JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

LÉON POMEY

Sur le dernier théorème de Fermat

Journal de mathématiques pures et appliquées 9^e série, tome 4 (1925), p. 1-22.
<http://www.numdam.org/item?id=JMPA_1925_9_4__1_0>

JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES.

Sur le dernier théorème de Fermat;

PAR LÉON POMEY.

1. *Introduction.* — D'après ce célèbre théorème, il serait impossible, pour tout degré n supérieur au second, de satisfaire par des entiers x, y, z non nuls à l'égalité

$$x^n = y^n + z^n.$$

Connu déjà des Chinois et des Marocains dans le cas le plus simple ($n = 3$), ce théorème fut formulé par Fermat, qui assura l'avoir démontré. Mais aucune démonstration générale n'en a encore été publiée, bien qu'il ait fait l'objet des recherches de très nombreux géomètres, au premier rang desquels on peut citer Euler, Legendre, Abel, Sophie Germain, Lejeune-Dirichlet, Lamé, Cauchy, Liouville et Kummer (1). On sait d'ailleurs qu'il suffirait de l'établir en supposant *n premier et x, y, z premiers entre eux* deux à deux.

(1) On trouve de multiples références bibliographiques et renseignements historiques dans l'*Encyclopédie mathématique* (*Théorie des nombres*), les

Admettons alors, n étant premier impair, que — par impossible — il existe trois entiers x_1, x_2, x_3 premiers entre eux et $\gtrless 0$ satisfaisant à

$$x_1^n + x_2^n + x_3^n = 0. \tag{1}$$

Nous nous proposons, dans ce Mémoire, de déduire de cette hypothèse diverses conditions nécessaires, sans lesquelles l'équation (1) est effectivement impossible. La plupart des résultats auxquels nous allons être conduits ont été résumés dans une Note des *Comptes rendus de l'Académie des Sciences* (3 décembre 1923, p. 1187). Nous les exposerons d'une manière aussi simple et concise que possible, sans d'ailleurs être obligé d'avoir recours aux méthodes et aux critères de Kummer.

Nous aurons à distinguer deux cas suivant que x_1, x_2, x_3 sont premiers à n (*premier cas* qu'on pourrait appeler *cas de S. Germain*) ou que l'un de ces nombres, soit x_1, est divisible par n (*second cas*).

2. *Formules fondamentales.* — Les indices i, j, k étant distincts et pouvant prendre indifféremment les valeurs 1, 2, 3, posons

$$x_j + x_k = N_i, \tag{2}$$

$$p = \sum_{i=1}^{i=3} x_i = \frac{\Sigma N_i}{2} = x_i + N_i, \tag{3}$$

$$S(x_j, x_k) = \frac{(x_j + x_k)^n - x_j^n - x_k^n}{n\, x_j x_k (x_j + x_k)}, \qquad P(x_j, x_k) = \frac{x_j^n + x_k^n}{x_j + x_k}. \tag{4}$$

Rappelons d'abord quelques formules fondamentales, où a_i, g_i, φ désigneront certains entiers premiers entre eux et avec n, et ν un entier ≥ 1.

Théorème I [Legendre (1), Abel]. — *Dans le premier cas, les*

Œuvres de Fermat, éditées par P. Tannery et Ch. Henry (particulièrement Tome IV), *l'Intermédiaire des Mathématiciens* [12 (1905), p. 11], le *Rapport sur la Théorie des corps de nombres algébriques*, de Hilbert (traduction de MM. Got et Lévy), etc.

(1) Legendre, *Mém. de l'Ac. des Sc.*, de 1823. — Abel, *Lettre à Holmboe*, du 24 juin 1823 (*Œuvres*, 2e édition, t. II, p. 264).

nombres x_i $(i = 1, 2, 3)$ *vérifient des relations de la forme*

$$X_i = a_i^n, \tag{8}$$

$$P(x_j, x_k) = g_i^n, \tag{9}$$

$$x_i = -a_i g_i. \tag{10}$$

THÉORÈME I *bis* (id.). — *Dans le second cas,* x_2 *et* x_3 *vérifient des relations de même forme que les précédentes (avec* $i = 2$ *ou* 3); *mais, pour* x_1, *ces relations deviennent*

$$X_1 = n^{n\nu-1} a_1^n, \tag{8'}$$

$$P(x_2, x_3) = n g_1^n, \tag{9'}$$

$$x_1 = -n^\nu a_1 g_1. \tag{10'}$$

THÉORÈME II (Legendre). — *Dans les deux cas, p est de la forme*

$$p = n^\nu a_1 a_2 a_3 \varphi. \tag{11}$$

3. ÉNONCÉ DE QUELQUES LEMMES. — Nous avons retrouvé ces résultats avant de connaître les travaux de Legendre et d'Abel par les considérations suivantes :

a. Pour démontrer les théorèmes I et I bis, nous sommes partis de l'équation

$$x_i^n = -X_i P(x_j, x_k) \tag{5}$$

équivalente à (1) et avons utilisé les lemmes suivants :

LEMME A. — *On a l'identité*

$$P(x_j, x_k) = X_i^2 R(x_j, x_k) + n(-x_j x_k)^{\frac{n-1}{2}} \tag{6}$$

avec

$$R(x_j, x_k) = \frac{x_j^{n-2} + x_k^{n-2}}{X_i} + 2(-x_j x_k)\frac{x_j^{n-4} + x_k^{n-4}}{X_i} + \ldots + \frac{n-1}{2}(-x_j x_k)^{\frac{n-3}{2}}.$$

COROLLAIRE B. — *Du moment que* X_i *est premier avec* $x_j x_k$, *le plus grand commun diviseur de* X_i *et de* $P(x_j, x_k)$ *est* 1 *ou* n, *suivant que* X_i *est premier ou non à* n, *et dans cette seconde hypothèse* $P(x_j, x_k)$ *n'est d'ailleurs divisible que par la première puissance de* n.

Observons en passant que ce corollaire B entraîne cette proposition:

LEMME C. — *Si le binome $x_i^n + x_k^n$ est divisible par n^λ, X_i l'est par $n^{\lambda-1}$.*

b. Quant au *théorème II*, nous l'avons démontré d'une première manière en nous appuyant sur une des relations (3), savoir $p = x_i + X_i$ et sur les théorèmes I et I *bis*, et d'une seconde manière en nous appuyant sur l'équation suivante, conséquence de (1) :

$$(7) \qquad p^n - np x_i X_i S(p_1 - X_i) - n x_j x_k X_i S(x_j, x_k) = 0,$$

ainsi que sur ce lemme

LEMME D.— *Du moment que le nombre X_i est premier avec $x_j x_k$, il l'est aussi avec $S(x_j, x_k)$.*

Nous ne nous étendrons pas davantage ici sur tous ces préliminaires.

4. AUTRES CONDITIONS NÉCESSAIRES. — Passons à des résultats que nous croyons nouveaux.

Premier cas.

THÉORÈME III. — *Dans le premier cas, ν étant le même exposant (≥ 1) qu'au théorème II, les nombres x_i doivent satisfaire aux trois congruences*

$$(12) \qquad S(x_j, x_k) \equiv 0 \pmod{n^\nu} \qquad (j, k = 1, 2, 3)$$

ou, ce qui revient au même, aux congruences

$$(13) \qquad (x_j + x_k)^n - x_j^n - x_k^n \equiv 0 \pmod{n^{\nu+1}}.$$

En effet, en vertu de (3) et du théorème II, on a

$$(14) \qquad X_i \equiv -x_i \pmod{n^\nu},$$

d'où

$$X_i^n \equiv -x_i^n \pmod{n^{\nu+1}},$$

ce qui, en vertu de (1) et (2), donne bien (13), et, par suite (12), en vertu de (4). C. Q. F. D.

Autre démonstration. — L'équation (7) en fournirait une immédiatement.

Cas particulier. — En se bornant à $\nu = 1$, on retombe sur un énoncé employé par Legendre et, pour $n = 197$, par M. E. Maillet.

Mais on peut aller plus loin, car ν doit en réalité, comme on va le voir, être > 1 et même ≥ 3.

THÉORÈME IV. — *Dans le premier cas, il faut que* ν *soit* ≥ 2.

En vertu du théorème I, la congruence (14) nous donne

$$a_i^n \equiv -x_i \pmod{n^\nu}$$

ou, par application du théorème de Fermat,

$$a_i \equiv -x_i \pmod{n} \tag{15}$$

et, par élévation à la puissance n,

$$a_i^n \equiv -x_i^n \pmod{n^2}; \tag{16}$$

d'où

$$\Sigma a_i^n \equiv -\Sigma x_i^n \equiv 0 \pmod{n^2}.$$

Or les formules (8), (3) et (11) conduisent aux égalités

$$\Sigma a_i^n = \Sigma X_i = 3p = 3n^\nu a_1 a_2 a_3 \varphi.$$

Puisque Σa_i^n est divisible par n^2, ν doit donc bien être ≥ 2.

C. Q. F. D.

Autre démonstration. — Une seconde démonstration peut être fondée sur l'équation suivante (où $\sigma = \Sigma a_i$) :

$$\begin{aligned}\sigma^n - n\sigma(a_j + a_k)a_i \mathrm{S}[\sigma, -(a_j + a_k)] \\ - n a_j a_k (a_j + a_k)\mathrm{S}(a_j, a_k) = 3n^\nu a_i a_j a_k \varphi,\end{aligned}$$

laquelle est une conséquence de la relation (11) du théorème II. Il suffit alors d'observer que σ et $\mathrm{S}(a_j, a_k)$ doivent évidemment être divisibles par n.

THÉORÈME V. — *Dans le premier cas, il faut qu'on ait*

$$x_i^n - x_i \equiv 0 \pmod{n^2}.$$

En effet, cette congruence s'obtient en retranchant membre à membre la congruence (14) — où l'on fait $\nu = 2$, d'après le théorème IV, — et la congruence (16), où l'on remplace a_i par X_i.

3. *Autre mode de démonstration.* — Indiquons encore une autre voie qu'on peut suivre pour établir les théorèmes IV et V. L'avantage de cette nouvelle méthode sera de nous conduire plus loin à une extension.

LEMME VI. — Dans le premier cas, *tous les facteurs premiers du nombre* g_i ($i = 1, 2, 3$) *sont de la forme* $1 + 2 \times n^{\gamma}\lambda$ *avec* $\gamma \geq 1$ (λ *étant un entier*).

En effet, tout facteur premier ρ de g_i divise $P(x_j, x_k)$ [d'après l'équation (9) du théorème I]; donc il divise $x_j^n + x_k^n$ mais est premier avec a_i, c'est-à-dire avec $(x_j + x_k)$. Donc, d'après un théorème connu, ρ est bien de la forme $1 + 2kn$. C. Q. F. D.

COROLLAIRE VII. — *Dans le premier cas, si* γ_0 *est le plus petit des exposants* γ *relatifs à* g_i, *on a* $g_i \equiv 1 \pmod{n^{\alpha_i}}$ *avec* $\alpha_i \geq \gamma_0 \geq 1$.

En effet, *la valeur absolue* de g_i est, d'après le théorème précédent, de la forme $1 + 2K_i n^{\alpha_i}$ (avec $\alpha_i \geq \gamma_0 \geq 1$); d'où $g_i \equiv \pm 1 \pmod{n^{\alpha_i}}$. D'ailleurs l'égalité (10) du théorème I et la congruence (15) du théorème IV donnent $a_i = a_i g_i \pmod{n}$ ou $g_i \equiv 1 \pmod{n}$. On a donc bien $g_i \equiv 1 \pmod{n^{\alpha_i}}$. C. Q. F. D.

THÉORÈME IV *bis*. — *Dans le premier cas, si* α *est le plus petit des trois nombres* α_i, *il faut que* ν *soit* $\geq \alpha + 1$ (*donc* $\nu \geq 2$).

En effet, en portant dans la formule (10) la valeur de g_i du théorème précédent, on a $x_i = -a_i (1 + 2K_i n^{\alpha_i})$. D'où $x_i^n = -a_i^n (1 + 2K_i n^{\alpha_i + 1} + \text{mult. } n^{\alpha_i + 2})$ et, par conséquent,

$$x_i^n \equiv -X_i \pmod{n^{\alpha_i + 1}}. \tag{17}$$

D'où $0 \equiv \Sigma X_i \pmod{n^{\alpha + 1}}$; donc [formule (3) du paragraphe **2**] $2p$ *est divisible par* $n^{\alpha + 1} \geq n^2$. Donc, d'après la formule (11) du théorème II, ν est $\geq \alpha + 1 \geq 2$. Le résultat $\nu \geq 2$ est ainsi démontré pour la *troisième* fois. C. Q. F. D.

THÉORÈME V *bis*. — *Dans le premier cas, il faut que pour* $i = 1, 2, 3$ *on ait* $x_i'' - x_i \equiv 0 \pmod{n^{\alpha+1}}$ *(avec* $\alpha + 1 \geq 2$*).*

En effet, cette congruence s'obtient en retranchant membre à membre les congruences (14) (du théorème III) et (17), puisque le module n^ν de (14) est, d'après le théorème précédent, au moins égal au module $n^{\alpha+1}$ de (17). C. Q. F. D.

6. *Extension des quatre derniers théorèmes.*

LEMME VI *bis*. — *Dans le premier cas, tous les facteurs premiers des trois nombres* g_i *sont de la forme* $1 + 2n^\gamma\lambda$ *avec* $\gamma \geq 2$.

En effet, tout facteur premier ρ de g_i divise $x_j'' + x_k''$ mais non $x_j + x_k = X_i$ (c'est ce qu'on a déjà constaté au lemme VI).

Or on a [équation (2) et (8)]

$$x_i + x_j = X_k = a_k''.$$

Donc ρ divisant g_i et par suite x_i [équation (10)], on a

$$x_j \equiv a_k'' \pmod{\rho};$$

et de même,

$$x_k \equiv a_j''.$$

Par conséquent ρ divise $a_k''^z + a_j''^z$ mais non $a_k'' + a_j''$, ni *a fortiori* $a_k + a_j$. Donc $\rho = 2\lambda n^2 + 1$. C. Q. F. D.

En tenant compte de cette proposition, les énoncés du corollaire VII et des théorèmes IV *bis* et V *bis* deviennent *ipso facto* (sans autre démonstration) :

COROLLAIRE VII *bis*. — *Dans le premier cas, pour chaque* g_i, *on a*

$$g_i \equiv 1 \pmod{n^{\alpha_i}} \quad \text{avec} \quad \alpha_i \geq 2.$$

THÉORÈME IV *ter*. — *Dans le premier cas, si* α *est le plus petit des* α_i, on a

$$\nu > \alpha + 1 \geq 3, \quad \text{c'est-à-dire} \quad \Sigma x_i \equiv 0 \pmod{n^3}.$$

THÉORÈME V *ter*. — *Dans le premier cas, on a*

$$x_i'' - x_i \equiv 0 \pmod{n^{\alpha+1}} \quad \text{avec} \quad \alpha + 1 \geq 3.$$

Conséquence. — Dans ces conditions, le théorème III peut s'énoncer :

THÉORÈME III *bis*. — *Dans le premier cas, on doit avoir*

$$(x_i + x_j)^n - x_i^n - x_j^n \equiv 0 \pmod{n^4}$$

ou

$$S(x_i, x_j) \equiv 0 \pmod{n^3}.$$

Ces trois derniers théorèmes (IV *ter*, V *ter*, III *bis*) paraissent être, en ce qui concerne le premier cas, les plus curieux de ceux que nous avons trouvés. Les théorèmes V *bis* et V *ter* ne sont pas évidemment sans faire penser aux conditions nécessaires bien connues de MM. Wieferich et Frobenius ($2^{n-1} - 1 \equiv 0 \pmod{n^2}$) et de M. Mirimanoff ($3^{n-1} - 1 \equiv 0 \pmod{n^2}$), conditions qui ont, il est vrai, été obtenues par ces géomètres en s'appuyant sur les critères de Kummer.

7. *Théorèmes analogues pour* X_i *et* a_i. — D'autre part, si l'on remplace x_i par $-X_i$, qui lui est congru (mod n^3), ou par $-a_i$ qui lui est congru (mod n^2), les théorèmes IV *ter*, V *ter* et III *bis* relatifs aux nombres x_i conduisent immédiatement, pour les nombres X_i et a_i, à des propositions analogues que nous résumons dans un seul énoncé :

THÉORÈME VIII. — *Dans le premier cas, les trois nombres* a_i *doivent satisfaire aux congruences*

$$\begin{aligned}
\Sigma X_i &\equiv 0 \pmod{n^3}, \\
\Sigma a_i &\equiv 0 \pmod{n^2}, \\
X_i^n - X_i &\equiv 0 \pmod{n^3}, \\
a_i^n - a_i &\equiv 0 \pmod{n^2}, \\
(X_i + X_j)^n - X_i^n - X_j^n &\equiv 0 \pmod{n^4}, \\
(a_i + a_j)^n - a_i^n - a_j^n &\equiv 0 \pmod{n^3}.
\end{aligned}$$

Autre forme des théorèmes IV ter, *V* ter *et III* bis. — On peut donner à ces théorèmes une autre forme en introduisant les deux nombres u et v qui sont tels qu'on ait

$$x_2 \equiv u x_1 \quad \text{et} \quad x_3 \equiv v x_1 \pmod{n^3}.$$

Il faut que les nombres x_1, u et v satisfassent aux congruences :

THÉORÈME IV :

$$1 + u + v \equiv 0 \pmod{n^3}.$$

THÉORÈME V :

$$x^n - x \equiv 0, \qquad u^n - u \equiv 0, \qquad v_n - v \equiv 0 \pmod{n^3}.$$

THÉORÈME III :

$$(1+u)^n - (1+u^n) \equiv 0, \qquad (1+v)^n - (1+v^n) \equiv 0,$$
$$(u+v)^n - (u^n + v^n) \equiv 0 \pmod{n^3}.$$

Nous allons montrer sur quelques exemples ($n = 3, 5, 59$) comment les théorèmes IV *ter*, V *ter* et III *bis* (ou III) peuvent permettre de prouver l'impossibilité de l'équation (1) dans le premier cas.

Nous indiquerons ensuite une méthode assez générale fondée sur les théorèmes IV, V, III (seconde forme) pour s'assurer de l'impossibilité de (1) dans le premier cas; elle est sans doute susceptible de perfectionnements; faute de temps, nous nous contenterons de l'illustrer par quelques exemples ($n = 3, 5, 11, 17, 23, 29$), où la vérification se fera en un instant.

8. APPLICATION DES THÉORÈMES IV *ter*, V *ter*, III *bis*. — *Nouvelles démonstrations de l'impossibilité de* (1) *dans le premier cas pour* $n = 3, 5, 59$:

Les conditions nécessaires fournies par ces trois théorèmes s'expriment par les congruences suivantes [où le symbole $((n^3))$ désigne abréviativement $\bmod n^3$] :

$$(1) \qquad \Sigma x_i \equiv 0 \qquad ((n^3)),$$
$$(2) \qquad x_i^n - x_i \equiv 0 \qquad ((n_3)),$$
$$(3) \qquad (x_i + x_j)^n - x_i^n - x_j^n \equiv 0 \qquad ((n^3)),$$

ou

$$S(x_i, x_p) \equiv 0 \qquad ((n^3)).$$

Appliquons-les à ces exemples-ci :

$n = 3$.

Premier procédé. [Emploi de la congruence (3) seule]. — $S_3(x_i, x_j)$, étant égal à 1, quels que soient x_i et x_j, ne peut pas être $\equiv o\,((n^3))$. Donc....

Deuxième procédé. [Emploi des congruences (1) et (2).] — Chaque nombre x_i étant par hypothèse premier à 3 est de la forme $\varepsilon_i + 3K_i$ ($\varepsilon_i = \pm 1$). Donc pour satisfaire à $x_i^3 - x_i \equiv o((n^3))$, il faut que $K_i = \text{mult.}\,3^2$. Mais alors la congruence (1) : $\Sigma x_i \equiv o((n^3))$ est visiblement impossible, à moins que l'un des ε_i ne soit nul. C. Q. F. D.

$n = 5$.

Premier procédé. [Emploi des congruences (1) et (3).] — Chaque nombre x_i, étant premier à 5, est de l'une des deux formes $5K_i + \varepsilon_i$ ou $5K_i + 2\varepsilon_i$ ($\varepsilon_i = \pm 1$). Or la congruence (1) n'est évidemment possible que si les trois nombres x_i n'appartiennent pas simultanément à la même de ces deux formes.

Il faut donc que l'un, x_1 par exemple, soit de la forme $5K_1 + \varepsilon_1$ et un autre, que nous appellerons x_2, de la forme $5K_2 + 2\varepsilon_2$, le troisième pouvant être indifféremment de l'une ou l'autre forme.

D'autre part, on a ici $S_5(x_1, x_2) = (x_1 + x_2)^2 - x_1 x_2$. La congruence (3) impose donc comme première condition que

$$(\varepsilon_1 + 2\varepsilon_2)^2 - \varepsilon_1 \times 2\varepsilon_2$$

soit divisible par 5, ce qui est impossible [puisque $(\varepsilon_1 + 2\varepsilon_2)^2$ est égal à 1 ou 9 suivant les signes de ε_1 et ε_2, et que le second terme vaut ± 2].

C. Q. F. D.

Deuxième procédé. [Emploi des congruences (1) et (2).] — La congruence (1) impose, on vient de le voir, qu'on ait par exemple

$$x_1 = 5K_1 + \varepsilon_1, \qquad x_2 = 5K_2 + 2\varepsilon_2,$$

x_3 étant soit $5K_3 + \varepsilon_3$, soit $5K_3 + 2\varepsilon_3$.

D'autre part, pour satisfaire aux congruences (2), il faut que

$x_1^5 - 1$ et $x_2^5 - 1$ soient divisibles par 5^3; donc K_1 doit être divisible par 5^2, d'où $x_1 = \varepsilon_1 + 5^3 h_1$; en outre, $x_2^5 - 1$ étant égal à $(x_2 + 1)(x_2 - 1)(x_2^2 + 1)$, il faut qu'on ait $x_2^2 + 1 \equiv 0((5^3))$, c'est-à-dire $5K_2^2 + 4\varepsilon_2 K_2 + 1 \equiv 0((5^2))$, et par suite $4\varepsilon_2 K_2 + 1 \equiv 0((5))$ ou $K_2 \equiv \varepsilon_2 \pmod 5$.

En conséquence, x_3 ne peut être que de la forme $5K_3 + \varepsilon_3$, car il devrait alors (comme x_1) être de la forme $5^3 l_1 + \varepsilon_3$ d'après la congruence (2), et la congruence (1) exigerait qu'on ait $\varepsilon_1 = \varepsilon_3 = -\varepsilon_2$ et $K_2 \equiv 0$, ce qui est incompatible avec $K_2 = \varepsilon_2$.

En outre x_3 ne peut pas non plus être de la forme $5K_3 + 2\varepsilon_3$, car dans ce cas la congruence (1) devient

$$(5^3 K_1 + \varepsilon_1) + (5K_2 + 2\varepsilon_2) + (5K_3 + 2\varepsilon_3) \equiv 0 \qquad (\mathrm{mod}\, 5^3),$$

ce qui entraîne $\varepsilon_1 = \varepsilon_2 = \varepsilon_3$ et $\varepsilon_1 + K_2 + K_3 \equiv 0$. Or cette congruence est impossible, puisqu'on doit avoir, en vertu des congruences (2), $K_2 \equiv \varepsilon_2 \equiv \varepsilon_1$ et $K_3 \equiv \varepsilon_3 \equiv \varepsilon_1$.

Donc x_3 ne peut être premier à 5. C. Q. F. D.

n = 59.

Emploi d'une seule des congruences du théorème III. — Rappelons que, d'après M. Arwin (*Acta mathematica*, t. 42, 1920, p. 190), si n est égal à 59, la congruence

$$(1 + u)^n - 1 - u^n \equiv 0$$

a des solutions quand on prend n^2 pour module (ce qui empêche de pouvoir appliquer à ce cas le critère de Legendre), mais au contraire n'en a aucune si l'on prend n^3 pour module.

Tenant compte de ce résultat, on en déduit qu'*a fortiori* il n'existe pas de solutions pour le module n^4, ce qui nous suffit *pour conclure à l'impossibilité de l'équation* $\Sigma x_i^{59} = 0$ *dans le premier cas.*

9. Application des théorèmes IV, V, VI. — Ceux-ci expriment, comme nous l'avons vu, que (1) est impossible dans le premier cas si l'on ne peut trouver des entiers a et c de la forme

$$a + bn + cn^2 \qquad (a, b, c < n)$$

satisfaisant aux congruences

$$(1)' \qquad 1 + u + v \equiv 0 \qquad ((n^3)),$$

$$(2)' \qquad u^n - u \equiv 0, \qquad v^n - v \equiv 0 \qquad ((n^3)),$$

$$(3)' \qquad \begin{cases} (u+v)^n - u^n - v^n \equiv 0, & (1+u)^n - 1 - u^n \equiv 0, \\ (1+v)^n - 1 - v^n \equiv 0 & ((n^3)). \end{cases}$$

MÉTHODE GÉNÉRALE FONDÉE SUR CES CONGRUENCES. — *Nouvelle démonstration de l'impossibilité pour* $n = 3, 5, 11, 17, 23, 29$.

D'une manière générale, les trois conditions (1)' et (2)' donnent, par élimination de v,

$$u^n - u \equiv 0, \qquad (u+1)^n - (u+1) \equiv 0 \qquad ((n^3)).$$

Celles-ci expriment que *parmi les racines* (*autres que* 0 *et* -1) *de la congruence*

$$x^n - x \equiv 0 \qquad (\mathrm{mod}\, n^3)$$

(et *a fortiori* de la même congruence prise avec le module n^2 au lieu de n^3) *doivent figurer au moins deux entiers* CONSÉCUTIFS

$$u = a + bn + cn^2 \qquad \text{et} \qquad u + 1 = (a+1) + bn + cn^2,$$

faute de quoi l'équation $\Sigma x_i^n = 0$ *est impossible dans le premier cas*.

Donnons quelques applications de ce principe très simple en nous aidant, pour abréger, de la petite table (reproduite plus loin) que Jacobi avait fait établir (*Journal de Crelle*, t. 3, 1828, p. 301) et qui donne, pour $n \leq 37$, les racines x de la congruence $x^{n-1} - 1 \equiv 0$, pour le module n^2 seulement, il est vrai. Ces racines étant supposées mises sous la forme $x = a + nb$ (a et b positifs et $< n$), à chaque valeur de a prise dans la colonne de gauche, cette table fait correspondre la valeur appropriée pour b, qu'on lit en regard dans celle des autres colonnes, en haut de laquelle est inscrit le module n envisagé; ainsi les racines de $x^{36} - 1 \equiv 0 \,(\mathrm{mod}\, 37^2)$ sont $x = 1$, $2 + 2 \times 37$, $3 + 17 \times 37$, etc. (1).

(1) Si $b = 0$, on tombe sur un nombre $a\,(1 < a < n)$, qui satisfait à la congruence; ce cas remarquable a lieu, d'après cette table, pour

n	11	29	37
a	3 et 9	14	18

Pour que la condition énoncée ci-dessus soit réalisée, il *faut* donc, n étant donné, trouver dans la table deux racines $a + nb$ et $(a + 1) + nb$ de ladite congruence, ce qui revient à chercher s'il *existe dans la colonne des b deux valeurs* CONSÉCUTIVES IDENTIQUES.

Un simple coup d'œil sur la table suffit à montrer que ceci n'a pas lieu pour $n = 3, 5, 11, 17, 23, 29$. *L'impossibilité de* $\Sigma x_i^n = 0$ (dans le premier cas) *est donc ainsi démontrée à nouveau pour ces valeurs.*

On voit que cette méthode est simple et assez générale.

REMARQUE. — Pour d'autres valeurs de n (7, 13, 19, 31, 37) au contraire, cette condition est remplie relativement au module n^2 (d'après la table ci-après); il resterait à vérifier si elle l'est ou non pour le module n^3.

Même dans un tel cas où la condition serait vérifiée par une valeur u, *les théorèmes IV ter, V ter, III bis ont pour effet de déterminer les premiers coefficients* $\alpha_i, \beta_i, \gamma_i$ du développement de

$$x_i = \alpha_i + \beta_i n + \gamma_i n^2 + \delta_i n^3 + \ldots,$$

ou tout au moins de délimiter assez étroitement leurs valeurs possibles; en effet x_1 doit être congru (mod n^3) à une des racines $a + bn + cn^2$ de la table, x_2 doit être $\equiv ux_1$ et $x_3 \equiv -(1 + u)x_1$.

Le temps nous manque pour poursuivre ces applications numériques. Elles seraient facilitées, comme on vient de le voir, par un travail préparatoire consistant à prolonger la table de Jacobi dans deux directions : 1° pour des valeurs de n au delà de 37 ; 2° pour le module n^3 au lieu de n^2 (même quand $n > 37$). Une telle table donnerait donc non seulement la valeur de b *mais celle de* c, et l'impossibilité serait démontrée pour tous les exposants n tels, qu'on ne trouve pas dans les colonnes correspondantes deux nombres b et c respectivement identiques aux deux nombres b et c immédiatement à la suite.

Bien entendu, cette méthode pourrait éventuellement être combinée avec d'autres méthodes connues.

Table de Jacobi

donnant les racines $x = a + nb$ *de la congruence* $x^{n-1} - 1 \equiv 0 \pmod{n^2}$ *pour* $n \leq 37$.

n	3.	5.	7.	11.	13.	17.	19.	23.	29.	31.	37.
a.	b.	b.	b.	b.	b.	b.	b.	b.	b.	b.	b.
1	0	0	0	0	0	0	0	0	0	0	0
2	2	1	4	10	6	9	6	11	2	12	2
3	.	3	4	0	11	13	16	5	16	30	17
4	.	4	2	7	11	2	5	21	8	17	8
5	.	.	2	2	5	9	3	1	2	14	34
6	.	.	6	8	1	2	13	20	9	14	3
7	.	.	.	3	11	4	15	15	22	27	25
8	.	.	.	10	7	6	15	17	24	30	24
9	.	.	.	0	1	10	1	7	7	27	28
10	.	.	.	10	1	12	17	11	14	26	21
11	.	.	.	..	6	14	3	8	21	13	21
12	.	.	.	..	12	7	3	14	1	7	18
13	.	.	.	..	..	14	6	11	22	25	13
14	.	.	.	..	..	3	15	15	0	14	27
15	.	.	.	..	..	7	13	5	28	18	9
16	.	.	.	..	..	16	2	7	6	12	27
17	.	.	.	..	..	..	12	2	27	16	11
18	.	.	.	..	..	..	18	21	7	7	0
19	.	.	.	..	..	..	..	1	14	23	36
20	.	.	.	..	..	..	..	17	19	17	35
21	.	.	.	..	..	..	..	11	4	4	9
22	.	.	.	..	..	..	..	22	6	3	27
23	.	.	.	..	..	..	..	..	19	10	9
24	.	.	.	..	..	..	..	..	26	3	23
25	.	.	.	..	..	..	..	..	30	16	18
26	.	.	.	..	..	..	..	..	12	16	15
27	.	.	.	..	..	..	..	..	26	13	15
28	.	.	.	..	..	..	..	..	26	10	8
29	.	.	.	..	..	..	..	..	..	18	13
30	.	.	.	..	..	..	..	..	..	30	11
31	.	.	.	..	..	..	..	..	..	..	33
32	.	.	.	..	..	..	..	..	..	..	12
33	.	.	.	..	..	..	..	..	..	..	23
34	.	.	.	..	..	..	..	..	..	..	19
35	.	.	.	..	..	..	..	..	..	..	34
36	.	.	.	..	..	..	..	..	..	..	36

10. Voici quelques *propositions secondaires :*

THÉORÈME IX. — *Dans le premier cas, on a*

$$g_i^n \equiv n(-x_j x_k)^{\frac{n-1}{2}} \pmod{a_i^{3n}}.$$

En effet, dans l'équation (5), remplaçons x_i par $-a_i g_i$ et X_i par a_i^n (théorème I), puis $P(x_j, x_k)$ par l'expression

$$a_i^{3n} R(x_j, x_k) + n(-x_j x_k)^{\frac{n-1}{2}},$$

que fournit le lemme A. L'égalité obtenue donne de suite la congruence cherchée. C. Q. F. D.

DÉFINITION. — *Appelons* D_i *le plus grand commun diviseur de* a_i *et de* $(a_j + a_k)$, *et* A_i, Q_i *les quotients respectifs* $\frac{a_i}{D_i}$ *et* $\frac{a_j + a_k}{D_i}$.

THÉORÈME X. — *Dans le premier cas, l'équation* (11) *du théorème II peut s'écrire :*

$$a_i^n + (a_j + a_k)^n = [2n^\nu a_i \varphi + n(a_j + a_k) S(a_j, a_k)] a_j a_k, \tag{18}$$

laquelle se décompose dans les deux suivantes (où M est un certain entier) :

$$A_i^n + Q_i^n = n a_j a_k M, \qquad 2n^{\nu-1} A_i \varphi + Q_i S(a_j, a_k) = D_i^{n-1} \times M. \tag{19}$$

Pour le voir, il suffit de remplacer p dans l'équation (11) par Σa_i^n, et d'exprimer $a_j^n + a_k^n$ en fonction de $S(a_j, a_k)$, d'où (18). Ensuite, dans (18), remplaçons a_i par $D_i A_i$ et $(a_j + a_k)$ par $D_i Q_i$, ce qui donne

$$D_i^{n-1}(A_i^n + Q_i^n) = n[2n^{\nu-1} A_i \varphi + Q_i S(a_j, a_k) a_j a_k \tag{20}$$

et remarquons que a_j et a_k sont premiers avec D_i et avec n (d'après le théorème I). D'où les équations (19).

THÉORÈME XI. — *Les trois membres* A_i *ont tous leurs facteurs premiers de la forme* $2Kn + 1$.

THÉORÈME XII. — *On doit avoir* $A_i \equiv -Q_i \pmod{n}$.

11. *Le théorème fondamental de S. Germain. Critères de Legendre. Application à des valeurs de n allant jusqu'à* 5003249. — On sait que S. Germain a pu démontrer « d'un trait de plume » le dernier théorème de Fermat (dans le premier cas) pour $n < 100$ grâce à ce théorème remarquable :

Théorème. — *L'équation* $\Sigma x_i^n = 0$ *est impossible en nombres entiers premiers à n* (1er cas), *s'il existe un nombre premier* $\theta = 2Kn + 1$ *tel que : 1° la congruence* $1 + \rho + \rho' \equiv 0 \pmod{\theta}$ *soit impossible*, ρ *et* ρ' *étant deux résidus de puissances* $n^{\text{èmes}}$ [*et par suite aussi toute congruence* $u^n + v^n + w^n \equiv 0 \pmod{\theta}$, *où u, v, w sont premiers à* θ]; *2° n ne soit pas un résidu de puissance* $n^{\text{ème}} \pmod{\theta}$.

De là Legendre a tiré divers corollaires (donnés ci-après), qui lui ont permis de prolonger la vérification jusqu'à $n < 197$. Depuis, des progrès considérables ont été réalisés dans cette voie par M. Dickson.

Critères de Legendre. — *L'équation* (1) *est impossible en nombres entiers premiers à n* (1er cas) *si le nombre premier n est tel que l'un des nombres* $2n + 1$, $4n + 1$, $8n + 1$, $10n + 1$ *soit également premier.*

Application à de grandes valeurs de n. — Nous avons recherché — entre certaines limites — les nombres premiers n qui sont tels que $2n + 1$ soit aussi premier.

Les nombres n jouissant de cette propriété et compris *entre* 9043 et 10001 sont : 9049, 9221, 9293, 9371, 9419, 9473, 9479, 9539, 9629, 9689, 9791.

Entre 5000000 et 5003371, ces valeurs de n (que nous désignons simplement par leur excédent sur 5000000) sont : 111 (c'est-à-dire 5000111), 263, 321, 381, 399, 741, 783, 903, 981, 1173, 1203, 1299, 1443, 1779, 2103, 2223, 2229, 2313, 2331, 2583, 2841, 3081, 3231, enfin 3249, c'est-à-dire 5003249.

Nous pensons que ces valeurs sont les plus grandes pour lesquelles un tel calcul ait été fait et pour lesquelles l'impossibilité de (1) *dans le premier cas se trouve ainsi vérifiée.*

Autres conséquences des critères de Legendre. — En nous appuyant

d'une part sur ces critères, d'autre part sur quelques-uns des nombreux résultats que nous avons obtenus dans la théorie des nombres premiers et que nous avons développés dans uu autre Mémoire étendu, nous pouvons énoncer ces théorèmes.

NOUVEAUX CRITÈRES. — *Dans le premier cas, on sera sûr que l'équation* (1) *est impossible en nombres entiers quand l'une quelconque des six circonstances suivantes se produira :*

1° *Si, n étant de la forme* $4K+3$, $2n+1$ *divise* 2^n-1; 2° *n étant de la forme* $4K+1$, *si* $2n+1$ *divise* 2^n+1; 3° *si* $4n+1$ *est de la forme* $8K+5$ *et divise* $2^{2n}+1$; 4° *si* $4n+1$ *est de la forme* $12K+5$ *et divise* $3^{2n}+1$; 5° *si* $8n+1$ *divise* $2^{4n}-1$; 6° *si* $10n+1$ *divise* $5^{5n}-1$.

Deuxième cas.

12. THÉORÈME III'. — *Dans le deuxième cas, les trois nombres* $S(x_i, x_j)$ *doivent être premiers à n.*

Cela résulte immédiatement de ce que, dans ce cas, l'un des trois nombres x_i, x_j (x_i+x_j) est toujours divisible par n et que $S(x_i, x_j)$ est premier avec chacun d'eux. C. Q. F. D.

THÉORÈME IV'. — *Dans le deuxième cas, il faut que l'exposant* ν (qui entre dans p et dans x_1) *soit* ≥ 2.

Première démonstration. — L'équation (11) conduit encore à une équation analogue à l'égalité (18) du théorème X (§ **10**), savoir

$$(18') \qquad n^{n\nu-1}a_1^n+(a_2+a_3)^n=[2n^\nu a_1\varphi+n(a_2+a_3)S(a_2,a_3)]a_2a_3,$$

d'où le théorème résulte sans peine (1).

Deuxième démonstration (analogue à la deuxième démonstration du théorème IV). — Les congruences (15) et (16) sont encore valables dans le deuxième cas pour $i=2$ et 3 (mais non pour $i=1$). On en déduit encore que la quantité $n^{n\nu-1}a_1^n+a_2^n+a_3^n$, c'est-à-dire

(1) C'est par cette méthode différente de celle de S. Germain, dont je ne connaissais pas encore les travaux, que j'ai retrouvé cette proposition.

$2n^{\nu}a_1a_2a_3\varrho$, d'après l'équation (11), est congrue (mod n^2) à $-\Sigma x_n'$ ou 0. Donc.... C. Q. F. D.

Troisième démonstration. — Plus simplement encore, l'équation (11), dans laquelle p a pour valeur $\frac{n^{n\nu-1}a_1''+a_2''+a_3''}{2}$, montre ici que $a_2''+a_3''$ doit être divisible exactement par n^{ν} (et non par $n^{\nu+1}$) (avec $\nu \geq 1$). Donc a_2+a_3 (congru à $a_2''+a_3''$) est divisible par n, d'où $a_2 \equiv -a_3$, et par suite $a_2'' \equiv -a_3''$ (mod n^2). D'où $\nu \geq 2$.

C. Q. F. D.

Théorème V'. — *Dans le deuxième cas, il faut qu'on ait*

$$x_i'' - x_i \equiv 0 \pmod{n^2}.$$

Première démonstration. — Identique à la première démonstration du théorème V, puisque les congruences (14) sont toujours valables et que, dans ce deuxième cas, on a encore $\nu \geq 2$ (théorème précédent). C. Q. F. D.

Nota. — Bien entendu, ce théorème n'a pas d'intérêt pour $i = 1$, c'est-à-dire pour x_1, qui par hypothèse est ici divisible par $n^{\nu} \geq n^2$.

13. *Autre mode de démonstration des deux derniers théorèmes IV' et V'* (analogue à celui du premier cas) :

Lemme VI'. — *Dans le deuxième cas, tous les facteurs premiers de chaque nombre g_i ($i = 1, 2, 3$) sont de la forme $1 + 2n^{\gamma}\lambda$ (avec $\gamma \geq 1$).*

Pour g_2 et g_3, le raisonnement est identique à celui du lemme VI (premier cas); pour g_1, il est analogue également, puisque g_1 étant premier non seulement avec a_1, mais avec n, l'est bien aussi avec $x_2 + x_3$; d'où la même conclusion. C. Q. F. D.

Corollaire VII'. — *Dans le deuxième cas, si γ_0 est le plus petit des exposants γ relatifs au nombre g_i ($i = 2$ et 3), on a*

$$g_i \equiv 1 \pmod{n^{\alpha_i}} \quad \text{avec} \quad \alpha_i \geq \gamma_0 > 1.$$

En effet, d'abord ces nombres g_i sont *en valeur absolue* de la forme

$1 + 2K_i n^{\alpha_i}$ avec $\alpha_i \geq \gamma_0 \geq 2$, d'après le lemme VI'; d'où

$$g_i = \pm 1 \qquad (\mathrm{mod}\, n^{\alpha_i}).$$

D'autre part, les égalités (10') et les congruences (15), qui leur sont applicables pour $i = 2$ et 3, donnent

$$a_i \equiv a_i g_i \qquad (\mathrm{mod}\, n),$$

c'est-à-dire

$$g_i - 1 \equiv g_i \qquad (\mathrm{mod}\, n).$$

On a donc bien

$$g_i = 1 \quad (\mathrm{mod}\, n^{\alpha_i}) \qquad \text{pour} \quad i = 2 \text{ et } 3.$$

C. Q. F. D.

THÉORÈME IV'. — *Dans le deuxième cas, si* α *est le plus petit des nombres* α_i (pour $i = 2$ et 3), ν *est* $\geq \alpha + 1$ (donc ≥ 2).

Le même raisonnement que dans le premier cas (théorème IV *bis*) montre pour $i = 2$ et 3 qu'on a

$$x_2'' \equiv X_2 \qquad \text{et} \qquad x_3'' \equiv X_3 \qquad (\mathrm{mod}\, n^{\alpha+1}). \tag{18}$$

D'ailleurs, d'après les équations (8') et (10') (théorème I'), on a

$$x_1'' \equiv -X_1 \qquad (\mathrm{mod}\, n^{\nu-1}).$$

Par suite $\Sigma x_i''$ ou 0 est congru à $-\Sigma X_i = -2p$ suivant le plus petit des deux modules $n^{\alpha+1}$ et $n^{\nu-1}$; donc $2p$ est divisible par $n^{\alpha+1}$ ou $n^{\nu-1}$. Donc, d'après l'équation (11) (théorème II), on a bien

$$\nu \geq \alpha + 1 > 2. \qquad \text{C. Q. F. D.}$$

THÉORÈME V'. — *Dans le deuxième cas, il faut qu'on ait*

$$x_i'' - x_i \equiv 0 \quad (\mathrm{mod}\, n^{\alpha+1}) \qquad \text{avec} \qquad \alpha + 1 \geq 2.$$

Même démonstration pour x_2 et x_3 que dans le premier cas (théorème V *bis*). Quant à x_1, il est divisible lui-même [formule (10')] par $n^\nu \geq n^2$.

14. *Extension des théorèmes précédents :*

LEMME VI''. — *Dans le deuxième cas, tous les facteurs premiers du nombre* g_1 *sont de la forme* $1 + 2n^\gamma \lambda$ *(avec* $\gamma \geq 2$*).*

Démonstration identique textuellement à celle du lemme VI *bis* (1er cas), en y supposant $i = 1$ (1).

THÉORÈME IX'. — *Dans le deuxième cas, on a les congruences* (*avec* j *et* $k \neq 1$)

$$g_1^n \equiv (-x_2x_3)^{\frac{n-1}{2}} \pmod{n^{2\alpha\gamma-3}a_1^{2\gamma}}, \qquad g_j^n \equiv n(-x_1x_k)^{\frac{n-1}{2}} \pmod{a_j^{2n}}.$$

Elles résultent instantanément des équations (5), quand on y remplace X_i et x_i par leurs valeurs (8') et (10') (théorème I'), et $P(x_j, x_k)$ par son expression $X_1^2 K(x_j, x_k) + n(-x_j x_k)^{\frac{n-1}{2}}$ (lemme A).

C. Q. F. D.

COROLLAIRE VII. — *Dans le deuxième cas, si* γ_0 *est le plus petit des exposants* γ *relatifs au nombre* g_1, *on a*

$$g_1 \equiv 1 \pmod{n^{\alpha_1}} \qquad \text{avec } \alpha_1 \geq \gamma_0 \geq 2.$$

En effet, d'après le lemme VI' g_1 doit être *en valeur absolue* de la forme $1 + 2K_1 n^{\alpha_1}$, avec $\alpha_1 \geq \gamma_0 \geq 2$, d'où $g_1 \equiv \pm 1 \pmod{n^{\alpha_1}}$. Or, il est facile de voir qu'on a $g_1 \equiv 1 \pmod{n}$; cela résulte de la première congruence du théorème précédent, car le second membre est congru à 1; en effet, on a

$$(31) \qquad \begin{cases} x_2 + x_3 \equiv X_1 \equiv 0 & \pmod{n^{\alpha\gamma-1}} \\ -x_2x_3 = x_2^2 \equiv x_3^2 & \pmod{n^{\alpha\gamma-1}}. \end{cases}$$

On a donc bien

$$g_1 = (x_3^2)^{\frac{n-1}{2}} = 1. \qquad \text{C. Q. F. D.}$$

THÉORÈME V'. — *Dans le deuxième cas, on doit avoir* (pour $i = 2$ et 3) $x_i^n - x_i \equiv 0 \pmod{n^3}$.

En effet, d'après le théorème précédent, on a

$$g_1^n \equiv 1 \pmod{n^{\alpha_1+1} n^3} \qquad \text{et} \qquad (-x_2x_3)^{\frac{n-1}{2}} = x_2^{n-1} = x_3^{n-1} \pmod{n^{\alpha\gamma-1}}.$$

Donc, d'après la première congruence du théorème IX', 1 est congru

(1) Cette démonstration est plus simple que celle par laquelle S. Germain a établi, *pour le deuxième cas seulement*, le lemme VI".

à x_2^{n-1} et à x_3^{n-1} suivant le plus petit des deux modules $\alpha_1 + 1$ et $n\nu - 1$; or $n\nu - 1$ est aussi ≥ 3, puisque ν est déjà ≥ 2 (théorème IV') et que n est ≥ 3. On a donc bien

$$x_2^n - x_2 \equiv 0 \quad \text{et} \quad x_3^n - x_3 \equiv 0 \pmod{n^3}. \qquad \text{C. Q. F. D.}$$

De là résulte que les autres conditions $x_i^n - x_i \equiv 0$ $(i = 1, 2, 3)$ et $\Sigma x_i \equiv 0 \pmod{n^2}$ sont absolument générales (dans les premier et deuxième cas).

Les conditions $x_i^n - x_i \equiv 0 \pmod{n^3}$ sont aussi valables dans les deux cas, sauf pour x_1 s'il est supposé divisible par n.

Dans le deuxième cas, x_2 et $-x_3$ doivent être congrus $(\mathrm{mod}\, n^2)$ à une même racine de la congruence $x_i^n - x_i \equiv 0 \pmod{n^2}$.

13. Les *propositions secondaires* suivantes se démontrent, à peu de chose près, comme leurs analogues du premier cas :

Conséquences du théorème II'. — D_1, A_1, Q_1 étant définis comme dans le premier cas, mais Q_1 étant, dans le deuxième cas, de la forme $n^{\nu-1} q_1$, on a :

THÉORÈME X'. — *Dans le deuxième cas, il existe un entier* N *tel que* (12)' *se décompose en*

$$n^{n-1} A_1^n + q_1^n \equiv a_2 a_3 N,$$
$$2 A_1 \varphi + q_1 S(a_2, a_3) \equiv n^{(n-1)(\nu-1)} D^{n-1} N.$$

NOTA. — *Dans le cas particulier du troisième degré*, on trouve que la valeur absolue de N se réduit à l'unité, ainsi que les nombres φ et $S(a_2, a_3)$.

THÉORÈME XI'. — *Le nombre* A_1 *a tous ses facteurs premiers de la forme* $2Kn + 1$.

THÉORÈME XII'. — *Dans le deuxième cas, on doit avoir*

$$2 A_1 + q_1 \equiv 0 \pmod{n}.$$

THÉORÈME. — *Dans le deuxième cas, tout nombre* 0 *répondant aux conditions du théorème de S. Germain et, en particulier, aux conditions des théorèmes VIII à XVIII, ne peut diviser ni* a_2 *ni* a_3 *et, s'il*

est de la forme $2Kn+1$, *il ne peut diviser* g_1; *mais il doit diviser l'un des trois* x_i, *donc ou* g_2 *ou* g_3 *ou* a_1, *ou même* g_1 *si* $0=2Kn^2+1$.

Équations équivalentes à l'équation $\Sigma x_i^n=0$. — Voici, parmi beaucoup d'autres analogues, quelques équations dont l'impossibilité entraînerait celle de (1), et réciproquement [en appelant $S_n(x_i, x_j)$ la fonction $S(x_i, x_j)$, relative au degré n, et en posant $(x_1x_2x_3)^n=\varpi_n$ et $\Sigma x_i^n x_j^n=\Delta$].

$$x_i^{3n}-x_j^n x_k^n=\Delta \qquad (i, j, k=1, 2, 3);$$

$$\Sigma x_i^{3n}=3\varpi_n; \qquad \Sigma x_i^{kn}=k\varpi_n S_k(x_i, x_j) \qquad (k \text{ impair});$$

$$\Sigma x_i^{9n}=3\varpi_n[10\varpi_n^3-3\Sigma x_i^{3n}x_j^{3n}]; \qquad \Sigma x_i^{9n}=3\varpi_n[\varpi_n^3+3\Delta^3];$$

$$\Sigma x_i^{6n}=(\Sigma x_i^{3n})^2-\Sigma(x_i^n-x_j^n)^3=(3\varpi_n)^2-3\Sigma x_i^{3n}x_j^{3n}=3\varpi_n^2+3\Delta^3;$$

$$(\Sigma x_i^{3n})^3=9\Sigma(3\varpi_n-3x_i^{3n})^3;$$

$$\Sigma x_i^{2n}=3\Delta; \qquad \Sigma(x_i^n x_j^n)^2=\Delta^2; \qquad \Sigma x_i^{4n}=3\Delta^2;$$

$$(x_1^{2n}+x_2^{3n})(x_2^{3n}+x_3^{3n})(x_3^{3n}+x_1^{3n})=3\Delta^3-\varpi_n^3.$$