nombre premier. Comme $n > 1$ et n non premier, l'ensemble

$$\mathcal{D}_n^* = \{k \in \mathbb{N} \mid k \text{ divise } n \text{ et } 1 < k < n\}$$

est une partie non vide de $\mathbb{N}$: par suite, elle possède un plus petit élément noté d.
Montrons que d est premier. Soit a un diviseur positif de d différent de 1. Montrons que $a = d$. On a $1 < a \leq d < n$, car $a, d \geq 0$ et a divise d et comme d divise n, par transitivité, a divise n.
Par suite, a appartient à $\mathcal{D}_n^*$. Or d est le plus petit élément de $\mathcal{D}_n^*$ donc $a \geq d$. Ainsi $d \leq a \leq d$ donc $a = d$.
Il en résulte que les diviseurs de d sont exactement 1 et lui-même donc d est premier. D'où n possède un diviseur premier.

Dans tous les cas, n possède un diviseur premier. □

Proposition 2.

Soit n un nombre entier supérieur ou égal à 2. Si n n'est pas premier, alors n possède un diviseur premier p tel que :

$$p \leq \sqrt{n}.$$

Démonstration.

Soit n un nombre entier supérieur ou égal à 2. On suppose que n n'est pas premier. Alors le plus petit diviseur p de n positif et différent de 1 est premier d'après la proposition 1. Comme n n'est pas premier, on a $p < n$ et comme p divise n et p positif, il existe $q \in \mathbb{N}$ tel que $n = pq$.
De plus, $q \neq 1$ car $p < n$ et $p \leq q$ car p est le plus petit diviseur de n positif et différent de 1.
Par suite, on a $p^2 \leq pq = n$ et donc, par croissance de la fonction $x \mapsto \sqrt{x}$, $p \leq \sqrt{n}$. □

Corollaire 1.

Soit n un nombre entier supérieur ou égal à 2. Si, pour tout entier $k \geq 2$ tel que $k \leq \sqrt{n}$, k ne divise pas n, alors n est un nombre premier.

Démonstration.

Soit n un nombre entier supérieur ou égal à 2. On suppose que, pour tout entier $k \geq 2$ tel que $k \leq \sqrt{n}$, k ne divise pas n. Par contraposée de la proposition précédente, on obtient :

Si n ne possède par de diviseur premier p tel que $p \leq \sqrt{n}$, alors n est premier.
Or, comme pour tout entier $k \geq 2$ tel que $k \leq \sqrt{n}$, k ne divise pas n alors, a fortiori, n ne possède par de diviseur premier p tel que $p \leq \sqrt{n}$. Donc n est premier. □

Exercice 1.

En utilisant le corollaire précédent, écrire en pseudo-code, un algorithme qui teste la primalité d'un entier n donné.

Algorithme de test de primalité

```
Argument : n entier naturel

Variables : D booléen

Initialisation : D = VRAI

Traitement :
    POUR k ALLANT DE 2 À E(sqrt(n)) FAIRE
        SI k divise n FAIRE
            D = FAUX
        FIN SI
    FIN POUR

Sortie :
    RETOURNER D
```

Théorème 1.

Il existe une infinité de nombres premiers.

Démonstration.

On raisonne par l'absurde. On suppose qu'il existe un nombre fini de nombre premiers : notons $p_1, ..., p_n$ la liste de ces nombres.
On pose $N = p_1...p_n + 1$. On a $N > 1$ et pour tout $i \in [\![1, n]\!]$, $N > p_i$, donc N est un entier supérieur ou égal à 2 qui n'est pas premier (il ne fait pas partie de la liste $p_1, ..., p_n$).
Ainsi, d'après la proposition 1, N possède un diviseur premier p. Alors p fait partie de la liste $p_1, ..., p_n$ et donc il divise le produit $p_1...p_n$. De plus, p divise N, donc, par combinaison linéaire,

$$p \text{ divise } N - (p_1...p_n) = p_1...p_n + 1 - p_1...p_n = 1.$$

Donc $p = 1$. Contradiction ! car p est un nombre premier.
Ainsi, l'hypothèse "il existe un nombre fini de nombre premier" est absurde : il existe donc une infinité de nombres premiers. □

2. Décomposition en facteurs premiers

Théorème 2. *Décomposition en facteurs premiers*

Soit n un entier supérieur ou égal à 2. Alors n se décompose en un produit de nombres premiers i.e. il existe $p_1, ..., p_k$ des nombres premiers et $\alpha_1, ..., \alpha_k$ des entiers naturels non nuls tels que :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}.$$

Cette décomposition est unique à l'ordre des facteurs près.

Exemple 3.

Les décompositions en facteurs premiers de 42 et de 720 sont :

$$42 = 2 \times 3 \times 7 \qquad \text{et} \qquad 720 = 2^4 \times 3^2 \times 5.$$

Exercice 2.

1. Déterminer les décompositions en facteurs premiers des nombres suivants :

$$12 \qquad 19 \qquad 90 \qquad 242 \qquad 2925.$$

2. Soit n un entier supérieur ou égal à 2 de décomposition en facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$.
   a) Déterminer $\mathcal{D}_n$ i.e. la liste des diviseurs positifs de n.
   b) En déduire l'ensemble $\mathcal{D}_{2925}$.
   c) Quel est le nombre de diviseurs positifs de n (c'est-à-dire le cardinal de $\mathcal{D}_n$) ?

3. Exercices

Exercice 3. *Nombres de Mersenne*

On appelle **nombre de Mersenne**, un nombre entier naturel de la forme :

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

1. Calculer M_n pour $n = 0, 1, ..., 6$. Que pourrais-t-on conjecturer de prime abord ?
2. On souhaite démontrer que si n n'est pas premier, alors M_n n'est pas premier.
   a) Soit $x, k \in \mathbb{N}^*$. Montrer que $x^k - 1$ est divisible par $x - 1$.
   b) En déduire que si $n \geq 2$ n'est pas un nombre premier, alors M_n n'est pas premier.
3. a) Calculer M_{11} et déterminer sa décomposition en facteur premier.
   b) Que dire de l'assertion "si n est premier, alors M_n est premier" ?

4. Soit $n \in \mathbb{N}^*$. En utilisant la question 2.a), exprimer $\sum_{k=0}^{n-1} M_k$ en fonction de M_n.

Correction.

1. On a :
   - $M_0 = 2^0 - 1 = 0$
   - $M_1 = 2^1 - 1 = 1$
   - $M_2 = 2^2 - 1 = 3$
   - $M_3 = 2^3 - 1 = 7$
   - $M_4 = 2^4 - 1 = 15$
   - $M_5 = 2^5 - 1 = 31$
   - $M_6 = 2^6 - 1 = 63$

   On a alors l'impression que si n n'est pas premier alors M_n n'est pas premier et que si n est premier, alors M_n est premier. Mais pour la deuxième affirmation, il ne s'agit que d'une impression !

2. a) Pour un entier $x \geq 2$, on a :
   $$x^k - 1 = (x-1)(1 + x + ... + x^{k-1}) = (x-1)q$$
   où $q = (1 + x + ... + x^{k-1}) \in \mathbb{N}$.
   Par suite, $x - 1$ divise $x^k - 1$.

   b) Soit $n \geq 2$. On suppose que n n'est pas premier. Alors il existe un entier d tel que $1 < d < n$ et $n = dk$ où $k \in \mathbb{N}^*$. On a alors :
   $$M_n = 2^n - 1 = 2^{dk} - 1 = (2^d)^k - 1$$
   Ainsi, d'après la question précédente, $2^d - 1$ divise M_n et de plus, par croissance de la fonction $t \mapsto 2^t$ sur $\mathbb{R}$, on a, comme $1 < d < n$:
   $$1 < 2^d - 1 < M_n.$$
   Par suite, $2^d - 1$ est un diviseur propre de M_n.
   Il en résulte que M_n n'est pas un nombre premier.

3. a) On a $M_{11} = 2027 = 23 \times 89$ donc M_{11} n'est pas premier

   b) Cette assertion est fausse car 11 est premier et M_{11} ne l'est pas.

4. Soit $n \in \mathbb{N}^*$. D'après la question 2a), on a :
   $$M_n = 2^n - 1 = (2-1)(1 + 2 + \ldots + 2^{n-1}) = \sum_{k=0}^{n-1} 2^k.$$
   Or on a :
   $$\sum_{k=0}^{n-1} M_k = \sum_{k=0}^{n-1} (2^k - 1) = \sum_{k=0}^{n-1} 2^k - \sum_{k=0}^{n-1} -1 = M_n - n$$
   Donc :
   $$M_n = n + \sum_{k=0}^{n-1} M_k.$$

Pour aller plus loin : Math'x Problème 4 p62

Partie B

PGCD, théorème de Bézout et théorème de Gauss

1. Le PGCD de deux nombres entiers

a. Définition

Proposition-Notation 3.

Soit a, b des entiers relatifs non tous nuls. On note $\mathcal{D}(a,b)$ l'ensemble des diviseurs communs de a et de b i.e.$\mathcal{D}(a,b) = \mathcal{D}_a \cap \mathcal{D}_b$.
L'ensemble $\mathcal{D}(a,b)$ admet un plus grand élément.

Démonstration.

Soit a, b des entiers relatifs non tous nuls. Quitte à échanger a et b, on peut supposer que a est non nul. Alors $\mathcal{D}_a$ est un ensemble majoré par a et donc, comme $\mathcal{D}(a,b) = \mathcal{D}_a \cap \mathcal{D}_b \subset \mathcal{D}_a$, $\mathcal{D}(a,b)$ est majoré par a.
De plus, comme 1 est positif et divise tous les entiers relatifs, 1 appartient à $\mathcal{D}_a$ et $\mathcal{D}_b$ donc $1 \in \mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}(a,b)$.
Par suite, $\mathcal{D}(a,b)$ est une partie non-vide et majorée de $\mathbb{N}$, donc elle possède un plus grand élément. □

Définition 2. *PGCD*

Soit a, b des entiers relatifs non tous nuls. On appelle **Plus Grand Commun Diviseur (PGCD) de a et b** et on note $\mathbf{pgcd(a,b)}$ le plus grand élément de l'ensemble $\mathcal{D}(a,b)$ des diviseurs communs de a et b.

Exemple 4.

$$\text{pgcd}(6,9) = 3 \qquad \text{pgcd}(8,28) = 4 \qquad \text{pgcd}(-10,25) = 5$$
$$\text{pgcd}(21,32) = 1 \qquad \text{pgcd}(0,11) = 11.$$

b. Propriétés

Lemme 1.

Soit a et b des entiers relatifs non tous nuls. Alors on a $\mathcal{D}(a,b) = \mathcal{D}(a-b,b)$ et plus généralement,

pour tout $k \in \mathbb{Z}$:

$$\mathcal{D}(a,b) = \mathcal{D}(a - kb, b).$$

Proposition 4. *Propriétés du PGCD*

Soit a et b des entiers relatifs non tous nuls.

i) Pour tout $k \in \mathbb{Z}$, $\text{pgcd}(a,b) = \text{pgcd}(a-b,b) = \text{pgcd}(a-kb,b)$.

ii) Si $0 < b < a$ et r est le reste de la division euclidienne de a par b :

$$\text{pgcd}(a,b) = \text{pgcd}(r,b)$$

iii) Si $b > 0$ et b divise a, $\text{pgcd}(a,b) = b$.

c. Algorithme d'Euclide

La propriété *ii)* de la proposition 4 nous permet d'obtenir un algorithme pratique du calcul du PGCD de deux entiers :

Algorithme d'Euclide

Arguments : a,b entiers relatifs avec $b \neq 0$

Variable : r entier naturel

Initialisation : r =reste de la division euclidienne de a par b

Traitement :

- TANT QUE r différent de 0 FAIRE
- r = reste de la division euclidienne de a par b
- $a = b$
- $b = r$
- FIN TANT QUE

Sortie :

- RETOURNER a

Exercice 4.

Soit a, b deux entiers naturels non nuls tel que $0 < b < a$ et b ne divise pas a.
Soit $(r_n)_{n\in\mathbb{N}}$ la suite des valeurs de la variable r dans l'algorithme d'Euclide.

1. En utilisant une deuxième suite d'entiers relatifs $(q_n)_{n\in\mathbb{N}}$, déterminer une relation de récurrence entre r_{n+1} et r_n.
2. Montrer qu'il existe $N \in \mathbb{N}$ tel que $r_N \neq 0$ et et pour tout $n > N$, $r_n = 0$.
3. Montrer que $r_N = \text{pgcd}(a,b)$.

Proposition 5.

Soit a, b deux entiers relatifs non nuls tel que $0 < b < a$ et b ne divise pas a.
Si r est le dernier reste non nul de l'algorithme d'Euclide, alors

$$\text{pgcd}(a, b) = r.$$

De plus, les diviseurs communs de a et b sont exactement les diviseurs de $\text{pgcd}(a, b)$ i.e.

$$\mathcal{D}(a, b) = \mathcal{D}_{\text{pgcd}(a,b)}.$$

Exercice 5.

Calculer le PGCD de 456 et 24 ; de 565 et 121 et de 121 et 18.

Proposition 6.

Soit a, b des entiers relatifs non nuls et c un entier naturel. On a :

$$\text{pgcd}(ac, bc) = c \times \text{pgcd}(a, b).$$

d. Nombres premiers entre eux

Définition 3.

Soit a et b deux entiers relatifs non tous nuls. On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$; sinon, ils ne le sont pas.

Proposition 7.

Soit a et b deux entiers relatifs non tous nuls. Si a et b sont premiers entre eux, alors 1 est le seul diviseur positif commun à a et b.

Méthode pour montrer que deux entiers a et b sont premiers entre eux :
On applique l'algorithme d'Euclide à a et b : si le dernier reste non nul est 1, a et b sont premiers entre eux.

Exercice 6.

Montrer que 2173 et 1961 ne sont pas premiers entre eux alors que 2173 et 1962 le sont.

Théorème 3.

Soit a, b des entiers relatifs non nuls et d un entier naturel non nul. Alors on a : $d = \text{pgcd}(a, b)$ si, et seulement si, il existe a', b' des entiers relatifs tels que :

$$a = da',\ b = db' \text{ ET } a' \text{ et } b' \text{ sont premiers entre eux.}$$

e. Exercices types

Exercice 7.

Soit n un entier naturel. Déterminer $\text{pgcd}(n+3, 2n+1)$ en fonction de n.

Correction.

On pose $d = \text{pgcd}(n+3, 2n+1)$. Alors d divise $n+3$ et $2n+1$ donc d divise la combinaison linéaire $2(n+3) - (2n=1) = 5$. Ainsi $d = 1$ ou $d = 5$.
On remarque alors que $d = 5$ si, et seulement si, 5 divise $n+3$ et $2n+1$ i.e.

$$n+3 \equiv 0 \mod 5\ (1) \quad \text{et} \quad 2n+1 \equiv 0 \mod 5\ (2)$$

si on calcule $(2) - (1)$, on obtient alors :

$$n \equiv 2 \mod 5$$

i.e. $n = 5k+2$ pour $k \in \mathbb{N}$.
Réciproquement, on remarque que si $n = 5k+2$ pour $k \in \mathbb{N}$, alors 5 divise $n+3$ et 5 divise $2n+1$ et donc $d = 5$.
Il en résulte que pour $n = 5k+2$ avec $k \in \mathbb{N}$,

$$\text{pgcd}(n+3, 2n+1) = 5$$

et das les autres cas :

$$\text{pgcd}(n+3, 2n+1) = 1$$

Exercice résolu 8 p87 ; exercice 24 p102

Exercice 8.

Déterminer tous les couples d'entiers (a, b) avec $0 < a < b$ tels que

$$\begin{cases} ab = 3468 \\ \text{pgcd}(a, b) = 17 \end{cases}$$

Correction.

$\text{pgcd}(a,b) = 17$ est équivalent à $a = 17a'$ et $b = 17b'$ où a' et b' sont des entiers premiers entre eux.
Par suite, on a :

$$3468 = ab = 17^2 a'b'$$

Or $3468 = 17^2 \times 6$ donc $a'b' = 12$ d'où, comme $a' < b'$, les couples possibles pour (a', b') sont :

$$(1, 12),\ (2, 6),\ \text{et}\ (3, 4)$$

De plus, comme $\text{pgcd}(a', b') = 1$, le couple $(2, 6)$ ne convient pas.
Il en résulte que les seuls couples $(a, b) = (17a', 17b')$ vérifiant le problème sont :

$$(17, 17 \times 12) = (17, 204) \text{ et } (17 \times 3, 17 \times 4) = (51, 68).$$

Exercice résolu 7 p87 ; exercice 20,21,22 p102

2. Théorème de Bézout et théorème de Gauss

a. Théorème de Bézout

Proposition 8. *Relation de Bézout*

Soit a, b des entiers non tous nuls et $d = \text{pgcd}(a, b)$. Alors il existe u, v des entiers **relatifs** tels que :

$$au + bv = d$$

Démonstration.

On remonte l'algorithme d'Euclide ! □

Méthode : pour trouver une combinaison linéaire de a et b égale au PGCD de a et b, on remonte l'algorithme d'Euclide

Exercice 9.

Déterminer une relation de Bézout pour le couple $(45, 81)$

Voire exercice résolu 9 p89 et exercices 30,31 p103

Théorème 4. *Théorème de Bézout*

Soit a, b des entiers non nuls.
Les entiers a et b sont premiers entre eux **si, et seulement si,** il existe u, v des entiers **relatifs** tels que

$$au + bv = 1$$

Exercice 10.

1. Soit $n \in \mathbb{N}$. Montrer que $7n + 4$ et $5n + 3$ sont premiers entre eux.
2. Soit a, b, c des entiers naturels non nuls. Montrer que si a est premier avec b et a est premier avec c alors a est premier avec bc.

Voire exercice 27,28 p103

Exercice 11.

Déterminer un couple d'entiers relatifs (x, y) tels que :

1. $59x + 27y = 1$
2. $59x + 27y = 10$
3. $12x + 18y = 30$
4. $12x + 18y = 21$

Voire exercice résolu 10 p89 et exercices 49,50 p104-105

b. Théorème de Gauss

Théorème 5. *Théorème de Gauss*

Soit a, b, c des entiers *naturels* non nuls. Si a est *premier avec* b et a divise bc alors a divise c.

Corollaire 2.

Soit n, a, b des entiers naturels non nuls. Si a divise n, b divise n et a, b sont premiers entre eux alors ab divise n.

Exercice 12.

Déterminer tous les couples d'entiers relatifs (x, y) tels que :

1. $59x + 27y = 1$
2. $59x + 27y = 10$
3. $12x + 18y = 30$
4. $12x + 18y = 21$

Voire exercice résolu 10 p89 et exercices 49,50 p104-105

3. Exercices

Exercice 13.

Dans un plan muni d'un repère orthonormé, on considère les points $A(-3; 28)$ et $B(24; 10)$.

1. Donner une équation cartésienne de la droite (AB) i.e. sous la forme $ax + by = c$.
2. Soit $M(x, y)$ un point du plan. Montrer que M appartient à la droite (AB) si, et seulement si, $2x = 3(26 - y)$.
3. Déterminer tous les points à coordonnées entières du segment $[A, B]$.

Voire exercice 51 p105

Exercice 14.

Exercice 47 p104

Exercice 15.

Le Centurion Caius Bonus voudrait déterminer le nombre de soldats Romains du camp fortifié Petitbonum. Il connaît approximativement ce nombre : entre 92 et 117. Il sait de plus que s'il demande à ses soldats de se regrouper par trois, alors un soldat se retrouve seul ; et s'il leur demande de se regrouper par sept, alors il reste un groupe de deux soldats.

Pouvez-vous aider Caius Bonus à retrouver le nombre exact de soldats qu'il dirige ?

Voire exercice 46 p104