Thème 2 : Arithmétique

Fiche 1

Divisibilité-Division euclidienne

Exercices

.1. Divisibilité

Exercice 89. Déterminer les couples $(x;y)$ d'entiers naturels qui vérifient :

1. $x^2 = y^2 + 21$.
2. $x^2 - 7xy = 17$.

Exercice 90. Déterminer les entiers relatifs n qui vérifient :

1. $n^2 + n = 20$.
2. $n^2 + 2n = 35$.

Exercice 91. L'exercice consiste à trouver les valeurs du naturel $n > 4$ pour lesquelles la fraction $\dfrac{n+17}{n-4}$ est un entier.

1. Démontrer que $n-4$ divise $n+17$ équivaut à $n-4$ divise 21.
2. Déterminer alors toutes les valeurs de n correspondant au problème.

Exercice 92. Soit l'équation (E) : $xy - 5x - 5y - 7 = 0$.

1. Montrer que :
   $xy - 5x - 5y - 7 = 0 \Leftrightarrow (x-5)(y-5) = 32$.
2. Déterminer les couples d'entiers naturels $(x;y)$ qui vérifient (E).

Exercice 93. n est un naturel. Démontrer que quel que soit n, $3n^4 + 5n + 1$ est impair et en déduire que ce nombre n'est jamais divisible par $n(n+1)$.

.2. Division euclidienne

Exercice 94. Le but de cet exercice est de montrer la validité de la définition de la division euclidienne.

1. Démontrer le **lemme d'Archimède** :
   soit deux entiers naturels a et b ($b \neq 0$), alors il existe un entier naturel n tel que : $nb > a$.
2. **Existence** d'un couple $(q;r)$ tel que :
   $a = bq + r$ avec $0 \leqslant r < b$.
   Soit S l'ensemble des entiers s tels que : $bs > a$.
   (a) Montrer que S admet un plus petit élément t.
   (b) En déduire alors qu'il existe un entier q tel que : $bq \leqslant a < b(q+1)$.

3. **Unicité** du couple (q,r).
   On suppose qu'il existe deux couples $(q\,;r)$ et $(q'\,;r')$ tels que : $a=bq+r=bq'+r'$ avec $0\leqslant r<b$ et $0\leqslant r'<b'$.
   Montrer alors que nécessairement $q=q'$ et $r=r'$.

Exercice 95. Trouver les entiers naturels n qui, dans la division euclidienne par 4, donnent un quotient égal au reste.

Exercice 96. Trouver un entier naturel qui, dans la division euclidienne par 23, a pour reste 1 et, dans la division euclidienne par 17, a le même quotient et pour reste 13.

Exercice 97. On divise un entier naturel n par 152, puis par 147. Les quotients sont égaux et les restes respectifs sont 13 et 98. Quel est cet entier naturel n ?

Exercice 98. Si l'on divise un entier A par 6, le reste est 4. Quels sont les restes possibles de la division de A par 18 ?

Fiche 2

Pgdc-Algorithme d'Euclide

Exercices

Pgcd

Exercice 99. Dresser la liste des diviseurs positifs de 72 et de 60. En déduire leur PGCD.

Exercice 100. Si, en un point donné du ciel, un astre A apparaît tous les 28 jours et un astre B tous les 77 jours, avec quelle périodicité les verra-t-on simultanément en ce point ?

Exercice 101. Déterminer tous les entiers naturels n inférieurs à 200 tels que : $\text{pgcd}(n;324) = 12$.

Exercice 102. a et b sont deux entiers naturels non nuls tels que $a > b$.

1. Démontrer que : $\text{pgcd}(a;b) = \text{pgcd}(a-b;b)$.
2. Calculer les PGCD des entiers suivants par cette méthode, répétée autant de fois que nécessaire :
   (a) 308 et 165.
   (b) 1 008 et 308.
   (c) 735 et 210.
3. (a) Écrire en langage Python une fonction retournant le pgcd de a et b donnés en entrée correspondant à cette méthode.
   (b) Expliquer la condition de la ligne 6.

Algorithme d'Euclide

Exercice 103. Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1. 441 et 777.
2. 2004 et 9185.

Exercice 104. Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1. 2 012 et 7 545.
2. 1 386 et 546.

Exercice 105. Utiliser l'algorithme d'Euclide pour trouver le PGCD des nombres suivants :

1. 4 935 et 517.
2. 1 064 et 700.

Exercice 106. Les entiers suivants sont-ils premiers entre eux ?

1. 4 847 et 5 633.

2. 5 617 et 813.

Exercice 107. Si on divise 4 294 et 3 521 par un même entier positif, on obtient respectivement 10 et 11 comme reste.
Quel est cet entier ?

Exercice 108. En divisant 1 809 et 2 527 par un même entier naturel, les restes sont respectivement 9 et 7.
Quel est le plus grand nombre que l'on peut obtenir comme diviseur ?

Exercice 109. On note n un naturel non nul, $a = 3n+1$ et $b = 5n-1$.

1. Montrer que le pgcd(a,b) est un diviseur de 8.
2. Pour quelles valeurs de n, pgcd(a,b) est-il égal à 8 ?

Exercice 110. n est un entier relatif quelconque. On pose :

$$A = n-1 \text{ et } B = n^2-3n+6.$$

1. (a) Démontrer que le PGCD de A et de B est égal au PGCD de A et de 4.
   (b) Déterminer, selon les valeurs de l'entier n, le PGCD de A et de B.
2. Pour quelles valeurs de l'entier relatif n, $n \neq 1$,

   $\dfrac{n^2-3n+6}{n-1}$ est-il un entier relatif ?

Fiche 3

Congruences

Exercices

Exercice 111. Soit un entier naturel $n \geqslant 2$ et a, b des entiers relatifs vérifiant : $a \equiv b\ (n)$.
Démontrer, en vous appuyant sur les preuves du théorème de compatibilité, que : $\forall\ k \in \mathbb{N},\quad a^k \equiv b^k\ (n)$.

Exercice 112. Résoudre dans $\mathbb{Z}$ les systèmes suivants :

1. $\begin{cases} x \equiv -2\ (5) \\ x > 0 \end{cases}$ 2. $\begin{cases} x+2 \equiv -1\ (7) \\ 100 \leqslant x < 125 \end{cases}$

Exercice 113. Trouver les restes de la division euclidienne par 7 des nombres : $351^{12} \times 85^{15}$ et $16^{12} - 23^{12}$.

Exercice 114. Vérifier que $2^4 \equiv -1\ (17)$ et $6^2 \equiv 2\ (17)$.
Quel est le reste de la division par 17 des nombres $1\,532^{20}$ et 346^{12} ?

Exercice 115. Vérifier que 999 est divisible par 27, puis que $10^{3n} \equiv 1\ (27)$, avec $n \in \mathbb{N}$.
Quel est alors le reste dans la division de $10^{100} + 100^{10}$ par 27 ?

Exercice 116. Démontrer que pour tout entier naturel k, on a :
$5^{4k} - 1$ divisible par 13.

Exercice 117. Démontrer que pour tout entier naturel n,
$5^{2n} - 14^n$ est divisible par 11.

Exercice 118.
1. Quels sont les restes possibles de la division de 3^n par 11 ?
2. En déduire les entiers n pour lesquels $3^n + 7$ est divisible par 11.

Exercice 119. Démontrer que pour tout entier n, n^2 est congru soit à 0, soit à 1, soit à 4, modulo 8.
Résoudre alors dans $\mathbb{Z}$ l'équation :
$(n+3)^2 - 1 \equiv 0\ (8)$.

Exercice 120. Déterminer les restes de la division euclidienne de 5^n par 11 suivant les valeurs de n.
On donnera les résultats sous forme d'un tableau.

Exercice 121.
1. Compléter cette table des restes dans la congruence modulo 4.

$x \equiv$	0	1	2	3
$x^2 \equiv$				

2. Prouver que l'équation $7x^2 - 4y^2 = 1$, d'inconnues x et y entiers relatifs, n'a pas de solution.

3. Résoudre dans $\mathbb{Z}$ l'équation $(x+3)^2 \equiv 1 \pmod 4$.

Exercice 122. Déterminer les entiers n tels que $2^n - 1$ est divisible par 9.

Exercice 123.
1. Déterminer l'ensemble E_1, des entiers relatifs x tels que le nombre $n = x^2 + x - 2$ est divisible par 7.
2. Déterminer l'ensemble E_2 des entiers relatifs x tels que le nombre $n = x^2 + x - 2$ est divisible par 3.
3. k est un entier relatif.
   Vérifier que si, $x = 1 + 21k$ ou $x = -2 + 21k$, alors $n = x^2 + x - 2$ est divisible par 42.

Exercice 124. Déterminer le reste dans la division euclidienne de 11^{2011} par 7.

Exercice 125. Soit n un entier naturel, on sépare son nombre de dizaines a et le chiffre des unités b. On a alors : $n = 10a + b$.
1. Prouver que n est divisible par 17 si, et seulement si, $a - 5b$ est divisible par 17.
2. Montrer par ce procédé (que l'on peut réitérer) que les nombres : 816 et 16 983 sont divisibles par 17.

Exercice 126. On pose $A_n = n^5 - n$, $n \in \mathbb{N}$.
1. Montrer que A_n est pair.
2. Montrer que A_n est divisible par 3.
3. En utilisant les congruences modulo 5, démontrer que A_n est divisible par 5.
4. Pourquoi A_n est-il divisible par 30 ?

Fiche 4

Bézout

I. Algorithme d'Euclide et Théorème de Bézout

I.1. Sur un exemple

On sait que l'algorithme d'Euclide permet de trouver le pgcd noté d de deux nombres a et b entiers.
On va prouver qu'il existe des coefficients entiers relatifs u et v tels que $a \times u + b \times v = d$.
Considérons le cas de $a = 125$ et $b = 70$.
Écrivons chacune des étapes de l'algorithme d'Euclide :

$a = 125$	$b = 70$	$q_0 = 1$	$r_0 = 55$	$r_0 = 125 - 1 \times 70$
$b = 70$	$r_0 = 55$	$q_1 = 1$	$r_1 = 15$	$r_1 = 70 - 1 \times 55 = 70 - 1 \times (125 - 70) = 2 \times 70 - 1 \times 125$
$r_0 = 55$	$r_1 = 15$	$q_2 = 3$	$r_2 = 10$	$r_2 = 55 - 3 \times 15 = (125 - 70) - 3 \times (2 \times 70 - 125) = -7 \times 70 + 4 \times 125$
$r_1 = 15$	$r_2 = 10$	$q_3 = 1$	$r_3 = 5$	$r_3 = 15 - 1 \times 10 = 2 \times 70 - 1 \times 125 - (-7 \times 70 + 4 \times 125)$
				$= 9 \times 70 - 5 \times 125$
$r_2 = 10$	$r_3 = 5$	$q_4 = 2$	$r_4 = 0$	

En organisant ainsi l'algorithme d'Euclide, on peut conclure que :
le pgcd de 125 et 70 est 5 et on a déterminé deux nombres u et v tels que :
$125 \times u + 70 \times v = 5$ ($u = -5$ et $v = 9$).

I.2. Extension au cas général

Soit a et b deux nombres entiers avec $a > b$. Ecrivons l'algorithme d'Euclide, et supposons que le reste nul soit à l'étape $k+1$ et notons le $r_{k+1} = 0$. Alors le pgcd de a et b est le reste à l'étape k.
Posons $r_{-1} = b$ et $r_{-2} = a$
Posons $u_{-2} = 1$ et $v_{-2} = 0$
Posons $u_{-1} = 0$ et $v_{-1} = 1$
On a alors
$r_{-2} = a \times u_{-2} + b \times v_{-2}$
$r_{-1} = a \times u_{-1} + b \times v_{-1}$

Soit i un entier compris entre 0 et k supposons que :

$$r_{i-2} = u_{i-2} \times a + v_{i-2} \times b$$

$$r_{i-1} = u_{i-1} \times a + v_{i-1} \times b$$

alors

$$r_i = r_{i-2} - q_i \times r_{i-1}$$

alors

$$r_i = u_{i-2} \times a + v_{i-2} \times b - q_i \times (u_{i-1} \times a + v_{i-1} \times b)$$

alors

$$r_i = (u_{i-2} - q_i \times u_{i-1}) \times a + (v_{i-2} - q_i \times v_{i-1}) \times b$$

posons alors $u_i = u_{i-2} - q_i \times u_{i-1}$ et $v_i = v_{i-2} - q_i \times v_{i-1}$ et on peut écrire que :

$$r_i = u_i \times a + v_i \times b$$

L'égalité précédente écrite avec $i = k$ permet d'écrire que : le pgcd peut s'écrire comme combinaison linéaire de a et b et on dispose d'un algorithme permettant de trouver ces coefficients.

I.3. Présentation de l'algorithme d'Euclide étendu

On présente sous forme d'un tableau. Application avec a=777 et b=441.

a	b	r	q	U	V
				1	0
				0	1
777	441	336	1	1	-1
441	336	105	1	-1	2
336	105	21	3	4	-7
105	21	0			

On peut vérifier que $777 \times 4 + 441 \times (-7) = 21$

I.4. Le théorème de Bézout

Théorème 5
Soient a et b deux entiers naturels non simultanément nuls. Notons d leur PGCD. Alors il existe des entiers u et v tels que :

$$d = au + bv$$

En particulier,
a et b sont premiers entre eux si, et seulement si, il existe des entiers u et v tels que :

$$au + bv = 1$$

De tels coefficients u et v sont appelés des coefficients de Bézout.

Exercices

Exercice 127. Soit l'égalité de Bézout : « Soit a et b deux entiers non nuls et D leur PGCD. Il existe un couple d'entiers relatifs telle que $au+bv=D$ ».

1. Démontrer le théorème de Bézout « a et b sont premiers entre eux si, et seulement si, il existe un couple d'entiers relatifs $(u;v)$ tel que $au+bv=1$ ».
2. En déduire que si $\text{pgcd}(a;b)=D$, alors $a=Da'$ et $b=Db'$ avec $\text{pgcd}(a';b')=1$.

Exercice 128. Démontrer que, pour tout relatif k,
$(7k+3)$ et $(2k+1)$ sont premiers entre eux.

Exercice 129. n est un entier naturel , $a=7n+4$ et $b=5n+3$.
Montrer, pour tout n, que a et b sont premiers entre eux.

Exercice 130. Démontrer que pour tout relatif n, les entiers $(14n+3)$ et $(5n+1)$ sont premiers entre eux. En déduire $\text{pgcd}(87;31)$.

Exercice 131. Prouver que la fraction $\dfrac{n}{2n+1}$ est irréductible pour tout entier naturel n.

Exercice 132. Prouver que la fraction $\dfrac{2n+1}{n(n+1)}$ est irréductible pour tout entier naturel n.

Exercice 133. La fraction $\dfrac{n^3+n}{2n+1}$ est-elle irréductible pour tout entier naturel n ?

Exercice 134. Montrer que 17 et 40 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x;y)$ tel que : $17x-40y=1$.

Exercice 135. Montrer que 23 et 26 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x;y)$ tel que : $23x+26y=1$.

Exercice 136. L'équation $6x+3y=1$ admet-elle des solutions entières ? Et l'équation $7x+5y=1$?

Exercice 137. Montrer que 221 et 331 sont premiers entre eux puis déterminer un couple d'entiers relatifs $(x;y)$ tel que : $221x-331y=1$.

Exercice 138 — Vrai ou faux ? S'il existe deux entiers relatifs u et v tel que $au+bv=3$, alors le PGCD de a et de b est égal à 3. Justifier.

Fiche 5

Gauss-Équations Diophantiennes

I. Théorème de Gauss et son corollaire

Théorème 6
Soit a, b et c des entiers,
Si a divise bc et si a est premier avec b alors a divise c.

Théorème 7
Corollaire : Si deux entiers a et b premiers entre eux divisent l'entier c alors le produit ab divise c.

II. Résolution d'équations Diophantienne $ax+by=c$

II.1. Résolution de $2x-3y=5$

Déterminer tous les couples d'entiers (x,y) solutions de l'équation $2x-3y=5$.

- ⋆ Recherche d'un couple solution :
  Le couple $(1;-1)$ est un couple solution de l'équation. Notons le $(x_0;y_0)$
- ⋆ Supposons que (x,y) soit un couple d'entiers solution de l'équation, alors :

$$2x-3y=5$$

alors

$$2x-3y=2x_0-3y_0$$

alors

$$2x-2x_0=3y-3y_0$$

alors

$$2(x-x_0)=3(y-y_0)$$

alors 2 divise $3(y-y_0)$ or 2 et 3 sont premiers entre eux, donc D'après le théorème de Gauss, 2 divise $y-y_0$.
Il existe ainsi un entier k relatif tel que
$y-y_0=2k$. En remplaçant $y-y_0$ dans l'équation $2(x-x_0)=3(y-y_0)$, on obtient que $x-x_0=3k$.
Ainsi
si (x,y) est solution de $2x-3y=5$ alors il existe un entier k tel que $x=1+3k$ et $y=-1+2k$.
Réciproquement, si il existe k entier tel que $x=1+3k$ et $y=-1+2k$ alors $2x-3y=2+6k-(-3+6k)$ alors $2x-3y=5$.

⋆ Conclusion :

$$S = \{(1+3k, -1+2k); k \in \mathbb{Z}\}$$

III. Exercices

Exercice 139. En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs $(a;b)$ qui vérifient :

$$33a - 45b = 0.$$

Exercice 140.

1. En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs $(x;y)$ qui vérifient :
$$7(x-3) = 5(y-2).$$
2. De la question précédente, déterminer les entiers naturels x tels que : $7x \equiv 1\ (5)$.

Exercice 141. En utilisant le théorème de de Gauss, démontrer le corollaire du théorème de Gauss :« Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a ».

Exercice 142.

1. Montrer que si $n \equiv 0\ (8)$ et $n \equiv 0\ (9)$, alors $n \equiv 0\ (72)$.
2. Montrer que si $n \equiv 3\ (8)$ et $n \equiv 2\ (9)$, alors $n \equiv 11\ (72)$.
3. Montrer que si $n \equiv c\ (a)$ et $n \equiv d\ (b)$, avec a et b premiers entre eux alors $n \equiv cbv + dau\ (ab)$ où u et v sont les coefficients de Bezout associés à a et b $(au + bv = 1)$.
4. En déduire les entiers naturels n compris entre 100 et 200 tels que $n \equiv 3\ (13)$ et $n \equiv 2\ (11)$.

III.1. PPCM

Exercice 143. Soit deux entiers relatifs a et b.
On appelle ppcm$(a;b)$ le plus petit multiple strictement positif de a et de b.

1. Calculer ppcm$(18;12)$ et ppcm$(24\ ;\ 40)$.
2. Calculer $\dfrac{7}{6} + \dfrac{11}{15}$. Que représente ppcm$(6\ ;\ 15)$?

Exercice 144. On appelle $D = \text{pgcd}(a\ ;\ b)$ et
$M = \text{ppcm}(a\ ;\ b)$.

1. Montrer que si $a = Da'$ et $b = Db'$, alors $M = Da'b'$.
2. En déduire que : $D \times M = ab$.

Exercice 145. Soit a et b deux naturels tels que $a < b$.
En utilisant les propriétés de l'exercice , déterminer a et b tels que : pgcd$(a\ ;\ b) = 6$ et ppcm$(a\ ;\ b) = 102$.

III.2. Équation du type $ax + by = c$

Exercice 146. Soit l'identité de Bézout : « Soit a et b deux entiers non nuls et D leur PGCD. Il existe un couple d'entiers relatifs tel que $au + bv = D$ ».
Démontrer le corollaire du théorème de Bézout : « L'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple du pgcd$(a\ ;\ b)$ ».

Exercice 147. Soit l'équation (E) : $4x - 3y = 2$.

1. Déterminer une solution particulière entière à (E).

2. Déterminer l'ensemble des solutions entières.

Exercice 148. Soit l'équation (F) : $3x-4y=6$.

1. Déterminer une solution particulière entière à (F).
2. Déterminer l'ensemble des solutions entières.

Exercice 149. Soit l'équation (G) : $5x+8y=2$.

1. Déterminer une solution particulière entière à (G).
2. Déterminer l'ensemble des solutions entières.

Exercice 150. Soit l'équation $13x-23y=1$.

1. Déterminer une solution particulière entière, à l'aide de l'algorithme d'Euclide, à cette équation.
2. Déterminer l'ensemble des solutions entières.

Exercice 151.

1. Déterminer l'ensemble des couples $(x;y)$ des nombres entiers relatifs, solutions de l'équation :
$$\text{(E)} \ : \ 8x-5y=3.$$
2. Soit m un nombre entier relatif tel qu'il existe un couple $(p;q)$ de nombres entiers vérifiant : $m=8p+1$ et $m=5q+4$.
Montrer que le couple (p,q) est solution de l'équation (E).
3. Déterminer le plus petit de ces nombres entiers m supérieur à 2 000.

Exercice 152.

1. On considère l'équation (E) à résoudre dans $\mathbb{Z}$:
$$7x-5y=1.$$
   (a) Vérifier que le couple $(3\,;4)$ est solution de (E).
   (b) Montrer que le couple d'entiers $(x;y)$ est solution de (E) si, et seulement si, $7(x-3)=5(y-4)$.
   (c) Montrer que les solutions entières de l'équation (E) sont exactement les couples $(x;y)$ d'entiers relatifs tels que :
$$\begin{cases} x=5k+3 \\ y=7k+4 \end{cases} \text{ où } k\in\mathbb{Z}.$$
2. Une boîte contient 25 jetons, des rouges, des verts et des blancs. Sur les 25 jetons, il y a x jetons rouges et y jetons verts.
Sachant que $7x-5y=1$, quels peuvent être les nombres de jetons rouges, verts et blancs ?

Fiche 6

Nombres premiers-Génétalités

I. Définition et propriétés

I.1. Définition

Définition 4
Un **nombre premier** est un entier naturel qui admet exactement deux diviseurs **positifs** : 1 et lui-même.

Consequences

- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur).
- Un nombre premier p est un entier naturel supérieur ou égal à 2, soit **: $p \geqslant 2$.**
- 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 et 97.
- Si un entier naturel n n'est pas premier, il admet un diviseur d tel que : $2 \leq d < n$.

Remarque
Un entier naturel non premier est parfois appelé un **nombre composé**.

I.2. Critère d'arrêt ou test de primalité

Propriété 8 (Critère d'arrêt)
Tout entier naturel n, $n \geq 2$, admet un diviseur premier.
Si n n'est pas premier, alors il admet un diviseur premier p tel que : $2 \leq p \leq \sqrt{n}$.

Démonstration :
- Si n est premier, il admet un diviseur premier : lui-même.
- Si n n'est pas premier, l'ensemble D des diviseurs d de n tels que : $2 \leq d < n$ n'est pas vide. D'après le principe du bon ordre, il admet donc un plus petit élément p.
  Si p n'était pas premier, il admettrait un diviseur d' tel que $2 \leq d' < p$ qui diviserait aussi n. Ceci est impossible car p est le plus petit élément de D. Donc p est premier.
- On a donc p premier et $n = p \times q$ avec $p \leq q$. En multipliant cette inégalité par p, on obtient :

$$p^2 \leq pq \quad \Leftrightarrow \quad p^2 \leq n, \quad \text{soit} \quad p \leq \sqrt{n}$$

Exercice 153 — Montrer qu'un nombre est premier Pour montrer qu'un naturel n est premier, on utilise la contraposée du critère d'arrêt :
« Si n n'admet pas de diviseur premier p tel que $2 \leq p \leq \sqrt{n}$, alors n est premier. »

Montrer que 109 est un nombre premier.
correction On a $10 < \sqrt{109} < 11$. Donc si 109 n'est pas premier, il admet un diviseur premier inférieur à 11.
On teste tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.

- Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
- En effectuant la division euclidienne de 109 par 7, on obtient : $109 = 7 \times 15 + 4$.
  109 n'est donc pas divisible par 7.
- Conclusion : 109 n'est pas divisible par 2, 3, 5, et 7 donc 109 est premier.

Exemple
Le programme ci-dessous détermine si un nombre N est premier. N'ayant pas à notre disposition la liste des nombres premiers :

- on teste si N est divisible par 2 ;
- puis on teste les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieurs à $\sqrt{N}$.

On obtient alors pour les nombres 527, 719, 11 111 et 37 589 que :

- 527 est divisible par 17 ;
- 719 est premier ;
- 11 111 est divisible par 41 ;
- 37 589 est premier.

Exercices

Exercice 154. **methode-test primarite**
Sans calculatrice, à l'aide de divisions successives et du critère d'arrêt, déterminer si les entiers suivants sont premiers ou non.

97 ; 117 ; 271 ; 323 ; 401 ; 527 ; 719

Exercice 155. Montrer que 271 est premier. On expliquera clairement la méthode utilisée.

Fiche 7

Nombres premiers

.1. Infinité des nombres premiers

Propriété 9
Il existe une infinité de nombres premiers.

Démonstration : Cette preuve, par l'absurde ou par contradiction est celle proposée au III^{e} siècle av. J.-C., par Euclide, dans son ouvrage « *Les Éléments* ».
Il en existe bien évidemment d'autres.
Supposons qu'il existe un nombre fini n de nombres premiers : p_1, p_2,..., p_i, ..., p_n.
Soit N un nombre entier non premier, supérieur à 2, tel que :
$N = p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n + 1$.

D'après le critère d'arrêt, N admet un diviseur premier.
Soit p_i, $i \in \{1, 2, \ldots, n\}$, ce diviseur premier.
p_i divise donc $p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n$ et N.
Il divise donc la différence $N - (p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n) = 1$.
Ceci est impossible car $P_i \geq 2$, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est contradictoire. □

.2. Crible d'Ératosthène

Pour dresser la liste des nombres premiers inférieurs ou égaux à N :

— Écrire la liste des entiers de 2 à N.
D'après le critère d'arrêt, tous les nombres composés (non premiers) plus petits que N ont un facteur premier inférieur ou égal à $\sqrt{N}$.

— Éliminer de la liste tous les multiples de 2 sauf 2.
Le nombre suivant non éliminé est alors premier. Ici on trouve 3.

— Éliminer de la liste tous les multiples de 3 sauf 3.
Le nombre suivant non éliminé est alors premier. Ici on trouve 5.

— Réitérer l'étape ci-dessus tant qu'il existe des multiples de nombres premiers inférieurs ou égaux à $\sqrt{N}$.

Remarques

1. Pour éliminer les multiples de a supérieurs à a, commencer à a^2, car les multiples inférieurs à a ont déjà été éliminés. En effet, les multiples de a inférieurs à a^2 sont aussi des multiples de nombres inférieurs à a. Par exemple lorsqu'on élimine les multiples de 7, on commence à partir de 49.

2. Si $N = 150$, comme $\sqrt{150} \approx 12,25$, alors tout nombre composé sera éliminé en tant que multiple de 2, 3, 5, 7 et 11.

Exemple
Pour $N = 100$, on obtient le tableau suivant.

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

Remarque
On appelle fonction de compte des nombres premiers, la fonction notée $\pi(x)$ qui compte les nombres premiers inférieurs ou égaux à x.
On a par exemple : $\pi(100) = 25$, $\pi(200) = 46$, $\pi(500) = 95$, $\pi(1000) = 168$.

.3. Théorème de Gauss et nombres premiers

Propriété 10
Un nombre premier divise un produit de facteurs si, et seulement si, il divise l'un de ces facteurs.
Soit p un nombre premier et a, b deux entiers :

$$\text{Si } p \text{ divise } ab \quad \Leftrightarrow \quad p \text{ divise } a \text{ ou } p \text{ divise } b.$$

Démonstration : Comme p est premier, on a : $\text{pgcd}(p,a) = p$ ou $\text{pgcd}(p,a) = 1$.

— Si $\text{pgcd}(p,a) = p$, alors p divise a.

— Si $\text{pgcd}(p,a) = 1$, alors p et a sont premiers entre eux. D'après le théorème de Gauss (voir chapitre 2), p divise b. □

Remarque
En particulier, si p est premier et divise une puissance a^k, alors nécessairement p divise a. De cela découle que p^k divise a^k.

Consequences

— Si un nombre premier p divise un produit de facteurs premiers, alors p est l'un de ces facteurs premiers.

— Si un nombre n est un carré, alors toutes les puissances des facteurs de sa décomposition en facteurs premiers sont paires.

— Soit $p_1, p_2, \ldots, p_k$ des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots, \alpha_k$ des entiers naturels non nuls. Si, pour tout $i \in \{1, 2, \ldots, k\}$, $p_i^{\alpha_i}$ divise un entier n, alors le produit $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ divise aussi l'entier n.

Exercices

Exercice 156. Donner la liste des nombres premiers inférieurs à 50. Les nombres 577 et 689 sont-ils premiers ?

Exercice 157. p est premier et $p \geqslant 5$.

1. Démontrer que $p^2 - 1$ est divisible par 3.
2. Démontrer que $p^2 - 1$ est divisible par 8.
3. En déduire que $p^2 - 1$ est divisible par 24.

Exercice 158. Soit p soit un nombre premier tel que $p > 3$.

1. Quels sont les restes possibles dans la division de p par 12 ?
2. Prouver que $p^2 + 11$ est divisible par 12.

Exercice 159. Démontrer que pour tout n entier ($n \geqslant 1$), $30n + 7$ n'est jamais la somme de deux nombres premiers.

Exercice 160. Soit le nombre $N = 2n^2 + n - 10$ avec $n \in \mathbb{N}$.

1. Factoriser N.
2. Pour quelles valeurs de n, le nombre N est-il premier ?

Exercice 161 — Vrai ou faux ? Soit le nombre $N = 2n^2 + 7n + 6$ avec $n \in \mathbb{N}$.
La proposition suivante est-elle vraie ou fausse ?
Justifier.
« Il existe une valeur de n telle que N soit premier. »

Exercice 162. On considère un entier n tel que $n^2 = 17p + 1$, où p est premier.

1. Écrire $17p$ comme le produit de deux facteurs.
2. Citer le théorème de Gauss appliqué aux nombres premiers.
3. En déduire n, puis p.

Exercice 163. On considère un entier n tel que $n^2 = 29p + 1$, où p est premier.

1. Écrire $29p$ comme le produit de deux facteurs en fonction de n.
2. Citer le théorème de Gauss appliqué aux nombres premiers.
3. En déduire n, puis p.

Exercice 164. Est-il possible de trouver un nombre premier p tel que $p + 1\,000$ et $p + 2\,000$ soient aussi premiers ?
Aide : On pourra raisonner modulo 3, c'est-à-dire que l'on analysera successivement les cas $p \equiv 0$, $p \equiv 1$ et $p \equiv 2$ modulo 3.

Exercice 165 — [Nombres de Mersenne] On appelle nombres de Mersenne, les nombres M_n de la forme : $M_n = 2^n - 1$, avec $n \in \mathbb{N}^*$.

1. Calculer les six premiers nombres de Mersenne.
   Quels sont ceux qui sont des nombres premiers ?
2. Soit n un entier naturel non nul et a un entier.
   Montrer la factorisation standard :
   $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$.
3. En déduire que, si d est un diviseur de n, M_n est divisible par $2^d - 1$.
4. Montrer que, si M_n est premier, alors n est premier. La réciproque est-elle vraie ? (On pourra calculer M_{11}.)
5. Soit a et n deux entiers tels que : $a \geqslant 2$ et $n \geqslant 2$.
   Montrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.

Exercice 166 — Nombres de Fermat Soit n un entier naturel, on appelle nombre de Fermat le nombre F_n tel que : $F_n = 2^{2^n} + 1$.

1. Soit k un entier naturel non nul.
   (a) Montrer pour tout entier naturel x que :
   $$x^{2k+1} + 1 = (x+1)(x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1).$$
   (b) Montrer que si m est un entier naturel impair, $2^m + 1$ n'est pas premier.
   (c) Montrer que si m est un entier naturel qui possède un diviseur impair, $2^m + 1$ n'est pas premier.
   (d) En déduire que les seuls entiers naturels de la forme $2^m + 1$ sont les nombres de Fermat.
2. Calculer les cinq premiers nombres de Fermat :
   F_0, F_1, F_2, F_3 et F_4 puis vérifier qu'ils sont premiers.
3. Vérifier que pour tout entier naturel n :
   $F_{n+1} = (F_n - 1)^2 + 1$.
   En déduire $\text{pgcd}(F_n\,;\, F_{n+1})$.
4. Montrer que, pour tout entier naturel n tel que $n \geqslant 2$, $F_n \equiv 7\ (10)$.

Fiche 8

Nombres premiers

I. Décomposition, diviseurs d'un entier

I.1. Théorème fondamental de l'arithmétique

Théorème 8
Tout entier $n \geq 2$ peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers. Soit $p_1, p_2 \dots p_m$ des nombres entiers premiers distincts et $\alpha_1, \alpha_2, \dots \alpha_m$ des entiers naturels non nuls :

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

Exercice 167 — Décomposer un nombre en produit de facteurs premiers Décomposer 16 758 en produit de facteurs premiers.
Correction

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

On présente la décomposition avec une barre verticale où l'on écrit à droite, les diviseurs premiers et, à gauche, le quotient des divisions successives par ces diviseurs premiers pris dans l'ordre croissant.

On a donc $16\,758 = 2 \times 3^2 \times 7^2 \times 19$.

Démonstration : Soit n un entier naturel supérieur ou égal à 2.

— Si n est premier, alors n se décompose en lui-même.

Sinon $n = p_1 \times q_1$ avec $p_1 \leq q_1$ et p_1 premier car, d'après le critère d'arrêt, n admet un diviseur premier p_1 tel que $2 \leq p_1 \leq \sqrt{n}$.

— Si q_1 est premier, alors n se décompose en $n = p_1 \times q_1$.

Sinon $q_1 = p_2 \times q_2$ avec $p_2 \leq q_2$ et p_2 premier car, d'après le critère d'arrêt, q_1 admet un diviseur premier p_2 tel que $2 \leq p_2 \leq \sqrt{q_1}$. On a alors $q_2 < q_1$.

— Si q_2 est premier, alors n se décompose en $n = p_1 \times p_2 \times q_2$.

Sinon on réitère le processus, obtenant q_3, q_4, …, q_n avec $q_3 > q_4 > \cdots > q_n \geq 2$.
Toute suite strictement décroissante dans $\mathbb{N}$ est stationnaire à partir d'un certain rang n donc q_n est premier.

n se décompose en produit de facteurs premiers : $n = p_1 \times p_2 \times \cdots \times p_n \times q_n$.

Les facteurs premiers p_1, p_2, …, p_n et q_n peuvent être éventuellement identiques. On les regroupe alors sous la forme $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_m^{\alpha_m}$, avec $\alpha_1, \alpha_2, \ldots, \alpha_m$ des entiers naturels non nuls.

L'**existence** de la décomposition est alors démontrée. L'**unicité** de la décomposition est admise. □

Exercice 168 — Déterminer le PGCD de deux nombres à partir d'une décomposition en produit de facteurs premiers
Déterminer pgcd(126 ; 735) à l'aide d'une décomposition en produit de facteurs premiers.

Correction

— On décompose les deux nombres en produit de facteurs premiers.

126	2	735	3	On a donc :
63	3	245	5	$126 = 2 \times 3^2 \times 7$
21	3	49	7	$735 = 3 \times 5 \times 7^2$
7	7	7	7	
1		1		

— On détermine les facteurs premiers communs pour trouver le pgcd de ces deux nombres.

$$\text{pgcd}(126\ ;\ 735) = 3 \times 7 = 21.$$

Remarque

L'algorithme d'Euclide est à préférer pour la recherche du pgcd à la méthode par décomposition car il est plus économe en opérations :

$$735 = 126 \times 5 + 105$$
$$126 = 105 \times 1 + 21$$
$$105 = 21 \times 5$$

On obtient pgcd(735 ; 126) en trois étapes.

I.2. Diviseurs d'un entier

Propriété 11

Soit un nombre n ($n \geq 2$) dont la décomposition en produit de facteurs premiers est :

$$n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times \cdots \times p_m^{\alpha m}.$$

Alors tout diviseur d de n a pour décomposition :

$$d = p_1^{\beta 1} \times p_2^{\beta 2} \times \cdots \times p_m^{\beta m} \quad \text{avec } 0 \leq \beta_i \leq \alpha_i \text{ et } i \in \{1, 2, \ldots, m\}$$

Le nombre N de diviseurs est alors : $N = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_m + 1)$.

Remarques

— Le nombre de diviseurs d'un entier se calcule facilement car la puissance d'un facteur premier p_i peut varier de 0 à α_i, ce qui fait $(\alpha_i + 1)$ possibilités.

— Pour qu'un entier n admette un nombre impair de diviseurs, les $(\alpha_i + 1)$ doivent être impairs, donc toutes les puissances α_i doivent être paires. Le nombre n est alors un carré.

Exercice 169 — Trouver le nombre de diviseurs d'un entier Trouver le nombre de diviseurs de 120, puis déterminer tous ses diviseurs.

— On décompose 120 en facteurs premiers : $120 = 2^3 \times 3 \times 5$.

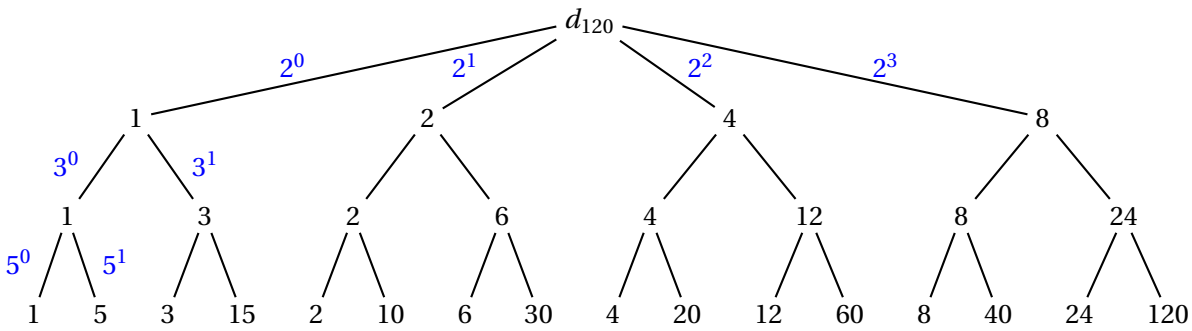
On alors : $(3+1)(1+1)(1+1) = 4 \times 2 \times 2 = 16$. Il y a 16 diviseurs pour 120.

— Pour déterminer tous ses diviseurs, on peut utiliser un tableau à double entrée en séparant les puissances de 2 et les puissances de 3 et 5. On obtient alors :

$\times$	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

Les 16 diviseurs de 120 sont donc : $D_{120} = \{1,2,3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$.

— On peut aussi utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles.



Exercice 170 — Déterminer un entier conditionné par ses diviseurs Un entier naturel n a 15 diviseurs. On sait de plus que n est divisible par 6 mais pas par 8. Déterminer cet entier n.**Correction**

— L'entier n a 15 diviseurs. Il faut donc connaître toutes les décompositions de 15 en facteurs supérieurs à 1. Il n'y a que deux décompositions possibles soit en un seul facteur 15, soit en deux facteurs 3×5.

— On sait que n est divisible par 6, il est donc divisible par 2 et par 3. Donc n admet au moins deux facteurs premiers. Comme 15 ne peut se décomposer en plus de deux facteurs, alors n ne peut admettre que deux facteurs premiers : 2 et 3. On a donc : $n = 2^\alpha 3^\beta$.

— Comme on a $15 = 3 \times 5$ diviseurs, alors : $(1+\alpha)(1+\beta) = 3 \times 5$.

— On trouve alors deux solutions : $\alpha = 2$ et $\beta = 4$ ou $\alpha = 4$ et $\beta = 2$.

— On sait de plus que n n'est pas divisible par $8 = 2^3$, donc α est inférieur à 3. n est donc :

$$n = 2^2 3^4 = 4 \times 81 = 324.$$

Exercice 171. Déterminer le plus petit entier naturel possédant 28 diviseurs.**Correction**

Soit n l'entier cherché.

Trouvons toutes les décompositions de 28 en produit de facteurs supérieurs à 1. On peut décomposer 28 en 1, 2 ou 3 facteurs : 28 ou 2×14 ou 4×7 ou $2\times 2\times 7$.

— En un facteur.
Le plus petit entier n est alors $n=2^{\alpha}$ avec $\alpha+1=28$, soit $\alpha=27$.
Donc $n=2^{27}=134\,217\,728$.

— En deux facteurs : $28=2\times 14$.
Le plus petit entier n est alors : $n=2^{\alpha}\times 3^{\beta}$ avec $\alpha+1=14$ et $\beta+1=2$.
On trouve : $\alpha=13$ et $\beta=1$, donc $n=2^{13}\times 3=24\,576$.

— En deux facteurs : $28=4\times 7$.
Le plus petit entier n est alors : $n=2^{\alpha}\times 3^{\beta}$ avec $\alpha+1=7$ et $\beta+1=4$.
On trouve : $\alpha=6$ et $\beta=3$, donc $n=2^{6}\times 3^{3}=1\,728$.

— En trois facteurs : $28=2\times 2\times 7$.
Le plus petit entier n est alors : $n=2^{\alpha}\times 3^{\beta}\times 5^{\gamma}$ avec $\alpha+1=7$, $\beta+1=2$ et $\gamma+1=2$.
On trouve : $\alpha=6$, $\beta=1$ et $\gamma=1$, donc $n=2^{6}\times 3\times 5=960$.

Conclusion, le plus petit entier naturel ayant 28 diviseurs est 960.

Exercices

Exercice 172 — methode-decomposition Décomposer 960 en produit de facteurs premiers. Quel est le nombre de diviseurs de 960 ?

Exercice 173. Décomposer en produit de facteurs premiers 221 122. Quel est le nombre de diviseurs de 221 122 ?

Exercice 174 — methode-pgcd
1. Déterminer le PGCD de 2 650 et 1 272 :
   (a) à l'aide de l'algorithme d'Euclide ;
   (b) à l'aide de la décomposition en produit de facteurs premiers de 2 650 et 1 272.
2. Quelle est la méthode la plus efficace ? Pourquoi ?

Exercice 175. Déterminer pgcd$(a\,;\,b)$ à l'aide d'une décomposition en facteurs premiers, puis à l'aide de l'algorithme d'Euclide des couples $(a\,;\,b)$ suivants :
1. $a=1\,188$ et $b=1\,485$
2. $a=3\,780$ et $b=3\,528$

Exercice 176.
1. Déterminer le PGCD de 428 904 et 306 360 :
   (a) à l'aide de l'algorithme d'Euclide ;
   (b) à l'aide de la décomposition en facteurs premiers de 428 904 et 306 360.
2. Quelle est la méthode la plus efficace ? Pourquoi ?

Exercice 177 — methode-diviseurs Décomposer 792 en produit de facteurs premiers. Quel est le nombre de diviseurs de 792 ? À l'aide d'un tableau ou d'un arbre déterminer tous les diviseurs de 792.

Exercice 178. Décomposer 8 316 en produit de facteurs premiers. Quel est le nombre de diviseur de 8 316 ?
À l'aide d'un tableau ou d'un arbre déterminer tous les diviseurs de 8 316.

Exercice 179. Trouver un nombre de trois chiffres qui soit un carré parfait divisible par 56.

Exercice 180.
1. Décomposer 2 016 en produit de facteurs premiers.
2. Déterminer, en expliquant la méthode choisie, la plus petite valeur de l'entier naturel k pour laquelle k^2 est un multiple de 2 016.

Exercice 181. Trouver tous les diviseurs de 84, puis résoudre dans $\mathbb{N}$ l'équation : $x(x+1)(2x+1) = 84$.

Exercice 182. Le produit de deux entiers naturels a et b ($a < b$) est 11 340. On note d leur pgcd.

1. (a) Pourquoi d^2 divise-t-il 11 340 ?
   (b) Pourquoi $d = 2^\alpha \times 3^\beta$,
   avec $0 \leqslant \alpha \leqslant 1$ et $0 \leqslant \beta \leqslant 2$?
2. On sait de plus que a et b ont six diviseurs communs et a est un multiple de 5.
   (a) Démontrer que $d = 18$.
   (b) En déduire a et b.

Exercice 183 — methode-conditions-diviseurs α et β sont deux entiers naturels et $n = 2^\alpha 3^\beta$.
Le nombre de diviseurs de n^2 est le triple du nombre de diviseurs de n.

1. Prouver que $(\alpha - 1)(\beta - 1) = 3$.
2. En déduire n.

Exercice 184. Un nombre n s'écrit $2^\alpha 3^\beta$ où α et β sont deux entiers naturels. Le nombre de diviseurs de $12n$ est le double du nombre de diviseurs de n.

1. Montrer que l'on a : $\beta(\alpha - 1) = 4$.
2. En déduire les trois valeurs possibles pour n.

Exercice 185. Un entier n a 5 diviseurs et $n - 16$ est le produit de deux nombres premiers.

1. Prouver que $n = p^4$, avec p premier.
2. Écrire $n - 16$ sous forme d'un produit de trois facteurs dépendant de p.
3. En déduire la valeur de n.

Exercice 186. Un détaillant de matériel audiovisuel effectue trois remises successives sur un article qui coûtait 300 € et qu'il vend 222,87 €.
Quels sont les pourcentages (nombres entiers) des trois remises ?

Exercice 187 — Les zéros de 1 000 ! L'exercice a pour but de déterminer par combien de zéros se termine le nombre 1 000 ! (factorielle mille et non « mille points d'exclamation »)

On rappelle que : $1\,000! = 1 \times 2 \times 3 \times \cdots \times 1\,000$.

1. Montrer qu'il existe des entiers p et q ($p \geqslant 1$ et $q \geqslant 1$) et un entier N premier avec 10 tels que :

$$1\,000! = 2^p \times 5^q \times N.$$

2. On justifiera clairement les questions suivantes :
   (a) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5 ?

(b) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5^2 ?

(c) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5^3 ?

(d) Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisibles par 5^4 ?

(e) En déduire alors que $q = 249$.

3. Établir que $p > q$ et que le nombre cherché est q.

Exercice 188 — Triplets pythagoriciens Soit p un nombre premier donné. On se propose d'étudier l'existence de couples $(x; y)$ d'entiers naturels strictement positifs vérifiant l'équation :

$$\text{(E)} \quad x^2 + y^2 = p^2.$$

1. On pose $p = 2$. Montrer que l'équation (E) est sans solution.
2. On suppose désormais que $p \neq 2$ et que le couple $(x; y)$ est solution de l'équation (E). Le but des questions suivantes est de prouver que x et y sont premiers entre eux.
   (a) Montrer que x et y sont de parités différentes.
   (b) Montrer que x et y ne sont pas divisibles par p.
   (c) En déduire que x et y sont premiers entre eux.
3. On suppose maintenant que p est une somme de deux carrés non nuls, c'est-à-dire que :
   $p = u^2 + v^2$,
   où u et v sont deux entiers naturels strictement positifs.
   (a) Vérifier que le couple $\left(\left|u^2 - v^2\right| ; 2uv\right)$ est solution de (E).
   (b) Donner une solution de l'équation (E) lorsque : $p = 5$, puis lorsque $p = 13$.
4. On se propose enfin de vérifier, sur deux exemples, que l'équation (E) est impossible lorsque p n'est pas la somme de deux carrés.
   (a) $p = 3$ et $p = 7$ sont-ils la somme de deux carrés ?
   (b) Démontrer que les équations :
   $x^2 + y^2 = 9$ et $x^2 + y^2 = 49$ n'admettent pas de couples solutions d'entiers strictement positifs.

Exercice 189 — Théorème d'Euclide On appelle nombre parfait un nombre dont la somme des diviseurs stricts est égal à lui-même.

1. Euclide donne la règle suivante pour trouver des nombres parfaits :
   « Si un nombre a s'écrit $2^n(2^{n+1} - 1)$ et si $2^{n+1} - 1$ est premier, alors a est parfait ».
   Exemples : Trouver les quatre premiers nombres parfaits.
2. **Démonstration**. On pose $a = 2^n(2^{n+1} - 1)$ et supposons que $2^{n+1} - 1$ est premier.
   (a) Quelle est la décomposition de a en produit de facteurs premiers ?
   (b) En déduire la liste des diviseurs de a.
   (c) Démontrer alors que la somme des diviseurs stricts est égale à ce nombre a.

Fiche 9

Nombres premiers

I. Le Petit Théorème de Fermat

I.1. Lemme

Définition 5
Une solution x_0 d'une congruence $f(x) \equiv 0$ modulo n est dite essentiellement unique si toutes les solutions sont congrues (modulo n) à x_0.

Théorème 9
Une condition nécessaire et suffisante pour qu'une congruence $ax \equiv b$ (modulo n) admette une solution essentiellement unique est que les entiers a et n soient premiers entre eux.

C'est le cas par exemple lorsque n est premier et qu'il ne divise pas a.

Démonstration :

- Si le PGCD d de a et n n'est pas égal à 1, on peut associer à une éventuelle solution x une autre solution $x' \equiv x$ définie par $x' = x + \frac{n}{d}$, puisqu'alors $ax' = ax + \frac{a}{d}n$. Il ne peut donc pas alors y avoir unicité essentielle d'éventuelles solutions, il se peut d'ailleurs qu'il n'y en ait aucune, comme dans le cas $4.x \equiv 1 \pmod 6$.
- Si le PGCD est égal à 1 alors le théorème de Bézout assure l'existence de (u, v) tel que $au + bv = 1$, ce qui conduit à la solution $x = bu$ puisqu'alors $ax = (au)b = b - b(vn)$. toute autre solution x' est telle que $n|a(x' - x)$ et le théorème de Gauss montre alors n divise $x' - x$, c'est à dire qu'il existe un entier k vérifiant $x' = x + kn$, c'est à dire encore que x et x' sont congrus modulo n. □

I.2. Son énoncé

Théorème 10
Pour tout couple d'entiers relatifs (a, p) tel que p soit un nombre premier, $a^p \equiv a \pmod p$.

Démonstration : Première preuve : Le résultat est clair si p divise a. Envisageons le cas où p ne divise par a. Notons $f(x)$ le reste modulo p du produit ax où x décrit l'ensemble $\{1, 2, ..., p-1\}$. On sait d'après le lemme que l'équation $f(x) = b$ a une solution unique lorsque b décrit également l'ensemble $\{1, 2, ..., p-1\}$. Le produit de ces solutions et le produit des nombres $f(x)$ sont tousles deux égaux à $(p-1)!$ puisqu'un produit ne dépend pas de l'ordre de ses facteurs.
Or le produit des $f(x)$ est congru modulo p au produit des nombres ax, donc à $a^{p-1}(p-1)!$. Il en

résulte que p divise $[a^{p-1}-1](p-1)!$ et à fortiori $[a^p-a](p-1)!$. Comme le nombre p est premier avec chacun des entiers 1, 2, ...,$p-1$, il est premier avec leur produit et le théorème de Gauss permet de conclure. □

Démonstration : Deuxième preuve :en exercice. □

Propriété 12
Pour tout couple d'entiers relatifs (a, p) tel que p soit un nombre premier et ne divise pas a, $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration : On sait que p divise a^p-a or $a^p-a = a^{p-1}(a-1)$. Le théorème de gauss permet de conclure si p ne divise pas a, ce qui signifie qu'il est premier avec a. □

Applications cryptographiques

La méthode RSA

La méthode RSA fut mise au point une première fois,mais restée secrète, par James Ellis et Clifford Cocks le 20 novembre 1973, et retrouvée indépendamment et publiée le 4 avril 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. (Texte issu du livre arithmétique dirigé par André Warusfel en 2002.)

Exercices préparatoires

1. Démontrer que pour tout triplet (t, p, q) d'entiers relatifs où p et q sont deux entiers premiers distincts ne divisant pas t, on a $t^{(p-1)(q-1)} \equiv 1$ modulo pq.
2. Démontrer que sous les hypothèses de la question précédente, si e est un entier premier avec $(p-1)(q-1)$ alors il existe un entier d tel qu'il existe un entier ℓ vérifiant l'égalité $e.d = 1+\ell(p-1)(q-1)$.
3. Démontrer que sous les hypothèse précédentes on dispose de la congruence $(t^e)^d \equiv t$ (modulo pq)

« De ces propriétés résulte la technique RSA. Soit t un texte, c'est à dire un entier représentant une certaine information à transmette secrètement à un récipiendaire R (par exemple ce texte est numérisé en remplaçant chaque lettre de l'information par un nombre compris entre 00- le blanc- et 26- le Z). pour simplifier, on supposera que 0<t<pq. Le nombres p et q sont connus et tenus secrets par R, mais leur produit $n = pq$ et l'entier e, servant à l'encryption, sont publics. l'expéditeur peut donc calculer le message $m = t^e$ (modulo n) qu'il envoie à R, message illisible pour qui ne connaît que m, e, et n. Par contre, il devient lisible par R, qui connaissant la décomposition $n = pq$ et donc le module $(p-1)(q-1)$, e eu tout le temps de son côté de calculer l'entier d grâce auquel il peut procéder au décryptage, puisque t est congru à m^d modulo n. Toute la force du système résulte sur la quasi impossibilité de résoudre la congruence $t^e \equiv m$ oùt est l'inconnue (c'est le problème du logarithme discret) et de pouvoir décomposer n, ce qui est le cas pour l'instant si n possède plusieurs centaines de chiffres. » Texte écrit en 2002.
Le chiffrement RSA est complété par une procédure de signature qui est construite de façon analogue. Si l'expéditeur veut persuader le récipiendaire R qu'il est bien l'auteur du texte t et s'il a rendu auparavant publics des entiers n' et e' et calculé d' il n'a qu'à construire le texte τ contenant par exemple son nom et son adresse, et à envoyer $\mu \equiv \tau^{d'}$ à R. ce dernier en calculant $\mu^{e'}$ a ainsi la preuve que l'expéditeur est l'auteur du texte.

Exercices

Exercice 190.

1. si p est premier et a et b entiers quelconques, démontrer que $(a+b)^p \equiv a^p + b^p$ modulo p
2. En déduire par récurrence sur n le petit théorème de Fermat.

Exercice 191. Démontrer que pour tout coupe (p,q) d'entiers premiers supérieurs ou égaux à 11, on dispose de la congruence $(p^2-1)(q^2-1)(p^6-q^6) \equiv 0$ modulo (2 903 040).

Fiche 10

Divers

Exercice 192. Résoudre l'équation dans $\mathbb{N}$, $x^2 = yz$.

Exercice 193. Résoudre l'équation dans $\mathbb{N}$, $x^2 + y^2 = z^2$. (Triplets Pythagoriciens)

Exercice 194. Démontrer que le cercle d'équation $x^2 + y^2 = 3$ n a pas de point dont les coordonnées sont rationnelles.

Exercice 195. Montrer que si n est un entier naturel somme de deux carrés d'entiers alors le reste de la division euclidienne de n par 4 n'est jamais égal à 3.

Exercice 196. Montrer que si r et s sont deux nombres entiers naturels somme de deux carrés d ?entiers alors il en est de même pour le produit rs.