Chapitre 6

Nombres premiers

Sommaire

Sauf indication contraire, dans tout le chapitre, on ne considèrera que des nombres entiers positifs et leurs diviseurs ou multiples positifs.

On rappelle trois axiomes [1] fondamentaux de l'arithmétique :

Axiome 1 : Toute partie non vide de $\mathbb{N}$ admet un plus petit élément (c'est faux dans $\mathbb{Z}$).

Axiome 2 : Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

Axiome 3 : Toute suite d'entiers naturels strictement décroissante est finie (c'est faux dans $\mathbb{Z}$).

Les preuves seront faites en classe.

6.1 Nombres premiers

6.1.1 Définition

Définition 6.1. Un entier naturel n est dit *premier* s'il possède exactement deux diviseurs dans $\mathbb{N}$: 1 et lui même.

$$n \text{ premier} \Leftrightarrow \text{card}(\mathscr{D}(n)) = 2$$

Un entier naturel n, distinct de 1, non premier est dit *composé*.

Remarques.

- 1 n'est ni premier, ni composé ;
- 2 est le plus petit nombre premier et le seul pair ;
- Un nombre composé admet au moins un autre diviseur que 1 et lui-même (sinon il serait premier) ; ces diviseurs sont parfois appelés *diviseurs stricts*.

1. Un axiome désigne une vérité première – donc qui ne se démontre pas – à l'intérieur d'une théorie.

6.1.2 Ensemble des nombres premiers

Théorème 6.1. *Il existe une infinité de nombres premiers.*

6.1.3 Divisibilité par un nombre premier

Propriété 6.2. *Soit $n \in \mathbb{N}$ et p un nombre premier. Alors soit p divise n, soit p et n sont premiers entre eux.*

Théorème 6.3. *Tout entier naturel n distinct de 1 admet au moins un diviseur premier.*

Propriété 6.4. *Soit $n \geqslant 2$ un entier.*
- *Si n est un nombre composé alors il existe un nombre premier p tel que p divise n et $p \leqslant \sqrt{n}$.*
- *Si un nombre entier $n \geqslant 2$ n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$, alors n est premier.*

Exemple 6.1. 317 est-il premier ?
$\sqrt{317} \approx 17,8$. On teste si les nombres premiers inférieurs à 17 divisent 317.
Si oui, 317 est composé, sinon il est premier.

Propriété 6.5. *Soit un entier premier p.*
- *Si p divise un produit de facteurs alors il divise au moins l'un des facteurs.*
- *Si p divise un produit de facteurs premiers, alors il est égal à l'un d'entre eux.*

6.2 Décomposition en produit de facteurs premiers

6.2.1 Décomposition en produit de facteurs premiers

Théorème 6.6. *Tout entier naturel $n \geqslant 2$ est premier ou est un produit de nombres premiers.*

Théorème 6.7. *Soit un entier naturel $n \geqslant 2$. Alors n se décompose de façon unique sous la forme :*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$$

avec p_i nombres premiers tels que $0 < p_1 < p_2 < \ldots < p_m$ et $\alpha_i \in \mathbb{N}^*$.

Propriété 6.8. *Soit un entier naturel $n \geqslant 2$ dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$ avec p_i nombres premiers tels que $0 < p_1 < p_2 < \ldots < p_m$ et $\alpha_i \in \mathbb{N}^*$.*
Alors d est un diviseur positif de n si et seulement si $d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_m^{\beta_m}$ avec, pour tout $i \in [\![1\,;m]\!]$, $0 \leqslant \beta_i \leqslant \alpha_i$.

Corollaire 6.9. *Soit un entier naturel $n \geqslant 2$, dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$ avec p_i nombres premiers tels que $0 < p_1 < p_2 < \ldots < p_m$ et $\alpha_i \in \mathbb{N}^*$.*
Alors n admet $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_m+1)$ diviseurs.

6.2.2 Savoir faire

Obtenir la décomposition en produits de facteurs premiers

On divise n par chaque nombre premier connu, dans l'ordre croissant, tant qu'il divise encore le quotient, puis on passe au suivant, jusqu'à obtenir 1 comme quotient.
La présentation ci-contre est celle choisie en général.
On obtient alors $924 = 2^2 \times 3 \times 7 \times 11$.

924	2
462	2
231	3
77	7
11	11
1	

Obtenir le PGCD de deux entiers naturels

Soit n et m deux entiers naturels supérieurs à 2.
Soit p_i les diviseurs premiers de n ou de m. Alors $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ et $m = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$.

Remarque. Si p_i ne divise pas, par exemple, n alors $\alpha_i = 0$.

Alors $n \wedge m = p_1^{\min(\alpha_1;\beta_1)} \times p_2^{\min(\alpha_2;\beta_2)} \times \ldots \times p_r^{\min(\alpha_r;\beta_r)}$.

Exemple.

924	2
462	2
231	3
77	7
11	11
1	

donc $924 = 2^2 \times 3 \times 7 \times 11$.

540	2
270	2
135	3
45	3
15	3
5	5
1	

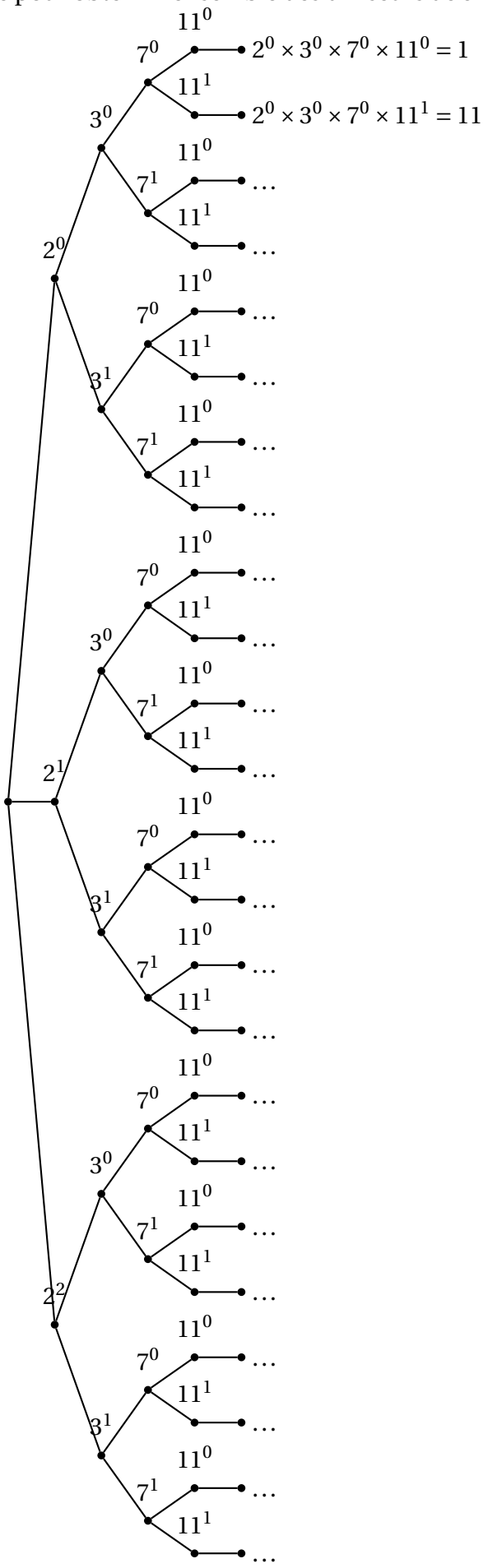
donc $540 = 2^2 \times 3^3 \times 5$.

Donc $924 \wedge 540 = 2^2 \times 3 = 12$.

Obtenir l'ensemble des diviseurs positif d'un entier naturel

D'après le corollaire 6.9, 924 a $3 \times 2 \times 2 \times 2 = 24$ diviseurs. Un arbre permet de les obtenir. Voir la figure 6.1, page suivante.

FIGURE 6.1: Arbre pour obtenir l'ensemble des diviseurs de $924 = 2^2 \times 3 \times 7 \times 11$



6.3 Exercices et problèmes

EXERCICE 6.1.
Soit a un entier naturel.

1. Développer $(a^2-a+1)(a^2+a+1)$.
2. Le nombre a^4+a^2+1 peut-il être premier ?
3. Trouver une factorisation de 10 101

EXERCICE 6.2.
Démontrer que si la somme de deux nombres entiers a et b est un nombre premier, alors a et b sont premiers entre eux.

EXERCICE 6.3 (Nombres de SOPHIE GERMAIN)**.**
Pour n entier naturel, on considère le nombre $N = n^4+4$.
On se demande s'il existe des valeurs de n pour lesquelles N est premier.

1. (a) Montrer que si n est un multiple de 10, N est un multiple de 4.
   (b) En étudiant le dernier chiffre de N en fonction de celui de n, démontrer que N est un multiple de 5 si et seulement si n n'est pas multiple de 5.
   (c) Les valeurs obtenues pour N lorsque $n = 5$, $n = 15$ ou $n = 25$ sont-elles des nombres premiers ?
   (d) Soit n un entier naturel, $n > 1$.
   Peut-on déduire des questions précédentes certaines des affirmations suivantes :
      i. si n est multiple de 5, N n'est pas premier
      ii. si n n'est pas multiple de 5, N est premier
      iii. pour que N soit premier, il faut que n ne soit pas multiple de 5
      iv. pour que N soit premier, il suffit que n ne soit pas multiple de 5
2. (a) Montrer l'identité dite *de Sophie Germain* :
   $$n^4+4m^4 = (n^2+2m^2+2mn)(n^2+2m^2-2mn)$$
   pour tous n et m entiers.
   (b) En déduire une factorisation de 5^4+4, de 15^4+4 et de 25^4+4.
   Peut-on prévoir la factorisation de N pour $n = 35$?
3. Conclure.

EXERCICE 6.4.
Décomposer mentalement les nombres suivants en facteurs premiers : 60 ; 84 ; 90 ; 120 ; 140 ; 240 ; 250 ; 900 ; 3 600.

EXERCICE 6.5.
Décomposer 10! en facteurs premiers. En déduire son nombre de diviseurs.

EXERCICE 6.6.
Un entier a exactement 36 diviseurs positifs. Sa décomposition en facteurs premiers comporte 2 élevé à la puissance 3 ainsi que 5 et 7 élevés à une même puissance. Quel est ce nombre ?

PROBLÈME 6.1 (De MERSENNE à LUCAS-LEHMER)**.**
Les trois plus grands nombres premiers connus janvier 2017 sont :

- $2^{74\,207\,281} - 1$ découvert le 7 janvier 2016. Il s'écrit avec 22 338 618 chiffres ;
- $2^{57\,885\,161} - 1$ découvert le 25 janvier 2013. Il s'écrit avec 17 425 170 chiffres ;
- $2^{43\,112\,609} - 1$ découvert le 23 août 2008. Il s'écrit avec 12 978 189 chiffres.

Les onze plus grands nombres premiers connus sont de la forme $2^n - 1$ (le douzième ne l'est pas). Est-ce un hasard ou ces nombres sont-ils particuliers ?

Les nombres de la forme $2^n - 1$ pour n entier naturel, s'appellent les nombres de MERSENNE. Leurs diviseurs possèdent des propriétés particulières et il existe un test de primalité spécifique à ces nombres, ce qui explique l'intérêt qu'on leur porte dans la recherche des nombres premiers [2].

On posera dans la suite $M_n = 2^n - 1$, $n \in \mathbb{N}$.

A. Exploration, premiers résultats.

1. Pour $0 \leqslant n \leqslant 20$, déterminer si M_n est premier ou composé. Qu'observe-t-on quand n est composé ? Quand n est premier ?
2. Vérifier que, pour tout entier naturel non nul n :

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + 1)$$

   En déduire que si n est composé alors M_n l'est aussi.
3. On suppose que M_n admet un diviseur premier d. Justifier que $2^n \equiv 1 \pmod{d}$.

Si n est composé, tous les M_n sont composés. Mais on a vu que si n est premier, il existe des M_n composés. Ce sont leurs diviseurs que l'on va étudier de plus près.

B. Étude du cas où p est premier.
On considère un entier p premier tel que $M_p = 2^p - 1$ admette un diviseur premier d. Soit I l'ensemble des entiers naturels n non nuls tels que $2^n \equiv 1 \pmod{d}$.

1. Justifier que I n'est pas vide puis qu'il admet un plus petit élément p_0 et que $p_0 > 1$.
2. En écrivant la division eucilienne de n par p_0, montrer que tout élément de I est multiple de p_0. En déduire que $p = p_0$.
3. On admet que $2^{d-1} \equiv 1 \pmod{d}$ (cette propriété s'appelle le petit théorème de FERMAT). Déduire de la même manière que p_0 divise $d-1$ puis qu'il existe k un entier naturel tel que $d = 2kp + 1$.

C. Étude de deux nombres de MERSENNE.

1. $M_{19} = 2^{19} - 1 = 524\,297$
   (a) Justifier que les éventuels diviseurs premiers de M_{19} sont de la forme $d = 38k + 1$ avec $k \in \mathbb{N}$.
   (b) Combien y a-t-il de diviseurs de la forme $d = 38k + 1$, avec $d \leqslant \sqrt{M_{19}}$?
   (c) M_{19} est-il premier ?
2. $M_{23} = 2^{23} - 1 = 8\,388\,607$
   Quel est le premier diviseur possible de M_{23} ? M_{23} est-il premier ?

2. Chercher GIMPS sur Internet

D. Un test moderne pour les nombres de MERSENNE : LUCAS-LEHMER

On considère la suite S définie par : $S_0 = 4$ et $S_i = S_{i-1}^2 - 2$ pour $i \geqslant 1$.
La suite S permet de tester si des nombres de MERSENNE sont premiers ou non.

1. Démontrer que les S_i sont divisibles par 2 pour tout $i \geqslant 0$.
2. Soit p un entier premier. Étudions les restes R_i des S_i dans la division euclidenne par M_p.
   (a) Démontrer que $R_{i+1} \equiv R_i^2 - 2 \pmod{M_p}$.
   (b) Calculer les restes R_i pour tous les nombres premiers p entre 3 et 20 pour i de 0 à 30 (un tableur peut être pratique).
   (c) Pour un des nombres p considérés, aucun des reste n'est nul. Quel est ce nombre p ? Le nombre M_p correspondant est-il premier ?
   (d) Pour tous les autres, quel lien peut-on conjecturer entre p et le rang r du reste nul ? À l'aide de la calculatrice ou d'un logiciel, vérifier que les nombres M_p sont premiers.
   (e) À quoi ont alors égaux les restes à partir du rang $r+2$?
   (f) Démontrer que si pour un rang r, S_r est multiple de $2^p - 1$, alors les restes de S_r dans la division euclidienne par $2^p - 1$ sont égaux à 2 à partir du rang $r+2$.
3. Propriété de LUCAS-LEHMER
   On admet que, pour p premier supérieur ou égal à 3 :

$$S_{p-2} \equiv 0 \pmod{M_p} \Rightarrow M_p \text{ premier}$$

   (a) Compléter l'affichage de l'algorithme ci-dessous.

```
Saisir p // p premier, p>2
s prend la valeur 4
M prend la valeur 2^p-1
Pour k de 1 a p-2 faire
 s prend la valeur le reste de la division de s^2-2 par M
Fin Pour
Si s = 0 alors afficher...
         sinon afficher...
Fin Si
```

   (b) Entrer le programme correspondant sur un logiciel de votre choix. Le tester sur les nombres de MERSENNE étudiés en C.
   (c) Utiliser ce programme pour déterminer le(s)quel(s) des nombres suivants sont premiers : M_{107}, M_{607}, M_{3217}.