SUR DIVERS PROCÉDÉS DE FACTORISATION

Autor(en): **Aubry, A.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **15 (1913)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-14857

SUR DIVERS PROCÉDÉS DE FACTORISATION[1]

Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resoluendi, ad gravissima ac utilissima arithmeticæ pertinere.

GAUSS.

Reconnaître si un nombre donné quelconque a est divisible par un autre nombre donné b est chose facile : on n'a qu'à effectuer la division de a par b. Même si a n'est pas donné explicitement, la chose est encore possible, en faisant appel à la théorie des congruences[2], d'après un procédé dû en principe à Euler.

La question inverse : *déterminer les nombres divisant un nombre donné*, c'est-à-dire résoudre l'équation $xy = n$, est au contraire d'une difficulté telle que, — sauf pour les nombres qu'on peut mettre sous certaines formes spéciales, — elle n'est pratiquement soluble que pour des nombres n'ayant guère plus de dix ou douze chiffres ; et encore les calculs qu'elle nécessite sont-ils alors d'une effrayante prolixité. D'après une assertion de Gauss, il ne faut pas se flatter de trouver une méthode dont la difficulté d'application ne croisse pas beaucoup plus rapidement que le nombre des chiffres à *factoriser*.

---

[1] Depuis une quinzaine d'années, on appelle ainsi, d'après les arithméticiens anglais, la décomposition d'un nombre entier en ses facteurs premiers.

[2] Ainsi *soit à trouver le reste de la division de* 2^{35} *par* 31867 : on a, suivant le module 31867,

$$2^{15} \equiv 32768 \equiv 901 \ , \qquad 2^{30} \equiv 901^2 \equiv 15126 \ , \qquad 2^{35} \equiv 15126 \cdot 32 \equiv 6027 \ .$$

On démontre de même que $7^{160} + 1$ est divisible par 641 (Euler, voir *Ens. math.*, 1907, p. 437), que $3^{1000} - 3$ l'est par 13 (Gauss, *id.*), que $189^{n+1} - 189^n + 189^{n-6}$ l'est par 191 (Desmarets, *id.*), que $2^{2^{36}} + 1$ l'est par 2 748 779 069 441 (Seelhof).

Certaines identités algébriques fournissent très simplement une infinité de résultats de ce genre. Ainsi on connaît la factorisation algébrique des expressions $a^n - b^n$, $a^{2n+1} + b^{2n+1}$, $a^4 + 4b^4$: *tout nombre de cette dernière forme est composé et égal au produit des deux suivants* $a^2 \pm 2ab + 2b^2$ (Euler) ; d'où trois théorèmes dus à Goldbach, Sophie Germain et Aurifeuille, en faisant

$$a = 1 \ ; \qquad b = 1 \ ; \qquad a = 1 \ , \quad b = 2^n \ .$$

Ed. Lucas et le lieut.-col. Cunningham entre autres, ont fait de nombreuses recherches sur ce genre de formules algébriquement décomposables.

La connaissance d'expressions jouissant de cette propriété est du reste extrêmement utile : pour factoriser un nombre donné, on cherche d'abord à le diviser par les plus petits nombres premiers, 3, 5, 7, 11, 13, ... ; on s'assure, par le calcul ou au moyen de tables, qu'il n'est ni carré, ni cube, ni triangulaire ; et on essaie ensuite de le mettre sous la forme d'une de ces expressions décomposables, ce qui — si on réussit — évite de longs calculs.

Les Anciens s'étaient probablement posé ce problème, mais sans aboutir jusqu'à Euclide, à d'autres résultats que la connaissance de certaines propriétés des nombres premiers. Peu après lui cependant, un pas important fut fait dans cette voie, l'invention du *crible d'Eratosthène.*

Les Indiens et les Arabes ont dû également s'en occuper; toutefois c'est dans Fibonacci qu'on voit, pour la première fois (1202), cette règle toute théorique d'*essayer la division du nombre à factoriser par tous les nombres premiers inférieurs à sa racine carrée*[1].

C'est seulement avec les Modernes qu'on est arrivé à reculer la limite des nombres qui peuvent être factorisés. A Frénicle paraît

---

[1] Les divisions à effectuer peuvent être facilitées par les considérations qui suivent :

Il y a avantage à commencer les essais en partant de la limite $\sqrt{n}$. En effet, soit $n = pa + r$; si un diviseur q de r ne divise pas a, il sera inutile d'essayer la division par q (E. Lebon). Ainsi $4171 = 68.61 + 23$: il est donc inutile de diviser par 23.

Si le quotient n'a pas plus de quatre ou cinq chiffres, on peut, avec Ed. Lucas, se servir d'une table de logarithmes à sept décimales.

Si le nombre à factoriser se termine à droite, par exemple par 7, les deux facteurs de ce nombre sont terminés l'un par 7 et l'autre par 1, ou bien l'un par 3 et l'autre par 9. On mettra sur une ligne les nombres premiers décroissants à partir de $\sqrt{n}$ et sur une deuxième ligne, les nombres croissants également à partir de $\sqrt{n}$ et qui, multipliés par leurs correspondants de la première ligne, paraissent devoir produire le nombre n. Ainsi soit le nombre $n = 4171$; on considère les couples

$$61.71\ ,\quad 59.69\ \text{ou}\ 59.79\ ,\quad 53.77\ ,\quad 47.93\ ,\quad 43.87\ \text{ou}\ 43.97\ ,\ \ldots$$

La preuve par 9 fait voir que $n \equiv 4 \pmod 9$; par l'addition des chiffres des différents couples, on voit qu'on peut se borner à essayer seulement les produits 53.77, 43.97, ... dont le deuxième réussit. Ainsi n se trouve décomposé en ses facteurs 43 et 97.

Si α *et* β *représentent les restes de la division de* a *et de* b *par* p, *celui de* $a^2 + b$ *divisé par* p *est congru à* $\alpha^2 + \beta$.

Soit $n = a^2 + b$: *cherchons le nombre impair* x *tel que* $\dfrac{ax + b}{a - x}$ *soit entier :* n *est divisible par* $a - x$. Par exemple, faisant $a = 14$, $b = 1$ et $x = 1, 3, 5, 7, 9, 11$; la formule qui précède prend les valeurs

$$\frac{15}{13}\ ,\quad \frac{43}{11}\ ,\quad \frac{71}{9}\ ,\quad \frac{99}{7}\ ,\quad \frac{127}{5}\ ,\quad \frac{155}{3}\ ,$$

dont aucune n'est entière : le nombre $14^2 + 1$ est donc premier.

Si n *est composé et* $p < E\sqrt{n}$, *l'un des nombres* $\dfrac{n-9}{3}$, $\dfrac{n-25}{5}$, $\dfrac{n-49}{7}$, $\dfrac{n-121}{11}$, $\dfrac{n-169}{13}$, ... $\dfrac{n-p^2}{p}$ *est entier : sinon* n *est premier.* Ainsi aucun des nombres $\dfrac{188}{3}$, $\dfrac{172}{5}$, $\dfrac{148}{7}$, $\dfrac{76}{11}$, $\dfrac{28}{13}$ n'est entier; donc 197 est premier.

Voici un autre procédé dû à M. E. Lebon : *soit* $n = a^2 + b$; *si aucun des nombres* $\dfrac{(a-3)^2+b}{3}$, $\dfrac{(a-5)^2+b}{5}$, $\dfrac{(a-7)^2+b}{7}$, ... *n'est entier,* n *est premier.* On peut l'appliquer à $n = 14^2 + 1$.

M. Barbette (*Les p^es puis.*, Liège, 1910), a remarqué que la question revient à rechercher le p.g.c.d. de deux nombres des formes $p - x$ et $n - (p - x)^2$, x prenant les valeurs 0, 1, 2, 3, ...

A signaler aussi : 1° cette remarque faite incidemment par Euler : *soit* p *le plus petit nombre premier qui divise* n, *et soit* $n = pa$: *on trouvera les diviseurs de* a *en divisant ce nombre par les nombres premiers compris entre* $\sqrt{a}$ *et* $\sqrt{n}$; d'où il suit que, comme l'a observé Legendre, *si* $p > \sqrt{a}$, a *est premier ;* 2° celle-ci: de Gauss : *le nombre* n *ne peut avoir plus d'un facteur supérieur à* $\sqrt{n}$.

due l'idée de réduire le nombre des essais, en classant les diviseurs sous certaines formes nécessaires qui montrent à priori l'inutilité de certains essais. L'ouvrage qu'il avait écrit sur cette question est resté manuscrit (voir *Divers ouvrages...*, Paris, 1693, préface de Lahire).

Fermat a beaucoup cultivé cette féconde théorie de l'*exclusion*, et semble avoir trouvé à ce sujet de nombreux théorèmes dont la plus grande partie est encore inconnue, malgré les recherches des érudits et des savants. On peut résumer ainsi qu'il suit ce qu'on sait des découvertes du célèbre géomètre sur cette question.

Dans ses *Cogitata* (1644), Mersenne, probablement d'après Frenicle, annonce que *jusqu'à* $n = 257$, *les seules valeurs de* n *qui font de* $2^{n-1}(2^n - 1)$ *un nombre parfait, c'est-à-dire de* $2^n - 1$ *un nombre premier, sont* 1, 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 et 257. On peut voir dans le t. I de *Récr. math.* de Rouse-Ball (seconde édition française, 1909), quelques-unes des tentatives faites pour démontrer cette proposition.

Dans le *Comm. epist.* de Wallis (1658), on trouve, de Fermat, les suivantes, qui ont été le point de départ de nombreux travaux d'Euler : *tout nombre premier* $4 + 1$ *est, d'une seule manière, une somme de deux carrés. Tout nombre premier* $3 + 1$ *divise* $y^2 + 3z^2$.

Dans les *Varia Opera* (1679), on voit celles-ci :

Une somme de deux carrés premiers entre eux n'a aucun facteur de la forme $4 - 1$, ainsi il est inutile d'essayer la division de $10^{10} + 1$ par 3, par 7, par 11, par 19, par 23, ...

Si, p *étant premier,* a^t *est la plus petite puissance de* a *qui soit* $\equiv 1 \pmod{p}$, t *est un diviseur de* $p - 1$ [1] ; *si* t *est impair, aucun nombre de la forme* $a^x + 1$ *n'est multiple de* p. *Si* t *est un nombre premier pair* 2z, *on a* $a^z + 1 \equiv 0$. *Si* $p = 4 - 1$ *et que* $a^{2n+1} \equiv b^2$, *on pourra écrire* $a^y \equiv 1$ *avec* y *impair, et par suite il sera possible de trouver un nombre* z *tel que* $a^z + 1 \equiv 0$.

Aucun diviseur de $a^2 - 2$ *n'est de la forme* $x^2 + 2$.

Si p *est premier, les diviseurs de* $2^p - 2$ *sont de la forme* 2px, *et ceux de* $2^p - 1$, *de la forme* $2px + 1$. Ainsi les diviseurs de $2^{37} - 1$ sont de la forme $74 + 1$. Essayant la division par les nombres premiers de cette forme, 149, 233, ... l'opération réussit au deuxième essai [2]. *Aucun nombre* $2^{xy} - 1$ *n'est premier.*

Tout nombre premier $3 + 1$ *est de la forme* $x^2 + 3y^2$. *Tout nombre premier* $8 + 1$ *ou* $8 + 3$ *est de la forme* $x^2 + 2y^2$.

---

[1] C'est là le théorème de Fermat.

L'exposant *t* s'appelle, d'après Ed. Lucas, le *gaussien* de *p* ; il serait, d'après ce qui précède, plus équitable de le désigner par un mot rappelant le nom de Fermat, qui l'a considéré le premier.

[2] On démontrera de même que $2^{11} - 1$ est divisible par 23 (Fermat) ; que $2^{23} - 1$, $2^{29} - 1$, $2^{43} - 1$, $2^{73} - 1$, sont respectivement divisibles par 47, 1103, 431, 439 (Euler) ; et autres factorisations analogues. (Voir Rouse-Ball, *op. cit.*, p. 311, et Ed. Lucas, *Th. des n.*, p. 51.)

Depuis, on a retrouvé et publié en 1880 et 1883 quelques lettres de Fermat, dont on citera ce qui suit :

Tout impair non carré est autant de fois de la forme $x^2 - y^2$ *qu'il est de fois le produit de deux facteurs*[1]. Soit à trouver les facteurs de $n = 2027651281$; l'extraction de la racine carrée donnera $n = 45029^2 + 40440$. Le carré immédiatement supérieur à n le surpasse de $2.45029 + 1 - 40440 = 49619$, nombre non carré, ce qu'indiquent suffisamment ses deux derniers chiffres à droite[2]. Le carré qui suit surpasse n de $49619 + 2.45029 + 3 = 139680$, nombre non carré. Continuant ainsi, on trouve à la dixième opération, $45041^2 = n + 1020^2$; de là la décomposition $n = 46061.44021$[3].

---

[1] A citer ces deux théorèmes analogues :

Si on peut écrire $a^2 + 4n = f^2$ et $a^2 - 4n = g^2$, *le nombre* n *est de la forme* $xy(x^2 - y^2)$. En effet, des deux relations données, on tire

$$\left(\frac{f+g}{2}\right)^2 + \left(\frac{f-g}{2}\right)^2 = a^2$$

ce qui conduit à poser

$$\frac{f+g}{2} = x^2 - y^2 \qquad \text{et} \qquad \frac{f-g}{2} = 2xy\ , \qquad \text{d'où} \qquad n = xy(x^2 - y^2)\ . \qquad \text{(Aurifeuille)}$$

Pour n *premier*, $v^2 + 8u$ *ne peut donner un carré que si* $v = 2n - 1$ *ou* $v = n - 2$. En effet, tout entier n peut se mettre sous la forme $xy - \frac{x(x-1)}{2}$, d'où $2x = 2y + 1 + \sqrt{(2y+1)^2 - 8n}$; donc, en posant $2y + 1 = u$, $u^2 - 8n$ doit être un carré v^2, qui doit être impair, car les nombres $u + v$ et $u - v$ sont de même parité et par suite tous les deux pairs puisque leur produit $8n$ est pair. Si n est premier, on a les deux solutions uniques

$$u + v = 4n\ ,\quad u - v = 2\ ,\quad \text{d'où}\quad v = 2n - 1\ ;$$
$$u + v = 2n\ ,\quad u - v = 4\ ,\quad \text{d'où}\quad v = n - 2\ .$$

Si n est composé, on a au moins les deux relations distinctes $u^2 - v^2 = 8n$, $u'^2 - v'^2 = 8n$, d'où, au moins, quatre solutions de l'équation $u^2 - v^2 = 8n$ (Barbette, *op. cit.*).

Posons $n = xy$; l'identité $nz = \left(\frac{x + yz}{2}\right)^2 - \left(\frac{x - yz}{2}\right)^2$ montre que si z est l'impair le plus voisin de $\frac{x}{y}$, zn sera une différence de deux carrés dont le plus petit sera aussi petit que possible : on pourra ainsi appliquer à zn la méthode de Fermat. La recherche des diviseurs de n est donc ramenée à celle de la valeur de z. Le plus souvent, z n'est pas très grand et il suffira d'appliquer la méthode aux nombres n, $3n$, $5n$. $7n$.

[2] On sait qu'un carré est toujours terminé par l'un des vingt-deux groupes suivants :

00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.

[3] Dans ce cas particulier, les opérations sont peu nombreuses, les deux facteurs différant peu l'un de l'autre. Toutefois, on pourrait abréger et exclure souvent dix nombres d'un coup.

Dans le même ordre d'idées, pour $n = 4171$, nombre examiné déjà plus haut, on a les deux relations

$$4n = 129^2 + 43 = (3.43)^2 + 43$$
$$13n - 12n = (232^2 + 399) - (241^2 + 313) = 473.9 - 86\ ,$$

dont chacune donne la solution.

Plus généralement, la décomposition se trouvera de la même manière, si on peut écrire :

$$An = fa^2 + gb^2 + ha + jb + c\ , \qquad Bn = fb^2 + ga^2 + hb + ja + c\ .$$

On pourrait assigner d'autres formules plus faciles à imaginer qu'à appliquer. Par exemple, en combinant, par voie d'addition, les deux suivantes

$$An = a(c + f) + b(d + f)\ , \qquad Bn = b(c + g) + a(d + g)\ .$$

Mais souvent l'habitude du calcul suggèrera des exclusions évidentes ; ainsi pour $n = 4171$,

Il convient de mentionner que ce procédé a été publié avant la lettre de Fermat, dans le *Dict. de math.* de Montferrier (Paris, 1835), et réinventé également par Landry et Aurifeuille.

p *désignant un nombre premier, l'entier* $\frac{2^p + 1}{3}$ *est de la forme* $2px + 1$.

Sauf le cas où ab ... *est de la forme* 2^x, *le nombre* $2^{ab\cdots} + 1$ *est composé.*

Aucun facteur de $a^2 + 3b^2$ *n'est de la forme* $3 - 1$.

Enfin on citera la décomposition du nombre 100895598169 proposée par Mersenne à Fermat, qui la donna sans d'ailleurs indiquer la méthode qu'il avait employée [1].

---

on a :

$$n = 100 \cdot 41 + 71 \ , \qquad 10n = 204^2 + 2 \cdot 47 \ , \qquad 3n = 112^2 - 31 \ ,$$

ce qui fait immédiatement voir qu'il est inutile d'essayer la division par 41, par 47 et par 31.

Soit $n = a^2 + b$; posons $n = (a + x)^2 - (x^2 + 2ax - b)$: la question est réduite à amener, par diverses substitutions, l'expression $x^2 + 2ax - b$ à être un carré. Supposons qu'on cherche seulement les facteurs premiers ≥ 17 ; on posera

$$a + x - \sqrt{x(x + 2a) - b} > 16 \ , \qquad \text{d'où} \qquad x < \frac{n + 256}{32} - a \ .$$

Soit, par exemple, $n = 4171$. Par l'extraction de la racine carrée, on trouve $n = 64^2 + 75$; $x(x + 128) - 75$ doit donc être un carré. Il faut éliminer toutes les valeurs de x inférieures à 64 et terminées à droite par l'un des chiffres 3, 4, 8, 9, car autrement le premier membre ne serait pas un carré. Pour le même motif, x ne peut être ni $3 + 2$, ni $7 + 1, 2, 3, 4$. ni $8 + 0, 1, 3, 4, 5$. Les nombres inférieurs à 74 et répondant à toutes ces conditions sont 6, 42 et 70, dont le premier donne le carré 27^2 ; en le mettant à la place de x dans $x^2 + 2ax - b$: on a ainsi

$$n = (64 + 6)^2 - 27^2 = (70 + 27)(70 - 27) = 97 \cdot 43 \ .$$

Si aucun de ces trois nombres n'avait donné de carré, le nombre n n'aurait aucun diviseur premier plus grand que 16, et, en divisant par 3, 5, 7, 11 et 13, il aurait été aisé de voir s'il était premier.

Souvent, comme on l'a vu plus haut, la décomposition se voit plus aisément sur un multiple que sur le nombre proposé lui-même. Ainsi, pour $n = 4171$, on a : $8n = 182^2 - 11^2$, d'où $n = 97 \cdot 43$. Pour $n = 1180\,17$, on a : $3n = 595^2 - 2^2 = 597 \cdot 593$, d'où $n = 199 \cdot 593$.

On arriverait aussi à la solution si on pouvait trouver deux égalités de la forme $An = a^2 + \alpha$, $Bn = b^2 \pm \alpha$, car il s'ensuivrait $(A \mp B)n = (a + b)(a - b)$. Ainsi soit $n = 4171$, il viendra :

$$19n = 274^2 + 2 \ , \qquad 33n = 371^2 + 2 \ , \qquad \text{d'où} \qquad 15n = 645 \cdot 97 \ .$$

En général, si kn peut se représenter par la différence de deux valeurs de la fonction entière $F(x) = Ax^h + Bx^g + \ldots$ la décomposition est immédiate, car $F(a) - F(b)$ est divisible par $a - b$; par exemple, on peut prendre pour F les carrés, les cubes, les bicarrés, les triangulaires, etc., dont on possède des tables étendues.

[1] On a émis diverses conjectures sur le principe dont s'était servi Fermat pour obtenir cette factorisation. Ne serait-ce pas simplement la considération des triangulaires, telle que l'indique M. Barbette (*op. cit.*) et qu'on peut exposer ainsi :

La factorisation est facile si n est un triangulaire, c'est-à-dire si on peut écrire $2n = x(x + 1)$ ou bien $2x = -1 + \sqrt{8n + 1}$. Ainsi la condition pour n d'être un triangulaire équivaut à celle, pour $8n + 1$, d'être un carré. Essayant cette formule avec le nombre de Mersenne, on voit, en extrayant la racine de $8n + 1$, que ce nombre n'est pas carré, et que

$$8n = 89423^2 + 898423 \ ,$$

d'où la décomposition demandée. Cette égalité avait du reste été signalée antérieurement par M. Petersen (*I. M.*, 1908).

Euler a beaucoup étendu ces procédés de Fermat[1].

Contrairement à ce que pensait celui-ci, il reconnaît que $2^{2^n}+1$ n'est pas toujours premier, même si n l'est, car $2^{32}+1$ est divisible par 641. Il donne les diviseurs de 2^x-1, pour $x=29, 43$ et 73; et diverses extensions ou conséquences du théorème de Fermat. (1732.)

Il donne les formes linéaires des diviseurs de x^2+py^2, pour les premières valeurs de p, et celles de ax^2+by^2, pour différentes valeurs de ab. Il observe que *les formes* ax^2+by^2 *et* x^2+aby^2 *ont les mêmes diviseurs, de même que* x^2+ay^2 *et* x^2+a. (1744.)

Tout diviseur de $a^{2^n}+b^{2^n}$ *est de la forme* $2^{n+1}x+1$. De là, la démonstration de la divisibilité de $2^{32}+1$ par 641. (1748.)

Le produit de deux sommes de deux carrés est une somme de deux carrés[2]. *Si* a *et* b *sont premiers entre eux, les diviseurs de* a^2+b^2 *sont des sommes de deux carrés. Un nombre* $4+1$, *qui ne peut se décomposer que d'une seule manière en une somme de deux carrés est premier; dans le cas contraire, il est composé* et on trouvera aisément sa décomposition[3]. (1752.)

Si un diviseur de a^2+2b^2 *ou* a^2+3b^2 *est de même forme, il en est de même du quotient. Tout nombre premier* $6+1$ *divise* $3x^2+y^2$ *et il est de la même forme.* (1759.)

Il montre comment on détermine des nombres de la forme x^2+1 qui soient multiples du nombre premier p de la forme $4+1$, ce qui facilite la recherche des conditions de divisibilité d'un nombre donné par p, et permet de trouver de très grands nombres immédiatement décomposables. (1760.)

On sait, d'après Fermat, qu'un nombre n, de la forme $4+1$, est premier s'il est, d'une seule manière, une somme x^2+y^2 de deux carrés; mais, pour peu que n soit considérable, on avait ainsi à calculer un grand nombre de carrés. Euler montre comment on peut réduire le nombre de ces opérations, en déterminant les formes linéaires de y d'après celles de n. Ainsi si $n=16x+1$ ou $16x+5$, x est de la forme 8 ± 1 : le nombre des carrés à calculer est ainsi réduit au quart. On comprend combien, avec des coefficients plus élevés, comme $60x+1$, $240x+1$,

---

[1] Pour les détails et les démonstrations de ce qui a rapport à Euler, voir *Ens. math.*, 1909, p. 330 et seq.

[2] Théorème déjà connu de Fibonacci et de Fermat, et peut-être de Diophante.

[3] Soit, par exemple, $n=a^2+b^2=\alpha^2+\beta^2$; si $\frac{f}{g}$ désigne la valeur de la fraction

$$\frac{a+\alpha}{\beta+b}=\frac{\beta-b}{a-\alpha}$$

réduite à sa plus simple expression, n est divisible par f^2+g^2.

Cette méthode paraît avoir été connue de Frenicle.

$14400x + 1$, ... on augmenterait le nombre des exclusions, et par suite la rapidité de la vérification de la divisibilité des grands nombres. (1765.)

Il vérifie ainsi que, comme l'avait annoncé Fermat, le nombre $n = 2^{31} - 1$ est premier : 31 étant premier, tout facteur de n est de la forme $62 + 1$ et, d'autre part, n divisant $2^{32} - 2$, il est des deux formes 8 ± 1 ; il est donc de l'une ou de l'autre forme $248 + 1$, 63. Essayant la division de n par les nombres premiers compris dans ces deux formes, Euler s'est assuré que ce nombre est premier[1]. (1772.)

Il propose, pour la construction des tables de nombres premiers, la méthode suivante : soit considérée l'expression $30a + \alpha$, où a représente un entier quelconque, et α, l'un des $\varphi(30)$ nombres 1, 7, 11, 13, 17, 19, 23, 29, inférieurs à 30 et premiers avec lui. Les valeurs de cette expression comprennent entre autres, tous les nombres premiers avec 30 ; il faut en éliminer tous les multiples de nombres premiers. Pour cela, on résoudra, dans chaque cas, l'équation $30a + \alpha = \beta y$, β désignant l'un quelconque des nombres α[2] : la formule $30(x + k\beta) + \alpha$, où k varie de 0 à ∞, donne la suite des nombres divisibles par β. Classant toutes ces suites en une même table, les nombres absents de celle-ci sont premiers[3]. (1774.)

Euler montre que *si* x *étant premier avec* k, *tous les nombres de*

---

[1] Landry et Ed. Lucas, comme on le verra plus loin, ont également vérifié cette assertion de Fermat, à l'aide de méthodes particulières. Legendre l'a fait par une méthode tout à fait générale.

[2] Par exemple, soit $30x + 1 = 7y$; on a

$$y = 4x + \frac{2x + 1}{7} ;$$

ainsi les valeurs de x qui rendent $30x + 1$ divisible par 7 sont les termes de la progression $\div$ 3.10.17.24...

[3] Cette méthode a été retrouvée et perfectionnée récemment par MM. Lebon et G. Tarry. Le premier prend $2310 = 2.3.5.7.11$, au lieu de 30, ce qui lui donne $\varphi(2310) = 480$ types de l'expression $2310x + \alpha$. Si on résout l'équation $\beta x - 2310y = \alpha$ et qu'on pose $y = a - bx$, il viendra :

$$2310a + \alpha = (2310b + \beta)x .$$

Le nombre $2310a + \alpha$ sera donc divisible par le nombre $2310b + \beta$. En déterminant toutes les solutions, on obtiendra de même tous les multiples de $2310b + \beta$.

M. Lebon a depuis perfectionné sa méthode et s'occupe de la construction de tables qui permettent de factoriser un nombre quelconque inférieur à cent millions.

M, Tarry pose

$$n = 20580a + \alpha , \qquad \alpha = 210b + \beta ,$$

d'où

$$n = 20580a + 210b + \beta .$$

Soit le nombre premier $p > 7$, c'est-à-dire non diviseur de 20580, et soit h l'associé de 20580, c'est-à-dire le nombre tel que $20580h \equiv 1$; on aura $hn \equiv a + 210hb + \beta h$, de sorte que, si α' et β' sont les restes de la division de $210hb$ et de βh par p, on pourra écrire

$$hn \equiv a + \alpha' + \beta' .$$

Ainsi p divise n si on a :

$$a + \alpha' + \beta' \equiv 0 .$$

forme $x^2 + k$ *et moindres que* $4k$ *sont premiers, ou des carrés de premiers, ou des puissances de* 2, *un nombre quelconque qui ne peut être représenté que d'une seule manière par la formule* $y^2 + kz^2$ *est premier.* Il donne la liste des soixante-cinq valeurs de k, qu'il appelle *numeri idonei,* et qui sont : 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, ... 1365, 1848. (1776.)

Il enseigne, sur des exemples, différents procédés d'exclusion dans la recherche des solutions de l'équation $n = a^2 + b^2 = x^2 + y^2$, par la considération des formes linéaires possibles des inconnues ; et il étend sa théorie au cas où n est de la forme $x^2 + ky^2$. (1778.)

Lagrange ne s'est pas spécialement occupé de la factorisation des nombres, mais il a démontré cette réciproque d'un théorème d'Euler : *si* k *est positif, le nombre premier* p *ne peut être que d'une seule manière, de la forme* $x^2 + ky^2$. En effet, soit

$$p = f^2 + kg^2 = f'^2 + kg'^2 ;$$

on aura

$$(\alpha) \qquad (ff' - kgg')^2 + k(fg' + f'g)^2 = p^2 .$$

Or

$$f^2g'^2 - f'^2g^2 = p(g'^2 - g^2) ;$$

p diviserait donc l'un des deux nombres $fg' \pm f'g$, ce qui est impossible, puisque, d'après (α), on a

$$fg' + f'g < p . \qquad (\textit{Misc. Taurin.}\ 1766\text{-}69.)$$

Il a démontré le théorème de Wilson (*Mém. de Berlin,* 1771) qui, comme on sait, fournit un moyen, malheureusement impraticable, de caractériser et vérifier les nombres premiers [1].

Enfin il a donné le moyen de trouver les formes linéaires des diviseurs d'un nombre quelconque qu'on a pu mettre sous la forme $ax^2 + bxy + cy^2$. (*Id.*, 1775.)

Legendre, dans sa *Th. des n.* dont la première édition est de 1798, — outre une table des formes des diviseurs numériques des nombres de la forme $x^2 \pm ky^2$, jusqu'à $k = 103$, — a indiqué plusieurs voies qu'il serait bon de soumettre à de nouvelles explorations.

---

[1] Ainsi 37 étant de la forme $4 + 1$, on calculera ainsi :

$$\left.\begin{array}{l} 1! \equiv 1,\ 2! \equiv 2,\ 3! \equiv 6,\ 4! \equiv 24,\ 5! \equiv 9,\ 6! \equiv 6.9 \equiv 17,\ 7! \equiv 7.17 \equiv 8, \\ 8! \equiv 8.8 \equiv 27,\ 9! \equiv 9.27 \equiv 21,\ 10! \equiv 10.21 \equiv 25, \ldots\ 18! \equiv 6.12 \equiv 6 . \\ (18!)^2 + 1 \equiv 6^2 + 1 \equiv 0 \end{array}\right\} \pmod{37}$$

donc 37 est premier.

Soit $n = af^2 + 2bfg + cg^2$, a, b, c étant premiers deux à deux. Posons

$$n = ax^2 + 2bxy + cy^2 \qquad \text{et} \qquad ac - b^2 = \Delta ,$$

il viendra

$$(\alpha) \qquad an = (af + bg)^2 + \Delta g^2 = (ax + by)^2 + \Delta y^2 .$$

Donc n peut se mettre de deux manières différentes sous la forme $\xi^2 + \Delta\eta^2$, et par suite, il est composé.

Δ est premier avec a et b, donc l'un des deux nombres $(af + bg) \pm (ax + by)$ doit être divisible par Δ, ce qui donne l'équation de condition

$$af + bg \mp (ax + by - \Delta z) = 0 ;$$

d'où, en substituant dans (α), la valeur de $ax + by$,

$$(\beta) \qquad g^2 + 2(af + bg)z - \Delta z^2 = y^2$$

et on aurait de même

$$(\gamma) \qquad f^2 + 2(bf + bg)w - \Delta w^2 = x^2 .$$

Si on peut trouver des valeurs de z et de w qui rendent les premiers membres de (β) et de (γ) des carrés parfaits, n est composé.

Inversement si on ne trouve aucune de ces valeurs de z et de w, il y a présomption que n est premier, mais il faut s'en assurer autrement. Ainsi considérons la formule $F = f^2 + f + 41$; comme l'expression $1 + (4f + 2)z - 163z^2$ ne peut représenter un carré positif que pour $z = 0$ et qu'elle est négative pour $4f + 2 < 163$, ou $f < 40$, *pour les trente-neuf premières valeurs entières de* f, *l'expression* F *donne un nombre premier*, comme l'avait annoncé Euler.

Pour voir si le premier membre de (β) ne peut devenir un carré, on essaiera toutes les valeurs entières de z comprises entre les racines de l'équation $g^2 + \ldots = 0$: le nombre des essais est $\frac{2}{\Delta}\sqrt{an}$ et pourra encore être réduit par l'examen des formes linéaires possibles de z. Legendre tire de ces remarques un moyen ingénieux — mais souvent illusoire — de trouver un nombre premier d'une forme assignée et supérieur à une limite donnée.

Un autre procédé de Legendre fournissant des résultats certains, sans nécessiter aucune connaissance préalable de la composition quadratique du nombre n à factoriser, consiste à utiliser les propriétés des fractions continues pour la recherche de ces mêmes formes, en développant par ce moyen le nombre n ou un de ses multiples.

Soient

$$\ldots f', \; g', \; h' \ldots$$
$$\ldots f'', \; g'', \; h'' \ldots$$

les deux séries auxquelles conduisent la décomposition de $\sqrt{n}$. On sait qu'on a

$$n = f''g'' + g'^2 = g''h'' + h'^2 ,$$

ce qui fait que $(g'h')^2 - f''h''g''^2$ est un multiple de n. On trouvera ainsi plusieurs expressions de la forme $x^2 - Ny^2$ dont n doit être diviseur.

Appliquant ce procédé au nombre $n = 10091401$ traité autrement par Euler, Legendre trouve qu'il est diviseur des formes

$$x^2 + 3y^2,\ x^2 + 31y^2,\ x^2 + 6y^2,\ x^2 + 5y^2,\ x^2 + 38y^2,$$
$$x^2 - 46y^2,\ x^2 - 55y^2,\ x^2 - 97y^2 ;$$

cherchant les nombres premiers inférieurs à $\sqrt{n}$ et appartenant à la forme $\mathbf{1320} + 1, 7, 49, 103, \ldots$ combinaison des formes

$$\mathbf{6} + 1 ; \quad \mathbf{24} + 1, 5, 19; 23 ; \quad \mathbf{20} + 1, 3, 7, 9 ;$$
$$\mathbf{44} + 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 ;$$

des diviseurs des formes quadratiques

$$x^2 + 3y^2,\ x^2 + 6y^2,\ x^2 + 5y^2,\ x^2 - 55y^2 ,$$

et retranchant de ces nombres ceux qui ne peuvent diviser

$$x^2 + 31y^2,\ \text{ni}\ x^2 + 38y^2,\ \text{ni}\ x^2 - 46y^2 ,$$

il reste, comme diviseurs possibles, les seuls nombres 727, 1423, 2281, dont aucun ne divise n : ce nombre est donc premier [1].

Gauss, dans ses *Disq. arith.*, a donné, sur le même sujet, plusieurs méthodes très ingénieuses, dont on donnera seulement le précis. La première (voir *Ens. math.*, 1907, p. 36) s'appuie sur les propriétés des résidus, qu'on déterminera en remarquant que si $kn = f\alpha^2 + g\beta^2$, $-fg\alpha^2\beta^2$ est résidu en même temps que $-fg$.

---

[1] Tchebichef, dans son traité des congruences, publié en 1849, trouve par les mêmes moyens, que le nombre 8520191, également considéré par Legendre, divise les formes

$$x^2 - 5y^2,\ x^2 - 2y^2,\ x^2 - 13y^2,\ x^2 - 37y^2,\ x^2 - 101y^2 .$$

De là les formules

$$\mathbf{260} + 1, 7, 9, 29, 33, \ldots \quad \mathbf{20} + 1, 9, 11, 19 \ldots \quad \mathbf{520} + 1, 9, 29, 49, 51, \ldots$$

Les nombres premiers de ces formes et inférieurs à $\sqrt{8520191}$ sont

$$521,\ 601,\ 1231,\ 1249,\ 1999,\ 2441,\ 2729,\ 2791.$$

Aucun d'eux ne divisant le nombre proposé, il est premier.

Soit $n = 4171 = 64^2 + 3.5^2 = 65^2 - 6.3^2$. Ses diviseurs sont de la forme $\mathbf{6} + 1$ et de l'une des formes $\mathbf{24} \pm 1, \pm 5$. Il s'ensuit que les diviseurs de n sont de l'une des formes $\mathbf{24} + 1, 19$. On essaiera donc la division par 25, 43, 49, dont le second seul est premier.

Ainsi, on a :

$$997331 = 999^2 - 2.5.67 = 994^2 + 5.11.13^2 = 2.706^2 + 3.17.3^2$$
$$= 3.575^2 + 11.31.2^2 ;$$

donc les nombres $-2.5.67$, 5.11, $2.3.17$, $3.11.31$ sont résidus, ainsi que $3.5.11^2.31$ ou $3.5.31$, etc. D'ailleurs, de ces résidus, on déduit de nouvelles conditions qui permettent d'exclure certaines formes de facteurs, à la manière d'Euler.

La seconde méthode de Gauss demande la résolution de deux équations importantes, qu'il montre à résoudre d'abord directement et ensuite par des procédés indirects tout à fait élémentaires quoique beaucoup plus rapides.

Soit d'abord à résoudre l'équation

$$(\alpha) \qquad a + ny = x^2 ;$$

il est permis de supposer qu'on a $0 < x \leq \frac{n}{2}$, car si $x = \theta$ est une solution, $x = n - \theta$ en est une autre. La valeur de y est ainsi comprise entre $-\frac{a}{n}$ et $\frac{n}{4} - \frac{a}{n}$.

Soit ϱ un non-résidu du nombre premier p et soit $y = \alpha$ une valeur qui donne $a + ny \equiv \varrho$; tout nombre congru à α donne à la formule $a + ny$ une valeur qui est un non-résidu et à fortiori un non-carré. On peut donc exclure, des solutions de (α), les valeurs de y comprises dans la formule $\alpha + pz$.

La considération d'un autre nombre p' fournirait des exclusions analogues.

Ainsi, soit $x^2 = 22 + 97y$:

pour	$p = 3$, $\varrho = 2$; $\alpha = 1$:	on exclura les nombres	$3z + 1$;
»	$p = 4$, $\varrho = 2, 3$; $\alpha = 0, 1$:	» »	$4z$ et $4z + 1$;
»	$p = 5$, $\varrho = 2, 3$; $\alpha = 0, 3$:	» »	$5z$ et $5z + 3$;
»	$p = 7$, $\varrho = 3, 5, 6$; $\alpha = 2, 3, 5$:	» »	$7z + 2, 3, 5$.

Eliminant des valeurs entières de y comprises entre $-\frac{22}{97}$ et $\frac{97}{4} - \frac{22}{97}$, celles qui sont comprises dans les formules qui précèdent, il ne reste que les nombres 6, 11 et 14, dont le second seul donne un carré. On a ainsi la solution $y = 11$, $x = 33$.

On arrive ainsi, de la manière suivante, à la connaissance des non-résidus α, α', α'' ... de p : soient f, f', f'' ... les solutions des congruences

$$(\beta) \qquad ny \equiv \varrho , \quad \equiv \varrho' , \quad \equiv \varrho'' , \ \ldots$$

et g, celle de la congruence $ny \equiv a$; on aura $\alpha \equiv f + g$. Si n est résidu de p, f, f', f''... sont non-résidus d'après (β) et se confondent avec les nombres $\alpha, \alpha', \alpha''$... Si n est non-résidu, f, f', ... forment l'ensemble des résidus : de là, les non-résidus.

Soit en second lieu à mettre n sous la forme $ax^2 + by^2$. On cherchera les valeurs de z qui rendent $n - az$ divisible par b, et on posera $x = bw \pm z$, w prenant les valeurs 0, 1, 2, 3, 4, ...; x sera une solution quand l'entier $\frac{n - ax^2}{b}$ sera un carré parfait positif. Cette dernière condition montre qu'il n'y a pas lieu d'examiner les valeurs de x supérieures à $\sqrt{\frac{n}{a}}$.

On peut encore réduire le nombre des essais, en remarquant que z doit être un résidu de b, puisqu'autrement on ne pourrait écrire

$$x^2 \equiv z \ , \qquad \text{ni par suite} \qquad n - ax^2 \equiv n - az \equiv 0 \pmod{b}$$

De même que plus haut, on limitera le nombre des essais, autant qu'on le voudra, en remarquant que si ϱ est un non-résidu de p et qu'on détermine z tel que $az \equiv n - b\varrho$, si on a en outre $x^2 \equiv z$, $\frac{n - ax^2}{b}$ sera $\equiv \varrho$, c'est-à-dire sera un non-résidu de p.

La résolution de l'équation $ax^2 + 2bxy + cy^2 = n$ se ramènerait à la précédente, en remarquant qu'on peut l'écrire $(ax + by)^2 + (ac - b)^2 y^2 = an$.

Maintenant remarquons d'abord que *tout résidu de* n *est en même temps résidu des diviseurs de* n. Soit $kn = \mathrm{A}^2 - a\alpha$: si a est non-résidu des nombres premiers p, q, r ... n n'est divisible par aucun de ces nombres; la question revient donc à trouver les résidus de n, comme on l'a dit tout à l'heure.

Si n est résidu de p, il l'est de p^2, car, en posant $\mathrm{A}^2 = n - ph$ et résolvant l'équation $2\mathrm{A}x - py = h$, il vient $(\mathrm{A} + px)^2 \equiv n \pmod{p^2}$. De là le moyen de mettre n sous la forme $\mathrm{B} - \mathrm{C}p^2$, qu'on rendra d'autant plus utile que $n - \mathrm{B}^2$ sera plus petit.

Soit $-a$ un résidu de n; cherchons les racines de l'équation $x^2 + a = ny$ et soient $f^2 + a = ng'$, $f'^2 + a = ng'$; il viendra, en soustrayant, puis en multipliant,

$$(f + f')(f - f') = nh \ , \qquad n^2 gg' = (ff' - a)^2 + a(f + f')^2$$

D'un autre côté, soit

$$n = ax^2 + by^2 = ax'^2 + by'^2 \ ;$$

il viendra d'abord la relation

$$a(x^2 y'^2 - x'^2 y^2) = n(y'^2 - y^2) \ ,$$

laquelle fait voir que n divise l'un ou l'autre des deux nombres $xy' \pm x'y$, ou qu'il a avec chacun d'eux un facteur commun. Ensuite on a cette autre

$$(axx' - byy')^2 + ab(xy' + x'y)^2 = n^2 ,$$

qui donne $xy' + x'y < n$. On n'a donc qu'à chercher le p. g. c. d. de n et de $xy' + x'y$.

Tchebichef a donné en 1851, dans le *J. L.*, une ingénieuse méthode de vérification des nombres premiers, dont voici le résumé :

α désignant la plus petite valeur de x *qui satisfait à l'équation* $x^2 - ky^2 = 1$, *si les nombres positifs* a *et* a', *inférieurs à* $\sqrt{\frac{(\alpha \pm 1)n}{2}}$, *sont des valeurs de* x *satisfaisant à l'équation* $x^2 - ky^2 = \pm n$, *et que* b *et* b' *soient les valeurs correspondantes de* y, *le nombre* n *est composé, et on en trouvera deux diviseurs en cherchant le p.g.c.d. de* n *et de chacun des deux nombres* ab' $\pm$ a'b [1].

Le nombre n *ne peut être premier que dans le cas où il n'est qu'une fois représentable par la forme* $x^2 - ky^2 = \pm n$, x *étant inférieur à la limite donnée plus haut. Si en outre les diviseurs de* $x^2 - ky^2$ *sont tous de la forme* $lx^2 - my^2$, *et si* n *est premier avec* k, *et de la forme des diviseurs de* $x^2 - ky^2$, *la condition est en même temps suffisante* [2].

Il applique ce théorème au nombre $n = 8520191$, de Legendre ; ce nombre, qui est $\mathbf{12} - 1$, est donc de la forme quadratique $3y^2 - x^2$, ce qui conduit à chercher y entre $\sqrt{\frac{n}{2}}$ et $\sqrt{\frac{n}{3}}$ [3]. Les hypothèses faites sur y relativement aux modules 2, 5, 7... font voir que y est de l'une des formes de chacun des groupes suivants :

$$\mathbf{4} ; \quad \mathbf{16} \pm 1 ; \quad \mathbf{5} + 0 , \pm 2 ; \quad \mathbf{7} \pm 1 , \pm 2 ; \quad \mathbf{11} \pm 1 , \pm 2 , + 5 ;$$
$$\mathbf{13} + 0 , \pm 1 , \pm 3 , \pm 6 ; \quad \mathbf{17} \pm 1 , \pm 2 , \pm 3 , \pm 4 , \pm 7 .$$

La valeur $y = 1937$ répond seule à toutes ces conditions, ce qui montre que n est premier.

Landry (*Procédés nouveaux...*, Paris, 1859) a posé les premiers jalons d'une voie nouvelle aussi féconde qu'élémentaire, celle de l'assimilation du nombre à factoriser au produit de deux fonctions linéaires convenablement choisies.

---

[1] Voir, pour la démonstration de ce théorème, *Ens. math.*, 1912, p. 201.

[2] Pour la démonstration de ce second théorème, trop longue pour pouvoir être reproduite ici, voir *loc. cit.*

[3] Cette deuxième limite résulte de ce que $3y^2 - x^2 = n$ et $x > 0$.

Les facteurs, s'ils existent, du nombre $n = 2^{31} - 1$ appartiennent aux formes $\mathbf{248} + 1, 63$ [1]. Posons en conséquence

$$\begin{aligned} n &= (62x + 1)(62y + 1) = 3844xy + 62(x + y) + 1 \\ &= 3844.558658 + 62.37 + 1 \\ &= 3844(558658 - h) + 62(62h + 37) + 1 , \end{aligned}$$

d'où les formules

$$(\alpha) \qquad xy = 558658 - h \qquad\qquad (\beta) \qquad x + y = 62h + 37 ,$$

ou, t désignant collectivement les nombres x et y,

$$(\gamma) \qquad t = 62h + 37 \pm \sqrt{3844h^2 + 4592h - 2233263} .$$

Le plus petit, y, des deux nombres x et y diminue à mesure que h augmente, puisque xy diminue et que l'autre nombre x ne cesse d'augmenter.

D'après (α) et (β), h est pair, et d'un autre côté, le nombre sous le radical dans (γ) est $\equiv h^2 + 2h - 3 \pmod 9$; de là, on conclut que h est de l'une des formes $\mathbf{18} + 2, 6, 8, 10, 14$. Or d'après (α) et (β) on a :

$$xy \equiv 1 - h \qquad \text{et} \qquad x + y \equiv 2h + 1 \pmod 3$$

d'où, pour $h = \mathbf{3} + 2$,

$$xy \equiv 2 , \qquad x + y \equiv 2 \qquad \text{(id.)}$$

congruences auxquelles on ne peut satisfaire, car il faudrait, pour la première, $x \equiv 1$ et $y \equiv 2$, ou $x \equiv 2$ et $y \equiv 1$, d'où $x + y \equiv 0 \pmod 3$. Ainsi h ne peut être $\mathbf{3} + 2$; il doit donc appartenir à l'une des formes $\mathbf{18} + 6, 10$.

De même (α) et (β) font voir que h ne peut être $\mathbf{5} + 0, 1, 2$, car autrement on aurait

$$x + y \equiv 3 - h , \qquad x + y \equiv 2h + 2 \pmod 5$$

d'où, pour

$h = \mathbf{5}$,	$xy \equiv 3$,	$x + y \equiv 2$	(id.)
$\mathbf{5} + 1$,	$xy \equiv 2$,	$x + y \equiv 4$	(id.)
$\mathbf{5} + 2$,	$xy \equiv 1$,	$x + y \equiv 1$	(id.)

résultats qui conduisent à des contradictions. Les seules formes admissibles sont donc $\mathbf{5} + 3, 4$, ou, comme h est pair, $\mathbf{10} + 4, 8$. Ecrivant les formes possibles relatives aux deux modules 18 et 10,

[1] Voir plus haut.

et ne conservant que celles qui sont communes aux deux suites, on verra que h ne peut être que de l'une des formes $90 + 24$, 28, 64, 78.

Remplaçant successivement h par $90k + 24$, 28, 64, 78, dans l'expression sous le radical; les suppositions $k = 0, 1, 2, 3, 4, 5, 6$ fourniront — en calculant à l'aide des différences premières et secondes — vingt-huit nombres dont aucun n'est un carré : ainsi, jusqu'à $h = 90.6 + 78 = 618$, il n'y a aucune valeur de h propre à conduire à la connaissance d'un facteur de n.

La valeur de t correspondant à $h = 168$ est inférieure à 16 et diminue quand h augmente; d'autre part, les nombres premiers de la forme $62 + 1$ et plus petits que $62.16 + 1$ sont 311, 373, 683, dont il y a lieu d'éliminer les deux derniers, qui ne sont pas de la forme 8 ± 1; il reste donc seulement à essayer le nombre 311, auquel correspond la valeur 5. Or dans ce cas, la formule

$$(\delta) \qquad h = \frac{558658 - t(37 - t)}{62t + 1}$$

donne $h = \frac{558498}{511}$, valeur non entière : le nombre proposé est donc premier.

Autrement. Remplaçons dans (δ), t successivement par $90k + 24$, 28, 64, 78, ce qui donne

$$\begin{aligned}(5580t + 90)k &= 558634 - t(1525 - t)\\ &= 558630 - t(1773 - t)\\ &= 558594 - t(4005 - t)\\ &= 558580 - t(4873 - t)\,.\end{aligned}$$

Comme $t(a - t)$ augmente, quand t varie de 0 à $\frac{a}{2}$, et que d'autre part, dans les seconds nombres des quatre égalités qui précèdent, les nombres 1525, 1773, 4005 et 4873 sont supérieurs à la limite de t déterminée par la relation $62t + 1 < \sqrt{n}$, limite qu'on trouve être égale à $\frac{\sqrt{n} - 1}{62} = 748$, on voit que k diminue quand t augmente; donc, comme pour $t = 60$, $k < 2$, et que pour $t = 80$, $k < 1$, il est inutile d'essayer des valeurs de k supérieures à 80. Faisant $k = 1$ et $= 2$, dans ces mêmes égalités, on n'aboutit à aucun résultat utile. On essaiera donc les valeurs de t inférieures à 60, mais seulement celles qui, mises dans la formule $62t + 1$, donnent des nombres premiers de l'une des deux formes 8 ± 1. Le calcul est, comme on le voit, très réduit; d'autres remarques de Landry permettraient de le réduire encore,

mais ce qui précède suffit pour faire sentir l'importance des idées nouvelles qu'il a introduites dans la théorie de la factorisation.

Genocchi (*Anali di Matematica*, 1868), dans un mémoire sur certaines formes de nombres premiers, s'appuie sur les propositions suivantes.

Posons $(a + \sqrt{b})^n = A_n + B_n \sqrt{b}$, on aura, d'après Euler, $(a - \sqrt{b})^n = A_n - B_n \sqrt{n}$, d'où

$$(\alpha) \quad 2A_n = (a+\sqrt{b})^n + (a-\sqrt{b})^n, \quad 2\sqrt{b}B_n = (a+\sqrt{b})^n - (a-\sqrt{b})^n.$$

Si n *est multiple de* k, B_n *sera multiple de* B_k [1]. On a aussi : $B_{2n} = 2A_n B_n$.

Soit p *un diviseur premier de* B_n, *et* k, *la plus petite valeur de* x *qui rende* B_x *divisible par* p ; k *divise* n [2].

Si $B_f \equiv B_g \equiv 0$, f *et* g *sont multiples de* k, *ainsi que leur p.g.c.d.*

Si p *est premier,* $A_p \equiv a$ *et* $B_p \equiv \left(\frac{b}{p}\right)$, ce symbole désignant le *caractère quadratique* de *b*.

On a : $B_{p\pm 1} \equiv 0$, *selon que* b *est résidu ou non-résidu* [3].

On a : $A_{kp} \equiv A_k$ *et* $B_{kp} \equiv \left(\frac{b}{p}\right) B_k$.

Ed. Lucas a exposé, de 1875 à 1878, une méthode de vérification des nombres premiers aussi originale que féconde en théorèmes particuliers simples ; elle s'applique surtout quand on connaît la composition d'un des deux nombres voisins du nombre considéré. On peut la présenter ainsi :

---

[1] Car les termes du quotient algébrique de ces deux nombres peuvent s'écrire deux à deux, ainsi :

$$(a+\sqrt{b})^f (a-\sqrt{b})^{f+h} + (a+\sqrt{b})^{f+h}(a-\sqrt{b})^f = 2(a^2-b)^f A_h,$$

ce qui montre que le quotient est un nombre rationnel et même entier.

[2] Supposons $n = kq + r$, on aura :

$$B_n \equiv 0 \qquad \text{et} \qquad B_k \equiv 0 \qquad \text{d'où} \qquad B_{kq} \equiv 0.$$

Or si dans l'identité

$$(\alpha^r - \beta^r)\alpha^{kq} + (\alpha^{kq} + \beta^{kq})\beta^r = \alpha^{r+kq} - \beta^{r+kq},$$

on fait $\alpha = a + \sqrt{b}$ et $\beta = a - \sqrt{b}$, il viendra :

$$(a^2-b)^{kq} B_r = (a-\sqrt{b})^{kq} B_n - (a-\sqrt{b})^n B_{kq}.$$

Le premier membre étant entier, on a $B_r \equiv 0$. Par suite k ne serait pas la plus petite valeur de x qui rende $B_x \equiv 0$, ce qui contredit l'hypothèse.

[3] Cette proposition est de Lagrange. On la démontre, ainsi que la précédente, en développant les relations (α) à l'aide de la formule du binôme.

1. Lemme. *Selon que* a *est résidu ou non-résidu de* p, p *divise* $a^m \mp 1$ [1].

2. *Tout diviseur de* $2^{4h} + 1$ *est de la forme* $16h + 1$. (Voir *Ens. math.*, 1907, p. 446.)

3. P *et* Q *représentant des entiers positifs ou négatifs premiers entre eux, si on pose :*

$$a + b = P , \quad ab = Q , \quad a - b = \delta = \sqrt{\Delta} ,$$

$$\delta u_k = a^k - b^k , \quad v_k = a^k + b^k ,$$

u_k *et* v_k *sont des nombres entiers, qu'on peut calculer de proche en proche, par exemple à l'aide des formules de récurrence suivantes :*

$$(1) \quad \begin{cases} u_1 = 1 , \quad u_2 = P , \quad u_{k+1} = Pu_k - Qu_{k-1} , \\ v_1 = P , \quad v_2 = P^2 - 2Q , \quad v_{k+1} = Pv_k - Qv_{k-1} , \end{cases}$$

4. u_{kn} *est algébriquement, et à fortiori arithmétiquement, divisible par* u_n, d'après la définition de δu_n.

Cor. *Si* n *est le p. g. c. d. de* f, g, h, ... u_n *est le p. g. c. d. des termes* u_f, u_g, u_h, ...

5. *Soit* $f > g$; *tout diviseur de* u_f *et de* u_g *divise* u_{f-g} [2].

6. *Les termes de la série des* u *comprennent tous les facteurs premiers contenus dans celle des* v. En effet, on a visiblement

$$(2) \quad u_{2k} = u_k v_k .$$

Cette formule et la suivante

$$(3) \quad v_{2k} = v_k^2 - 2Q^k ,$$

permettent de calculer rapidement les termes de la série u_1, u_2, u_4, u_8, u_{16}, ... dont il sera fait grand usage plus loin.

---

[1] Par exemple 2 est résidu des nombres premiers 8 ± 1 et non résidu des nombres premiers 8 ± 3. Donc si k est plus grand que 2, et si le nombre $p = 2^k \pm 1$ est premier, il divise $2^m - 1$; si $p = 2^k \pm 3$ est premier, il divise $2^m + 1$. La lettre m est mise pour $\frac{p-1}{2}$.

Ainsi $2^4 + 1 = 17$ est un nombre premier $8 + 1$, donc 17 divise $2^8 - 1$. De même, $2^6 - 3 = 61$ est un nombre premier $8 - 3$; donc 61 divise $2^{30} + 1$, ce qu'on vérifie ainsi :

$$2^6 \equiv 3, \quad 2^{12} \equiv 9, \quad 2^{24} \equiv 81 \equiv 20, \quad 2^{30} \equiv 2^6 . 2^{24} \equiv 60 \qquad (\text{mod. } 61).$$

[2] Cela résulte de l'identité suivante

$$(a^g + b^g)(a^{f-g} - b^{f-g}) + (a^g - b^g)(a^{f-g} + b^{f-g}) = 2(a^f - a^g) .$$

7. *Les nombres* u_k *et* v_k *n'ont d'autres facteurs communs que ceux de* Q, car on a :

$$v_k^2 - \Delta u_k^2 = 4Q^k \quad (4)$$

ce qui prouve en outre que u_{2k+1} divise $x^2 - Qy^2$.

8. u_k *et* v_k *sont premiers entre eux.* Autrement, comme $P^k - v_k$ est divisible par Q, tout diviseur de v_k et de Q diviserait P, qui est, par hypothèse, premier avec Q.

9. *Soit* $Q = 2q^2$; à cause de (3), v_{4k+2} *peut, dans ce cas, se décomposer en deux facteurs assignables :* c'est une généralisation de l'identité d'Aurifeuille.

10. *Il en est de même pour* v_{4k} *si* $\Delta = -f^2$, *ou si* $Q\Delta = -2f^2$ *pour* v_{4k+2}.

11. De même v_{2k} divise $x^2 + \Delta y^2$ *et* v_{2k+1} *divise* $x^2 + Q\Delta y^2$: d'où les formules linéaires de v_k.

Ed. Lucas considère particulièrement les quatre cas suivants :

$P = 3$, $Q = 2$, $a = 2$, $b = 1$, $\Delta = 1$, d'où les *séries de Fermat* $u_k = 2^k - 1$, $v_k = 2^k + 1$.

$P = 1$, $Q = -1$, $2a = 1 + \sqrt{5}$, $2b = 1 - \sqrt{5}$, $\Delta = 5$, d'où la *série de Fibonacci* 1, 1, 2, 3, 5, 8, ... $u_{k+1} = u_k + u_{k-1}$.

$P = 2$, $Q = -1$, $a = 1 + \sqrt{2}$, $b = 1 - \sqrt{2}$, $\Delta = 8$, d'où la série 1, 2, 5, 12, 29, 70, 167, ... $u_{k+1} = 2u_k + u_{k-1}$, qu'il nomme très improprement *série de Pell,* car d'une part Pell ne s'en est pas occupé, et d'autre part elle était connue bien avant lui. (Voir, par exemple, Théon de Smyrne.)

$P = 4$, $Q = 1$, $a = 2 + \sqrt{3}$, $b = 2 - \sqrt{3}$, $\Delta = 12$, d'où la série 2, 6, 14, 34, 82, 198, ... $v_{k+1} = 2v_k + v_{k-1}$, qu'on pourrait appeler *série d'Ed. Lucas.*

Ainsi, d'après **11**, les termes u_{2k+1} des suites de Fibonacci et de Théon, et les termes v_{2k} de celle de Fermat n'ont que des diviseurs premiers de la forme $4 + 1$; ceux des termes u_{2k+1}, de la suite de Fermat, et v_{2k+1} de celle de Théon sont de la forme 8 ± 1 ; etc.

12. D'après le théorème de Fermat, *si* a *et* b *sont entiers, c'est-à-dire si* Δ *est un carré,* u_{n-1} *est divisible par* n *quand* n *est premier et s'il ne divise ni* a *ni* b. Donc *si* u_n *est divisible par* p, n *est égal à* $p - 1$ *ou à un diviseur de* $p - 1$. Réciproquement *les nombres premiers qui divisent* u_n, *sans diviser aucun des termes précédents, sont de la forme* $nx + 1$.

De même *si* v_n *est le premier terme divisible par* p, p *est de la forme* $2nx + 1$.

13. *Si* a *et* b *sont irrationnels et réels,* $u_{p\pm1}$ *est divisible par* p *selon que* Δ *est un non-résidu ou un résidu*[1].

Donc *si* u_n *est divisible par* p, n *est divisible par* $p+1$ *ou par* $p-1$ *suivant les cas.*

14. *Le nombre* n *est premier si* $u_{n\pm1}$ *est divisible par ce nombre, sans qu'aucun des termes dont le rang est un diviseur de* $n\pm1$, *soit divisible par* n. Supposons n égal au produit des deux nombres premiers p et q; p divise u_k et q divise u_l, k et l désignant respectivement des multiples quelconques de $p\pm1$ et de $q\pm1$. Donc n divise $u_{(p\pm1)(q\pm1)}$. Or il divise $u_{pq\pm1}$ d'après l'énoncé; donc, en appelant f le plus grand des deux nombres $(p\pm1)(q\pm1)$, $(pq\pm1)$ et g le plus petit, n divise u_{f-g}: or $f-g<n$ conclusion contradictoire avec l'hypothèse; n est donc premier.

Cor. 1. *Nombres de Mersenne.* Soit $p=2^{4h+1}-1$; les diviseurs de $p+1$ sont les puissances de 2, de la première à la $(4h+1)^{\text{ème}}$. Mais $p=(2^{4h+1}+1)-2=\mathbf{3}+1$. Or p *est en même temps* $\mathbf{4}-1$, de même que 3; donc on peut écrire

$$\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right)=-\left(\frac{1}{3}\right)=-1$$

et 3 est non-résidu de p de même, en général, que $3v^2$.

Prenons la série d'Ed. Lucas, qui fournit $\Delta=3.2^2$; on aura

$$v_{2k}=v_k^2-2\ ,$$

et la série se calculera ainsi :

$$\begin{aligned} u_1&=1 & v_1&=4\\ u_2&=4u_1 & v_2&=14\\ u_4&=14u_2 & v_4&=194\\ u_8&=194u_4 & v_8&=37634\ . \end{aligned}$$

---

[1] Posons $m=\dfrac{p-1}{2}$, on aura :

$$\begin{aligned} 2^p u_{p+1}&=C_{p+1,1}P^p+C_{p+1,3}P^{p-2}\Delta+C_{p+1,5}P^{p-4}\Delta^2+\ldots+C_{p+1,1}P\Delta^m\\ &\equiv(p+1)(P^p+P\Delta^m)\equiv P^p+P\Delta^m\equiv P+P\Delta^m\ .\\ 2^{p-1}u_p&\equiv C_{p,1}P^{p-1}+C_{p,3}P^{p-3}\Delta+C_{p,5}P^{p-5}\Delta^2+\ldots+\Delta^m\\ &\equiv\Delta^m\ . \end{aligned}$$

Ainsi, si Δ est non-résidu, $u_p\equiv-1$ et $u_{p+1}\equiv0$. Comme on a :

$$Qu_{p-1}=Pu_p-u_{p+1}$$

on peut dire que si Δ est résidu, $u_p\equiv1$ et $u_{p-1}\equiv0$.

La première partie de ce théorème est de Lagrange, la seconde de Genocchi.

Considérons, par exemple, la série de Théon. Comme $\Delta=8$, on peut dire que Δ est résidu ou non-résidu selon que p est de l'une des formes 8 ± 1 ou de l'une des formes 8 ± 3; donc dans les mêmes cas, p divise u_{p-1} ou u_{p+1}.

Comme A est un non résidu, u_{p+1} est divisible par p. De là, cette règle : *calculer la suite de nombres* 1, 4, 14, 194, 37634, ... *dont chacun est égal au carré du précédent diminué de* 2 ; *le nombre* n *est premier si le* $(4h + 1)^{ème}$ *terme de cette suite est le premier qui soit divisible par* $n = 2^{4h+1} - 1$.

Au lieu de cette suite, on peut, puisque n est impair, employer la suivante 1, 2, 7, 97, 18817, ... dont chaque terme est égal au double du carré du précédent diminué de 1 [1].

II. *Nombres de Fermat.* Soit $p = 2^h + 1$, h désignant une puissance de 2. Si h est > 2, p est de la forme $8 + 1$ et 2 est résidu. Prenons la série de Théon ; $A = 8$ est résidu de p, et la série est

$$u_1 = 1 \qquad v_1 = 2$$

$$u_2 = 2u_1 \qquad v_2 = 6$$

$$u_4 = 6u_2 \qquad v_4 = 34$$

$$u_8 = 34u_4 \qquad v_8 = 1154 .$$

On a ainsi cette règle : *le nombre* n *est premier si le* $h^{ème}$ *terme de la série* 1, 3, 17, 577, ... *dont chacun est égal au double du carré du précédent* — 1 *est le premier qui soit divisible par* n [2].

III. *Réciproque du théorème de Fermat* [3]. *Si* $a^x - 1$ *est divisible par* n *pour* $x = n - 1$ *et non pour* $x < n - 1$, n *est premier.*

Soit $a = 3$, $n = 2^{16} + 1$; les diviseurs de $n - 1$ sont 1, 2, 4, 8, 16, ... et chaque reste s'obtient en divisant par n le carré du précédent, ce qui donne 3, 9, 81, 6561, — 11088, ... 1. Il n'y a aucun reste égal à 1 avant le dernier terme de cette suite : le nombre $2^{16} + 1$ est donc premier.

Comme le remarque Ed. Lucas, cette méthode se distingue des autres en ce qu'elle ne demande pas la construction préalable d'une table de nombres premiers, et qu'au lieu d'effectuer des divisions par des nombres différents, on divise, par un nombre fixe, différents nombres se déduisant les uns des autres par une loi très simple.

---

[1] Par exemple, soit $h = 1$, $n = 31$; on aura :

$$1 = 1,\ 2 \equiv 2,\ 7 \equiv 7,\ 97 \equiv 4.\ 2.4^2 - 1 \equiv 0 \qquad (\text{mod } 31)$$

donc 31 est premier.

[2] Ainsi soit $h = 3$, $n = 257$; on aura :

$$1 \equiv 1,\ 3 \equiv 3,\ 17 \equiv 17,\ 577 \equiv 63,\ 2.63^2 - 1 \equiv 227 \equiv -30,\ 2.30^2 - 1 \equiv 0 \quad (\text{mod } 257)$$

on a ainsi $u_{32} \equiv 0$: la question reste indécise.

[3] Trouvée presque en même temps par Proth (*C. R.*, t. 57).

15. Pour n impair, on a :

$$\delta^{n-1} u_k^n = u_{nk} + Q^k C_{n,1} u_{(n-2)k} + C_{n,2} Q^{2k} u_{(n-4)k} + \dots + \dots + C_{n,\frac{n-1}{2}} Q^{\frac{n-1}{2}k} u_k .$$

Comme u_{fg} est divisible par u_g et que $C_{p,g} \equiv 0$, on voit, en remplaçant n par le nombre premier p, que *si* u_k *est divisible par* p^l, u_{pk} *est divisible par* p^{l+1} *et non par une puissance supérieure.*

16. La série de Fibonacci étant celle dont les termes croissent le moins rapidement, Ed. Lucas l'a étudiée d'une façon particulière. Voici en résumé son étude.

Si $p = 5 \pm 1$, *le terme* u_{p-1} *de la série de Fibonacci est* $\equiv 0$, *et si* $p = 5 \pm 2$, *on a :* $u_{p+1} \equiv 0$. En effet :

1° Soit $p = 5 \pm 1$, on a : $p^2 = 5 + 1$ ou $p^{\frac{5-1}{2}} \equiv 1 \pmod 5$ ou bien $\left(\frac{p}{5}\right) = 1$, d'où $\left(\frac{5}{p}\right) = 1$, ou encore $5^m - 1 \equiv 0$. Or on a :

$$2^{p-2} u_{p-1} = C_{p-1,1} + 5C_{p-1,3} + \dots + 5^{m-1}$$
$$\equiv -(1 + 5 + 5^2 + \dots + 5^{m-1})$$

puisque $C_{p-1,k} + C_{p-1,k-1} = C_{p,k} \equiv 0$, d'où $C_{p-1,k} \equiv -C_{p-1,k-1} \equiv C_{p-1,k-2} \equiv \dots \equiv C_{p-1,1} \equiv -1$. On peut donc écrire

$$2^{p-2} u_{p-1} \equiv 1 - 5^m \equiv 0 .$$

2° Soit $p = 5 \pm 2$; on a : $p^2 = 5 - 1$ ou $\left(\frac{p}{5}\right) = -1$ d'où $\left(\frac{5}{p}\right) = -1$. Ainsi p divise $5^m + 1$. Or on a :

$$2^p u_{p+1} = C_{p+1,1} + 5C_{p+1,3} + \dots + 5^m \equiv 1 + 5^m \equiv 0 .$$

Cor. I. *Tout nombre premier* $p = 5 \pm 1$ *divise et divise seulement les termes* u_{kx}, k *désignant un certain diviseur de* $p - 1$. *Tout nombre premier* $p = 5 \pm 2$ *divise et divise seulement les termes* u_{kx}, k *désignant un certain diviseur de* $p + 1$. Par exemple, $u_{29} = 514229$ n'est divisible — puisque 29 est premier — par aucun des facteurs premiers contenus dans les termes précédents, et tous ses diviseurs sont de la forme 29 ± 1 ; d'ailleurs 29 étant un nombre impair, ces mêmes diviseurs sont $4 + 1$ et par suite il faut les chercher dans les deux formules $116 + 1$, 57 ; on arrive ainsi à conclure que ce terme est un nombre premier.

Réciproquement, *si* n *divise* $u_{n\mp1}$ *sans qu'on ait* u_k *divisible par* n *pour aucune valeur de* k *diviseur de* $n \mp 1$, n *est un nombre premier, qui est de la forme* $\mathbf{5} \pm 1$ *ou de la forme* $\mathbf{5} \pm 2$, *suivant le cas.*

II. La série $u_2, u_4, u_8, \ldots$ sert comme au n° **14**, dans la vérification des nombres premiers de Mersenne. Soit $n = 127$; on a :

$$\left.\begin{array}{l} v_2 \equiv 3\,,\ v_4 \equiv 3^2 - 2 \equiv 7\,,\ v_8 \equiv 7^2 - 2 \equiv 47\,,\ v_{16} \equiv 47^2 - 2 \equiv 48\,, \\ v_{32} \equiv 48^2 - 2 \equiv 16\,,\ v_{64} \equiv 16^2 - 2 \equiv 0\,. \end{array}\right\} \pmod{127}$$

Donc le nombre 127 est premier.

De même on trouve, suivant le module $2^{31} - 1$,

$$v_2 \equiv 3\,,\quad v_4 \equiv 7\,,\quad v_8 \equiv 47\,,\quad v_{16} \equiv 2207\,,\ \ldots$$

le reste zéro arrive à la trentième opération et pas avant : $2^{31} - 1$ est donc premier.

Soit $n = 2^{127} - 1$. Ce nombre est terminé par 7 : s'il est premier, il doit diviser u_{n+1} et un de ses facteurs doit diviser u_k, k désignant un facteur de $n + 1$, c'est-à-dire un nombre de la forme 2^x. Ce facteur serait un nombre premier $2^f \pm 1$ diviseur de n, ce qui est impossible puisque 127 est premier. Ed. Lucas a vérifié que n ne divise u_{2^h} que pour $h = 127$: donc, s'il ne s'est pas trompé dans ses calculs, n est premier.

17. On terminera par ces deux théorèmes analogues à ceux d'Ed. Lucas.

1° h *désignant une puissance de* 2, *pour que le nombre* $n = 2^h + 1$ *soit premier, il faut et il suffit que* $5^{\frac{n-1}{2}} + 1$ *soit divisible par* n.

En effet, pour $h > 2$, on a $n = \mathbf{5} = 2^{\,1}$, d'où $n^{\frac{5-1}{2}} = \mathbf{5} - 1$; donc $\left(\frac{n}{5}\right) = -1$, et, si n est premier, $\left(\frac{5}{n}\right) = -1$, c'est-à-dire que n divise $5^{\frac{n-1}{2}} + 1$.

Cette condition est suffisante : admettons en effet que n n'est pas premier et que p est un de ses diviseurs premiers ; on aura

$$(\alpha) \qquad 5^{\frac{n-1}{2}} + 1 \equiv 0 \qquad \text{d'où} \qquad 5^{n-1} \equiv 1\ ;$$

or $5^{p-1} \equiv 1$. Le p. g. c. d. de $n - 1$ et de $p - 1$ est une puis-

[1] En effet si on remplace la puissance h par la suivante, n devient $(n-1)^2 + 1$; ce qui fait voir que si $n = \mathbf{5} + 2$, il en est de même de la nouvelle valeur de n. Or pour $h = \mathbf{4}$, $n = 17 = \mathbf{5} + 2$. Il en est donc de même en général.

sance k de 2, donc $5^k \equiv 1$ [1], et comme $\frac{n-1}{2}$ est un multiple de k, on peut écrire $5^{\frac{n-1}{2}} \equiv 1$, ce qui est en contradiction avec (α). Le p. g. c. d. est donc n, et n est premier.

De là cette règle plus précise que celle d'Ed. Lucas : pour vérifier la *nature du nombre* n, *on formera la suite* $5, 5^2, 5^4, 5^8, 5^{16}, \ldots$ *dont chacun est le carré du précédent, en négligeant à mesure, les multiples de* n : *si le* $\left(\frac{n-1}{2}\right)^{\text{ème}}$ *terme divisé par* n *donne le reste* -1, n *est premier* [2]. (Pépin, *C. R.*, t. 85.)

2° *Pour que le nombre* $n = 2^h + 1$ *où* h *désigne une puissance de* 2, *soit premier, il faut et il suffit qu'il divise* $3^{2^{h-1}} + 1$ (Proth). Démonstration de M. Hurwitz. Supposons n un nombre premier p; comme $p = 4 + 1$, on a :

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1 \text{ [3]} ;$$

3 est donc non-résidu [4] et p divise $3^{2^{h-1}} + 1$.

Supposons maintenant que $3^{2^{h-1}} + 1$ soit divisible par le nombre n; on aura $3^{\frac{n-1}{2}} \equiv -1 \pmod{n}$; donc $n - 1$ est le plus petit exposant f pour lequel on ait $3^f \equiv 1 \pmod{n}$. Donc, d'après le théorème d'Euler, $n - 1$ divise $\varphi(n)$, ce qui ne peut avoir lieu que si $\varphi(n) = n - 1$, c'est-à-dire si n est premier.

Landry a fait connaître sa méthode définitive dans le vol. de l'*A. F.* de 1880. Elle est très élémentaire, très générale et a été le point de départ de tout ce qui a été fait depuis sur ce sujet.

Un nombre premier avec 6 est de l'une des formes 6 ± 1 et on peut le supposer pouvoir se décomposer ainsi :

$$(6x \pm 1)(6y \pm 1) \qquad \text{ou} \qquad (6x \pm 1)(6y \mp 1) .$$

---

[1] En effet, soit $A^{fd} \equiv A^{gd} \equiv 1$, et soit d le p. g. c. d. de fd et de gd; f et g sont premiers entre eux; on peut donc écrire $fx - gy = 1$, d'où, en posant $A^d \equiv \alpha$,

$$\alpha^{fx} \equiv \alpha^f \equiv 1 \equiv \alpha^g \equiv \alpha^{gy} \equiv \alpha^{1+fx} ;$$

donc $A^d \equiv \alpha \equiv 1$.

[2] Ainsi soit $h = 8$, $n = 257$, on a :

$$\left.\begin{array}{l} 5 \equiv 5,\ 5^2 \equiv 25,\ 25^2 \equiv 111,\ 111^2 \equiv -15,\ 15^2 \equiv -32,\ 32^2 \equiv -4 \\ 4^2 \equiv 16,\ 16^2 \equiv -1 \end{array}\right\} \pmod{257}$$

Donc 257 est premier.

[3] $2^{2f} + 1 = 2(2^{2f-1} + 1) - 1 = 3 - 1$.

[4] Tchebichef avait fait voir ainsi auparavant que, plus généralement, 3 est non-résidu de $p = 2^x + 1$.

Soit, par exemple,

$$n = 6a + 1 \qquad \text{et} \qquad a = 6q + r \ ;$$

posons

$$(\alpha) \qquad n = (6x + 1)(6y + 1) \qquad (x > y)$$

il viendra

$$(\beta) \qquad 6xy + x + y = a$$

$$(\gamma) \qquad x + y = 6z + r \qquad\qquad (\delta) \qquad xy = q - z$$

d'où, en éliminant x,

$$(\varepsilon) \qquad z = \frac{q - y(r - y)}{6y + 1} \ .$$

Quand z augmente, le plus petit y des deux nombres x et y diminue et le plus grand augmente[1]. La valeur supérieure de y étant $\frac{\sqrt{n} - 1}{6}$, cette valeur, mise dans (ε), donnera une limite supérieure de z. On essaie les valeurs entières de z jusqu'à cette limite; le nombre des essais est trente-six fois moindre que celui qu'exigerait la méthode classique, puisque $n > 36q$. On réduit encore ce nombre par différentes considérations sur les formes linéaires de x, y, z, r par rapport à différents nombres premiers.

Cette méthode a été grandement perfectionnée par MM. Barbette et Gérardin, comme on le verra plus loin.

Le P. Pépin (*Mem. acad. nuovi lincei,* 1880) a voulu faire profiter la méthode d'Euler des perfectionnements que Gauss a apportés à la théorie des formes; mais la moindre simplicité théorique et pratique qui en résulte rend ses procédés peu avantageux.

Il a aussi utilisé la théorie des racines primitives, pour le cas de $n = a^k - 1$: considérons le nombre premier p et soit $a^k \equiv \alpha$; si g est une racine primitive de p, on peut toujours poser $g^A \equiv \alpha$ et A est donné par le *Canon mathematicus* de Jacobi. Si $p - 1$ est un multiple de k, on peut ainsi écrire

$$g^{\left(\frac{p-1}{k}\right)A} - a \equiv 0$$

[1] A mesure que z augmente, xy diminue d'après (δ) et $x + y$ augmente, d'après (γ). Si x' et y' sont les nouvelles valeurs de x et de y correspondant à une valeur plus grande de z, on aura

$$(\zeta) \qquad xy > x'y' \qquad\qquad (\eta) \qquad x + y < x' + y' \ .$$

Elevant au carré (η) et ajoutant à l'inégalité $-4xy < -4x'y'$, il vient cette autre relation $x - y < x' - y'$, laquelle ajoutée à (η), donne $x' > x$, et, en comparant avec (ζ), $xyx' > x'y'x$, d'où $y > y'$.

et cette congruence indique par conséquent que n est divisible par p.

Il a montré comment on peut resserrer les limites des essais en mettant n sous la forme xy, $x > y$, et cherchant les valeurs de y inférieures à différentes limites l, l', ... ce qui renferme les valeurs $x + y$ entre les limites $2\sqrt{n}$ et $l + \frac{n}{l}$.

Lawrence (*Mes. of math.*, 1894, *Quart. J.*, 1896, et *Proceed.*, 1897), a donné, pour préciser les régions où peuvent se trouver des facteurs du nombre n, une méthode d'exclusion aussi simple qu'ingénieuse, et consistant dans l'examen des hypothèses faites sur la valeur de la somme des deux facteurs supposés de n ou d'un multiple de n. On peut l'exposer ainsi.

Posons $\mathrm{n} = \mathrm{xy}$, $2\mathrm{X} = \mathrm{x} + \mathrm{y}$, $\mathrm{x} > \mathrm{y}$. *Si on a :* $\mathrm{X} > \mathrm{a} > \sqrt{\mathrm{n}}$, *on a également cette autre relation*

$$x > a + \sqrt{a^2 - n} > \sqrt{n} > a - \sqrt{a^2 - n} > y \ [1] .$$

Cor. I. *Si aucune valeur de* X *n'est possible entre* a *et* $\sqrt{\mathrm{n}}$, *il n'y a aucun facteur de* n *entre* $\sqrt{\mathrm{n}}$ *et* $\mathrm{a} - \sqrt{\mathrm{a}^2 - \mathrm{n}}$. [2]

II. *Posons* $\mathrm{kn} = \mathrm{x'y'}$ *et* $2\mathrm{X'} = \mathrm{x'} + \mathrm{y'}$; *si aucune valeur de* X' *n'est possible entre* b *et* $\sqrt{\mathrm{kn}}$, *il n'y a aucun facteur de* kn *entre* $\mathrm{b} + \sqrt{\mathrm{b}^2 - \mathrm{kn}}$ *et* $\mathrm{b} - \sqrt{\mathrm{b}^2 - \mathrm{kn}}$, *et par conséquent aucun facteur de* n *entre*

$$\frac{\mathrm{b} + \sqrt{\mathrm{b}^2 - \mathrm{kn}}}{\mathrm{k}} \quad \text{et} \quad \frac{\mathrm{b} - \sqrt{\mathrm{b}^2 - \mathrm{kn}}}{\mathrm{k}} .$$

Par exemple, si n est $9 + 4$, x et y sont, l'un d'une des formes $9 + 1, 2, 5, 7$ et l'autre $9 + 4, 2, 8, 7$, d'où $2\mathrm{X} = 9 + 5, 4, 13, 14$ ou $9 + 14, 4, 4, 14$ et $\mathrm{X} = 9 + 2, 7$. Agissant de même avec d'autres modules, on connaîtra de nouvelles conditions que doit

---

[1] Cette relation est une conséquence de ce que : en premier lieu, on peut écrire

$$\sqrt{xy} \pm \sqrt{a^2 - xy} \gtrless a ,$$

comme on s'en assurera en élevant les deux membres au carré ; en second lieu, on a

$$x > \mathrm{X} > a > \sqrt{n} > y ;$$

et enfin, que de l'inégalité $x + y > 2\mathrm{X}$, on tire, en multipliant par x, puis par y, et ajoutant a^2 aux deux membres de chacune des deux inégalités ainsi produites, les deux suivantes

$$(x - a)^2 > a^2 - xy , \qquad (a - y)^2 > a^2 - xy .$$

[2] Ce corollaire peut s'énoncer ainsi : *posons* $\mathrm{x} - \mathrm{y} = 2\mathrm{Y}$; *si, jusqu'à la limite* $\mathrm{X} = \mathrm{a} > \sqrt{\mathrm{n}}$, *l'équation* $\mathrm{X}^2 - \mathrm{Y}^2 = \mathrm{n}$ *ne peut avoir lieu, on a* $\mathrm{y} < \mathrm{a} - \sqrt{\mathrm{a}^2 - \mathrm{n}}$. Par exemple, soit $n = 118007$; on peut rechercher directement ainsi la limite de X : on a $344^2 - n = 329$ et $2.344 + 1 = 689$; ajoutons successivement à 329 les termes de la progression 689, 691, 693, ... on obtiendra les valeurs des termes de la suite $344^2 - n$, $345^2 - n$, $346^2 - n$, ... $380^2 - n$, dont aucun n'est un carré. On peut écrire par conséquent $a = 380$, d'où $\mathrm{X} > 380$ et $y < 380 - \sqrt{380^2 - n} = 218$; on essaiera donc la division de n par les nombres premiers 213, 211, 219, ... dont le troisième réussit.

On a ainsi un perfectionnement notable de la méthode de Fermat.

remplir le nombre X, lesquelles serviront à déterminer, peu à peu, la limite a de ses valeurs possibles [1].

On comprend dès lors la construction et l'usage du tableau suivant, qu'on pourrait étendre autant qu'on voudrait.

Formes de n.	Formes de X.	Formes de n.	Formes de X.
3 + 1	**3** + 1, 2	**13** + 1	**13** + 0, 1, 2, 6, 7, 11, 12
2	**3**	2	1, 4, 5, 8, 9, 12
4 + 1	**2** + 1	3	0, 2, 4, 5, 8, 9, 11
3	**2**	4	0, 1, 2, 4, 9, 11, 12
5 + 1	**5** + 0, 1, 4	5	1, 2, 3, 10, 11, 12
2	1, 4	6	3, 4, 6, 7, 9, 10
3	2, 3	7	2, 4, 6, 7, 9, 11
4	0, 1, 3	8	2, 3, 5, 8, 10, 11
7 + 1	**7** + 1, 3, 4, 6	9	0, 3, 5, 6, 7, 8, 10
2	2, 3, 4, 5	10	0, 1, 3, 6, 7, 10, 12
3	0, 2, 5	11	1, 5, 6, 7, 8, 12
4	1, 2, 5, 6	12	0, 3, 4, 5, 8, 9, 10
5	0, 3, 4	**8** + 3	**4** + 2
6	0, 1, 6,	7	**4**
11 + 1	**11** + 1, 2, 4, 7, 9, 10	**9** + 1	**9** + 1, 8
2	0, 4, 5, 6, 7	4	2, 7
3	1, 2, 5, 6, 9, 10	7	4, 5
4	2, 3, 4, 7, 8, 9	**12** + 5	**6** + 3
5	3, 4, 5, 6, 7, 8	7	4
6	0, 2, 3, 8, 9	11	0
7	0, 1, 4, 7, 10	**15** + 2	**15** + 6, 9
8	0, 1, 3, 8, 10	8	3, 12
9	1, 3, 5, 6, 8, 10	11	0, 6, 9
10	0, 2, 5, 6, 9	14	0, 3, 12

[1] Soit le nombre déjà plusieurs fois traité $n = 4171$, qui est des formes **3** + 1, **5** + 1 et **7** + 6 : X doit être de l'une des formes **3** + 1, 2, de l'une de celles-ci **5** + 0, 1, 4 et de l'une de celles-ci **7** + 0, 1, 6. Le plus petit nombre à la fois de ces formes et supérieur à $\sqrt{n}$ est 70, ce qui donne la limite $70 - \sqrt{70^2 - n} = 43$. Essayant la division de n pour les nombres premiers 43, 41, 37, ... elle réussit avec le premier de ces nombres.

Soit $n = 4177 = \mathbf{3} + 1 = \mathbf{4} + 1 = \mathbf{5} + 2 = \mathbf{7} + 5$. Le plus petit nombre $> \sqrt{n}$ et appartenant à chacun des groupes de formes **3** + 1, 2; **2** + 1; **5** + 1, 4; **7** + 0, 3, 4; est 91. Ainsi il n'y a aucun facteur de n entre $\sqrt{n}$ et $91 - \sqrt{91^2 - n}$, ou entre 64 et 20. De même $11n$ est des formes **3** + 2, **4** + 3, **5** + 2, **7** + 4; donc X′ est **3**, **2**, de l'une des formes **5** + 1, 4 et de l'une des suivantes **7** + 1, 2, 5, 6. Le plus petit nombre $> \sqrt{11n}$ des formes possibles pour X′ est 246 : il n'y a pas par conséquent de facteurs de n entre les deux nombres

$$\frac{\sqrt{11n} \pm \sqrt{246^2 - 11n}}{11}$$

ou entre 30 et 9. Il reste donc les seuls nombres 7, 5 et 3 à essayer.

Voici un autre procédé assez pratique. Si $n = \mathbf{24} + 23$, on a $X = \mathbf{12}$. Si n n'est pas de cette forme, on la multipliera par 23, 19, 17, 13, 11, 7 ou 5, suivant qu'il sera de l'une ou de l'autre des formes **24** + 1, 5, 7, 11, 13, 17 ou 19, et on agira de même sur le produit, ce qui exclura pour X tous les nombres non multiples de 12. D'autres modules 5, 7, ... donneront de nouvelles exclusions.

Dans certains cas, on connaît une forme linéaire des facteurs, ce qui peut donner des moyens d'exclusion plus rapides. Ainsi, si on sait que x et y sont tous les deux $\equiv \alpha \pmod h$, en posant $x - y = 2Y$, il viendra

$$2X \equiv 2\alpha \quad \text{d'où} \quad X \equiv \alpha \quad \text{et} \quad Y \equiv 0 \pmod h$$

par suite, comme $X^2 - Y^2 = n$, $X^2 \equiv n \pmod{h^2}$.

Soit $n = 2^{2k+1} + 1$; n est de la forme $2u^2 + v^2$, et ses diviseurs sont donc de la forme $8 + 1$, ou de la forme $8 + 3$. Les deux facteurs x et y sont tous deux $8 + 1$ ou tous deux $8 + 3$; de là, la relation

$$X^2 = 64 + n = 64 + 1$$

si $k > 2$, et par suite

$$X = 32 \pm 1 \text{ [1]}.$$

Soit $n = 2^{2k+1} - 1$; n est de la forme $2u^2 - v^2$ et n'a par suite que des diviseurs de la forme 8 ± 1 : les diviseurs x et y sont donc l'un $8\xi + 1$ et l'autre $8\eta - 1$, d'où

$$n + 1 = 64\xi\eta + 8(\xi - \eta) \ ;$$

$\xi + \eta$ est de la parité de $\xi - \eta$ et par suite de celle de $\frac{n+1}{8}$; donc $2X = x + y = 8(\xi + \eta)$ est de la forme $n + 1 + 16 = 16$ et $X = 8$.

Ainsi les diviseurs de $n = 2^{71} - 1$ étant de la forme $71 + 1$, on a $2X = 71 + 2$ et $X = 71 + 1$. En outre, on a :

$$\left.\begin{aligned} X^2 &\equiv n = 1 + 4.71\ ^2 \\ X &\equiv \pm 1 + 2.71\ . \end{aligned}\right\} \pmod{71^2}$$

Il faut prendre $+ 1$, d'après ce qui précède, c'est-à-dire que X est $\equiv 143 \pmod{5041}$.

De plus, comme X est divisible par 8 et que n est des deux formes $9 + 4$ et $5 + 2$, X est également des deux formes 9 ± 2 et 5 ± 1.

Lawrence a en outre proposé la solution mécanique suivante : on représentera, à une même échelle, les valeurs de X sur des

---

[1] Si le nombre $H = ah^2 + 2bch + c^2$ est un carré parfait, avec b et $c < h$, la racine $\sqrt{H}$ est de la forme $zh^2 \pm bh + c$. Posons, en effet,

$$(\alpha) \qquad H = (zh^2 + sh + t)^2$$

s et t étant supposés $< h$, ce qui est toujours possible. On verra, en développant, que $c^2 - t^2$ doit être multiple de h, ce qui, à cause de c et $t < h$, demande qu'on ait $t = \pm c$.

Introduisant cette valeur de t dans (α) et simplifiant, il s'ensuivra que $bc - tn$ doit être divisible par h, ce qui conduit à la relation $s = \pm b$.

En particulier, si $ah + b^2$ est un carré parfait, avec $b < h$, sa racine est de la forme $zh \pm b$.

[2] $2^{16} = 3.13 + 71^2$, d'où $2^{35} \equiv 72 \pmod{71^2}$, $2^{70} \equiv 1 + 2.71$ (id.), $2^{71} - 1 \equiv 1 + 4.71$ (id.).

bandes de papier quadrillé faites une fois pour toutes ; soit deux bandes pour le module 3, quatre pour le module 5, dix pour le module 11, etc. On indiquera, par exemple, pour $X = 9 + 4$, les longueurs 0, 2, 3, 5, 7, 8, 10, 12, 13, ... Pour l'application, on n'aura qu'à aligner convenablement côte à côte les bandes correspondant aux diverses expressions demandées pour X, et à noter la première division se trouvant à la fois dans toutes les bandes ; le nombre ainsi déterminé donnera aisément la limite cherchée a.

MM. Kraïtchik et Gérardin ont réalisé et montré comme elle est pratique. (Voir *S. Œ.*, 1912, p. 62, ainsi que le compte rendu du Congrès de l'A. F. à Nîmes.)

Ce qu'on vient de dire de l'important travail de Lawrence n'en contient que le principe théorique. Pour les détails et les applications pratiques, voir les recueils cités ou la traduction française publiée en 1910, dans le *S. Œ.* de M. Gérardin.

M. Barbette (*M.*, 1899) met le nombre à factoriser sous la forme $100a + 10b + c$. Pour trouver les facteurs de forme $10x \pm 1$, il pose

$$100x^2 \pm 4(5b + c)x + (b^2 - 4ac) = y^2 ,$$

et pour trouver ceux de la forme $10x \pm 3$,

$$100x^2 \mp 4(5b - 4c)x + (b^2 + c^2 + 2bc + 36ac) = y^2 .$$

La question est ramenée à résoudre des équations de la forme $A^2x^2 + Bx + C = y^2$. Cette équation se résout, soit par la méthode de Gauss donnée plus haut, soit par tâtonnements, en éliminant en bloc les formes linéaires de x qui donnent, au premier membre, des valeurs pouvant se mettre sous l'une des formes inapplicables à un carré, $3 + 2$; $8 - 1, \pm 2, \pm 3$; 5 ± 2 ; $7 + 3, 5, 6$; etc. ; ce qui se trouve aisément, en faisant successivement $x = 3 + 0, 1, 2$; $5 + 0, 1, 2, 3, 4$; etc.

M. Gérardin (*S. Œ.*, 1906) a d'abord proposé d'écrire, suivant que n est $10 + 1, 3, 7, 9$ [1],

$$n = (10x \pm 1)(10y \pm 1) \quad \text{ou} \quad (10x + 3)(10y - 3)$$
$$n = (10x \pm 1)(10y \pm 3)$$
$$n = (10x \pm 1)(10y \mp 3)$$
$$n = (10x + 1)(10y - 1) \quad \text{ou} \quad (10x \pm 3)(10y \pm 3)$$

[1] On pourrait considérer les formes $12 \pm 1, \pm 5$, également au nombre de quatre et qui réduiraient encore le nombre des diviseurs à essayer.

soit $n = 100a + 10b + 1 = (10x + 1)(10y + 1)$, ce qui donne

$$10xy + x + y = 10a + b$$

$$x + y = b + 10z\ , \qquad xy = a - z$$

$$(\alpha) \qquad x^2 - (b + 10z)x + a - z = 0\ .$$

Le minimum de z et, en même temps, celui de $x + y$, sont déterminés par la relation connue $x + y > 2\sqrt{xy}$, dont le second membre est sensiblement égal à $2\sqrt{a}$ et qu'on représentera ainsi $10\alpha + \beta$. On posera donc :

$$b + 10z = 10\alpha + \beta\ .$$

Le minimum de z est donc égal à α puisque b et β sont des nombres < 10.

D'après cela, on résoudra l'équation (α) et on agira de même sur les formes $(10x - 1)(10y - 1)$ et $(10x + 3)(10y - 3)$.

Pour des nombres très grands, on décomposerait ainsi le nombre donné :

$$n = 120^2a + 120b + c = (120x + f)(120y + g)\ ,$$

c désignant l'un des trente-deux nombres inférieurs à 120 et premiers avec lui ; f et g deux nombres dont le produit est $\equiv c \pmod{120}$ [1]. On trouvera la liste des nombres c, f, g dans le t. III de *S. Œ.*

Ansi, par exemple, pour le nombre $n = 289524791$, on posera :

$$\begin{aligned} n = 20105.120^2 + 106.120 + 71 &= (120x + 7)(120y + 113) \\ &= (120x + 11)(120y + 61) \\ &= (120x + 13)(120y + 107) \end{aligned}$$

ce qui amènera autant d'équations de la forme $A^2x^2 + Bx + C = y^2$ à résoudre. L'examen des formes linéaires des coefficients amènera d'ailleurs de nombreuses exclusions dans ces équations. On réduira également le nombre des essais en cherchant, par divers moyens, les limites supérieures ou inférieures de x, soit fixes,

---

[1] En général, posons

$$\begin{aligned} n &= (ax + \xi)(ay + \eta) = a^2xy + a(\xi y + \eta x) + \xi\eta \\ &= a^2A + aB + C\ . \end{aligned}$$

a, B, C sont donnés. Le nombre C est congru à un des $\varphi(a)$ nombres inférieurs à a et premiers avec lui. Faisons $\xi\eta \equiv n - C \pmod{a}$, prenons pour ξ un quelconque f de ces mêmes nombres ; η en sera un autre g, et on pourra poser :

$$aA + B \equiv axy + fy + gx\ , \quad fy + gx \equiv B \qquad \text{d'où} \qquad x \text{ et } y\ .$$

On aura à résoudre $\varphi(a)$ équations de ce genre.

soit obtenues en resserrant de plus en plus l'intervalle à examiner. Ainsi, soit à déterminer les valeurs de x supérieures à B et à C; on a, comme on peut le vérifier aisément,

$$\frac{B+1}{2A} > y - Ax > \frac{B}{2A+1}.$$

Or y est de la forme $Ax + D$, D étant $< x$. On a donc de la sorte circonscrit une région dans laquelle doit se trouver D; de là x, en égalant $A^2x^2 + Bx + C$ au carré de $Ax + D$.

On trouvera du reste dans ce recueil de nombreux et intéressants exemples de cette méthode, ainsi que des aperçus de toutes sortes sur la conduite des calculs auxquels conduit le difficile problème qui fait l'objet de la présente étude, laquelle a été entreprise comme une application de la théorie élémentaire des nombres, et comme suite aux articles de l'*Ens. math.* sur le même sujet publiés en 1907 (p. 24, 286 et 417), en 1909 (p. 329 et 430), en 1910 (p. 457) et 1911 (p. 187).

A. Aubry (Dijon).

SUR QUELQUES PROBLÈMES CONCERNANT LE JEU DE TRENTE ET QUARANTE

Les problèmes fondamentaux concernant le jeu de trente et quarante ont été traités pour la première fois, à ma connaissance du moins, par Poisson en 1820, dans un beau mémoire inséré dans le t. 16 des *Annales math. de Gergonne.* Quarante-sept ans plus tard le géomètre allemand Œttinger retrouvait en les complétant en plusieurs points la plupart des résultats donnés par Poisson; mais son travail, inséré dans le t. 67 du *Journal de Crelle* et cité par H. Laurent dans son traité du *Calcul des Probabilités,* semble avoir passé inaperçu.

Bien que les déductions de Poisson et d'Œttinger présentent des lacunes, je n'aurais pas cru utile de revenir sur ce sujet, si Bertrand, en traitant dans son Calcul des Probabilités l'un des problèmes déjà résolus dans les mémoires cités, n'était arrivé à des résultats ne concordant pas entièrement avec ceux d'Œttinger et de Poisson; le désaccord n'est pas grand, il est vrai, mais il existe, et cela suffirait pour justifier une étude nouvelle.

Il était facile de refaire les calculs, dans le cas particulièrement simple envisagé par Bertrand. Je dirai tout de suite qu'un certain