Arithmétique
(par André Joyal)

Ces notes ont été préparées pour le camp mathématique UQAM 2003

Mathématiques sur Internet:

Wikipedia: The free encyclopedia. http://www.wikipedia.org/wiki/Mathematics
Eric Weisstein's World of Mathematics. http://mathworld.wolfram.com/

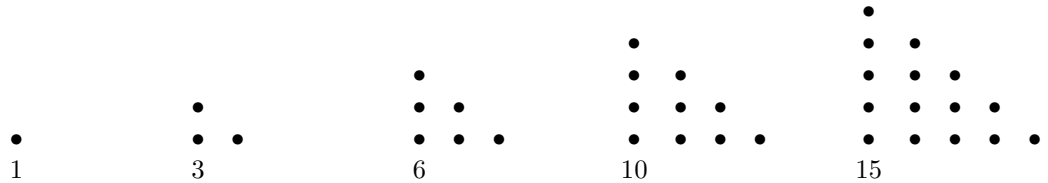
Synopsis:

0 Au commencement était Pythagore

Pythagore (572 à 501 avant notre ère) est né sur l'île de Samos en mer dÉgée, à proximité des côtes de l'Asie Mineure (Turquie). Durant sa jeunesse il voyage en Orient pour y rencontrer sages, savants et chefs religieux. C'était l'époque des enseignements de Zoroastre en Perse, de Bouddha aux Indes, de Confucius et de Lao-Tzu en Chine (mais on ne pense pas que Pythagore ait rencontré ces personnages). Au terme de ses voyages Pythagore s'établit à Crotone, ville grecque d'Italie, pour y fonder une secte religieuse et philosophique. Sur le plan mystique les Pythagoriciens croient en l'immortalité de l'âme humaine et en la possibilité de la réincarnation. Sur le plan philosophique leur doctrine peut se résumer à ceci: *la compréhension ultime des choses se trouve dans les nombres entiers.* Les Pythagoriciens attribuent une valeur mystique à certains nombres et les classent selon leurs propriétés arithmétiques ou géométriques. Ils disent qu'un entier est *parfait* s'il est égal à la somme de ses diviseurs propres. Par exemple, les nombres 6 et 28 sont parfaits car $6 = 3+2+1$ et $28 = 14+7+4+2+1$. Ils disent aussi que deux entiers sont *amicaux* si chacun est la somme des diviseurs propres de l'autre. Par exemple, 220 et 284 sont amicaux car on a

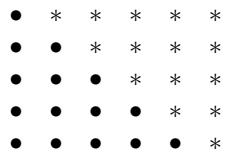
$$220 = 1+2+4+71+142$$
$$284 = 1+2+4+5+10+11+20+22+44+55+110.$$

Ils introduisent les nombres *triangulaires, carrés, pentagonaux, hexagonaux.* Par exemple, les nombres triangulaires sont $1, 3, 6, 10, 15, 21, \ldots$

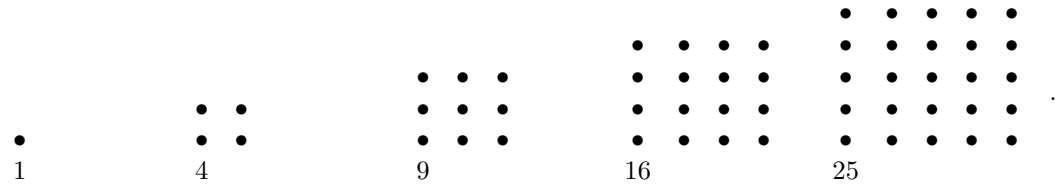


Les pythagoriciens utilisent ces représentations pour obtenir diverses relations. Par exemple, la figure suivante illustre le fait que le n-ième nombre triangulaire $T_n = 1 + 2 + 3 + \cdots + n$ vaut

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



Les nombres carrés sont $1, 4, 9, 16, 25, 36, \ldots$

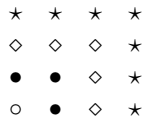


La figure suivante illustre le fait que la somme de deux nombres triangulaires successifs est un carré:

$$10 + 15 = 5^2$$

La figure suivant illustre le fait que la somme des n-premiers nombres impairs est un carré:

$$4^2 = 1 + 3 + 5 + 7$$



On attribue à Pythagore la découverte que $\sqrt{2}$ est un nombre irrationel. En réalité, les grecs ne connaissaient pas le concept moderne de nombres réels, rationnels ou irrationnels. Pour eux, un nombre est avant tout un *rapport* entre des quantités de même nature. Deux quantités sont dites *commensurables* (co-mesurables) si elles sont multiples entiers d'une troisième quantité; sinon elles sont *incommensurables*. Pythagore découvre que la diagonale d'un carré et son côté sont incommensurables.

Pythagore est l'auteur d'une théorie mathématique de l'harmonie musicale encore acceptée de nos jours. Il mesure la hauteur du son émi par une corde vibrante par la longeur de cette corde. Aujourd'hui, on mesure la hauteur d'un son par sa fréquence, c'est à dire par le nombre de battements par seconde. Nous décrirons la théorie de Pythagore en utilisant la notion de fréquence (la fréquence d'une corde vibrante est inversement proportionnelle à sa longuer). En expérimentant sur des instruments comme la harpe, la lyre et la cithare, Pythagore découvre que les sons de fréquences f, $2f$, $4f$, $8f$, ... etc sont *semblables* bien que de hauteur différente. L'*octave* est l'intervalle musical séparant une fréquence f de son double $2f$. Par exemple, si f est un *ré* alors $2f$ est un *ré* situé dans l'octave suivant. Pythagore découvre aussi qu'il faut mesurer l'intervalle musical séparant deux fréquences f et g par le *rapport* g/f (et non pas par la différence $g - f$ comme on pourrait le penser). Autrement dit, deux intervalles musicaux $[f, g]$ et $[u, v]$ sont *équivalents* si les rapports g/f et v/u sont égaux. Pythagore choisit de subdiviser l'octave $[f, 2f]$ en 12 intervalles musicaux égaux. Le choix de 12 n'est pas arbitraire car ce nombre possède un grand nombre de diviseurs. Pour subdiviser l'octave $[f, 2f]$ en deux intervalles égaux il faut trouver une fréquence intermédiaire $f < g < 2f$ pour laquelle

$$\frac{g}{f} = \frac{2f}{g}.$$

Ce qui donne $g = f\sqrt{2}$. Pour subdiviser l'octave $[f, 2f]$ en 12 intervalles égaux il faut trouver des fréquence intermédiaires

$$f - f_0 < f_1 < f_2 < f_3 < f_4 < f_5 < f_6 < f_7 < f_8 < f_9 < f_{10} < f_{11} < f_{12} = 2f$$

de sorte que

$$\frac{f_1}{f_0} = \frac{f_2}{f_1} = \frac{f_3}{f_2} = \frac{f_4}{f_3} = \frac{f_5}{f_4} = \frac{f_6}{f_5} = \frac{f_7}{f_6} = \frac{f_8}{f_7} = \frac{f_8}{f_7} = \frac{f_9}{f_8} = \frac{f_{10}}{f_9} = \frac{f_{11}}{f_{10}} = \frac{f_{12}}{f_{11}}.$$

Si r dénote ce rapport commun alors

$$r^{12} = \frac{f_1}{f_0} \cdot \frac{f_2}{f_1} \cdot \frac{f_3}{f_2} \cdot \frac{f_4}{f_3} \cdot \frac{f_5}{f_4} \cdot \frac{f_6}{f_5} \cdot \frac{f_7}{f_6} \cdot \frac{f_8}{f_7} \cdot \frac{f_8}{f_7} \cdot \frac{f_9}{f_8} \cdot \frac{f_{10}}{f_9} \cdot \frac{f_{11}}{f_{10}} \cdot \frac{f_{12}}{f_{11}} = \frac{f_{12}}{f_0} = \frac{2f}{f} = 2$$

Par suite, $r = 2^{\frac{1}{12}}$ et $f_i = fr^i$. Les musiciens disent que l'intervalle qui sépare f_i et f_{i+1} est un *demi-ton*. Les fréquences f_i pour $0 \leq i \leq 12$ forment une *gamme chromatique*. Si f_0 est un *do* cette gamme est constituée des notes suivantes:

$$\text{do}, \quad \text{do}^\sharp, \quad \text{ré}, \quad \text{ré}^\sharp, \quad \text{mi}, \quad \text{fa}, \quad \text{fa}^\sharp, \quad \textit{sol}, \quad \text{sol}^\sharp, \quad \text{la}, \quad \text{la}^\sharp, \quad \text{si}, \quad \text{do}.$$

Une troisième découverte de Pythagore concerne les *harmoniques* d'un son donné. Il découvre qu'un son de fréquence f vibre en accord (en harmonie) avec les sons de fréquences $2f, 3f, 4f, 5f, \ldots$. Les musiciens d'aujourd'hui disent que $3f$ est la *quinte* de f (mais c'est mal nommé). La fréquence $3f$ est située dans l'octave $[2f, 4f]$. Comme $2^{\frac{7}{12}} \times 2 = 2.99661 \simeq 3$, la quinte est la septième note qui suit $2f$ dans l'octave $[2f, 4f]$. Elle équivaut à la septième note qui suit f dans l'octave $[f, 2f]$. La quinte d'un *do* est un *sol* et la quinte d'un *mi* est un *si*.

Exercices pour la section 0

Le volume II des Élements d'Euclide porte sur une forme d'algèbre géométrique. Les identités suivantes y sont démontrées géométriquement:

1. $a(b + c + d + \cdots) = ab + ac + ad + \cdots$
2. $(a + b)a + (a + b)b = (a + b)^2$
3. $(a + b)a = ab + a^2$
4. $(a + b)^2 = a^2 + 2ab + b^2$
5. $(a + b)(a - b) + b^2 = a^2$
6. $(2a + b)b + a^2 = (a + b)^2$
7. $a^2 + b^2 = 2ab + (a - b)^2$
8. $4ab + (a - b)^2 = (a + b)^2$
9. $(a + b)^2 + (a - b)^2 = 2(a^2 + b^2)$

Exercice 1: Vérifier chacune des identités ci-haut.

D'après Pythagore, le carré de l'hypoténuse d'un triangle rectangle est égal à la somme des carrés des autres côtés. Inversement, si la relation $c^2 = a^2 + b^2$ est satisfaite alors le triangle de cotés (a, b, c) est rectangle. Si a, b et c sont des nombres entiers, on dit alors que le triplet (a, b, c) est *pythagoricien*. Par exemple, les triplets $(3, 4, 5)$ et $(5, 12, 13)$ sont pythagoriciens. Il est interessant de rechercher tous les triplets

pythagoriciens. Si un triplet (a, b, c) est pythagoricien alors il en est de même triplet (na, nb, nc) pour tout entier n. On se limite à rechercher les triplets pythagoricien sans diviseurs communs.

Exercise 2: Vérifier l'identité (attribuée à Platon)

$$(2ab)^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2.$$

Trouver un grand nombres de triplets pythagoriciens sans diviseurs communs.

On dit qu'une suite de nombres

$$a_1 \quad a_2 \quad a_3 \quad \cdots \quad a_n$$

est en *progression arithmétique* si la différence entre deux termes successifs $a_{i+1} - a_i$ est constante. On dit que cette constante est la *raison* de la progression arithmétique.

Exercice 3: Montrer que la différence $a_n - a_i$ entre le n-ième terme et le i-ième terme d'une progression arithmétique de raison r vaut $(n - i)r$.

Exercice 4: Montrer que la somme des termes $a_1, a_2, \cdots, a_n$ d'une progression arithmétique de raison r vaut

$$\frac{n(a_1 + a_n)}{2} = na_1 + r\frac{n(n-1)}{2} = na_n - r\frac{n(n-1)}{2}.$$

Le n-ième nombre triangulaire, carré, pentagonal, hexagonal, heptagonal, etc, est la somme des n premiers termes d'une progression arithmétiques de raison $1, 2, 3, 4, 5$, etc:

nombres triangulaires	:	1	2	3	4	5	6	7	$\cdots$
carrés	:	1	3	5	7	9	11	13	$\cdots$
pentagonaux	:	1	4	7	10	13	16	19	$\cdots$
$\cdots$	$\cdots$								

Exercice 5: Montrer que la n-ième nombre l-gonal vaut

$$n + (l - 2)\frac{n(n-1)}{2}.$$

Si $a_0, a_1, a_2, \cdots$ est suite de nombres, posons $\Delta a_n = a_{n+1} - a_n$. Alors on a

$$a_n = a_0 + \Delta a_0 + \Delta a_1 + \cdots + \Delta a_{n-1}$$

Par exemple, comme on a $\Delta n^2 = (n+1)^2 - n^2 = 2n + 1$, on obtient que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

De même, comme on a

$$\Delta n(n+1)(n+2) = (n+1)(n+2)(n+3) - n(n+1)(n+2) = 3(n+1)(n+2)$$

on obtient que

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Exercice 6: Trouver une expression pour la somme des n premiers nombres l-gonaux.

Exercise 7: Montrer que

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

Suggestion: Utiliser la décomposition $n^2 = n(n-1) + n$.

Si $a_0, a_1, a_2, \cdots$ est suite de nombres, posons $\Delta a_n = a_{n+1} - a_n$. Alors on a

$$a_n = a_0 + \Delta a_1 + \Delta a_2 + \cdots + \Delta a_{n-1}$$

Par exemple, comme on a $\Delta n^2 = (n+1)^2 - n^2 = 2n + 1$, on obtient que

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

De même, comme on a

$$\Delta n(n+1)(n+2) = (n+1)(n+2)(n+3) - n(n+1)(n+2) = 3(n+1)(n+2)$$

on obtient que

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Exercice 8: Montrer que

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

Suggestion: Utiliser l'identité $a^2 - b^2 = (a-b)(a+b)$ pour calculer la différence du second membre.

On définit la k-ième *puissance montante* de n comme le produit des k entiers suivant n, à partir de n:

$$(n)^k = n(n+1)\cdots(n+k-1).$$

On pose $(n)^0 = 1$ et $k! = (1)^k = 1 \cdot 2 \cdot 3 \cdots k$. Remarquer que

$$(n)^k = \frac{(n+k-1)!}{(n-1)!}.$$

Exercice 9: Montrer que $\Delta(n)^k = k(n+1)^{k-1}$. En déduire que

$$(1)^k + (2)^k + (3)^k + \cdots + (n)^k = \frac{(n)^{k+1}}{k+1}.$$

On définit la k-ième *puissance descendante* de n en posant

$$(n)_k = n(n-1)\cdots(n-k+1).$$

Remarquer que $(n)_k = 0$ si $n < k$. Remarquer que

$$(n)_k = \frac{n!}{(n-k)!}.$$

Exercice 10: Montrer que $\Delta(n)_k = k(n)_{k-1}$. En déduire que

$$(1)_k + (2)_k + (3)_k + \cdots + (n)_k = \frac{(n+1)_{k+1}}{k+1}.$$

Les coefficients du binôme

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

figurent dans le *triangle de Pascal*:

$$\begin{array}{ccccccccccccccccc}
 & & & & & & & 1 & & & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & & \\
 & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 & \\
 & & & & & & \cdots & & & & & & & & & &
\end{array}.$$

$$\begin{array}{ccccccccccccccccc}
 & & & & & & & \binom{0}{0} & & & & & & & & & \\
 & & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & & \\
 & & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & & \\
 & & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & & \\
 & & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & & \\
 & & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & & & \\
 & \binom{6}{0} & & \binom{5}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} & & & \\
\binom{7}{0} & & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7} & & \\
 & \binom{8}{0} & & \binom{8}{1} & & \binom{8}{2} & & \binom{8}{3} & & \binom{8}{4} & & \binom{8}{5} & & \binom{8}{6} & & \binom{8}{7} & & \binom{8}{8} \\
 & & & & & & & \cdots & & & & & & & & &
\end{array}.$$

Exercice 11: (Pascal) Utiliser la relation $(x+y)^{n+1} = (x+y)^n(x+y)$ pour montrer que l'on a

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Comparer avec la relation

$$\frac{(n+1)_k}{k!} = \frac{(n)_k}{k!} + \frac{(n)_k}{(k-1)!}.$$

En déduire que

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}.$$

Exercice 12: Montrer que l'on a

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \binom{n-3}{k-1} + \cdots + \binom{k-1}{k-1}.$$

On dit qu'une suite de nombres $a_1, a_2, a_3 \cdots$ est en *progression géométrique* de raison r si $a_{i+1}/a_i = r$.

Exercice 13: Montrer que le rapport a_n/a_i entre le n-ième terme et le i-ième terme d'une progression géométrique de raison r vaut $r^{(n-i)}$.

Exercice 14: Si $x \neq 1$, montrer que

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

En déduire que $1 + 2 + 2^3 + \cdots + 2^n = 2^n - 1$.

Exercice 15: Montrer que la somme des n premiers termes d'une progression géométrique $a_1, a_2, \cdots$ de raison $r \neq 1$ vaut

$$\frac{a_{n+1} - a_1}{r - 1} = a_1 \frac{r^{n+1} - 1}{r - 1}.$$

1. Arithmétique et nombres premiers

Soit $\mathbf{N}$ l'ensemble des entiers positifs ou nuls. Si $n \in \mathbf{N}$ nous dénoterons par $n\mathbf{N}$ l'ensemble des multiples entiers de n:

$$n\mathbf{N} = \{na \mid a \in \mathbf{N}\}.$$

Nous dirons qu'un entier $n \in \mathbf{N}$ *divise* un entier $m \in \mathbf{N}$, et nous écrirons $n \mid m$, si $m \in n\mathbf{N}$.

Exercice : Montrer que si $0 \mid n$ alors $n = 0$.

Proposition 1.1.
(i) On a $n \mid mn$, $n \mid 0$, $1 \mid n$ et $n \mid n$;
(ii) si $m \mid n$ et $n \mid r$ alors $m \mid r$.
(iii) si $n \mid m$ et $m \mid n$ alors $m = n$.
(iv) si $n \mid a$ et $n \mid b$ alors $n \mid (a + b)$.
(iii) si $n \mid a$ et $n \mid a + r$ alors $n \mid r$.

Preuve: (i) C'est clair. (ii) si $n = mq$ et $r = np$ alors $r = mqp$. (ii) si $n = mq$ et $m = np$ alors $n = npq$; donc $1 = pq$ si $n \neq 0$: dans ce cas $p = q = 1$ et $n = m$; si $n = 0$ alors $m = 0p = 0$. (iii) si $a = np$ et $b = nq$ alors $a + b = n(p + q)$. (iv) si $a = np$ et $a + r = nq$ alors $r = n(q - p)$.

Definition 1.2: Nous dirons qu'un entier $n > 1$ est *composé* s'il admet une factorisation $n = ab$ avec $a, b > 1$; sinon, nous dirons qu'il est *premier*.

Il y a 25 nombres premiers ≤ 100:

2	3	5	7	11	13	17	19	23	29	31	37	41
	43	47	53	59	61	67	71	73	79	83	89	97

Le plus petit diviseur > 1 d'un entier est forcément premier.

Proposition 1.3. *Tout entier composé n possède un diviseur $1 < d \leq \sqrt{n}$.*

Preuve: Si n est composé alors on a une factorisation $n = ab$ avec $a < n$ et $b < n$. Si on avait $a > \sqrt{n}$ et $b > \sqrt{n}$ on aurait aussi $ab > \sqrt{n}\sqrt{n} = n$, ce qui est absurde puisque $ab = n$. CQFD

Si un entier $n > 1$ n'est pas divisible par aucun nombre premier $\leq \sqrt{n}$ alors il est premiers. Par exemple, 101 est premier car il n'est divisible ni par 2, ni par 3, ni par 5 et ni par 7.

La proposition 1.3 est à la base de la méthode du *crible d'Ératosthène* pour dresser la liste de tous les nombres premiers $\leq N$. On procède par élimination successive à partir des nombres impairs $\leq N$. Par exemple, pour obtenir la liste des nombres premiers ≤ 100 on commence par faire la liste des nombres impairs ≤ 100 (à l'exception de 2 que l'on ajoute à la liste):

$$\begin{array}{c} 2^* \quad 3 \quad 5 \quad 7 \quad 9 \quad 11 \quad 13 \quad 15 \quad 17 \quad 19 \quad 21 \quad 23 \quad 25 \quad 27 \quad 29 \quad 31 \quad 33 \\ 35 \quad 37 \quad 39 \quad 41 \quad 43 \quad 45 \quad 47 \quad 49 \quad 51 \quad 53 \quad 55 \quad 57 \quad 59 \quad 61 \quad 63 \quad 65 \quad 67\,. \\ 69 \quad 71 \quad 73 \quad 75 \quad 77 \quad 79 \quad 81 \quad 83 \quad 85 \quad 87 \quad 89 \quad 91 \quad 93 \quad 95 \quad 97 \quad 99. \end{array}$$

Di on élimine ensuite les multiples de 3 (sauf 3), il reste:

$$\begin{array}{c} 2 \quad 3^* \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 25 \quad 29 \quad 31 \\ 35 \quad 37 \quad 41 \quad 43 \quad 47 \quad 49 \quad 53 \quad 55 \quad 59 \quad 61 \quad 65 \quad 67 \\ 71 \quad 73 \quad 77 \quad 79 \quad 83 \quad 85 \quad 89 \quad 91 \quad 95 \quad 97. \end{array}$$

Si on élimine ensuite les multiples de 5 (sauf 5), il reste

$$\begin{array}{c} 2 \quad 3 \quad 5^* \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29 \quad 31 \\ 37 \quad 41 \quad 43 \quad 47 \quad 49 \quad 53 \quad 59 \quad 61 \quad 67 \\ 71 \quad 73 \quad 77 \quad 79 \quad 83 \quad 89 \quad 91 \quad 97. \end{array}$$

Si on élimine ensuite les multiples de 7 (sauf 7), il reste

$$\begin{array}{c} 2 \quad 3 \quad 5 \quad 7^* \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29 \quad 31 \\ 37 \quad 41 \quad 43 \quad 47 \quad 53 \quad 59 \quad 61 \quad 67 \\ 71 \quad 73 \quad 79 \quad 83 \quad 89 \quad 97. \end{array}$$

Le criblage est terminé car $11^2 > 100$. Il ne reste alors que des nombres premiers. On en compte 25.

Tout entier $n > 1$ est un produit de nombres premiers. Démontrons-le, même si ça peut paraitre évident. Si n n'est pas premier, divisons-le par son plus petit diviseur d_1. Ce dviseur est forcément premier. Si le quotient n/d_1 n'est pas premier, divisons-le par son plus petit diviseur d_2. Si le quotient n/d_1d_2 n'est pas premier, divisons-le par son plus petit diviseur premier d_3. Continuant ainsi, on obtient une suite décroissante d'entiers

$$n > (n/d_1) > (n/d_1d_2) > (n/d_1d_2d_3) > \cdots.$$

Cette suite ne peut se prolonger indéfiniment. Après un certain nombre $k < n$ de divisions le quotient $q = n/d_1d_2 \cdots d_k$ sera premier. On obtient alors une décomposition en facteurs premiers

$$n = d_1 \cdot d_2 \cdot d_3 \cdots d_k \cdot q.$$

Théorème 1.4. *(Théorème fondamental de l'Arithmétique) Tout nombre entier $n > 1$ se factorise en produit de nombres premiers. Cette factorisation est unique à l'ordre des facteurs près.*

L'unicité de la factorisation peut paraitre évidente, du moins pour les entiers familiers. Comme on n'en trouve pas mention dans les textes anciens, elle semble avoir été admise par les mathmaticiens de l'antiquité

Mais qu'en est-il de la factorisation des entiers grands? Supposons par exemple que Pierre ait trouvé une décomposition en facteurs premiers

$$\begin{aligned} 235711131719232931374143 &= 4546201954997 \cdot 51847923619 \\ &= p \cdot q, \end{aligned}$$

et que Paul en ait trouvé une autre

$$\begin{aligned} 235711131719232931374143 &= 1239743299603 \cdot 190128982181 \\ &= p' \cdot q'. \end{aligned}$$

En quoi cela contredit-il notre intuition? L'unicité d'une décomposition en facteurs premiers pourrait être vrai pour des entiers petits mais fausse pour certains entiers très grands. Il ne faut pas oublier qu'il y a des entiers GIGANTESQUES, incroyablement grands. Considérons par exemple la suite entiers

$$1+2, \quad 1+2^2, \quad 1+2^{2^2}, \quad 1+2^{2^{2^2}}, \quad 1+2^{2^{2^{2^2}}}, \ldots$$

Quelle est la nature arithmétique de l'entier occupant par exemple la 100^e position de la suite? Il est physiquement impossible de décrire le développement décimal de cet entier car l'univers semble trop petit. Malgré sa taille gigantesque, il faut réaliser qu'il est minuscule à comparer aux véritables géants qui peuplent en très grande majorité l'ensemble des nombres naturels. Peut-être objecterez-vous que les entiers gigantesques ont peu d'importance. Mais vous conviendrez avec moi que c'est une bonne chose que de savoir que l'unicité de la factorisation est vrai pour tout les entiers sans aucune exception. La première démonstration est due à Gauss. Elle est basé sur le lemme suivant:

Lemme 1.5. *(Gauss) Si un nombre premier p divise le produit de deux nombres entiers alors il divise l'un des facteurs.*

Nous en donnerons une démonstration plus bas (après la proposition 10) . On peut reformuler le lemme de la façon suivante: si un entier q divise le produit mn de deux entiers sans diviser m et n, alors q n'est pas premier. Par exemple, remarquer que le facteur $p = 4546201954997$ de Pierre ne divise aucun des facteurs trouvés par Paul. En effet, p est plus grand que chacun de ces facteurs. Donc p n'est pas premier. Pierre a fait une erreur. On voit que l'on peut montrer qu'un nombre est composé sans en calculer de facteurs!

Rappelons que le *plus grand diviseur commun* de deux entiers non nuls a et b est le plus grand des entiers divisant à la fois a et b; on le dénote par $\text{pgdc}(a, b)$. Par exemple, le plus grand diviseur commun de 60 et de 72 est 12 car les diviseurs de 60 sont 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60, et les diviseurs de 72 sont 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72. On dit que a et b sont *relativement premiers* (ou *sans diviseurs communs*) si $\text{pgdc}(a, b) = 1$. Nous écrirons $a \perp b$ pour indiquer que a et b sont relativement premiers. Par exemple, on a $72 \perp 125$. Le *plus petit multiple commun* de m et n est le plus petit des entiers > 0 divisés à la fois par m et n; on le dénote par $\text{ppmc}(m, n)$. Par exemple, on a $\text{ppmc}(60, 72) = 360$.

Théorème 1.6. *(Division euclidienne) Soit b un entier > 0. Alors pour tout entier $a \in \mathbf{N}$ il existe des entiers q et r tels que*

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

Les entiers q et r sont déterminés uniquement par a et b.

Preuve: Soit q le plus grand des entiers $\leq a/b$. Par definition, on a $q \leq a/b$ et $a/b < q+1$. Par suite, $qb \leq a$ et $a < (q+1)b$. Posons $r = a - bq$. Alors on a $r \geq 0$ et $r < b$. Cela montre l'existence du couple (q, r). L'unicité est évidente car la condition $0 \leq a - bq < b$ équivaut à la condition $qb \leq a < (q+1)b$, qui équivaut aux condition $q \leq a/b$ et $a/b < q + 1$. CQFD

On dit que que r est le *reste* de la division de a par b, et que q le *quotient*. Le reste est nul ssi b divise a.

Lemme 1.7. *Si $a = bq + r$ avec $r > 0$, alors* $\mathrm{pgdc}(a, b) = \mathrm{pgdc}(b, r)$.

Preuve: Si un entier d divise a et b alors il divise aussi $r = a - bq$ par la proposition 2(i) et (ii). Inversement, si d divise b et r alors il divise $a = bq + r$ par la même proposition. Cela montre que tout diviseur commun de a et b est un diviseur commun de b et r. En particulier, le plus grand diviseur commun de a et b est égal au plus grand diviseur commun de b et r. CQFD

L'*algorithme d'Euclide* pour calculer le plus grand diviseur commun de deux entiers $a, b \geq 1$ est l'un des plus anciens et l'un des plus importants de mathématiques. Il est basé sur le lemme 5. On effectue successivement les divisions euclidiennes suivantes jusqu'à l'obtention d'un reste nul:

$$\begin{aligned}
a &= bq_1 + r_1 \quad \text{avec} \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2 \quad \text{avec} \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 \quad \text{avec} \quad 0 < r_3 < r_2 \\
&\cdots \qquad\qquad\qquad\quad \cdots \\
r_{n-2} &= r_{n-1} q_n + r_n \quad \text{avec} \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0.
\end{aligned}$$

Alors on a $\mathrm{pgdc}(a, b) = r_n$. Autrement dit, le $\mathrm{pgdc}(a, b)$ est *le dernier reste non nul* de la suite de division. En effet, d'après le lemme, on a

$$\mathrm{pgdc}(a, b) = \mathrm{pgdc}(b, r_1) = \mathrm{pgdc}(r_1, r_2) = \cdots = \mathrm{pgdc}(r_{n-1}, r_n).$$

Mais $\mathrm{pgdc}(r_{n-1}, r_n) = r_n$ car r_n divise r_{n-1}.

Par exemple, on a $\mathrm{pgdc}(3456, 465) = 3$ car

$$\begin{aligned}
3456 &= 465 \cdot 7 + 201 \\
465 &= 201 \cdot 2 + 63 \\
201 &= 63 \cdot 3 + 12 \\
63 &= 12 \cdot 5 + 3 \\
12 &= 3 \cdot 4 + 0.
\end{aligned}$$

Calculons le pgcd entre le facteur $p = 4546201954997$ de Pierre et le facteur $p' = 1239743299603$ de Paul.

$$\begin{aligned}
4546201954997 &= 1239743299603 \cdot 3 + 826972056188 \\
1239743299603 &= 826972056188 \cdot 1 + 412771243415 \\
826972056188 &= 412771243415 \cdot 2 + 1429569358 \\
412771243415 &= 1429569358 \cdot 288 + 1055268311 \\
1429569358 &= 1055268311 \cdot 1 + 374301047 \\
1055268311 &= 374301047 \cdot 2 + 306666217 \\
374301047 &= 306666217 \cdot 1 + 67634830 \\
306666217 &= 67634830 \cdot 4 + 36126897 \\
67634830 &= 36126897 \cdot 1 + 31507933 \\
36126897 &= 31507933 \cdot 1 + 4618964 \\
31507933 &= 4618964 \cdot 1 + 3794149 \\
4618964 &= 3794149 \cdot 1 + 824815 \\
3794149 &= 824815 \cdot 1 + 494889 \\
824815 &= 494889 \cdot 1 + 329926 \\
494889 &= 329926 \cdot 1 + 164963 \\
329926 &= 164963 \cdot 1 + 0
\end{aligned}$$

Donc $\text{pgcd}(p, p') = 164963$. On obtient par suite les factorisations

$$p = 164963 \cdot 27558919, \quad \text{et} \quad p' = 164963 \cdot 7515281.$$

Cela permet de calculer la factorisation suivante de l'entier de départ:

$$n = 23571113171923293137 4143 = 6899 \cdot 164963 \cdot 7515281 \cdot 27558919.$$

La factorisation de Pierre s'obtient en regroupant les facteurs comme suit

$$p \cdot q = (164963 \cdot 27558919) \cdot (6899 \cdot 7515281),$$

et celle de Paul en regroupant les facteurs comme suit

$$p' \cdot q' = (164963 \cdot 7515281) \cdot (6899 \cdot 27558919).$$

Le résultat suivant est la clé qui permettra de démontrer le lemme de Gauss.

Théorème 1.8. *(Relation de Bézout) Pour tout entiers $a, b \geq 1$, il existe des entiers $u, v \in \mathbf{Z}$ tels que*

$$\text{pgdc}(a, b) = u \cdot a + v \cdot b.$$

Preuve: On peut supposer que $a \geq b$. Nous raisonnerons par induction sur b. Le résultat est évident si $b = 1$ et plus généralement si $b \mid a$ car alors $\text{pgdc}(a, b) = b = 0 \cdot a + 1 \cdot b$. Sinon, on a $a = bq + r$ avec $0 < r < b$. Dans ce cas on a $\text{pgdc}(a, b) = \text{pgdc}(b, r)$ par le lemme ?. Comme $r < b$ on peut supposer (par l'hypothèse d'induction) que l'on a $\text{pgdc}(b, r) = xb + yr$ pour des entiers x et y. Par suite,

$$\text{pgdc}(a, b) = xb + yr = xb + y(a - br) = ya + (x - yr)b.$$

CQFD

Proposition 1.9. *Deux entiers a et b sont relativement premiers si et seulement si il existe des entiers $u, v \in \mathbf{Z}$ tels que $1 = ua + vb$.*

Preuve: Si $\text{pgdc}(a, b) = 1$ alors il existe des entiers $u, v \in \mathbf{Z}$ tels que $1 = ua + vb$ d'après le théorème 6. Inversement, supposons qu'il existe des entiers $u, v \in \mathbf{Z}$ tels que $1 = ua + vb$. Tout diviseur commun $d > 0$ de a et de b doit diviser $ua + vb = 1$ par la proposition ?. Cela montre que $d = 1$. CQFD

Proposition 1.10. *Si $n \perp a$ et $n \perp b$, alors $n \perp ab$.*

Preuve: Si $n \perp a$, alors il existe des entiers s, t tels que $1 = sa + tn$ d'après 9. De même, si $b \perp n$ alors il existe des entiers u, v tels que $1 = ub + vn$. En faisant le produit de ces égalités, on obtient que

$$1 = (sa + tn)(ub + vn) = (su) \cdot (ab) + (sav + tub + tvn) \cdot n.$$

Elle entraîne par la proposition 9 que $n \perp ab$. CQFD

Nous pouvons maintenant démontrer le lemme de Gauss: *Si un nombre premier p divise le produit de deux nombres entiers alors il divise l'un des facteurs.* Il suffit de montrer que si un nombre premier p ne divise pas deux entiers a et b alors il ne divise pas leur produit ab. En effet, si p ne divise pas a alors on a $p \perp a$ puisque p est premier. De même, on a $p \perp b$. Par suite, $p \perp ab$ par le proposition 10. CQFD

Nous pouvons maintenant démontrer le théorème fondamental de l'arithmétique: *Tout nombre entier $n > 1$ se factorise en produit de nombres premiers. Cette factorisation est unique à l'ordre des facteurs près.* L'existence d'une factorisation en facteurs premiers a déjà été démontré. Il reste à démontrer l'unicité. Nous allons raisonner par induction sur n. Le résultat est clair si n est premier. On peut donc supposer que n est composé. Supposons que l'on ait deux factorisations en facteurs premiers

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r.$$

On peut ranger les facteurs en ordre croissant $p_1 \leq p_2 \leq \cdots \leq p_k$ et $q_1 \leq p_2 \leq \cdots \leq q_r$. Nous allons montrer que $k = r$ et que $p_i = q_i$ pour tout $1 \leq i \leq k$. Commencons par montrer que $p_k = q_r$. Le facteur p_k doit diviser l'un des facteurs q_j d'après le lemme de Gauss. On a alors $p_k \leq q_r$ car on a $q_j \leq q_r$. Le même raisonnement montre que $q_r \leq p_k$. Nous avons montré que $p_k = q_r$. Par suite,

$$\frac{n}{p_k} = p_1 p_2 \cdots p_{k-1} = q_1 q_2 \cdots q_{r-1}.$$

Comme $n/p_k < n$, l'hypothèse d'induction entraîne que $k - 1 = r - 1$ et que $p_i = q_i$ pour tout $1 \leq i \leq k - 1$. CQFD

Il est commode de regrouper les facteurs égaux d'une factorisation en facteurs premiers. Cela donne une factorisation dont les facteurs sont des puissances de nombres premiers distincts:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Si on accepte les exposants nuls, on peut écrire que $n = 2^a 3^b 5^c \cdots$ avec $a, b, c, \ldots \geq 0$.

Il est facile d'obtenir tous les diviseurs d'un entier n à partir d'une décomposition de cet entier en puissance de facteurs premiers. Si $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ alors les diviseurs d de n sont de la forme $d = p_1^{b_1} \cdots p_k^{b_k}$ pour des exposants $b_i \leq a_i$ pour tout $1 \leq i \leq k$.

Il est facile de calculer le produit deux entiers à partir d'une décomposition de ces entiers en puissance de facteurs premiers. Si

$$m = p_1^{a_1} \cdots p_k^{a_k} \quad \text{et} \quad m = p_1^{b_1} \cdots p_k^{b_k}$$

alors on a

$$mn = p_1^{a_1+b_1} \cdots p_k^{a_k+b_k}.$$

De même, on a

$$\text{pgdc}(m, n) = p_1^{a_1 \wedge b_1} \cdots p_k^{a_k \wedge b_k} \quad \text{et} \quad \text{ppmc}(m, n) = p_1^{a_1 \vee b_1} \cdots p_k^{a_k \vee b_k},$$

où $a \wedge b$ désigne désigne le plus petit de deux entiers a et b, et où $a \vee b$ désigne désigne le plus grand.

Proposition 1.11. *Pour tout entier $m, n \geq 1$, on a*

$$\text{pgdc}(m, n) \cdot \text{ppmc}(m, n) = m \cdot n.$$

Preuve: C'est une conséquence de l'identité $a \wedge b + a \vee b = a + b$. CQFD

En particulier, si $m \perp n$ alors $\text{ppmc}(m, n) = m \cdot n$.

Voici quelques exemples amusants de factorisation. Le nombre $M_n(a) = 1 + a + a^2 + \cdots + a^{n-1}$ est composé si n est composé. En effet, l'identité

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

entraîne que l'on a

$$a^{mn} - 1 = (a^m - 1)(1 + a^m + a^{2m} + \cdots + a^{(n-1)m})$$

et par suite que $M_{mn}(a) = M_m(a)M_n(a^m)$. On dit que l'entier $M_n(10)$ est un *repunit* car son développement décimal est formé du chiffre 1 répété n-fois.

$$
\begin{aligned}
M_2(10) = 11 &= 11 \\
M_3(10) = 111 &= 3 \cdot 37 \\
1111 &= 11 \cdot 101 \\
M_5(10) = 11111 &= 41 \cdot 271 \\
111111 &= 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \\
M_7(10) = 1111111 &= 239 \cdot 4649 \\
11111111 &= 11 \cdot 73 \cdot 101 \cdot 137 \\
111111111 &= 3^2 \cdot 37 \cdot 333667 \\
1111111111 &= 11 \cdot 41 \cdot 271 \cdot 9091 \\
M_{11}(10) = 11111111111 &= 21649 \cdot 513239 \\
111111111111 &= 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901 \\
M_{13}(10) = 1111111111111 &= 53 \cdot 79 \cdot 265371653 \\
11111111111111 &= 11 \cdot 239 \cdot 4649 \cdot 909091 \\
111111111111111 &= 3 \cdot 31 \cdot 37 \cdot 41 \cdot 271 \cdot 2906161 \\
1111111111111111 &= 11 \cdot 17 \cdot 73 \cdot 101 \cdot 137 \cdot 5882353 \\
M_{17}(10) = 11111111111111111 &= 2071723 \cdot 5363222357 \\
111111111111111111 &= 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 52579 \cdot 333667 \\
M_{19}(10) = 1111111111111111111 &= 1111111111111111111 \\
11111111111111111111 &= 11 \cdot 41 \cdot 101 \cdot 271 \cdot 3541 \cdot 9091 \cdot 27961 \\
111111111111111111111 &= 3 \cdot 37 \cdot 43 \cdot 239 \cdot 1933 \cdot 4649 \cdot 10838689 \\
1111111111111111111111 &= 11^2 \cdot 23 \cdot 4093 \cdot 8779 \cdot 21649 \cdot 513239 \\
M_{23}(10) = 11111111111111111111111 &= 11111111111111111111111 \\
111111111111111111111111 &= 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 73 \cdot 101 \cdot 137 \cdot 9901 \cdot 99990001
\end{aligned}
$$

On dit que l'entier $M_n = M_n(2) = 2^n - 1$ est un *nombre de Mersenne*. Il est souvent premier si n est

premier.

$$
\begin{aligned}
M_2 &= 3\\
M_3 &= 7\\
M_5 &= 31\\
M_7 &= 127\\
M_{11} &= 23 \cdot 89\\
M_{13} &= 8191\\
M_{17} &= 131071\\
M_{19} &= 524287\\
M_{23} &= 47 \cdot 178481\\
M_{29} &= 233 \cdot 1103 \cdot 2089\\
M_{31} &= 2147483647\\
M_{37} &= 223 \cdot 616318177\\
M_{41} &= 13367 \cdot 164511353\\
M_{43} &= 431 \cdot 9719 \cdot 2099863\\
M_{47} &= 2351 \cdot 4513 \cdot 13264529\\
M_{53} &= 6361 \cdot 69431 \cdot 20394401\\
M_{59} &= 179951 \cdot 3203431780337\\
M_{61} &= 2305843009213693951\\
M_{67} &= 193707721 \cdot 761838257287\\
M_{71} &= 48544121 \cdot 212885833 \cdot 228479\\
M_{73} &= 439 \cdot 2298041 \cdot 9361973132609\\
M_{79} &= 2687 \cdot 202029703 \cdot 1113491139767\\
M_{83} &= 167 \cdot 57912614113275649087721\\
M_{89} &= 618970019642690137449562111\\
M_{91} &= 127 \cdot 911 \cdot 8191 \cdot 112901153 \cdot 23140471537\\
M_{97} &= 11447 \cdot 13842607235828485645766393
\end{aligned}
$$

Marin Mersenne (1588-1648) est un moine mineur, mathématicien et physicien, qui vécut à Paris. Il utilisa sa cellule monastique comme lieu de rencontres entre Pascal, Fermat et Roberval. Il défendit les idées de Galilé. Il écrivit l'*Harmonie Universelle*, un traité de physique-mathématique. Mersenne affirma que M_p est premier pour $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ et 257, mais qu'il est composé pour les autres valeurs de p premier ≤ 257. L'affirmation de Mersenne contenait cinq erreurs: M_{67} et M_{257} sont composés alors que M_{61}, M_{89} et M_{107} sont premiers. L'historien des mathématiques E.T. Bell [] raconte comment le mathématicien américain F.N. Cole présenta sa découverte d'une factorisation de M_{67} lors d'une rencontre de l'American Mathematical Society en 1903. Sans prononcer un seul mot, Cole effectua la multiplication suivante sur un tableau noir:

$$193707721 \times 761838257287 = 147573952589676412927 = 2^{67} - 1.$$

Lorqu'il déposa sa craie, un tonnerre d'applaudissements éclata dans la salle. Les nombres premiers de

Mersenne pour $p \leq 257$ sont les suivants:

$$\begin{aligned}
M_2 &= 3 \\
M_3 &= 7 \\
M_5 &= 31 \\
M_7 &= 127 \\
M_{13} &= 8191 \\
M_{17} &= 131071 \\
M_{19} &= 524287 \\
M_{31} &= 2147483647 \\
M_{61} &= 2305843009213693951 \\
M_{89} &= 618970019642690137449562111 \\
M_{107} &= 162259276829213363391578010288127 \\
M_{127} &= 170141183460469231731687303715884105727
\end{aligned}$$

On connait aujourd'hui (juillet 2003) 39 nombres premiers de Mersenne. Le dernier $M_{13466917}$ est le plus grand nombre premier connu à ce jour. Il comporte plus de 4 millions de décimales.

Les nombres premiers de Mersenne apparaissent dans le théorème d'Euclide sur les nombres parfaits (pour la définition des nombres parfaits voir la section 0).

Proposition 1.12. *(Euclide) Si le nombre $q = 2^p - 1$ est premier alors le nombre $2^{p-1}q$ est parfait.*

Preuve: Supposons q premier. Calculons la somme σ de tous les diviseurs propres de $2^{p-1}q$. Ces diviseurs propres sont de deux formes: (i) les divieurs $1, 2 \ldots, 2^{p-1}$; (ii) les divieurs $q, 2q, \ldots, 2^{p-2}q$. Comme on a

$$2^p - 1 = 1 + 2 + \cdots + 2^{p-1} \quad \text{et} \quad (2^{p-1} - 1)q = q + 2q + \cdots + 2^{p-2}q$$

on obtient que $\sigma = (2^p - 1) + 2^{p-1}q - q = 2^{p-1}q$. CQFD

Les nombres parfaits d'Euclide sont pairs. Inversement, Euler a montré qu'un nombre parfait pair est forcément un nombre parfait d'Euclide. On ignore s'il existe des nombres parfaits impairs. On connait aujourd'hui (juillet 2003) 39 nombres parfaits.

Le résultat suivant d'Euclide est fameux :

Proposition 1.13. *(Euclide) Il existe une infinité de nombres premiers.*

Preuve: Montrons que toute liste finie des nombres premiers est forcément incomplète. Si $p_1, p_2, \ldots, p_n$ sont des nombres premiers posons $N = p_1 p_2, \ldots p_n$. Soit p un diviseur premier de $1 + N$. Comme N et $N + 1$ sont relativement premiers, p ne peut diviser N. Donc p est différent de p_i (puisque p_i divise N). CQFD

La preuve d'Euclide fournit un algorithme pour obtenir des nombres premiers de plus en plus grands:

$$\begin{aligned}
2 + 1 &= 3 \\
2 \cdot 3 + 1 &= 7 \\
2 \cdot 3 \cdot 7 + 1 &= 43 \\
2 \cdot 3 \cdot 7 \cdot 43 + 1 &= 13 \cdot 139 \\
2 \cdot 3 \cdot 7 \cdot 13 \cdot 43 \cdot 139 + 1 &= 3263443 \\
2 \cdot 3 \cdot 7 \cdot 13 \cdot 43 \cdot 139 \cdot 3263443 + 1 &= 547 \cdot 607 \cdot 1033 \cdot 31051 \\
&\ldots
\end{aligned}$$

L'algorithme n'est pas efficace car il faut factoriser des entiers très grands, ce qui est difficile.

Il a plusieurs démonstrations de l'infinitude des nombres premiers. Voici un argument heuristique dans ce sens. Intuitivement, la proportion des nombres entiers divisibles par un entier n donné est égale à $1/n$. La proportion de ceux qui ne sont pas divisibles par n est par suite égale à $1 - 1/n$. Par exemple, le tiers des nombres sont divisibles par 3 et les deux tiers ne le sont pas:

		*			*			*			*			*			*			*			*	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Si m et n sont relativement premiers, le fait d'être divisible par m est une propriété indépendante du fait d'être divisible par n. En effet, un entier est divisible par m et n ssi il est divisible par mn puisque m et n sont relativement premiers. La proportion des entiers divisibles par m et n est donc $1/mn$. Cela implique que la proportion des entiers qui sont ni divisibles par m ni par n est donné par le produit

$$\Big(1 - \frac{1}{m}\Big)\Big(1 - \frac{1}{n}\Big).$$

En effet, cette quantité peut se calculer en retranchant de la proportion des nombres qui ne sont pas divisibles par n celle des nombres qui ne sont pas divisibles par n mais divisibles par m. La première vaut $1 - 1/n$, et la seconde vaut $1/m - 1/mn$. On trouve

$$(1 - 1/n) - (1/m - 1/mn) = \Big(1 - \frac{1}{m}\Big)\Big(1 - \frac{1}{n}\Big).$$

En particulier, si p et q sont des nombres premiers distincts, la proportion des nombres entiers relativement premiers au produit pq est $(1 - 1/p)(1 - 1/q)$. Par exemple, le tiers des nombres sont relativement premiers à $6 = 2 \cdot 3$:

*				*		*				*		*				*		*				*	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Plus généralement, si $p_1, \ldots, p_n$ sont de nombres premiers distincts, alors le proportion des nombres entiers relativement premiers au produit $p_1 \cdots p_n$ est donnée par le produit

$$\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_n}\Big).$$

Par exemple, la proportion des nombres entiers sans diviseurs premiers ≤ 100 est donnée par

$$\frac{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot 22 \cdot 28 \cdot 30 \cdot 36 \cdot 40 \cdot 42 \cdot 46 \cdot 52 \cdot 58 \cdot 60 \cdot 66 \cdot 70 \cdot 72 \cdot 78 \cdot 82 \cdot 88 \cdot 96}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97}$$
$$= \frac{3377854583194719250022400000}{280745566149397514974281352 7} = .1203172905...$$

Plus généralement, le produit

$$\prod_{p \text{ premier } \leq n} \Big(1 - \frac{1}{p}\Big)$$

représente la proportion des nombres entiers dont tous les diviseurs premiers sont $> n$. Comme ce produit est non nul, il faut bien qu'il y ait des nombres premiers $> n$. Il y a donc une infinité des nombres premiers!

Proposition 1.14. *(Euler) On a*

$$0 = \Big(1 - \frac{1}{2}\Big) \cdot \Big(1 - \frac{1}{3}\Big) \cdot \Big(1 - \frac{1}{5}\Big) \cdot \Big(1 - \frac{1}{7}\Big) \cdots.$$

Il existe donc une infinité de nombres premiers.

Preuve: Intutivement, ce produit représente la proportion des nombres entiers sans aucun diviseurs premiers! Cette proportion est nulle car tout nombre entier > 1 est divisible par un nombre premier au moins. Malheureusement, ce raisonnement souffre d'un manque de rigueur. À ce sujet, voir l'exercice ? Nous allons reproduire le raisonnement rigoureux d'Euler. Il repose sur le fait que la série harmonique

$$S = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \cdots$$

diverge Pour le voir on peut en regrouper les termes comme suit:

$$S = \frac{1}{1} + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \left(\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}\right) + \cdots$$

Si on remplace les termes de chaque groupe par le plus petit d'entre eux on obtient que

$$\begin{aligned} S \geq & \frac{1}{1} + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \left(\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16}\right) + \cdots \\ = & 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots = \infty. \end{aligned}$$

Remarquons maintenant que la série géométrique

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots$$

converge pour $\mid x \mid < 1$. Pour le voir il suffit d'utiliser l'identité

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

valable pour $x \neq 1$. La convergence provient du fait que $x^{n+1} \to 0$ lorsque $n \to \infty$ si $\mid x \mid < 1$. En particulier, la somme des inverses des puissances de 2 converge:

$$\frac{1}{1 - \frac{1}{2}} = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots$$

Plus généralement, la somme des inverses des puissances d'un nombre entier $n > 1$ converge:

$$\frac{1}{1 - \frac{1}{n}} = 1 + \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^3} + \cdots$$

Que peut-on dire de la somme des inverses des nombres entiers de la forme $2^a 3^b$ pour $a, b \geq 0$. Elle converge car on a

$$\begin{aligned} \frac{1}{1 - \frac{1}{2}} \cdot \frac{1}{1 - \frac{1}{3}} = & \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots\right) \\ = & 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{2 \cdot 3} + \frac{1}{2^3} + \frac{1}{3^2} + \frac{1}{2^2 \cdot 3} + \frac{1}{2^4} + \cdots \end{aligned}.$$

De même, la somme des inverses des nombres entiers de la forme $2^a 3^b 5^c$ converge car on a

$$\frac{1}{1 - \frac{1}{2}} \cdot \frac{1}{1 - \frac{1}{3}} \cdot \frac{1}{1 - \frac{1}{5}} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{2^3} + \frac{1}{3^2} + \frac{1}{2 \cdot 5} + \frac{1}{2^2 \cdot 3} + \frac{1}{2^4} + \cdots.$$

On peut continuer ainsi en ajoutant un facteur

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots$$

pour chaque nombre premier p. Comme tout entier se décompose uniquement en produit de facteurs premiers on obtient que

$$\frac{1}{1-\frac{1}{2}}\cdot\frac{1}{1-\frac{1}{3}}\cdot\frac{1}{1-\frac{1}{5}}\cdot\frac{1}{1-\frac{1}{7}}\cdots = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\cdots.$$

Le second membre de cette dernière égalité est la série harmonique qui diverge. Par suite,

$$\frac{1}{1-\frac{1}{2}}\cdot\frac{1}{1-\frac{1}{3}}\cdot\frac{1}{1-\frac{1}{5}}\cdot\frac{1}{1-\frac{1}{7}}\cdots = \infty.$$

En inversant on obtient que

$$\Big(1-\frac{1}{2}\Big)\cdot\Big(1-\frac{1}{3}\Big)\cdot\Big(1-\frac{1}{5}\Big)\cdot\Big(1-\frac{1}{7}\Big)\cdots = 0.$$

CQFD

Proposition 1.15. *(Euler)*

$$\infty = \frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\cdots.$$

Il existe donc une infinité de nombres premiers.

Preuve: En prenant le logarithme du produit

$$\infty = \frac{1}{1-\frac{1}{2}}\cdot\frac{1}{1-\frac{1}{3}}\cdot\frac{1}{1-\frac{1}{5}}\cdot\frac{1}{1-\frac{1}{7}}\cdots$$

on obtient que

$$\infty = \ln\frac{1}{1-\frac{1}{2}}+\ln\frac{1}{1-\frac{1}{3}}+\ln\frac{1}{1-\frac{1}{5}}+\ln\frac{1}{1-\frac{1}{7}}\cdots.$$

Pour continuer, on utilise ensuite le fait que l'on a

$$\ln\frac{1}{1-\frac{1}{n}} \leq \frac{\ln 4}{n}$$

pour tout $n \geq 2$ (voir le lemme 16 qui suit). Par suite

$$\infty \leq (\ln 4)\cdot\Big(\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\cdots\Big).$$

CQFD

La démonstration du lemme 1.16 utilise le concept de fonction convexe. On dit qu'une fonction continue $f(x)$ définie dans un intervalle (a,b) est *convexe* si son graphe est courbé vers le haut, comme un sourire. Il est facile de vérifier qu'une fonction différentiable f est convexe ssi sa dérivée $f'(x)$ est croissante. Lorsque f est convexe, on a l'inégalité

$$f((1-t)x+ty) \leq (1-t)f(x)+tf(y)$$

pour tout $x,y \in (a,b)$ et pour tout $t \in [0,1]$. Cette inégalité traduit le fait que le segment de droite joignant les points de coordonnées $(x,f(x))$ et $(y,f(y))$ est situé au dessus du graphe de f dans l'intervalle $[x,y]$ (si $x<y$).

Lemme 1.16. *Pour tout $n \geq 2$ on a*

$$\ln \frac{1}{1-\frac{1}{n}} \leq \frac{\ln 4}{n}$$

Preuve: la fonction

$$f(x) = \ln \frac{1}{1-x}$$

est différentiable pour $x < 1$. C'est une fonction convexe dans l'intervalle $(-\infty, 1)$ car sa dérivé $f'(x) = \frac{1}{1-x}$ est croissante pour $x < 1$. Comme $f(0) = 0$ on obtient en prenant $x = 0$ que $f(ty) \leq tf(y)$ pour tout $y < 1$ et $t \in [0, 1]$. En particulier, si $y = 1/2$ et $t = 2/n$ on obtient l'inégalité

$$f(\frac{1}{n}) \leq \frac{2}{n} \cdot f(\frac{1}{2})$$

pour $n \geq 2$. Cela montre que l'on a

$$\ln \frac{1}{1-\frac{1}{n}} \leq \frac{2\ln 2}{n}$$

pour $n \geq 2$. CQFD

On peut observer que les nombres premiers grands sont plus rares que les petits. Par exemple, on trouve 25 nombres premiers dans l'intervalle $[1, 100]$ et 21 dans l'intervalle $[200, 300]$. Dans le tableau suivant nous avons indiqué pour certaines valeurs de n, le nombre $\pi(n, 100)$ de nombres premiers compris dans l'intervalle $[n, n + 100]$.

n	0	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}	10^{50}
$\pi(n, 100)$	25	21	16	11	6	6	2	2	7	5	7	4	0.

Le tableau montre que la valeur de $\pi(n, 100)$ fluctue autour d'une moyenne qui va en décroissant lorsque n croit. Il montre aussi que l'intervalle $[10^{50}, 10^{50} + 100]$ ne contient aucun nombre premier. Dénotons par $\pi(n)$ le nombre de nombres premiers $p \leq n$. Le mathématicien Paul-Marie Legendre (1752-1833) a conjecturé que $\pi(n)$ est asymptotique à $\frac{n}{\log n}$:

$$\pi(n) \sim \frac{n}{\log n}.$$

Je rappelle que deux fonctions $f(n)$ et $g(n)$ sont *asymptotiques*, $f(n) \sim g(n)$, si le rapport $\frac{f(n)}{g(n)}$ tend vers 1 lorsque $n \to \infty$. Le mathématicien Carl Frederic Gauss (1777-1855) fit une conjecture plus précise en 1849:

$$\pi(n) = \int_2^n \frac{dx}{\ln(x)}.$$

On peut reformuler la conjecture de Gauss en disant que la fréquence des nombres premiers au voisinage d'un entier x grand est approximativement donnée par

$$f(x) = \frac{1}{\ln(x)}.$$

Si $x = 10^n$ on a

$$f(10^n) = \frac{1}{\ln(10^n)} = \frac{.43429448}{n}.$$

Cette formule prédit qu'environ un nombre sur 10 est premier dans le voisinage de 10^4, qu'environ un nombre sur 100 est premier dans le voisinage de 10^{43} et qu'environ un nombre sur 1000 est premier au voisinage de 10^{434}. Cela entraîne qu'il y au au moins 10^{431} nombres premiers $\leq 10^{434}$.

Bigre! Il y a énormément de nombres premiers!

La précision de la formule de Gauss est remarquable. Par exemple, on compte 44 nombres premiers dans l'intervalle $[10^{10}+1, 10^{10}+10^3]$ ce qui donne une fréquence empirique de 44/1000. Le fréquence théorique obtenue de la formule de Gauss est

$$f(10^{10}) = \frac{43.4}{1000}.$$

La conjecture de Gauss été démontrée par Jacques Hadamard et par Charles de La Vallée Poussin en 1896.

On ne connait pas de méthode simple pour engendrer une infinité des nombres premiers. On conjecture qu'il existe un infinité de nombres premiers de Mersenne. Tout polynôme $p(n)$ à coefficients entiers admet des valeurs composées pour une infinité d'entiers n. Toutefois, Euler a donné l'exemple remarquable du polynôme $p(n) = n^2 + n + 41$ qui prend des valeurs premières pour tous les entiers $n = 0, 1, \ldots, 39$:

41	43	47	53	61	71	83	97	113	131	151	173	197	223	251
281	313	347	383	421	461	503	547	593	641	691	743	797	853	911
971	1033	1097	1163	1231	1301	1373	1447	1523	1601					

On a conjecturé que le polynôme $n^2 + 1$ prend une infinité de valeurs premières mais on ne sait pas le démontrer.

Le mathématicien Fermat (1601-1665) a conjecturé que tous les nombres de Fermat

$$F_n = 2^{2^n} + 1$$

sont premiers. Les cinq premiers nombres de Fermat sont effectivement premiers:

$$\begin{aligned}
F_0 &= 2^1 + = 3 \\
F_1 &= 2^2 + 1 = 5 \\
F_2 &= 2^4 + 1 = 17 \\
F_3 &= 2^8 + 1 = 257 \\
F_4 &= 2^{16} + 1 = 65537.
\end{aligned}$$

Mais la conjecture de Fermat est fausse. Euler a trouvé que F_5 est composé:

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

En 1880 le mathématicien F. Landry a montré (à l'âge de 82 ans) que F_6 est composé:

$$F_6 = 2^{64} + 1 = 18446744073709551617 = 274177 \times 67280421310721.$$

En 1970 Morrison et Brillhart décomposent F_7 en facteurs premiers en utilisant un ordinateur:

$$F_7 = 2^{128} + 1 = 59649589127497217 \times 5704689200685129054721.$$

En 1980 Pollard et Brent décomposent F_8 en utilisant une variante de l'algorithme de factorisation de Pollard:

$$\begin{aligned}
F_8 = 2^{256} + 1 = {} & 1238926361552897 \\
& \times 93461639715357977769163558199606896584051237541638188580280321.
\end{aligned}$$

En 1990 Lenstra, Lenstra, Manasse et Pollard décomposent F_9:

$$\begin{aligned}
F_9 = 2^{512} + 1 = {} & 2424833 \times 7455602825647884208337395736200454918783366342657 \\
& \times 741640062627530801524787141901937474059940781097 51 \\
& 9023905821316144415759504705008092818711693940737.
\end{aligned}$$

Le plus grand facteur premier de F_9 est un nombre de 99 décimales. Les nombres F_{10} et F_{11} ont été décomposé en facteurs premiers par Brent (1995 et 1988). Le plus grand facteur premier de F_{11} est un nombre de 512 décimales. Aujourd'hui, on sait que tous les nombres de Fermat F_n sont composés pour $5 \leq n \leq 50$.

L'un des plus beaux résultats sur les nombres de Fermat est du à Christian Goldbach (1690-1764).

Théorème 1.17. *(Goldbach). Les nombres de Fermat sont relativement premiers deux à deux.*

Preuve: Partant de l'identité $x^2 - 1 = (x-1)(x+1)$ on montre que

$$x^{2^n} - 1 = (x-1)(x+1)(x^2+1)(x^4+1)\cdots(x^{2^{n-1}}+1).$$

Si on pose $x = 2$ on obtient que

$$F_n - 2 = F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_{n-1}.$$

Cette relation entraîne que tout diviseur commun à F_n et à F_k pour $k < n$ est un diviseur de 2. Comme les nombres de Fermat sont impairs il faut que ce diviseur soit égal à 1.

Le résultat de Goldbach entraîne l'existence d'une infinité de nombres premiers. En effet, soit p_n le plus petit diviseur premier de F_n. Si $m \neq n$ alors $p_m \neq p_n$ car aucun diviseur premier de F_m n'est un diviseur de F_n.

Les nombres premiers de Fermat interviennent dans l'un des plus beaux résultats de Gauss. Depuis Euclide, les géomètres ont voulu faire leurs constructions géométriques en utilisant uniquement la règle et le compas. Euclide avait donné une construction des polygones réguliers avec 3,4,5,6,8,10 et 12 côtés. En fait, il est facile de doubler le nombre de côtés d'un polygone déjà construit. Vers 150 après JC, Claude Ptolémée obtient la valeur de $\sin 3^o$ pour ses tables de trigonométrie en construisant le coté d'un polygone régulier de $120 = 8 \cdot 15$ côtés. Mais Ptolémée ne put trouver la construction du polygone régulier de $360 = 8 \cdot 3^2 \cdot 5$ côtés car il n'arrivait pas à construire le polygone de 9 côtés. Gauss montra qu'un polygone régulier de n côtés est constructible par règle et compas si et seulement la décomposition de n en facteurs premiers est de la forme

$$n = 2^a p_1 p_2 \cdots p_r$$

avec $p_1, \ldots, p_r$ des nombres premiers de Fermat distincts. Par exemple, le polygone de 17 côtés est constructible car $17 = F_2$. Ceux de 7 et de 9 côtés ne le sont pas. Remarquer que les seuls nombres premiers de Fermat connus sont les cinq premiers F_0, F_1, F_2, F_3, F_4.

Un grand nombres de questions sur les nombres premiers restent sans réponses. L'une concerne les nombres premiers jumeaux. On dit que deux nombres premiers p et q sont *jumeaux* si $q = p + 2$. Voici la liste des nombres premiers jumeaux ≤ 1000.

$(3,5)$	$(5,7)$	$(11,13)$	$(17,19)$	$(29,31)$	$(41,43)$	$(59,61)$	$(71,73)$
$(101,103)$	$(107,109)$	$(137,139)$	$(149,151)$	$(179,181)$	$(191,193)$	$(197,199)$	$(227,229)$
$(239,241)$	$(269,271)$	$(281,283)$	$(311,313)$	$(347,349)$	$(419,421)$	$(431,433)$	$(461,463)$
$(521,523)$	$(569,571)$	$(599,601)$	$(617,619)$	$(641,643)$	$(659,661)$	$(809,811)$	$(821,823)$
$(827,829)$	$(857,859)$	$(881,883)$					

On croit qu'il existe une infinité de nombres premiers jumeaux mais on ne sait pas le démontrer.

Pour les applications, il est important d'avoir un algorithme permettant de calculer efficacement les coefficients u et v de la relation de Bezout. D'après l'algorithme d'Euclide, le pgcd de deux entiers a et b

s'obtient comme le dernier reste non-nul r_n de la suite de divisions suivantes:

$$\begin{array}{rl} a = bq_1 + r_1 & \text{evec} \quad 0 < r_1 < b \\ b = r_1 q_2 + r_2 & \text{avec} \quad 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 & \text{avec} \quad 0 < r_3 < r_2 \\ \cdots & \cdots \\ r_{n-2} = r_{n-1} q_n + r_n & \text{avec} \quad 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} + 0 & \end{array} .$$

Posons $p_i = q_{n+1-i}$. La suite $p_1, \ldots, p_n$ est obtenue en renversant la suite des quotients $q_1, \ldots, q_n$. On définit une suite $(\beta_0, \ldots, \beta_n)$ en posant

$$\begin{array}{rl} & \beta_0 = 1; \\ & \beta_1 = p_1; \\ \text{et} \quad & \beta_k = p_k \cdot \beta_{k-1} + \beta_{k-2} \quad \text{pour} \quad 2 \leq k \leq n. \end{array}$$

Proposition 1.18. *On a*

$$\text{pgdc}(a, b) = (-1)^n (\beta_n b - \beta_{n-1} a)$$

Preuve: Nous utiliserons les matrices. Pour une autre démonstration, voir l'exercice ?. On a

$$\begin{array}{rl} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix} & \\ \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} & \cdots \\ \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} & \end{array}$$

Par suite,

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}.$$

Posons $J = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Remarquer que

$$J \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} = - \begin{pmatrix} -q & 1 \\ 1 & 0 \end{pmatrix} J = - \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}^{-1} J.$$

Par suite

$$\begin{pmatrix} -a \\ b \end{pmatrix} = (-1)^n \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}^{-1} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}^{-1} \begin{pmatrix} -r_{n-1} \\ r_n \end{pmatrix},$$

et on obtient en inversant que

$$\begin{aligned} (-1)^n \begin{pmatrix} -r_{n-1} \\ r_n \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} -a \\ b \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & p_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & p_n \end{pmatrix} \begin{pmatrix} -a \\ b \end{pmatrix}. \end{aligned}$$

Remarquer que $(1, p_1) = (\beta_0, \beta_1)$ et que

$$(\beta_{k-1},\, \beta_k) \begin{pmatrix} 0 & 1 \\ 1 & p_{k+1} \end{pmatrix} = (\beta_k,\, \beta_{k+1})$$

pour tout $1 \leq k < n$. Par suite,

$$(0,1)\begin{pmatrix} 0 & 1 \\ 1 & p_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & p_n \end{pmatrix} = (\beta_{n-1},\, \beta_n).$$

On obtient alors que

$$(-1)^n r_n = (-1)^n (0,1)\begin{pmatrix} -r_{n-1} \\ r_n \end{pmatrix} = (\beta_{n-1},\, \beta_n)\begin{pmatrix} -a \\ b \end{pmatrix}.$$

CQFD

Voici un exemple d'application de la proposition 18. Le plus grand diviseur commun de $a = 3456$ et $b = 465$ est 3. La suite des quotients dans le calcul de ce plus grand diviseur commun est $(7, 2, 3, 5)$. La suite renversée est $(5, 3, 2, 7)$. On obtient que

$$\begin{aligned} &\beta_0 = 1; \\ &\beta_1 = 5; \\ &\beta_2 = 3 \cdot 5 + 1 = 16; \\ &\beta_3 = 2 \cdot 16 + 5 = 37; \\ &\beta_4 = 7 \cdot 37 + 16 = 275. \end{aligned}$$

On a donc $3 = (-1)^4(275 \cdot b - 37 \cdot a) = -37 \cdot a + 275 \cdot b$.

Exercices pour la section 1

Exercice : Dans notre exemple du crible d'Ératosthène, le premier multiple de 3 à être éliminé est $9 = 3^2$, le premier multiple de 5 à être éliminé est $25 = 5^2$ et le premier multiple de 7 à à être éliminé est $49 = 7^2$. Pouvez-vous expliquer ces observations ?

Exercice : Montrer que pour tout entiers $m, n, d \geq 1$, on a

$$\begin{aligned} \text{pgcd}(dm, dn) &= d \cdot \text{pgcd}(dm, dn) \\ \text{ppmc}(dm, dn) &= d \cdot \text{ppmc}(m, n) \end{aligned}$$

Suggestion: Utiliser les identités $c + (a \wedge b) = (c + a) \wedge (c + b)$ et $c + (a \vee b) = (c + a) \vee (c + b)$.

Les exercices qui suivent portent sur les nombres de Mersenne généralisés $M_n(a) = 1 + a + a^2 + \cdots + a^{n-1}$.

Exercice : Si $d = \text{pgdc}(m, n)$ montrer que $\text{pgdc}(a^m - 1, a^n - 1) = a^d - 1$. En déduire que

$$\text{pgdc}(M_m(a), M_m(a)) = M_d(a).$$

Suggestion: Si $m < n$ utiliser l'identité $a^n - 1 = a^{n-m}(a^m - 1) + a^{n-m} - 1$ pour montrer que

$$\text{pgdc}(a^m - 1, a^n - 1) = \text{pgdc}(a^m - 1, a^{n-m} - 1).$$

En déduire que si $n = mq + r$ alors

$$\text{pgdc}(a^m - 1, a^n - 1) = \text{pgdc}(a^m - 1, a^r - 1).$$

Utiliser ensuite l'algorithme d'Euclide pour calculer le $\text{pgdc}(m, n)$ et obtenir le résultat cherché.

Les exercices qui suivent portent sur les nombres de Mersenne doublement généralisés:

$$M_n(a,b) = b^{n-1} + ab^{n-2} + a^2b^{n-3} + \cdots + a^{n-1}.$$

Par convention, $M_0(a,b) = 0$ et $M_1(a,b) = 1$. On a évidemment $M_n(a,b) = M_n(b,a)$.

Exercice : Démontrer les identités:

$$M_{mn}(a,b) = M_n(a,b)M_m(a^n,b^n) \quad \text{et} \quad M_{m+n}(a,b) = a^m M_n(a,b) + M_m(a,b)b^n.$$

Exercice : Si $m = nq + r$ montrer que

$$M_m(a,b) = M_n(a,b)M_q(a^n,b^n)a^r + b^{nq}M_r(a,b).$$

Exercice : Supposons a et b relativement premiers. Si $d = \text{pgdc}(m,n)$, montrer que $M_d(a,b)$ est le plus grand diviseur commun de $M_m(a,b)$ et de $M_n(a,b)$.

Exercice : Le but de cet exercice est de donner une autre démonstration de la proposition ?. Posons $\beta_{-1} = 0$ et $(s_{-1}, s_0, \ldots, s_n) = (r_n, \ldots, r_1, b, a)$. Remarquer que pour tout $0 < k \leq n$, on a

$$\beta_k = p_k\beta_{k-1} + \beta_{k-2} \quad \text{et} \quad s_k = p_k s_{k-1} + s_{k-2}.$$

Montrer par induction sur k que l'on a

$$\text{pgdc}(a,b) = (-1)^k \begin{vmatrix} \beta_k & s_k \\ \beta_{k-1} & s_{k-1} \end{vmatrix}.$$

pour tout $0 \leq k \leq n$.

Les exercices qui suivent ont pour but d'étudier la décomposition en facteurs premiers de $n!$. On a

$$\begin{aligned}
1! &= 1 \\
2! &= 2 \\
3! &= 2 \cdot 3 \\
4! &= 2^3 \cdot 3 \\
5! &= 2^3 \cdot 3 \cdot 5 \\
6! &= 2^4 \cdot 3^2 \cdot 5 \\
7! &= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \\
8! &= 2^7 \cdot 3^2 \cdot 5 \cdot 7 \\
9! &= 2^7 \cdot 3^4 \cdot 5 \cdot 7 \\
10! &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \\
11! &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \\
12! &= 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11
\end{aligned}$$

Pour tout nombre premier p, soit $e_p(n)$ l'exposant de la plus grande puissance de p qui divise n. On a $e_p(mn) = e_p(m) + e_p(n)$. Par suite,

$$e_p(n!) = \sum_{k=1}^{n} e_p(k).$$

Dans le tableau suivant nous avons indiqué les valeurs de $e_2(n)$ par une colonne d'étoiles:

															*									
							*								*								*	
			*				*				*				*				*				*	
	*		*		*		*		*		*		*		*		*		*		*		*	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On trouve que

$$e_2(25!) = 1 + 2 + 1 + 3 + 1 + 2 + 1 + 4 + 1 + 2 + 1 + 3 = 22.$$

C'est le nombre total d'étoiles du tableau. On peut compter les étoiles horizontalement plutôt que verticalwment. Il y a 12 étoiles de niveau 1, 6 de niveau 2, 3 de niveau 3 et 1 de niveau 4. On peut calculer le nombre détoile de niveau donné en utilisant $[x]$, la partie entière d'un nombre réel x. On a

$$\begin{aligned} e_2(25!) &= \left[\frac{25}{2}\right] + \left[\frac{25}{4}\right] + \left[\frac{25}{8}\right] + \left[\frac{25}{16}\right]. \\ &= 12 + 6 + 3 + 1 = 22 \end{aligned}$$

Exercice : Montrer que

$$e_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

Par exemple, on obtient que

$$e_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{100}{4}\right] + \left[\frac{100}{8}\right] + \left[\frac{100}{16}\right] + \left[\frac{100}{32}\right] + \left[\frac{100}{64}\right] = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

$$e_3(100!) = \left[\frac{100}{3}\right] + \left[\frac{100}{9}\right] + \left[\frac{100}{27}\right] + \left[\frac{100}{81}\right] = 33 + 11 + 3 + 1 = 48$$

$$e_5(100!) = \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 20 + 4 = 24$$

$$e_7(100!) = \left[\frac{100}{7}\right] + \left[\frac{100}{49}\right] = 14 + 2 = 16$$

$$e_{11}(100!) = \left[\frac{100}{11}\right] = 9, \quad e_{13}(100!) = \left[\frac{100}{13}\right] = 7, \quad e_{17}(100!) = \left[\frac{100}{17}\right] = 5, \quad e_{19}(100!) = \left[\frac{100}{19}\right] = 5,$$

$$e_{23}(100!) = \left[\frac{100}{23}\right] = 4, \quad e_{29}(100!) = \left[\frac{100}{29}\right] = 3, \quad e_{31}(100!) = \left[\frac{100}{31}\right] = 3, \quad e_{37}(100!) = \left[\frac{100}{37}\right] = 2,$$

$$e_{41}(100!) = \left[\frac{100}{41}\right] = 2, \quad e_{43}(100!) = \left[\frac{100}{43}\right] = 2 \quad , e_{47}(100!) = \left[\frac{100}{47}\right] = 2$$

$$e_{51}(100!) = \left[\frac{100}{51}\right] = 1 \quad \text{etc.}$$

Cela donne

$$\begin{aligned} 100! = 2^{97} \cdot 3^{48} \cdot 5^{24} \cdot 7^{16} \cdot 11^9 \cdot 13^7 \cdot 17^5 \cdot 19^5 \cdot 23^4 \cdot 29^3 \cdot 31^3 \cdot 37^2 \cdot 41^2 \cdot 43^2 \cdot 47^2 \cdot \\ \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \end{aligned}$$

Cet exemple suggère que l'exposant de 2 dans la décomposition de $n!$ est légèrement inférieur à n, et que l'exposant de 3 est légèrement inférieur à $n/2$. Remarquer que

$$e_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p}\frac{1}{\left(1-\frac{1}{p}\right)} = \frac{n}{p-1}.$$

En particulier, on a $e_2(n!) < n$. Pour calculer la différence $n - e_2(n!)$ il est bon d'exprimer n à la base 2. Par exemple, $100 = (1100100)_2 = 2^6 + 2^5 + 2^2$ et

$$\begin{aligned}
\left[\frac{100}{2}\right] &= 2^5 + 2^4 + 2 \\
\left[\frac{100}{4}\right] &= 2^4 + 2^3 + 1 \\
\left[\frac{100}{8}\right] &= 2^3 + 2^2 \\
\left[\frac{100}{16}\right] &= 2^2 + 2 \\
\left[\frac{100}{32}\right] &= 2 + 1 \\
\left[\frac{100}{64}\right] &= 1.
\end{aligned}$$

Si on additionne les membres de droite par colonne verticale, on obtient

$$\begin{aligned}
e_2(100!) &= (2^5 + 2^4 + 2^3 + 2^2 + 2 + 1) + (2^4 + 2^3 + 2^2 + 2 + 1) + (2 + 1) \\
&= (2^6 - 1) + (2^5 - 1) + (2^2 - 1) \\
&= (2^6 + 2^5 + 2^2) - 3 \\
&= 100 - 3
\end{aligned}$$

La différence $100 - e_2(100!) = 3$ est la somme $s_2(n)$ des bits du développement binaire $(1100100)_2$.

Exercice: Montrer que $e_2(n!) = n - s_2(n)$.

Par exemple, comme $1000 = (1111101000)_2$ on obtient que $e_2(1000!) = 10000 - 6 = 984$.

Plus généralement, dénotons par $(a)_p = a_0 + a_1 p + a_2 p^2 + \cdots$ le développement d'un entier a à la base p. Par définition, on a $0 \leq a_i < p$. Posons $s_p(n) = a_0 + a_1 + a_2 + \cdots$.

Exercice: Montrer que

$$e_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Par exemple, comme $10^6 = (1212210202001)_3$ on obtient que $e_3(10^6!) = (10^6 - 14)/2 = 499993$.

2. Fractions décimales et congruences

La théorie des résidus est l'un des principaux outils de la théorie des nombres. C'est l'oeuvre de plusieurs générations de mathématiciens, Fermat, Euler, Lagrange, Legendre et Gauss y ont contribués. Elle permet d'expliquer un grand nombre de phénomênes mathématiques. C'est le cadre naturel pour répondre à plusieurs questions sur la périodicité du développement décimal des nombres rationnels. Nous commencerons notre

excursion par étudier cette périodicité. Elle conduit directement à des résultats fondamentaux de Fermat, d'Euler et de Lagrange, et elle conduit à des questions non encore résolues.

On raconte que durant sa jeunesse, Gauss calcula le développement décimal de toutes les fractions $1/n$ pour $n \leq 1000$. C'est un travail considérable. Certaines fractions ont une période comportant des centaines de chiffres. Ce faisant, Gauss accumulait un savoir empirique qui devait lui servir toute sa vie. Suivant son exemple, commencons par examiner le développement décimal de quelques fractions.

La développement décimal d'une fraction comme $9/56$ s'obtient par division successive. Comme $9 < 56$ on multiplie 9 par 10 et on divise le résultat par 56. Le reste de cette division est 34. On multiplie ensuite 34 par 10 et on divise le résultat par 56. Le reste de cette division est 4. On multiplie 4 par 10 et on divise le résultat par 56. Le reste de cette division est 40, etc

$$\begin{aligned}
90 &= 56 \times 1 + 34 \\
340 &= 56 \times 6 + 4 \\
40 &= 56 \times 0 + 40 \\
400 &= 56 \times 7 + 8 \\
80 &= 56 \times 1 + 24 \\
240 &= 56 \times 4 + 16 \\
160 &= 56 \times 2 + 48 \\
480 &= 56 \times 8 + 32 \\
320 &= 56 \times 5 + 40
\end{aligned}$$

Il n'est pas nécessaire de poursuivre les divisions car la périodicité est manifeste. Cela donne que

$$9/56 = 0,16071428571428571428571428571428571429...$$

Le trois chiffre du début forment une partie transitoire suivie d'une partie récurrente 714285 de longueur 6. Remarquer que la suite 714285714285 de longueur 12 est aussi récurrente. On dit que la partie récurrente de longueur minimale est la *période* du développement. Dans notre exemple, cette période débute à la 4^e décimale. Nous écrirons

$$9/56 = 0,160\dot{7}1428\dot{5}.$$

Remarquons à ce stade que les restes que l'on obtient en calculant le développement décimal de $9/56$ sont identiques à ceux que l'on obtiendrait en divisant succesivement les nombres $90, 900, 9000$, etc. En effet,

$$\begin{aligned}
90 &= 56 \times 1 + 34 \\
900 &= 56 \times 16 + 4 \\
9\ 000 &= 56 \times 160 + 40 \\
90\ 000 &= 56 \times 1607 + 8 \\
900\ 000 &= 56 \times 16071 + 24 \\
9\ 000\ 000 &= 56 \times 160714 + 16 \\
90\ 000\ 000 &= 56 \times 1607142 + 48 \\
900\ 000\ 000 &= 56 \times 16071428 + 32 \\
9\ 000\ 000\ 000 &= 56 \times 160714285 + 40
\end{aligned}$$

Certaines fractions ont un développement avec une période réduite à 0 : [1]

$$\begin{aligned}
1/2 &= 0,500000000000000000... \\
1/4 &= 0,250000000000000000... \\
1/8 &= 0,125000000000000000... \\
1/5 &= 0,200000000000000000... \\
1/25 &= 0,040000000000000000...
\end{aligned}$$

Il est facile de voir que c'est le cas des fractions avec un dénominateur de la forme $2^k 5^r$. En effet, on peut toujours les mettre sous la forme $a/10^n$ pour un entier a.

Certaines fractions ont un développement sans partie transitoire. Par exemple,

$$
\begin{aligned}
1/3 &= 0,33333333333333333... \\
2/3 &= 0,66666666666666666... \\
1/7 &= 0,142857142857142857... \\
2/7 &= 0,285714285714285714... \\
3/7 &= 0,428571428571428571... \\
4/7 &= 0,571428571428571428... \\
5/7 &= 0,714285714285714285... \\
6/7 &= 0,857142857142857142... \\
1/9 &= 0,111111111111111111... \\
2/9 &= 0,222222222222222222... \\
4/9 &= 0,444444444444444444... \\
5/9 &= 0,555555555555555555... \\
7/9 &= 0,777777777777777777... \\
8/9 &= 0,888888888888888888...
\end{aligned}
$$

Nous dirons que ces développements sont *strictement périodiques*. Pour y voir plus clair, calculons le développement décimal de $1/7$.

$$
\begin{aligned}
10 &= 7 \times 1 + 3 & 10 &= 7 \times 1 + 3 \\
30 &= 7 \times 4 + 2 & 10^2 &= 7 \times 14 + 2 \\
20 &= 7 \times 2 + 6 & 10^3 &= 7 \times 142 + 6 \\
60 &= 7 \times 8 + 4 & 10^4 &= 7 \times 1428 + 4 \\
40 &= 7 \times 5 + 5 & 10^5 &= 7 \times 14285 + 5 \\
50 &= 7 \times 7 + 1 & 10^6 &= 7 \times 14285 + 1 \\
10 &= 7 \times 1 + 3 & 10^7 &= 7 \times 142851 + 3
\end{aligned}
$$

Le premier reste à revenir est 3. Le reste qui précède est 1; il marque la fin de la première période et annonce la suivante. On voit sur cet exemple que la fin de première période du développement de $1/n$ est marqué par un reste qui vaut 1.

Pour tout entier $n \in \mathbf{Z}$ posons $n\mathbf{Z} = \{na \mid a \in \mathbf{Z}\}$.

Definition 2.1 : Soit n un entier ≥ 0. Nous dirons que deux entiers $a, b \in \mathbf{Z}$ sont *congrus modulo* n si leur différence $a - b$ est divisible par n, autrement dit, si $a - b \in n\mathbf{Z}$. Nous écrirons

$$a \equiv b \mod n$$

pour indiquer que a est congru à b modulo n.

Proposition 2.2. *Soit n un entier > 0. Si $x \equiv y$ dénote la relation de congruence modulo n alors on a:*
(i) $x \equiv x$ (réflexivité)
(ii) Si $x \equiv y$ et $y \equiv z$ alors $x \equiv z$ (transitivité)
(iii) Si $x \equiv y$ alors $y \equiv x$ (symétrie)

(iv) Si $x \equiv y$ et $u \equiv v$ alors $x+u \equiv y+v$ et $xu \equiv yv$.

Preuve: (i) On a $n \mid (x-x)$ car $n \mid 0$. (ii) Si $n \mid (x-y)$ et $n \mid (y-z)$ alors $n \mid (x-y)+(y-z) = (x-z)$. (iii) Si $n \mid (x-y)$ alors $n \mid -(x-y) = (y-x)$. (iv) Si $n \mid (x-y)$ et $n \mid (u-v)$ alors $n \mid (x-y)+(u-v) = (x+u)-(y+v)$. De plus, $n \mid x(u-v)+v(x-y) = xu-yv$. CQFD

La proposition suivante généralise la division euclidienne à tous les entiers de $\mathbf{Z}$

Proposition 2.3. *(Division euclidienne des entiers dans $\mathbf{Z}$) Soit n un entier > 0. Alors pour tout entier $a \in \mathbf{Z}$ il existe des entiers $q \in \mathbf{Z}$ et $0 \leq r < n$ tels que*

$$a = nq + r.$$

Les entiers q et r sont déterminés uniquement par a et n.

Preuve: Soit $q \in \mathbf{Z}$ le plus grand des entiers $\leq a/n$. Par definition, on a $q \leq a/n$ et $a/n < q+1$. Par suite, $qn \leq a$ et $a < (q+1)n$. Posons $r = a - nq$. Alors on a $r \geq 0$ et $r < n$. Cela montre l'existence du couple (q, r). L'unicité est évidente. CQFD

Proposition 2.4. *Soit n un entier > 0. Tout entier $a \in \mathbf{Z}$ est congru modulo n à un et un seul entier $r \in \{0, 1, \cdots, n-1\}$. L'entier r est le reste de la division de a par n.*

Preuve: On a $a = nq + r$ avec $0 \leq r < n$ par division euclidienne. Donc $a \equiv r \bmod n$ et $r \in \{0, 1, \cdots, n-1\}$. L'unicité de r provient de l'unicité du reste d'une division euclidienne. CQFD

Deux entiers a et b sont congrus modulo n ssi le reste de la division euclidienne de a par n est égal au reste de la division euclidienne de b par n.

Proposition 2.5. *Si $b \perp n$ alors il existe un entier $k > 0$ pour lequel $b^k \equiv 1$ modulo n.*

Preuve: Soit r_k le reste de la division de b^k par n. Les restes $r_0, r_1, r_2, \ldots, r_n$ ne peuvent être tous différents car $0 \leq r_i < n$. On a donc $r_i = r_{i+k}$ pour des exposants $0 \leq i < i+k \leq n$. Dans ce cas,

$$b^i \equiv r_i = r_{i+k} \equiv b^{i+k} \mod n.$$

Ce qui montre que n divise la différence $b^i - b^{i+k} = b^i(b^k - 1)$. Cela implique que n divise $b^k - 1$ puisque $n \perp b$. CQFD

Definition 2.6: Soit $a \in \mathbf{Z}$ un entier relativement premier à $n > 0$. Nous dirons que le plus petit entier $e > 0$ tel que

$$a^e \equiv 1 \mod n$$

est l'*ordre* de a modulo n; nous le dénoterons par $\mathrm{ord}(a; n)$.

Proposition 2.7. *Soit $a \in \mathbf{Z}$ un entier relativement premier à un entier $n > 0$. Si $e = \mathrm{ord}(a; n)$ alors pour tout entier $k > 0$ on a*

$$a^k \equiv 1 \mod n \quad \Leftrightarrow \quad e \mid k.$$

Preuve: Posons $e = \text{ord}(a; n)$. Si $e \mid k$ alors $k = qe$ pour un entier q. Par suite, $a^k \equiv a^{qe} \equiv (a^e)^q \equiv (1)^q \equiv 1$ modulo n. Inversement, supposons que l'on ait $a^k \equiv 1$ modulo n. Par division euclidienne on a $k = eq + r$ avec $0 \leq r < e$. Par suite,

$$1 \equiv a^k \equiv a^{qe+r} \equiv a^{qe}a^r \equiv a^r \mod n$$

On ne peut avoir $r > 0$ car cela contredirait la minimalité de e. Donc $r = 0$ et $e \mid k$. CQFD

Proposition 2.8. *Soit $n > 0$ un entier relativement premier à 10. Alors l'ordre de 10 modulo n est égal à la longueur de la période du développement décimal de $1/n$. Le développement décimal de $1/n$ est strictement périodique.*

Par exemple, l'ordre de 10 modulo 11 est 2 car $10^2 \equiv 1$ modulo 11 mais $10 \not\equiv 1$ modulo 11. La longueur de la période du développement décimal de $1/11$ est donc 2. En effet,

$$1/11 = 0,090909090909090909...$$

Considérons maintenant les développements décimaux des fractions (réduites) a/n.

$$\begin{aligned}
1/11 &= 0,090909090909090909...\\
2/11 &= 0,181818181818181818...\\
3/11 &= 0,272727272727272727...\\
4/11 &= 0,363636363636363636...\\
5/11 &= 0,454545454545454545...\\
6/11 &= 0,545454545454545454...\\
7/11 &= 0,636363636363636363...\\
8/11 &= 0,727272727272727272...\\
9/11 &= 0,818181818181818181...\\
10/11 &= 0,909090909090909090...
\end{aligned}$$

Cet exemple et les autres suggèrent le résultat suivant:

Proposition 2.9. *Si n est relativement premier à 10, le développement décimal des fractions réduites $0 < a/n \leq 1$ est strictement périodique. La longueur de la période ne dépend pas de a, seulement de n.*

Preuve: Soit r_i le reste de la division de $10^i a$ par n. Considérons la suite des restes $r_0, r_1, r_2, \ldots, r_n$. On a $r_0 = a$. Soit $e > 0$ l'ordre de 10 modulo n. Montrons que $r_e = a$. En effet, comme on a $10^e \equiv 1$ modulo n, on a $10^e a \equiv a$ modulo n. D'autre part, montrons que $r_i \neq a$ pour tout $0 < i < k$. Raisonnons par l'absurde. Si on avait $r_i = a$, on aurait $10^i \equiv a$ modulo n. L'entier $10^i a - a = a(10^i - 1)$ serait alors divisible par n. Et aussi l'entier $10^i - 1$ puisque $n \perp a$. Mais cela contredirait la minimalité de e. CQFD

Les fractions de dénominateurs 11 se regroupent naturellement en 5 classes de 2 éléments chacun:

$$\begin{aligned}
1/11 &= 0,090909090909090909...\\
10/11 &= 0,909090909090909090...
\end{aligned}$$

$$\begin{aligned}
2/11 &= 0,181818181818181818...\\
9/11 &= 0,818181818181818181...
\end{aligned}$$

$$\begin{aligned}
3/11 &= 0,272727272727272727...\\
7/11 &= 0,636363636363636363...
\end{aligned}$$

$$4/11 = 0,363636363636363636...$$
$$7/11 = 0,636363636363636363...$$

$$5/11 = 0,454545454545454545...$$
$$6/11 = 0,545454545454545454...$$

Deux fractions sont dans la même classe si le développement de l'une est obtenue en décalant celui de l'autre. Pour plus de clarté, considérons un autre exemple:

$$1/21 = 0,047619047619047619...$$
$$10/21 = 0,476190476190476190...$$
$$16/21 = 0,761904761904761904...$$
$$13/21 = 0,619047619047619047...$$
$$4/21 = 0,190476190476190476...$$
$$19/21 = 0,904761904761904761...$$

$$2/21 = 0,095238095238095238...$$
$$20/21 = 0,952380952380952380...$$
$$11/21 = 0,523809523809523809...$$
$$5/21 = 0,238095238095238095...$$
$$8/21 = 0,380952380952380952...$$
$$17/21 = 0,809523809523809523...$$

Dans ce cas, les fractions se regroupent en 2 classes de 6 éléments chaque. Les fractions d'une classe s'obtiennent en multipliant l'une d'entre elle par les puissances de 10 et en conservant la partie fractionnaire. En effet,

$$1/21 = 0,047619047619047619...$$
$$10/21 = 0,476190476190476190...$$
$$100/21 = 4,761904761904761904...$$
$$1000/21 = 47,619047619047619047...$$
$$10000/21 = 476,190476190476190476...$$
$$100000/21 = 4761,904761904761904761...$$

Chaque classe contient un nombre déléments égal à la longueur de la période. Cette longueur est l'ordre de 10 modulo 21 d'après ?.

Considérons le cas général des fractions de dénominateur $n > 0$. Avec Euler, désignons par $\phi(n)$ le nombre de fractions réduites $0 < a/n \leq 1$. C'est aussi le nombre d'entiers $0 < a \leq n$ relativement premier à n.

$\phi(1) = 1 : 1/1$.
$\phi(2) = 1 : 1/2$.
$\phi(3) = 2 : 1/3, 2/3$.
$\phi(4) = 2 : 1/4,3/4$.
$\phi(5) = 4 : 1/5, 2/5, 3/5,4/5$.
$\phi(6) = 2 : 1/6, 5/6$.
$\phi(7) = 6 : 1/7, 2/7, 3/7, 4/7, 5/7, 6/7$.
$\phi(8) = 4 : 1/8, 3/8, 5/8, 7/8$.
$\phi(9) = 6 : 1/9, 2/9, 4/9, 5/9, 7/9, 8/9$.
$\phi(10) = 4 : 1/10, 3/10, 7/10, 9/10$.
$\phi(12) = 4 : 1/12, 5/12, 7/12, 11/12$.

Si n est relativement premier à 10, les fractions réduites $0 < a/n \leq 1$ se regroupent en classes de décalage, chacune ayant un nombre d'éléments égal à la longeur de la période du développement décimal de $1/n$. Nous avons montré que la longueur de la période du développement décimal de $1/n$ divise $\phi(n)$. Autrement dit, l'ordre de 10 modulo n est un diviseur de $\phi(n)$. Plus généralement:

Proposition 2.10. *Si b est relativement premier à n, l'ordre de b modulo n est un diviseur de $\phi(n)$.*

Preuve: Soit e l'ordre de b modulo n. Nous allons diviser les fractions réduites $0 < a/n \leq 1$ en classes, chacune de cardinalité e. Pour cela, nous dirons que deux fractions réduites a_1/n et a_2/n ont le *même type*, $a_1/n \sim a_2/n$, s'il existe des entier $i, j \geq 0$ tel que $b^i a_1 \equiv b^j a_2$ modulo n. On voit facilement que la relation $\sim$ est reflexive, symétrique et transitive. On définit la classe $C(a)$ d'une fraction réduite a/n comme l'ensemble des fractions réduites ayant le même type que a/n. Il reste à vérifier que $C(a)$ contient exactement e éléments. Soit r_i le reste de la division de $b^i a$ par n. Remarquer que $r_e = a = r_0$ puisque $b^e a \equiv a$ modulo n. Montrons que $C(a) = \{r_1/n, r_2/n, \ldots, r_e/n\}$. On a évidemment $\{r_1/n, r_2/n, \ldots, r_e/n\} \subseteq C(a)$. Inversement, si $a'/n \in C(a)$, montrons que $a' = r_k$ pour un entier $1 \leq k \leq n$. On sait qu'il existe des entier $i, j \geq 0$ tel que $b^i a \equiv b^j a'$ modulo n. On peut supposer $i \geq j$, quitte à remplacer i par $i + ue$ avec u assez grand. Dans ce cas, n divise l'entier $b^{i-j}a - a'$ puisqu'il divise l'entier $b^i a - b^j a' = b^j(b^{i-j}a - a')$ et que $n \perp b$. On peut donc supposer que $j = 0$, quitte à remplacer i par $i - j$. Pour le reste nous allons supposer que $b^i a \equiv a'$ modulo n. Soit k le reste de la division de i par e. On a $i = eq + k$ et par suite, $b^i \equiv b^k$ modulo n. Donc $a' \equiv b^i a \equiv b^k a \equiv r_k$. Par suite, $a' = r_k$ puisque $0 \leq r_k < n$ et $0 \leq a' < n$. Montrons que $C(a)$ contient exactement e éléments. Pour cela il suffit de montrer que les fractions $r_1/n, r_2/n, \ldots, r_e/n$ sont distinctes. Sinon on aurait $r_j = r_{j+k}$ pour entiers $1 \leq j < j + k \leq e$. Dans ce cas, n diviserait la différence $b^j a - b^{j+k} a = b^j a(b^k - 1)$, et il diviserait par suite l'entier $b^k - 1$ puisque $n \perp b$ et $n \perp a$. Cela contredirait la minimalité de e car $0 < k < e$. CQFD

Si p est premier, alors $\phi(p) = p - 1$ puisque tout entier $0 < a < p$ est relativement premier à p. En particulier, si p est un nombre premier ne divisant pas 10, alors la longueur de la période du développement décimal de $1/p$ est un diviseur de $p - 1$. Vérifions ce résultat pour $p \leq 100$.

$$
\begin{aligned}
1/3 &= .\dot{3} \\
1/7 &= .\dot{1}42857\dot{} \\
1/11 &= .\dot{0}9\dot{} \\
1/13 &= .\dot{0}7692\dot{3} \\
1/17 &= .\dot{0}588235294117647\dot{} \\
1/19 &= .\dot{0}52631578947368421\dot{} \\
1/23 &= .\dot{0}4347826086956521739\dot{1} \\
1/29 &= .\dot{0}3448275862068965517241379\dot{3} \\
1/31 &= .\dot{0}32258064516129\dot{} \\
1/37 &= .\dot{0}27\dot{} \\
1/41 &= .\dot{0}243\dot{9} \\
1/43 &= .\dot{0}23255813953488372093\dot{} \\
1/47 &= .\dot{0}212765957446808510638297872340425531914893617\dot{} \\
1/53 &= .\dot{0}1886792452\dot{83} \\
1/59 &= .\dot{0}16949152542372881355932203389830508474576271186440677966\dot{1}
\end{aligned}
$$

$$1/61 = .\dot{0}1639344262295081967213114754098360655737704918032786885245\dot{9}$$
$$1/67 = .\dot{0}1492537313432835820895522388059\dot{7}$$
$$1/71 = .\dot{0}1408450704225352112676056338028169\dot{0}$$
$$1/73 = .\dot{0}136986\dot{3}$$
$$1/79 = .\dot{0}126582278481\dot{0}$$
$$1/83 = .\dot{0}120481927710843373493975903614457831325\dot{3}$$
$$1/89 = .\dot{0}112359550561797752808988764044943820224719\dot{0}$$
$$1/97 = .\dot{0}1030927835051546391752577319587628865979381443298969072164948453608247422680412371134020618556\dot{7}$$

Dans tous les cas, la longueur de la période du développement décimal de $1/p$ divise $p-1$. Cette longueur est exactement $p-1$ pour $p = 7, 17, 19, 23, 29, 47, 59, 61$ et 97. On dit que ces nombres premiers sont *longs*.

Conjecture 2.11. *(Gauss) Il existe une infinité de nombres premiers longs.*

Empiriquement, il semble qu'un peu plus du tiers des nombres premiers sont longs. Emil Artin a conjecturé que cette proportion est donnée par le produit

$$\prod_{p \text{ premier}} \Big(1 - \frac{1}{p(p-1)}\Big) = \Big(1-\frac{1}{2}\Big)\Big(1-\frac{1}{3\cdot 2}\Big)\Big(1-\frac{1}{5\cdot 4}\Big)\Big(1-\frac{1}{7\cdot 6}\Big)\Big(1-\frac{1}{11\cdot 10}\Big)\cdots$$
$$= .37395\ldots$$

On ne sait pas démontrer la conjecture de Gauss, et encore moins celle d'Artin.

Proposition 2.12. *(Euler) Si n est relativement premier à 10, alors n divise $10^{\phi(n)} - 1$.*

Preuve: Soit k la longueur de la période du développement décimal de $1/n$. Alors n divise $10^k - 1$. De plus, k divise $\phi(n)$ d'après la proposition C. Posons $\phi(n) = kr$. Remarquer que $a-1$ divise toujours $a^r - 1$:

$$a^r - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1}).$$

En particulier, $10^k - 1$ divise $10^{kr} - 1 = 10^{\phi(n)} - 1$. Cela prouve que n divise $10^{\phi(n)} - 1$. QED

Proposition 2.13. *(Fermat) Si un nombre premier p ne divise pas 10, alors il divise $10^{p-1} - 1$.*

Preuve: En effet, $\phi(p) = p - 1$. CQFD

Les propositions 2.11, 2.12 et 2.13 se généralisent facilement au cas d'une base quelconque. Nous ferons cette généralisation dans le cadre de la théorie des congruences.

Exercices

Exercice : Calculer le développement décimal de 1/81.

Exercice : Calculer les développements décimaux de 1/9, 1/99, 1/999, etc. Ceux de 1/11, 1/111, 1/1111, etc.

Exercice : Calculer la longueur de la période du développement décimal de 1/983 (Gauss a fait ce calcul à 17 ans)., aurait choisi de faire ce calcul avec un ordinateur).

On définit *classe de congruence* d'un entier a modulo un entier $n > 0$ comme l'ensemble des entiers congrus à a modulo n. Nous dénoterons cette classe par $\underline{a}$. On a

$$\underline{a} = \{x \in \mathbf{Z} \mid x \equiv a \mod n\} = \{a + nk \mid k \in \mathbf{Z}\} = a + n\mathbf{Z}$$

Par exemples, si $n = 2$ on a

$$\underline{0} = 2\mathbf{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$
$$\underline{1} = 1 + 2\mathbf{Z} = \{\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots\}.$$

Si $n = 3$ on a

$$\underline{0} = 3\mathbf{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$
$$\underline{1} = 1 + 3\mathbf{Z} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$$
$$\underline{2} = 2 + 3\mathbf{Z} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}.$$

Il y a exactement n classes de congruences modulo n. Deux entiers sont congrus modulo n ssi leur classe sont égales:

$$a \equiv b \mod n \iff \underline{a} = \underline{b}.$$

Nous dénoterons par $\mathbf{Z}_n$ l'ensemble des classes de congruence modulo n. On peut additionner et multiplier les éléments $\mathbf{Z}_n$. Voici les tables d'addition et de multiplication pour $2 \leq n \leq 9$.

$\mathbf{Z}_2 = \{\underline{0}, \underline{1}\} = \{0, 1\}$,

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

$\mathbf{Z}_3 = \{\underline{0}, \underline{1}, \underline{2}\} = \{0, 1, 2\}$,

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbf{Z}_4 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}\} = \{0, 1, 2, 3\}$,

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbf{Z}_5 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}\} = \{0, 1, 2, 3, 4\}$,

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbf{Z}_6 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}\} = \{0, 1, 2, 3, 4, 5\}$,

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbf{Z}_7 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}\} = \{0, 1, 2, 3, 4, 5, 6\}$,

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$\mathbf{Z}_8 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$,

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$\mathbf{Z}_9 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$,

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

×	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

La classe de congruence modulo 9 d'un entier n est particulièrement facile à calculer à partir du développement décimal de n. En effet, comme on a $10 \equiv 1 \bmod 9$ on a $10^k \equiv 1 \bmod 9$ pour tout $k \geq 0$. Par suite

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 \cdots + a_r \mod 9$$

Par example, $257593 \equiv 2 + 5 + 7 + 5 + 9 + 3 \equiv 2 + 5 + 7 + 5 + 3 \equiv 22 \equiv 2 + 2 = 4$ modulo 9.

Comme application des congruences, vérifions que le nombre de Fermat $F_5 = 2^{2^5} + 1$ est divisible par 641. Pour cela, il suffit d'élever 2 au carré modulo 641 cinq fois:

$$2^2 \equiv 4 \mod 641$$
$$2^4 \equiv 16 \mod 641$$
$$2^8 \equiv 256 \mod 641$$
$$2^{16} \equiv 154 \mod 641$$
$$2^{32} \equiv -1 \mod 641$$

Définition 2.14: Nous dirons qu'un entier a est *inversible* modulo un entier $n > 0$ s'il existe un entier b tel que $ab \equiv 1$ modulo n.

Par exemple, 4 est inversible modulo 9 car $4 \cdot 7 \equiv 1$ modulo 9.

Si a est inversible modulo n, alors la congruence $ax \equiv c \bmod n$ possède une solution $x = a^{-1}c$ où a^{-1} est l'inverse de a modulo n. Cette solution est unique modulo n. Par exemple, la congruence $7x \equiv 8 \bmod 9$ a pour solution $x \equiv 4 \times 8 \equiv 5 \bmod 9$ (car 4 est l'inverse de 7 modulo 9). Si a est inversible modulo n alors l'implication

$$ax \equiv ay \mod n \quad \Rightarrow \quad x \equiv y \mod n$$

est vrai. Autrement dit, a est concellable modulo n. En effet, si b est l'inverse de a modulo n alors on a $bax \equiv bay \bmod n$, et par suite, $x \equiv y \bmod n$ car $ba \equiv 1 \bmod n$.

Proposition 2.15. *Un entier a est inversible modulo un entier $n > 0$ si et seulement si a est relativement premier à n.*

Preuve: Si a est inversible modulo n il existe un entier $b \in \mathbf{Z}$ tel que $ab \equiv 1 \bmod n$. On a alors $ab - 1 = nk$ pour un entier $k \in \mathbf{Z}$. La relation $1 = ab - nk$ implique que a est relativement premier à n d'après la

proposition 9. Inversement, si a est relativement premier à n alors il existe des entiers $u, v \in \mathbf{Z}$ tels que $1 = ua + vn$ d'après la proposition 9. On a alors $1 \equiv ua$ modulo n. CQFD

Corollaire 2.16. *Soit p un nombre premier. Un entier a est inversible modulo p ssi $a \not\equiv 0$ modulo p*

Preuve: Si $a \not\equiv 0$ alors p ne divise pas a. Donc p et a sont relativement premiers puisque p est premier. CQFD

Proposition 2.17. *Si a est relativement premier à $n > 0$ alors il existe un entier $e > 0$ tel que*

$$a^e \equiv 1 \mod n.$$

Preuve: Les classes de congruences modulo n des entiers $1, a, a^2, a^3, \ldots, a^n$ ne peuvent être toutes distinctes car il n'y a n classes de congruence modulo n. On a donc $a^k \equiv a^r$ modulo n pour des entiers $0 \leq k < r \leq n$ Mais on peut canceller le facteur a^k dans la congruence $a^k \equiv a^k a^{r-k}$ puisque a est concellable modulo n. On obtient que $1 \equiv a^{r-k}$ modulo n.

Definition 2.18: Soit a un entier relativement premier à n. Nous dirons que le plus petit entier $e > 0$ tel que $a^e \equiv 1$ modulo n est l'*ordre* de a modulo n; nous le dénoterons par $\mathrm{ord}(a; n)$.

Soit n un nombre entier relativement premier à 10. L'ordre de 10 modulo n est égal à longueur de la période du développement décimal de $1/n$ d'après la première partie. Par exemple, l'ordre de 10 modulo 7 est 6 car

$$1/7 = 0, \dot{1}42857\dot{}.$$

L'ordre de 10 modulo 13 est égal à 6 car

$$1/13 = .\dot{0}7692\dot{3}.$$

L'ordre de 10 modulo 17 est 16 car

$$1/17 = 0, \dot{0}588235294117647\dot{}.$$

Proposition 2.19. *Soit a un entier relativement premier à un entier $n > 0$. Pour tout entier $k > 0$ on a*

$$n \mid a^k - 1 \quad \Leftrightarrow \quad \mathrm{ord}(a; n) \mid k.$$

Preuve: Posons $e = \mathrm{ord}(a; n)$. Si $e \mid k$ alors $k = qe$ pour un entier q. Par suite, $a^k \equiv a^{qe} \equiv (a^e)^q \equiv (1)^d \equiv 1$ modulo n. Inversement, supposons que l'on ait $a^k \equiv 1$ modulo n. Raisonnons par l'absurde en supposant que e ne divise pas k. On a alors $k = eq + r$ avec $0 < r < e$. Par suite $1 \equiv a^k \equiv a^{qe+r} \equiv a^{qe} a^r \equiv a^r$. C'est une contradiction car $r < e$ et que a est d'ordre n. CQFD

Proposition 2.20. *Soit a un entier relativement premier à $mn > 0$. Alors*

$$\mathrm{ord}(a; \mathrm{ppmc}(m, n)) = \mathrm{ppmc}(\mathrm{ord}(a, m), \mathrm{ord}(a, n)).$$

En particulier, si m et n sont relativement premiers, alors on a

$$\mathrm{ord}(a; mn) = \mathrm{ppmc}(\mathrm{ord}(a, m), \mathrm{ord}(a, n)).$$

Preuve: Pour tout entier $k > 0$ on a

$$\begin{aligned}\mathrm{ord}(a;\mathrm{ppmc}(m,n)) \mid k &\Leftrightarrow \mathrm{ppmc}(m,n) \mid k\\ &\Leftrightarrow m \mid k \quad \text{et} \quad n \mid k\\ &\Leftrightarrow \mathrm{ord}(a;m) \mid k \quad \text{et} \quad \mathrm{ord}(a;n) \mid k\\ &\Leftrightarrow \mathrm{ppmc}(\mathrm{ord}(a,m),\mathrm{ord}(a,n)) \mid k.\end{aligned}$$

Cela prouve que $\mathrm{ord}(a;\mathrm{ppmc}(m,n)) = \mathrm{ppmc}(\mathrm{ord}(a,m),\mathrm{ord}(a,n))$.

Corollaire 2.21. *Soit a un entier relativement premier à $n = p_1^{k_1}\cdots p_r^{k_r}$. Alors*

$$\mathrm{ord}(a;n) = \mathrm{ppmc}(\mathrm{ord}(a;p_1^{k_1}),\ldots,\mathrm{ord}(a;p_r^{k_r})).$$

Par exemple, l'ordre de 10 modulo 119 est $\mathrm{ppmc}(6,16) = 48$. Effectivement, on a

$$1/119 = 0,\dot{0}0840336134453781512605042016806722689075630252\dot{1}.$$

Soit $\phi(n)$ le nombre d'entiers $1 \le k \le n$ relativement premiers à n. On dit que ϕ est la *fonction indicatrice d'Euler*. On peut définir $\phi(n)$ comme le nombre de fractions réduites $0 < k/n \le 1$ de dénominateur n.

Un entier $1 \le k \le n$ est inversible modulo n ssi k est relativement premier à n d'après 25. Dénotons par U_n l'ensemble des éléments inversibles de Z_n. Si $u, v \in U_n$ alors $uv \in U_n$. En effet, le produit de deux entiers relativement premiers à n est relativement premier à n. Voici la table de multiplication de U_n pour $2 \le n \le 9$.

$U_2 = \{\underline{1}\} = \{1\}$,

×	1
1	1

$U_3 = \{\underline{1},\underline{2}\} = \{1,2\}$,

×	1	2
1	1	2
2	2	1

$U_4 = \{\underline{1},\underline{3}\} = \{1,3\}$,

×	1	3
1	1	3
3	3	1

$U_5 = \{\underline{1},\underline{2},\underline{3},\underline{4}\} = \{1,2,3,4\}$,

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$U_6 = \{\underline{1}, \underline{5}\} = \{1, 5\}$,

$\times$	1	5
1	1	5
5	5	1

$U_7 = \{\underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}\} = \{1, 2, 3, 4, 5, 6\}$,

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$U_8 = \{\underline{1}, \underline{3}, \underline{5}, \underline{7}\} = \{1, 3, 5, 7\}$,

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U_9 = \{\underline{1}, \underline{2}, \underline{4}, \underline{5}, \underline{7}, \underline{8}\} = \{1, 2, 4, 5, 7, 8\}$,

$\times$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Théorème 2.22. *(Euler) Si un entier a est relativement premier à un entier $n > 0$, alors on a*

$$a^{\phi(n)} \equiv 1 \mod n.$$

L'ordre de a modulo n est un diviseur de $\phi(n)$.

Preuve: Soit $x_1, x_2, \ldots, x_{\phi(n)}$ une liste des élements de U_n. Montrons la que la suite de classes

$$\underline{a} \cdot x_1, \ \underline{a} \cdot x_2, \ \ldots, \ \underline{a} \cdot x_{\phi(n)}$$

ne diffère de la suite $x_1, x_2, \ldots, x_{\phi(n)}$ que par l'ordre des termes. En effet, on a $\underline{a} \cdot x_i \in U_n$ puisque $\underline{a} \in U_n$ et $x_i \in U_n$. Les éléments $\underline{a} \cdot x_1, \underline{a} \cdot x_2, \ldots, \underline{a} \cdot x_{\phi(n)}$ sont distincts puisque a est cancellable modulo n. Cela

entraîne que tous les élément de U_n figurent une et une seule fois dans la liste $\underline{a} \cdot x_1, \underline{a} \cdot x_2, \ldots, \underline{a} \cdot x_{\phi(n)}$. (on pourrait aussi raisonner en utilisant le fait que la congruence $ax \equiv y$ est résoluble pour tout entier y). On a donc

$$\prod_{i=1}^{\phi(n)} \underline{a} \cdot x_i = \prod_{i=1}^{\phi(n)} x_i$$

puisque la valeur d'un produit ne dépend pas de l'ordre des facteurs. Mais on a

$$\prod_{i=1}^{\phi(n)} \underline{a} \cdot x_i = \Big(\prod_{i=1}^{\phi(n)} \underline{a}\Big) \cdot \Big(\prod_{i=1}^{\phi(n)} x_i\Big) = \underline{a}^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} x_i$$

car il y a $\phi(n)$ éléments dans U_n. On voit donc que

$$\underline{a}^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} x_i.$$

On peut canceller le produit $\prod_{i=1}^{\phi(n)} x_i$ de chaque membre car les facteurs x_i sont concellables. Cela donne

$$\underline{a}^{\phi(n)} = 1.$$

Le résultat est démontré. Autrement dit, $n \mid a^{\phi(n)} - 1$. Donc $\mathrm{ord}(a; n) \mid \phi(n)$ par la proposition 30. CQFD

Corollaire 2.23. *(Fermat) Si un nombre premier p ne divise pas un entier a alors on a*

$$a^{p-1} \equiv 1 \mod p.$$

L'ordre de a modulo p est un diviseur de $p - 1$.

Preuve: En effet, $\phi(p) = p - 1$. CQFD

Le théorème 2.22 serait incomplet sans une formule permettant de calculer $\phi(n)$. Pour y arriver, nous utiliserons le résultat suivant:

Théorème 2.24. *(Théorème Chinois) Soit m et n deux entiers relativement premiers. Alors pour tout couple d'entiers a et b, le système de congruences*

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

possède une solution x. Cette solution est unique modulo mn.

Preuve : Commençons par montrer que le système le système de congruence

$$\begin{aligned} x &\equiv 1 \mod m \\ x &\equiv 0 \mod n \end{aligned}$$

possède une solution e_1. La condition $e_1 \equiv 0 \bmod n$ signifie alors que l'on a $e_1 = nu$ pour un certain entier u. La condition $e_1 \equiv 1 \bmod m$ signifie que l'on a $nu \equiv 1 \bmod m$. Autrement dit, l'entier u est un inverse de n modulo m. Cet inverse existe d'après la proposition 22 puisque n est relativement premier à m. Cela montre l'existence de e_1. On montre de même que le système de congruence

$$\begin{aligned} x &\equiv 0 \mod m \\ x &\equiv 1 \mod n \end{aligned}.$$

possède une solution e_2. La solution au problème initial est alors obtenue en posant $x = ae_1 + be_2$. En effet, on a

$$\begin{aligned} ae_1 + be_2 &\equiv a1 + b0 \equiv a \mod m \\ ae_1 + be_2 &\equiv a0 + b1 \equiv b \mod n \end{aligned}.$$

Il reste à démontrer l'unicité. Pour cela supposons que l'on ait une autre solution:

$$\begin{aligned} y &\equiv a \mod m \\ y &\equiv b \mod n. \end{aligned}$$

On a alors $x \equiv a \equiv y \bmod m$ et $x \equiv a \equiv y \bmod n$. La différence $x - y$ est donc divisible par m et de n. Cette différence est par suite divisible par $\text{ppmc}(m, n)$. Mais on a $\text{ppmc}(m, n) = mn$ puisque m et n sont relativement premiers. Cela montre que $x \equiv y$ modulo mn. QED

Voici un tableau illustrant le théorème chinois dans le cas $m = 9$ et $n = 8$. Les valeurs de a se trouvent dans la bordure horizontale supérieure et les valeurs de b dans la bordure verticale gauche. Par exemple, Le système de congruences

$$\begin{aligned} x &\equiv 5 \mod 9 \\ x &\equiv 3 \mod 8 \end{aligned}$$

a pour solution $x = 59$.

	0	1	2	3	4	5	6	7	8
0	0	64	56	48	40	32	24	16	8
1	9	1	65	57	49	41	33	25	17
2	18	10	2	66	58	50	42	34	26
3	27	19	11	3	67	59	51	43	35
4	36	28	20	12	4	68	60	52	44
5	45	37	29	21	13	5	69	61	53
6	54	46	38	30	22	14	6	70	62
7	63	55	47	39	31	23	15	7	71

Proposition 2.25. *Si m et n sont relativement premiers alors $\phi(mn) = \phi(m)\phi(n)$.*

Preuve: Il suffit de montrer que, dans le théorème chinois, l'entier x est relativement premier à mn si et seulement si l'entier a est relativement premier à m et l'entier b est relativement premier à n. Supposons que x soit relativement premier à mn. Alors x est relativement premier à m, donc a est relativement premier à m puisque $x \equiv a \bmod m$. De même, b est relativement premier à n. Réciproquement, supposons que a soit relativement premier à m et b relativement premier à n. Alors x est relativement premier à m puisque $x \equiv a$ modulo m. De même, x est relativement premier à n puisque $x \equiv b$ modulo n. Donc, mn est relativement premier à x puisque m et n sont relativement premiers à x. CQFD

Voici un tableau illustrant le fait que $\phi(8 \times 9) = \phi(8)\phi(9)$. Dans la bordure horizontale, nous avons marqué par une étoile la position des entiers relativement premiers à 9, et dans la bordure verticale, la position des entiers relativement premiers à 8. Dans le rectangle 8×9 nous avons marqué la position des entiers relativement premiers à $8 \cdot 9$.

		*	*		*	*		*	*
*		*	*		*	*		*	*
*		*	*		*	*		*	*
*		*	*		*	*		*	*
*		*	*		*	*		*	*

Proposition 2.26. *Si $n = p_1^{a_1} \cdots p_k^{a_k}$ avec $a_i > 0$ et les facteurs premiers p_i sont distincts, alors on a*

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}) = n\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big).$$

Preuve: On a $\phi(n) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k})$ d'après 39 puisque les entiers $p_1^{a_1}, \ldots p_k^{a_k}$ sont relativement premiers deux à deux. Si p est premier et $a > 0$ montrons que $\phi(p^a) = p^a - p^{a-1}$. Le nombre $\phi(p^a)$ s'obtient en retranchant de p^a le nombre d'entiers $0 < k \leq p^a$ ayant un diviseur commun avec p^a. Un entier k possède un diviseur commun avec p^a ssi $k = pu$ pour un entier u. La condition $0 < pu \leq p^a$ équivaut à la condition $0 < u \leq p^{a-1}$. Ceci montre que le nombre d'entiers $0 < k \leq p^a$ ayant un diviseur commun avec p^a est égal à p^{a-1}. CQFD

Exercices pour la section 2

Il est intéressant de réduire le triangle de Pascal modulo un nombre premier p. Si $p = 2$, on obtient

$$\begin{array}{lccccccccccccccc}
0 \to & & & & & & & 1 & & & & & & & & \\
1 \to & & & & & & 1 & & 1 & & & & & & & \\
2 \to & & & & & 1 & & 0 & & 1 & & & & & & \\
3 \to & & & & 1 & & 1 & & 1 & & 1 & & & & & \\
4 \to & & & 1 & & 0 & & 0 & & 0 & & 1 & & & & \\
5 \to & & 1 & & 1 & & 0 & & 0 & & 1 & & 1 & & & \\
6 \to & 1 & & 0 & & 1 & & 0 & & 1 & & 0 & & 1 & & \\
7 \to & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 \\
8 \to 1 & & 0 & & 0 & & 0 & & 0 & & 0 & & 0 & & 0 & & 1 \\
 & & & & & & & \cdots & & & & & & & & &
\end{array}$$

On voit que $\binom{2^n}{k} \equiv 0$ modulo 2 pour tout $0 < k < 2^n$.

Exercice : (Leibniz) Soit p un nombre premier. Montrer que pour tout $0 < k < p$ on a

$$\binom{p}{k} \equiv 0 \quad \text{modulo} \quad p.$$

Suggestion: Utiliser le fait que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. En déduire que pour tout paire d'entiers a et b on a

$$(a+b)^p \equiv a^b + b^p \quad \text{modulo} \quad p.$$

En déduire que si $a_1, a_2, \ldots, a_k$ sont des entiers, alors on a

$$(a_1 + a_2 + \cdots + a_k)^p \equiv a_1^p + a_2^p + \cdots + a_k^p \quad \text{modulo} \quad p.$$

En déduire que pour tout entier k on a

$$k^p \equiv k \quad \text{modulo} \quad p.$$

Suggestion: Substituer $a_i = 1$ dans la relation précédente. En déduire le théorème de Fermat: si p ne divise pas k, alors

$$k^{p-1} \equiv 1 \quad \text{modulo} \quad p.$$

Exercice : Soit p^n une puissance de nombre premier. Montrer que pour tout $0 < k < p^n$ on a

$$\binom{p^n}{k} \equiv 0 \quad \text{modulo} \quad p.$$

Suggestion: Montrer par induction sur n que

$$(x+y)^{p^n} \equiv x^{p^n} + y^{p^n} \bmod \quad p$$

Exercice : Soit $a = a_0 + a_1 p + a_2 p^2 + \cdots$ le développement de l'entier a à la base p, et soit $b = b_0 + b_1 p + b_2 p^2 + \cdots$ le développement de l'entier b. Montrer que

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2}\cdots \quad \text{modulo} \quad p.$$

Suggestion: Montrer que

$$(x+y)^a \equiv (x+y)^{a_0}(x^p + y^p)^{a_1}(x^{p^2} + y^{p^2})^{a_2}\cdots \mod \quad p$$

Remarque: Si $b > a$ on pose $\binom{a}{b} = 0$.

Exercice : Trouver tous les entiers n pour lequels $\text{ord}(10, n) = 1, 2, 3, 4$ et 5 respectivement. Dresser une table du développement décimal de $1/n$.

Exercice : (Fermat) Soit p un nombre premier. Si q est un diviseur premier de $M_p = 2^p - 1$ montrer que $q \equiv 1 \bmod p$. *Suggestion*: Soit e l'ordre de 2 modulo q. Montrer en utilisant 30 que $e \mid p$. En déduire que $e = p$. Utiliser ensuite le théorème de Fermat 33 pour conclure que p divise $q - 1$.

Ce résultat est à la base d'une méthode de Fermat pour trouver des diviseurs premiers d'un nombre de Mersenne M_p. Par exemple, cherchons un diviseur premier q de M_{11}. On a forcément $q \equiv 1 \bmod 11$. Il faut donc que $q = 2n \cdot 11 + 1$ (puisque q est impair). Si $n = 1$, on obtient $q = 23$. On trouve effectivement que $2^{11} - 1 = 23 \cdot 89$. Mersenne avait sagement exclu M_{11} de sa liste. Cherchons un diviseur premier de $M_{13} = 8191$. Il faut que $q = 2n \cdot 13 + 1 = n \cdot 26 + 1$. Comme $91^2 > 8191$ on peut supposer que $q < 91$. Si

$n = 1$, on a $q = 27$ qui n'est pas premier. Si $n = 2, 3$ on a $q = 53, 79$. Mais on vérifie que 53 et 79 ne divisent pas 8191. Nous avons montré que M_{13} est premier.

Exercice : (Mersenne) Montrer que M_{17} et M_{19} sont premiers. Montrer que M_{23} et M_{29} sont composés.

Aux exercices de la section 2 nous avons introduit des nombres de Mersenne généralisés:

$$M_n(a) = \frac{a^n - 1}{a - 1} = 1 + a + a^2 + \cdots + a^{n-1}$$

où $n > 0$ et $a > 1$.

Exercice : Soit p un nombre premier. Si q est un diviseur premier de $M_p(a)$ ne divisant pas $a - 1$ alors on a $q \equiv 1 \bmod p$. *Suggestion*: Soit e l'ordre de a modulo q. Montrer que $e \mid p$. En déduire que $e = p$. Utiliser ensuite le théorème de Fermat pour conclure que p divise $q - 1$.

Exercice : (Euler) Soit q est un diviseur premier de $F_n = 2^{2^n} + 1$. Montrer que $q \equiv 1 \bmod 2^{n+1}$. Trouver un diviseur de F_5. *Suggestion*: Soit e l'ordre de 2 modulo q. Montrer que $e \mid 2^{n+1}$ mais que e ne divise pas 2^n. En déduire que $e = 2^{n+1}$. Utiliser ensuite le théorème de Fermat pour conclure que 2^{n+1} divise $q - 1$.

Exercice : (Lucas) Soit q est un diviseur premier de $F_n = 2^{2^n} + 1$. Montrer que $q \equiv 1 \bmod 2^{n+2}$. *Suggestion*: Posons $b = 2^{2^{n-2}}(2^{2^{n-1}} - 1)$. Montrer que $b^2 \equiv 2$ modulo q. Soit e l'ordre de b modulo q. Montrer que $e \mid 2^{n+2}$ mais que e ne divise pas 2^{n+1}. En déduire que $e = 2^{n+2}$. Utiliser ensuite le théorème de Fermat pour conclure que 2^{n+2} divise $q - 1$.

3. Une application à la cryptographie

La théorie des nombres ressemble à un pur jeu intellectuel. Elle parait inutile sinon comme divertissement de l'esprit. Le mathématicien Hardy, l'une des grandes figures de la théorie des nombres de la première moitié du 20^e-siècle, était fier de cette inutilité. Malheureusement, la théorie des nombres a trouvé de nombreuses applications depuis 30 ans, particulièrement dans les méthodes de cryptographie. Dans cette partie, nous décrivons la méthode de cryptographie RSA du nom de ses inventeurs: Rivest, Shamir et Adleman. Nous aurons besoin du résultat suivant.

Lemme 3.1. *Si a est relativement premier à n et si $k \equiv r$ modulo $\phi(n)$ alors*

$$a^k \equiv a^r \mod n$$

De plus, si $ed \equiv 1$ mod $\phi(n)$ alors

$$(a^e)^d \equiv a \mod n.$$

Preuve: Supposons que $k \equiv r \bmod \phi(n)$. On a alors $k = r + q\phi(n)$. Donc

$$a^k = a^{r+q\phi(n)} = a^r \cdot (a^{\phi(n)})^q \equiv a^r \mod n$$

car on $a^{\phi(n)} \equiv 1$ d'après le théorème d'Euler. Par suite, si $ed \equiv 1 \bmod \phi(n)$ alors

$$(a^e)^d \equiv a^{ed} \equiv a^1 \equiv a \mod n.$$

CQFD

Nous pouvons maintenant décrire la méthode de cryptographie RSA. Sa sureté repose sur le fait qu'il est très difficile de factoriser un nombre entier dont les facteurs premiers sont tous grands. Supposons qu'un personne que nous appellerons Fatima veuille s'assurer du secret des messages que d'autres personnes pourraient lui faire parvenir. Pour utiliser la méthode RSA, elle choisit deux nombres premiers p et q comportant une centaine de décimales chacun. Il existe pour cela des algorithmes très efficaces et nous n'en discuterons pas ici. Fatima calcule ensuite le produit $n = pq$ et $\phi(n) = (p-1)(q-1)$. Elle choisit ensuite un nombre e relativement premier à $\phi(n)$ qu'on appelle la *clé d'encodage*. Elle calcule ensuite l'inverse d de e modulo $\phi(n)$. On dit que d est la *clé de décodage*. Fatima fait parvenir n et e à toutes personnes souhaitant lui faire parvenir un message secret. Elle peut même afficher ces nombres publiquement. C'est pourquoi on dit que la crypthographie RSA est à *clé publique*. Fatima doit toutefois conserver secret le nombre d qui est la clé de décodage. Toute personne souhaitant faire parvenir un message secret à Fatima utilisera n et e pour encoder le message. Par exemple, supposons qu'une personne que nous appellerons David veuille envoyer un message secret à Fatima. Pour ce faire, il découpe son message en une suite de segments representés par des nombres $a_1, a_2, \ldots$ inférieurs à n. Il doit s'assurer que chaque nombre a_i est relativement premier à n. Cette condition est presque automatiquement satisfaite car la proportion des nombres relativement premiers à n est donnée par

$$\frac{\phi(n)}{n} = \Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{1}{q}\Big).$$

Cette quantité est très proche de 1 car $p, q > 10^{100}$. David encode ensuite chaque nombre a par le nombre $b \equiv a^e$ modulo n. Il transmet ensuite par courrier la suite $b_1, b_2, \ldots$ des nombres encodés. Pour déchiffrer le message recu Fatima doit décoder chacun des nombres b_i. Pour décoder un nombre b, elle calcule b^d modulo n. En effet, si $b = a^e$ alors

$$b^d = (a^e)^d = a^{ed} \equiv a \mod n$$

d'après le lemme 36. La message original est donc donné par la suite $b_1^d, b_2^d, \ldots$ modulo n. La sureté de la méthode repose sur le fait que seule Fatima connait la décomposition de n en facteurs premiers. Sans cette décomposition on ne peut calculer ni $\phi(n)$ ni d.

La faisabilité de la métode RSA dépend de la capacité de faire certains calculs sur ordinateur. En premier lieu, il faut disposer d'un algorithme permettant de choisir à volonté de grands nombres premiers Comme les nombres premiers sont très nombreux, il suffit d'un algorithme capable de reconnaitre rapidement si un grand nombre entier est premier ou non. On prend un grand nombre au hasard et on le rejette si l'algorithme ne le reconnait pas premier. Pour des nombres comportant une centaine de décimales on est pratiquement certain de tomber sur un nombre premier après un millier d'essais. Le tout peut se faire en une fraction de seconde avec un ordinateur. Pour coder (ou décoder) un messages il faut pouvoir aussi calculer rapidement les puissances a^r modulo n. Pour y arriver, on ramène l'opération d'exponentiation à des carrés et à des multiplications. Voici comment. Dénotons par $Q(x)$ le carré modulo n d'un nombre x. Si on applique k-fois l'opération Q on obtient une opération que nous dénoterons Q^k. On a

$$Q^k(x) = x^{2^k} \mod n.$$

Tout entier peut s'exprimer comme une somme de puissances de 2 en le développant à la base 2. Si $r = \sum_i 2^{k_i}$ alors on a

$$a^r = \prod_i a^{2^{k_i}} \equiv \prod_i Q^{k_i}(a) \mod n.$$

Cette méthode permet de ramener le calcul de a^r modulo n à un petit nombre de multiplications modulo n.

Nous allons illustrer la méthode RSA sur un exemple. Supposons que Fatima choisisse deux nombres premiers p et q dont le produit est

$$\begin{aligned} n = pq = {} & 364615485029501136970713101143871109540079913994317049087258562868354903436255206 \\ & 595580958951461147024129894416770392933752888490885711614193520646632973108 \\ & 751496411205454301933653621610762952359760633015466919606414418247273955697 4 \\ & 502462402438903115845725630946428943768540714098264727068026730424033578827 8869 \\ & 167617014292649505738991861 77. \end{aligned}$$

Elle se garde de révéler la factorisation $n = pq$ à quiconque. Supposons que Fatima choisisse ensuite la clé d'encodage suivante:

$$\begin{aligned} e =& 61236041383216780461848130017520495056527897282773324515417694382704004578956878070180147610111027621046907371564049014274722806296588432313034017228659717947654701666073461507815678579317437453094092 7 \end{aligned}$$

Elle vérifie que e est relativement premier à $\phi(n) = (p-1)(q-1)$. Elle calcule ensuite l'inverse d de e modulo $\phi(n)$. Elle se garde de révéler d à quiconque. Fatima affiche les nombres n et e sur son site web. Supposons maintenant que David fasse parvenir à Fatima un court message représenté par un entier $a < n$ relativement premier à n. Pour cela, il calcule $b = a^e$ modulo n et fait parvenir le résultat à Fatima par courrier électronique normal:

$$\begin{aligned} b =& 17625744501924345109878124630673256866678025110105065425143515703901863216344159410481044239319582998436351975479479033307060956350192980883359851606273488853970490387337105012487817424766791014862809424441254161086547658789472293665421172412141822629738484574434341548820462176582203359992048493353809217331687670144353382801454157424429 2 3. \end{aligned}$$

Pouvez-vous déchiffrer le message de David à Fatima?

Exercice: Fatima est mathématicienne. Elle n'a pas choisit les nombres premiers p et q au hasard, car elle adore certains nombres premiers. C'est une grave erreur. Cette information peut suffire à déchiffrer les messages destinés à Fatima. En effet, les nombres premiers ayant fait l'objet d'une étude ont pour la plupart fait l'objet d'une publication. Il y en a quelques milliers au plus. On pourrait en faire l'inventaire. On pourrait chercher ensuite des diviseurs de n dans cet inventaire. Cela réduirait considérablement les calculs pour factoriser n. Par exemple, il y a moins de 40 nombres premiers de Mersenne connus. Chercher par ordinateur un diviseur de n parmi les nombres de Mersenne. Factoriser n. Calculer $\phi(n)$ et ensuite d. Déchiffrer le message secret de David à Fatima.

4. Racines primitives

Soit p est un nombre premier ne divisant pas un entier a. D'après le théorème de Fermat, l'ordre de a modulo p est un diviseur de $p-1$. Si cet ordre est exactement $p-1$ on dit que a est une *racine primitive* modulo p. Le nombre 10 est une racine primitive modulo p ssi la longueur de la période du développement décimal de $1/p$ est égale à $p-1$. Dans ce cas, on dit que p est un nombre premier *long*. Examinons les valeurs de la fonction $\mathrm{ord}(a;p)$ pour $0 < a < p$ et $p \leq 17$.

a	1
$\mathrm{ord}(a;2)$	1

a	1	2
$\mathrm{ord}(a;3)$	1	2

a	1	2	3	4
$\mathrm{ord}(a;5)$	1	4	4	2

a	1	2	3	4	5	6
$\mathrm{ord}(a;7)$	1	3	6	3	6	2

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ord}(a;11)$	1	10	5	5	5	10	10	10	5	2

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ord}(a;13)$	1	12	3	6	4	12	12	4	3	6	12	2

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ord}(a;17)$	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

On voit par exemple que 3 et 5 sont des racines primitives modulo 7, et que 2,6,7 et 11 sont des racines primitives modulo 13. Sur la base de ces donnés on peut conjecturer qu'il y a toujours au moins une racine primitive modulo p. Les puissances d'une racine primitive

$$a^0, a^1, a^2, \ldots a^{p-1}$$

sont distinctes modulo p. En effet, si on avait $a^k \equiv a^{k+r} \bmod p$ avec $0 < r < p$ on aurait $1 \equiv a^r \bmod p$ ce qui est absurde puisque a est d'ordre $p-1$. On en déduit que toute classe de congruence non nulle $x \in \mathbf{Z}_p$ est de la forme a^r pour un unique $0 < r < p-1$. L'exponentiation $r \mapsto a^r$ fournit une bijection entre l'ensemble $\mathbf{Z}_{p-1}$ des classes de congruences modulo $p-$ et l'ensemble U_p des classes de congruence non nulle modulo p. La bijection inverse est une forme de logarithme $log_a(;p) : U_p \to \mathbf{Z}_{p-1}$. Par exemple, si $p = 13$ on peut prendre $a = 2$ comme racine primitive. On obtient

$r(\mathrm{mod}\ 12):$	0	1	2	3	4	5	6	7	8	9	10	11
$2^r(\mathrm{mod}\ 13):$	1	2	4	8	3	6	12	11	9	5	10	7

$x(\mathrm{mod}\ 13):$	1	2	3	4	5	6	7	8	9	10	11	12
$log_2(x;13):$	0	1	4	2	9	5	11	3	8	10	7	6

La relation $a^r a^s = a^{r+s}$ entraîne que pour tout $x, y \in U_p$ on a

$$log_a(xy;p) \equiv log_a(x;p) + log_a(y;p) \mod p-1.$$

Le logarithme permet de ramener la multiplication modulo p à une addition modulo $p-1$.

Mous allons démontrer l'existence d'une racine primitive modulo p pour tout nombre premier p. Nous aurons besoin de quelques résultats préliminaires. Soit U_n l'ensemble des élements inversibles de $\mathbf{Z}_n$.

Lemme 4.1. *Si un entier $d > 0$ divise l'ordre d'un élement $x \in U_n$ alors*

$$\mathrm{ord}(x^d;n) = \frac{1}{d} \cdot \mathrm{ord}(x;n).$$

Si l'ordre de $x \in U_n$ est relativement premier à l'ordre de $y \in U_n$ alors

$$\mathrm{ord}(xy;n) = \mathrm{ord}(x;n) \cdot \mathrm{ord}(y;n)$$

Preuve: Posons $r = \mathrm{ord}(x;n)$. Montrons que l'ordre de x^d est égal à r/d. On a $(x^d)^{r/d} = x^e = 1$. Soit $k > 0$ et supposons que $(x^d)^k = 1$. On a alors $r \mid dk$ puisque $x^{dk} = (x^d)^k = 1$. Par suite $(r/d) \mid k$. Cela montre que l'ordre de x^d est égal à r/d. Soit $x, y \in U_n$ et supposons que les entiers $r = \mathrm{ord}(x;n)$ et $s = \mathrm{ord}(y;n)$ soient relativement premiers. Il existe des entiers $u, v \in \mathbf{Z}$ tels que $1 = ur + vs$ d'après ?. Remarquer que $(xy)^{vs} = x^{vs}y^{vs} = x^{vs} = x^{1-ur} = x$. De même, $(xy)^{ur} = y$. Montrons que l'ordre de xy est égal à rs. On a $(xy)^{rs} = x^{rs}y^{rs} = 1$. Soit $k > 0$ et supposons que $(xy)^k = 1$. On a alors $x^k = (xy)^{vsk} = 1$ et $y^k = (xy)^{urk} = 1$. Donc $e \mid k$ et $f \mid k$. Par suite, $ef \mid k$ puisque e et f sont relativement premier. CQFD

Nous dirons qu'un élément $g \in U_n$ est *d'ordre maximum* si son ordre est $\geq$ à l'ordre de tous les éléments de U_n. Il est évident que U_n contient un élément d'ordre maximum.

Lemme 4.2. *Soit $g \in U_n$ un élément d'ordre maximum. Alors l'ordre de tout élement de U_n divise l'ordre de g.*

Preuve: Posons $r = \mathrm{ord}(g; n)$. Si $x \in U_n$ montrons que $s = \mathrm{ord}(x; n)$ divise r. Sinon, il existe une puissance de nombre premier p^a divisant s mais ne divisant pas r. L'élement $z = x^{f/p^a}$ est d'ordre p^a par le lemme précédent. Quitte à remplacer x par z on peut donc supposer que x est d'ordre p^a. Soit p^b est la plus grande puissance de p divisant r. On a $b < a$ puisque p^a ne divise pas r. L'élément $y = g^{p^b}$ est d'ordre r/p^b par le lemme précédent. Les entiers p^a et r/p^b sont relativement premiers car les entiers p et r/p^b sont relativement premiers. Le produit xy est donc d'ordre $p^a \cdot r/p^b$ par le lemme précédent. C'est une contradiction car $p^a \cdot r/p^b = p^{a-b} \cdot r > r$ et g est d'ordre maximum. CQFD

Soit p un nombre premier. Nous voulons démontrer l'existence d'une racine primitive modulo p. Voici l'idée de la démonstration. Il s'agit de démontrer que U_p contient un élément d'ordre $p-1$. On peut toujours trouver un élément d'ordre maximum $g \in U_p$. Posons $r = \mathrm{ord}(g; p)$. Nous voulons montrer que $r = p - 1$. On sait que $r \mid p - 1$ par le théorème de Fermat. Nous allons raisonner par l'absurde en supposant que $r < p-1$. D'après le lemme 44 on a $a^r = 1$ pour tout $a \in U_p$. Autrement dit, modulo p, le polynôme $X^r - 1$ a pour racine $X = 1, 2, \cdots, p-1$. On peut donc le diviser par $(X-1), (X-2), \ldots, (X-p+1)$. Mais c'est impossible car $X^r - 1$ est de degré $r < p - 1$.

Le tableau suivant donne la valeur r d'une plus petite racine primitive modulo p pour $p \leq 89$.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89
r	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2	2	7	2	5	3	2	3

5. Fonctions arithmétiques

Nous dirons qu'une fonction $f(n)$ (à valeurs réelles) définie pour tout n entier ≥ 1 est une *fonction arithmétique*. La fonction indicatrice d'Euler ϕ est un exemple de fonction arithmétique. Soit $d(n)$ le nombre de diviseurs d'un entier $n \geq 1$. La fonction d est une fonction arithmétique. Soit $\sigma(n)$ la somme des diviseurs d'un entier $n \geq 1$. La fonction σ est une fonction arithmétique.

On définit la *somme* $f + g$ de deux fonctions arithmétiques f et g en posant $(f+g)(n) = f(n) + g(n)$. On définit le *produit de convolution* $f \star g$ en posant

$$(f \star g)(n) = \sum_{d|n} f(d)g(n/d).$$

Nous dénoterons par δ la fonction arithmétique définie par

$$\delta(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon.} \end{cases}$$

Proposition 5.1. *On a*
(i) $f \star g = g \star f$ *(commutativité)*
(ii) $f \star (g \star h) = (f \star g) \star h$ *(associativité)*
(iii) $f \star \delta = \delta \star f = f$ *(unité)*
(iv) $f \star (g + h) = f \star g + f \star h$ *(distributivité)*

Preuve: Démontrons (i). On a

$$(f \star g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ba=n} g(b)f(a) = (g \star f)(n).$$

Démontrons (ii). On a

$$(f\star(g\star h))(n)=\sum_{ad=n}f(a)(g\star h)(d)=\sum_{ad=n}\sum_{bc=d}f(a)g(b)h(c)=\sum_{abc=n}f(a)g(b)h(c)$$

$$((f\star g)\star h)(n)=\sum_{dc=n}(f\star g)(d)h(c)=\sum_{dc=n}\sum_{ab=d}f(a)g(b)h(c)=\sum_{abc=n}f(a)g(b)h(c)$$

Démontrons (iii). On a

$$(\delta\star f)(n)=\sum_{d|n}\delta(d)f(n/d)=f(n)$$

Démontrons (iv). On a

$$\begin{aligned}(f\star(g+h))(n)&=\sum_{ab=n}f(a)(g(b)+h(b))=\sum_{ab=n}f(a)g(b)+f(a)h(b)\\&=\sum_{ab=n}f(a)g(b)+\sum_{ab=n}f(a)h(b)=f\star g+f\star h\end{aligned}$$

On définit la fonction arithmétique Z en posant $Z(n)=1$ pour tout $n\geq 1$. Pour toute fonction arithmétique f, on a

$$(Z\star f)(n)=\sum_{d|n}f(d).$$

En particulier, $(Z\star Z)(n)$ est le nombre de diviseurs de n. Donc $Z\star Z$ est égale à la fonction d qui donne le nombre de diviseurs. On définit la fonction arithmétique I en posant $I(n)=n$ pour tout $n\geq 1$. On a

$$(Z\star I)(n)=\sum_{d|n}d.$$

Donc $Z\star I$ est égale à la fonction σ qui donne la somme des diviseurs.

On dit qu'une fonction arithmétique f est *multiplicative* si $f(1)=1$ et si on a $f(mn)=f(m)f(n)$ pour m et n relativement premiers.

Par exemple, la fonction indicatrice d'Euler ϕ est multiplicative d'après ?. Une fonction multiplicative f est déterminée par ses valeurs $f(p^a)$ pour p premier et $a>0$. En effet, si $n=p_1^{a_1}\cdots p_k^{a_k}$ alors $f(n)=f(p_1^{a_1})\cdots f(p_k^{a_k})$.

Lemme 5.2. *Soient $m,n>0$ des entiers relativement premiers. Tout diviseur d de mn est un produit $d=ab$ pour un couple unique de diviseurs $a\mid m$ et $b\mid n$.*

Proposition 5.3. *Le produit de convolution de deux fonctions multiplicatives est une fonction multiplicative.*

Preuve: Soient f et g deux fonctions multiplicatives. On a $(f\star g)(1)=f(1)g(1)=1$. Si m et n sont des entiers relativement premiers alors tout diviseur d de mn est un produit $d=ab$ pour un couple unique de diviseurs $a\mid m$ et $b\mid n$. Les entiers a et b sont relativement premier, de même que les entiers m/a et n/b. Par suite

$$\begin{aligned}(f\star g)(mn)&=\sum_{d|mn}f(d)g(\frac{mn}{d})=\sum_{a|m}\sum_{b|n}f(ab)g(\frac{mn}{ab})\\&=\sum_{a|m}\sum_{b|n}f(a)f(b)g(m/a)g(n/b)=\Big(\sum_{a|m}f(a)g(m/a)\Big)\Big(\sum_{b|n}f(b)g(n/b)\Big)\\&=(f\star g)(m)(f\star g)(n).\end{aligned}$$

Corollaire 5.4. *Les fonctions d et σ sont multiplicatives. Si $n = p_1^{a_1} \cdots p_k^{a_k}$ alors on a*

$$d(n) = (a_1 + 1) \cdots (a_k + 1)$$
$$\text{et} \quad \sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \cdots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Preuve: Les fonctions Z et N sont multiplicatives. Donc aussi les fonctions $d = Z \star Z$ et $\sigma = Z \star I$. Si p est premier et $a > 0$ les diviseurs de p^a sont $1, p, p^2, \ldots, p^a$. Par suite $d(p^a) = a + 1$ et

$$\sigma(p^a) = 1 + p + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$$

CQFD

On définit la *fonction de Mœbius* $\mu(n)$ en posant

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers } \textit{distincts}; \\ 0 & \text{sinon.} \end{cases}$$

Par exemple, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$ et $\mu(6) = 1$. La fonction de Mobius est multiplicative. Si p est premier et $a > 0$ on a

$$\mu(p^a) = \begin{cases} -1 & \text{si } a = 1 \ ; \\ 0 & \text{sinon.} \end{cases}$$

Proposition 5.5. *On a $Z \star \mu = \delta$.*

Preuve: La fonction $Z \star \mu$ est multiplicative puisque les fonctions Z et μ sont multiplicatives. Pour vérifier que l'on a $Z \star \mu = \delta$ il suffit donc de vérifier que l'on a $(Z \star \mu)(p^a) = \delta(p^a)$ pour p premier et $a > 0$. Mais

$$(Z \star \mu)(p^a) = \sum_{i=0}^{a} \mu(p^i) = \mu(1) + \mu(p) = 1 - 1 = 0,$$

ce qui donne le résultat cherché car $\delta(p^a) = 0$. CQFD

Corollaire 5.6. *(Mœbius) Si f et g sont des fonctions arithmétiques, alors les deux identités suivantes sont équivalentes*

$$\text{(i)} \ \ g(n) = \sum_{d|n} f(d) \quad \text{et} \quad \text{(ii)} \ \ f(n) = \sum_{d|n} g(d)\mu(n/d)$$

Preuve: L'identité (i) signifie que l'on a $g = Z \star f$ et l'identité (ii) que l'on a $f = \mu \star g$. Mais si $g = Z \star f$ alors

$$\mu \star g = \mu \star (Z \star f) = (\mu \star Z) \star f = \delta \star f = f.$$

Et si $f = \mu \star g$ alors

$$Z \star f = Z \star (\mu \star g) = (Z \star \mu) \star g = \delta \star g = g.$$

CQFD

Corollaire 5.7. *Pour tout $n > 0$ on a*

$$\text{(i)} \ \ n = \sum_{d|n} \phi(d) \quad \text{et} \quad \text{(ii)} \ \ \phi(n) = \sum_{d|n} \mu(n/d) \cdot d$$

Preuve: Pour démontrer (i) considérons d'abord un exemple avec $n = 12$. Les fractions de dénominateurs 12 sont

$$1/12, 2/12, 3/12, 4/12, 5/12, 6/12, 7/12, 8/12, 9/12, 10/10, 11/12, 12/12$$

Parmi ces 12 fractions on trouve

$\phi(12) = 4$ fractions réduites: $1/12, 5/12, 7/12, 11/12$;
$\phi(6) = 2$ fractions dont le dénominateur réduit est 6: $1/6, 5/6$;
$\phi(4) = 2$ fractions dont le dénominateur réduit est 4: $1/4, 3/4$;
$\phi(3) = 2$ fractions dont le dénominateur réduit est 3: $1/3, 2/3$;
$\phi(2) = 1$ fraction dont le dénominateur réduit est 2: $1/2$;
$\phi(1) = 1$ fraction dont le dénominateur réduit est 1: $1/1$.
Comme il y a 12 fractions en tout on obtient que

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) = 12.$$

Le même raisonnement montre plus généralement que l'identité (i) est vrai. L'identité (ii) est alors une conséquence de (i). CQFD

Ce résultat permet de donner une nouvelle démonstration de la proposition ?. la fonction ϕ est multiplicative car $\phi = I \star \mu$ et les fonctions I et μ sont multiplicatives. Il suffit donc de calculer les valeurs $\phi(p^a)$ pour p est premier et $a > 0$. Mais on a

$$\phi(p^a) = \sum_{i=0}^{a} p^{a-i}\mu(p^i) = p^a - p^{a-1}.$$

Exercices pour la section 5

Exercice: On définit une fonction arithmétique Λ en posant

$$\Lambda(n) = \begin{cases} \ln(p) & \text{si } n = p^a \text{ avec } p \text{ premier et } a > 0 \\ 0 & \text{sinon} \end{cases}$$

Montrer que l'on a

$$\ln(n) = \sum_{d|n} \Lambda(d).$$

6. Produits Eulériens

La série

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

a été considérée pour la première fois par Euler. Elle définit la *fonction zeta de Riemann*. Vérifions que la série converge pour $s > 1$. Si $n \geq 2$ on a

$$\frac{1}{n^s} \leq \int_{n-1}^{n} \frac{dx}{x^s}$$

car la fonction x^{-s} est décroissante dans l'intervalle $[n-1, n]$. Par suite

$$\zeta(s) - 1 \leq \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s} = \int_{2}^{\infty} \frac{dx}{x^s} = \frac{x^{1-s}}{1-s} \,|_2^\infty = \frac{2^{1-s}}{s-1}.$$

Exercices 6.1. *(Euler) Soit s un nombre réel > 1. Montrer que l'on a*

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - \frac{1}{p^s}}$$

Suggestion: *Utiliser la série géométrique*

$$\frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots.$$

Exercices 6.2. *Soit s un nombre réel > 1. Montrer que l'on a*

$$\begin{aligned} 2^{-s}\zeta(s) &= 1 + \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{10^s} + \frac{1}{12^s} + \cdots \\ (1 - 2^{-s})\zeta(s) &= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots \\ (1 - 2^{1-s})\zeta(s) &= 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \cdots \end{aligned}$$

Une remarque s'impose. On dit qu'une série de la forme

$$S = a_0 - a_1 + a_2 - a_3 + \cdots$$

avec $a_n \geq 0$ est une série *alternée*. Supposons que $a_n \geq a_{n+1}$ pour tout $n \geq 0$ et que $a_n \to 0$ lorsque n croit. Dans ce cas la série alterné converge. En effet, considérons les sommes partielles $S_n = a_0 - a_1 + a_2 - \ldots + (-)^n a_n$. On peut voir que

$$S_1 \leq S_3 \leq S_5 \leq \cdots \leq S_4 \leq S_2 \leq S_0$$

Comme l'écart $S_{2n} - S_{2n+1} = a_{2n+1}$ tend vers 0, on voit que les sommes partielles S_n s'approchent d'une limite S:

$$S_1 \leq S_3 \leq S_5 \leq \cdots \leq S \leq \cdots \leq S_4 \leq S_2 \leq S_0.$$

Par exemple, la série harmonique alternée $1 - 1/2 + 1/3 - 1/4 + \cdots$ converge. On peut même en calculer la somme. En effet, en intégrant la série géométrique

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$$

on obtient que

$$\ln\Big(\frac{1}{1-x}\Big) = x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \cdots.$$

Si on substitue ensuite $x = -1$ on obtient que

$$\ln 2 = 1 - 1/2 + 1/3 - 1/4 + \cdots.$$

Remarquons maintenant que la série

$$(1 - 2^{1-s})\zeta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \cdots$$

est alternée. Elle converge pour tout $s > 0$. Cela permet de définir la fonction $\zeta(s)$ pour $0 < s < 1$ en posant

$$\zeta(s) = \frac{1}{1 - 2^{1-s}}\Big(1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \cdots\Big).$$

Exercices 10. *Montrer que*

$$\lim_{s\to 1}(s-1)\zeta(s) = 1$$

Suggestion: *Utiliser le développement* $2^x = e^{x\ln 2} = 1 + x\ln 2 + \cdots$.

On dit qu'une série de la forme

$$\sum_{n=1}^{\infty}\frac{a_n}{n^s} = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \frac{u_5}{5^s} + \cdots$$

est une *série de Dirichlet*. Le produit de deux séries de Dirichlet est encore un série de Dirichlet. En effet,

$$\Big(\sum_{n=1}^{\infty}\frac{a_n}{n^s}\Big)\Big(\sum_{n=1}^{\infty}\frac{b_n}{n^s}\Big) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{a_n}{n^s}\frac{b_m}{m^s} = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{a_nb_m}{(nm)^s} = \sum_{l=1}^{\infty}\sum_{mn=l}\frac{a_nb_m}{l^s} = \sum_{l=1}^{\infty}\frac{c_l}{l^s}$$

avec $c_l = \sum_{mn=l} a_nb_m$.

Exercices 11. *Si*

$$f(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

montrer que l'on a

$$\zeta(s)f(s) = \sum_{n=1}^{\infty}\frac{b_n}{n^s}$$

avec $b_n = \sum_{d|n} a_d$. *En déduire que l'on*

$$\zeta(s)^2 = \sum_{n=1}^{\infty}\frac{d(n)}{n^s} \quad \text{et} \quad \zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty}\frac{\sigma(n)}{n^s}$$

où $d(n)$ *est le nombre de diviseur de* n *et* $\sigma(n)$ *la somme des diviseurs de* n. Suggestion: *Pour la seconde égalité, utiliser le fait que*

$$\zeta(s-1) = 1 + \frac{2}{2^s} + \frac{3}{3^s} + \frac{4}{4^s} + \frac{5}{5^s} + \cdots.$$

Exercices 12. *Soit* $a(n)$ *une fonction multiplicative. Montrer (en négligeant les questions de convergence) que l'on a*

$$\sum_{n=1}^{\infty}\frac{a(n)}{n^s} = \prod_{p \text{ premier}}\Big(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \frac{a(p^3)}{p^{3s}} + \cdots\Big).$$

Pour tout nombre entier $n > 0$ posons

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers } \textit{distincts}; \\ 0 & \text{sinon.} \end{cases}$$

Par exemple, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$ et $\mu(6) = 1$. On dit que $\mu(n)$ est la *fonction de Mœbius*.

Exercices 13. *Montrer que la fonction de Mœbius est multiplicative. En déduire que*

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \prod_{p \text{ premier}}\Big(1 - \frac{1}{p^s}\Big) = \frac{1}{\zeta(s)}$$

Exercices 14. *Soit $a(n)$ une fonction définie pour n entier > 0. Si $b(n) = \sum_{d|n} a(d)$ montrer que*

$$a(n) = \sum_{d|n} b(d)\mu(\frac{n}{d}).$$

Suggestion: *Si $f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ alors $\zeta(s)f(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$. Donc*

$$f(s) = \frac{1}{\zeta(s)} \sum_{n=1}^{\infty} \frac{b(n)}{n^s}.$$

7 Bibliographie

J.H. Conway, K.R. Guy. "The Book of Numbers" Springer-Verlag. New York, Berlin.
P. Damphousse. "L'arithmétique ou l'art de compter" Édition quatre à quatre, France.
H. Davenport. "The Higher Arithmetic". Cambridge University Press.
Jean-Paul Delahaye. "Merveilleux Nombres Premiers" Belin, Collection Pour La Science. Paris.
G.H. Hardy & E.M. Wright. "An Introduction to the Theory of Numbers" Oxford Univ. Press.
J-M. De Koninck A. Mercier. "Introduction à la théorie des nombres" Modulo, Quebec.
M. Krizeck, F. Luca & L. Somer. "17 Lectures on Fermat Numbers" Sringer, CMS. New York, Berlin.
Paulo Ribenboim. "My Numbers, My Friends" Springer. New York, Berlin.