2013-2014

Les cours du Lycée J. Durand

Mathématiques

Terminale S

Enseignement de spécialité

Rédaction :

David Zancanaro

Réalisé à l'aide de :

LaTeX

Table des matières

Leçon 2

Arithmétiques et problèmes de codage, partie 2

LSB \ MSB	8 1000	9 1001	A 1010	B 1011	C 1100	D 1101	E 1110	F 1111
0 0000	Ç	É	á	▒	└	ð	Ó	-
1 0001	ü	æ	í	▓	┴	Ð		±
2 0010	é	Æ	ó	▓	┬	Ê	ô	_
3 0011	â	ô	ú	┃	├	Ë	ò	¾
4 0100	ä	ö	ñ	┤	─	È	ő	¶
5 0101	à	ò	Ñ	Á	┼	I	Ő	§
6 0110	å	û	ª	Â	ã	í	µ	÷
7 0111	ç	ù	º	À	Ã	î	þ	¸
8 1000	ê	ÿ	¿	©	╚	ï	Þ	°
9 1001	ë	Ö	®	╣	╔	┘	Ú	¨
A 1010	è	Ü	¬	║	╩	┌	Û	·
B 1011	ï	ø	½	╗	╦	█	Ù	¹
C 1100	î	£	¼	╝	╠	▄	ý	³
D 1101	ì	Ø	¡	¢	=	¦	Ý	²
E 1110	Ä	×	«	¥	╬	Ì	¯	■
F 1111	Å	ƒ	»	┐	¤	▀	´	

I. Nombres premiers

I.1. Généralité

Rappelons que :

Définition 1.

On dit qu'un entier naturel p est premier s'il possède exactement 2 diviseurs positifs : 1 et lui-même.

Exemples :

- 0 n'est pas premier car il admet une infinité de diviseurs
- 1 n'est pas premier car il n'admet qu'*un seul* diviseur : lui-même.
- 2 est le seul nombre premier pair (les autres sont divisibles au moins par 1, eux-mêmes et 2).
- 3, 5, 7, 11, 13 sont des nombres premiers.
- 6 n'est pas un nombre premier, car il est divisible par 1, 6, 2 et 3.

Théorème 1.

Soit $n \in \mathbb{N}$ supérieur ou égal à 2. Alors :

- n admet au moins un diviseur premier
- Si n n'est pas premier, alors il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.

Preuve

- Si n est premier, alors il s'admet lui-même comme diviseur premier.
  Sinon, n admet au moins un diviseur propre c'est-à-dire un diviseur p tel que $1 < p < n$.
  Considérons l'ensemble E des diviseurs propres de n, cet ensemble est fini, non vide et contient au maximum $n-2$ éléments compris entre 1 et n. Il admet donc un plus petit élément, disons p_0.
  Si p_0 n'est pas un nombre premier, alors il admet au moins un diviseur d tel que $1 < d < p_0$.
  Cependant si d divise p_0 qui divise n alors d divise n. C'est-à-dire d est un diviseur propre de n strictement inférieur au plus petit diviseur propre de n, ce qui est absurde...
  Par conséquent p_0 est premier ce qui prouve que n admet un diviseur premier.
- Puisque n n'est pas premier, il admet un diviseur premier, notons le p. Puisque $p|n$ il existe un entier naturel k tel que $n = pk$. Si $p \leq \sqrt{n}$ alors le théorème est démontré.
  Si $p > \sqrt{n}$ alors $k < \sqrt{n}$ car dans le cas contraire on aurait :

$$pk > \sqrt{n} \times \sqrt{n} = n$$

  Si k est un nombre premier alors le théorème est démontré.
  Si k n'est pas un nombre premier alors il admet au moins un diviseur premier $p_0 < k < \sqrt{n}$, ce nombre p_0 divise k qui divise n, donc p_0 est un nombre premier inférieur ou égal à $\sqrt{n}$ qui divise n, ce qui prouve le théorème.

Corollaire 1.

Soit $n \in \mathbb{N}$ supérieur ou égal à 2. Alors si n n'admet aucun diviseur inférieur ou égal à sa racine carré, alors n est premier

Preuve

C'est la contraposée du théorème.

Exercice 1. 317 est-il un nombre premier ? Répondre sans utiliser de calculatrice.

Exercice 2. Montrer que si p est premier si p divise a^2 alors p divise a. [1]

I.2. Infinité des nombres premiers

Théorème 2.

Il existe une infinité de nombres premiers.

1. *Lemme d'euclide* : Si un nombre premier p divise le produit ab alors il divise a ou il divise b.

Preuve

Supposons qu'il existe un nombre fini n de nombres premiers, notés p_1, p_2, …, p_n. On pose $N = p_1 \times p_2 \times \cdots \times p_n + 1$.
Puisque $N < p_n$, N n'est pas premier, donc il admet un certain diviseur premier k. Nous connaissons l'ensemble des nombres premiers donc k est un des p_i c'est-à-dire il existe i entre 1 et n tel que $k = p_i$.
De plus $k|p_1 p_2 \ldots p_n$ et $k|N$ donc $k|1$ (la différence). Donc $k = 1$ ce qui est absurde puisque k est un nombre premier. Par conséquent il est absurde de supposer qu'il existe un nombre fini de nombres premiers.
On en conclut qu'il existe une infinité de nombres premiers.

I.3. Décomposition en nombres premiers

Théorème 3.

Tout entier naturel $n \geq 2$ peut s'écrire comme le produit de nombres premiers c'est-à-dire il existe k nombres premiers $p_1 < p_2 < \cdots < p_k$ et k entiers naturels $\alpha_1, \alpha_2, \ldots, \alpha_k$ tels que :

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

Une telle décomposition est unique.

Exercice 3. Décomposer 9510 en produit de facteurs premiers puis en déduire l'ensemble des diviseurs positifs de 9510.

Exercice 4. On considère la suite (u_n) définie pour tout entier naturel n par $u_n = \overline{11\ldots1}$, nombre qui s'écrit avec n fois le chiffre 1.

1. Quels sont les nombres premiers parmi u_2, u_3, …, u_6 ?
2. Montrer que si n est multiple de 3, alors u_n admet 111 comme diviseur et n'est donc pas premier.
3. (a) Montrer que, pour tout entier naturel n on a :

$$u_n = \frac{10^n - 1}{9}$$

   (b) Montrer que pour tout $x \in \mathbb{R}$ on a :

$$x^n - 1 = (1 + x + x^2 + \cdots + x^{n-1}(x - 1)$$

   (c) En déduire que, si n n'est pas premier alors u_n n'est pas premier.
   Indication : On montrera que u_n est un multiple de u_p où p est un diviseur de n.

Exercice 5. Soit p un nombre premier et l'équation (E) : $x^2 - y^2 = p$.

1. Démontrer si x et y sont des entiers naturels solutions de (E), alors ils sont consécutifs.
2. En déduire tous les couples d'entiers naturels solutions de (E).
3. Déterminer tous les couples d'entiers naturels solutions de (E′) : $x^2 - y^2 = p^2$.

Preuve

Existence :

Si n est un nombre premier alors le théorème est valable trivialement.

Sinon, si n n'est pas un nombre premier il existe au moins un nombre premier p qui divise n. Notons p_1 le plus petit d'entre eux. On peut donc écrire $n = p_1 \times n_1$ avec $n_1 < n$. On réitère le même raisonnement avec n_1 qui, s'il n'est pas premier admet au moins diviseur premier p. En notant p_2 le plus petit d'entre eux (p_2 est alors aussi un diviseur de n donc $p_1 \leq p_2$). On obtient alors :

$$n = p_1 p_2 n_2$$

avec $1 \leq n_2 < n_1 < n$. Si $n_2 = 1$ alors n_1 est premier et le résultat est démontré. Sinon on réitère le raisonnement tant que le quotient est différent de 1.

La liste des quotients est une liste décroissante d'entiers naturels, elle admet donc un plus petit élément n_k et est finie. On a alors $n = p_1 p_2 \dots p_k$

Comme certains p_i peuvent être égaux il existe des entiers naturels $\alpha_1, \alpha_2, \dots, \alpha_k$ tels que :

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

Unicité : Supposons que n admettent deux décompositions en facteurs premiers différentes, cela peut se traduire de deux manières :

- soit les nombres premiers intervenant dans les deux décompositions ne sont pas tous identiques.
- soit les nombres premiers intervenant dans les deux décompositions sont identiques et ce sont les puissances qui diffèrent.

Dans le premier cas, supposons donc que n se décompose en utilisant le nombre premier p d'une part et sans l'utiliser d'autre part. p est donc un diviseur de n. n admet une décomposition en facteurs premiers ne faisant pas intervenir p de la forme :

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

p divise par exemple le produit $p_1 \times k$ avec $k = p_1^{\alpha_1 - 1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$ donc d'après le lemme d'euclide il divise soit p_1 soit k. En réitérant ce raisonnement il vient que p divise un nombre premier différent de lui-même ce qui est absurde.

Dans le second cas, seule les puissances diffèrent. n admet donc deux décompositions de la forme :

$$n = p^{\alpha} \times k = p^{\beta} \times k' \qquad \text{avec } \alpha < \beta$$

Ainsi :

$$\frac{n}{p^{\alpha}} = k = p^{\beta - \alpha} k'$$

p divise $p^{\beta-\alpha}k'$ donc p divise k qui est un produit de nombre premiers tous différents de p, on est ramené au premier cas.

Par conséquent un nombre ne peut pas admettre deux décompositions en produit de facteurs premiers différentes.

Exemples :

On utilise les critères de divisibilité. $105 = 3 \times 5 \times 7$; $83160 = 2^3 \times 3^3 \times 5 \times 7 \times 11$.

Théorème 4.

Soit n un entier naturel supérieur ou égal à 2 se décomposant en produit de facteurs premiers sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
Les diviseurs positifs de n sont les nombres de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq k$.

Preuve

Il est clair que les nombres de cette forme divisent n car $\alpha_i - \beta_i \geq 0$ pour tout $1 \leq i \leq k$.
Démontrons maintenant que tout diviseur de n est de cette forme.
Soit d un diviseur de n. Alors il existe un entier d' tel que $n = d \times d'$. Le produit des décompositions en facteurs premiers de d et d' est une décomposition en produit de facteurs premiers de n.
Comme elle est unique, c'est la même.
Les seuls diviseurs premiers intervenant dans les décompositions de d et d' sont donc les p_i et leur exposant ne peuvent être qu'inférieurs ou égaux aux α_i.
L'entier d est donc forcément de la forme indiquée.

Corollaire 2.

Soit un entier $n \leq 2$ se décomposant en produit de facteurs premiers sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
Alors, n possède $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1)$ diviseurs positifs.

Preuve

Dénombrement. Un arbre de probabilité permet assez rapidement de se convaincre.

Exercice 6.

1. Indiquer pour chacun des nombres suivants s'il est premier : 481, 483, 485, 487.
2. Pour quelles valeurs du nombre entier n, le nombre suivant est-il premier ?
   (a) $n^2 - 8n + 15$
   (b) $n^2 + 4n + 3$. *Essayer de factoriser ces polynômes.*
3. Pour quelles valeurs des nombres entiers naturels n et m le nombre $2n^2 + 5nm + 3m^2$ est-il premier ?
   Indication : On montrera que $2n^2 + 5nm + 3m^2 = (n + m)(2n + 3m)$
4. Factoriser $n^4 + 4$ en partant de $n^4 + 4 = (n^2 + 2)^2 - 4n^2$. Pour quelles valeurs entières de n l'entier $n^4 + 4$ est-il premier ?
5. Si p est un nombre premier et n un entier naturel non nul. Montrer que deux cas seulement peuvent se présenter :
   – soit p divise n ;
   – soit p et n sont premiers entre eux, c'est-à-dire ils ont pour plus grand diviseur 1.

6. Deux nombres premiers sont dits jumeaux si leur différence est égale à 2. Pour vérifier que 1607 et 1609 sont des nombres premiers jumeaux, par quels nombres premiers faut-il vérifier qu'ils ne sont pas divisibles ?
   Les nombres $33218925 \times 2^{169690} \pm 1$ sont deux nombres premiers jumeaux de plus de 50000 chiffres (découverts en 2002). On ne sait toujours pas s'il existe une infinité de nombres premiers jumeaux.

Exercice 7. Le but de l'exercice est de montrer qu'il existe une infinité de nombres premiers de la forme $6k+5$ où $k \in \mathbb{N}$.

1. (a) Déterminer six nombres premiers de cette forme.
   (b) Déterminer six nombres composés de cette forme.
2. Montrer que tout nombre premier, autre que 2 et 3 est de la forme $6k+1$ ou $6k+5$, où $k \in \mathbb{N}$.
3. On suppose qu'il existe un nombre fini de nombres premiers de la forme $6k+5$ que l'on nomme $p_1, p_2, \ldots, p_n$.
   On considère le nombre
   $$N = 6p_1 p_2 \ldots p_n - 1$$
   (a) Justifier que $N \equiv -1\,[6]$.
   (b) En déduire que N est de la forme $6k+5$ puis qu'il ne peut être premier.
   (c) Montrer qu'aucun des nombres $p_1, p_2, \ldots, p_n$ ne divisent N et en déduire que les diviseurs premiers de N sont de la forme $6k+1$.
   (d) Montrer que $N \equiv 1\,[6]$.
4. Conclure.

Exercice 8. Antilles-Guyanne, Juin 2005 (5 points)

1. (a) Déterminer suivant les valeurs de l'entier naturel non nul n le reste dans la division euclidienne par 9 de 7^n.
   (b) Démontrer alors que $2005^{2005} \equiv 7\,[9]$
2. (a) Démontrer que pour tout entier naturel non nul n : $10^n \equiv 1\,[9]$
   (b) On désigne par N un entier naturel écrit en base 10, on appelle S la somme de ses chiffres. Démontrer la relation suivante : $N \equiv S\,[9]$
   (c) En déduire que N est divisible par 9 si et seulement si S est divisible par 9.
3. On suppose que $A = 2005^{2005}$; on désigne par :
   – B la somme des chiffres de A
   – C la somme des chiffres de B
   – D la somme des chiffres de C
   (a) Démontrer la relation suivante : $A \equiv D\,[9]$
   (b) Sachant que $2005 < 10000$, démontrer que A s'écrit en numération décimale avec au plus 8020 chiffres.
   En déduire que $B \leq 72180$.
   (c) Démontrer que $C \leq 45$
   (d) En étudiant la liste des entiers inférieurs à 45, déterminer un majorant de D plus petit que 15.
   (e) Montrer que $D = 7$.

I.4. Questions diverses sur les nombres premiers

I.4.a. Les nombres de Carmichaël

Définition 2.

Un entier $n \geq 3$ est un nombre de Carmichaël si et seulement si :

1. il est le produit d'au moins trois nombres premiers impairs ;
2. il est tel que, pour chaque diviseur premier p de n, l'entier $p-1$ divise $n-1$

Exercice 9.

1. 30 et 561 sont-ils des nombres de Carmichaël ?
2. Les nombres premiers sont-ils des nombres de Carmichaël ?
3. Décomposer 1729 puis 2695 en produit de facteurs premiers.
4. 1729 et 2695 sont-ils des nombres de Carmichaël ?

Remarque : Le petit théorème de Fermat énonce que les nombres premiers ont la propriété $\mathscr{P}$: si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1}-1$ est un multiple de p. ». Autrement dit, sous les mêmes conditions sur a et p :. Sa réciproque est fausse, les nombres de Carmichael sont les nombres positifs qui satisfont à $\mathscr{P}$ sans être premiers, ce sont des menteurs de Fermat ; l'existence de tels nombres pseudo-premiers absolus est ce qui empêche d'utiliser le test de primalité de Fermat pour prouver qu'un nombre est premier. Plus les nombres deviennent grands et plus les nombres de Carmichael deviennent rares, la majorité d'entre eux rendent le test de primalité de Fermat largement inutile comparé aux autres tests de primalité comme le test de primalité de Solovay-Strassen. Par exemple, le 646e nombre de Carmichael vaut 993905641 et il existe 105212 nombres de Carmichael entre 1 et 10^{15}.

I.4.b. Les nombres parfaits

Exercice 10. Nombre parfaits ♠♠♠

Définition : Dire qu'un entier naturel n est parfait signifie que la somme de tous ses diviseurs positifs est égale à $2n$.

1. Montrer que :
$$\forall x \neq 1, \qquad \sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$$
Indication : On pourra calculer $(1-x)\sum_{i=0}^{n} x^i$.
2. Démontrer que 28 est un nombre parfait.
3. p désigne un nombre premier tel que $q = 2^p - 1$ soit premier.
   (a) Déterminer les diviseurs positifs de 2^{p-1}.
   (b) Déterminer les diviseurs positifs de $2^p - 1$.
   (c) Calculer la somme des diviseurs positifs de l'entier $\mathrm{E}^p = 2^{p-1}(2^p-1)$.
   Remarque : Les nombres E_p sont appelés *nombres d'Euclide.*

(d) En déduire que $2^{p-1}(2^p-1)$ est un nombre parfait.

(e) Déterminer alors trois nombres parfaits.

4. ♠♠♠♠♠

p et q désignent des nombres premiers distincts supérieurs ou égaux à 3 et α et β sont des entiers naturels non nuls ; on note $n = p^\alpha q^\beta$.

(a) Déterminer les diviseurs positifs de p^α et de q^β.

(b) Démontrer que la somme S des diviseurs positifs de n est donnée par :

$$S = \frac{p^{\alpha+1}-1}{p-1} \times \frac{q^{\beta+1}-1}{q-1}$$

(c) Démontrer que n est parfait, si et seulement si $p^\alpha q^\beta\left((p-2)(q-2)-2\right) = 1-p^{\alpha+1}-q^{\beta+1}$.

(d) En étudiant le signe de chaque membre, démontrer qu'il ne peut pas exister de nombres parfaits impairs dont la décomposition en produit de facteurs premiers ne contienne que deux facteurs premiers distincts.

(e) Démontrer que s'il existe un nombre parfait impair, il est supérieur à 105.
Remarque : On ignore, à l'heure actuelle, s'il existe des nombres parfaits impairs.

I.4.c. Les nombres de Fermat

Un nombre de Fermat est un entier naturel qui peut s'écrire sous la forme $2^{2^n}+1$, avec n entier. Le n-ème nombre de Fermat, $2^{2^n}+1$, est noté F_n.

Ces nombres doivent leur nom au mathématicien français Pierre de Fermat (1601-1665) qui émit la conjecture que tous ces nombres étaient premiers. Cette conjecture se révéla fausse, F_5 étant composé, de même que tous les nombres de Fermat jusqu'à F_{32}. On ne sait pas si les nombres à partir de F_{33} sont premiers ou composés. Les seuls nombres de Fermat premiers connus sont donc F_0, F_1, F_2, F_3 et F_4.

Ces nombres disposent de propriétés intéressantes, en général issues de l'arithmétique modulaire ; en particulier, Carl Friedrich Gauss a établi un lien entre ces nombres et la construction à la règle et au compas des polygones réguliers : un polygone régulier à n côtés peut être construit à la règle et au compas si et seulement si n est une puissance de 2, ou le produit d'une puissance de 2 et de nombres de Fermat premiers distincts.

II. PGCD - PPCM

Soient a et b deux entiers non tous les deux nuls. On notera $\mathscr{D}(a,b)$ l'ensemble de leurs diviseurs communs.

II.1. Généralité

Définition 3. (et Propriété)

$\mathscr{D}(a,b)$ est un ensemble non vide fini. Il admet donc un plus grand élément, appelé PGCD(a,b) (Plus Grand Diviseur Commun de a et b). On le note parfois $a \wedge b$.
L'ensemble des multiples communs strictement positifs de a et b est un ensemble dénombrable minoré. Il admet un plus petit élément, appelé PPCM(a,b) (Plus Petit Multiple Commun de a et b).

Exemples :

PGCD$(4,6) = 2$ PGCD$(12,13) = 1$ PGCD$(21,35) = 7$
PPCM$(4,6) = 12$ PPCM$(12,13) = 156$ PPCM$(21,35) = 105$

Définition 4.

On dit que a et b sont premiers entre eux si et seulement si PGCD$(a,b) = 1$

Exemples :

PGCD$(3,2) = 1$ PGCD$(10,21) = 1$ PGCD$(51,113) = 1$

Propriété 1. (Immédiates)

1. $0 < \text{PGCD}(a,b) = \text{PGCD}(b,a) = \text{PGCD}(|a|,|b|) < min(|a|,|b|)$
2. PGCD$(a,0) = |a|$
3. PGCD$(a,1) = 1$
4. Si $b|a$ alors PGCD$(a,b) = |b|$

Remarque : Dans tout le chapitre, sauf indication contraire, on considérera désormais les diviseurs positifs communs à deux entiers naturels a et b non tous les deux nuls.

Propriété 2. (Réduction)

L'ensemble des diviseurs de a et b est égal à l'ensemble des diviseurs de b et $a-b$. En fait :

$$\mathscr{D}(a,b) = \mathscr{D}(a-b,b) = \mathscr{D}(a-kb,b) \quad \text{pour tout } k \in \mathbb{Z}$$

Preuve

Il s'agit de montrer une double inclusion. Soit $k \in \mathbb{Z}$.
$\mathscr{D}(a,b) \subset \mathscr{D}(a-kb,b)$: Si d divise a et b, il divise aussi $a-kb$.
$\mathscr{D}(a,b) \supset \mathscr{D}(a-kb,b)$: Si d divise b et $a-kb$ alors il divise $(a-kb)+kb=a$.
D'où l'égalité $\mathscr{D}(a,b) = \mathscr{D}(a-kb,b)$. En prenant $k=1$, on obtient la propriété.

Exemple :

p et q étant deux entiers naturels non nuls, on note $a = 9p+4q$ et $b = 2p+q$.

1. Démontrer que $pgcd(a,b) = pgcd(p,q)$
2. Démontrer que $9p+4$ et $2p+1$ sont premiers entre eux.
3. Déterminer $pgcd(9p+4, 2p-1)$ en fonction des valeurs de p. Vérifier pour $p=5$ et $p=9$.

Corollaire 3.

Si $0 < b \leq a$, alors $\mathscr{D}(a,b) = \mathscr{D}(r,b)$ où r est le reste de la division euclidienne de a par b.

Preuve

Cas particulier de la propriété précédente puisque r est tel que $a = bq+r \Leftrightarrow a-bq = r$ avec $q \in \mathbb{N}$

II.2. Détermination du PGCD et du PPCM

II.2.a. Lien PGCD -PPCM

Propriété 3. (Relation PGCD-PPCM)

Si $d = pgcd(a,b)$ et $m = ppcm(a,b)$ alors $md = ab$.

Preuve

$d = pgcd(a,b)$ donc il existe a' et b' deux entiers tels que $a = da'$ et $b = db'$ avec $pgcd(a',b') = 1$.
Considérons l'ensemble des multiples communs à a et b. Soi tM l'un quelconque d'entre eux.
Alors il existe deux entiers p et q tels que :

$$\text{M} = ap = bq \Rightarrow a'dp = b'dq \Leftrightarrow a'p = b'q$$

D'après le théorème de Gauss, on a alors que $a' | q$ d'où il existe un entier k tel que $ka' = q$. Donc $\text{M} = ap = bq = ba'k = db'a'k$.
Ainsi tout multiple commun à a et b peut s'écrire sous la forme $\text{M} = da'b'k$.
De plus, tout nombre de la forme $da'b'k$ est un multiple de a et b car $da'b'k = ab'k = a'bk$.
Le multiples communs à a et b sont donc les multiples de $da'b'$. Le plus petit étant $m = da'b' = \dfrac{ab}{d}$.

Propriété 4. (Homogénéité)

Pour tout $k \in \mathbb{N}^*$ on a $\text{PPCM}(ka, kb) = k\text{PPCM}(a, b)$

Preuve

Découle directement de la propriété ci-dessus et de l'homogénéité du pgcd.

II.2.b. Décomposition en facteurs premiers

Soit a et b deux nombres dont voici la décomposition en facteur premier, (faisant intervenir tous les nombres premiers qui interviennent dans la décomposition de a et tous les nombres premiers qui interviennent dans celle de b, pour cela certain des α_i et des β_i peuvent-être nul) :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \times \ldots\ldots p_n^{\alpha_n} \qquad \text{et} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \times \ldots\ldots p_n^{\beta_n}$$

Alors :

$$pgcd(a;b) = p_1^{min(\alpha_1,\beta_1)} p_2^{min(\alpha_2,\beta_2)} \times \cdots \times p_n^{min(\alpha_n,\beta_n)}$$

Exemple :

Déterminer le pgcd de $2^6 \times 3^2 \times 11^2 \times 17$ et $3^4 \times 7^4 \times 11 \times 19^2$.

Propriété 5.

Soient a et b deux entier supérieur ou égaux à 2. Leur PPCM est le produit des facteurs premiers figurant dans l'une ou l'autre de leurs décompositions, chacun étant affecté de son plus grand exposant.

Preuve

Découle du lien PGCD-PPCM et de la manière de trouve le PGCD de deux nombres à partir de leurs décompositions.

II.2.c. Algorithme d'Euclide

Il existe plusieurs méthodes pour trouver le pgcd de deux nombres, tels que :

1. *Lister les diviseurs*
2. *Décomposer les nombres en produits de facteurs premiers*
3. *Faire l'algorithme d'Euclide, l'objet de cette partie.*

On cherche à déteminer $\text{PGCD}(a, b)$ où a et b sont deux nombres entiers tels que $0 < b < a$.
On s'appuyera les résultats suivants :

- Si $b|a$ alors $\text{PGCD}(a, b) = b$.
- Si b ne divise pas a, alors $\exists!\,(q, r) \in \mathbb{N}^2$ tel que $0 < r < b$ et l'on a $\mathscr{D}(a, b) = \mathscr{D}(b, r)$.

Dans le deuxième cas, comme $b < a$ et $r < b$, on s'est ramené à travailler sur des nombres plus petits. De plus, comme $r > 0$ (b ne divise pas a), on peut réitérer le processus, autant de fois que nécessaire (c'est-à-dire tant que le reste n'est pas nul).
Il arrivera forcément un moment où le reste de la division sera nul, car la suite des restes est strictement décroissante, minorée par 0.
On aura alors $\mathscr{D}(a,b) = \mathscr{D}(b,r) = \mathscr{D}(r,r_1) = \mathscr{D}(r_1,r_2) = \cdots = \mathscr{D}(r_k,0)$, d'où $pgcd(a,b) = r_k$.

Le principe de l'algorithme d'Euclide est donc d'effectuer des divisions euclidiennes successives et bien choisies. Le $pgcd$ des deux nombres sera donc le dernier reste non nul obtenu.

Algorithme d'Euclide

On note D = $pgcd(a,b)$. On cherche D

1. J'effectue la division euclidienne de a par b : $a = bq + r$. On a alors $\mathscr{D}(a,b) = \mathscr{D}(b,r)$
2. Si $r = 0$ alors $\mathscr{D}(a,b) = \mathscr{D}(b,0)$ et $pgcd(a,b) = pgcd(b,0) = b$.
   Sinon :
   - On pose $r_0 := b$, $r_1 := r$, $i :=< 1$
   - Tant que $r_i \neq 0$:
     - J'effectue la division euclidienne de r_{i-1} par r_i : $r_{i-1} = r_i q_{i+1} + r_{i+1}$.
       On a alors $\mathscr{D}(a,b) = \mathscr{D}(r_i, r_{i+1})$
     - i prend la valeur $i+1$
3. On a alors $\mathscr{D}(a,b) = \mathscr{D}(r_i, r_{i+1}) = \mathscr{D}(r_i,0)$ et $pgcd(a,b) = pgcd(r_i,0) = r_i$.

Exemple :

Trouver le pgcd de 246 et 168.

$$\begin{aligned} 264 &= 168 \times 1 + 96 \\ 168 &= 96 \times 1 + 72 \\ 96 &= 72 \times 1 + 24 \\ 72 &= 24 \times 3 + 0 \end{aligned}$$

Le dernier reste non nul est 24 : c'est donc le pgcd de 264 et 168.

II.3. Quelques propriétés

II.4. Propriétés

Propriété 6.

L'ensemble des diviseurs de a et b est aussi l'ensemble des diviseurs de leur pgcd.

$$\mathscr{D}(a,b) = \mathscr{D}(pgcd(a,b))$$

En particulier, tous les diviseurs communs à deux nombres sont aussi des diviseurs de leur pgcd.

Preuve

Découle du fait que $\mathscr{D}(a,b) = \mathscr{D}(r_k,0) = \mathscr{D}(r_k)$, avec $r_k = pgcd(a,b)$

Propriété 7. (Homogénéité)

Pour tout $k \in \mathbb{N}^*$ on a $\text{PGCD}(ka,kb) = k\text{PGCD}(a,b)$

Preuve

Si $a = 0$ ou $b = 0$, c'est trivial.
Sinon, on peut faire l'algorithme d'Euclide dans lequel, chaque égalité est multipliée par k, dont celle contenant le dernier reste non nul.

Propriété 8. (Caractéristique)

Soit $d \in \mathbb{N}$. $\quad d = pgcd(a,b) \iff \begin{cases} a = da' \text{ et } b = db' \\ pgcd(a',b') = 1 \end{cases}$

Preuve

$\Rightarrow$: Si $d = pgcd(a,b)$ alors $d|a$ et $d|b$ et il existe a', b' tels que $a = da'$ et $b = db'$.
De plus, on a $pgcd(a,b) = pgcd(da',db') = d \times pgcd(a',b')$. Donc nécessairement $pgcd(a',b') = 1$.
$\Leftarrow$: Si $a = da'$ et $b = db'$ avec $pgcd(a',b') = 1$.
Comme a et b ne sont pas tous les deux nuls, on a $d \neq 0$ et donc $pgcd(a,b) = d \times pgcd(a',b') = d$.

Remarque : Toute fraction peut alors s'écrire sous forme irréductible.

Propriété 9.

Soient a et b deux entier supérieur ou égaux à 2.

- S'ils n'ont aucun facteur commun, $pgcd(a,b) = 1$
- Sinon, $pgcd(a,b)$ est égal au produit des facteurs premiers communs aux deux nombres, chacun étant affecté du plus petit exposant avec lequel il figure dans leur deux décomposition.

Preuve

Découle de l'homogénéité.

III. Equation diophantienne - théorème de bezout et de gauss.

III.1. Théorème de Bezout

Etienne Bezout (1730-1783) fut un génie assez précoce puisqu'à 19 ans, il était déjà adjoint de l'Académie des Sciences. Sa plus grande oeuvre, *Théorie générale des équations algébriques*, un traité clair et détaillé, témoigne de sa pédagogie et de sa volonté de rendre parfaitement accessibles ses découvertes.
Bézout fit aussi une brillante carrière dans la marine royale et de chargé de l'enseignement des élèves du corps d'artillerie.

Propriété 10.

Soient a et b deux entiers relatifs non tous les deux nuls et $d = pgcd(a,b)$.

1. Il existe u et v entiers relatifs tels que $au+bv = d$
2. L'ensemble des entiers $au+bv$ (avec u et v entiers relatifs) est l'ensemble des multiples de d.

Preuve

1. On utilise l'algorithme d'Euclide. On a :
   $a = bq_0 + r_0 \iff r_0 = a - bq_0 = au_0 + bv_0$ avec $u_0 = 1$ et $v_0 = -q_0$ deux entiers relatifs.
   $b = r_0q_1 + r_1 \iff r_1 = b - r_0q_1 = b - (au_0 + bv_0)q_1 = au_1 + bv_1$ avec $u_1 = -u_0q_1$ et $v_1 = 1 - v_0q_1$ deux entiers.
   Pas à pas, on exprime chaque reste comme combinaison linéaire enitère de a et b jusqu'à r_k, ie le $pgcd(a,b)$.
2. $\subset$: Soit $n = au+bv$ alors comme d divise a et b on a $d|n$, ie n est un multiple de d.
   $\supset$: Soit n un multiple de d. On sait qu'il existe u et v tels que $d = au+bv$. Alors il existe k tel que $n = kd = k(au+bv) = a\mathrm{U} + b\mathrm{V}$. Donc n est une combinaison linéaire de a et b.

Théorème 5. (de Bezout)

Deux entiers relatifs a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au+bv = 1$.

Preuve

$\Rightarrow$: Si a et b sont premiers entre eux, on applique la propriété pour $d = 1$.
$\Leftarrow$: S'il existe des entiers relatifs u et v tels que $au+bv = 1$ alors d'après la propriété, 1 est un multiple du $pgcd(a,b)$. Par conséquent $d = 1$.

Exemple :

- $a = 4$ et $b = 9$ sont premiers entre eux et $9 \times 1 - 4 \times 2 = 1$. Donc $(u, v) = (-2; 1)$ convient.
- $a = 7$ et $b = 17$
- $a = 71$ et $b = 19$
- Montrer que pour tout $n \in \mathbb{Z}$, n et $n+1$ sont premiers entre eux
- Même question pour $2n+1$ et $3n+1$.

Remarque : Il découle du théorème que l'équation $ax + by = c$, avec $d = pgcd(a, b) \neq 0$ admet des solutions entières si et seulement si $d|c$

Exercice 11. Montrer que, pour tout entier naturel n, $2n+5$ et $3n+7$ sont premiers entre eux.

Exercice 12. Déterminer le PGCD$(2n+1; 2n+3)$ pour tout entier naturel n

III.2. Théorème de Gauss

Carl Friedrich Gauss (1777-1855) fut un mathématicien, astronome et physicien allemand. Il n'existe pas un seul domaine scientifique qu'il n'ait pas abordé, et on lui doit, entre autres, des travaux sur les polygone régulier, sur les nombres complexes, le magnétisme, l'algèbre et bien sûr, l'arithmétique. Il s'impliqua de plus dans les affaires politiques de son temps.

Théorème 6.

Soient a, b, et c trois entiers relatifs non nuls.
Si $a|bc$ et $pgcd(a, b) = 1$ alors $a|c$.

Preuve

$a|bc$ donc il existe $k \in \mathbb{Z}$ tel que $bc = ka$.
a et b sont premiers entre eux, donc il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bn = 1$.
Donc $c = cau + cbv = cau + kav = a(cu + kv)$ avec $cu + kv$ entier. Donc $a|c$.

Corollaire 4.

Si deux entiers a et b divise un entier c avec $pgcd(a, b) = 1$ alors $ab|c$.

Preuve

$a|c$ donc il existe un entier k tel que $c = ka$. De même il existe un entier k' tel que $c = bk'$.
Donc $ak = bk'$ et $a|bk'$. Comme a et b sont premiers entre eux on a $a|k'$.
Alors il existe un entier l tel que $k' = al$ et $c = bk' = bal$. Donc $ab|c$.

Remarque : Par conséquent :

- Si un nombre premier p divise un produit ab, alors $p|a$ ou $p|b$
- Si un entier a est premier avec des entiers $b_1, b_2, \ldots, b_n$, alors a est premier avec $b_1 \times b_2 \times \cdots \times b_n$.

– L'unicité de la décomposition en nombre premier vu au chapitre 2 en découle.

Exercice 13.

1. Résoudre dans $\mathbb{Z}$ l'équation $3x = 5y$.
2. Résoudre dans $\mathbb{Z}$ l'équation $273x = 637y$.

III.3. Equations du type $ax + by = c$.

Définition 5.

Une équation diophantienne est une équation à coefficients entiers et dont les inconnues sont entières.
Cette année, nous ne résolvons que les équations de la forme $ax + by = k \times \text{PGCD}(a, b)$.

Exemples :

– $5x + 7y = 1$
– $6x + 15y = 3$
– $5x - 8y = 2$
– $6x + 14y = 100$

Méthode de Résolution

1. Simplification de l'équation.
   – On calcule $d = pgcd(a, b)$
   – On divise l'équation par d : on obtient $a'x + b'y = d'$ avec $pgcd(a', b') = 1$
2. Recherche d'une solution particulière :
   – On cherche $(x_0, y_0) \in \mathbb{Z}^2$ tels que $a'x_0 + b'y_0 = d'$ à l'aide des divisions euclidiennes
3. Recherche de toutes les solutions :
   – On désigne par x et y d'autres solutions. On a alors $a'(x - x_0) + b'(y - y_0) = 0 \Leftrightarrow a'(x - x_0) = -b'(y - y_0)$
   – D'après le théorème de Gauss, on a alors que $a' | (y - y_0)$ ie qu'il existe $k \in \mathbb{Z}$ tel que $ka' = y - y_0 \Leftrightarrow y = ka' + y_0$.
   – Alors $a'(x - x_0) = -b' \times ka' \Leftrightarrow x = -b'k + x_0$
4. Conclusion : Les solutions sont les couples de la forme $(-b'k + x_0; a'k + y_0)$, avec $k \in \mathbb{Z}$

Exercice 14. On cherche les solutions entières de l'équation :

$$(E) : 7x + 13y = 1$$

1. Déterminer une solution $(x_0; y_0)$ de (E).
2. Montrer qu'une solution $(x; y)$ de (E) vérifie l'équation :

$$7(x - x_0) = 13(y_0 - y)$$

3. Résoudre cette équation.

Exercice 15. a et b étant deux entiers naturels non nuls et c un entier relatif, on veut résoudre l'équation :

$$ax + by = c$$

PARTIE A. **Résolution de l'équation** $au + bv = \text{PGCD}(a;b)$

On note g le PGCD de a et b.

1. Justifier qu'il existe un couple $(u_0;v_0)$ solution de cette équation.
2. On suppose qu'il existe une autre solution $(u;v)$ et on pose $a' = \dfrac{a}{g}$ et $b' = \dfrac{b}{g}$.
   (a) Montrer que $au + bv = au_0 + bv_0$, puis que $a'(u-u_0) + b'(v-v_0) = 0$.
   (b) En déduire que a' divise $b'(v_0 - v)$, puis à l'aide du théorème de Gauss que a' divise $v_0 - v$.
   (c) Justifier qu'il existe un entier relatif k tel que $v = v_0 - ka'$ puis montrer que $u = u_0 + kb'$.
   (d) Réciproquement, montrer que, quel que soit l'entier relatif k, les couples $(u_0 + kb'; v_0 - ka')$ sont solutions de l'équation $au + bv = g$.
3. PGCD(15;9) = 3. Déterminer l'ensemble des solutions entières de l'équation $15x + 9y = 3$.

PARTIE B. **Résolution de l'équation** $ax + by = c$**.**

1. Montrer que si c n'est pas un multiple de g alors l'équation $ax + by = c$ n'admet pas de solution.
2. On suppose désormais que c est un multiple de g et que $c = c'g$ avec c' entier relatif.
   Montrer que l'équation $ax + by = c \iff a'x + b'y = c'$.
3. Montrer qu'il existe un couple $(x_0;y_0)$ solution de l'équation $a'x + b'y = c'$.
4. Résoudre alors l'équation $a'x + b'y = c'$ en vous inspirant de la partie A.
5. Résoudre $15x + 9y = 21$.

PARTIE C. **Applications**

Léo prend le métro pour aller au travail. A la station Bézout, il doit changer de rame, la correspondance est sur le même quai. Il sait que son premier métro (Ligna A - durée du trajet 8 minutes) passe toutes les 7 minutes et le second (ligne B) toutes les 11 minutes. Ce matin il a pris son premier métro à 6 h 52, il est arrivé à $7h$ à la station Bézout et il a du attendre 6 minutes la rame de la ligne B.
Léo voudrait savoir à qu'elle heure partir entre $6h$ et $9h$ pour ne pas attendre la rame de la ligne B à la station Bézout.
On note x le nombre de rames de la ligne A et y le nombre de rames de la ligne B passées à la station Bézout **après** 7 h.

1. Montrer que, pour que l'attente soit nulle à la station Bézout, x et y doivent vérifier l'équation $(E_1) : 7x - 11y = -12$.
2. Déterminer une solution particulière de (E_1).
3. Déterminer l'ensemble des solutions de (E_1).
4. Déterminer à quelles heures entre 6 h et 9 h, Léo peut prendre son premier métro pour ne pas attendre à la station Bézout.

III.4. Petit théorème de Fermat.

Théorème 7. (Petit Théorème de Fermat)

Si p est un entier premier et a un entier naturel non divisble par p, alors $a^{p-1}-1$ est divisble par p (ou encore $a^{p-1} \equiv 1\,[p]$)

Preuve

On suppose donc que a n'est pas divisible par p.
On considère le nombre

$$\mathrm{N} = a \times 2a \times 3a \times \cdots \times (p-1)a = (p-1)!a^{p-1}$$

On note r_k le reste de la division euclidienne de ka par p, k étant un nombre entre 1 et $p-1$. Il résulte que :

$$ka \equiv r_k(p) \qquad \text{et} \qquad 0 \leq r_k < p$$

Si l'un des $r_k = 0$ alors p divise ka donc d'après le lemme d'Euclide p divise k ou p divise a. Ceci est impossible car d'une part $k < p$ et d'autre part on suppose que p ne divise pas a. Ainsi on peut affirmer que :

$$ka \equiv r_k(p) \qquad \text{et} \qquad 0 < r_k < p$$

De plus les r_k sont deux à deux distincts, en effet si on suppose le contraire, c'est-à-dire qu'il existe $i < j$ tel que $r_i = r_j$ alors on obtient :

$$ia \equiv ja(p) \Longrightarrow (j-i)a \equiv 0(p)$$

Et on vient de montrer que p ne divise pas ka, pour $0 < k < p-1$ donc en particulier il ne divise pas $(j-i)a$. Ainsi les $p-1$ restes valent chacune des valeurs entières comprises entre 1 et $p-1$. D'autre part puisque $\mathrm{N} = a \times 2a \times 3a \times \cdots \times (p-1)a$ on obtient :

$$\mathrm{N} \equiv r_1 \times r_2 \times \cdots \times r_k(p) \Longleftrightarrow (p-1)!a^{p-1} \equiv r_1 \times r_2 \times \cdots \times r_k(p)$$

c'est-à-dire compte tenu du fait que les r_k valent toutes les valeurs entre 1 et $p-1$:

$$(p-1)!a^{p-1} \equiv (p-1)!(p) \Longleftrightarrow < (p-1)!\left(a^{p-1}-1\right) \equiv 0(p)$$

Il vient que p divise le produit $(p-1)!\left(a^{p-1}-1\right)$, et puisqu'il ne divise pas $(p-1)!$ il divise d'après le lemme d'euclide $a^{p-1}-1$ ce qui montre le petit théorème de Fermat.

Exemple :

$2^{2002}-1$ est divisible par 2003 (qui est premier).

Exercice 16. Déterminer un diviseur premier des nombres suivants :

$$2^{10}-1 \qquad 4^{16}-4 \qquad 4^{14}-4 \qquad 6^6-1$$

Exercice 17. En écrivant 999999 sous la forme $10^n - 1$, déterminer un diviseur premier de 999999 autre que 3.

Corollaire 5.

Si p est un entier premier et a un entier naturel, alors $a^p - a$ est divisible par p (ou encore $a^p \equiv a\,[p]$)

Preuve

Si p divise a alors p divise en particulier $a^{p-1} \times a - a$ ce qui donne le résultat.
Sinon on sait d'après le petit théorème de Fermat que $a^{p-1} \equiv 1(p)$ donc en multipliant par a on obtient le résultat voulu.

Exemple :

Déterminer tous les entiers p premiers tels que $p|(2^p + 1)$.

Exercice 18. Soit p un nombre premier, a et b deux entiers relatifs.

1. A l'aide du corollaire du petit théorème de Fermat, montrer que si p divise $a+b$, alors p divise $a^p + b^p$.
2. En déduire un diviseur de $5^{11} + 6^{11}$ et vérifier ce résultat.
3. Déduire de la question 1. une valeur de p telle que $5^p + 7^p$ soit divisible par p.
4. Déterminer, par une démarche analogue, une valeur de p telle que $11^p - 4^p$ soit divisible par p.

III.5. Chiffrement de Hill

Un message codé, assez long, dans lequel chaque lettre a été codée par une autre toujours de la même façon comme le codage affine, est assez facile à attaquer en s'appuyant par exemple sur la fréquence des lettres dans un texte suivant la langue.
Une amélioration, publiée en 1931 par le mathématicien américain Lester Hill, consiste à coder des blocs de lettres, le codage d'une lettre dépendant alors de sa place dans le bloc.
Comment fonctionne un tel codage sur des blocs de deux lettres ?

Le principe :

On choisit quatre entiers a, b, c et d constituant la **clé** du chiffrement. Les lettres de l'alphabet sont codées de 0 à 25. A un bloc de deux lettres correspondent un couple $(x; y)$ d'entiers compris entre 0 et 25. On calcule les codes du message chiffré en associant au couple $(x; y)$ le couple $(x'; y')$ tel que :

$$\begin{cases} x' & \equiv & ax + by \quad (26) \\ y' & \equiv & cx + dy \quad (26) \end{cases}$$

IV. Exemple de chiffrement

On souhaite chiffrer le mot ETUDIER.
On partage le mot en blocs de 2 lettres : ET - UD - IE - RA (le dernier bloc est complété au hasard).

IV.1. Cle - $a=-5$, $b=8$, $c=-2$ et $d=3$

1. Chiffrement du premier bloc ET. Déterminer x et y puis en déduire x' et y'. Vérifier que ET est chiffré par CX.
2. Terminer le chiffrement du mot ETUDIER.
3. Quelle remarque ce chiffrement occasionne-t-il ?

IV.2. Clé $a=6$ $b=7$, $c=-8$ et $d=5$.

Coder le mot ETUDIER avec cette clé. Quel problème cela pose-t-il ?

V. Chiffrement et déchiffrement : approche mathématique

Toujours suivant le même principe, posons par exemple :

$$(1): \quad \begin{cases} x' \equiv 5x+11y \quad (26) \\ y' \equiv 8x+3y \quad (26) \end{cases}$$

1. Coder le mot REQUIN en détachant les trois blocs de deux lettres.
2. Montrer que si x, y, x' et y' vérifient (1) alors $\begin{cases} -3x'+11y' \equiv 73x \quad (26) \\ 8x'-5y' \equiv 73y \quad (26) \end{cases}$
3. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$, l'équation $73x+26y=1$ avec $0\leq x\leq 25$.
   On se contentera de déterminer l'inverse de 73 *modulo* 26 *puis de proposer une fonction de décodage.*
4. Décoder alors le mot XEJQVVLDVW.

V.1. Code RSA

Le but du jeu est bien sûr de pouvoir transmettre un message codé, que seul le récepteur « officiel » puisse décrypter, c'est-à-dire qui ne puisse pas être décrypté par un tiers qui intercepterait ledit message. Nous appellerons Alice la destinatrice du message, et Bernard l'émetteur.

Principe Général

1. Alice génère deux gros nombres premiers p et q, ainsi qu'un gros nombre d premier avec $\varphi(n)$.
2. Alice calcule $n = pq$ et cherche e tel que $de \equiv 1[\varphi(n)]$.
3. Alice diffuse n et e, garde en mémoire d et oublie $\varphi(n)$.
4. Bernard crypte un message M par $M \longmapsto M^e[n]$ et envoie le résultat à Alice.
5. Alice décode alors le message crypté par $C \longmapsto C^d[n]$.

Exemple :

Voyons ce qui se passe si on prend pour les deux nombres p et q les valeurs 11 et 17.
On a alors $n = 187$ et $\varphi(n) = (11-1)(17-1) = 160$.
Comme $160 = 7 \times 23 + 1$, on a $7 \times 23 \equiv 1[\varphi(n)]$.
On peut prendre $e = 7$ et $d = 23$.

Alice va rendre public le couple (la clé) $(187, 7)$.

Bernard veut transmettre à Alice un message codé (nécessairement un nombre plus petit que $n = 187$, mettons la date à laquelle ils vont faire une surprise à Elodie (par exemple, le 10), message qui ne doit pas être intercepté par ladite Elodie, bien sûr.

Bernard va donc calculer $10^7(187)$, or $10^7 = 187 \times 53475 + 175$ donc $10^7 \equiv 175(187)$, et envoyer le résultat 175 à Alice.

Alice va calculer le reste de la division euclidienne de 175^{23} par 187.
En utilisant Python, en tapant 175^{23}%187 on trouve 10.
Alice retrouve donc bien le message envoyé, à savoir 10.

Exercice 19.

1. Trouver n, p, q, d, e qui conviennent à un cryptage RSA.
2. Transmettre la clé publique (n, e) à vos voisins de gauche et de droite et conserver la clé privée d.
3. Coder votre jour de naissance à l'aide de la clé publique fournit par votre voisin de gauche et lui transmettre votre message crypté.
4. Décrypter le message que vous a transmit votre voisin de droite et vérifier qu'il s'agit bien du bon message (en lui demandant confirmation).
5. Avec la clé publique que vous a transmis votre voisin de droite, essayer de trouver la clé privée d.

Exercice 20. Le but du protocole est bien sûr qu'Alice retrouve le message d'origine. Démontrons que c'est bien le cas. Les transformations appliquées au message sont :

$$\mathrm{M} \longmapsto \mathrm{M}^e[n] \longmapsto \left(\mathrm{M}^e[n]\right)^d[n]$$

On veut donc montrer que $\left(\mathrm{M}^e[n]\right)^d[n] = \mathrm{M}$ c'est-à-dire que :

$$\left(\mathrm{M}^e\right)^d \equiv \mathrm{M}[n] \Longleftrightarrow \mathrm{M}^{de} \equiv \mathrm{M}[n]$$

1. Montrer qu'il existe un entier relatif k tel que :

   $$de = 1 + k\varphi(n)$$

   En déduire que l'on souhaite démontrer que :

   $$\mathrm{M} \times \mathrm{M}^{k\varphi(n)} \equiv \mathrm{M}[n]$$

2. **On suppose que** M **est premier avec** n**.**
   En utilisant le théorème 2 montrer que

   $$\mathrm{M} \times \mathrm{M}^{k\varphi(n)} \equiv \mathrm{M}[n]$$

3. **On suppose que** M **n'est pas premier avec** n**.**
   (a) Donner la liste des diviseurs positifs de n.
   (b) En déduire que M est un multiple de p ou de q.
   Dans le cas où M est un multiple de q on peut écrire que :

   $$\mathrm{M} = p^{\alpha} m \qquad \text{avec } \alpha \text{ un entier naturel et } m \text{ un entier non multiple de } p$$

   (c) Montrer que m est premier avec n.
   En déduire que $m^{de} \equiv m[n]$.
   (d) Montrer que :

   $$\mathrm{M}^{de} \equiv p^{\alpha de} \times m[n]$$

   Il nous reste à démontrer que $p^{\alpha de} \equiv p^{\alpha}(n)$.
   (e) Montrer que $p^{\alpha de} \equiv p^{\alpha}(n)$ est un multiple de p.
   (f) Montrer que

   $$p^{de} = p \times p^{k(p-1)(q-1)}$$

   En déduire en utilisant le petit théorème de Fermat (ou le théorème 2, ce qui revient au même) que :

   $$p^{de} \equiv p[q]$$

   (g) En déduire que $p^{\alpha de} - p^{\alpha}$ est un multiple de q.
   (h) En déduire, en utilisant Gauss que $p^{\alpha de} - p^{\alpha}$ est un multiple de n puis conclure.