

Chapitre II — Petit théorème de Fermat - Théorème d'Euler

On présente dans ces notes certains résultats fondamentaux sur les entiers, issus de la notion de divisibilité décrite dans le premier chapitre. Étant donné un nombre premier p , le petit théorème de Fermat affirme que pour tout $a \in \mathbb{Z}$, non divisible par p , on a

$$a^{p-1} \equiv 1 \pmod{p},$$

ou ce qui revient au même, que pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \pmod{p}$. Fermat l'énonça en 1640. Il semble que la première démonstration de ce résultat fut publiée par Euler en 1736. Par la suite, Euler généralisa cet énoncé en établissant que pour tout $n \geq 1$ et tout $a \in \mathbb{Z}$ premier avec n , on a

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

où $\varphi(n)$ est le nombre d'entiers compris entre 1 et n et premiers avec n . Si n est premier, on a $\varphi(n) = n - 1$, et on retrouve ainsi le petit théorème de Fermat. Les applications de ces résultats sont considérables en théorie élémentaire des nombres. Comme conséquence du théorème d'Euler, on définira pour tout $n \geq 1$ ce que l'on appelle, l'ordre multiplicatif modulo n d'un entier premier avec n , qui est une notion essentielle en arithmétique.

On établira en application quelques propriétés concernant les entiers de la forme

$$2^p - 1,$$

où p est un nombre premier. Ces entiers s'appellent les nombres de Mersenne. Nous verrons notamment certaines questions ou conjectures à leur sujet, datant de plusieurs siècles, qui suscitent de nos jours de nombreuses recherches.

Table des matières

1. Le petit théorème de Fermat	2
2. Test de Fermat	5
3. La fonction indicatrice d'Euler	7
4. Le théorème d'Euler	11
5. L'ordre multiplicatif modulo n d'un entier premier avec n	13
6. Nombres de Mersenne	16

1. Le petit théorème de Fermat¹

Il s'agit de l'énoncé suivant.

Théorème 2.1. *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, non divisible par p , on a*

$$(1) \quad a^{p-1} \equiv 1 \pmod{p}.$$

Démonstration : Soit a un entier relatif non divisible par p . Posons

$$N = \prod_{k=1}^{p-1} ka.$$

Pour tout $k = 1, \dots, p-1$, notons r_k le reste de la division euclidienne de ka par p . On a

$$N \equiv \prod_{k=1}^{p-1} r_k \pmod{p}.$$

Vérifions que si $k \neq k'$, on a $r_k \neq r_{k'}$. Si $r_k = r_{k'}$, on a $ka \equiv k'a \pmod{p}$ i.e. p divise $a(k - k')$. Par hypothèse, p ne divise pas a , donc p divise $k - k'$ (cor. 1.1). Parce que k et k' sont plus petits que $p-1$, on obtient $k = k'$ et notre assertion. Par ailleurs, r_k n'est pas nul. On en déduit que l'on a

$$\prod_{k=1}^{p-1} k = \prod_{k=1}^{p-1} r_k.$$

L'égalité

$$N = a^{p-1} \prod_{k=1}^{p-1} k$$

et le corollaire 1.1 impliquent alors le résultat.

¹ Pierre de Fermat est né près de Toulouse en 1601 et mourut à Castres en 1665. Bien qu'il consacra une partie de sa carrière à sa fonction de conseiller à la Cour de Toulouse, il restera comme l'un des grands mathématiciens de son temps, notamment pour ses travaux en théorie de nombres et en probabilité. Il existe aussi un «grand théorème de Fermat», qui en réalité n'est devenu un théorème qu'en 1994. Il s'agit de l'énoncé suivant : pour tout entier $n \geq 3$, il n'existe pas d'entiers relatifs x, y et z tels que $x^n + y^n = z^n$ avec $xyz \neq 0$. L'entier $n = 2$ doit évidemment être exclu vu que pour tous a et b dans \mathbb{Z} , on a l'égalité $(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$, ce qui géométriquement signifie qu'il existe une infinité de triangles rectangles dont les longueurs des côtés sont des entiers. La recherche d'une démonstration, ne serait-ce que pour des valeurs particulières de l'exposant n , a par exemple donné naissance à la notion d'idéal d'un anneau, puis à toute la théorie algébrique des nombres.

Corollaire 2.1. Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, on a

$$(2) \quad a^p \equiv a \pmod{p}.$$

Démonstration : La congruence (2) est vraie si p divise a . Si p ne divise pas a , elle se déduit directement de (1).

Autre démonstration du corollaire. Il suffit d'établir la congruence (2) pour tout $a \in \mathbb{N}$. On procède par récurrence sur a . Elle est vraie si $a = 0$. Supposons la condition (2) satisfaite par un entier $a \in \mathbb{N}$. Vérifions qu'elle l'est aussi avec l'entier $a + 1$. D'après la formule du binôme de Newton², on a

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

On a l'égalité

$$p! = k!(p - k)! \binom{p}{k}.$$

Pour tout $k = 1, \dots, p - 1$, il en résulte que p divise $\binom{p}{k}$. On obtient ainsi

$$(a + 1)^p \equiv 1 + a^p \pmod{p}.$$

D'après l'hypothèse de récurrence, on a $a^p \equiv a \pmod{p}$, d'où $(a + 1)^p \equiv a + 1 \pmod{p}$ et le résultat.

² Isaac Newton était, entre autres, un mathématicien et physicien britannique, qui vécut de 1642 à 1727. Il est considéré comme l'un des plus grands scientifiques de tous les temps. En mathématiques, il s'est intéressé notamment au calcul différentiel et intégral. Rappelons que la formule du binôme, qui porte aujourd'hui son nom, affirme que pour tous $n \in \mathbb{N}$ et a, b dans un anneau commutatif (par exemple $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \dots$), on a l'égalité

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

Voyons pourquoi. Le calcul de $(a + b)^n$ s'obtient en choisissant dans chacun des n facteurs $a + b$, ou bien a ou bien b , en effectuant ensuite le produit des termes ainsi choisis et en additionnant tous les résultats obtenus (il y en a 2^n). Pour tout $k = 0, \dots, n$, si l'on choisit k fois a et donc $n - k$ fois b , on obtient le terme $a^k b^{n-k}$. Tous les termes du développement de $(a + b)^n$ sont donc de cette forme pour un certain k entre 0 et n . Il reste alors à remarquer que, pour k fixé, le nombre de tels termes est le nombre de façons de choisir k fois a parmi les n possibles, qui n'est autre que le nombre $\binom{n}{k}$ de parties à k éléments dans un ensemble à n éléments.

Exemples 2.1

1) Vérifions que 13 divise $2^{70} + 3^{70}$. On a $2^{12} \equiv 1 \pmod{13}$ (th. 2.1), d'où la congruence $2^{60} \equiv 1 \pmod{13}$. Par ailleurs, on a $2^5 \equiv 6 \pmod{13}$, d'où $2^{10} \equiv -3 \pmod{13}$, de sorte que $2^{70} \equiv -3 \pmod{13}$. La congruence $3^3 \equiv 1 \pmod{13}$ entraîne $3^{69} \equiv 1 \pmod{13}$, d'où $3^{70} \equiv 3 \pmod{13}$ et l'assertion.

2) Posons $a = (1035125)^{5642}$. Déterminons le reste de la division euclidienne de a par 17. On a $1035125 \equiv 12 \pmod{17}$, $12^{16} \equiv 1 \pmod{17}$ (th. 2.1) et $5642 \equiv 10 \pmod{16}$. On en déduit que l'on a $a \equiv 12^{5642} \equiv 12^{10} \pmod{17}$. On a $12 \equiv -5 \pmod{17}$, $12^2 \equiv 8 \pmod{17}$, $12^4 \equiv -4 \pmod{17}$, $12^8 \equiv -1 \pmod{17}$, d'où $a \equiv 9 \pmod{17}$. Le reste cherché est donc 9.

3) Soit p un nombre premier divisant $2^p + 1$. Vérifions que $p = 3$. L'entier $2^p - 2$ est divisible par p (cor. 2.1), donc p divise la différence $2^p + 1 - (2^p - 2) = 3$, d'où l'assertion.

4) Soit p un nombre premier impair. Il existe une infinité d'entiers n tels que p divise $n2^n + 1$. Vérifions que tel est le cas des entiers n de la forme

$$(p-1)(1+kp) \quad \text{où } k \in \mathbb{N}.$$

Pour un tel entier n , on a $n \equiv -1 \pmod{p}$. Par ailleurs, p divise $2^{p-1} - 1$ et $p-1$ divise n , donc on a $2^n \equiv 1 \pmod{p}$, d'où $n2^n + 1 \equiv 0 \pmod{p}$.

5) Soient p un nombre premier et a un entier non divisible par p . Il existe $b \in \mathbb{Z}$ tel que l'on ait

$$(3) \quad ab \equiv 1 \pmod{p}.$$

Par exemple, l'entier $b = a^{p-2}$ convient (th. 2.1). Il est unique modulo p . On dit que b est l'inverse de a modulo p . Cette assertion est aussi une conséquence du théorème de Bézout.

6) Soient p un nombre premier impair et a, b des entiers non divisibles par p , tels que p divise $a^2 + b^2$. Démontrons l'on a

$$p \equiv 1 \pmod{4}.$$

Puisque p ne divise pas a , il existe d'après (3) un entier c tel que l'on ait $ac \equiv 1 \pmod{p}$. Posons $d = bc$. D'après la congruence $a^2 + b^2 \equiv 0 \pmod{p}$, on obtient

$$d^2 \equiv -1 \pmod{p}.$$

On a $d^{p-1} \equiv 1 \pmod{p}$ (th. 2.1), d'où l'on déduit que l'on a

$$(d^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{puis} \quad (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

ce qui entraîne le résultat.

7) Démontrons qu'il n'existe pas de triplets (x, y, z) dans \mathbb{N}^3 , avec $xyz \neq 0$, tels que

$$(4) \quad 4xy - x - y = z^2.$$

Supposons qu'il existe un tel triplet $(x, y, z) \in \mathbb{N}^3$. L'entier $4x - 1$ est au moins égal à 3 et il possède un diviseur premier p congru à 3 modulo 4. De l'égalité

$$(4x - 1)(4y - 1) = (2z)^2 + 1,$$

on déduit que p divise $(2z)^2 + 1$ et que p ne divise pas z . Le résultat établi dans l'alinéa 6 conduit alors à une contradiction.

Signalons qu'il existe une infinité de triplets $(x, y, z) \in \mathbb{Z}^3$, avec $xyz \neq 0$ vérifiant (4). Tel est le cas pour tout $n \in \mathbb{Z}$ du triplet

$$(-1, 2n - 5n^2, 5n - 1).$$

8) Démontrons qu'il n'existe pas de couples (x, y) dans \mathbb{Z}^2 tels que

$$y^2 = x^3 + 7.$$

Supposons qu'il existe un tel couple $(x, y) \in \mathbb{Z}^2$. Supposons de plus que x soit pair. Dans ce cas, on a $y^2 \equiv 7 \pmod{8}$ et y est impair. On obtient une contradiction car le carré de tout nombre impair est congru à 1 modulo 8. Par suite, x est impair. On a

$$y^2 + 1 = (x + 2)((x - 1)^2 + 3).$$

L'entier $(x - 1)^2 + 3$ est congru à 3 modulo 4. Il possède donc un diviseur premier p congru à 3 modulo 4. Ainsi p divise $y^2 + 1$, p ne divise pas y , et l'alinéa 6 conduit de nouveau à une contradiction.

2. Test de Fermat

Un entier est dit composé s'il n'est pas premier. On a déjà évoqué dans le chapitre I le problème de savoir décider si un entier donné est premier ou non. Voyons à ce sujet ce que l'on entend par test de primalité. C'est en fait un critère de non primalité i.e. un critère de composition. Étant donné un entier n , il permet de démontrer que n est composé si tel est le cas. Il suffit qu'il ne satisfasse pas une condition du test. Si n «passe» avec succès de nombreux tests, il y a une grande probabilité pour que n soit premier, mais cela n'en fournit pas la preuve. Le petit théorème de Fermat constitue un test de primalité que l'on appelle le test de Fermat. En rapport avec son efficacité, c'est le test de primalité le plus simple.

Lemme 2.1 (Test de Fermat). Soit n un entier ≥ 2 . S'il existe un entier a tel que

$$(5) \quad 1 < a < n \quad \text{et} \quad a^n \not\equiv a \pmod{n},$$

alors n est composé.

Démonstration : C'est une conséquence directe du corollaire 2.1.

Si n est composé, ce test permet très souvent de l'établir, mais pas toujours. En effet, il existe des entiers n composés pour lesquels il n'existe pas d'entiers a satisfaisant la condition (5), autrement dit pour lesquels on a

$$a^n \equiv a \pmod{n} \quad \text{pour tout} \quad a \in \mathbb{Z}.$$

On les appelle les nombres de Carmichael, mathématicien américain qui vécut de 1879 à 1967. On peut démontrer que ce sont exactement les entiers n composés qui sont sans facteurs carrés, et tels que pour tout diviseur premier p de n , l'entier $p - 1$ divise $n - 1$. Rappelons qu'un entier n est dit sans facteurs carrés si pour tout nombre premier p , on a

$$v_p(n) \leq 1,$$

où $v_p(n)$ est la valuation p -adique de n . L'entier $561 = 3 \times 11 \times 17$ est le plus petit d'entre eux. On sait par ailleurs qu'il existe une infinité de nombres de Carmichael. En fait, pour tout x assez grand, il y a au moins $x^{\frac{2}{7}}$ nombres de Carmichael plus petits que x (Alford, Granville, Pomerance, 1994).

Remarques 2.1.

1) Soit n un nombre de Carmichael. On a $(-1)^n \equiv -1 \pmod{n}$, donc n est impair (on a $n \neq 2$). En admettant le critère signalé ci-dessus, vérifions que n a au moins trois diviseurs premiers. Par définition, n est composé. Supposons que l'on ait $n = pq$, où p et q sont des nombres premiers distincts. On a $n - 1 = (p - 1)q + (q - 1)$. Puisque p divise n , $p - 1$ divise $n - 1$, donc $p - 1$ divise $q - 1$. De même $q - 1$ divise $p - 1$, d'où $p = q$ et une contradiction.

2) Soit m un entier ≥ 1 . Supposons que $6m + 1$, $12m + 1$ et $18m + 1$ soient des nombres premiers. Posons

$$N = (6m + 1)(12m + 1)(18m + 1).$$

On a $N - 1 = 1296m^3 + 396m^2 + 36m$, qui est divisible par $6m$, $12m$ et $18m$. En admettant de nouveau le critère ci-dessus, N est donc un nombre de Carmichael. Cela fournit un moyen assez simple d'expliciter de tels entiers. Par exemple, pour $m = 1$, on obtient $N = 7 \times 13 \times 19 = 1729$ qui est donc un nombre de Carmichael. Cela étant, on ne sait pas s'il existe une infinité d'entiers m tels que $6m + 1$, $12m + 1$ et $18m + 1$ soient premiers. C'est vraisemblable au vu de l'expérimentation numérique.

Exemple 2.2. Prenons $n = 10^{100} + 3$. On peut vérifier, en moins d'une seconde sur machine, que n est composé en constatant que 2^{n-1} n'est pas congru à 1 modulo n .

On est resté longtemps avec l'idée que la congruence

$$(6) \quad 2^{n-1} \equiv 1 \pmod{n}$$

devait caractériser les entiers premiers impairs n . Ce n'est qu'en 1819 qu'on a trouvé un contre-exemple (Sarrus) avec $n = 341$, qui est le produit de 11 par 31. Signalons cependant que la condition (6) caractérise le fait pour certains entiers n d'être premiers. Par exemple, on établira plus loin (voir prop. 2.4) que si p est premier, on a l'équivalence

$$(7) \quad 2p + 1 \text{ est premier} \iff 2^{2p} \equiv 1 \pmod{2p + 1}.$$

Cela fournit un critère de primalité pour les entiers de la forme $2p + 1$ où p est premier. On ne sait pas démontrer l'existence d'une infinité de p premiers tels que $2p + 1$ le soit aussi. Là encore, on peut se convaincre facilement sur machine que c'est vraisemblable.

3. La fonction indicatrice d'Euler³

Il s'agit de la fonction $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$ définie comme suit.

Définition 2.1. Pour tout $n \geq 1$, l'entier $\varphi(n)$ est le nombre des entiers k pour lesquels on a

$$1 \leq k \leq n \quad \text{et} \quad \text{pgcd}(k, n) = 1.$$

Autrement dit, $\varphi(n)$ est le nombre d'entiers compris entre 1 et n et premiers avec n . Par exemple, on a $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, et pour tout nombre premier p , on a $\varphi(p) = p - 1$. Plus généralement :

Lemme 2.2. Pour tout nombre premier p et tout entier $r \geq 1$, on a

$$\varphi(p^r) = p^r - p^{r-1}.$$

Démonstration : Il y a p^{r-1} entiers multiples de p compris entre 1 et p^r , ce qui implique l'assertion car les entiers premiers avec p^r sont ceux non multiples de p .

³ Leonhard Euler était un mathématicien suisse. Il est né à Bâle en 1707 et décède à Saint-Petersbourg en 1783. Il apporta d'importantes contributions en théorie des nombres et en analyse. Il établit sa renommée en calculant la somme des inverses des carrés des entiers, en démontrant l'égalité $\sum \frac{1}{n^2} = \frac{\pi^2}{6}$, où n parcourt les entiers ≥ 1 .

Explicitons $\varphi(n)$ pour tout $n \geq 1$. On va voir en particulier que $\frac{\varphi(n)}{n}$ ne dépend que de l'ensemble des diviseurs premiers de n .

Théorème 2.2. *Soit n un entier ≥ 1 . On a l'égalité*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

où p parcourt l'ensemble des diviseurs premiers de n .

Démontrons cet énoncé. Adoptons pour cela la terminologie suivante.

Terminologie. Soit n un entier naturel non nul. Appelons système réduit modulo n , tout ensemble X formé d'entiers naturels premiers avec n , tel que chaque entier relatif premier avec n soit congru à un unique élément de X modulo n .

Lemme 2.3. *Pour tout $n \geq 1$, il existe un système réduit modulo n . Chaque système réduit modulo n est fini de cardinal $\varphi(n)$.*

Démonstration : Posons

$$X = \left\{ k \in \mathbb{N} \mid 1 \leq k \leq n \text{ et } \text{pgcd}(k, n) = 1 \right\}.$$

C'est un système réduit modulo n . En effet, soit a entier relatif premier avec n . Il existe un unique entier k tel que l'on ait $1 \leq k \leq n$ et que $a \equiv k \pmod{n}$ (cf. lemme 1.4). Parce que a est premier avec n , il en est de même de k , donc k est dans X . De plus, $|X|$ désignant le cardinal de X , on a par définition

$$|X| = \varphi(n).$$

Par ailleurs, soit X' un système réduit modulo n . Tout élément de X' est congru à un unique élément de X modulo n . Deux éléments distincts de X' n'étant pas congrus modulo n , on en déduit l'existence d'une injection de X' dans X . Ainsi X' est fini de cardinal au plus celui de X . De même, on a $|X| \leq |X'|$, d'où le résultat.

Proposition 2.1. *Soient m et n des entiers naturels non nuls premiers entre eux. On a*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Démonstration : Soient X et Y des systèmes réduits modulo m et n respectivement. Posons

$$Z = \left\{ xn + ym \mid x \in X, y \in Y \right\}.$$

Vérifions que l'on a l'égalité

$$|Z| = \varphi(m)\varphi(n).$$

Soient x, x' (resp. y, y') des éléments de X (resp. de Y) tels que $xn + ym = x'n + y'm$. On a $n(x - x') = m(y' - y)$. Les entiers m et n étant premiers entre eux, n divise donc $y' - y$ et m divise $x - x'$ (th. 1.7, lemme de Gauss), d'où $x = x'$ et $y = y'$. On en déduit que l'on a $|Z| = |X||Y|$, d'où l'égalité annoncée (lemme 2.3).

Montrons que Z est un système réduit modulo mn , ce qui, d'après le lemme 2.3, établira l'assertion. Les éléments de Z sont premiers avec mn : si un nombre premier ℓ divise m (ou n) et $xn + ym$, avec $x \in X$ et $y \in Y$, alors ℓ divise x (ou y), ce qui n'est pas. Soit a un entier relatif premier avec mn . Vérifions que a est congru modulo mn à un élément de Z . D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$, d'où $(au)m + (av)n = a$. On a $\text{pgcd}(av, m) = 1$ et $\text{pgcd}(au, n) = 1$. Il existe donc $x \in X$ et $y \in Y$ tels que $av \equiv x \pmod{m}$ et $au \equiv y \pmod{n}$. On obtient $a \equiv xn + ym \pmod{mn}$ et notre assertion. Par ailleurs, le lemme de Gauss entraîne, comme ci-dessus, que deux éléments distincts de Z ne sont pas congrus modulo mn , d'où le résultat.

Démonstration du théorème 2.2 : On peut supposer $n \geq 2$. Soit $\{p_1, \dots, p_r\}$ l'ensemble des diviseurs premiers de n . Soit

$$n = \prod_{i=1}^r p_i^{n_i},$$

la décomposition en facteurs premiers de n . On a (prop. 2.1)

$$\varphi(n) = \prod_{i=1}^r \varphi(p_i^{n_i}).$$

Par ailleurs, on a (lemme 2.2)

$$\varphi(p_i^{n_i}) = p_i^{n_i} \left(1 - \frac{1}{p_i}\right),$$

d'où le résultat.

Corollaire 2.2. *Pour tout $n \geq 3$, l'entier $\varphi(n)$ est pair.*

Démonstration : D'après le théorème 2.2, on a

$$\varphi(n) = \prod_{p|n} p^{v_p(n)-1} (p-1),$$

où p parcourt l'ensemble des diviseurs premiers de n . Si n possède un diviseur premier impair p , alors $p-1$ est pair, et il en est donc de même de $\varphi(n)$. Si n est une puissance de 2, disons $n = 2^r$ avec $r \geq 2$, alors $\varphi(n) = 2^{r-1}$, d'où l'assertion.

Corollaire 2.3. Soient m et n deux entiers naturels non nuls tels que m divise n . Alors, $\varphi(m)$ divise $\varphi(n)$.

Démonstration : Soient P_m (resp. P_n) l'ensemble des diviseurs premiers de m (resp. de n). On a l'égalité (th. 2.2)

$$\frac{\varphi(n)}{\varphi(m)} = \frac{n}{m} \prod_{p \in P_n - P_m} \left(1 - \frac{1}{p}\right).$$

Par ailleurs, pour tout $p \in P_n - P_m$, p divise n sans diviser m , donc p divise n/m . Le second membre de cette égalité est donc un entier, d'où le résultat.

Remarquons que l'implication réciproque du corollaire 2.3 est fausse, comme le montre les égalités $\varphi(3) = \varphi(4) = 2$.

Lemme 2.4. Pour tout entier $n \geq 1$, on a

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

Démonstration : Considérons l'ensemble

$$F = \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n}, \frac{n}{n} = 1 \right\}.$$

Pour tout diviseur d de n , posons

$$F_d = \left\{ \frac{a}{d} \mid 1 \leq a \leq d \text{ et } \text{pgcd}(a, d) = 1 \right\}.$$

L'ensemble F est la réunion disjointe des F_d , où d parcourt l'ensemble des diviseurs (positifs) de n . En effet, tout élément de $\frac{a}{d} \in F_d$ s'écrit sous la forme $\frac{ka}{n}$ avec $kd = n$, qui appartient à F (car $a \leq d$), et inversement, chaque élément de F a un représentant irréductible dans l'un des F_d . Par ailleurs, si $\frac{a}{d} = \frac{a'}{d'}$ est dans $F_d \cap F_{d'}$, on a $d'a = a'd$, ce qui conduit à $a = a'$ et $d = d'$ car on a $\text{pgcd}(a, d) = \text{pgcd}(a', d') = 1$ (lemme de Gauss), d'où notre assertion, puis le résultat car le cardinal de F est n et que celui de F_d est $\varphi(d)$.

La fonction indicatrice d'Euler a suscité de nombreux travaux et il reste encore beaucoup de problèmes non résolus à son sujet⁴.

⁴ Citons-en deux : le problème de Lehmer. On a vu que si p premier, on a $\varphi(p) = p - 1$. En 1932, Lehmer, mathématicien américain (1905-1991), a posé la question suivante :

existe-t-il des entiers n composés tels que $\varphi(n)$ divise $n - 1$?

On conjecture que non. Soit $\omega(n)$ le nombre de diviseurs premiers de n . Lehmer a démontré que si un tel entier n existe, alors n est impair, sans facteurs carrés, et $\omega(n) \geq 7$. Ce résultat a été amélioré par la suite. Sans être exhaustif, signalons qu'il a été démontré en 1980, que pour un tel entier n , on a $n > 10^{20}$ et $\omega(n) \geq 14$. En fait, si $\varphi(n)$ divise $n - 1$, alors n est un nombre de Carmichael.

Voici une autre conjecture sur la fonction φ , qui a été énoncée par Carmichael en 1907, et qui n'est toujours pas élucidée : pour tout entier pair $n \geq 1$, il existe un entier $m \neq n$ tel que $\varphi(n) = \varphi(m)$ (si n est impair, on a $\varphi(n) = \varphi(2n)$ d'après la prop. 2.1).

4. Le théorème d'Euler

Il a été démontré par Euler en 1760 :

Théorème 2.3. *Soit n un entier ≥ 1 . Pour tout entier relatif a premier avec n , on a*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Démonstration : Elle est analogue à celle du théorème 2.1. On peut supposer $n \geq 2$. Posons $t = \varphi(n)$. Soit a un entier relatif premier avec n . Notons b_1, \dots, b_t les entiers premiers avec n compris entre 1 et n , et r_i le reste de la division euclidienne de ab_i par n . On a la congruence

$$\prod_{i=1}^t ab_i \equiv \prod_{i=1}^t r_i \pmod{n}.$$

Par ailleurs, les entiers ab_i étant premiers avec n , on a $\text{pgcd}(r_i, n) = 1$ et $1 \leq r_i \leq n$ (on a $r_i \neq 0$ car $n \geq 2$). Vérifions alors que l'on a

$$\{b_1, \dots, b_t\} = \{r_1, \dots, r_t\}.$$

Il suffit pour cela de montrer que si i et j sont distincts, on a $r_i \neq r_j$. Dans le cas contraire, on aurait $ab_i \equiv ab_j \pmod{n}$ i.e. n diviserait $a(b_i - b_j)$. Puisque a et n sont premiers entre eux, $b_i - b_j$ serait divisible par n , et l'on aurait $b_i = b_j$, d'où une contradiction. On en déduit les congruences

$$\prod_{i=1}^t ab_i \equiv \prod_{i=1}^t b_i \pmod{n} \quad \text{i.e.} \quad (a^t - 1) \prod_{i=1}^t b_i \equiv 0 \pmod{n}.$$

Puisque les b_i sont premiers avec n , il en est de même du produit des b_i . Le lemme de Gauss entraîne alors le résultat.

Exemples 2.3.

1) Vérifions que l'écriture décimale de 3^{1000} , qui possède quatre cent soixante dix huit chiffres, se termine par 01. Il s'agit de déterminer l'entier a compris entre 0 et 99 tel que $3^{1000} \equiv a \pmod{100}$. On a $\varphi(100) = 40$. D'après le théorème d'Euler, on obtient $3^{40} \equiv 1 \pmod{100}$. Puisque $1000 = 40 \times 25$, on a donc $3^{1000} \equiv 1 \pmod{100}$, d'où $a = 1$.

2) Vérifions que l'écriture décimale de 2^{1000} , qui possède trois cent deux chiffres, se termine par 76. Le raisonnement précédent ne s'applique pas directement (car 2 n'est pas premier avec 100). On a $2^{1000} \equiv 0 \pmod{4}$. L'idée est alors de déterminer la congruence de 2^{1000} modulo 25 et d'utiliser le théorème chinois. On a $2^{20} \equiv 1 \pmod{25}$ (théorème d'Euler), d'où $2^{1000} \equiv 1 \pmod{25}$. Il en résulte que $2^{1000} \equiv -24 \pmod{100}$ (cf. le théorème chinois), d'où l'assertion.

3) Pour tout entier $n \geq 1$ impair, on a $2^{n!} \equiv 1 \pmod{n}$. En effet, n étant impair, on a

$$2^{\varphi(n)} \equiv 1 \pmod{n}.$$

Par ailleurs, on a $\varphi(n) \leq n$, donc $\varphi(n)$ divise $n!$. On en déduit que $2^{\varphi(n)} - 1$ divise $2^{n!} - 1$ (si a et b sont des entiers naturels tels que a divise b , alors $2^a - 1$ divise $2^b - 1$), d'où le résultat.

Donnons une autre application du théorème d'Euler, en démontrant l'énoncé suivant, qui est dû au mathématicien Polonais Schinzel, né en 1937.

Proposition 2.2. *Soit k un entier relatif distinct de 1. Il existe une infinité d'entiers n tels que $2^{2^n} + k$ soit composé.*

Démonstration : On peut supposer k impair. Soit a un entier naturel. Il suffit de prouver l'existence d'un entier n tel que $2^{2^n} + k$ ne soit pas premier et que $2^{2^n} + k > a$. Puisque k est distinct de 1, il existe $s \in \mathbb{N}$ et un entier impair h tels que

$$k - 1 = 2^s h.$$

Soit t un entier naturel tel que l'on ait

$$p = 2^{2^t} + k > a \quad \text{et} \quad t > s.$$

On peut supposer que p est un nombre premier. Il existe un entier impair h_1 tel que

$$p - 1 = 2^s h_1.$$

D'après le théorème d'Euler, on a

$$2^{\varphi(h_1)} \equiv 1 \pmod{h_1},$$

d'où l'on déduit la congruence

$$2^{s+\varphi(h_1)} \equiv 2^s \pmod{p-1}.$$

Puisque l'on a $t > s$, on obtient

$$2^{t+\varphi(h_1)} \equiv 2^t \pmod{p-1}.$$

L'entier p étant premier impair, on a $2^{p-1} \equiv 1 \pmod{p}$. Il en résulte que

$$2^{2^{t+\varphi(h_1)}} + k \equiv 0 \pmod{p}.$$

L'entier $2^{2^{t+\varphi(h_1)}} + k$, qui est strictement plus grand que p , n'est donc pas premier. Il est plus grand que a , d'où le résultat.

Nombres de Fermat. On conjecture que cet énoncé est vrai si $k = 1$, mais on ne sait pas le démontrer. C'est un problème qui remonte à Fermat. Étant donné $n \in \mathbb{N}$, l'entier

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

s'appelle un nombre de Fermat. Pour $n \leq 4$, les F_n sont premiers. Fermat avait alors conjecturé qu'ils le sont tous. Euler donna un contre-exemple pour $n = 5$, en montrant que F_5 est divisible par 641. Pour le vérifier, on peut remarquer que l'on a

$$641 = 2^4 + 5^4 = 5 \times 2^7 + 1.$$

On en déduit que

$$5^4 \times 2^{28} \equiv 1 \pmod{641},$$

d'où $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$. En fait, les seuls nombres premiers de Fermat connus sont les F_n pour $n \leq 4$, et on conjecture qu'il n'y en a qu'un nombre fini.

Remarquons que les nombres de Fermat apparaissent naturellement dans l'étude de la primalité des entiers de la forme $2^n + 1$, car on a l'implication

$$2^n + 1 \text{ est premier} \implies n \text{ est une puissance de } 2.$$

En effet, supposons $2^n + 1$ premier. Posons $n = 2^r d$ où d est impair. Parce que d est impair, -1 est racine du polynôme $X^d + 1$, donc $X + 1$ divise $X^d + 1$, par suite $2^{2^r} + 1$ divise $2^n + 1$. On a $2^{2^r} + 1 > 1$, d'où $2^n + 1 = 2^{2^r} + 1$, puis $n = 2^r$.

5. L'ordre multiplicatif modulo n d'un entier premier avec n

Soit n un entier naturel non nul.

Lemme 2.5. *Soit a un entier relatif premier avec n . Il existe un plus petit entier $d \geq 1$ tel que l'on ait $a^d \equiv 1 \pmod{n}$.*

Démonstration : D'après le théorème d'Euler, il existe une puissance au moins égale à 1 de a qui est congrue à 1 modulo n (th. 2.3). On en déduit l'assertion, car toute partie non vide de \mathbb{N} possède un plus petit élément.

Définition 2.2. *Soit a un entier relatif premier avec n . Le plus petit entier $d \geq 1$ tel que l'on ait $a^d \equiv 1 \pmod{n}$ s'appelle l'ordre multiplicatif de a modulo n .*

Lemme 2.6. *Soit a un entier relatif premier avec n , d'ordre multiplicatif d modulo n . Soit k un entier ≥ 1 . On a l'équivalence*

$$a^k \equiv 1 \pmod{n} \iff d \text{ divise } k.$$

En particulier, d divise $\varphi(n)$.

Démonstration : Supposons $a^k \equiv 1 \pmod{n}$. Il existe des entiers q et r tels que l'on ait $k = dq + r$ avec $0 \leq r \leq d - 1$. On a $a^d \equiv 1 \pmod{n}$. Il en résulte que l'on a $a^r \equiv 1 \pmod{n}$. D'après le caractère minimal de d , cela implique $r = 0$ donc d divise k . Inversement, il existe $s \in \mathbb{N}$ tel que $k = sd$. On a ainsi $a^k = (a^d)^s \equiv 1 \pmod{n}$, d'où l'équivalence annoncée, puis le résultat (th. 2.3).

Exemples 2.4.

1) Soit p un nombre premier. Pour tout entier relatif a , non divisible par p , on a la congruence $a^{p-1} \equiv 1 \pmod{p}$. Par suite, l'ordre multiplicatif de a modulo p divise $p - 1$.

2) L'ordre multiplicatif de 2 modulo 17, qui divise 16, est 8. En effet, 1, 2, 4 ne sont pas congrus à 1 modulo 17 et on a $2^4 \equiv -1 \pmod{17}$, d'où $2^8 \equiv 1 \pmod{17}$.

3) Soit d l'ordre multiplicatif de 2 modulo 19. Vérifions que l'on a $d = 18$. Tout d'abord, d divise $\varphi(19) = 18$. On a donc $d \in \{1, 2, 3, 6, 9, 18\}$. Visiblement, d n'est pas 1, 2 ni 3. On a $2^6 = 64 \equiv 7 \pmod{19}$ et $2^9 \equiv -1 \pmod{19}$. Ainsi, 2^6 et 2^9 ne sont pas congrus à 1 modulo 19, d'où $d = 18$.

4) Démontrons qu'il n'existe pas d'entiers $n \geq 2$ tels que n divise $2^n - 1$. Supposons qu'il existe un tel entier n et considérons le plus petit diviseur premier p de n . Soit d l'ordre multiplicatif de 2 modulo p . On a $2^n \equiv 1 \pmod{p}$. Parce que p est impair, on a $2^{p-1} \equiv 1 \pmod{p}$. Ainsi d divise n et $p - 1$ (lemme 2.6). Le caractère minimal de p implique alors $d = 1$: si on a $d \geq 2$, il existe un nombre premier ℓ divisant d ; on a alors $\ell < p$ et ℓ divise n , d'où une contradiction et l'assertion.

Remarques 2.2.

1) On peut démontrer, et c'est un résultat essentiel, que pour tout nombre premier p , il existe un entier a compris entre 1 et p tel que l'ordre multiplicatif de a modulo p soit exactement $p - 1$. On l'admettra ici. Un tel entier a s'appelle un générateur modulo p .

2) On conjecture qu'il existe une infinité de nombres premiers p tels que 2 soit un générateur modulo p . Cette conjecture a été formulée par Emil Artin vers 1925, mathématicien américain qui vécut de 1898 à 1962. Par exemple, il en est ainsi des nombres premiers

$$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, \dots$$

Voici une caractérisation de l'ordre multiplicatif d'un entier.

Lemme 2.7. Soient n un entier ≥ 1 et $a \in \mathbb{Z}$ premier avec n . Soit r un entier ≥ 1 . Les conditions suivantes sont équivalentes :

1) l'ordre multiplicatif de a modulo n est r .

2) On a $a^r \equiv 1 \pmod{n}$, et pour tout diviseur premier p de r on a $a^{\frac{r}{p}} \not\equiv 1 \pmod{n}$.

Démonstration : Le fait que la première condition entraîne la seconde est une conséquence de la définition. Inversement, supposons la condition 2 réalisée. Notons d l'ordre multiplicatif de a modulo n . Il existe $k \geq 1$ tel que l'on ait $r = kd$. Supposons $k \geq 2$. Soit p un diviseur premier de k . On a alors les égalités

$$a^{\frac{r}{p}} = (a^d)^{\frac{k}{p}} \equiv 1 \pmod{n},$$

ce qui contredit l'hypothèse faite. On a donc $k = 1$, puis $r = d$.

Application (Critères de primalité)

1) Établissons un critère de primalité, concernant en pratique les entiers n pour lesquels on connaît les diviseurs premiers de $n - 1$. Ce type de critères a été étudié par Lehmer.

Proposition 2.3. Soit n un entier ≥ 2 . Supposons qu'il existe $a \in \mathbb{Z}$ tel que les deux conditions suivantes soient satisfaites :

1) on a $a^{n-1} \equiv 1 \pmod{n}$

2) On a $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ pour tout diviseur premier q de $n - 1$.

Alors, n est premier.

Démonstration : La congruence $a^{n-1} \equiv 1 \pmod{n}$ entraîne que a est premier avec n . Il résulte alors du lemme 2.7 que l'ordre de a modulo n est $n - 1$. Par suite, $n - 1$ divise $\varphi(n)$. On a donc les inégalités $n - 1 \leq \varphi(n) < n$, d'où $\varphi(n) = n - 1$, et le fait que n soit premier (si n n'était pas premier, il posséderait un diviseur autre que 1 et lui-même, et l'on aurait $\varphi(n) < n - 1$).

Exemple 2.5. Ce critère, utilisé avec $a = 5$, permet de démontrer, en moins d'une seconde sur machine, que l'entier

$$3 \times 2^{3189} + 1$$

est premier. Il possède neuf cent soixante et un chiffres dans son écriture décimale.

2) Voyons un autre critère de primalité permettant de démontrer l'équivalence (7) comme annoncé.

Proposition 2.4. Soient p un nombre premier et h un entier naturel strictement plus petit que p . Posons $n = hp + 1$ et supposons $2^h \not\equiv 1 \pmod{n}$. Alors, on a l'équivalence

$$n \text{ est premier} \iff 2^{n-1} \equiv 1 \pmod{n}.$$

Démonstration : Supposons n premier. L'égalité $n = hp + 1$ entraîne en particulier que n est impair, d'où $2^{n-1} \equiv 1 \pmod{n}$.

Inversement, supposons $2^{n-1} \equiv 1 \pmod{n}$. L'entier n est impair. Soit d l'ordre multiplicatif de 2 modulo n . Il divise $n-1 = hp$. La condition $2^h \not\equiv 1 \pmod{n}$ entraîne que d ne divise pas h . Par suite, p divise d (si p ne divisait pas d , d et p seraient premiers entre eux et d'après le lemme de Gauss, d devrait diviser h). Puisque d divise $\varphi(n)$, il en résulte que p divise $\phi(n)$. Soit

$$n = p_1^{n_1} \cdots p_r^{n_r}$$

la décomposition de n en facteurs premiers. On a (th. 2.2)

$$\varphi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1} (p_1 - 1) \cdots (p_r - 1).$$

Parce que p ne divise pas n , il existe donc i tel que $p_i \equiv 1 \pmod{p}$. Posons $n = p_i m$. On a $m \equiv 1 \pmod{p}$ car tel est le cas de p_i et n . Vérifions que $m = 1$, ce qui prouvera le résultat. Posons $p_i = up + 1$ et $m = vp + 1$ où $u, v \in \mathbb{N}$. On a alors $hp + 1 = (up + 1)(vp + 1)$, d'où $h = uvp + u + v$. L'inégalité $h < p$ entraîne alors $v = 0$. On obtient $m = 1$, d'où $n = p_i$ et le fait que n soit premier.

L'équivalence (7) s'en déduit en utilisant cet énoncé avec $h = 2$.

6. Nombres de Mersenne

Marin Mersenne était un moine français qui vécut de 1588 à 1648. Il resta célèbre, entre autres, pour l'étude des entiers

$$M_p = 2^p - 1,$$

où p est un nombre premier. L'objectif de ce paragraphe est d'en décrire quelques propriétés et de présenter certaines questions les concernant.

6.1. Définition - Premières propriétés

Définition 2.3. *Un nombre de Mersenne est un entier M_p avec p premier.*

Lemme 2.8. *Pour tout entier $n \geq 1$, si $2^n - 1$ est premier alors n l'est aussi. L'implication réciproque est fausse.*

Démonstration : Si n n'est pas premier, il possède un diviseur a tel que $1 < a < n$. L'entier $2^a - 1$ est donc un diviseur strict de $2^n - 1$ qui n'est donc pas premier. L'implication réciproque, qui en termes de quantificateurs s'écrit

$$\forall p \geq 1 \quad (p \text{ premier} \implies M_p \text{ premier}),$$

est fausse, car il existe un nombre premier p tel que M_p ne le soit pas, comme on le constate avec l'égalité

$$M_{11} = 23 \times 89.$$

Lemme 2.9. *Pour tous nombres premiers p et q distincts, les entiers M_p et M_q sont premiers entre eux.*

Démonstration : Il suffit de démontrer plus généralement que si a et b sont deux entiers naturels non nuls, en posant $d = \text{pgcd}(a, b)$, on a

$$\text{pgcd}(2^a - 1, 2^b - 1) = 2^d - 1.$$

On peut utiliser l'exercice 6 du chapitre I, ou bien le vérifier avec l'algorithme d'Euclide. En effet, il existe s et r dans \mathbb{N} tels que l'on ait $a = bs + r$ avec $0 \leq r < b$. On a les égalités

$$2^a - 1 = (2^b)^s 2^r - 1 = ((2^b)^s - 1)2^r + (2^r - 1).$$

Par ailleurs, $2^b - 1$ divise $(2^b)^s - 1$. Il existe donc $t \in \mathbb{N}$ tel que l'on ait

$$2^a - 1 = (2^b - 1)t + 2^r - 1.$$

On a $0 \leq 2^r - 1 < 2^b - 1$ donc $2^r - 1$ est le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$. Puisque d est le dernier reste non nul dans l'algorithme d'Euclide de division de a par b , il en résulte que $2^d - 1$ est le dernier reste non nul dans l'algorithme d'Euclide de division de $2^a - 1$ par $2^b - 1$, d'où le lemme.

6.2. Lien avec les nombres parfaits

Définition 2.4. *Un entier $n \geq 2$ est dit parfait s'il est la somme de ses diviseurs d tels que $1 \leq d < n$.*

Leur étude remonte à Euclide.

Exemple 2.6. Les entiers 6, 28, 496 et $8128 = 2^6 M_7$ sont parfaits. Ce sont les seuls plus petits que 10000.

Remarque 2.3. On ne sait pas s'il existe une infinité de nombres parfaits, ni s'il en existe qui soient impairs. S'il existe des nombres parfaits impairs, il sont plus grands que 10^{300} .

Notation. Pour tout entier $n \geq 1$, notons $\sigma(n)$ la somme de ses diviseurs.

Lemme 2.10. *Un entier $n \geq 1$ est parfait si et seulement si on a $\sigma(n) = 2n$.*

Démonstration : On le constate en utilisant l'égalité

$$\sigma(n) = n + \sum_{d|n, d \neq n} d.$$

Le lien entre les nombres de Mersenne et les nombres parfaits apparaît dans l'énoncé suivant.

Proposition 2.5. *Soit $n \geq 2$ un entier pair. Alors, n est parfait si et seulement si il existe un entier $p \geq 1$ tel que l'on ait*

$$n = 2^{p-1}M_p \quad \text{avec } M_p \text{ premier.}$$

Démonstration : Supposons que n soit de la forme indiquée. La somme de ses diviseurs, autres que lui même, est alors

$$(1 + 2 + \cdots + 2^{p-1}) + (1 + 2 + \cdots + 2^{p-2})M_p = M_p + (2^{p-1} - 1)M_p = 2^{p-1}M_p,$$

donc n est parfait. Euclide avait démontré cette implication.

Inversement, supposons n parfait. Posons $n = 2^{r-1}m$ où m est impair et $r \geq 2$. On a⁵

$$2^r m = 2n = \sigma(n) = \sigma(2^{r-1})\sigma(m) = (2^r - 1)\sigma(m).$$

La valuation 2-adique de $\sigma(m)$ est donc r et il existe c tel que $\sigma(m) = 2^r c$. Par suite, on a $m = (2^r - 1)c$. Ainsi m et c sont des diviseurs de m et on a

$$m + c = 2^r c = \sigma(m).$$

Il en résulte que m et c sont les seuls diviseurs positifs de m . On en déduit que m est premier et que $c = 1$. On obtient $m = 2^r - 1$, d'où $n = 2^{r-1}M_r$ où M_r est premier. Cette implication est due à Euler.

⁵ La fonction σ est multiplicative, autrement dit, si m et n sont premiers entre eux, on a $\sigma(mn) = \sigma(m)\sigma(n)$. En effet, pour tout $a \geq 1$, soit D_a l'ensemble des diviseurs positifs de a . Si n et m sont premiers entre eux, l'application $(d_1, d_2) \mapsto d_1 d_2$ est une bijection de $D_m \times D_n$ sur D_{mn} . Ainsi

$$\sigma(m)\sigma(n) = \sum_{d_i \in D_m} d_i \sum_{d_j \in D_n} d_j = \sum_{d \in D_{mn}} d = \sigma(mn).$$

En particulier, $\sigma(n)$ s'exprime directement à partir de la décomposition en nombres premiers de n . En effet, si $n = p_1^{n_1} \cdots p_r^{n_r}$ est la décomposition de n en facteurs premiers, on a les égalités

$$\sigma(n) = \sigma(p_1^{n_1}) \cdots \sigma(p_r^{n_r}) = (1 + p_1 + \cdots + p_1^{n_1}) \cdots (1 + p_r + \cdots + p_r^{n_r}),$$

autrement dit, on a

$$\sigma(n) = \prod_{i=1}^r \left(\frac{p_i^{n_i+1} - 1}{p_i - 1} \right).$$

La connaissance des nombres parfaits pairs est donc équivalente à celle des nombres de Mersenne premiers. Notons que tout nombre parfait pair est triangulaire i.e. est de la forme $\frac{k(k+1)}{2}$ pour un entier k convenable : on a l'égalité

$$2^{p-1}M_p = \frac{M_p(M_p + 1)}{2}.$$

Corollaire 2.4. *Le dernier chiffre décimal d'un entier pair parfait est 6 ou 8.*

Démonstration : Soit n un entier pair parfait. Il existe un nombre premier p tel que $n = 2^{p-1}M_p$. Si $p = 2$, on a $n = 6$. Supposons $p \equiv 1 \pmod{4}$. Posons $p = 4k + 1$. On a alors

$$n = 16^k(2 \cdot 16^k - 1).$$

Le dernier chiffre de 16^k est 6 et celui de $2 \cdot 16^k - 1$ est 1, donc le dernier chiffre de n est 6. Si on a $p \equiv 3 \pmod{4}$, posons $p = 3 + 4k$. On a

$$n = 4 \cdot 16^k(8 \cdot 16^k - 1).$$

Le dernier chiffre de $4 \cdot 16^k$ est 4 et celui de $8 \cdot 16^k - 1$ est 7, le dernier chiffre de n est donc 8.

Tout entier de la forme $2^{p-1}M_p$, avec $p \in \mathbb{N}$ impair, peut s'écrire comme une somme de $2^{\frac{p-1}{2}}$ cubes de nombres impairs. En particulier, tel est le cas des nombres parfaits pairs. Plus précisément :

Proposition 2.6. *Soit p un entier naturel impair. On a*

$$2^{p-1}M_p = 1^3 + 3^3 + \cdots + (2m-1)^3 \quad \text{avec} \quad m = 2^{\frac{p-1}{2}}.$$

Démonstration : On a

$$\sum_{k=1}^m (2k-1)^3 = \sum_{k=1}^m (8k^3 - 12k^2 + 6k - 1) = 8 \sum_{k=1}^m k^3 - 12 \sum_{k=1}^m k^2 - 6 \sum_{k=1}^m k - m.$$

On peut vérifier par récurrence que l'on a

$$\sum_{k=1}^m k = \frac{m(m+1)}{2}, \quad \sum_{k=1}^m k^2 = \frac{m(m+1)(2m+1)}{6}, \quad \sum_{k=1}^m k^3 = \frac{m^2(m+1)^2}{4}.$$

Il en résulte les égalités

$$\sum_{k=1}^m (2k-1)^3 = m^2(2m^2 - 1) = 2^{p-1}M_p.$$

6.3. Un test de non primalité

L'énoncé qui suit permet parfois d'établir qu'un nombre de Mersenne est composé.

Proposition 2.7. *Soit p un nombre premier congru à 3 modulo 4. On a l'équivalence*

$$2p + 1 \text{ est premier} \iff 2p + 1 \text{ divise } M_p.$$

Démonstration : Posons $n = 2p + 1$. Supposons que n divise M_p . On a alors

$$2^{n-1} = 2^{2p} \equiv 1 \pmod{n}.$$

La proposition 2.4, utilisée avec $h = 2$, entraîne que n est premier. Inversement, supposons n premier. On a $p \equiv 3 \pmod{4}$, d'où $n \equiv 7 \pmod{8}$. Il résulte alors de la congruence (8) ci-dessous⁶, que l'on a

$$2^{\frac{n-1}{2}} \equiv 1 \pmod{n},$$

autrement dit que n divise M_p .

⁶ Soit ℓ un nombre premier congru à 3 modulo 4. Démontrons que l'on a

$$(8) \quad 2^{\frac{\ell-1}{2}} \equiv (-1)^{\frac{\ell+1}{4}} \pmod{\ell}.$$

Il existe $k \in \mathbb{N}$ tel que $\ell = 3 + 4k$. Posons $M = 2^{2k+1}(2k+1)!$. On a

$$M = \prod_{i=1}^{2k+1} (2i) = \prod_{i=1}^k (2i) \prod_{i=1}^{k+1} (2k+2i).$$

Par ailleurs, on a $2k+2i \equiv -(2k+3-2i) \pmod{\ell}$, d'où la congruence

$$\prod_{i=1}^{k+1} (2k+2i) \equiv (-1)^{k+1} \prod_{i=1}^{k+1} (2k+3-2i) \pmod{\ell}.$$

De l'égalité

$$\prod_{i=1}^k (2i) \prod_{i=1}^{k+1} (2k+3-2i) = (2k+1)!,$$

on déduit alors que l'on a

$$M \equiv (-1)^{k+1} (2k+1)! \pmod{\ell}.$$

On a $2k+1 = \frac{\ell-1}{2}$, donc $(2k+1)!$ n'est pas divisible par ℓ , d'où

$$2^{2k+1} \equiv (-1)^{k+1} \pmod{\ell},$$

puis la congruence (8).

Exemple 2.7. Le résultat précédent permet d'expliciter des «grands» nombres premiers p pour lesquels M_p est composé. À titre indicatif, tel est le cas de $M_{999999191}$.

Étant donné un nombre premier p tel que M_p soit composé, un problème naturel qui se pose est de déterminer ses diviseurs premiers. C'est un problème très difficile, comme d'ailleurs en général le problème de la factorisation des entiers. On dispose néanmoins de l'information suivante.

Lemme 2.11. *Soit p un nombre premier. Les facteurs premiers de M_p sont congrus à 1 modulo p . En particulier, si $p \neq 2$, ils sont congrus à 1 modulo $2p$.*

Démonstration : Soit q un diviseur premier de M_p . On a $2^p \equiv 1 \pmod{q}$. Par suite, p est l'ordre multiplicatif de 2 modulo q . On a $2^{q-1} \equiv 1 \pmod{q}$, donc p divise $q-1$. De plus, si $p \neq 2$, alors $2p$ divise $q-1$ (car $q-1$ est pair).

Remarque 2.4. Ce lemme apporte une aide très relative pour factoriser un nombre de Mersenne. Par exemple, la décomposition de M_{67} en facteurs premiers est donnée par l'égalité

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

et il y a 162904 nombres premiers plus petits que 193707721 congrus à 1 modulo 67. Pour autant, Cole a annoncé en 1903 cette factorisation lors d'un congrès de la société mathématique américaine. Il l'avait obtenue en calculant «à la main» tous les dimanches pendant trois ans. La factorisation de M_{67} est aujourd'hui instantanée sur machine, indépendamment du lemme 2.11.

Exemple 2.8. Il n'existe pas de nombres de Mersenne divisibles par 5, 11, 13 ou 17.

6.4. Un critère de primalité

On connaît «beaucoup» de nombres premiers de Mersenne M_p , en fait quarante neuf,

$$M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, \dots, M_{23209}, \dots, M_{44497}, \dots$$

Le dernier a été découvert en septembre 2015, avec

$$p = 74207281.$$

C'est le plus grand nombre premier connu. Il possède 22338618 chiffres décimaux. Les grands nombres premiers de Mersenne ont été détectés en utilisant un critère de primalité, établi par Lucas⁷ en 1878, qui leur est spécifique.

Théorème 2.4 (Test de Lucas). *Soit $(L_i)_{i \geq 1}$ la suite d'entiers définie par les égalités*

$$L_1 = 4 \quad \text{et} \quad L_{i+1} = L_i^2 - 2.$$

Pour tout nombre premier $p \geq 3$, on a l'équivalence

$$M_p \text{ est premier} \iff L_{p-1} \equiv 0 \pmod{M_p}.$$

Nous admettrons ce résultat. Il peut se démontrer simplement dans un cours de quatrième année d'université.

Exemple 2.9. On peut vérifier facilement sur machine avec ce test que M_{23209} est premier. Il a 6987 chiffres. Avec un MacBook Pro, le temps nécessaire à cette vérification est de l'ordre de la minute. De même, M_{44497} est premier. Il a 13395 chiffres et le temps d'exécution du test est d'environ huit minutes. Le fait que ces deux nombres de Mersenne soient premiers a été découvert en 1979.

6.5. Questions ouvertes célèbres

Question 1. Existe-t-il une infinité de nombres de Mersenne premiers ?

Question 2. Existe-t-il une infinité de nombres de Mersenne composés ?

Question 3. Tout nombre de Mersenne est-il sans facteurs carrés ?

Les méthodes actuelles pour aborder ces questions semblent inefficaces. On conjecture que la réponse aux questions 1 et 2 est positive. Il est peut-être moins clair d'avoir une conviction pour la question 3. Heuristiquement, pour x assez grand, le nombre des nombres premiers de Mersenne plus petits que x est de l'ordre de

$$\frac{e^\gamma}{\log 2} \log \log x,$$

où γ est la constante d'Euler, définie comme étant la limite de la suite de terme général

$$\sum_{k=1}^n \frac{1}{k} - \log n.$$

⁷ Édouard Lucas était un mathématicien français qui vécut de 1842 à 1891. Il resta célèbre pour ses travaux en théorie des nombres, en particulier pour l'étude des suites qui portent son nom : soit a un entier relatif. La suite d'entiers $(V_k)_{k \in \mathbb{N}}$ définie par les égalités

$$V_0 = 2, \quad V_1 = a \quad \text{et} \quad V_{k+1} = aV_k - V_{k-1} \quad \text{pour tout } k \geq 1,$$

est appelée suite de Lucas associée à l'entier a . Elle intervient dans les tests de primalité concernant les entiers n pour lesquels on connaît les diviseurs premiers de $n+1$ (typiquement, les nombres de Mersenne).

Signalons que l'on a $\gamma \simeq 0,577215\dots$.

En ce qui concerne la question 2, l'expérimentation numérique à elle seule rend plausible l'existence d'une infinité de nombres de Mersenne composés. Pour le démontrer, «il suffirait» d'établir l'existence d'une infinité de nombres premiers p congrus à 3 modulo 4 tels que $2p + 1$ soit premier (prop. 2.7). Signalons dans cette direction l'énoncé suivant, établi par Powell en 1983.

Proposition 2.8. *Soit k un entier > 1 . Il existe une infinité de nombres premiers p tels que $2^p - k$ soit composé.*

Démonstration partielle : Elle utilise le fait que pour tout entier $n \geq 1$, il existe une infinité de nombres premiers congrus à 1 modulo n . La démonstration de cette assertion nous entraînerait trop loin. C'est un cas particulier du théorème de la progression arithmétique de Dirichlet que l'on a admis (voir le chapitre I), mais qui est néanmoins beaucoup plus simple à établir.

On peut supposer k impair, ce n'est pas restrictif. Supposons $k > 3$. On a $k - 2 \geq 2$, donc il existe un diviseur premier $q \neq 2$ de $k - 2$. On a $2^{q-1} \equiv 1 \pmod{q}$. Pour tout nombre premier $p \equiv 1 \pmod{q-1}$, on a ainsi

$$2^p - k \equiv 2 - k \equiv 0 \pmod{q}.$$

Parce qu'il existe une infinité de tels nombres premiers p , on obtient le résultat dans ce cas. Supposons $k = 3$. Pour tout nombre premier $p \equiv 3 \pmod{4}$, on a $2^p - 3 \equiv 0 \pmod{5}$, d'où le résultat.

À propos de la question 3, il semble que le seul résultat connu soit le suivant :

Lemme 2.12. *Soient p et q des nombres premiers. Si p^2 divise M_q , on a*

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Démonstration : Il existe un entier k tel que $p = 2kq + 1$ (lemme 2.11). On a donc

$$2^{\frac{p-1}{2k}} = 2^q \equiv 1 \pmod{p^2},$$

ce qui implique la congruence annoncée.

Les seuls nombres premiers p connus pour lesquels on a $2^{p-1} \equiv 1 \pmod{p^2}$ sont

$$1093 \quad \text{et} \quad 3511,$$

découverts il y a environ un siècle. On sait qu'il n'y en a pas d'autres plus petits que 10^{15} . On ne sait pas s'il en existe une infinité, ni d'ailleurs s'il existe une infinité de p premiers

tels que $2^{p-1} \not\equiv 1 \pmod{p^2}$. On conjecture en fait qu'il y en a une infinité dans les deux cas. Cela étant :

Corollaire 2.5. *L'une des deux assertions suivantes est vraie :*

- 1) *il n'existe qu'un nombre fini de nombres de Mersenne divisibles par le carré d'un nombre premier.*
- 2) *Il existe une infinité de nombres premiers p tels que $2^{p-1} \equiv 1 \pmod{p^2}$.*

Démonstration : Cela résulte du lemme 2.12 et du fait que deux nombres de Mersenne distincts sont premiers entre eux (lemme 2.9).