ARITHMETIQUE

PLAN

I : Les entiers naturels

1- Le principe de récurrence

Peano (1858-1932) a posé les axiomes qui régissent $\mathbb{N}$. (Un **axiome** est une propriété servant de base à la construction d'une théorie et dont il est impossible de montrer la véracité ou la fausseté. Ils servent à poser les règles de fonctionnement de l'objet que l'on définit et sont considérés comme inhérents à la nature de cet objet).

Il existe un ensemble noté $\mathbb{N}$ dont les éléments seront appelés **entiers naturels** et une fonction appelée **successeur** définie sur cet ensemble, et vérifiant les axiomes suivants :

i) 0 est un entier naturel.

ii) Tout entier naturel possède un successeur.

iii) Deux entiers naturels ayant le même successeur sont égaux.

iv) 0 n'est le successeur d'aucun entier naturel.

v) Si une partie A de $\mathbb{N}$ contient 0 et si le successeur de tout élément de A appartient à A, alors A est égale à $\mathbb{N}$.

v) est à la base du **principe de récurrence**. Soit P un **prédicat** sur $\mathbb{N}$, i.e. une fonction définie sur $\mathbb{N}$ à valeur dans {vrai, faux} (autrement dit, pour tout n, P(n) est l'une des valeurs vrai ou faux).

$$\text{si} \left[\begin{array}{l} \text{P}(0) \\ \forall\, n \in \mathbb{N},\ (\text{P}(n) \Rightarrow \text{P}(n+1)) \end{array} \right. \qquad \text{alors } \forall\, n \in \mathbb{N},\ \text{P}(n)$$

On applique en effet l'axiome v) avec la partie A = {n | P(n)}. Le fait que v) soit un axiome est développé dans une annexe de L1/ENSEMBLE.PDF.

EXEMPLE :

❑ On rappelle que, pour tout entier n, $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. Qu'en est-il de la somme des carrés ?

Montrons par récurrence que :

$$\forall\, n,\ \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

On note P(n) le prédicat $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

P(0) est vérifié car P(0) $\Leftrightarrow 0 = 0$

Soit n quelconque. Supposons P(n) vérifié. Montrons P($n+1$) :

$$\sum_{k=0}^{n+1} k^2 = \sum_{k=0}^{n} k^2 + (n+1)^2$$

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \qquad \text{car P}(n) \text{ est supposée vraie}$$

$$= \frac{(n+1)(2n^2+n+6n+6)}{6} = \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

$$= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$$

ce qui est bien la propriété P($n+1$) demandée.

On pourra de même montrer par récurrence que $\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$

Les axiomes de Peano permettent de définir sur $\mathbb{N}$ l'addition, le produit, la relation d'ordre, avec toutes leurs propriétés bien connues ... Nous ne nous étendrons pas sur ce sujet et nous admettrons (ce qui est bien connu) que :

+ est associative	$\forall (a, b, c), (a + b) + c = a + (b + c)$
+ est commutative	$\forall (a, b), a + b = b + a$
+ possède un élément neutre 0	$\forall a, a + 0 = a$
$\times$ est associatif	
$\times$ est commutatif	
$\times$ possède un élément neutre, 1, successeur de 0	$\forall a, a \times 1 = a$
$\times$ est distributif par rapport à l'addition	$\forall (a, b, c), (a + b) \times c = ac + bc$

La relation d'ordre est telle que, pour tout entier naturel n, il n'existe aucun entier x vérifiant $n < x < n + 1$, $0 \leq n$ et pour tout couple d'entiers (n, m), $n < m \Leftrightarrow n + 1 \leq m$.

$\mathbb{Z}$ est construit de façon que tout les éléments de $\mathbb{N}$ possède un symétrique pour +. Les éléments de $\mathbb{Z}$ sont les **entiers relatifs**. $(\mathbb{Z}, +, \times)$ est un **anneau**. Cet anneau est commutatif (car le produit est commutatif), unitaire (car le produit admet un neutre), intègre (ce qui signifie que : $ab = 0 \Rightarrow a = 0$ ou $b = 0$). $\mathbb{Q}$ est construit de façon que tout élément non nul possède un inverse pour $\times$. $(\mathbb{Q}, +, \times)$ est alors un **corps** (voir L1/ENSEMBLE.PDF).

2- Propriétés de $\mathbb{N}$

Les propriétés de ce paragraphe paraîtront évidentes en soi. Une démonstration est cependant donnée, car il s'agit de théorèmes se déduisant du principe de récurrence, et non d'axiomes supplémentaires.

PROPOSITION :
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

Cette propriété est connue sous le nom de **principe du bon ordre**.

Démonstration :
❑ La démonstration de cette propriété utilise le principe de récurrence. Soit A une partie non vide. Raisonnons par l'absurde en supposant que A n'admet pas de plus petit élément. On a :

$\forall a \in A, 0 \leq a$

si n vérifie : $\forall a \in A, n \leq a$, alors n minore A, mais comme A ne possède pas de plus petit élément, n ne peut être élément de A. Donc :

$$\forall a \in A, n < a$$

Cette dernière affirmation est équivalente à :

$$\forall a \in A, n + 1 \leq a.$$

Soit P(n) le prédicat $\forall a \in A, n \leq a$. On a montré que :

$$\begin{cases} P(0) \\ \forall n \in \mathbb{N}, P(n) \Rightarrow P(n + 1) \end{cases}$$

Le principe de récurrence permet de conclure : $\forall n \in \mathbb{N}$, P(n).

ou encore : $\forall\, n \in \mathbb{N}$, $\forall\, a \in$ A, $n \leq a$.

Or ceci est absurde. Il suffit de prendre $a \in$ A et $n = a + 1$ pour arriver à une contradiction.

COROLLAIRE

Toute suite strictement décroissante de $\mathbb{N}$ *est finie.*

Démonstration :

❑ Prendre comme partie A l'ensemble des termes de la suite. Le fait que A admette un plus petit élément x_n et que la suite soit strictement décroissante entraîne que x_n est nécessairement le dernier élément de la suite.

Cette propriété a été utilisée par Fermat (1601-1665) sous la forme suivante : Pour montrer qu'une propriété P est vraie pour tout *n*, Fermat montre que si P est fausse pour un entier, alors elle est fausse pour un entier strictement plus petit. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers. Cette méthode s'appelle **principe de descente infinie** de Fermat. C'est une des premières méthodes utilisées pour montrer qu'une propriété est vraie pour tout entier, à une époque où le principe de récurrence n'était pas encore clairement formulé.

COROLLAIRE :

Toute partie de $\mathbb{N}$ *non vide majorée admet un plus grand élément.*

Démonstration :

❑ Soit A une partie non vide majorée. L'ensemble M de ses majorants est donc non vide. M étant non vide admet un plus petit élément *m*.

si $m = 0$, alors nécessairement A = {0} et 0 est le plus grand élément de A.

si $m > 0$, alors $m - 1$ n'appartient pas à M, (puisque *m* est le plus petit élément de M), donc $m - 1$ ne majore pas A. Il existe donc un élément *a* de A tel que :

$$m - 1 < a \leq m$$

Donc $a = m$, et comme *m* majore A, *a* est bien le plus grand élément de A.

3- La division euclidienne

La plupart des propriétés de $\mathbb{Z}$ développées dans le paragraphe II reposent sur la division euclidienne.

PROPOSITION (DIVISION EUCLIDIENNE) :

Soit a et b deux entiers (relatifs) tels que b soit strictement positif. Alors il existe un couple unique (*q*, *r*) *tels que :*

$$a = bq + r$$
$$et\ 0 \leq r < b$$

q s'appelle le **quotient**, *r s'appelle le* **reste**.

Ainsi la division de 36 par 5 donne 7 comme quotient et 1 comme reste.

Démonstration :

❑ Prouvons l'existence. Considérons d'abord le cas où $a \geq 0$. Soit A l'ensemble des entiers naturels *q* tels que $a - bq \geq 0$. A est non vide car 0 appartient à A. A est majoré par *a*. En effet :

$$q \in A \Rightarrow a \geq bq \text{ or } bq \geq q \text{ car } b \geq 1 \text{ donc } a \geq q$$

A admet donc un plus grand élément q. $q + 1$ n'est donc pas élément de A. D'où :

$$\begin{cases} a - bq \geq 0 \\ a - b(q+1) < 0 \end{cases} \Leftrightarrow 0 \leq a - bq < b$$

La quantité $r = a - bq$ vérifie donc bien $0 \leq r < b$.

Si $a < 0$, on applique le résultat précédent à $-a$. Il existe donc q et r tels que :

$$\begin{cases} -a = bq + r \\ 0 \leq r < b \end{cases} \Rightarrow \begin{cases} a = b(-q) - r = b(-q-1) + b - r \\ 0 < b - r \leq b \end{cases}$$

Si $r = 0$, $a = b(-q)$ convient. Si $r > 0$, $-q - 1$ est le quotient, $b - r$ est le reste.

Une autre démonstration consiste à se placer dans $\mathbb{R}$ et à poser $q = \lfloor \frac{a}{b} \rfloor$ où $\lfloor\ \rfloor$ désigne la partie entière (voir L1/REELS.PDF). On a donc $q \leq \frac{a}{b} < q + 1$, et donc $qb \leq a < qb + q$. Si on pose $r = a - qb$, on a :

$a = bq + r$ et $0 \leq r < q$

Cependant, l'existence de la partie entière repose sur un axiome de $\mathbb{R}$, l'existence de la borne supérieure, et il n'est pas très élégant d'utiliser cet axiome pour traiter une question portant uniquement sur les entiers.

❑ Il reste à prouver l'unicité. Si l'on a :

$$\begin{cases} a = bq + r = bq' + r' \\ 0 \leq r < b \text{ et } 0 \leq r' < b \end{cases}$$

alors :

$b(q - q') = r' - r$ avec $|r' - r| < b$

donc $|b(q - q')| < b$

donc $|q - q'| < 1$ car $b \neq 0$

donc $|q - q'| = 0$ et $q = q'$

donc on a aussi $r = r'$.

Lorsque $r = 0$, on dit que b **divise** a, et on note $b \mid a$.

Pour n entier non nul, on définit également une **relation de congruence**, reliant deux entiers a et b ayant même reste dans la division euclidienne par n :

$$a \equiv b \bmod n \Leftrightarrow \exists\, q,\ a = b + nq \Leftrightarrow n \mid a - b$$

ce qu'on note encore $a \equiv b\ [n]$, et ce qu'on dit a est **congru** à b modulo n. Il s'agit d'une relation d'équivalence, compatible avec la somme et le produit. Autrement dit :

$$\begin{cases} a \equiv b \bmod n \\ a' \equiv b' \bmod n \end{cases} \Rightarrow \begin{cases} a + a' \equiv b + b' \bmod n \\ aa' \equiv bb' \bmod n \end{cases}$$

En effet :

$$\begin{cases} a \equiv b \bmod n \\ a' \equiv b' \bmod n \end{cases} \Rightarrow \exists\ (q, q') \text{ tel que } \begin{cases} a = b + nq \\ a' = b + nq' \end{cases}$$

$$\Rightarrow \quad \begin{cases} a + a' = b + b' + n(q + q') \equiv b + b' \bmod n \\ aa' = bb' + n(bq' + qb' + nqq') \equiv bb' \bmod n \end{cases}$$

EXEMPLE :

❑ On appelle **sous-groupe** G de $\mathbb{Z}$, une partie non vide de $\mathbb{Z}$ telle que :

$$\begin{cases} \forall\, x \in G, \forall\, y \in G, x + y \in G \\ \forall\, x \in G, -x \in G \end{cases}$$

On se propose de déterminer les sous-groupes de $\mathbb{Z}$.

G = {0} est un exemple trivial de sous-groupe. Soit G un sous-groupe de $\mathbb{Z}$, différent de {0}. On a :

i) $0 \in G$

prendre x dans G et calculer $x + (-x)$.

ii) si $x \in G$, alors $\forall\, n \in \mathbb{Z}$, $nx \in G$

Il suffit de le montrer pour n élément de $\mathbb{N}$. La propriété P(n) : $nx \in G$ est vérifiée pour $n = 0$ et pour $n = 1$. Si elle est vraie pour n, elle est vraie pour $n + 1$, puisque $(n + 1)x = nx + x$, que nx et x sont tous deux dans G et que G est stable pour la somme. Par récurrense, la propriété P(n) est vraie pour tout entier.

iii) $\exists\, x \in G, x > 0$

Prendre x non nul, et si $x < 0$, prendre $-x$

iv) Soit m le plus petit élément strictement positif de G (qui existe puisque l'ensemble des éléments de G strictement positifs est non vide d'après iii). Montrons que : $\forall\, x \in G, \exists\, q \in \mathbb{Z}$ tel que $x = qm$. En effet, il existe q et r tels que : $x = mq + r$ avec $0 \leq r < m$. Donc $r = x - mq$. Or x est élément de G, mq aussi (d'après ii), donc r aussi. Or r est positif ou nul, et inférieur à m. m étant le plus petit élément de G strictement positif, r est nécessairement nul.

Nous avons ainsi montré que $G = \{mq \mid q \in \mathbb{Z}\}$, ensemble noté $m\mathbb{Z}$. Inversement, il n'est pas difficile de voir que tout ensemble de la forme $m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Ainsi, les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$.

L'étude des congruences est menée de manière plus approfondie dans L2/ZSURNZ.PDF.

4- Bases de numération

On a l'habitude de noter les nombres à l'aide de 10 chiffres. En fait, le nombre 10 est arbitraire, et l'on aurait pu choisir n'importe quel entier b supérieur ou égal à 2.

PROPOSITION

Soit b un entier supérieur ou égal à 2. *Tout entier naturel n s'écrit en effet de manière unique sous la forme* :

$$n = d_0 + d_1 b + d_2 b^2 + \ldots + d_k b^k, \text{ avec } 0 \leq d_i < b$$

Démonstration :

❑ Montrons l'existence par récurrence :

Si $n < b$ alors, on pose $n = d_0$.

Supposons la propriété vraie jusqu'à $n - 1$. Montrons-là pour n. On effectue la division euclidienne de n par b. On a $n = bq + d_0$ avec $d_0 < b$. Par ailleurs, $b \geq 2 \Rightarrow q < n$ donc on peut appliquer l'hypothèse de récurrence sur q en posant $q = d_1 + d_2 b + \ldots + d_k b^{k-1}$.

❑ Montrons l'unicité. Supposons que l'on ait :

$$n = d_0 + d_1 b + d_2 b^2 + ... + d_k b^k = c_0 + c_1 b + ... + c_k b^k$$

On peut obtenir le même k dans les deux membres, quitte à rajouter des coefficients nuls à l'un des membres. Supposons par l'absurde que les deux décompositions sont différentes. On peut supposer $d_k \neq c_k$, quitte à simplifier les termes de plus haut degré s'ils sont égaux. Supposons par exemple $d_k > c_k$. On a alors :

$$d_0 + d_1 b + d_2 b^2 + ... + d_k b^k \geq d_k b^k$$

et, en majorant c_0, ..., c_{k-1} par $b - 1$:

$$\begin{aligned} c_0 + c_1 b + ... + c_k b^k &\leq b - 1 + (b-1)b + ... + (b-1)b^{k-1} + c_k b^k \\ &\leq b^k - 1 + c_k b^k = (c_k + 1)b^k - 1 \\ &\leq d_k b^k - 1 < d_k b^k \end{aligned}$$

Les deux membres ne peuvent donc être égaux.

Les bases les plus répandues sont :

la base 10 (nombres décimaux)

la base 2, avec les chiffres 0 et 1 (**nombres binaires**)

la base 16, avec les chiffres 0, 1, ..., 9, A, B, C, D, E, F (**nombres hexadécimaux**).

Les babyloniens, vers 2000 avant JC, utilisaient la base 60 qui a survécu jusqu'à nos jours à travers les civilisations grecque, arabe et occidentale dans le format des heures, minutes, secondes et dans les degrés, minutes, secondes d'angle.

Les algorithmes de calculs dans une base b sont identiques aux algorithmes décimaux, mais les retenues se font à partir de b et non de 10.

EXEMPLES :

Pour distinguer les entiers exprimés en décimal et dans une base quelconque, on indique par un indice la base non décimale dans laquelle s'effectue le développement.

❑ Convertir en base $h = 16$ l'entier décimal 1457 :

$$\begin{aligned} 1457 &= 16 \times 91 + 1 \\ &= 16 \times (16 \times 5 + 11) + 1 \\ &= 5B1_h \end{aligned}$$

❑ Convertir en base $b = 2$ l'entier donné en base $a = 7$ par 2455_a. Ci-dessous, on opère la conversion directement sans passer par la base décimale :

$$\begin{aligned} 2455_a &= 1226_a \times 2 && \text{car } 15_a = 6 \times 2 \\ &= (446_a \times 2 + 1) \times 2 && \text{car } 12_a = 4 \times 2 + 1 \text{ et } 16_a = 6 \times 2 + 1 \\ &= 223_a \times 2^3 + 2 \\ &= (111_a \times 2 + 1) \times 2^3 + 2 \\ &= (40_a \times 2 + 1) \times 2^4 + 2^3 + 2 && \text{car } 11_a = 4 \times 2 \\ &= 20_a \times 2^6 + 2^4 + 2^3 + 2 \\ &= 10_a \times 2^7 + 2^4 + 2^3 + 2 \\ &= (3 \times 2 + 1) \times 2^7 + 2^4 + 2^3 + 2 \\ &= (2 + 1) \times 2^8 + 2^7 + 2^4 + 2^3 + 2 \\ &= 2^9 + 2^8 + 2^7 + 2^4 + 2^3 + 2 \\ &= 1110011010_b \end{aligned}$$

❑ Convertir en base $b = 2$ ou $h = 16$ l'entier décimal 125 624

$$
\begin{aligned}
125\,624 &= 2^2 \times 31406 = 2^3 \times 15703 \\
&= 2^3 + 2^3 \times 15702 = 2^3 + 2^4 \times 7851 \\
&= 2^3 + 2^4 + 2^4 \times 7850 = 2^3 + 2^4 + 2^5 \times 3925 \\
&= 2^3 + 2^4 + 2^5 + 2^5 \times 3924 = 2^3 + 2^4 + 2^5 + 2^7 \times 981 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^7 \times 980 = 2^3 + 2^4 + 2^5 + 2^7 + 2^9 \times 245 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^9 \times 244 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} \times 61 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{11} \times 60 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} \times 15 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{13} \times 14 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} \times 7 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} + 2^{14} \times 6 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} + 2^{15} \times 3 \\
&= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} + 2^{15} + 2^{16} \\
&= 1\ 1110\ 1010\ 1011\ 1000_b \\
&= 1\ \mathrm{EAB8}_h
\end{aligned}
$$

❑ Voici maintenant un exemple d'addition directement en base $h = 16$.

$$
\begin{array}{r}
14\mathrm{ED}_h \\
+\ 27\mathrm{F}_h \\
\hline
= 176\mathrm{C}_h
\end{array}
$$

II : L'anneau ℤ

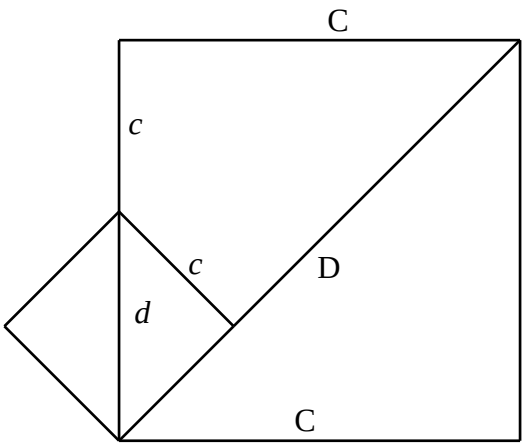
1- Diviseurs communs, PGCD

On appelle **diviseur commun** de deux entiers non nuls a et b un nombre d tel que d divise a et d divise b. On s'intéresse en particulier au plus grand d'entre eux, le **PGCD** (plus grand commun diviseur), et on le note PGCD(a, b) ou $a \wedge b$. Cette notion intervient couramment quand on cherche à simplifier une fraction rationnelle. Il est en effet avantageux de diviser numérateur et dénominateur par leur PGCD.

A noter que les Grecs se posaient un problème comparable pour des grandeurs quelconques. Le problème était le suivant : étant données deux grandeurs A et B (longueurs, aires, mais aussi entiers), trouver une quantité X dite *mesure commune* à A et B, i.e. trouver X tel que A et B soient des multiples entiers de X. A l'époque pythagoricienne (VI^{ème} siècle avant J.C.) l'existence de X ne faisait pas de doute. Un algorithme pour trouver X existait probablement déjà. Il est clairement exposé dans les *Eléments* d'Euclide (315-255 avant J.C.) :

> Si A > B, retrancher B de A autant de fois que possible.
> S'il reste une quantité R à A, recommencer sur B et R.
> S'il ne reste rien, X est la plus petite des deux quantités considérées.

Pour des quantités A et B quelconques, on peut se poser la question de savoir si l'algorithme se termine. Si oui, les quantités A et B sont dites *commensurables* (Aujourd'hui, on dirait A/B est rationnel), sinon, elles sont *incommensurables* (A/B est irrationnel). La découverte de grandeur incommensurable a été un événement marquant des mathématiques grecques. Prenons par exemple le cas de $\sqrt{2}$.



Prenons un petit carré de côté c et de diagonale d, et construisons un grand carré dont le côté a pour longueur C = $d + c$. Soit D sa diagonale. On a :

C = $c + d$

D = $2c + d$ (car $D^2 = 2C^2 = 2c^2 + 4cd + 2d^2 = (2c + d)^2$ puisque $d^2 = 2c^2$)

On va chercher la mesure commune à A = C + D et à B = C. On voit que C va deux fois dans C + D. Donc le premier quotient est égal à 2. Le premier reste R est c car :

$$R = C + D – 2C = D – C = c$$

On est donc maintenant amené à comparer B = C et R = c, c'est-à-dire $c + d$ et c. Ainsi, ayant fait l'opération une fois sur C + D et C, on trouve pour quotient 2, et les deux nouvelles quantités à considérer sont $c + d$ et c. On se retrouve dans la même situation car, par homothétie, les deux rapports sont égaux. Par conséquent, les quotients successifs valent tous 2, jusqu'à l'infini. Ceci démontre que le rapport est irrationnel.

PROPOSITION

Pour deux entiers non nuls, l'algorithme d'Euclide se termine nécessairement et donne le PGCD.

Démonstration :

❑ Soient deux entiers strictement positifs a et b. L'algorithme d'Euclide consiste successivement à diviser a par b, puis b par le reste obtenu précédemment, puis les deux restes entre eux, etc.... Commençons par un exemple. Pour a = 1236 et b = 96, on obtient successivement :

1236	96	$1236 = 96 \times 12 + 84$
96	84	$96 = 84 + 12$
84	12	$84 = 12 \times 7$

Sur cet exemple, on observe bien que la *mesure commune* à 1236 et 96 est 12. 12 est le PGCD cherché.

Plus généralement :

Soit a et b deux entiers, $a > b > 0$. On a, par divisions euclidiennes successives :

$a = bq_1 + r_1$ avec $0 \leq r_1 < b$

$b = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$

$r_1 = r_2q_3 + r_3$ avec $0 \leq r_3 < r_2$

...

$r_{n-1} = r_nq_{n+1} + r_{n+1}$ avec $0 \leq r_{n+1} < r_n$

jusqu'à obtenir un reste nul (par exemple r_{n+1}). L'algorithme est nécessairement fini, sinon (r_n) formerait une suite strictement décroissante d'entiers positifs ou nuls, ce qu'on sait impossible. Montrons que le dernier reste calculé r_n est le PGCD :

❑ r_n divise a et b. En effet, r_n divise r_{n-1} puisqu'on a $r_{n+1} = 0$. Il se divise également lui-même. Par récurrence descendante, si r_n divise r_{p+1} et r_p, il divise r_{p-1} (car $r_{p-1} = r_p q_{p+1} + r_{p+1}$). Donc r_n divise r_1 et r_2, puis r_1 et b, puis a et b.

❑ Un diviseur d commun à a et b divise également r_1 (car $r_1 = a - bq_1$). Il divise également r_2 (car $r_2 = b - r_1 q_2$). Par récurrence ascendante, si d divise r_{p-1} et r_p, il divise r_{p+1} (car $r_{p+1} = r_{p-1} - q_{p+1} r_p$). d divise donc r_n.

Ainsi, r_n est un diviseur commun à a et à b, et tout diviseur commun à a et b divise r_n. r_n est le plus grand diviseur commun de a et b, au sens de la relation d'ordre de divisibilité.

L'algorithme est le suivant. La fonction *mod* (*mod* pour modulo) donne le reste de la division euclidienne. Dans cet algorithme, la propriété PGCD(A,B) = PGCD(A0, B0) est conservée en permanence au début de chaque itération et s'appelle **invariant de boucle** :

```
lire(A,B)                  # A = A0, B = B0,
                           #        A0 et B0 valeurs initiales.
                           #        PGCD(A,B) = PGCD(A0,B0)
tant que B ≠ 0 faire       # invariant de boucle :  PGCD(A0,B0) = PGCD(A,B)
        R ← A mod B        # PGCD(A0,B0) = PGCD(A,B) = PGCD(B,R) car (A, B) et (B, R) ont
                           #     mêmes diviseurs communs donc même PGCD
        A ← B              # PGCD(A0,B0) = PGCD(A,R)
        B ← R              # PGCD(A0,B0) = PGCD(A,B)
fin faire                  # On quitte la boucle quand B = 0 donc
                           # quand PGCD(A0,B0) = PGCD(A,B) = A
resultat ← A
```

Si $d = 1$, on dit que a et b sont **premiers entre eux**, ce qu'on note $a \wedge b = 1$. On peut également définir le PGCD de n nombres. Si celui-ci vaut 1, ces nombres sont dits **premiers entre eux dans leur ensemble**. Par exemple, 6, 10, 15 sont premiers entre eux dans leur ensemble, mais ne le sont pas deux à deux.

2- Egalité de Bézout

PROPOSITION

(i) *Soit a et b deux entiers non nuls de* PGDC *d. Alors il existe x et y entiers tels que :*

$$ax + by = d$$

(ii) *La condition nécessaire et suffisante pour que a et b soient premiers entre eux est qu'il existe x et y tels que* $ax + by = 1$.

(iii) *Si* $a_1, a_2, ..., a_n$ *sont n entiers non nuls de* PGCD d_n, *il existe* $x_1, x_2, ..., x_n$ *tels que* :

$$a_1x_1 + ... + a_nx_n = d_n$$

En particulier, $a_1, ..., a_n$ *sont premiers entre eux dans leur ensemble si et seulement si il existe* $x_1, x_2, ..., x_n$ *tels que* $a_1x_1 + ... + a_nx_n = 1$.

Démonstration :

❑ (i) On applique l'algorithme d'Euclide sur a et b de façon que, pour tout p :

$r_{p-1} = r_p q_{p+1} + r_{p+1}$

jusqu'à obtenir un reste nul. (r_p) est la suite des restes, (q_p) celle des quotients.
On part de :

$a \times 1 + b \times 0 = a$ de la forme $ax_{-1} + by_{-1} = r_{-1}$ avec $r_{-1} = a$
$a \times 0 + b \times 1 = b$ de la forme $ax_0 + by_0 = r_0$ avec $r_0 = b$
$a - bq_1 = r_1$ de la forme $ax_1 + by_1 = r_1$

Si l'on a :

$ax_{p-1} + by_{p-1} = r_{p-1}$
$ax_p + by_p = r_p$

on retranche q_{p+1} fois la deuxième de la première pour obtenir :

$ax_{p+1} + by_{p+1} = r_{p+1}$

avec $r_{p+1} = r_{p-1} - q_{p+1}r_p$
$x_{p+1} = x_{p-1} - q_{p+1}x_p$
$y_{p+1} = y_{p-1} - q_{p+1}y_p$

Si l'on définit les vecteurs $W_p = (r_p, x_p, y_p)$ avec $W_{-1} = (a, 1, 0)$ et $W_0 = (b, 0, 1)$ alors, les trois égalités précédentes s'interprètent vectoriellement par :

$W_{p+1} = W_{p-1} - q_{p+1}W_p$

Le dernier reste non nul r_n donne le PGCD d, et on a alors $ax_n + by_n = r_n = d$ comme désiré.

❑ (ii) En particulier, si deux entiers a et b sont premiers entre eux, alors $d = 1$ et il existe x et y tels que $ax + by = 1$.
Réciproquement, si cette relation est vérifiée, alors tout diviseur positif de a et b divise $ax + by$ donc divise 1 donc vaut 1, donc le PGCD de a et b est 1, et a et b sont premiers entre eux.

Dans le cas général, on remarquera que, si on pose $a = da'$ et $b = db'$, alors a' et b' sont premiers entre eux. En effet, l'identité de Bézout donne $ax + by = d$, donc $da'x + db'y = d$ donc $a'x + b'y = 1$.

❑ (iii) On procède par récurrence sur n. Le (i) prouve la relation pour $n = 2$. Supposons la relation vérifiée au rang $n - 1$, pour $n > 2$. Soit d_{n-1} le PGCD de $a_1, ..., a_{n-1}$. Remarquons que d_n est le PGCD de d_{n-1} et de a_n. En effet :

Tout diviseur de $a_1, ..., a_n$ divise $a_1, ..., a_{n-1}$ et divise a_n, donc divise d_{n-1} et a_n.
Tout diviseur de d_{n-1} et a_n divise $a_1, ..., a_{n-1}$ et divise a_n, donc divise $a_1, ..., a_n$.

Les diviseurs de (d_{n-1}, a_n) étant les mêmes que les diviseurs de $(a_1, ..., a_n)$, leur PGCD respectif est le même.
Par conséquent, il existe x et y tels que $d_{n-1}x + a_ny = d_n$ d'après le (i), et il existe $y_1, ..., y_{n-1}$ tels que $a_1y_1 + ... + a_{n-1}y_{n-1} = d_{n-1}$ d'après l'hypothèse de récurrence. Donc :

$a_1y_1x + ... + a_{n-1}y_{n-1}x + a_ny = d_n$

et la relation est prouvée au rang n en prenant $x_1 = y_1x, ..., x_{n-1} = y_{n-1}x, x_n = y$.
Une autre démonstration est donnée dans le chapitre L2/ZSURNZ.PDF.
La fin de la proposition (iii) se montre comme le (ii).

EXEMPLES :
❑ $a = 123$ et $b = 27$:

$1 \times a + 0 \times b = 123$ $[L_1]$
$0 \times a + 1 \times b = 27$ $[L_2]$ or $123 = 27 \times 4 + 15$
$\Rightarrow$ $a - 4b = 15$ $[L_3 = L_1 - 4L_2]$ or $27 = 15 \times 1 + 12$
$\Rightarrow$ $-a + 5b = 12$ $[L_4 = L_2 - L_3]$ or $15 = 12 \times 1 + 3$
$\Rightarrow$ $2a - 9b = 3$ $[L_5 = L_3 - L_4]$
dernier calcul puisque 3 divise 12.

L'identité de Bézout est $2a - 9b = 3$.

❑ $a = 123$ et $b = 26$:

	$1 \times a + 0 \times b = 123$	$[L_1]$	
	$0 \times a + 1 \times b = 26$	$[L_2]$	or $123 = 26 \times 4 + 19$
$\Rightarrow$	$a - 4b = 19$	$[L_3 = L_1 - 4L_2]$	or $26 = 19 \times 1 + 7$
$\Rightarrow$	$-a + 5b = 7$	$[L_4 = L_2 - L_3]$	or $19 = 7 \times 2 + 5$
$\Rightarrow$	$3a - 14b = 5$	$[L_5 = L_3 - 2L_4]$	or $7 = 5 + 2$
$\Rightarrow$	$-4a + 19b = 2$	$[L_6 = L_4 - L_5]$	or $5 = 2 \times 2 + 1$
$\Rightarrow$	$11a - 52b = 1$	$[L_7 = L_5 - 2L_6]$	

123 et 26 sont premiers entre eux et l'identité de Bézout correspondante est $11a - 52b = 1$.

❑ $a_1 = 143$, $a_2 = 77$ et $a_3 = 91$.

On commence par traiter $a_1 = 143$ et $a_2 = 77$:

	$1 \times a_1 + 0 \times a_2 = 143$	$[L_1]$	
	$0 \times a_1 + 1 \times a_2 = 77$	$[L_2]$	or $143 = 77 + 66$
$\Rightarrow$	$a_1 - a_2 = 66$	$[L_3 = L_1 - L_2]$	or $77 = 66 + 11$
$\Rightarrow$	$-a_1 + 2a_2 = 11$	$[L_4 = L_2 - L_3]$	

Comme 11 divise 66, on a prouvé que $77 \wedge 143 = 11 = d_2$ avec l'identité de Bézout :

$$-a_1 + 2a_2 = d_2 = 11$$

On traite ensuite $a_3 = 91$ et $d_2 = 11$:

	$1 \times a_3 + 0 \times d_2 = 91$	$[L_1]$	
	$0 \times a_3 + 1 \times d_2 = 11$	$[L_2]$	or $91 = 11 \times 8 + 3$
	$a_3 - 8d_2 = 3$	$[L_3 = L_1 - 8L_2]$	or $11 = 3 \times 3 + 2$
	$-3a_3 + 25d_2 = 2$	$[L_4 = L_2 - 3L_3]$	or $3 = 2 + 1$
	$4a_3 - 33d_2 = 1$	$[L_5 = L_3 - L_4]$	

On a prouvé que PGCD(143, 77, 91) = 1. L'identité de Bézout correspondante est :

$$1 = 4a_3 - 33d_2 = 4a_3 - 33(-a_1 + 2a_2) = 33a_1 - 66a_2 + 4a_3$$

Un algorithme de l'identité de Bézout est le suivant :

X1,Y1,X2,Y2	sont des entiers, coefficients utilisés dans deux lignes successives de calcul
R,Q	sont des entiers, reste et quotient provisoires
Temp	est un entier, variable temporaire de transfert

Les commentaires prouvent la validité de l'algorithme.

```
lire(A,B)                          # A = A0, B = B0, valeurs initiales
                                   # PGCD(A0,B0) = PGCD(A,B)
X1 ← 1
Y1 ← 0                             # A0.X1 + B0.Y1 = A
X2 ← 0
Y2 ← 1                             # A0.X2 + B0.Y2 = B
tant que B ≠ 0 faire               # Les invariants de boucles sont :
                                   # A0.X1 + B0.Y1 = A
                                   # A0.X2 + B0.Y2 = B
                                   # PGCD(A0,B0) = PGCD(A,B)
    R ← A mod B
    Q ← A//B                       # on convient de noter ici par // le quotient de A par B
    Temp ← X1                      # A0.X1 + B0.Y1 = A et Temp = X1
                                   # A0.X2 + B0.Y2 = B
    X1 ← X2                        # A0.Temp + B0.Y1 = A
```

	# A0.X1 + B0.Y2 = B et X1 = X2
X2 ← Temp – X1*Q	# A0.Temp + B0.Y1 = A
	# A0.X1 + B0.Y2 = B et X2 = Temp – X1.Q
	# ce qui implique :
	# A0.Temp + B0.Y1 = A
	# A0.X1 + B0.Y2 = B
	# A0.X2 + A0.X1.Q + B0.Y1 = A
Temp ← Y1	# Temp = Y1
	# A0.X1 + B0.Y2 = B
	# A0.X2 + A0.X1.Q + B0.Temp = A
Y1 ← Y2	# Y1 = Y2
	# A0.X1 + B0.Y1 = B
	# A0.X2 + A0.X1.Q + B0.Temp = A
Y2 ← Temp – Y1*Q	# Y2 = Temp – Y1.Q
	# A0.X1 + B0.Y1 = B
	# A0.X2 + A0.X1.Q + B0.Y2 + B0.Y1.Q = A
	# ce qui implique
	# A0.X2 + B0.Y2 = A – B.Q = R
	# PGCD(A0,B0) = PGCD(A,B) = PGCD(B,R)
A ← B	# A0.X1 + B0.Y1 = A
	# A0.X2 + B0.Y2 = R
	#PGCD(A0,B0) = PGCD(A,R)
B ← R	# A0.X1 + B0.Y1 = A
	# A0.X2 + B0.Y2 = B
	# PGCD(A0,B0) = PGCD(A,B)
jusqu'à B = 0	# lorsque B = 0, le PGCD est A.

On a bien obtenu les coefficients (X1, Y1) de l'égalité de Bézout

3- Le théorème de Gauss

PROPOSITION

Soit trois entiers non nuls a,b et c tels que c | ab, et que c ∧ a = 1. Alors c | b.

Démonstration :

❑ Puisque $c \wedge a = 1$, il existe x et y tels que $ax + cy = 1$ donc $abx + bcy = b$ or $\exists\, q$, $ab = cq$ donc $b = c(qx + by)$ donc c divise b.

COROLLAIRES

(i) Si on a une solution (x, y) à l'identité de Bézout relative à (a, b), comment s'obtiennent les autres ? Soit a' tel que $a = da'$ et b' tel que $b = db'$, avec $d = a \wedge b$. On a alors $a' \wedge b' = 1$. Soit (x', y') une autre solution de l'identité de Bézout. On a :

$$\begin{cases} ax + by = d \\ ax' + by' = d \end{cases} \Rightarrow \begin{cases} a'x + b'y = 1 \\ a'x' + b'y' = 1 \end{cases}$$

$\Rightarrow$ $a'(x' - x) = b'(y - y')$. Donc $a' \mid b'(y - y')$, or $a' \wedge b' = 1$, donc $a' \mid y - y'$. Il existe donc k tel que $y = y' + ka'$. En remplaçant dans l'égalité $a'(x' - x) = b'(y - y')$, on obtient $x' = x + kb'$. Les solutions sont donc nécessairement de la forme $x' = x + kb'$ et $y' = y - ka'$, et réciproquement, de tels nombres sont bien solutions car :

$$a(x + kb') + b(y - ka') = d$$

puisque $ab' - ba' = d(a'b' - b'a') = 0$.

Le raisonnement précédent appliqué à $a = 123 = 3 \times 41$ et $b = 27 = 3 \times 9$ pour qui $2a - 9b = 3$ donnera :

$$a(2 + 9k) - b(9 + 41k) = 3$$

(ii) $\forall\, n \in \mathbb{Z}, a \wedge b = a \wedge (b + na)$

En effet, un diviseur commun a a et b est diviseur commun à a et $b + na$, et inversement. Donc le le plus grand diviseur commun est le même pour les deux membres. Cette règle permet parfois de calculer le PGCD de deux nombres plus vite qu'avec l'algorithme d'Euclide. Par exemple, par l'algorithme d'Euclide, on a :

$$144 \wedge 89 = 89 \wedge 55 = 55 \wedge 34 = 34 \wedge 21 = 21 \wedge 13 = 13 \wedge 8 = 8 \wedge 5$$
$$= 5 \wedge 3 = 3 \wedge 2 = 2 \wedge 1 = 1$$

alors que :

$144 \wedge 89 = 89 \wedge 34$ obtenu en remplaçant 144 par $2 \times 89 - 144 = 34$
$= 34 \wedge 13$ obtenu en remplaçant 89 par $3 \times 34 - 89 = 13$
$= 13 \wedge 5$ obtenu en remplaçant 34 par $3 \times 13 - 34 = 5$
$= 5 \wedge 2$ obtenu en remplaçant 13 par $3 \times 5 - 13 = 2$
$= 2 \wedge 1$ obtenu en remplaçant 5 par $5 - 2 \times 2 = 1$
$= 1$

soit cinq calculs au lieu de neuf.

(iii) $\left[\begin{array}{l} a \wedge b = 1 \\ c \text{ divise } a \end{array}\right. \Rightarrow c \wedge b = 1$

En effet, il existe d tel que $a = dc$, et il existe u et v tel que :

$$au + bv = 1$$

donc $cdu + bv = 1$

donc $c \wedge b = 1$

(iv) $c \wedge a = 1 \Rightarrow a \wedge b = a \wedge (bc)$

En effet, un diviseur commun de a et b est évidemment diviseur commun de a et bc. Inversement, soit d diviseur commun de a et bc. On a, d'après la propriété précédente $d \wedge c = 1$. Or d divise bc. Il résulte du théorème de Gauss que d divise b. Ainsi a et b ont mêmes diviseurs communs que a et bc et donc même PGCD. Cette règle permet également d'accélérer les calculs de PGCD. Par exemple :

$$144 \wedge 89 = (4 \times 36) \wedge 89$$

or $4 \wedge 89 = 1$ donc le PGCD cherché est égal à $36 \wedge 89$, ou à $9 \wedge 89 = 1$.

(v) Si a est premier avec n nombres $b_1, b_2, ..., b_n$, alors a est premier avec leur produit

Par récurrence sur k, on a :

$$a \wedge b_1...b_k = 1$$

Cette propriété est vraie pour $k = 1$. Soit k quelconque. Supposons que $a \wedge b_1...b_k = 1$. Alors $a \wedge b_1...b_k b_{k+1} = a \wedge b_1...b_k = 1$ puisque $a \wedge b_{k+1} = 1$ (en utilisant la règle (iv) ci-dessus).

(vi) Si a est divisible par $b_1, b_2, ..., b_n$ est que les b_i sont premiers entre eux deux à deux, alors a est divisible par le produit des b_i.

$a = b_1 q_1$ et donc $b_1 q_1$ est divisible par b_2. Or b_1 est premier avec b_2 donc b_2 divise q_1 d'après le théorème de Gauss. Donc il existe q_2 tel que $q_1 = b_2 q_2$ et $a = b_1 b_2 q_2$. Par récurrence, supposons que $a = b_1 b_2 ... b_k q_k$. b_{k+1} divise a donc divise $b_1 b_2 ... b_k q_k$, mais b_{k+1} est premier avec $b_1 b_2 ... b_k$ (d'après v) donc, d'après le théorème de Gauss, b_{k+1} divise q_k donc il existe q_{k+1} tel que $q_k = b_k q_{k+1}$ et $a = b_1 b_2 ... b_{k+1} q_{k+1}$. On itère jusqu'a $k = n$.

(vii) $b \wedge c = 1 \Rightarrow a \wedge bc = (a \wedge b) \times (a \wedge c)$

Soit $d = a \wedge bc$, $q = a \wedge b$ et $r = a \wedge c$. Il existe u, v, x, y tels que :

$ax + by = q$

$au + cv = r$

donc $(ax + by)(au + cv) = qr = a(axu + xcv + byu) + bcvy$ quantité de la forme aX + bcY. Donc qr est un multiple de d car d divise aX + bcY.

Par ailleurs, q divise a et b, donc divise a et bc donc divise d. De même, r divise d. Enfin, q est premier avec r car un diviseur commun de q et r est aussi un diviseur commun de b (que divise q) et de c (que divise r), or $b \wedge c = 1$. Comme q et r divise d et sont premiers entre eux, qr divise d (d'après v ci-dessus).

Donc $qr = d$.

(viii) Si *a* et *b* sont premiers entre eux, alors, pour tout *m* et *p*, a^m et b^p sont premiers entre eux.

$a \wedge b = 1$, donc en appliquant (v) sur p fois b, on obtient $a \wedge b^p = 1$, puis en appliquant m fois (v) sur a, on obtient $a^m \wedge b^p = 1$.

On appelle **nombre premier** tout entier naturel strictement supérieur à 1, divisible uniquement par 1 et par lui–même. Les premiers entiers premiers sont :

2 3 5 7 11 13 17 19 23 29 31 37 41 ...

Un nombre qui n'est pas premier est dit **composé**.

(ix) Si p_1, ..., p_k sont des nombres premiers distincts, et si $p_i^{n_i}$ divise *a*, alors *a* est divisible par le produit.

Le (ix) est une application directe du (vi), en remarquant que les $p_i^{n_i}$ sont premiers entre eux deux à deux d'après (viii).

Par exemple : 4 divise n et 9 divise $n \Rightarrow$ 36 divise n.

(x) Si *p* est premier et ne divise pas *a*, alors *p* et *a* sont premiers entre eux.

Un diviseur commun à a et p est un diviseur de p, donc vaut 1 ou p. Or ce n'est pas p, donc c'est 1.

(xi) Si *p* est premier et divise un produit de facteurs, alors *p* divise l'un des facteurs.

Sinon, p serait premier avec chacun des facteurs, donc avec le produit d'après (v). Si on raisonne modulo p (i.e. à un multiple entier de p près), cela se traduit de la façon suivante : si un produit de facteurs est nul modulo p premier, alors l'un des facteurs est nul modulo p. On cherchera un exemple prouvant que ce résultat est faux si p n'est pas premier.

Voici une application qui généralise l'irrationalité de $\sqrt{2}$. Soit n entier. Alors $\sqrt{n}$ est soit irrationnel (par exemple $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, ...), soit entier (par exemple $\sqrt{16}$, $\sqrt{25}$ ...)

En effet, si $\sqrt{n}$ est rationnel, égal à $\frac{a}{b}$ avec $\frac{a}{b}$ qu'on peut supposer irréductible, on a $nb^2 = a^2$. Or a est premier avec b, donc (d'après viii) a^2 est premier avec b^2. Mais b^2 divise a^2. Donc le PGCD de a^2 et b^2 est égal d'une part à 1, d'autre part à b^2. Ainsi $b^2 = 1$, $n = a^2$ et $\sqrt{n}$ est entier.

4- PPCM

On appelle **multiple commun** de deux entiers a et b un entier m qui est multiple de a et multiple de b. On s'intéresse au plus petit d'entre eux, le **PPCM** (plus petit commun multiple). Le PPCM intervient couramment quand on cherche à additionner deux rationnels. Il est intéressant de minimiser le dénominateur final en prenant comme dénominateur commun le PPCM des dénominateurs des deux fractions.

PROPOSITION
Soit m le PPCM *et d le* PGCD *de a et b. Alors ab = md.*

Démonstration :

❑ Posons $a = da'$, et $b = db'$ avec $a' \wedge b' = 1$. Posons $m = \frac{ab}{d} = da'b' = ab' = ba'$. On a donc m multiple commun à a et à b.
Soit maintenant n multiple de a et b. Il existe x et y tels que :

$n = ax = by \Leftrightarrow n = da'x = db'y \Rightarrow a'x = b'y$

Ainsi, b' divise $a'x$. Or b' est premier avec a'. Donc b' divise x. Il existe donc q tel $x = b'q$ donc $a'x = a'b'q$ donc $n = da'b'q = mq$. Donc tout multiple commun n de a et b est multiple de m. m est bien le plus petit multiple commun.

Le PPCM de a et b est noté PPCM(a, b) ou $a \vee b$.

On notera que si a et b sont premiers entre eux, le PGCD vaut 1 et le PPCM vaut ab.

5- Les nombres premiers

PROPOSITION
Tout entier naturel supérieur strictement à 1 *se décompose de manière unique (à commutativité près) en le produit (éventuellement réduit à un seul terme) de nombres premiers.*

Démonstration :

❑ Par récurrence : on suppose que tout entier inférieur ou égal à n se décompose en produits de facteurs premiers (ce qui est vrai pour $n \leq 2$). Considérons $n + 1$.

Si $n + 1$ est premier, alors $n + 1 = n + 1$ est une décomposition.

Sinon, $n + 1 = ab$, avec $1 < a < n + 1$, et $1 < b < n + 1$. L'hypothèse de récurrence s'applique sur a et b, qui se décomposent donc en produits de facteurs premiers. Il en est donc de même de $n + 1$.

❑ Montrons l'unicité de la décomposition. Si :

$p_1^{r_1}...p_n^{r_n} = p_1^{s_1}...p_n^{s_n}$ avec $r_i \geq 0$ et $s_i \geq 0$ (on complète éventuellement les deux membres par des p_i^0 pour avoir les mêmes facteurs premiers dans les deux membres). $p_1^{r_1}$ divise le membre de droite, mais est premier avec p_2, ..., p_n donc avec $p_2^{s_2}...p_n^{s_n}$, donc, d'après le théorème de Gauss, $p_1^{r_1}$ divise $p_1^{s_1}$, donc $r_1 \leq s_1$. Symétriquement, $s_1 \leq r_1$. Ainsi $s_1 = r_1$, et de même pour les autres puissances.

PROPOSITION
Si $a = p_1^{r_1}...p_n^{r_n}$ et $b = p_1^{s_1}...p_n^{r_n}$, *où les* p_i *sont des nombres premiers, alors* :

le PGCD *est égal à* $p_1^{t_1}...p_n^{t_n}$, *où* $t_i = \text{Min}(s_i, r_i)$.

le PPCM *est égal à* $p_1^{t_1}...p_n^{t_n}$, *où* $t_i = \text{Max}(s_i, r_i)$.

Par exemple :

$156 = 2^2 \times 3 \times 13$

$24 = 2^3 \times 3$

Donc le PGCD vaut $2^2 \times 3 = 12$; $156 = 12 \times 13$ et $24 = 12 \times 2$

le PPCM vaut $2^3 \times 3 \times 13 = 312 = 156 \times 2 = 24 \times 13$

La puissance de p intervenant dans la décomposition d'un nombre n s'appelle **valuation p-adique** de n, votée $v_p(n)$. Les notations précédentes se traduisent donc sous la forme :

$v_p(a \wedge b) = \text{Min}(v_p(a), v_p(b))$ pour tout facteur premier p

$v_p(a \vee b) = \text{Max}(v_p(a), v_p(b))$

Démonstration :

❑ Soit $d = p_1^{t_1}...p_n^{t_n}$. Comme, pour tout i, $t_i \le r_i$ et $t_i \le s_i$, il est clair que d divise a et b. Montrons que c'est le plus grand diviseur. Considérons un diviseur q quelconque et décomposons-le en facteurs premiers. Comme q divise a, pour tout nombre premier p, $p^{v_p(q)}$ divise q donc divise a, donc $p^{v_p(q)}$ divise $p^{v_p(a)}$ donc $v_p(q) \le v_p(a)$. De même $v_p(q) \le v_p(b)$. Donc $v_p(q) \le \text{Min}(v_p(a), v_p(b)) = v_p(d)$. Le même raisonnement ayant lieu pour tout facteur premier p, on a q diviseur de d.

❑ Si $m = \text{PPCM}(a, b)$, comme $m = \frac{ab}{d}$, on a, pour tout p premier :

$v_p(m) = v_p(a) + v_p(b) - v_p(d) = v_p(a) + v_p(b) - \text{Min}(v_p(a), v_p(b)) = \text{Max}(v_p(a), v_p(b))$

comme on le vérifiera aisément

PROPOSITION

L'ensemble des nombres premiers est infini.

Démonstration :

❑ La démonstration est connue depuis Euclide. En effet, soit p_1, ..., p_n n nombres premiers. Montrons qu'il en existe nécessairement un autre. On considère la quantité $p_1p_2...p_n + 1$. Soit q un nombre premier divisant cette quantité. Alors q est nécessairement différent de tous les p_i. Car s'il existe i tel que $q = p_i$, q divise $p_1p_2...p_n$ d'une part, et divise $p_1p_2...p_n + 1$ d'autre part, donc divise la différence 1, ce qui est impossible. Ainsi, la famille de nombres premiers ne peut être finie.

On notera qu'il se peut que $p_1p_2...p_n + 1$ lui–même soit premier. En fait, on ignore si la quantité $p_1p_2...p_n + 1$ prend une infinité de fois une valeur première, ou si elle prend une infinité de fois une valeur non première. Par ailleurs, si $p_1 = 2$ et si on pose p_n le plus petit premier diviseur de $p_1p_2...p_{n-1} + 1$, on construit une suite infinie de nombres premiers distincts deux à deux . Voici les premiers termes de la suite :

2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17,...

On conjecture que tous les nombres premiers apparaissent dans la liste ci-dessus. La même conjecture s'applique également à la variante suivante : on prend $q_1 = 3$ et on définit q_n comme le plus petit premier de la suite $q_1q_2...q_{n-1} - 1$ dont les premiers termes sont :

3, 2, 5, 29, 11, 7, 13, 37, 32222189, 131, 136013303998782209, 31, 197, 19, 157, 17...

Les démonstrations de l'infinitude des nombres premiers sont innombrables. En voici une autre, datant de 1955 (preuve de Furstenberg[1]). Pour tout a et b entiers, notons $a + b\mathbb{Z} = \{a + nb, n \in \mathbb{Z}\}$. Pour tout entier n, l'ensemble des non-multiples de n est :

$\text{NM}(n) = \{m \mid n \text{ ne divise pas } m\} = (1 + n\mathbb{Z}) \cup (2 + n\mathbb{Z}) \cup ... \cup (n - 1 + n\mathbb{Z})$

[1] Voir H. Furstenberg, On the infinitude of primes, Amer. Math. Monthly, 62:5 (1955), 353, et I. D. Mercer, On Furstenberg's proof of the infinitude of primes, Amer. Math. Monthly, 116:4 (2009), 355-356.

On note par ailleurs que, pour toute famille finie (r_i) et (n_i), $i \in I$, n_i étant non nuls, $\bigcap_{i\in 1} (r_i + n_i\mathbf{Z})$ est vide ou infinie. Car si x appartient à cette intersection, alors il en est de même de tous les $x + k\prod_{i\in I} n_i$, $k \in \mathbf{Z}$. Supposons maintenant que la famille des nombres premiers soit une famille finie P. L'ensemble $\bigcap_{p\in P}$ NM(p) est constituée des entiers multiples d'aucun nombre premier. Il s'agit donc simplement de l'ensemble constitué des deux éléments {–1, 1}. Mais on a également :

$$\bigcap_{p\in P} \mathrm{NM}(p) = \bigcap_{p\in P} \bigcup_{k=1}^{p-1} (k + p\mathbf{Z})$$

Or $\cap$ est distributif par rapport à $\cup$ de sorte qu'une intersection finie de réunion finie de $k + p\mathbf{Z}$ est également une réunion finie d'une intersection finie de tels ensembles. Mais nous avons vu qu'une telle intersection est vide ou infinie. Il en est a fortiori de même pour la réunion qui, vide ou infinie, ne peut en aucun cas être égale à {–1, 1}.

Les records de nombres premiers sont (entre 1983 et 2024) :

$2^{86243} - 1$	qui possède 25 962 chiffres	(1983)
$2^{132049} - 1$	qui possède 39 751 chiffres	(1984)
$2^{216091} - 1$	qui possède 65 050 chiffres	(1985)
$391581 \times 2^{216193} - 1$	qui possède 65 087 chiffres	(1989)
$2^{756839} - 1$	qui possède 227 832 chiffres	(1992)
$2^{859433} - 1$	qui possède 258 716 chiffres	(1994)
$2^{1257787} - 1$	qui possède 378 632 chiffres	(1996)
$2^{1398269} - 1$	qui possède 420 921 chiffres	(1996)
$2^{2976221} - 1$	qui possède 895 932 chiffres	(1997)
$2^{3021377} - 1$	qui possède 909 526 chiffres	(1998)
$2^{6972593} - 1$	qui possède 2 098 960 chiffres	(1999)
$2^{13466917} - 1$	qui possède 4 053 946 chiffres	(2001)
$2^{20996011} - 1$	qui possède 6 320 430 chiffres	(2003)
$2^{24036583} - 1$	qui possède 7 235 733 chiifres	(2004)
$2^{25964951} - 1$	qui possède 7 816 230 chiffres	(2005)
$2^{30402457} - 1$	qui possède 9 152 052 chiffres	(2005)
$2^{32582657} - 1$	qui possède 9 808 358 chiffres	(2006)
$2^{43112609} - 1$	qui possède 12 978 189 chiffres	(2008)
$2^{57885161} - 1$	qui possède 17 425 170 chiffres	(2013)
$2^{74207281} - 1$	qui possède 22 338 618 chiffres	(2016)
$2^{77232917} - 1$	qui possède 23 249 425 chiffres	(2017)
$2^{82589933} - 1$	qui possède 24 862 048 chiffres	(2018)
$2^{136279841} - 1$	qui possède 41 024 320 chiffres	(2024)

Cette progression traduit à la fois les progrès des algorithmes utilisés et des moyens de calculs. On pourra consulter le site internet https://www.mersenne.org pour de plus amples renseignements. On voit que la plupart de ces nombres sont de la forme $2^n - 1$. Ce sont les **nombres de Mersenne**, pour lesquels Lucas a défini au XIXème un algorithme efficace permettant de déterminer leur primalité. Voir l'annexe I.

6- Le petit théorème de Fermat

Il s'énonce comme suit :

THEOREME

Soit p premier et a non multiple de p. Alors $a^{p-1} \equiv 1 \bmod p$.

On rappelle que la notation $x \equiv y \bmod p$ signifie : $\exists\, k \in \mathbb{Z},\ x = y + kp$.

On peut aussi énoncer le théorème de Fermat sous la forme suivante :

$$\forall\ a,\ a^p \equiv a \bmod p.$$

Cette deuxième formulation est équivalente à la première car $a^p \equiv a \bmod p$ signifie que p divise $a^p - a$ et donc divise $a(a^{p-1} - 1)$. Donc, si a est non multiple de p et donc premier avec lui, le théorème de Gauss permet de conclure que p divise $a^{p-1} - 1$.

Démonstration :

❑ La relation $a^p \equiv a \bmod p$ se montre par exemple par récurrence sur a. Elle est vraie pour $a = 1$, et si elle est vraie pour un nombre a, on a :

$$(a+1)^p = \sum_{k=0}^{n} \binom{p}{k} a^k = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

Or $\binom{p}{k} = \dfrac{p(p-1)...(p-k+1)}{k!}$ est un entier donc $k!$ divise $p(p-1)...(p-k+1)$. Par ailleurs $p > k$ donc p ne divise aucun nombre inférieur ou égal à k, donc p est premier avec tous les nombres inférieurs ou égaux à k donc p est premier avec leur produit $k!$. Puisque $k!$ divise $p(p-1)...(p-k+1)$ et que $k!$ est premier avec p, $k!$ divise $(p-1)...(p-k+1)$. Donc $\binom{p}{k} = p \times$ un entier, donc $\binom{p}{k} \equiv 0 \bmod p$. Il en résulte que :

$(a+1)^p \equiv a^p + 1 \bmod p \equiv a + 1 \bmod p$ en appliquant l'hypothèse de récurrence.

On consultera l'annexe III sur les tests de primalité pour voir comment on utilise ce théorème de Fermat dans la recherche de nombres premiers.

III : L'anneau des polynômes $\mathbb{K}[X]$

Les propriétés des polynômes sont en tout point comparables à celles des entiers. C'est pour cette raison que ce paragraphe a été placé dans le chapitre L1/ARITHMTQ.PDF et non dans le chapitre L1/POLYNOME.PDF.

Rappelons qu'il existe une division euclidienne dans les polynômes (voir L1/POLYNOME.PDF) :

Soient A *et* B *deux polynômes tel que* $B \neq 0$. *Alors il existe un unique couple* (Q, R) *de polynômes tels que :*

$$A = BQ + R,\ \deg(R) < \deg(B)$$

Q *est le quotient,* R *est le reste.*

Cette division euclidienne permet de prouver les mêmes propriétés arithmétiques que celles montrées pour les entiers.

1- Algorithme du calcul du PGCD

On cherche le polynôme plus grand diviseur commun à deux polynômes A et B, le plus grand signifiant pour le moment de degré maximal. L'algorithme d'Euclide, appliqué à deux entiers, admet une traduction pour les polynômes. Cherchons le PGCD de $X^3 + 2X^2 - X - 2$ et de $X^2 + 4X + 3$. On a :

$$X^3 + 2X^2 - X - 2 = (X^2 + 4X + 3)(X - 2) + 4X + 4$$

$$X^2 + 4X + 3 = (4X + 4)(\frac{X}{4} + \frac{3}{4})$$

Le PGCD est donc 4X + 4, ou plutôt X + 1, l'habitude étant de donner le polynôme normalisé ou unitaire, i.e. celui dont le coefficient du terme de plus haut degré vaut 1. Prouvons que la démarche suivie donne bien le PGCD. La démonstration pourra être comparée avec ce qui se passe dans **Z**.

Soient A et B deux polynômes. On a, par divisions euclidiennes successives :

$A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$

$B = R_1Q_2 + R_2$ avec $\deg(R_2) < \deg(R_1)$

$R_1 = R_2Q_3 + R_3$ avec $\deg(R_3) < \deg(R_2)$

...

$R_{n-1} = R_nQ_{n+1} + R_{n+1}$ avec $\deg(R_{n+1}) < \deg(R_n)$

jusqu'à obtenir un reste nul (par exemple R_{n+1}). L'algorithme est nécessairement fini, sinon ($\deg(R_n)$) formerait une suite strictement décroissante d'entiers, ce qui est impossible. Le dernier reste calculé R_n est le PGCD. La démonstration est identique à celle des entiers.

Le PGCD est en fait défini à une constante non nulle multiplicative près. On choisit donc le polynôme unitaire correspondant. Le qualificatif de *plus grand* s'applique non seulement au sens de *diviseur commun de plus haut degré* mais également aussi au sens de *diviseur commun multiple de tout autre diviseur commun*, comme pour les entiers.

Si D = 1, on dit que A et B sont **premiers entre eux**. On peut également définir le PGCD de *n* polynômes. Si celui-ci vaut 1, ces polynômes sont dits **premiers entre eux dans leur ensemble**. C'est le cas par exemple de (X + 1)(X + 2), (X + 1)(X + 3), (X + 2)(X + 3).

On appelle **polynôme irréductible** tout polynôme de degré supérieur ou égal à 1, divisible uniquement par 1 et par lui–même (à une constante multiplicative près). Les polynômes irréductibles jouent dans $\mathbb{K}[X]$ le même rôle que les nombres premiers dans **Z**.

2- Egalité de Bézout

Il existe une identité de Bézout en tout point comparable à celle des entiers.

PROPOSITION

(i) *Soit* A *et* B *deux polynômes. Il existe* P *et* Q *polynômes tels que :*

$$AP + BQ = D$$

où D *est le* PGCD *de* A *et* B.

(ii) *La condition nécessaire et suffisante pour que* A *et* B *soient premiers entre eux est qu'il existe* P *et* Q *tels que* AP + BQ = 1.

(iii) *Si* $A_1, A_2, ..., A_n$ *sont n polynômes de* PGCD D_n, *il existe des polynômes* $P_1, P_2, ..., P_n$ *tels que* :

$$A_1P_1 + ... + A_nP_n = D_n$$

En particulier, A_1, ..., A_n *sont premiers entre eux dans leur ensemble si et seulement si il existe* P_1, P_2, ..., P_n *tels que* $A_1P_1 + ... + A_nP_n = 1$.

On remarquera que, si on pose A = DA' et B = DB', alors A' et B' sont premiers entre eux.

Il suffit de reprendre la démonstration donnée dans $\mathbb{Z}$, qui s'adapte mot à mot.

EXEMPLE :

❑ $A = X^4 + X^3 - 2X + 1$ et $B = X^2 + X + 1$. On a:

L_0 $A + 0B = X^4 + X^3 - 2X + 1$

L_1 $0A + B = X^2 + X + 1$ or $X^4+X^3-2X+1 = (X^2+X+1)(X^2-1) - X + 2$

L_2 $A - (X^2 - 1)B = - X + 2$ or $X^2+X+1 =(-X+2)(-X-3) + 7$

L_3 $(X + 3)A - (X^3 + 3X^2 - X - 4)B = 7$

On a fait :

$L_2 = L_0 - (X^2 - 1)L_1$

$L_3 = L_1 - (- X - 3)L_2$

Les deux polynômes sont premiers entre eux (en divisant l'égalité L_3 par 7).

3- Le théorème de Gauss

PROPOSITION

Soit trois polynômes A,B *et* C *tels que* C *divise le produit* AB, *et que* C *soit premier avec* A. *Alors* C *divise* B.

Démonstration :

❑ Identique aux entiers. On peut la rappeler rapidement : il existe P et Q tels que AP + CQ = 1 donc ABP + BCQ = B. On voit alors facilement que C divise le premier membre, donc divise B.

Tous les corollaires énoncés dans le cas des entiers s'appliquent ici. Citons par exemple :

(i) *Si* A *est premier avec n polynômes* B_1, B_2, ..., B_n, *alors* A *est premier avec leur produit.*

(ii) *Si* A *est divisible par* B_1, B_2, ..., B_n *est que les* B_i *sont premiers entre eux deux à deux, alors* A *est divisible par le produit des* B_i.

(iii) *Si* P_1, ..., P_k *sont des polynômes irréductibles distincts, et si* $P_i^{n_i}$ *divise* A, *alors* A *est divisible par le produit.*

(iv) *Si* P *est irréductible et ne divise pas* A, *alors* P *et* A *sont premiers entre eux.*

(v) *Si* P *est irréductible et divise un produit de facteurs, alors* P *divise l'un des facteurs.*

Voici une application de ce qui précède :

PROPOSITION

Soit P *un polynôme non nul de degré n. Alors le nombre de ses racines, comptées avec leur ordre de multiplicité est inférieur ou égal à n.*

Démonstration :

❑ Notons les racines a_i, de multiplicité k_i. Alors P est divisible par $(X - a_i)^{k_i}$. Or ces facteurs sont premiers entre eux deux à deux. Donc P est divisible par le produit. Le degré du produit ne pouvant excéder le degré de P, on en déduit que la somme des k_i est inférieure ou égale au degré de P.

COROLLAIRE

Soit P *un polynôme de degré inférieur ou égal à n, et admettant plus de n racines. Alors* P *est nul.*

COROLLAIRE
Soit P *un polynôme à coefficients dans un sous-corps de* $\mathbb{C}$*. Alors, si la fonction polynomiale associée à* P *est identiquement nulle,* P *a tous ses coefficients nuls.*

Démonstration :
❑ Si la fonction polynomiale est nulle, elle admet une infinité de racines. Le polynôme ne peut donc qu'être nul.

4- Les polynômes irréductibles

On rappelle qu'on nomme **polynôme irréductible** tout polynôme de degré supérieur ou égal à 1, divisible uniquement par 1 et par lui–même (à une constante multiplicative près). Voici des exemples de polynômes irréductibles :

Dans $\mathbb{C}[X]$: $X - 2$, $X + i$
Dans $\mathbb{R}[X]$: $X - 2$, $X^2 + 1$
Dans $\mathbb{Q}[X]$: $X - 2$, $X^2 + 1$, $X^2 - 2$

On voit que la condition d'irréductibilité dépend du corps sur lequel on travaille. $X^2 + 1$ est irréductible sur $\mathbb{R}$ ou $\mathbb{Q}$ mais ne l'est pas sur $\mathbb{C}$. $X^2 - 2$ est irréductible sur $\mathbb{Q}$ (car $\sqrt{2}$ est irrationnel), mais ne l'est pas dans $\mathbb{R}$. Dans $\mathbb{C}$, les polynômes irréductibles sont de degré 1. C'est le **théorème de D'Alembert**.

PROPOSITION
Tout polynôme unitaire de degré supérieur ou égal à 1 *se décompose de manière unique (à commutativité près) en produit (éventuellement réduit à un seul terme) de polynômes irréductibles unitaires.*

Démonstration :
❑ Elle peut se faire par récurrence sur le degré du polynôme, d'une façon analogue à celle des entiers. On peut aussi procéder comme suit. Soit E l'ensemble des polynômes n'admettant pas de décomposition. Nous voulons montrer que E est vide. Raisonnons par l'aburde. S'il était non vide, il y aurait un polynôme de plus petit degré A. Si A n'admet pour diviseur que 1 et lui–même, A est irréductible. A = A est une décomposition de A en facteurs premiers, ce qui est contraire à l'hypothèse. Donc A admet au moins deux diviseurs B et C. A étant de degré minimum dans E, B et C ne sont pas éléments de E, et se décomposent donc en produit de facteurs irréductibles. Il en est donc de même de A qui est leut produit, ce qui conduit à une contradiction.

❑ Montrons l'unicité de la décomposition. On procède comme pour les entiers. Si :

$$P_1^{r_1}...P_n^{r_n} = P_1^{s_1}...P_n^{s_n} \text{ avec } r_i \geq 0$$

le théorème de Gauss permet de dire que $P_1^{r_1}$ divise le membre de droite, mais il est premier avec P_2, ..., P_n, donc il divise $P_1^{s_1}$, donc $r_1 \leq s_1$. Symétriquement, $s_1 \leq r_1$. Ainsi $s_1 = r_1$, et de même pour les autres puissances.

Si $A = P_1^{r_1}...P_n^{r_n}$ et $B = P_1^{s_1}...P_n^{s_n}$, où les P_i sont des polynômes irréductibles, alors le PGCD est égal à $P_1^{u_1}...P_n^{u_n}$, où $u_i = \text{Inf}(s_i, r_i)$. Par exemple, le PGCD de $(X - 2)^3(X + 1)^2$ et de

$(X-2)^2(X+1)^4(X+3)$ est égal à $(X-2)^2(X+1)^2$, mais en général, on ne possède pas d'algorithme pour décomposer un polynôme en facteurs irréductibles. Il est plus efficace de calculer le PGCD par l'algorithme d'Euclide donné plus haut.

L'ensemble des polynômes irréductibles est infini. Une fois de plus, la démonstration est parfaitement identique à celle de $\mathbb{Z}$. En effet, soit P_1, ..., P_n n polynômes irréductibles. Montrons qu'il en existe nécessairement un autre. On considère la quantité $P_1P_2...P_n + 1$. Soit Q un facteur irréductible divisant cette quantité. Alors Q est nécessairement différent de tous les P_i. Car si $Q = P_i$, Q divise $P_1P_2...P_n$ d'une part, et divise $P_1P_2...P_n + 1$ d'autre part, donc divise la différence 1, ce qui est impossible.

5- PPCM

On appelle **PPCM** de A et B (respectivement de A_1, A_2, ..., A_n) le polynôme unitaire multiple commun à A et B (ou à A_1, ..., A_n) de plus bas degré.

Si $A = P_1^{r_1}...P_n^{r_n}$ et $B = P_1^{s_1}...P_n^{s_n}$, où les P_i sont des polynômes irréductibles, alors le PPCM est égal à $P_1^{t_1}...P_n^{t_n}$, où $t_i = \mathrm{Sup}(s_i, r_i)$. Par exemple, le PPCM de $(X-2)^3(X+1)^2$ et de $(X-2)^2(X+1)^4(X+3)$ est égal à $(X-2)^3(X+1)^4(X+3)$. On a également AB = MD, où D est le PGCD de A et B, et M le PPCM (Si les polynômes ne sont pas unitaires, il y a une constante en facteur). La démonstration est identique à celle des entiers.

Annexe I : La recherche des grands nombres premiers, le test de Lucas

Nous avons vu que les plus grands nombres premiers connus sont de la forme $2^q - 1$. Ces nombres sont appelés les nombres de Mersenne. D'une part, leur forme est adaptée au calcul sur ordinateur, d'autre part, on dispose du **test de Lucas** qui permet de déterminer s'ils sont premiers ou non.

On remarque d'abord qu'il faut que q soit premier. En effet, si $q = q_1q_2$, avec $1 < q_1 < q$ et $1 < q_2 < q$, alors $2^q - 1$ est divisible par $2^{q_1} - 1$ et par $2^{q_2} - 1$. En effet, si on calcule modulo $2^{q_1} - 1$, on a :

$$2^{q_1} \equiv 1 \bmod 2^{q_1} - 1$$
$$\Rightarrow \quad 2^{q_1q_2} \equiv 1^{q_2} \equiv 1 \bmod 2^{q_1} - 1$$
$$\Rightarrow \quad 2^q - 1 \equiv 0 \bmod 2^{q_1} - 1$$

De même avec $2^{q_2} - 1$.

Cette condition n'est pas suffisante. 11 est premier, mais $2^{11} - 1 = 2047 = 23 \times 89$. La primalité de M_{13} était connue depuis 1461, celle de M_{17} et M_{19} depuis 1588. En 1640, Mersenne pensait que M_{13}, M_{17}, M_{19}, M_{31}, M_{67}, M_{127} et M_{257}, étaient premiers. Il se trompait sur M_{67} et M_{257} et il oublia M_{61}, M_{89} et M_{107}. Euler montra en 1750 que M_{31} (qui possède déjà dix chiffres) est premier. Ce nombre resta le plus grand nombre premier connu pendant plus d'un siècle. En 1876, Lucas mit au point son test de primalité et prouva que M_{67} n'était pas premier, mais ce nombre ne fut décomposé en facteurs premiers qu'en 1903 sous la forme $193707721 \times 761838257287$. Ce calcul, invalidant une conjecture de Mersenne vieille de 250 ans, ne demande aujourd'hui qu'une fraction de seconde sur un simple ordinateur de bureau. La primalité de M_{127} fut prouvée par Lucas en 1876, celle de M_{61} en 1883, celle de M_{89} en 1911, celle de M_{107} en 1913. M_{127} est le plus grand nombre premier connu avant l'invention des machines à calculer et des ordinateurs. Il possède 39 chiffres. Lehmer montra en 1927 que M_{257} était décomposable, sa décomposition étant établie en 1980 seulement sous la forme :

535006138814359 ×
115568539524661918267303 3 ×
374550598501810936581776630096313181393

En 1878, Lucas écrivait au sujet de ce nombre :

> *Pour vérifier la dernière affirmation du P. Mersenne, sur le nombre supposé premier* $2^{257} - 1$, *et qui a soixante-dix-huit chiffres, il faudrait à l'humanité toute entière, formée de mille millions d'individus, calculant simultanément et sans interruption, un temps supérieur à un nombre de siècles représenté par un nombre de vingt chiffres ; par notre méthode, il suffit d'effectuer successivement les carrés de* 250 *nombres ayant* 78 *chiffres, au plus ; cette opération ne demanderait pas, à deux calculateurs habiles contrôlant leurs opérations, plus de huit mois de travail.*

Voici en quoi consiste le test de Lucas. On suppose q premier supérieur ou égal à 3. On pose $p = 2^q - 1$. On définit la suite $(L_n)_{n\in\mathbf{N}}$ par :

$$L_0 = 4 \text{ et } L_{n+1} \equiv L_n^{\,2} - 2 \bmod p$$

Le test de Lucas énonce que p est premier si et seulement si $L_{q-2} \equiv 0 \bmod p$.

EXEMPLE :

❑ Pour $q = 7$, $p = 2^q - 1 = 127$ et les valeurs successives de la suite modulo 127 sont 4, 14, 67, 42, 111, 0. Donc $2^7 - 1$ est premier.

❑ Pour $q = 11$, $p = 2^q - 1 = 2047$ et les valeurs successives de la suite modulo 2047 sont 4, 14, 194, 788, 701, 119, 1877, 240, 282, 1736. Donc $2^{11} - 1$ n'est pas premier.

Nous nous contenterons de montrer que la condition énoncée par Lucas est nécessaire. On suppose donc p et q premiers, $q \geq 3$. Montrons que le test est valide. On a une expression explicite de L_n, à savoir $\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{2^{n+1}} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{2^{n+1}}$, comme on pourra le vérifier par récurrence.

Notons que le petit théorème de Fermat énonce que $2^{q-1} \equiv 1 \bmod q$, autrement dit, il existe m tel que $2^{q-1} - 1 = qm$. On a également $2^q = p + 1 \equiv 1 \bmod p$. Il en résulte que :

$$2^{(p-1)/2} = 2^{2^{q-1}-1} = 2^{qm} \equiv 1^m \bmod p \equiv 1 \bmod p$$

Admettons par ailleurs provisoirement que $3^{(p-1)/2} \equiv -1 \bmod p$ et considérons L_{q-1} :

$$L_{q-1} = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{2^q} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{2^q} = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{p+1} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{p+1}$$

Développons cette expression. On obtient :

$$L_{q-1} = \frac{1}{2^{p+1}} \sum_{k=0}^{p+1} \binom{p+1}{k} \sqrt{2}^{\,p+1-k} \sqrt{6}^{k} + \frac{1}{2^{p+1}} \sum_{k=0}^{p+1} \binom{p+1}{k} \sqrt{2}^{\,p+1-k} \sqrt{6}^{k} (-1)^k$$

$$= \frac{1}{2^p} \sum_{k \text{ pair}} \binom{p+1}{k} \sqrt{2}^{\,p+1-k} \sqrt{6}^{k}$$

$$= \frac{1}{2^p} \sum_{j=0}^{(p+1)/2} \binom{p+1}{2m} 2^{(p+1)/2-j}\, 6^j \qquad \text{en posant } k = 2j$$

$$= \frac{1}{2^{(p-1)/2}} \sum_{j=0}^{(p+1)/2} \binom{p+1}{2j} 3^j$$

$$\Rightarrow \qquad 2^{(p-1)/2} L_{q-1} = \sum_{j=0}^{(p+1)/2} \binom{p+1}{2j} 3^j$$

Or pour $2 \le k \le p-1$, on a $\binom{p+1}{k} \equiv 0 \bmod p$. En effet, le facteur premier p apparaît au numérateur du coefficient binomial, et pas au dénominateur. Donc :

$2^{(p-1)/2} L_{q-1} \equiv 1 + 3^{(p+1)/2} \bmod p$

$\equiv 1 - 3 \bmod p$ puisque nous avons admis que $3^{(p-1)/2} \equiv -1 \bmod p$

$\equiv -2 \bmod p$

donc $L_{q-1} \equiv -2 \bmod p$ puisqu'au début de cette étude, nous avons vu que $2^{(p-1)/2} \equiv 1 \bmod p$.

Or $L_{q-1} = L_{q-2}^2 - 2$, donc $L_{q-2}^2 = L_{q-1} + 2 \equiv 0 \bmod p$ donc p divise L_{q-2}^2 donc, p étant premier, p divise L_{q-2}, et on a bien $L_{q-2} \equiv 0 \bmod p$. Nous avons donc montré que le test de Lucas est vérifié.

Pour cela, nous avons admis que $3^{(p-1)/2} \equiv -1 \bmod p$. Montrons cette propriété. Remarquons que $p-1$ est divisible par 3. En effet :

$p - 1 = 2^q - 2 \equiv (-1)^q - 2 \bmod 3 \equiv (-1)^q + 1 \bmod 3$

or q est impair car premier supérieur ou égal à 3 donc :

$p - 1 \equiv -1 + 1 \equiv 0 \bmod 3$

$\frac{p-1}{3}$ est donc entier et nous pouvons donc considérer le polynôme $X^{(p-1)/3} - 1$. Lorsqu'on effectue les calculs sur les entiers modulo p, avec p premier, on obtient un corps dont les éléments (modulo p) sont $\{0, 1, ..., p-1\}$. En effet, le fait que a non nul modulo p admet un inverse résulte de l'identité de Bézout, car a n'est pas divisible par p et donc, p étant premier, a est premier avec p. Il existe donc b et m tel que $ab + pm = 1$ soit $ab \equiv 1$ modulo p. a possède donc un inverse modulo p. Ce corps est noté $\mathbb{Z}/p\mathbb{Z}$ et fait l'objet d'une étude plus approfondie dans L2/ZSURNZ.PDF. Dans ce corps, le polynôme $X^{(p-1)/3} - 1$ étant de degré $\frac{p-1}{3}$ admet au plus $\frac{p-1}{3}$ racines. Il reste donc au moins $p - 1 - \frac{p-1}{3}$ éléments a en dehors de ces racines et du 0, vérifiant :

$a \not\equiv 0 \bmod p$ et $a^{(p-1)/3} \not\equiv 1 \bmod p$

Posons $b = a^{(p-1)/3}$ pour un tel a. On a :

$b^3 = a^{p-1} \equiv 1 \bmod p$ encore d'après le petit théorème de Fermat

$b^3 - 1 \equiv 0 \bmod p$

$\Rightarrow$ $(b-1)(b^2 + b + 1) \equiv 0 \bmod p$

donc p divise $(b-1)(b^2 + b + 1)$, mais il ne divise pas $b - 1 = a^{(p-1)/3} - 1$,

donc p étant premier, il divise nécessairement $b^2 + b + 1$

$\Rightarrow$ $b^2 + b + 1 \equiv 0 \bmod p$

$\Rightarrow$ $(2b + 1)^2 \equiv -3 \bmod p$ il suffit de développer le membre de gauche

$\Rightarrow$ $-1 \equiv 3^{(p-1)/2} \bmod p$ en élevant à la puissance impaire $\frac{p-1}{2}$ et en utilisant à nouveau le petit théorème de Fermat pour conclure que $(2b + 1)^{p-1} \equiv 1 \bmod p$, sachant que $2b + 1 \not\equiv 0 \bmod p$ puisque $3 \not\equiv 0 \bmod p$. CQFD

Annexe II : Les nombres parfaits

On appelle **nombre parfait** tout entier positif égal à la somme de ses diviseurs positifs autre que lui-même. Par exemple, 6 est parfait car 6 = 1 + 2 + 3. Le but de cet annexe est de décrire la forme générale des nombres parfaits pairs. Pour tout entier n positif, on note $\sigma(n)$ la somme de tous ses diviseurs positifs. Ainsi, $\sigma(6)$ est égal à 12. Un nombre n est donc parfait si et seulement si $\sigma(n) = 2n$.

On peut vérifier que 28, 496 et 8128 sont d'autres nombres parfaits, et que 6, 28, 496 et 8128 peuvent tous s'écrire sous la forme $2^n(2^{n+1} - 1)$, avec $2^{n+1} - 1$ premier. A titre de curiosité, nous indiquons que le cinquième nombre parfait (découvert en 1456) est 33 550 336, et est également de la forme précédente. Il n'est pas difficile de montrer qu'un tel nombre est parfait. Ses diviseurs sont en effet de la forme 2^k, $0 \le k \le n$, ou bien $2^k(2^{n+1} - 1)$, $0 \le k \le n$. Il n'y en a pas d'autres si $2^{n+1} - 1$ est premier. La somme de ces diviseurs vaut :

$$\begin{aligned}\sigma(2^n(2^{n+1} - 1)) &= 1 + 2 + ... + 2^n + (2^{n+1} - 1) + 2(2^{n+1} - 1) + ... + 2^n(2^{n+1} - 1)\\ &= (1 + 2 + ... + 2^n)(1 + 2^{n+1} - 1)\\ &= (2^{n+1} - 1)2^{n+1}\\ &= 2 \times 2^n(2^{n+1}-1)\end{aligned}$$

donc $2^n(2^{n+1}-1)$ est parfait. Ce résultat, ainsi que la valeur des quatre premiers nombres parfaits, est connu depuis Euclide.

Il a cependant fallu attendre Euler au XVIIIème pour voir établir la réciproque. Tous les nombres parfaits pairs sont de cette forme. Il n'y en a pas d'autres. Nous devons pour cela faire plusieurs remarques préliminaires :

(i) $\sigma(2^n) = 1 + 2 + ... + 2^n = 2^{n+1} - 1$

(ii) $\sigma(p) = p + 1$ si et seulement si p est premier

(iii) Si m et n sont deux entiers premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$. En effet, les diviseurs de mn sont de la forme uv avec u diviseur de m et v diviseur de n (pour le voir, décomposer un tel diviseur en facteurs premiers et regrouper dans u les facteurs premiers diviseurs de m et dans v les facteurs premiers divisant n) de sorte que :

$$\sigma(mn) = \sum_{d|mn} d = \sum_{u|m \text{ et } v|n} uv = \sum_{u|m} u \times \sum_{v|n} v = \sigma(m)\sigma(n)$$

Considérons alors $m = 2^n k$ un nombre parfait, avec k impair. Notre but est de montrer que $k = 2^{n+1} - 1$ et que k est premier. k étant impair est premier avec 2^n de sorte que :

$$\sigma(m) = \sigma(k)\sigma(2^n) = \sigma(k)(2^{n+1} - 1)$$

Comme m est parfait, $\sigma(m) = 2m$, et on a $\sigma(k)(2^{n+1} - 1) = 2m = 2^{n+1}k$. Donc 2^{n+1} divise $\sigma(k)(2^{n+1} - 1)$ et est premier avec $2^{n+1} - 1$ donc divise $\sigma(k)$. Il existe donc un entier t tel que :

$$\sigma(k) = 2^{n+1}t \qquad \text{(a)}$$

$$k = t(2^{n+1} - 1) \qquad \text{(b)}$$

Supposons t strictement supérieur à 1. k admet donc comme diviseurs au moins 1, t et lui-même, de sorte que $\sigma(k)$ est au moins égal à $1 + t + t(2^{n+1} - 1) = t2^{n+1} + 1$ qui est strictement supérieur à $2^{n+1}t$ contredisant le (a).

Donc nécessairement, $t = 1$, $k = 2^{n+1} - 1$, $m = 2^n(2^{n+1} - 1)$. Enfin $\sigma(k) = 2^{n+1} = k + 1$, donc les seuls diviseurs de k sont k et 1, donc k est premier. CDFD

Si l'on connaît parfaitement la forme des nombres parfaits pairs, on ignore actuellement si les nombres parfaits pairs sont en nombre fini ou non. On ignore également s'il existe des nombres parfaits impairs. On a démontré en 1976 qu'il n'existe aucun parfait impair inférieur à 10^{100}. Cette limite a été portée à 10^{160} en 1989, à 10^{300} en 1991, ..., et à 10^{1500} en 2010. S'il existe un nombre parfait impair *m*, on sait qu'il se décompose en facteurs premiers comme produit de p^k où les facteurs *p* sont au moins au nombre de 9, et où tous les exposants *k* sont pairs sauf un qui est congru à 1 modulo 4. Le nombre de facteurs, distincts ou non, est au moins égal à 101. Le plus grand facteur premier est supérieur à 10^8. L'une des puissances p^k est supérieure à 10^{62}. Si *m* possède *n* facteurs premiers distincts, *m* est majoré par 2^{4^n}.

Annexe III : Curiosités

1- Problèmes de la factorisation des entiers

On ne connaît pas d'algorithme efficace pour décomposer un entier *n* en facteurs premiers. La recherche naïve de diviseurs est un algorithme en $O(\sqrt{n})$ (i.e. le temps de calcul est majoré par une constante $\times \sqrt{n}$) qui est exponentiel en le nombre *r* de chiffres de *n* puisque *n* est de l'ordre de 10^r et $O(\sqrt{n}) = O(10^{r/2})$. Un tel algorithme prend plusieurs milliards d'années dès que *n* atteint une centaine de chiffres. Certains algorithmes très astucieux ont été développés pour déterminer un diviseur de *n*. Citons par exemple la méthode **rho de Pollard** : on considère une fonction *f* définie sur les entiers modulo *n*. On part de x_0, et l'on calcule les itérés $x_{j+1} = f(x_j)$, jusqu'à ce que le PGCD de $x_j - x_i$ et de *n* soit non trivial. Cette méthode donne en général un diviseur *p* de *n* en un temps $O(\sqrt{p})$, et non $O(\sqrt{n})$. Au pire, pour un nombre non premier, l'algorithme est en $O(\sqrt[4]{n})$. On connaît des algorithmes en $O(\exp(C\sqrt{r \ln r}))$ pour un nombre *n* de *r* chiffres.

A titre d'exemple sur la difficulté de factoriser les grands entiers, le nombre suivant (RSA-250) de 250 chiffres n'a été factorisé qu'en 2020 :

21403246502407449612644230728393335630086147151447550177977549208814180234471401
36643345519095804679610992851872470914587687396261921557363047454770520805119056
49310668769159001975940569345745223058932597669747168173806936489469987157849497
5937497937

à savoir :

64135289477071580278790190170577389084825014742943447208116859632024532344630238
62359875266834770873766192558569463979885336 7
×
33372027594978156556226010605355114227940760344767554666784520987023841729210037
08025744867329688187756571898625803693206271 1

Mais le problème reste ouvert pour le nombre RSA-260 constitué de 260 chiffres. (Voir **http://fr.wikipedia.org/Nombre%20RSA** pour plus de précisions).

A l'inverse, comme le montre l'exemple de RSA-250, vérifier que le produit des deux entiers ci-dessus redonne bien le nombre initial ne demande qu'une fraction de seconde avec un logiciel permettant le calcul avec de grands entiers. Prouver qu'un nombre *n* est composé ne demande qu'une multiplication. Il suffit de donner deux nombres d_1 et d_2 supérieurs à 1 tels que $d_1 d_2 = n$. Mais on ne

dispose d'aucune procédure efficace pour trouver d_1 et d_2. On se trouve donc devant la siuation suivante :

Si on se donne un entier *n* de plusieurs dizaines de chiffres, on est incapable en général d'en donner un diviseur en un temps raisonnable. On ne connaît pas d'algorithme qui donnerait un tel diviseur en un temps qui serait une fonction polynomiale du nombre de chiffres de *n*. On ignore si un tel algorithme existe.

Si on se donne *n* ainsi qu'un nombre *d*, il suffit d'une fraction de seconde pour tester si *d* divise *n*. On peut montrer que le temps de calcul de la division est une fonction polynomiale du nombre de chiffre de *n*.

On dit que le problème de la factorisation de *n* est un problème algorithmique de type NP (pour non déterministe polynomial), ce qui signifie qu'un tirage au hasard chanceux du nombre *d* permettrait de tester que *n* est composé en un temps qui soit une fonction polynomiale du nombre de chiffres de *n*. Mais il n'existe aucune procédure efficace de déterminer un tel *d* et l'on ignore si ce problème algorithmique est de type P (pour déterministe polynomial), ce qui signifie qu'on ne connaît pas à ce jour d'algorithme en temps polynomial permettant de déterminer un tel *d*. La question de savoir si les problèmes de type NP sont en fait de type P est un problème central de l'algorithmique. Elle fait partie des sept problèmes dits du millénaire par la fondation Clay qui offre une récompense d'un million de dollars à qui saura la résoudre (voir http://www.claymath.org/millennium-problems/p-vs-np-problem).

Un dernier exemple : le nombre de Fermat $2^{2^8} + 1$ n'est pas premier puisqu'on pourra vérifier en une fraction de seconde que :

$$2^{2^8} + 1 = 1238926361552897 \times$$
$$93461639715357977769163558199606896584051237541638188580280321$$

Cependant, la décomposition précédente n'a été trouvée qu'un 1981.

Voici un aperçu de l'évolution de nos capacités de calcul :

- En 1874, on pensait impossible de factoriser les nombres d'une dizaine de chiffres, par exemple 8 616 460 799. Ce n'est qu'en 1925 qu'on le factorisa (96 079 × 89 681). Cette factorisation est aujourd'hui instantanée sur un modeste ordinateur de bureau.
- Dans les années 1960, la factorisation des nombres de 25 chiffres semblait hors de portée. On factorisa en 1970 un nombre de 39 chiffres.
- A la fin des années 1970, on s'attaque à des nombres de 80 chiffres. Le cap des 100 chiffres est atteint en 1990. Le défi RSA-129, lancé en 1977 consistait à factoriser un nombre de 129 chiffres. Le temps de calcul était alors évalué à quelques millions d'années. Les progrès algorithmique permirent d'atteindre le but en 1994. Le défi RSA-768 a été remporté en 2009, mais comme nous l'avons vu, le défi plus modeste RSA-260 est encore à relever.
- On sait que le nombre de Fermat $F_{20} = 2^{2^{20}} + 1$ est composé, mais on ne connaît aucun de ses facteurs. Il est possible qu'on n'en connaîtra jamais aucun.

Le lecteur intéressé pourra se reporter au livre de Jean-Paul Delahaye, *Merveilleux nombres premiers*, Belin (2000).

2- Un test probabiliste de primalité

Bien que ne sachant que difficilement factoriser un nombre d'une centaine de chiffres, on possède des algorithmes permettant de déterminer la primalité de nombres d'un millier de chiffres. Bien

entendu, ces tests de primalité n'utilise pas la recherche de diviseurs, mais d'autres moyens plus détournés. Il existe également des tests probabilistes permettant de tester de manière quasi-certaine la primalité des nombres de quelques dizaines de milliers de chiffres. La plupart utilise le petit théorème de Fermat. Malheureusement, le théorème de Fermat ne permet pas de tester si n est premier, car certains nombres n vérifient la conclusion du théorème de Fermat sans être premier. Il s'agit des nombres de Carmichael dont le plus petit est 561. On a donc affiné le théorème de Fermat de façon à obtenir une condition nécessaire et suffisante sur la primalité de n et pas seulement une condition nécessaire. En voici un exemple :

Le test de Miller-Rabin :
Soit n un nombre impair. Posons $n - 1 = 2^s t$, avec t impair. Soit b premier avec n. On dit que b et n passent le test si $b^t \equiv 1 \bmod n$ ou si il existe r, $0 \leq r < s$ tel que $b^{t.2^r} \equiv -1 \bmod n$. (Le théorème de Fermat énonce seulement que $b^{n-1} = b^{t.2^s} \equiv 1 \bmod n$)

On prouve que, si n est premier, le test réussit pour tout b premier avec n, mais si n n'est pas premier, le test échoue pour au moins $\frac{3}{4}$ des nombres b. On choisit donc k nombres b au hasard. Si l'un des tests échoue, on est certain que n est composé. Si le test réussit, alors n est premier avec une probabilité d'erreur inférieure à $\frac{1}{4^k}$, soit $\frac{1}{10^{18}}$ si $k = 30$. La probabilité d'erreur est en fait certainement encore plus faible. Pour $b = 2, 3, 5$ ou 7 seulement, le seul nombre composé n inférieur à 10^{11} qui passe le test est 3215031751. En outre, il a été prouvé que le test précédent serait déterministe (et non plus probabiliste) en un temps de calcul $O(\ln(n)^2)$, à condition que la conjecture dite de Riemann soit vérifiée. (Cette conjecture est aussi dotée d'un prix d'un million de dollars par la fondation Clay).

La fonction *isprime* de certains logiciels tels MAPLE est un test probabiliste comparable à celui qui vient d'être exposé. Une réponse *false* assure que le nombre proposé n'est pas premier, mais l'aide de MAPLE précise qu'une réponse *true* assure seulement que "*n is very probably prime [...]. No counter example is known and it has been conjectured that such a counter example must be hundreds of digits long*".

3- Les certificats de primalité
Un certificat de primalité est une donnée permettant d'assurer qu'un entier n est premier en temps de calcul polynomial en le nombre de chiffres de n. Ce certificat est la donnée d'une liste (a, q_1, a_1, q_2, a_2, ..., q_k, a_k) telle que les trois conditions suivantes soient vérifiées :

$$\begin{cases} n - 1 = q_1^{a_1} q_2^{a_2} \dots q_k^{a_k}, \text{ les } q_k \text{ étant premiers} \\ a^{n-1} \equiv 1 \bmod n \\ \forall\, i \in \{1, \dots, k\},\ a^{(n-1)/q_i} \neq 1 \bmod n \end{cases}$$

Pratt a montré en 1975 que ces conditions sont équivalentes à dire que n est premier. (Les q_k peuvent également être accompagné de leur certificat s'il n'apparaît pas de façon évidente qu'ils sont premiers).

Ainsi, le nombre 2801196269419097900390625 1 est premier de façon certaine, son certificat étant (2, 2, 1, 3, 24, 5, 18, 13, 1). En effet :

$$2801196269419097900390625 1 - 1 = 2 \times 3^{24} \times 5^{18} \times 13$$
$$2^{n-1} \equiv 1 \bmod n$$

$2^{(n-1)/2} \equiv 280119626941909790039062 50 \bmod n \neq 1$
$2^{(n-1)/3} \equiv 114091892404576104880784 53 \bmod n \neq 1$
$2^{(n-1)/5} \equiv 191498652216316279684816 81 \bmod n \neq 1$
$2^{(n-1)/13} \equiv 190331129945142881395380 07 \bmod n \neq 1$

Mais tout le problème est de trouver la bonne liste. *n* étant donné, on tombe en effet sur le problème de décomposer $n - 1$ en facteurs premiers, problème dont nous avons souligné la difficulté plus haut.

Un pas théorique extrêmement important a été franchi en août 2002 par trois mathématiciens Indiens, Agrawal, Kayal et Saxena qui ont mis au point un test de primalité déterministe dont le temps de calcul est polynomial en le nombre de chiffres de *n*. Cette découverte a fait le tour de la planète en peu de temps. Mais ce test est encore trop lent pour pouvoir être mis efficacement en pratique par rapport aux tests probabilistes.

4- Le polynôme de Jones

En 1976, Jones a explicité un polynôme des 26 variables entières positives ou nulles *a*, *b*, ..., *z*, dont l'ensemble des valeurs positives coïncide avec l'ensemble des nombres premiers. Le voici :

$$(k+2)[1 - (wz+h+j-q)^2 - [(gk+2g+k+1)(h+j) + h - z]^2$$
$$- (2n+p+q+z-e)^2 - [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2$$
$$- [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2$$
$$- [16r^2y^4(a^2-1) + 1 - u^2]^2$$
$$- [((a+u^2(u^2-a))^2-1)(n+4dy)^2 + 1 - (x+cu)^2]^2 - [n+l+v-y]^2$$
$$- [(a^2-1)l^2 + 1 - m^2]^2 - [ai+k+1-l-i]^2$$
$$- [p + l(a-n-1) + b(2an+2a-n^2-2n-2) - m]^2$$
$$- [q+ y(a-p-1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2$$
$$- [z + pl(a-p) + t(2ap - p^2 - 1) - pm]^2]$$

Pour prouver qu'un nombre est premier, il suffit de donner les "bonnes" valeurs entières aux 26 variables, et de faire le calcul pour voir si on trouve bien le nombre premier en question[2]. Malheureusement, ce résultat, trouvé en corollaire d'un problème plus fondamental (le 10ème problème de Hilbert) n'a qu'un intérêt théorique et nullement pratique, car le polynôme de Jones n'est en fait qu'un codage extrêment astucieux d'un critère fort peu efficace de primalité à savoir : $k + 2$ est premier si et seulement si $(k + 1)! + 1 \equiv 0 \bmod (k + 2)$ (**théorème de Wilson**). Les nombres intervenant dans ce polynôme sont gigantesques. Ainsi, les valeurs des variables permettant d'obtenir le nombre premier 2 sont-elles :

$a = 79016903580988961616855568797499491863263807134092 90912$
$b = 0$
$e = 32,$
$f = 17$
$g = 0$
$h = 2$
$i = 0$
$j = 5$
$k = 0$
$l = 1$

[2] James P. Jones, Daihachiro Sato, Hideo Wada, Douglas Wien, Diophantine representation of the set of prime numbers, Amer. Math. Monthly, 83:6 (1976), p.449-464.

m = 790169035809889616168555687974994918632638071340929091 2

n = 2

o = 834035301564579468329946270481226888212608613465610836377 7

p = 3

q = 16

s = 1

t = 0

v = 158033807161977923233711137594998983726527614268185818 21,

w = 1

x = 124873421030546123716955456199915227363498042625369404787663046 0688618240305377713493375059050669591252915834 87

y = 158033807161977923233711137594998983726527614268185818 24

z = 9

u et r sont trop grands pour être affichés (et peut-être même calculés). Ils sont solutions de l'équation :

623103237477467837531548712748569488106977789848995186243400722213058 5819467692530519441368990697501076667981494902945038290563249052108414 1729062190213501628290192909949095484073533946150864915984334572822465 2061515542425077120390471654182964600840783563926683798305093390159899 2 $\times r^2 - u^2 + 1 = 0$

c et d sont solutions d'une équation comparable. ☹ ☹ ☹

5- Les fractions de Conway et Guy

Dans le même genre d'exploit loufoque, J.H. Conway et R.K. Guy, dans le livre *The Book of Numbers*, (Springer-Verlag 1996), donne la curiosité suivante ("*our best effort along these lines*" selon les auteurs). Considérons la suite de fractions qui suit :

$\frac{17}{91}$	$\frac{78}{85}$	$\frac{19}{51}$	$\frac{23}{38}$	$\frac{29}{33}$	$\frac{77}{29}$	$\frac{95}{23}$	$\frac{77}{19}$	$\frac{1}{17}$	$\frac{11}{13}$	$\frac{13}{11}$	$\frac{15}{14}$	$\frac{15}{2}$	$\frac{55}{1}$
A	B	C	D	E	F	G	H	I	J	K	L	M	N

Démarrez avec une puissance de 2 de la forme 2^p, où p est premier, puis multipliez de façon répétée par la première fraction (en commençant par la gauche) qui fournira un résultat entier. Alors la prochaine puissance de 2 que l'on obtiendra sera de la forme 2^q où q est le nombre premier immédiat supérieur à p. Par exemple, en partant de 2, on obtient ainsi, en multipliant successivement par les fractions M, N, E, F, K, A, etc... les nombres suivants :

$2 \to 15 \to 825 \to 725 \to 1925 \to 2275 \to 425 \to 390 \to 330 \to 290 \to 770 \to 910 \to 170 \to 156 \to 132 \to 116 \to 308 \to 364 \to 68 \to 4$

avec $4 = 2^2$. Si on continue, on obtiendra ensuite 2^3, puis 2^5 (sans jamais passer par 2^4), etc...(Ne pas partir de p trop grand car le programme est assez long à se terminer). Nous ne résistons pas à l'envie de donner la suite des valeurs qui suivent $32 = 2^5$. On notera que l'on parvient à $128 = 2^7$ sans jamais être passé par $64 = 2^6$!! Le calcul analogue nous faisant passer de 2^7 à 2^{11} prendrait six pages !! ☺ ☺ ☺

$32 \to 240 \to 1800 \to 13500 \to 101250 \to 759375 \to 41765625 \to 36703125 \to 97453125 \to 85640625 \to 227390625 \to 199828125 \to 530578125 \to 466265625 \to 1238015625 \to 1087953125 \to 2888703125 \to 3413921875 \to 637765625 \to 585243750 \to 109331250 \to 100327500 \to 18742500 \to 17199000 \to 3213000 \to 2948400 \to 550800 \to 505440 \to 427680 \to 375840 \to 997920 \to 876960 \to 2328480 \to 2046240 \to 5433120 \to 4774560 \to 12677280 \to$

11140640 → 29580320 → 34958560 → 6530720 → 5992896 → 1119552 → 417088 → 252448 → 1042720 → 631120 → 2606800 → 1577800 → 6517000 → 3944500 → 16292500 → 9861250 → 40731250 → 24653125 → 101828125 → 412671875 → 487703125 → 91109375 → 83606250 → 15618750 → 14332500 → 2677500 → 2457000 → 459000 → 421200 → 356400 → 313200 → 831600 → 730800 → 1940400 → 1705200 → 4527600 → 3978800 → 10564400 → 12485200 → 2332400 → 2140320 → 399840 → 366912 → 68544 → 25536 → 15456 → 63840 → 38640 → 159600 → 96600 → 399000 → 241500 → 997500 → 603750 → 2493750 → 1509375 → 6234375 → 25265625 → 22203125 → 58953125 → 69671875 → 13015625 → 11943750 → 2231250 → 2047500 → 382500 → 351000 → 297000 → 261000 → 693000 → 609000 → 1617000 → 1421000 → 3773000 → 4459000 → 833000 → 764400 → 142800 → 131040 → 24480 → 22464 → 19008 → 16704 → 44352 → 38976 → 103488 → 90944 → 241472 → 285376 → 53312 → 3136 → 3360 → 3600 → 27000 → 202500 → 1518750 → 11390625 → 626484375 → 550546875 → 1461796875 → 1284609375 → 3410859375 → 2997421875 → 7958671875 → 6993984375 → 18570234375 → 16319296875 → 43330546875 → 38078359375 → 101104609375 → 119487265625 → 22321796875 → 20483531250 → 3826593750 → 3511462500 → 655987500 → 601965000 → 112455000 → 103194000 → 19278000 → 17690400 → 3304800 → 3032640 → 2566080 → 2255040 → 5987520 → 5261760 → 13970880 → 12277440 → 32598720 → 28647360 → 76063680 → 66843840 → 177481920 → 155968960 → 414124480 → 489419840 → 91430080 → 83900544 → 15673728 → 5839232 → 3534272 → 14598080 → 8835680 → 36495200 → 22089200 → 91238000 → 55223000 → 228095000 → 138057500 → 570237500 → 345143750 → 1425593750 → 862859375 → 3563984375 → 14443515625 → 17069609375 → 3188828125 → 2926218750 → 546656250 → 501637500 → 93712500 → 85995000 → 16065000 → 14742000 → 2754000 → 2527200 → 2138400 → 1879200 → 4989600 → 4384800 → 11642400 → 10231200 → 27165600 → 23872800 → 63386400 → 55703200 → 147901600 → 174792800 → 32653600 → 29964480 → 5597760 → 5136768 → 959616 → 357504 → 216384 → 893760 → 540960 → 2234400 → 1352400 → 5586000 → 3381000 → 13965000 → 8452500 → 34912500 → 21131250 → 87281250 → 52828125 → 218203125 → 884296875 → 777109375 → 2063359375 → 2438515625 → 455546875 → 418031250 → 78093750 → 71662500 → 13387500 → 12285000 → 2295000 → 2106000 → 1782000 → 1566000 → 4158000 → 3654000 → 9702000 → 8526000 → 22638000 → 19894000 → 52822000 → 62426000 → 11662000 → 10701600 → 1999200 → 1834560 → 342720 → 314496 → 58752 → 21888 → 13248 → 54720 → 33120 → 136800 → 82800 → 342000 → 207000 → 855000 → 517500 → 2137500 → 1293750 → 5343750 → 3234375 → 13359375 → 54140625 → 47578125 → 126328125 → 111015625 → 294765625 → 348359375 → 65078125 → 59718750 → 11156250 → 10237500 → 1912500 → 1755000 → 1485000 → 1305000 → 3465000 → 3045000 → 8085000 → 7105000 → 18865000 → 22295000 → 4165000 → 3822000 → 714000 → 655200 → 122400 → 112320 → 95040 → 83520 → 221760 → 194880 → 517440 → 454720 → 1207360 → 1426880 → 266560 → 244608 → 45696 → 17024 → 10304 → 42560 → 25760 → 106400 → 64400 → 266000 → 161000 → 665000 → 402500 → 1662500 → 1006250 → 4156250 → 2515625 → 10390625 → 42109375 → 49765625 → 9296875 → 8531250 → 1593750 → 1462500 → 1237500 → 1087500 → 2887500 → 2537500 → 6737500 → 7962500 → 1487500 → 1365000 → 255000 → 234000 → 198000 → 174000 → 462000 → 406000 → 1078000 → 1274000 → 238000 → 218400 → 40800 → 37440 → 31680 → 27840 → 73920 → 64960 → 172480 → 203840 → 38080 → 34944 → 6528 → 2432 → 1472 → 6080 → 3680 → 15200 → 9200 → 38000 → 23000 → 95000 → 57500 → 237500 → 143750 → 593750 → 359375 → 1484375 → 6015625 → 7109375 → 1328125 → 1218750 → 1031250 → 906250 → 2406250 → 2843750 → 531250 → 487500 → 412500 → 362500 →

962500 → 1137500 → 212500 → 195000 → 165000 → 145000 → 385000 → 455000 → 85000 → 78000 → 66000 → 58000 → 154000 → 182000 → 34000 → 31200 → 26400 → 23200 → 61600 → 72800 → 13600 → 12480 → 10560 → 9280 → 24640 → 29120 → 5440 → 4992 → 4224 → 3712 → 9856 → 11648 → 2176 → 128

Exercices

1- Enoncés

Exo.1) Soit b entier supérieur ou égal à 2 et (a_n) la suite définie par :

$$a_0 = 0,\ a_1 = 1, \text{ et } \forall\ n,\ a_{n+2} = ba_{n+1} - a_n$$

Montrer l'équivalence :

$$\begin{cases} x^2 - bxy + y^2 = 1 \\ y < x \\ x \in \mathbb{N},\ y \in \mathbb{N} \end{cases} \Leftrightarrow \exists\ n,\ y = a_n,\ x = a_{n+1}$$

Exo.2) Soient a et b deux entiers naturels premiers entre eux et q_1, ..., q_n la suite des quotients intervenant dans le calcul du PGCD selon l'algorithme d'Euclide.

a) Montrer que $\dfrac{a}{b} = q_1 + \dfrac{1}{q_2 + \ldots \dfrac{1}{q_n + \dfrac{1}{q_{n+1}}}}$

b) On pose $\dfrac{c}{d} = q_1 + \dfrac{1}{q_2 + \ldots \dfrac{1}{q_n}}$ avec $c \wedge d = 1$. Montrer que $ad - bc = \pm 1$

EXEMPLE :

Prenons $a = 123$ et $b = 26$.

$$\frac{123}{26} = 4 + \frac{19}{26} = 4 + \frac{1}{\frac{26}{19}} = 4 + \frac{1}{1 + \frac{7}{19}} = 4 + \frac{1}{1 + \frac{1}{\frac{19}{7}}} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{5}{7}}}$$

$$= 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\frac{7}{5}}}} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{2}{5}}}} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{5}{2}}}}} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}}}$$

et $$\frac{c}{d} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\frac{3}{2}}}} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{2}{3}}} = 4 + \frac{1}{1 + \frac{1}{\frac{8}{3}}}$$

$$= 4 + \frac{1}{1 + \frac{3}{8}} = 4 + \frac{1}{\frac{11}{8}} = 4 + \frac{8}{11} = \frac{52}{11}$$

et on a bien $123 \times 11 - 26 \times 52 = 1$

Exo.3) Résoudre dans $\mathbb{Z}^2$ l'équation : $323x - 391y = 612$.

Exo.4) Euler vous propose cet exercice : Quelqu'un achète des chevaux et des boeufs. Il paie 31 écus par cheval et 20 écus par boeuf, et il se trouve que les boeufs lui ont coûté 7 écus de plus que ne lui ont coûté les chevaux. Combien cet homme a-t-il acheté de boeufs et de chevaux ?

Exo.5) Soient n un entier strictement positif, m un entier quelconque, et $p = m \wedge n$. Montrer que, dans $\mathbb{C}$, $\{\exp(\frac{2imk\pi}{n} \mid k \in \mathbb{Z}\} = \{\exp(\frac{2ipk\pi}{n}) \mid k \in \mathbb{Z}\}$.

Exo.6) Soit m un entier strictement positif. Quel est le plus grand entier diviseur de deux termes successifs de la suite $(n^2 + m)_{n\in\mathbb{N}}$?

Exo.7) Soit x entier positif différent de 0 et 1. Soit p et q deux entiers de PGCD d. Montrer que le PGCD de $x^p - 1$ et $x^q - 1$ est égal à $x^d - 1$. De même, dans $\mathbb{K}[X]$, le PGCD de $X^p - 1$ et de $X^q - 1$ est $X^d - 1$.

Exo.8) Montrer que les nombres dont le développement dans une base b quelconque est de la forme 10101, 101010101, 1010101010101, etc... sont composés.

Exo.9) Soit $a = \sum_{k\geq 0} a_k 2^k$ et $b = \sum_{k\geq 0} b_k 2^k$ la décomposition en base 2 de deux nombres a et b, les a_k et b_k valant 0 ou 1. On note :

$$a \lozenge b = \sum_{k\geq 0} \min(a_k, b_k)\, 2^k$$

$$a \prec b \Leftrightarrow \forall\, k,\ a_k \leq b_k$$

a) Montrer que $a \prec b \Leftrightarrow a \lozenge b = a$
b) Montrer que $\prec$ est une relation d'ordre.
c) Montrer que $c = a \lozenge b \Leftrightarrow c \prec a$ et $a \prec a + b - c$

Exo.10) Soit n entier strictement positif. Déterminer un entier a tel que $[a, a + n[$ ne contienne aucun nombre premier.

Exo.11) Prouver que $\text{PPCM}(a_1, a_2, ..., a_n) = \frac{a_1 a_2 ... a_n}{\text{PGCD}(b_1, b_2, ..., b_n)}$ avec $b_i = \frac{a_1 a_2 ... a_n}{a_i}$. Cette formule généralise $\text{PPCM}(a, b) = \frac{ab}{\text{PGCD}(a, b)}$.

Exo.12) A et B désignent des entiers ou des polynômes. Que vaut le PGCD de A + B et de PPCM(A, B) ?

Exo.13) A et B désigne des entiers ou des polynômes. Soit $M = A \vee B$. Montrer qu'il existe U et V tels que M = UV avec U | A, V | B et $U \wedge V = 1$. La décomposition est-elle unique ?

Exo.14) A, B, C désignant des entiers ou des polynômes, montrer que :

a) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

b) $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

où $\wedge$ désigne le PGCD et $\vee$ désigne le PPCM. Ainsi, les deux opérateurs sont mutuellement distributifs l'un par rapport à l'autre.

Exo.15) Montrer qu'il existe une infinité de nombres premiers de la forme $4n - 1$. Votre démonstration vous permet-elle de montrer le même résultat pour les nombres de la forme $4n + 1$?

Exo.16) Soit p_1, p_2, ... p_r premiers distincts. On pose $q_i = \frac{p_1 p_2 ... p_r}{p_i}$.

a) Montrer que $p_1 p_2 ... p_r \wedge (q_1 + ... + q_r) = 1$

b) En déduire une autre démonstration de l'existence d'une infinité de nombres premiers (**Preuve de Metrod** ou de **Stieljes**).

Exo.17) Pour k variant de 1 à n, on pose $b_k = k \times n! + 1$.

a) Montrer que : $\forall\ i \neq j,\ b_i \wedge b_j = 1$.

b) En déduire une autre démonstration de l'existence d'une infinité de nombres premiers (**Preuve de Schorn**).

Exo.18) Soit n entier et r le nombre de nombres premiers intervenant dans la décomposition des entiers compris entre 1 et 2^n. Autrement dit, tout entier compris entre 1 et n s'écrit sous la forme $p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ avec p_1, p_2, ... p_r premiers distincts et k_1, ..., k_r entiers positifs ou nuls.

a) Prouver que, pour tout i, $k_i \leq n$.

b) En déduire que $2^n \leq (n + 1)^r$.

c) En déduire une autre démonstration de l'existence d'une infinité de nombres premiers (**Preuve de Thue** ou d'**Auric**)

Exo.19) Pour tout $n \geq 0$, soit $F_n = 2^{2^n} + 1$ (nombre de Fermat).

a) Montrer que, pour tout $n \geq 0$, F_n divise $2^{F_n} - 2$.

b) Montrer que, pour tout $n \geq 1$, $F_n = {F_{n-1}}^2 - 2F_{n-1} + 2$

c) Montrer que, pour tout $n \geq 1$, $F_n = F_0 F_1 F_2 ... F_{n-1} + 2$

d) Montrer que, pour tout $n < m$, $F_n \wedge F_m = 1$

e) En déduire qu'il existe une infinité de nombres premiers (**preuve de Goldbach**).

Exo.20) Pour tout nombre entier strictement positif n, on pose $s(n) = \sum_{d|n,\ 1 \leq d < n} d$ (somme des diviseurs de n autres que n lui-même). Deux nombres n et m sont dits **amicaux** si $s(n) = m$ et $s(m) = n$. Ainsi, 220 et 284 sont amicaux car 220 est la somme des diviseurs 1, 2, 4, 71, 142 de 284, et 284 est la somme des diviseurs 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110 de 220.

a) Montrer que, si a, b, c sont des nombres premiers de la forme $a = 3 \times 2^n - 1$, $b = 3 \times 2^{n-1} - 1$ et $c = 9 \times 2^{2n-1} - 1$, alors $2^n ab$ et $2^n c$ sont amicaux (Thabit Ibn Qurra, IXème).

b) Vérifier que le couple (220, 284) est de cette forme (Thabit Ibn Qurra), et qu'il en est de même de (17296, 18416) (Fermat) et de (9363584, 9437056) (Descartes). Ce sont les seuls couples de nombres amicaux connus ayant la forme donnée.

Exo.21) Montrer que, pour tout m et n entiers naturels, 56786730 divise $mn(m^{60} - n^{60})$.

Exo.22) Montrer que tout entier strictement positif m s'écrit de manière unique $m = a^n$, où a est un entier qui ne peut lui-même s'exprimer comme puissance supérieure ou égale à 2 d'un autre entier. Par exemple, 64 s'écrira sous cette forme 2^6 mais non 4^3.

Exo.23) Montrer que, pour tout a élément de $\mathbb{N}^*$, la fraction $\dfrac{2a^3 + 3a}{2a^4 + 5a^2 + 1}$ est irréductible.

Exo.24) Trouver un polynôme A de degré minimal, tel que A soit divisible par $X^2 + 1$ et $A - 1$ par $X^3 + 1$.

2- Solutions

Sol.1) Montrons par récurrence que la suite (a_n) est strictement croissante. On a $a_1 > a_0$, et si $a_{n+1} > a_n$, alors $a_{n+2} = ba_{n+1} - a_n \geq 2a_{n+1} - a_n > 2a_{n+1} - a_{n+1} = a_{n+1}$.
Montrons par récurrence que : $\forall\ n,\ {a_{n+1}}^2 - ba_{n+1}a_n + {a_n}^2 = 1$. C'est vrai pour $n = 0$, et si c'est vrai pour n, alors :

$$\begin{aligned} {a_{n+2}}^2 - ba_{n+2}a_{n+1} + {a_{n+1}}^2 &= (ba_{n+1} - a_n)^2 - b(ba_{n+1} - a_n)a_{n+1} + {a_{n+1}}^2 \\ &= b^2{a_{n+1}}^2 - 2ba_na_{n+1} + {a_n}^2 - b^2{a_{n+1}}^2 + ba_na_{n+1} + {a_{n+1}}^2 \\ &= -ba_na_{n+1} + {a_n}^2 + {a_{n+1}}^2 \\ &= 1 \end{aligned}$$

Donc, si $y = a_n$, $x = a_{n+1}$, alors $y < x$ et $x^2 - bxy + y^2 = 1$.
Réciproquement, soient x et y vérifiant $y < x$ et $x^2 - bxy + y^2 = 1$. Montrons par récurrence sur y qu'il existe n tel que $y = a_n$ et $x = a_{n+1}$. Si $y = 0$, alors $x^2 - bxy + y^2 = 1$ implique que $x = 1$ et donc $(x, y) = (a_1, a_0)$. Si, maintenant, $y \geq 1$ et la propriété demandée est vérifiée pour tout couple dont la deuxième composante est inférieure ou égale à $y - 1$, alors considérons le couple $(y, by - x)$. On a :

$$y^2 - by(by - x) + (by - x)^2 = y^2 - b^2y^2 + bxy + b^2y^2 - 2bxy + x^2 = y^2 - bxy + x^2 = 1$$

De plus $0 \leq by - x < y$. En effet :

$by - x < y$
$\Leftrightarrow$ $bxy - x^2 < xy$ en multipliant par x non nul puisque $x > y$.
$\Leftrightarrow$ $y^2 - 1 < xy$ car $bxy - x^2 = y^2 - 1$
$\Leftrightarrow$ $y^2 < xy + 1$

qui est vrai car $y < x$.
Puis $0 \leq by - x$
$\Leftrightarrow$ $x \leq by$
$\Leftrightarrow$ $x^2 \leq bxy = x^2 + y^2 - 1$ qui est vrai car $y > 0$

On peut donc appliquer l'hypothèse de récurrence au couple $(y, by - x)$. Il existe n tel que $(y, by - x) = (a_n, a_{n-1})$, donc $y = a_n$ et $x = ba_n - a_{n-1} = a_{n+1}$. Donc la relation demandée est vérifiée pour le couple (x, y).

Sol.2) a) On a :

$a = bq_1 + r_1$
$b = r_1q_2 + r_2$
...
$r_{k-1} = r_kq_{k+1} + r_{k+1}$
...

$$r_{n-1} = r_n q_{n+1}$$

On a $\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}}$, puis, par récurrence sur k :

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \ldots \cfrac{1}{q_{k-1} + \cfrac{1}{q_k + \frac{r_k}{r_{k-1}}}}}$$

jusqu'au rang $k = n$.

b) Considérons le rationnel $\frac{a_n}{b_n} = q_n + \frac{1}{q_{n+1}} = \frac{q_n q_{n+1} + 1}{q_{n+1}}$ pour lequel $q_{n+1} \wedge (q_n q_{n+1} + 1) = 1$, car un diviseur commun de q_{n+1} et $q_n q_{n+1} + 1$ divise $(q_n q_{n+1} + 1) - q_n q_{n+1} = 1$. On a donc $a_n = q_n q_{n+1} + 1$ et $b_n = q_{n+1}$. Soit $\frac{c_n}{d_n} = q_n$, i.e. $c_n = q_n$, $d_n = 1$. On a ici :

$$a_n d_n - b_n c_n = 1$$

comme on le vérifie facilement. On procède ensuite par récurrence descendante sur k en posant :

$$\frac{a_k}{b_k} = q_k + \cfrac{1}{q_{k+1} + \cfrac{1}{q_{k+2} + \ldots \cfrac{1}{q_n + \frac{1}{q_{n+1}}}}}, \quad \frac{c_k}{d_k} = q_k + \cfrac{1}{q_{k+1} + \cfrac{1}{q_{k+2} + \ldots \frac{1}{q_n}}}$$

et on suppose que $a_k d_k - b_k c_k = \pm 1$, $a_k \wedge b_k = 1$, $c_k \wedge d_k = 1$ (relation prouvée pour $k = n$). Montrons que les relations restent vraies au rang $k - 1$. On a :

$$\frac{a_{k-1}}{b_{k-1}} = q_{k-1} + \frac{1}{\frac{a_k}{b_k}} = q_{k-1} + \frac{b_k}{a_k} = \frac{q_{k-1} a_k + b_k}{a_k}$$

$$\frac{c_{k-1}}{d_{k-1}} = q_{k-1} + \frac{1}{\frac{c_k}{d_k}} = q_{k-1} + \frac{d_k}{c_k} = \frac{q_{k-1} c_k + d_k}{c_k}$$

donc $a_{k-1} = q_{k-1} a_k + b_k$ et $b_{k-1} = a_k$ qui sont bien premiers entre eux car :

$$a_{k-1} \wedge b_{k-1} = (q_{k-1} a_k + b_k) \wedge a_k = b_k \wedge a_k = 1$$

et de même $c_{k-1} = q_{k-1} c_k + d_k$ et $d_{k-1} = c_k$. On a alors :

$$a_{k-1} d_{k-1} - b_{k-1} c_{k-1} = (q_{k-1} a_k + b_k) c_k - a_k (q_{k-1} c_k + d_k) = b_k c_k - a_k d_k = \pm 1$$

On poursuit ainsi jusqu'à $k = 1$.

Sol.3) On a :

$323 \times 0 + 391 \times 1 = 391$	L_1	
$323 \times 1 + 391 \times 0 = 323$	L_2	or $391 = 323 + 68$
$-323 + 391 = 68$	$L_3 = L_1 - L_2$	or $323 = 68 \times 4 + 51$
$323 \times 5 - 391 \times 4 = 51$	$L_4 = L_2 - 4L_3$	or $68 = 51 + 17$
$-323 \times 6 + 391 \times 5 = 17$	$L_5 = L_3 - L_4$	

et $17 \mid 51$, donc $323 \wedge 391 = 17$. Or $612 = 17 \times 36$. Une solution particulière est donc, en multipliant 17 par 36 :

$$-323 \times 216 + 391 \times 180 = 612$$

(x, y) vérifie $323x - 391y = 612$ si et seulement si :

$323 \times (x + 216) - 391 \times (y + 180) = 0$

$\Leftrightarrow$ $19 \times (x + 216) - 23 \times (y + 180) = 0$ en divisant par 17

$\Leftrightarrow$ $19 \times (x + 216) = 23 \times (y + 180)$

donc nécessairement, 19 divise $23 \times (y + 180)$ donc 19 divise $y + 180$ car $19 \wedge 23 = 1$. On a donc :

$y \equiv -180 \bmod 19 \equiv 10 \bmod 19$

et $\exists\, k,\ y = 10 + 19k$

Si on reporte dans $19 \times (x + 216) = 23 \times (y + 180)$, on obtient :

$19 \times (x + 216) = 23 \times (19k + 190)$

$\Leftrightarrow$ $x + 216 = 23 \times (k + 10)$

$\Leftrightarrow$ $x = 23k + 14$

Les solutions sont donc $(14 + 23k, 10 + 19k)$, $k \in \mathbb{Z}$.

Sol.4) Soit c le nombre de chevaux acheté et b le nombre de boeufs. On a $31c + 7 = 20b$. L'identité de Bézout entre 31 et 20 est :

$-9 \times 31 + 14 \times 20 = 1$

donc, en multipliant par 7 :

$-63 \times 31 + 98 \times 20 = 7 = -31c + 20b$

donc $(63 - c) \times 31 = (98 - b) \times 20$

Comme 31 divise $(98 - b) \times 20$ et est premier avec 20, 31 divise $98 - b$ donc il existe k tel que $98 - b = 31k$. Si on reporte dans la dernière équation, on obtient $63 - c = 20k$. Donc :

$b = 98 - 31k$ $\qquad$ $c = 63 - 20k$

Comme $b \geq 0$, $c \geq 0$, on doit prendre $k \leq 3$ (mais éventuellement négatif). Il y a donc mathématiquement une infinité de solutions. Concrètement, on peut supposer que les animaux se comptent en quelques unités, le plus vraisemblable étant obtenu pour $k = 3$: $b = 5$, $c = 3$.

Sol.5) Comme m est un multiple de p, on a clairement $\exp(\frac{2imk\pi}{n}) \in \{\exp(\frac{2ipk\pi}{n} \mid k \in \mathbb{Z}\}$.

Réciproquement, l'identité de Bézout donne l'existence de x et y entiers tels que $xm + yn = p$. Donc :

$$\exp(\frac{2ipk\pi}{n}) = \exp(\frac{2i(xm + yn)k\pi}{n})$$

$$= \exp(\frac{2ixmk\pi}{n}) \in \{\exp(\frac{2imk\pi}{n} \mid k \in \mathbb{Z}\}$$

Sol.6) Utilisons le fait que, pour tout k, $a \wedge b = a \wedge (b + ka)$:

$$(n^2 + m) \wedge ((n + 1)^2 + m) = (n^2 + m) \wedge (n^2 + 2n + 1 + m)$$
$$= (n^2 + m) \wedge (2n + 1)$$
$$= (4n^2 + 4m) \wedge (2n + 1) \qquad \text{car } 4 \wedge (2n + 1) = 1$$
$$= (4n^2 - (2n + 1)^2 + 4m) \wedge (2n + 1)$$
$$= (-4n + 4m - 1) \wedge (2n + 1)$$
$$= (-4n + 2(2n + 1) + 4m - 1) \wedge (2n + 1)$$
$$= (4m + 1) \wedge (2n + 1)$$

Le plus grand diviseur est $4m + 1$, obtenu par exemple pour $n = 2m$.

Sol.7) Supposons par exemple $p \geq q$. On a :

$$(x^p - 1) \wedge (x^q - 1) = ((x^p - 1) - (x^q - 1)) \wedge (x^q - 1)$$
$$= (x^p - x^q) \wedge (x^q - 1)$$

$= x^q(x^{p-q} - 1) \wedge (x^q - 1)$
$= (x^{p-q} - 1) \wedge (x^q - 1)$ car $x^q \wedge (x^q - 1) = 1$

Ainsi, l'opération $(p, q) \to (p - q, q)$ sur les exposants de x laissent le PGCD invariant. En itérant la soustraction par q, il en est de même de l'opération $(p, q) \to (r, q)$, où r est le reste de la division euclidienne de p par q. Cela signifie qu'on peut appliquer sur les exposants (p, q) l'algorithme d'Euclide tout en laissant le PGCD $(x^p - 1) \wedge (x^q - 1)$ invariant. Lorsque l'algorithme d'Euclide se termine avec le couple d'exposants (d, d), où $d = p \wedge q$, on obtient :

$(x^p - 1) \wedge (x^q - 1) = (x^d - 1) \wedge (x^d - 1) = x^d - 1$

Sol.8) On a, pour tout n :

$$1 + b^2 + b^4 + b^6 + ... + b^{4n} = \frac{b^{4n+2} - 1}{b^2 - 1} = \frac{b^{2n+1} - 1}{b - 1} \times \frac{b^{2n+1} + 1}{b + 1}$$
$$= (1 + b + b^2 + b^3 + ... + b^{2n})(1 - b + b^2 - b^3 + ... + b^{2n})$$

Sol.9) a) $a \lozenge b = a \Leftrightarrow \sum_{k\geq 0} \min(a_k, b_k)\, 2^k = \sum_{k\geq 0} a_k\, 2^k \Leftrightarrow \forall\, k, \min(a_k, b_k) = a_k \Leftrightarrow \forall\, k, a_k \leq b_k \Leftrightarrow a \prec b$

b) pas de difficulté.

c) Si $c = a \lozenge b$ avec $c = \sum_{k\geq 0} c_k$, alors, pour tout k, $c_k = \min(a_k, b_k) \leq a_k$ donc $c \prec a$. De plus :

$$a + b - c = \sum_{k\geq 0} (a_k + b_k - c_k)\, 2^k$$

et l'égalité précédente donne la décomposition de $a + b - c$ en base 2 car, pour tout k, $a_k + b_k - c_k$ est égal à b_k ou a_k selon que $c_k = a_k$ ou b_k, donc vaut 0 ou 1. Comme $c_k \leq b_k$, on a $a_k \leq a_k + b_k - c_k$ donc $a \prec a + b - c$.

Réciproquement, supposons $c \prec a$ et $a \prec a + b - c$. Alors $\forall\, k$, $c_k \leq a_k$ donc $a - c = \sum_{k\geq 0} (a_k - c_k)\, 2^k$ est

la décomposition en base 2 de $a - c$ car, pour tout k, $a_k - c_k$ vaut 0 ou 1. Il s'agit maintenant d'étudier la décomposition binaire de $a + b - c$ pour la comparer à celle de a. Montrer par récurrence sur k que le calcul de $(a - c) + b$ ne nécessite aucune retenue lors de l'addition des chiffres binaires de $a - c$ avec ceux de b. Supposons que la somme des $k - 1$ premiers chiffres binaires n'aient pas donné lieu à une retenue (ce qui est vrai pour $k = 0$ puisqu'alors, il n'y a pas de chiffre qui précédent ceux de rang 0). Regardons ce qu'il en est lorsqu'on additionne $a_k - c_k$ avec b_k.
Le cas $a_k = 0$ et $c_k = 1$ ne se produit pas car $c_k \leq a_k$.
Si $a_k = c_k = 0$, alors $a_k - c_k = 0$. b_k peut être quelconque, et il n'y a pas de retenue au rang k.
Si $a_k = c_k = 1$, alors $a_k - c_k = 0$. Il n'y a pas de retenue au rang k, le chiffre binaire de rang k de $(a - c) + b$ étant $a_k - c_k + b_k = b_k$, mais nécessairement $b_k = 1$ car la condition $a \prec a + b - c$ impose alors que $a_k \leq b_k$.
Si $a_k = 1$, $c_k = 0$ et $b_k = 0$, il n'y a pas de retenue, le chiffre binaire de rang k de $(a - c) + b$ étant $a_k - c_k + b_k = 1$.
Si $a_k = 1$, $c_k = 0$ et $b_k = 1$, alors le calcul au rang k de la somme $(a - c) + b$ donne $a_k - c_k + b_k = 2$, ce qui conduira, dans la décomposition binaire de $(a - c) + b$ à un chiffre binaire nul au rang k et une retenue au rang $k + 1$. Mais ce cas est en contradiction avec $a \prec a + b - c$ car le chiffre binaire de rang k de $(a - c) + b$, dont on vient de voir qu'il est nul, devrait être supérieur ou égal à a_k qui vaut 1.

Ainsi, les seuls cas possibles sont, pour tout k :

$a_k = c_k = 0$ et b_k est quelconque

$a_k = c_k = 1$ et $b_k = 1$

$a_k = 1$, $c_k = 0$ et $b_k = 0$

On constate que, pour tout k, $c_k = \min(a_k, b_k)$, ce qui donne bien $c = a \lozenge b$.

Sol.10) Prendre $a = (n + 1)! + 2$. Alors, pour tout k variant de 2 à $n + 1$, k divise $(n + 1)! + k$ donc tous les entiers entre a et $a + n - 1$ ont un diviseur strict. Ils ne sont donc pas premiers.

Sol.11) Prendre une décomposition en facteurs premiers p_k .

$$a_i = \prod_k p_k^{\alpha_{ki}},\ \alpha_{ki} \geq 0$$

$$\text{PPCM}(a_1, ..., a_n) = \prod_k p_k^{\text{Max}(\alpha_{ki},\ 1 \leq i \leq n)}$$

$$a_1...a_n = \prod_k p_k^{\alpha_{k1}+...+\alpha_{kn}}$$

$$b_i = \prod_k p_k^{\alpha_{k1}+...+\alpha_{kn}-\alpha_{ki}}$$

$$\text{PGCD}(b_1, ..., b_n) = \prod_k p_k^{\text{Min}(\alpha_{k1}+...+\alpha_{kn}-\alpha_{ki},\ 1 \leq i \leq n)}$$

$$= \prod_k p_k^{\alpha_{k1}+...+\alpha_{kn} - \text{Max}(\alpha_{ki},\ 1 \leq i \leq n)}$$

$$= a_1...a_n/\text{PPCM}(a_1, ..., a_n)$$

Sol.12) Le PGCD de A + B et de PPCM(A, B) est égal à PGCD(A, B). En effet, soit D = A $\wedge$ B, A' et B' tels que A = DA', B = DB'. On a :

A' $\wedge$ B' = 1

A + B = D(A' + B')

A $\vee$ B = DA'B'

Puis :

(A' + B') $\wedge$ A'B' = 1

car tout diviseur premier de A' + B' et A'B' divise l'un des facteurs de A'B', par exemple A'. Il divise A' et A' + B' donc il divise B'. Il divise A' et B' donc il divise 1. Il n'existe donc pas de tel diviseur premier.

On a alors :

PGCD(A + B, A $\vee$ B) = D(A' + B') $\wedge$ DA'B' = D((A' + B') $\wedge$ A'B') = D

Sol.13) Posons A' et B' tels que A = DA', B = DB', D = A $\wedge$ B et donc A' $\wedge$ B' = 1. Alors M = DA'B'. Comme A' $\wedge$ B' = 1, un facteur premier de D ou bien divise A' mais pas B', ou bien divise B' mais pas A', ou bien ne divise ni A' ni B'. On regroupe ensemble les facteurs divisant A' avec A' lui-même dans U, ceux divisant B' avec B' lui-même dans V, et ceux ne divisant ni A' ni B'

indifféremment dans U ou V. Il n'y a donc pas unicité en général, sauf si D = 1. Dans ce dernier cas en effet, on a M = AB = UV avec A = KU, B = LV donc KL = 1 donc K = L = 1, U = A, V = B.
EXEMPLE :

A = 1260
B = 1320
M = 27720
D = 60 = $2^2 \times 3 \times 5$
A' = 21
B' = 22

On place le facteur 3 de D avec A', 2^2 avec B', et 5 indifféremment avec A' ou B'. On a ainsi :

U = 63
V = $22 \times 2^2 \times 5 = 440$

ou bien

U = $63 \times 5 = 315$
V = $22 \times 2^2 = 88$

Sol.14) Posons D = A $\wedge$ B $\wedge$ C, A', B', C' tels que A = DA', B = DB', C = DC'. Remarquons que A' $\wedge$ B' $\wedge$ C' = 1, car un diviseur commun E de A', B', C' est tel DE est un diviseur commun de A, B et C donc divise leur PGCD D donc DE = D donc E = 1. Posons X = B' $\wedge$ C', Y = A' $\wedge$ C', Z = A' $\wedge$ B'. On a Y $\wedge$ Z = A' $\wedge$ B' $\wedge$ C' = 1 or Y | A' et Z | A', donc YZ | A'. Il existe donc A" tel que :

A = DA' = DYZA"

De même, il existe B" et C" tels que :

B = DB' = DXZB"
C = DC' = DXYC"

Comme X = B' $\wedge$ D' = XZB" $\wedge$ XYC" = X(ZB" $\wedge$ YC"), on a ZB" $\wedge$ YC" = 1, et de même YA" $\wedge$ XB" = 1 et ZA" $\wedge$ XC" = 1. En particulier A" $\wedge$ B" = 1 et A" $\wedge$ X = 1, et de même en permutant circulairement les lettres. On a alors :

a)	A $\wedge$ B = D(A' $\wedge$ B') = DZ	
	A $\wedge$ C = DY	
	(A $\wedge$ B) $\vee$ (A $\wedge$ C) = DZ $\vee$ DY = DYZ	car Y $\wedge$ Z = 1
puis	B $\vee$ C = DX(ZB" $\vee$ YC") = DXYZB"C"	car ZB" $\wedge$ YC" = 1
	A $\wedge$ (B $\vee$ C) = DYZ(A" $\wedge$ XB"C") = DYZ	car A" $\wedge$ X = 1, A" $\wedge$ C" = 1 et A" $\wedge$ B" = 1 donc A" $\wedge$ XB"C" = 1

On a bien A $\wedge$ (B $\vee$ C) = (A $\wedge$ B) $\vee$ (A $\wedge$ C)

b)	A $\vee$ B = DZ(YA" $\vee$ XB") = DXYZA"B"	car YA" $\wedge$ XB" = 1
	A $\vee$ C = DXYZA"C"	de même
	(A $\vee$ B) $\wedge$ (A $\vee$ C) = DXYZA"	car B" $\wedge$ C" = 1
puis	B $\wedge$ C = DX	car ZB" $\wedge$ YC" = 1
	A $\vee$ (B $\wedge$ C) = D(YZA" $\vee$ X) = DXYZA"	car X $\wedge$ Y = X $\wedge$ Z = X $\wedge$ A" = 1 donc YZA" $\wedge$ X = 1 donc YZA" $\vee$ X = XYZA"

On a bien A $\vee$ (B $\wedge$ C) = (A $\vee$ B) $\wedge$ (A $\vee$ C)

Sol.15) On adapte la preuve de l'infinitude des nombres premiers. Soient p_1, ..., p_k des premiers congrus à – 1 mod 4. Considérons le produit P = $4 \times p_1 \times p_2 \times ... \times p_k - 1$. Il est de la forme $4n - 1$ et, en raisonnant modulo 4, on voit qu'il ne peut être produit de premiers uniquement de la forme $4n + 1$ car un tel produit est lui-même de la forme $4n + 1$. Donc il admet au moins un diviseur

premier q de la forme $4n - 1$. q est différent de p_1, p_2, ..., p_k car si q est égal à l'un des p_i, comme q divise P, q diviserait aussi -1. On a montré ainsi que, quelle que soit la collection finie de nombres premiers congrus à $-1 \bmod 4$, on peut toujours trouver un nombre premier supplémentaire de la même forme.
Une démonstration pour les premiers de la forme $4n + 1$ existe mais est beaucoup plus difficile. D'une manière générale, Dirichlet a prouvé en 1837 que toute suite arithmétique $(an + b)$, avec $a \wedge b = 1$, contenait une infinité de nombres premiers.

Sol.16) a) Soit p un diviseur premier de $p_1p_2...p_r \wedge (q_1 + ... + q_r)$, s'il en existe. Comme p divise $p_1p_2...p_r$, il est égal à l'un d'entre eux, par exemple $p = p_1$. p divise alors les q_i, pour $i \geq 2$, car $q_i = p_1...p_{i-1}p_{i+1}...p_r$. p divise donc la somme $q_2 + ... + q_r$. Comme p divise aussi $q_1 + ... + q_r$, il divise $q_1 = p_2...p_r$ ce qui est absurde, car $p = p_1$ est différent de tous les facteurs p_2, ..., p_r. Donc on a bien $p_1p_2...p_r \wedge (q_1 + ... + q_r) = 1$.
b) Pour toute collection finie de nombres premiers distincts p_1, ..., p_r, on peut toujours trouver un nombre premier supplémentaire. Il suffit de prendre un facteur premier de $q_1 + ... + q_r$.

Sol.17) a) Si p premier divisait b_i et b_j, alors p diviserait $jb_i - jb_i = j - i$, donc $p \leq n$, donc $p \mid n!$, et comme il divise $i \times n! + 1$, p diviserait 1.
Ou bien :

$$(i \times n! + 1) \wedge (j \times n! + 1) = (i \times n! + 1) \wedge ((j - i) \times n!) \text{ or } n! \wedge (i \times n! + 1) = 1$$

donc $(i \times n! + 1) \wedge ((j - i) \times n!) = (i \times n! + 1) \wedge (j - i)$ mais $j - i \leq n$ donc $j - i$ divise $n!$
donc $(i \times n! + 1) \wedge (j - i) = 1 \wedge (j - i) = 1$
b) Pour tout k variant de 1 à n, prendre un facteur premier p_k de b_k. Comme les b_k sont premiers entre eux, les p_k sont distincts. On est donc capable, pour tout n, de trouver n facteurs premiers distincts.

Sol.18) a) Pour tout i, $2^n \geq p_1^{k_1}p_2^{k_2}...p_r^{k_r} \geq p_i^{k_i} \geq 2^{k_i}$ donc $k_i \leq n$.
b) Les nombres compris entre 1 et 2^n sont définis la suite $(k_1, ..., k_r)$ intervenant dans leur décomposition en facteurs premiers. Comme $0 \leq k_i \leq n$, il y a au plus $(n + 1)^r$ tels nombres.
c) On a donc $r \geq \dfrac{n \ln(2)}{\ln(n + 1)}$ qui tend vers l'infini quand n tend vers l'infini.

Sol.19) a) On a $2^{F_n} - 2 = 2^{2^{2^n}+1} - 2 = 2\,(2^{2^{2^n}} - 1)$. Il suffit donc de montrer que F_n divise $2^{2^{2^n}} - 1$. Posons $N = 2^n$ et $Q = 2^{2^n - n}$, de sorte que $2^{2^{2^n}} - 1 = 2^{NQ} - 1$ et que $F_n = 2^N + 1$. $2^N + 1$ est bien un diviseur de $2^{NQ} - 1$ car, en posant $X = 2^N$:

$$2^{NQ} - 1 = X^Q - 1 = (X + 1)(X^{Q-1} - X^{Q-2} + X^{Q-3} + ... + X - 1) \quad \text{car Q est pair}$$

b) $F_{n-1}^2 - 2F_{n-1} + 2 = (2^{2^{n-1}} + 1)^2 - 2(2^{2^{n-1}} + 1) + 2$

$$= 2^{2^n} + 2 \times 2^{2^{n-1}} + 1 - 2 \times 2^{2^{n-1}}$$
$$= 2^{2^n} + 1$$
$$= F_n$$

c) Par récurrence, c'est vrai pour $n = 1$ ou $n = 2$ ($F_0 = 3$, $F_1 = 5 = F_0 + 2$, $F_2 = 17 = F_0F_1 + 2$). Si c'est vrai au rang n, alors :

$$F_0F_1F_2...F_n + 2 = (F_0F_1F_2...F_{n-1} + 2)F_n - 2F_n + 2 = F_n^2 - 2F_n + 2 = F_{n+1}$$

qui a été prouvé au b)
d) D'après le c), F_m divise $F_n - 2$, donc $F_m \wedge F_n = F_m \wedge (F_n - 2 + 2) = F_m \wedge 2 = 1$ car F_m est impair.
e) Pour tout n, prendre p_n nombre premier diviseur de F_n. Tous les p_n sont distincts d'après le d).

Sol.20) a) Les diviseurs de $2^n ab$ (y compris $2^n ab$) sont 1, 2, ..., 2^n, a, $2a$, ..., $2^n a$, b, $2b$, ..., $2^n b$, ab, $2ab$, ..., $2^n ab$. Leur somme $s(2^n ab) + 2^n ab$ vaut :

$$s(2^n ab) + 2^n ab = \sum_{k=0}^{n} 2^k(1 + a + b + ab)$$
$$= (2^{n+1} - 1)(1 + a)(1 + b) = (2^{n+1} - 1) \times 3 \times 2^n \times 3 \times 2^{n-1}$$
$$= 9 \times 2^{2n-1} \times (2^{n+1} - 1)$$

Les diviseurs de $2^n c$ sont 1, 2, ..., 2^n, c, $2c$, ..., $2^n c$. Leur somme $s(2^n c) + 2^n c$ vaut :

$$s(2^n c) + 2^n c = \sum_{k=0}^{n} 2^k(1 + c) = (2^{n+1} - 1) \times 9 \times 2^{2n-1}$$

Enfin :

$$2^n ab + 2^n c = 2^n \times (9 \times 2^{2n-1} - 3 \times 2^n - 3 \times 2^{n-1} + 1 + 9 \times 2^{2n-1} - 1)$$
$$= 2^n \times (9 \times 2^{2n} - 9 \times 2^{n-1})$$
$$= 2^{2n-1} \times 9 \times (2^{n+1} - 1)$$
$$= s(2^n ab) + 2^n ab = s(2^n c) + 2^n c$$

donc $s(2^n ab) = 2^n c$ et $s(2^n c) = 2^n ab$.
b) $220 = 2^2 \times 5 \times 11$ et $284 = 2^2 \times 71$. Prendre $n = 2$, $a = 11$, $b = 5$, $c = 71$.
$17296 = 2^4 \times 23 \times 47$ et $18416 = 2^4 \times 1151$. Prendre $n = 4$, $a = 47$, $b = 23$, $c = 1151$
$9363584 = 2^7 \times 191 \times 383$ et $9437056 = 2^7 \times 73727$. Prendre $n = 7$, $a = 383$, $b = 191$, $c = 73727$.

Sol.21) On a la décomposition en facteurs premiers. $56786730 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 31 \times 61$. Il suffit donc de montrer que $mn(m^{60} - n^{60})$ est divisible par chacun de ces nombres premiers p. C'est évidemment le cas si p divise m ou n. Reste à traiter le cas où ni m ni n ne sont divisibles par p. Montrons alors que p divise $m^{60} - n^{60}$. Selon le théorème de Fermat, pour tout entier x non divisible par p, $x^{p-1} \equiv 1 \bmod p$. Or, pour $p = 2, 3, 5, 7, 11, 13, 31, 61$, $p - 1 = 1, 2, 4, 6, 10, 12, 30, 60$. Dans chaque cas, 60 est un multiple de $p - 1$. On a donc :

$m^{p-1} \equiv 1 \bmod p$ d'après le théorème de Fermat

donc $m^{60} \equiv 1 \bmod p$ en élevant l'égalité précédente à la puissance $\dfrac{60}{p-1}$

de même, $n^{60} \equiv 1 \bmod p$, donc p divise $m^{60} - n^{60}$.
La démonstration donne un moyen de généraliser l'exercice. Soient p_1, p_2, ..., p_k des nombres premiers distincts, et soit $N = PPCM(p_1 - 1, p_2 - 1, ..., p_k - 1)$. Alors pour tout entier m et n, $mn(m^N - n^N)$ est divisible par $p_1 p_2 ... p_k$. Ainsi, on pourra vérifier que $mn(m^{5040} - n^{5040})$ est divisible par 33202626730.

Sol.22) (i) Existence de la décomposition. Décomposons m en produit de ses facteurs premiers p : $m = \prod_{p \text{ premier}} p^{k_p}$, $k_p > 0$. Soit d le PGCD des exposants k_p, et pour tout p, q_p l'entier tel que $k_p = dq_p$.

Prenons $a = \prod_{p \text{ premier}} p^{q_p}$ et $n = d$. On a alors $m = a^n$. De plus, a n'est pas une puissance t-ème d'un autre

entier $b = \prod_{p \text{ premier}} p^{r_p}$, $t \geq 2$, car sinon, on aurait $q_p = tr_p$ pour tout p, donc $k_p = dtr_p$ donc dt serait diviseur commun des k_p, en contradiction avec le fait que d est le PGCD des k_p.

(ii) Unicité de la décomposition. Si m peut s'écrire b^s avec $b = \prod_{p \text{ premier}} p^{r_p}$, alors l'égalité $m = a^n = b^s$ conduit à la relation $k_p = nq_p = sr_p$. s est un diviseur commun des k_p et n en est le PGCD. Donc s divise n, donc $b = a^{n/s}$ avec $\frac{n}{s}$ entier. Si b est supposé ne pas être puissance supérieure ou égal à 2 d'un autre entier, on a nécessairement $\frac{n}{s} = 1$ et $b = a$.

On peut aussi dire que, si A est l'ensemble des entiers dont m est une puissance, alors a est le plus petit élément de A, a étant "plus petit" que b étant pris aussi bien au sens "$a \leq b$", qu'au sens "$a \mid b$", ou même au sens "b est une puissance de a".

Sol.23) Si on applique l'identité de Bézout sur les polynômes $A(X) = 2X^3 + 3X$ et $B(X) = 2X^4 + 5X^2 + 1$, on trouve :

$$(1 + X^2)B(X) - (X^3 + 2X)A(X) = 1$$

Donc a fortiori $(1 + a^2)B(a) - (a^3 + 2a)A(a) = 1$, ce qui prouve que $A(a) \wedge B(a) = 1$ d'après le théorème de Bézout sur les entiers.

Sol.24) On cherche deux polynômes P et Q tels que $A = (X^2 + 1)P = 1 + (X^3 + 1)Q$. Il suffit d'établir l'identité de Bézout entre $X^2 + 1$ et $X^3 + 1$:

$$1 \times (X^3 + 1) + 0 \times (X^2 + 1) = X^3 + 1$$
$$0 \times (X^3 + 1) + 1 \times (X^2 + 1) = X^2 + 1$$
$$1 \times (X^3 + 1) - X \times (X^2 + 1) = -X + 1 \qquad L_3 \leftarrow L_1 - XL_2$$
$$X \times (X^3 + 1) + (1 - X^2) \times (X^2 + 1) = X + 1 \qquad L_4 \leftarrow L_2 + XL_3$$
$$(1 + X) \times (X^3 + 1) + (1 - X - X^2) \times (X^2 + 1) = 2 \qquad L_5 \leftarrow L_3 + L_4$$

Il suffit de prendre :

$$A = \frac{1 - X - X^2}{2} \times (X^2 + 1) = 1 - \frac{1 + X}{2} \times (X^3 + 1) = \frac{-X^4 - X^3 - X + 1}{2}$$

◆