Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 11 (1909)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: L'ŒUVRE ARITHMÉTIQUE D'EULER
Autor: Aubry, A.
DOI: https://doi.org/10.5169/seals-11866

L'ŒUVRE ARITHMÉTIQUE[1] D'EULER

Recte facta refert : orientia tempora notis
Instruit exemplis. HORAT.

Par *Théorie des nombres,* on entend l'*Arithmétique*, qui classe les nombres et étudie leurs propriétés générales ; et l'*Analyse indéterminée,* qui enseigne la manière de déterminer[2] les nombres jouissant de propriétés données. La première est plutôt théorique ; la seconde est une application des principes les plus simples de la première : elle demande moins de profondeur, mais plus de souplesse d'esprit que celle-ci.

FERMAT a excellé dans l'une et dans l'autre, comme on peut en juger d'après les quelques écrits qui nous restent de lui. Mais c'est surtout aux spéculations arithmétiques qu'il a ouvert de nouvelles voies, — particulièrement les *congruences exponentielles,* ainsi que la considération des *formes* des diviseurs numériques et des nombres premiers, — et donné une méthode puissante de démonstration, celle de la *descente infinie.* En outre, à défaut d'exposition ou d'application de ses théories, on lui doit d'avoir par ses préceptes, fait comprendre la nécessité d'une rigueur qu'on ne connaissait plus guère depuis les Anciens, en arithmétique surtout, et de remplacer, par des raisonnements en règle, les démonstrations fondées sur l'induction[3].

Les merveilles révélées au monde savant par la découverte

---

[1] Ce serait également une œuvre fort utile que l'exposé historique de l'analyse indéterminée, particulièrement des nombreux artifices, aussi variés qu'ingénieux, employés par Diophante, Fermat, Euler et autres. Mais nous avons dû nous borner cette fois à l'arithmétique.

[2] C'est avec intention que ce mot est rapproché de l'expression « *analyse indéterminée* », laquelle est tout à fait impropre : le problème de trouver les racines entières et positives de $ax - by = c$, par exemple, est effectivement aussi déterminé que celui de la recherche des racines de $ax^2 + bx + c = 0$.

[3] « Ce qui se déduit par comparaison en géométrie n'est pas toujours véritable... Telle règle bonne à quelques cas particuliers, n'est pas universelle. Elle peut être fort utile, mais non pour fondement de quelque science, car alors on ne doit se contenter de rien moins que d'une démonstration. » (Lettre à Digby, 1657).

et les applications du calcul infinitésimal, — découverte à laquelle Fermat avait eu d'ailleurs une si large part, — ne permettaient guère de prendre garde à une théorie qui ne paraissait susceptible d'aucune application pratique, et d'ailleurs vaguement indiquée dans des lettres et des notes qui n'étaient pas destinées à la publicité. Aussi n'y eut-il que de BILLY, OZANAM, LEIBNIZ, WOLFF, GOLDBACH, JACQUEMET, PRESTET et quelques autres, qui aient, avant EULER, accordé quelque attention aux découvertes arithmétiques de FERMAT.

EULER, qui avait employé ses prodigieuses facultés à perfectionner, agrandir et enrichir de précieuses découvertes, toutes les parties de la science mathématique, ne pouvait manquer d'explorer les nouvelles régions ainsi offertes aux investigations des savants. Il s'aperçut bientôt de la beauté et de l'importance des théorèmes de Fermat, et s'appliqua à les démontrer, à les généraliser et à en dégager les principes. Ce fut l'origine, et en grande partie, l'objet de ses nombreux travaux sur l'Arithmétique, dont l'histoire va nous occuper.

(C[1], 1732). — Il montre l'inexactitude d'une proposition de Fermat (E. M.[2] 1907, p. 444) ; donne les diviseurs des nombres $2^{29} - 1$, $2^{43} - 1$, $2^{73} - 1$; exprime le *théorème de Fermat* sous deux formes qui reviennent à l'interprétation des *congruences*.

$$(1) \qquad a^{p-1} - b^{p-1} \equiv 0 \ , \quad a^{p-1} - 1 \equiv 0 \ ^{3} \ ;$$

et donne divers théorèmes qu'on peut reproduire ainsi :

$$(2) \qquad a^{p^k(p-1)} \equiv 1 \qquad (\text{mod } p^k) \ ;$$

$$(3) \qquad a^n \equiv 1 \ (\text{mod } pp'p''\ldots) \ , \quad (h, \text{ p.g.c.d. de } p-1, p'-1, \ldots) \ ;$$

$$(4) \qquad 3^m \equiv \mp 1, \text{ selon que } p = \mathbf{12} \pm 5 \text{ ou } \mathbf{12} \pm 1, \left(m = \frac{p-1}{2}\right),$$

ainsi que la forme $\mathbf{24} + a$ des diviseurs de $3^m \pm 2^m$.

(Id.). — Méthode pour ramener la solution de $ax^2 + bx$

[1] *Commentarii Academiæ Petropolitanæ.*

[2] *Enseignement Mathématique.* Cette proposition lui avait été signalée par Goldbach, en 1727.

[3] Nous sous-entendons le *module* premier indéterminé p.

$+ c = y^2$ à celle de l'*équation de Pell*, $x^2 - ky^2 = 1$. Liste des solutions de celle-ci, jusqu'à $k = 68$.

(C, 1734). La théorie algébrique des fractions continues et leur emploi dans l'analyse indéterminée sont dus à Euler, qui a montré leur usage pour la solution des équations simultanées

$$x \equiv a \pmod{k} \ , \quad x \equiv b \pmod{l} \ .$$

(C, 1736). — Il démontre le théorème de Fermat, en partant du développement de $(1 + a)^p$, (E. M. 1907, p. 439), et lui donne cette forme plus générale

$$a^p - a \equiv 0 \ . \tag{5}$$

(C, 1738). — Il fait voir ainsi, en appliquant la méthode de la *descente infinie*, l'impossibilité de l'équation $x^4 + y^4 = z^2$. On peut supposer x, y, z premiers entre eux. On verra aisément que ces trois nombres ne peuvent être tous trois impairs et que z ne peut être pair ; d'où il suit que y par exemple doit être pair et x impair. Puisque les nombres x^2, y^2, z forment un *triangle* [1], on peut écrire :

$$x^2 = a^2 - b^2 \ , \quad y^2 = 2ab \ ,$$

a et b étant premiers entre eux ; a et b sont donc des carrés. Or x, b, a est un autre triangle ; on peut donc poser :

$$a = a'^2 + b'^2 \ , \quad b = 2a'b' \ .$$

$2b = 4a'b'$ est un carré ainsi que $a'b'$; mais a' et b' sont premiers entre eux, donc a' et b' sont des carrés, a''^2 et b''^2. On peut donc écrire $a''^4 + b''^4 = a$, et ce dernier est un carré : on a de la sorte une égalité semblable à la proposée, mais en termes plus petits.

De là le théorème et plusieurs autres du même genre [2].

(C. 1744). — Fermat avait enseigné que *les diviseurs premiers de* $a^2 + b^2$ *sont de la forme* $4 + 1$, a *et* b *étant supposés*

---

[1] E. M. 1907, p. 417.

[2] Entre autres, cette proposition de Fermat : *l'aire d'un triangle rectangle ne peut être représentée par un carré*. Il faut faire voir que $(X^2 - Y^2)XY$ ne peut désigner un nombre carré. Autrement, comme on peut supposer X et Y premiers entre eux, X et Y seraient des carrés x^2 et y^2, de même que $X^2 - Y^2$. On est ramené à faire voir que $x^4 - y^4$ ne peut représenter un carré.

premiers entre eux[1]*; que les nombres premiers* $4 + 1$ *sont de la forme* $x^2 + y^2$; et quelques autres théorèmes analogues. Euler donne, sans démonstration, les formules linéaires, — probablement trouvées par induction, — des diviseurs de $x^2 + py^2$ jusqu'à $p = 19$; celle des diviseurs de $ax^2 + by^2$ pour $ab = 6, 10, 14, 15, 21, 22, 30, 33, 35$; et d'importantes remarques, dont les suivantes :

les diviseurs de $x^2 + py^2$ *sont de l'une des formes* $4ph + a$, $2ph + a$;

les formules $ax^2 + by^2$ *et* $x^2 + aby^2$ *ont les mêmes diviseurs, de même que* $x^2 + ay^2$ *et* $x^2 + a$.

(C, 1748). — Il présente d'une manière plus générale sa démonstration du théorème de Fermat, et en déduit les corollaires suivants :

$$(6) \qquad (a + b)^p - a^p - b^p \equiv 0 \; ; \quad (a + b)^p - a - b \equiv 0 \; ;$$

$a^2 + b^2$ *ne peut avoir de diviseurs premiers de la forme* $4 - 1$. (E. M. 1907, p. 31[2];) *tout diviseur de* $a^4 + b^4$ *est de la forme* $8 + 1$[3]; *tout diviseur de* $a^8 + b^8$ *est de la forme* $16 + 1$; etc.

De là, la vérification de la divisibilité de $2^{32} + 1$ par 641. (E. M. 1907, p. 444) ;

Si $a^k - b^k \equiv 0$ et que f soit le p. g. c. d. de $p - 1$ et de k, $a^f - b^f \equiv 0$;

Si $a^1 \equiv r$, $r^m \equiv 1$, remarque déjà faite par Fermat ;

Si $a^k \equiv r$, $r^{\frac{p-1}{k}} \equiv 1$; de là, la considération des résidus de degrés supérieurs ;

Si $af^k \equiv b^k$, $a^{\frac{p-1}{k}} \equiv 1$;

Si $af^k \equiv bg^k$, $a^{\frac{p-1}{k}} \equiv b^{\frac{p-1}{k}}$.

(*Introd. in anal. inf.* Lausanne, 1748). Une des grandes découvertes d'Euler est sa méthode *de partitione numerorum*, dont l'étude lui fut proposée par Naudé. Il s'agit de déterminer le nombre de manières dont un entier donné peut

[1] Cette condition sera toujours sous-entendue pour toute expression de la forme $x^2 + ky^2$.

[2] Cette démonstration avait été communiquée à Goldbach, en 1742. (Voir Fuss. *Corresp. phys. et math.* Pétersbourg, 1843, t. I, p. 116).

[3] Communiqué à Goldbach, en 1743, (Fuss, op. cit., p. 264).

être considéré comme somme d'entiers positifs. La solution d'Euler repose sur cette remarque que *le terme en* x^k *dans le développement du produit*

$$\frac{1}{(1-x^a)(1-x^b)\dots(1-x^c)} = (1+x^a+x^{2a}+\dots)\dots(1+x^c+\dots)$$

a pour coefficient le nombre des solutions de l'équation $ax+by+\dots+cz=n$. De même, *les coefficients de* $z^h x^k$ *dans ceux des deux expressions.*

$$(7)\qquad (1+xz)(1+x^2z)(1+x^3z)\dots,\quad \frac{1}{(1-xz)(1-x^2z)\dots}$$

indiquent de combien de manières le nombre k *peut être formé par l'addition de* h *nombres inférieurs à* k, *différents dans le premier cas, différents ou égaux dans le second.*

Cette théorie, — première application des séries à la théorie des nombres, — nécessiterait en pratique des calculs inextricables ; mais elle conduit à des théorèmes remarquables d'un genre absolument nouveau, tels que le suivant : *le coefficient de* x^k *dans la première des expressions*

$$\frac{1}{(1-x)(1-x^2)\dots(1-x^h)},\quad \frac{1}{(1-x)\dots(1-x^k)}$$

étant le même que celui de x^h *dans la seconde, il s'ensuit qu'il y a autant de manières de décomposer* $k+h$ *en* h *parties que de former* k *en ajoutant des entiers plus petits que* h. Euler donne d'ailleurs des tables étendues de ces décompositions.

Elle l'a également conduit aux remarquables développements en séries [1]

$$(8)\qquad \Sigma\frac{x^{\frac{k(k+1)}{2}}z^k}{(1-x)(1-x^2)\dots(1-x^k)},\quad \Sigma\frac{x^k z^k}{(1-x)\dots(1-x^k)},$$

[1] Au moyen du procédé suivant, employé pour la première fois par Stirling (*Methodus differentialis*, Londres 1730) : faisons

$$F(a)\,F(a+h)\,F(a+2h)\,F(a+3h)\dots = A+Ba+Ca^2+Da^3+\dots$$

on déterminera les coefficients A, B, C, ... en changeant a en $a+h$, ce qui donnera

$$A+B(a+h)+C(a+h)^2+\dots = (A+Ba+Ca^2+\dots)\,F(a)$$

Ainsi pour $F(a+kh)=1+za^k$, on a la première expression (7).

des expressions (7), ainsi qu'aux suivants :

$$\Pi\left(1+\frac{1}{p^k}\right)=1+\Sigma\,\frac{1}{a^k}\,, \tag{9}$$

$$\Pi\,\frac{1}{1-\frac{1}{p^k}}=1+\Sigma\,\frac{1}{b^k}\,, \tag{10}$$

p désignant tous les nombres premiers, a tous les entiers non multiples de puissances, b les entiers 1, 2, 3, ... Dans (8) k prend les valeurs 1, 2, 3, ... ; dans (9) et (10), il a une valeur fixe.

$$(1+a)(1+a^2)(1+a^4)(1+a^8)\ldots=\frac{1}{1-a}\,, \tag{11}$$

$$\left\{\begin{array}{l}(a^{-1}+1+a)(a^{-3}+1+a^3)(a^{-9}+1+a^9)\ldots\\ =1+(a+a^2+a^3+\ldots)+(a^{-1}+a^{-2}+a^{-3}+\ldots)\,,\end{array}\right. \tag{12}$$

$$(1-a)(1-a^2)(1-a^3)\ldots=\Sigma(-1)^x a^{\frac{(3x-1)x}{2}}+\Sigma(-1)^x a^{\frac{(3x+1)x}{2}}\,[1] \tag{13}$$

Les formules (11) et (12) démontrent cette propriété de tout entier d'être représentable par les deux formules

$$a+2a+4a+8a+\ldots\,,\quad b+3b+9b+27b+\ldots$$

a pouvant prendre les valeurs 0 ou 1, et b, les valeurs — 1,0, ou 1. Pour $k=1$, (10) montre que les nombres premiers forment une suite illimitée.

Ces idées ont donné lieu de la part de Gauss, Legendre et surtout Jacobi, à d'importantes découvertes. Lejeune-Dirichlet et Rieman ont tiré de (10) des conséquences extrêmement importantes.

Ajoutons qu'on doit voir l'origine des *clés algébriques*

---

[1] Les exposants de a sont les *nombres pentagones*. Euler avait communiqué ce développement à D. Bernouilli en 1741, et à Goldbach en 1746, ceux des expressions

$$\Pi(1+a^{2^x})\,,\quad \Pi(1-a^{2^x})\,,\quad \Pi(1-n^x a)\,.$$

Jacobi écrit ainsi le second membre de (13) :

$$\sum_{-\infty}^{\infty}(-1)^x a^{\frac{(3x+1)x}{2}}\,.$$

(Cauchy) et des *nombres complexes* (Gauss) dans la démonstration élémentaire de la *formule de Moivre*, donnée dans le même ouvrage, démonstration fondée sur le développement du produit $(\cos a + i \sin a)(\cos b + i \sin b)$, dans lequel on égale séparément les parties réelles et les parties imaginaires.

(*Opuscula varii argumenti*, Berlin, 1750). La théorie des nombres amiables a été pour Euler l'occasion de découvrir les importantes formules

$$f(ab) = (f\,a)\,(f\,b)\ , \tag{14}$$

$$f(a^k) = \frac{a^k - 1}{a - 1}\ ^1 \tag{15}$$

(N. C.[2], 1752). *Si* a *et* b *sont deux sommes de deux carrés, il en est de même de* ab[3]. *Il en est de même de* b *si* ab *et* a *sont des sommes de deux carrés, et inversement.*

Si k *divise* $a^2 + b^2$, *on peut trouver* x *et* y *tels que* $x^2 + y^2$ *soit* $< \frac{1}{2} k^2$ [4], *et de là il suit que tous les diviseurs de* $a^2 + b^2$ *sont des sommes de deux carrés*[5].

La démonstration de ce théorème de Fermat : *tout nombre premier de la forme* 4h + 1 *est une somme de deux carrés* se ramène à faire voir qu'on peut toujours trouver x et y tels que la congruence $x^{2h} - b^{2h} \equiv 0$ soit impossible[6] ; car si cela a lieu, on peut écrire $x^{2h} + y^{2h} \equiv 0$, puisque $x^{4h} - y^{4h} \equiv 0$.

Un nombre $n = 4 + 1$, *qui ne peut se décomposer que d'une seule manière en une somme de deux carrés est premier*. En

---

[1] Les *Cogitata* de Mersenne, les *Exercit. géom.* de Schooten, les *Lettres* de Descartes et l'*Algebra* de Wallis montrent que Fermat et les géomètres contemporains connaissaient l'équivalent de ces deux formules. On voit la seconde exprimée explicitement par Kraft en 1749 (N.C.).

[2] *Novi Commentarii Academiæ Petropolitanæ.*

[3] Théorème de Fibonacci, retrouvé par Fermat et Euler (Voir Fuss, op. cit. p. 313, lettre à Goldbach, de 1715).

[4] On remplace a et b par les multiples de k qui se rapprochent le plus de ces deux nombres.

[5] Démonstration communiquée à Goldbach en 1747 (Fuss. op. cit., p. 418), ainsi que les suivantes.

[6] Lors de la publication de ce mémoire, Euler savait démontrer cette proposition ; car dans une lettre à Goldbach de 1749 (Fuss, op. cit., p. 496), il remarque que tous les nombres $2^m - 1$, $3^m - 2^m$, $4^m - 3^m$, ... ne sont pas tous $\equiv 0$, car leur différence m^e. qui est égale à $m\,!$ n'est pas $\equiv 0$.

effet s'il est composé, il est de la forme $(a^2 + b^2)(c^2 + d^2)$, d'où successivement,

$$n = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$$

$$ac + bd = ad + bc \quad \text{ou bien} \quad ac + bd = ad - bc \ ;$$

ce qui donne

$$a = b \quad \text{ou} \quad c = d \ ,$$

ou bien

$$b = 0 \ , \quad c = 0 \ .$$

Dans le premier cas l'un des nombres $a^2 + b^2$, ou $c^2 + d^2$ est pair et ne peut diviser le nombre impair n. Dans le deuxième cas, $n = (ac)^2 + (ad)^2$ ou $(ac)^2 + (bc)^2$: n ne serait donc pas la somme de deux carrés premiers entre eux.

Ainsi, à l'aide de calculs faciles[1], Euler trouve que le nombre 82421 est seulement la somme des deux carrés $25^2, 286^2$: Il est donc premier.

Réciproquement, si

$$n = \alpha^2 + \beta^2 = \gamma^2 + \delta^2 \ ;$$

posons

$$\alpha = \gamma + x \ , \ \delta = \beta + y \ ,$$

il viendra :

$$2\gamma x + x^2 = 2\beta y + y^2 = xyz \ ,$$

d'où

$$2\gamma = yz - x \ , \ 2\beta = xz - y \ , \ 2\alpha = yz + x \ , \ 2\delta = xz + y \ ,$$

et par suite

$$4n = (x^2 + y^2)(1 + z^2) \ .$$

On trouve ainsi les facteurs de n : posons

$$\alpha = ac + bd \ , \ \beta = ad - bc \ , \ \gamma = ad + bc \ , \ \delta = ac - bd \ ,$$

on aura, par exemple,

$$\frac{\gamma - \beta}{\alpha - \delta} = \frac{c}{d} \ .$$

On simplifiera la fraction, ce qui donnera le diviseur

[1] On calcule les carrés successifs à l'aide de leurs différences secondes.

$c^2 + d^2$. Soit à décomposer le nombre $1000009 = 1000^2 + 3^2 = 235^2 + 972^2$; on a :

$$\frac{1000 - 972}{235 - 3} = \frac{2}{17} .$$

Le nombre proposé est donc divisible par $2^2 + 17^2$ [1].

(1752 [2], N. C. 1754). Euler donne ces curieuses formules, trouvées par induction [3].

$$(16) \qquad \Sigma \frac{xa^x}{1 - a^x} = \Sigma x \int x \ ,$$

$$(17) \qquad \int a = \Sigma(-1)^x \int \left[a - \frac{(3x-1)x}{2}\right] + \Sigma(-1)^x \int \left[a - \frac{(3x+1)x}{2}\right].$$

(N. C. 1754). *Si* $k < p - 1$, *la congruence* $Ax^k + Bx^{k-1} + \ldots + M \equiv 0$ *ne saurait être satisfaite pour toutes les valeurs* 1, 2, 3, ... $p - 1$ *de* x. La démonstration d'Euler utilise la théorie des différences. (Voir E. M. 1907, p. 295). De là, il suit que la congruence $x^m - a^m \equiv 0$ a toujours des non-racines, ce qui complète la démonstration du théorème de Fermat rappelée plus haut.

Tout nombre premier p *a* $m = \frac{p-1}{2}$ *résidus* [4].

Le produits de deux non-résidus est congru à un résidu. Le quotient, s'il est entier, de deux résidus est un résidu. Le produit d'un résidu par un non-résidu est un non-résidu.

A chaque résidu r *correspond un résidu* $-r$, *si* -1 *est résidu,* ce qui a lieu uniquement quand $p = 4 + 1$, et alors on peut écrire $a^2 \equiv r$, $b^2 \equiv -r$, d'où $a^2 + b^2 \equiv 0$.

Aucun nombre $4 - 1$, *ne peut diviser* $a^2 + b^2$.

Aucun nombre de la forme $4xy - x - y$ *ne peut être un*

---

[1] Communiqué à Goldbach en 1747 (Fuss, op. cit. p. 419).

[2] La première date est celle de la divulgation ; la seconde, celle de la publication.

[3] Les formules (13) et (17) avaient été communiquées par Euler à divers savants dès 1747. C'est probablement la formule (16) qui a donné à Lambert l'idée de sa célèbre série

$$\Sigma \frac{a^x}{1 - a^x} = \Sigma \theta(x) a^x$$

$\theta(x)$ désignant le nombre des diviseurs de x, y compris x (1771).

[4] Les noms de *résidu* (residuum) et de *non-résidu* (non-residuum) sont dus à Euler, ainsi que la notion du *reste minimum* (complementum residui) — a, pour $p - a$, quand $p - a > \frac{p}{2}$.

carré ; car, d'après ce qui vient d'être dit, on ne saurait avoir $(4x - 1)(4y - 1) = z^2 + 1$. Cette remarque fut proposée à Goldbach par Euler, en 1741. Elle donne lieu à de nombreuses conséquences. (Voir Fuss, op. cit., pp. 107 et seq.).

Si $p = 4 - 1$, *on peut trouver un résidu* r *tel que* $r + 1$ *soit non-résidu, et par suite* p *divise une somme de trois carrés* (E. M. 1907, p. 31).

Le produit de deux sommes de quatre carrés est une somme de quatre carrés[1].

De ces deux dernières propositions, Euler déduit que la démonstration du *théorème de Bachet* revient à faire voir que *les diviseurs d'une somme de quatre carrés sont eux-mêmes des sommes de quatre carrés,* ce qui a été démontré plus tard par Lagrange[2].

(Id.) Euler revient sur les formules (13) et (17) et les démontre, la première, à l'aide de l'identité suivante, communiquée à Goldbach, en 1750 (Fuss, op. cit., p. 522),

$$(18)\quad (1+a)(1+b)(1+c)\ldots = 1 + a + b(1+a) + c(1+a)(1+b) + \ldots ;$$

et la seconde, en partant de (16) : le premier membre étant multiplié par $-\frac{da}{a}$, puis intégré, ensuite transformé au moyen de (13), enfin différentié et divisé par $-\frac{da}{a}$, on trouve :

$$(19)\quad \frac{a + 2a^2 - 5a^5 - 7a^7 + 12a^{12} + \ldots}{1 - a - a^2 + a^5 + a^7 - a^{12} - \ldots} = a\int 1 + a^2 \int 2 + \ldots$$

---

[1] Euler a communiqué cette célèbre identité à Goldbach en 1748. (Fuss, op. cit., p. 452).

[2] Euler s'était approché de cette démonstration de Lagrange. Dans une lettre à Goldbach, de 1749 (Fuss, op. cit., p. 496), il montre que si $a^2 + b^2 + c^2 + d^2$ est un multiple de p, en posant $a = Ap + \alpha$, ..., avec $\alpha < \frac{p}{2}$, ... le nombre $\alpha^2 + \ldots$ sera un multiple de p et de plus on aura $\alpha^2 + \ldots < 4\frac{p^2}{4} = p^2$, d'où, en posant

$$(\alpha)\qquad \alpha^2 + \ldots = hp ,$$

$hp < 4\frac{p^2}{4}\, p^2$ et $h < p$. Euler s'arrête là.

Le reste se démontre ainsi d'après Lagrange : h divisant $\alpha^2 + \ldots$, il divise également

$$(\beta)\qquad (\alpha - \lambda h)^2 + (\beta - \mu h)^2 + \ldots = hj .$$

Si on prend λ, μ, ... de manière que chacun des nombres $\alpha - \lambda h$ soit $< \frac{h}{2}$, il viendra $j < h$. Or le produit des deux égalités (α) et (β) en donne une autre, de la forme $(h\alpha')^2 + \ldots = jh^2 p$, ou bien $\alpha'^2 + \ldots = jp$, analogue à (α) mais avec $j < h$. Opérant de même, on trouvera une suite décroissante $h, j, k, l, \ldots$ qui s'arrêtera au terme 1.

d'où (17), en multipliant par $1 - a - a^2 + a^5 + \ldots$ et égalant les diverses puissances de x. C'est là le premier exemple de l'emploi, en Arithmétique, du Calcul infinitésimal, qui devait y produire tant de belles découvertes, à la suite des travaux de Jacobi et de Lejeune-Dirichlet.

(1754, N. C. 1756). Propositions et applications analogues à celles rappelées plus haut (N. C. 1752), aux nombres de la forme $x^2 + 2y^2$, avec la liste de ces nombres et leur décomposition jusqu'à 499, continuée plus tard par Jacobi, jusqu'à 5953.

(Id.) Etude des équations $x^3 + y^3 + z^3 = w^3$ et $x^3 + y^3 = v^3$, avec la table des nombres de la forme $x^2 + 3y^2$ inférieurs à 1000, table poussée par Jacobi jusqu'au nombre 12007. On y trouve aussi cette remarquable identité

$$(20) \qquad k(fla + gb)^2 + l(kfb - ga)^2 = (g^2 + klf^2)(la^2 + kb^2) \ .$$

(N. C. 1758). Seconde démonstration du théorème de Fermat, qu'il préfère de beaucoup à la première, parce qu'elle repose sur la seule considération des puissances. Euler l'étend au cas de p non premier (1759, N. C. 1760), telle que nous l'avons reproduite (E. M. 1907, p. 439), ainsi que les propositions également signalées (E. M. pp. 438, 452).

Dans ce mémoire, Euler donne ce que nous avons appelé le *lemme fondamental*, et les théorèmes suivants :

$$(21) \qquad \varphi(p^k) = p^{k-1}(p - 1)$$

$$(22) \qquad \varphi(pp' \ldots) = (p - 1)(p' - 1)\ldots$$

$$(23) \qquad \varphi(ab) = \varphi(a)\,\varphi(b) \qquad (a \text{ et } b \text{ premiers entre eux.})$$

$$(24) \qquad \varphi(p^a p'^{a'} \ldots) = p^{a-1} p'^{a'-1} \ldots (p - 1)(p' - 1)\ldots$$

(1759, N. C. 1760.) Euler montre que, de même que pour $a^2 + b^2$ et $a^2 + 2b^2$, a et b étant premiers entre eux, si un diviseur de $a^2 + 3b^2$ est de la même forme, il en est de même du quotient[1]; — que tout nombre premier $a^2 + 3b^2$

[1] En généralisant la démonstration qu'Euler donne pour $k = 2$ et $k = 3$, on dira que *si* $a^2 + kb^2$ *est divisible par le nombre premier* $\alpha^2 + k\beta^2$, *le quotient est de la même forme.* En effet, le nombre

$$\alpha^2(a + kb^2) - a^2(\alpha^2 + k\beta^2) = k(\alpha^2 b^2 - a^2 \beta^2)$$

est évidemment divisible par $\alpha^2 + k\beta^2$. Ce dernier nombre est premier et il ne peut diviser k,

est en même temps $6 + 1$; — que pour $p = 6h + 1$, on a

$$(a^{2h} - b^{2h})(a^{4h} + a^{2h}b^{2h} + b^{4h}) \equiv 0,$$

que d'ailleurs $f^2 \pm fg + g^2$ peut toujours se mettre sous la forme $x^2 + 3y^2$, et que la congruence $x^2 - y^2 \equiv 0$ a toujours des non-racines, d'où il suit que tout nombre premier $6 + 1$ divise un nombre de forme $x^2 + 3y^2$ et par suite est de même forme.

(1759, N. C. 1762.) *Le produit de deux expressions de la forme* $x^2 + ky^2$ *est de la même forme*[1], car on a :

$$(25) \qquad (a^2 + kb^2)(\alpha^2 + k\beta^2) = (a\alpha \pm kb\beta)^2 + k(a\beta \mp b\alpha)^2 ;$$

d'où il suit que si $(x = a,\ y = b)$ est une solution de l'équation de Pell $x^2 - ky^2 = 1$, et $(x = \alpha,\ y = \beta)$ une solution de l'équation $x^2 - ky^2 = l$, on en aura d'autres de cette dernière, en posant

$$x = a\alpha \pm kl\beta , \qquad y = a\beta \pm b\alpha .$$

Euler donne aussi l'identité

$$(26) \qquad (ka^2 + lb^2)(k\alpha^2 + l\beta^2) = (ka\alpha \pm lb\beta)^2 + kl(a\beta \mp b\alpha)^2 ,$$

et montre à trouver une foule de solutions de $g + hx + kx^2 = y^2$, quand on en connaît une seule et en outre une de

---

que celui-ci soit positif ou qu'il soit négatif. $\alpha^2 + k\beta^2$ doit ainsi diviser l'un ou l'autre des nombres $\alpha b + a\beta$ et $\alpha b - a\beta$. Appelons u le quotient et écrivons

$$\alpha b \pm a\beta = u(\alpha^2 + k\beta^2)$$
$$b = x + \alpha u , \qquad a = y \pm k\beta u ;$$

il viendra $\alpha x \pm \beta y = 0$; ce qui, — à cause de α et β premiers entre eux, — ne peut avoir lieu que si $y = t\alpha$, $x = \mp t\beta$, d'où il suit

$$a^2 + kb^2 = (t^2 + ku^2)(\alpha^2 + k\beta^2) .$$

Euler avait communiqué cette démonstration pour le cas de $k = 1$, à Goldbach en 1747. (Fuss, op. cit., p. 416.)

[1] Goldbach paraît avoir remarqué le premier cet important théorème : dans une lettre à Euler, de 1753 (Fuss, op. cit., p. 612), il dit que le produit

$$(\alpha^2 + e\beta^2)(e + a^2)(e + b^2)(e + c^2)\ldots$$

est de la forme $A^2 + eB^2$.

On a su depuis que les Indiens connaissaient ces belles formules mille ans auparavant.

$x^2 - ky^2 = 1$: d'abord par récurrence, ensuite au moyen de formules de ce genre

$$x = (a + b\sqrt{k})(\alpha + \beta\sqrt{k})^n + (a - b\sqrt{k})(\alpha - \beta\sqrt{k})^n \text{ [1]}$$

$$y\sqrt{k} = (a + b\sqrt{k})(\alpha + \beta\sqrt{k})^n - (a - b\sqrt{k})(\alpha - \beta\sqrt{k})^n$$

n désignant un entier indéterminé et a, b, α, β, des fonctions des coefficients de la proposée. Cette théorie lui sert dans la recherche des nombres g de la forme $y^2 - kx^2$.

Il réduit la méthode de Brouncker, pour la solution de l'équation de Pell, au développement de $\sqrt{k}$ en une fraction continue, qu'il montre être symétrique et périodique.

(N. C. 1762.) *Aucune fonction entière* $F(x) = A + Bx + Cx^2 + \ldots$ *ne peut représenter exclusivement des nombres premiers*. Car, en changeant x en $kF(a) + a$, $F(x)$ est divisible par $F(a)$.

Trouver les nombres de la forme $x^2 + 1$, *qui sont multiples d'un nombre premier donné*, p, *de forme* $4 + 1$. On pose

$$x^2 + 1 = (a^2 + b^2)(y^2 + z^2), \qquad \text{d'où} \qquad az - by = \pm 1 .$$

Le développement de $\frac{a}{b}$, en fraction continue, donne $\frac{y}{z}$, et de là $x = kp \pm (ay + bz)$.

Ainsi pour $p = 29$, on trouve $a = 5$, $b = 2$, $y = 2$, $z = 1$ et $x = 29k \pm 12$ [2].

De là une nouvelle méthode (1765, N. C. 1768) de recherche des diviseurs des grands nombres, pour l'emploi de laquelle Euler donne les formules relatives aux valeurs de p inférieures à 2000, avec la décomposition de $p = 4 + 1$ en une somme de deux carrés jusqu'à la même limite [3], celle

---

[1] A la demande de Goldbach, Euler (Fuss, op. cit., p. 34), donne la formule

$$\frac{(3 + \sqrt{2})^k - (3 - \sqrt{2})^k}{4\sqrt{2}}$$

des nombres dont les carrés sont en même temps des triangulaires; ce qui montre que, dès 1730, il avait étudié l'équation de Pell. Il essaie même d'étendre la solution à l'équation $ax^2 + bx + c = y^2$.

[2] Dans une lettre à Goldbach, de 1743, Euler trouve de même, par le moyen des fractions continues, que les nombres de la forme $x^2 + 1$ divisibles par 1381 sont compris dans la formule $1381h \pm 1366$.

[3] Cette table a été poussée par Jacobi jusqu'au nombre 11981.

des nombres premiers de forme $x^2 + 1$ jusqu'à $1494^2 + 1$, et la liste des diviseurs de $x^2 + 1$ jusqu'à $x = 1500$.

(Id.) Fermat avait enseigné qu'un nombre $4 + 1$ est premier, s'il est une seule fois de la forme $x^2 + y^2$. On avait ainsi le moyen de vérifier si le nombre n, de cette forme, est premier; mais, pour peu que n soit élevé, on avait à calculer un très grand nombre de carrés. Euler montre comment on peut réduire le nombre de ces opérations, en déterminant les formes linéaires de x d'après celles de n. Ainsi $x = 8 \pm 1$ si $n = 16 + 1$ ou $16 + 5$, et $x = 8 \pm 3$ si $n = 16 + 9$ ou $16 + 13$: le nombre des carrés à calculer sera ainsi réduit au quart. Déterminons de même les formes de x correspondant aux formes $60 + 1$, $60 + 7$, $60 + 11$, ... de n, et combinons-les avec les premières, on connaîtra les formules de x dans $x^2 + y^2 = 240 + 1$, $240 + 7$, ... ; et ainsi de suite.

Par exemple, celles qui correspondent à $n = 14400h + 11401$ sont :

$$x = 480 \pm 75, 195,$$
$$x = 1440 \pm 85, 355, 445, 715,$$
$$x = 2400 \pm 99, 501, 651, 1149,$$
$$x = 7200 \pm 149, 949, 1301, 1949, 2101, 2749, 3101, 3297.$$

Opérant sur le nombre 10091401 [1] qui correspond à $h = 700$, on le trouve égal à $1251^2 + 2920^2$ et à nulle autre somme de deux carrés : il est donc premier.

(1768, N. C. 1769.) De nouvelles recherches sur la partitio numerorum l'amènent à exposer des idées qui devaient porter des fruits plus tard; c'est que le théorème de Fermat : *tout entier est la somme de trois triangulaires ou de quatre carrés* serait démontré si on pouvait prouver que le cube de la série $1 + x^1 + x^3 + x^6 + x^{10} + \ldots$ et le bicarré de cette autre $1 + x^1 + x^4 + x^9 + x^{16} + \ldots$ sont

[1] Legendre, par le développement de la racine carrée de ce nombre en fraction continue, a fait voir que les diviseurs appartiennent aux formes suivantes :

$$x^2 + ky^2, \qquad k = 31, 6, -57, 5.38, -30, -46;$$

combinant ces diverses formules, il est arrivé à prouver que le nombre proposé ne peut avoir comme diviseurs que les nombres 727, 1423, 2281. Or la division par aucun d'eux ne réussit : il est donc premier.

égaux à $1 + x^1 + x^2 + x^3 + x^4 + \ldots$; ou encore, en cherchant le coefficient de z^3 dans la première et celui de z^4 dans la seconde des expressions

$$\frac{1}{(1-z)(1-xz)(1-x^3z)(1-x^6z)\ldots}, \quad \frac{1}{(1-z)(1-xz)(1-x^4z)(1-x^9z)\ldots}$$

développées en séries. Ces résultats avaient été communiqués à Goldbach en 1748.

Dans son *Einleitung zur Algebra* (Pétersbourg, 1770), Euler a réuni un grand nombre d'artifices touchant l'analyse diophantine. Nous citerons les suivants, à cause de leurs conséquences ou de leur généralité.

L'introduction de la considération des irrationnelles et des imaginaires, pour la démonstration à priori de certaines identités; par exemple celle-ci :

$$(a^2 + b^2)^2 = (a + bi)^2 (a - bi)^2 = (a^2 - b^2 + 2abi)(a^2 - b^2 - 2abi)$$
$$= (a^2 - b^2)^2 + (2ab)^2$$

$$(a^2 + b^2)(\alpha^2 + \beta^2) = [(a + bi)(\alpha - \beta i)][(a - bi)(\alpha + \beta i)]$$
$$= (a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 .^1$$

Ces remarquables théorèmes : *posons* $(a + \sqrt{b})^n = A + B\sqrt{b}$, *on a* $(a - \sqrt{b})^n = A - B\sqrt{b}$, [2] ce qui donne une nouvelle clé algébrique, car de

$$F(x) + f(y)\sqrt{k} = \varphi(x) + \psi(y)\sqrt{k} ,$$

on tire

$$F(x) = \varphi(x) \quad \text{et} \quad f(x) = \psi(x) . \tag{27}$$

Le produit de facteurs compris sous les formes $kx^2 + ly^2$ *et* $x^2 + kly^2$ *est de la première ou de la seconde forme selon que le nombre des facteurs de la première est impair ou pair.*

Une méthode de recherche des facteurs de $a^2 + kb^2$ fon-

---

[1] Hermite a étendu cette démonstration au cas du produit de deux sommes de quatre carrés, et Catalan a décomposé de la même manière un carré en trois autres carrés. Euler a généralisé autrement en opérant de même sur $a^2 + kb^2$ au lieu de $a^2 + b^2$.

[2] Ce théorème, déjà employé implicitement par Euler et Lagrange, se démontre aisément, sans utiliser la formule du binome. Il a été l'objet d'importantes applications de Lagrange, de Lejeune-Dirichlet, de Genocchi et d'Ed. Lucas.

L'usage le plus important qu'Euler fait de ce théorème est de poser $x + y\sqrt{k} = (t + u\sqrt{k})^n$ pour résoudre $x^2 + ky^2 = z^n$.

dée sur l'assimilation de cette expression au produit $(x^2 \pm ky^2)(z^2 \pm kw^2)$.

Enfin la démonstration, par la méthode de la descente, de l'impossibilité de l'équation $x^3 + y^3 = z^3$. (Communiqué à Goldbach en 1753. Voir Fuss, op. cit., p. 618.)

(1772, N. C. 1773.) Euler remarque que, pour certaines valeurs de x, les restes de la division des $p - 1$ premières puissances de x par p sont tous différents, et que le nombre de ces valeurs est $\varphi(p - 1)$. Il les appelle *radices primitives*, et en donne la liste jusqu'à $p = 37$ [1].

A signaler encore les propositions suivantes :

Pour $\mathrm{p} = 6 + 1$, *si* f, g, h *sont les racines de* $\mathrm{x}^3 \equiv 1$, *on a :*

$$f + g + h \equiv 0 , \quad fg + gh + hf \equiv 0 , \quad f^2 + g^2 + h^2 \equiv 0 ;$$

de là, les formules linéaires de p donnant 3 et -3 pour résidus [2].

Les diviseurs de $\mathrm{a}^4 + \mathrm{b}^4$ *sont de la forme* $8 + 1$; et comme ce nombre peut se mettre sous les deux formes $(a^2 \mp b^2)^2 \pm 2(ab)^2$, il s'ensuit que 2 *et* -2 *sont résidus de* $\mathrm{p} = 8 + 1$.

On a identiquement :

$$x^5 - a^5 = \left(x + \frac{xa}{2} + a^2\right)^2 - 5\left(\frac{xa}{2}\right)^2$$

$$x^7 - a^7 = \left(x^3 + \frac{x^2a - a^2x}{2} - a^3\right)^2 + 7\left(\frac{x^2a + a^2x}{2}\right)^2$$

et, comme pour $p = 5 + 1$ ou $p = 7 + 1$, certaines valeurs de x donnent $x^5 - a^5 \equiv 0$ ou $x^7 - a^7 \equiv 0$, il s'ensuit que, dans les mêmes cas, p divise $x^2 - 5y^2$ ou $x^2 + 7y^2$.

(M. B. [3] 1772.) 10 est non-résidu de $p = 4h \pm 1$, si, parmi les diviseurs des nombres h, $h \mp 2$, $h \mp 6$, ne se trouve qu'un seul des nombres 2, 5 ; il est résidu si ces mêmes diviseurs comprennent les deux nombres 2, 5, ou s'ils n'en comprennent aucun [4].

---

[1] Ostrogradsky a continué cette liste jusqu'à 200, Jacobi jusqu'à 1000 et Desmarests jusqu'à 10000.

[2] On peut, avec Gauss, s'étonner qu'Euler n'ait pas démontré les mêmes choses pour les résidus 2 et -2, d'autant plus que la marche à suivre était analogue.

[3] *Mémoires de l'Académie de Berlin.*

[4] Cette propriété se démontre aisément en partant des formes linéaires des diviseurs de $x^2 \pm 10y^2$.

Le nombre $2^{31} - 1$ est premier. (Voir E. M., p. 443.)[1]

Les quarante premières valeurs entières de x dans la fonction $x^2 - x + 41$ fournissent des nombres premiers[2].

(*Acta eruditorum*, 1773.) Lagrange avait démontré le théorème de Bachet (M. B. 1770); Euler simplifie sa démonstration du lemme déjà énoncé plus haut : *les diviseurs d'une somme de quatre carrés sont eux-mêmes des sommes de quatre carrés.*

(Id.) Euler aborde la recherche du minimum de la fonction $Ax^2 + Bxy + Cy^2$, en vue de la résolution des équations indéterminées du second degré, question reprise plus tard par Lagrange.

(N. C. 1774.) Euler généralise la méthode de calcul des tables de nombres premiers appelée *crible arithmétique*, en partant de cette remarque que les nombres premiers sont de l'une des formes $30h + r$, r désignant l'un des nombres 1, 7, 11, 13, 17, 19, 23, 29. Or, par exemple, les valeurs de h qui rendent $30h + 1$ divisible par 7, sont les termes de la suite $\div 3 . 10 . 17 . 24 \ldots$, ce qui se vérifie en remarquant que de $30h + 1 = 7g$, on tire $g = 4h + \frac{2h + 1}{7}$. Il opère de même, pour déterminer les valeurs de h qui rendent multiples de 7, les formules $30h + 7$, $30h + 11$, ... ; ensuite celles qui rendent multiples de 11, les formules $30h + r$; multiples de 13, les mêmes formules, etc. Classant tous ces résultats en une table à double entrée ayant pour argument les valeurs $h = 1, 2, 3, 4, \ldots$ et pour têtes de colonnes les nombres r, les cases pleines contenant les valeurs de $30h + r$, qu'on vient de définir; les cases vides désigneront les nombres premiers[3].

---

[1] Landry a donné de ce fait une autre démonstration très intéressante, comprenant la solution de l'équation $a = (n + x)(n - y)$, n désignant l'entier le plus voisin de $\sqrt{a}$.

[2] Legendre et M. Escott ont donné plusieurs autres formules de ce genre. (Voir *Int. math.*, 1898, pp. 114 et 184, et 1899, p. 10.) Le premier qui s'en est avisé est Goldbach; dans une lettre à Euler, de 1742, il lui en annonce plusieurs, entre autres $x^2 + 19x - 19$, laquelle donne des nombres premiers, pour les quarante-sept premières valeurs entières de x, sauf quatre. On peut vérifier que ces quatre valeurs sont $x = 19$, 25, 36 et 38; les quarante-trois autres donnent des nombres premiers. (Voir Fuss, op. cit., pp. 257 et 262.)

[3] Les *Tables* de Wega, de Burkardt, de Lebesgue, etc., sont fondées sur les principes analogues. Seulement la formule $30h + r$ est remplacée par $210h + r$ ou $300h + r$, ..., r désignant alors tous les nombres premiers inférieurs à 210 ou à 300. Voir les *Tables* de Lebesgue (1864), celles de Lebon et de Parry (1906).

Il cherche de même les formules des nombres de la forme $30h + r$ qui sont en même temps multiples de $30h \pm 1$ [1], $30a \pm 7$, $30a \pm 11$, ... et en déduit une autre table ayant mêmes têtes de colonnes, et pour arguments, les nombres premiers, chaque case contenant la valeur de h telle que l'argument soit le plus petit diviseur de $30h + r$. Il tire de là une méthode de construire une table des nombres premiers supérieurs à une limite donnée.

M. B. 1776.) Euler parle pour la première fois de ses fameux *numeri idonei*, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, ... 1365, 1848 [2], qu'il caractérise par cette propriété qu'un nombre premier quelconque ne peut être représenté que d'une seule manière par la forme $x^2 + ky^2$, si k est un numerus idoneus; et il les détermine par la règle suivante : k *est un numerus idoneus si*, x *étant premier avec* k, *tous les nombres de forme* $x^2 + k$ *et moindres que* 4k *sont, ou premiers, ou des carrés de premiers, ou des puissances* de 2.

(1775, A.[3] 1780). Euler traite la série $1 - x - x^2 + x^5 + x^7 - \ldots = (1 - x)(1 - x^2)(1 - x^3)\ldots$, en décomposant chaque facteur du second membre en ses facteurs imaginaires, et en tire diverses conséquences intéressantes au point de vue de la théorie des équations.

(Id.) *Entre* 0 *et* 1, *combien y a-t-il de fractions réduites dont les termes sont inférieurs au nombre donné* n? Ce nombre est, pour $n = 10$, 31; pour $n = 100$, 3043; ...

On a, p, q, ... *désignant les facteurs premiers de* x,

$$(28) \qquad \int \Sigma\, \varphi(x)\, a^{x-1}\, da = \Sigma \frac{(p-1)(q-1)\ldots}{pq\ldots}$$

(Id.) La question de la possibilité de décomposer un nombre donné en une somme de trois triangulaires revient à faire voir que *tout nombre* 8a + 3 *est la somme de trois carrés impairs*, car de $a = \Sigma \frac{x^2 + x}{2}$, on tire : $8a + 3 = \Sigma(2x + 1)^2$. (Fuss, op. cit., lettre à Goldbach, de 1730.)

---

[1] Dans ce cas, $h = 2a(15a + n) + k(3a \pm 1)$ et $r = \pm 2n - 1$.

[2] Gauss a retrouvé ces soixante-cinq nombres dans ses recherches sur différents modes de classification des formes quadratiques binaires.

[3] *Acta Academiæ Petropolitanæ.*

(1773, *Opuscula analytica*, 1783.) Euler revient sur la théorie des résidus. Il montre que les résidus sont *associés* deux à deux, et donne le théorème suivant, dont il souhaite connaître la démonstration.

« *Existente* s *numero quocunque primo, dividantur tantum quadrata imparia* 1, 9, 25, 49, *etc., per divisorem* 4s, *notenturque residua, quæ omnia erunt formæ* $4q + 1$, *quorum quodvis littera* $\mathfrak{a}$ *indicetur, reliquorum autem numerorum, formæ* $4q + 1$, *qui inter residua non occurrunt, quilibet littera* $\mathfrak{A}$ *indicetur, quo facto si fuerit.*

divisor numerus primus formæ	*tum est*
$4ns + \mathfrak{a}$	+ s *residuum et* — s *residuum*
$4ns - \mathfrak{a}$	+ s *residuum et* — s *non-residuum*
$4ns + \mathfrak{A}$	+ s *non-residuum et* — s *non-residuum*
$4ns - \mathfrak{A}$	+ s *non-residuum et* — s *residuum.* »

C'est, sous une forme rudimentaire, la célèbre *loi de réciprocité.*

(Id.) Il donne, pour reconnaître la possibilité de l'équation $fx^2 + gy^2 = hz^0$, une méthode qui manque de rigueur; Legendre et Gauss ont repris la question et l'ont complètement résolue.

(Id.) Euler indique une méthode pour déterminer x tel que $a^x \equiv f$, et qu'on saisira suffisamment par l'exemple suivant. Soient $a = 2$, $f = 1$, $p = 23$; on a

$$2^3 . 3 \equiv 1 , \quad -2^2 . 5 \equiv 3 , \quad -2^2 . 7 \equiv -5 , \quad 2^4 \equiv -7 \pmod{23}$$

d'où, en multipliant,

$$2^{3+2+2+4} 3 . 5 . 7 \equiv 1 . 3 . 5 . 7 \quad \text{ou} \quad 2^{11} \equiv 1 . \qquad \text{(id.)}$$

(Id.) Il démontre le théorème de Wilson[1] en se basant sur l'existence d'une racine primitive (E. M., 1907, p. 459), existence qu'il admet sans la démontrer.

(1774, *Opuscula analytica*, II, 1785). La démonstration de l'égalité d'un entier quelconque à une somme $\Sigma \frac{3x^2 - x}{2}$ de

[1] Dont Lagrange venait de trouver deux démonstrations rappelées, E. M., 1907, pp. 299 et 441.

cinq pentagones se ramène à celle de l'équation $24a + 4 = \Sigma(6x^2 - 1)$ [1], ou à celle de la relation

$$(1 + x + x^5 + x^{12} + \ldots)^5 = 1 + x + x^2 + x^3 + x^4 + \ldots$$

A cette occasion, il montre comment on peut obtenir le développement de la k^{me} puissance, $S^k = T = 1 + Ax + Bx^2 + \ldots$, de la série $S = 1 + x^a + x^b + \ldots$, au moyen de la relation

$$\frac{Sx\,dT}{dx} = \frac{kTx\,dS}{dx},$$

d'après la méthode de Jacques Bernoulli.

(Id.) Il somme la série $\Sigma \pm \frac{1}{pk}$, où le signe + a lieu quand p est $4 + 1$, et le signe — quand $p = 4 - 1$, à l'aide des considérations déjà utilisées dans l'*Anal. in inf.*, en partant des formules de Wallis et de Leibniz, donnant la valeur du nombre π. (Fuss, op. cit., lettre à Goldbach, de 1752.)

(Id.) Il montre à résoudre l'équation $(a^2 + kb^2)^x = y^2 + kz^2$, à l'aide de la formule (27); ou encore à l'aide de la formule de Moivre, en posant $a + b\sqrt{-k} = x(\cos y + i \sin y)$.

(1778, N. A.[2], 1792.) *Tout nombre qui est, de deux manières différentes, la somme de deux carrés, est composé.* Soit $a^2 + b^2 = \alpha^2 + \beta^2$; soit de plus $\frac{f}{g}$ la valeur simplifiée de la fraction

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

Posons $a + \alpha = kf$, $\beta - b = lf$, $\beta + b = kg$, $a - \alpha = lg$, on a :

$$a + \frac{kf + lg}{2}, \quad b = \frac{kg - lf}{2}, \quad \text{d'où} \quad a^2 + b^2 = \frac{(k^2 + l^2)(f^2 + g^2)}{4}.$$ [3]

soit $n = 1000^2 + 3^2$ et posons $n = x^2 + y^2$. Le nombre $1000009 - x^2$ ne peut être un carré que s'il est divisible

---

[1] En général, le cas du n^{gone} se réduit à la décomposition de l'expression $8na + (n + 2)(n - 2)^2$ en une somme de n carrés de la forme $(2nx + 2 - n)^2$. (Legendre.)

[2] *Nova Acta.*

[3] Fuss, *loc. cit.*, Lettre à Goldbach, de 1744.

par 5, et par suite par 25. Ecrivons donc $x = 25z + 3$; le nombre $1000000 - 150z - (25z)^2$ doit être un carré, de même que $40000 - 6z - 25z^2$. Pour $z = 4 - 1$, cette expression a la forme $8 - 3$, non représentative d'un carré. Pour $z = 4w + 1$, il viendra la formule $39969 - 224w - (20w)^2$; où, faisant $w = 0, 1, 2, 3, 4, \ldots, -1, -2, -3, \ldots$, et s'aidant de la différence seconde, qui est $= 800$, on trouve pour $w = 10$, le carré 2209, d'où $z = -39$ et $x = -972$. On a ainsi :

$$n = 1000^2 + 5^2 = 872^2 + 235^2 , \quad \text{d'où} \quad \frac{1235}{975} = \frac{969}{765} = \frac{19}{15} .$$

n est donc divisible par $19^2 + 15^2$.

L'étude de z pair conduit à la même conséquence.

(1778, N. A. 1795.) Si $n = af^2 + bg^2 = aF^2 + bG^2$, a et b désignant des entiers positifs, l'une des deux quantités $fG \pm gF$ est divisible par n, ainsi que l'une des suivantes $afF \pm bgG$; car on a :

$$n(G^2 - g^2) = a(f^2G^2 - F^2g^2) \quad \text{et} \quad n(aG^2 - bf^2) = (afF)^2 - (bgG)^2 .$$

De plus,

$$n = (k^2 + abl^2)(ar^2 + bs^2) ,$$

relation où r et s sont les termes de la fraction $\frac{f + F}{g + G}$, réduite à sa plus simple expression, et où $f + F = kr$, $g + G = ks$, $f - F = bls$, $G - g = alr$.

(1778, N. A. 1797.) On peut, de cette manière, trouver de grands nombres premiers. Considérons le numerus idoneus 232. Tout nombre qui pourra se mettre sous les deux formes $232x^2 + y^2$ et $232z^2 + 1$ sera composé. On aura ainsi, en changeant y en $58w \pm 1$,

$$z^2 - x^2 = \frac{w}{2}(29w \pm 1) .$$

Le premier membre, et par suite le second, représentent un nombre composé rs. Posons $z + x = r$, $z - x = s$, d'où

$$z = \frac{r + s}{2} .$$

r et s sont de même parité. Soit $w = 13$; on aura : $rs = 13.4.47$ ou $23.13.7$, d'où

$$r = 94,\ 351,\ 273,\ 189,\ 117,\ 91,\ 63\ ;$$
$$s = 26,\ \ 7,\ \ 9,\ \ 13,\ \ 21,\ 27,\ 39\ ;$$
$$z = 60,\ 179,\ 141,\ 101,\ \ 69,\ 59,\ 51\ .$$

Euler donne la table des valeurs de z correspondant à $w = 1, 2, 3, 4, \ldots 78$, valeurs qu'il trouve être 4, 8, 11, 14, 19, 21, 23, 25, 29, ... 295, 296, 298. Il conclut que les autres valeurs $z = 1, 2, 3, 5, 6, 7, 9, 10, 12, 13, 15, \ldots 294, 297, 299$ mises dans la formule $232z^2 + 1$, donnent des nombres premiers [1].

(Id.) Euler montre ainsi comment on peut trouver les diviseurs d'un nombre n qu'on a pu mettre sous la forme $a^2 + kb^2$. Supposons $n = a^2 + kb^2 = x^2 + ky^2$. En appelant $\frac{f}{g}$ la fraction $\frac{y-b}{a-x}$ réduite à sa plus simple expression, et posant

$$(\alpha) \qquad a + x = kft\ ,\quad y - b = fu\ ,\quad y + b = tg\ ,\quad a - x = ug\ ,$$

il viendra

$$n = \frac{1}{4}(u^2 + kt^2)(g^2 + kf^2)\ ,$$

soit $n = 10003 = 100^2 + 3.1^2$ et posons $n = x^2 + 3y^2$; n étant impair, x et y sont de parité différente ; de plus n étant $8 + 3$, on doit avoir $x^2 = 8$ et $y^2 = 8 + 1$, d'où $x = 4t$ et $y = 2u + 1$, et de là

$$4t^2 + 3u^2 + 3u = 2500\ ,$$

ce qui fait voir que u est de la forme de $4v$, ce qui donne

$$625 - 12v^2 - 3v = t^2\ .$$

v ne peut être pair, car 625 étant $8 + 1$, v serait 8 : or les valeurs $v = 8, 16, \ldots$ rendraient t^2 négatif.

---

[1] Ces ingénieuses méthodes d'exclusions sont d'excellents exemples des procédés indirects par lesquels peuvent être attaquées les démonstrations arithmétiques, quand les méthodes directes ne réussissent pas. L'habileté de l'arithméticien, dans les questions de ce genre, doit porter sur le groupement des exclusions, de manière à réduire le nombre des cas à examiner, sans trop les compliquer.

v ne peut être $4 + 1$ car t^2 serait $4 + 2$, ce qui est impossible.

Posons $v = 4q - 1$, il viendra

$$154 - 48q^2 + 21q = \left(\frac{t}{2}\right)^2$$

la valeur $q = 2$ répond seule à la question et donne $v = 7$, $y = 57$, $x = 16$. Ainsi

$$10003 = 100^2 + 3 . 1^2 = 16^2 + 3 . 57^2 .$$

Appliquant les formules (α), avec $k = 3$, $a = 100$, $b = 1$, $x = 16$, $y = 57$, il vient

$$\frac{3f}{g} = \frac{116}{58} = 3 . \frac{2}{3}$$

d'où $f = 2$, $g = 3$; le nombre $3f^2 + g^2 = 21$ est donc diviseur de n.

Euler remarque que, même pour k premier, il ne s'ensuit pas nécessairement que n soit premier s'il est, d'une seule manière, de la forme $x^2 + ky^2$, car $15 = 2^2 + 11 . 1^2$ est dans ce cas : il faut en outre que k soit un numerus idoneus. Mais, quels que soient k et l, n est composé s'il est, de plusieurs manières, de la forme $kx^2 + ly^2$.

Il traite ainsi les nombres de la forme $ka^2 + lb^2$, (kl) désignant un numerus idoneus. Ses procédés sont analogues à ceux qu'on a exposés tout à l'heure; mais il les perfectionne à mesure que se présentent de nouvelles difficultés. Malgré leur intérêt, nous ne pouvons songer à donner de nouveaux exemples; nous nous contenterons de signaler la formule $1848x^2 + 197^2$, qui lui donne de très grands nombres premiers, dont ceux qu'on obtient en faisant $x = 3, 5, 6, 7, 8, 13, \ldots 70, 80, 100$.

Jusqu'à présent, nous n'avons parlé que des travaux d'Euler publiés ou au moins divulgués de son vivant. La précieuse *Correspondance* éditée par Fuss, — celle surtout qui eut lieu entre Euler et Goldbach et que nous avons citée plusieurs fois pour fixer la date de certaines découvertes d'Euler, — contient de celui-ci beaucoup d'essais sur les-

quels il n'est pas revenu et qui paraissent pourtant dignes d'être notés. Nous indiquerons les plus remarquables. En outre, il semble, — et c'est l'avis de Fuss, — qu'Euler doit à Goldbach l'impulsion qui lui a fait entreprendre ses recherches arithmétiques : non seulement ce dernier a signalé à son attention les principaux théorèmes de Fermat, mais il lui a proposé un grand nombre de théorèmes et d'aperçus qui ont certainement averti Euler de l'intérêt qui s'attachait à cette science nouvelle qu'il a tant illustrée. Nous mentionnerons également quelques-uns de ceux-ci.

(1730.) Goldbach remarque un cycle qu'on peut rendre par les relations suivantes :

$$a^n \equiv b\ ,\quad b^n \equiv c\ ,\quad c^n \equiv d\ ,\ \ldots\ f^n \equiv g\ ,\quad g^n \equiv d\ ,$$

et qui ne peut avoir plus de $p - 1$ termes.

(Id.) Euler donne, pour le nombre des diviseurs de A, la curieuse formule

$$(29)\qquad \frac{3 + (-1)^A + 1 + (-1)^B + 1 + (-1)^C + \ldots}{2}\ ,$$

où B est le A^e terme de la série 1, 1, 4, 7, 13, 22, ... dont chaque terme est égal aux deux précédents plus 2; C le A^e de la série 1, 1, 1, 6, 11, 21, 41, ... dont chaque terme égale la somme des trois précédents, plus 3; D, le A^e de la série 1, 1, 1, 1, 8, 15. 29, 57, ... dont chaque terme égale la somme des quatre précédents plus 4; et ainsi de suite.

(Id.) Goldbach annonce qu'*un triangulaire ne peut être un bicarré.*

(1739.) Il propose à Euler l'étude de la série

$$\Sigma \frac{(-1)^{\theta(x)}}{x^a}\ .$$

(1742.) Il énonce son fameux théorème, qu'on n'a encore ni démontré ni improuvé : *un nombre entier quelconque est la somme de deux nombres premiers*[1].

[1] « ... jede Zahl, aus zweyen numeris primis zuzammengesetz ist, ... » Waring (*Médit. Alg.* Cantab. 1782), le donne également presque dans les mêmes termes : « Omnis par numerus constat a duobus primis numeris... »

Ce théorème a été généralisé par Deboves et Sylvester.

(Id.) Il annonce avoir remarqué que *le nombre* $4a^4 + 1$ *n'est jamais premier;* à quoi Euler répond qu'en effet on a l'identité

$$(\alpha) \qquad 4a^4 + 1 = (2a^2 + 2a + 1)(2a^2 - 2a + 1) .^1$$

(Id.) Il propose à Euler ce théorème et le suivant : *un terme quelconque de la série* 2, 4, 6, 10, 14, 16, 20, 24, ... *des nombres* x *tels que* $x^2 + 1$ *soit premier, est la somme de deux termes de la série.*

(1743.) *Si* $4n \pm 1$ *est un nombre premier,* n *est, suivant les cas, la somme d'un carré et de deux triangulaires ou de deux carrés et d'un triangulaire.*

(Id.) Il propose l'étude des nombres décimaux de la forme $0,1a\,1aa\,1aaa\,1aaaa\,1a \ldots$

(1746.) Euler donne les suites

$$(30) \qquad \frac{1 - a^n}{1 - a} + \frac{(1 - a^n)(1 - a^{n-1})}{1 - a^2} + \frac{(1 - a^n)(1 - a^{n-1})(1 - a^{n-2})}{1 - a^3} + \ldots = n ,$$

$$(31) \qquad 1 - a^{n-1} + a^{2n-3} - a^{3n-6} + a^{4n-10} - \ldots = 0 .$$

(1747.) Goldbach remarque que, dans la série 1, 3, 7, 17, 41, 99, ... soumise à la loi $u_{n+1} = 2u_n + u_{n-1}$, les termes de rang pair sont de la forme $x^2 \pm 1$, et qu'aucun terme de rang impair n'est un carré. Euler démontre ces propositions.

(1748.) Il donne plusieurs solutions[2] de l'égalité $a^2 + b^2 + c^2 = x^2 + y^2 + z^2$; propose de démontrer que $8a + 3$ est la somme de trois carrés x^2, y^2, z^2, en posant

$$x = 1 + fa + ga^2 + ha^3 + \ldots$$
$$y = 1 + fa - ga^2 + ha^3 - \ldots$$

---

[1] Leibniz avait déjà indiqué (*Acta erud.*, 1725) celle-ci

$$(\beta) \qquad a^4 + b^4 = (a^2 + \sqrt{2}\,ab + b^2)(a^2 - \sqrt{2}\,ab + b^2) .$$

Sophie Germain a remarqué qu'*aucun nombre de la forme* $x^4 + 4$ *sauf* 5, *n'est premier* (lettre à Gauss, du 22 mai 1909), ce qui se démontre en changeant a en $\frac{1}{a}$ dans (α), chose évidemment possible, puisque cette relation a lieu identiquement.

Le Lasseur a retrouvé un cas particulier remarquable de (α), celui où $a = 2^n$. Antérieurement, Catalan avait découvert cette génération de (β)

$$(\gamma) \qquad a^4 + 2ka^2 + l^2 = (a^2 + a\sqrt{2(l-k)} + l)(a^2 - a\sqrt{2(l-k)} + l) .$$

[2] Continuées plus tard par lui et par Euler.

d'où

$$z^2 = 1 + 8a - 4f - 2f^2a^2 - 2g^2a^4 - 4ghg^5 - \ldots ;$$

et énonce plusieurs théorèmes, dont les suivants : *tout nombre pair est la somme de trois carrés; tout entier est la somme d'un triangulaire, du double d'un autre triangulaire et du quadruple d'un troisième.*

(1749.) Euler démontre les théorèmes suivants : *si* 8a + 4 *est la somme de quatre carrés impairs,* 4a + 2 *et* 2a + 1 *sont également des sommes de quatre carrés assignables* [1].

Si 3a *est une somme de quatre carrés il en est de même de* a [2] *De même pour* 5a.[3] *De même pour* 7a.

(1752.) Goldbach observe que *toute somme de trois carrés peut se mettre sous la forme*

$$\frac{x^2 + 2y^2 + 3z^2}{6} .$$

Euler donne la solution [4] et généralise la question.

(Id.) Euler énonce les théorèmes empiriques suivants : *si* a *n'est pas la somme :* 1° *d'un carré et du double d'un triangulaire,* 2° *d'un carré et d'un triangulaire,* 3° *d'un triangulaire et du double d'un autre triangulaire,* 4a + 1 *dans le premier cas,* 8a + 1 *dans le second et* 8a + 3 *dans le troisième sont composés.*

Tout nombre 4 + 2 *est la somme de deux nombres premiers* 4 + 1.[5]

---

[1] C'est une conséquence de l'identité

$$(2a + 1)^2 + (2b + 1)^2 = 2(a + b + 1)^2 + 2(a - b)^2$$

et de ce que $4a + 2$ ne peut être composé que de deux carrés pairs et de deux carrés impairs.

[2] Euler considère deux cas qu'on retrouvera facilement à l'aide des résultats que voici :

$$a = (x + y + z)^2 + (x - y + w)^2 + (x - z - w)^2 + (y - z + w)^2 ;$$
$$a = (1 + x + y + z)^2 + (x - y + z)^2 + (x - z - w)^2 + (y - z + w)^2 .$$

[3] Trois cas à considérer dont il suffira de donner les résultats :

$$a = (2x + y)^2 + (2y - x)^2 + (2z + w)^2 + (2w - z)^2 ;$$
$$a = (1 + x + 2y)^2 + (2x - y)^2 + (2z + w)^2 + (z - 2w)^2 ;$$
$$a = (1 + x + 2y)^2 + (2x - y)^2 + (1 + z + 2w)^2 + (2z - w)^2 .$$

[4] $x = 2a + b - c$, $y = a - b + c$, $z = b + c$. Jacobi a démontré que les nombres $x^2 + 2y^2 + 3z^2 + 6w^2$ sont des sommes de quatre carrés; Liouville a également donné des relations de ce genre.

[5] Lagrange a donné des théorèmes analogues.

(1753.) Euler résout les équations

$$x^2 + y^2 = z^2 + 2w^2 \text{ [1]} \quad \text{et} \quad x^2 + by^2 = z^2 + aw^2 \text{ [2]}$$

(1755). Il suppose que le théorème non démontré de Fermat : *l'équation* $x^n + y^n = z^n$ *est impossible pour* $n > 2$, doit être remplacé par celui-ci : *un cube est égal à la somme de trois cubes ; un bicarré, à celle de quatre bicarrés, etc.*

(Id.) Enfin divers essais de solution de l'équation $x^2 + y^2 = p = 4 + 1$, solution découverte par Gauss et Jacobi.

Les *Commentationes Arithmeticæ* (Pétersbourg, 1849), seule partie publiée d'un ensemble qui devait comprendre tous les mémoires détachés d'Euler, contiennent ceux de ses travaux relatifs à la théorie des nombres, sauf ceux qui se trouvent dans l'*Introd. in anal. inf.* et dans son *Algebra ;* et en outre divers travaux posthumes, dont nous citerons son *Tractatus de numerorum doctrinæ,* le premier qu'on ait écrit sur l'arithmétique. On y voit un exposé des propriétés des nombres premiers, des diviseurs numériques, des restes des fonctions ax, a^x, x^a, des formes des diviseurs de $a^x + b^x$, des résidus quadratiques et même des résidus cubiques, biquadratiques et quintiques. On y voit ébauchés des théorèmes retrouvés et démontrés par Gauss et Jacobi sur les *caractères cubiques* et *biquadratiques* du nombre 2.

En somme, Euler a largement ouvert la voie que Fermat avait simplement indiquée : à la vérité il n'a pas entièrement élucidé toutes les questions constituant le fondement de la nouvelle arithmétique ; et même son *Tractatus*, d'ailleurs inachevé, ne peut guère être considéré que comme un essai. Néanmoins le court résumé de ses découvertes, qui va nous servir de conclusion, témoignera de l'importance de l'œuvre de l'illustre analyste.

Démonstrations du théorème de Fermat ; de l'impossibilité des équations $x^3 + y^3 = z^3$, $x^4 + y^4 = z^4$, $xy(x^2 - y^2) = z^2$;

---

[1] $x = a^2 - b^2$, $y = c^2 \pm 2ab$, $z = a^2 + b^2 - c^2$, $w = (a \pm b)c$.

[2] $x = a\alpha^2 - b\beta^2 + \gamma^2$, $y = 2\beta\gamma$, $z = a\alpha^2 - b\beta^2 - \gamma^2$, $w = 2\alpha\gamma$.

de la divisibilité de $a^2 + b^2$ par $x^2 + y^2$ et autres théorèmes analogues ; utilisation de ces théorèmes dans la recherche des diviseurs des nombres : tout cela dû en principe à Fermat, mais démontré et grandement perfectionné par Euler.

On lui doit en propre : la théorie de *partitione numerorum* ; de curieuses formules et séries sur les nombres premiers et les diviseurs des nombres ; la considération des racines des congruences, de leur nombre possible, des racines primitives ; l'extension du crible arithmétique ; l'emploi des fractions continues dans la théorie des nombres ; un grand nombre d'identités des plus utiles ; des vues variées et ingénieuses sur l'analyse indéterminée, qu'il a enrichie de méthodes et de questions nouvelles ; enfin de nombreuses tables dont il souhaitait l'extension, pour favoriser la découverte des propriétés des nombres.

A. AUBRY (Dijon).

LE POLYGONE INSCRIT EN GÉOMÉTRIE NON-EUCLIDIENNE

L'article publié par M. A. PADOA dans l'*Ens. math.* du 15 mars 1909, attire de nouveau l'attention sur l'intéressant problème de l'inscription dans un cercle d'un polygone de côtés donnés dans leur ordre de succession et leur grandeur. Ce problème de Géométrie élémentaire peut être résolu d'une manière rigoureuse seulement par des équations algébriques de degré élevé, mais le recours à un postulat tel que celui invoqué par M. Padoa me paraît plutôt compliquer les choses que les faciliter. En effet, quand on étudie le maximum ou le minimum de la surface d'un polygone articulé, la possibilité de l'inscription dans un cercle n'est qu'un premier pas vers la solution du problème. De plus il en va ici comme toutes les fois qu'on s'appuie sur une propriété de maximum pour établir un théorème d'existence : à sup-