

T.J. STIELTJES

Sur la décomposition en carrés des nombres premiers de la forme $3n + 1$

Annales de la faculté des sciences de Toulouse 1^{re} série, tome 11, n° 2 (1897), p. D1-D6

<http://www.numdam.org/item?id=AFST_1897_1_11_2_D1_0>

© Université Paul Sabatier, 1897, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (<http://picard.ups-tlse.fr/~annales/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR

LA DÉCOMPOSITION EN CARRÉS

DES NOMBRES PREMIERS DE LA FORME $3n + 1$,

PAR T. J. STIELTJES ⁽¹⁾.

Tout nombre premier p de la forme $3n + 1$ peut être représenté par la somme d'un carré et de trois fois un autre carré

$$(1) \quad p = cc + 3dd.$$

Le quadruple d'un tel nombre premier peut, de plus, être représenté de la manière suivante :

$$(2) \quad 4p = AA + 27BB.$$

Chacune de ces décompositions n'est possible que d'une seule façon. Tout cela se déduit facilement de la théorie générale des formes quadratiques.

Dans le Mémoire : *De residuis cubicis commentatio numerosa*, inséré au Tome 2 du *Journal de Crelle*, Jacobi a indiqué, sans démonstration, que la valeur de A dans la relation (2) est égale au reste qu'on obtient en divisant le nombre entier

$$\frac{(n+1)(n+2)(n+3)\dots 2n}{1.2.3\dots n}$$

par p et choisissant le reste compris entre $-\frac{1}{2}p$ et $+\frac{1}{2}p$. A cela s'ajoute encore la circonstance remarquable que $A + 1$, après ce choix de A , est toujours divisible par 3.

⁽¹⁾ Traduction du travail suivant : *Over de quadratische ontbinding van priemgetallen van den vorm $3n + 1$* (*Verslagen en Mededeelingen der Koninklijke Akademie van Wetenschappen te Amsterdam*, 2^e série, t. XIX, p. 105-111; 1884).

Pour les premiers nombres premiers, on obtient par exemple

$$\begin{array}{llll}
 p = 7, & n = 2, & A = -1, & 28 = 1^2 + 27 \cdot 1^2, \\
 p = 13, & n = 4, & A = +5, & 52 = 5^2 + 27 \cdot 1^2, \\
 p = 19, & n = 6, & A = -7, & 76 = 7^2 + 27 \cdot 1^2, \\
 p = 31, & n = 10, & A = -4, & 124 = 4^2 + 27 \cdot 2^2, \\
 p = 37, & n = 12, & A = +11, & 148 = 11^2 + 27 \cdot 1^2, \\
 p = 43, & n = 14, & A = +8, & 172 = 8^2 + 27 \cdot 2^2, \\
 p = 61, & n = 20, & A = -1, & 244 = 1^2 + 27 \cdot 3^2.
 \end{array}$$

La démonstration de cette proposition, qui est étroitement liée aux propriétés de l'équation algébrique dont dépend la division de la circonférence en p parties égales, peut être trouvée dans le *Mémoire sur la Théorie des nombres* de Cauchy (*Mémoires de l'Académie des Sciences*, t. XVII, 1840) et chez Lebesgue dans le *Journal de Liouville*, t. II, p. 279. Pour d'autres détails complémentaires, on pourra consulter : BACHMANN, *Die Lehre von der Kreistheilung*, p. 144.

Ce théorème de Jacobi est aussi démontré d'une autre manière dans le n° 40 ⁽¹⁾ du *Mémoire Contribution à la Théorie des résidus cubiques et biquadratiques*. Comme addition aux développements qui s'y trouvent, je me propose ici de déduire du théorème de Jacobi une détermination directe de la racine c du carré cc figurant dans la relation (1); il en résultera que c est le reste, compris entre $-\frac{1}{2}p$ et $+\frac{1}{2}p$, qu'on obtient dans la division du nombre entier

$$2^{n-1} \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n}$$

par p , et, en outre, que $c - 1$ est divisible par 3. Par exemple

$$\begin{array}{llll}
 p = 7, & n = 2, & c = -2, & 7 = 2^2 + 3 \cdot 1^2, \\
 p = 13, & n = 4, & c = +1, & 13 = 1^2 + 3 \cdot 2^2, \\
 p = 19, & n = 6, & c = +4, & 19 = 4^2 + 3 \cdot 1^2, \\
 p = 31, & n = 10, & c = -2, & 31 = 2^2 + 3 \cdot 3^2, \\
 p = 37, & n = 12, & c = -5, & 37 = 5^2 + 3 \cdot 2^2.
 \end{array}$$

Soit alors, comme dans le *Mémoire* cité, ρ une racine cubique primitive de l'unité, $a + b\rho$ un facteur primaire de p ; ainsi

$$p = (a + b\rho)(a + b\rho^2) = a^2 - ab + b^2,$$

⁽¹⁾ Voir Tome XI de ce Recueil, page C.65.

$a + 1$ et b sont tous deux divisibles par 3; soit, de plus, f une des deux racines de la congruence

$$1 + x + x^2 \equiv 0 \pmod{p},$$

f étant choisi de telle manière que $a + bf$ soit divisible par p .

D'après le théorème de Jacobi cité plus haut, on a

$$(3) \quad 2a - b \equiv -\frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p},$$

et, de plus, il résulte du critérium relatif au caractère cubique de 2 que

$$\begin{aligned} 2^n &\equiv 1 \pmod{p} && \text{lorsque } b \text{ est pair,} \\ 2^n &\equiv f \pmod{p} && \text{lorsque } a \text{ est pair,} \\ 2^n &\equiv f^2 \pmod{p} && \text{lorsque } a \text{ et } b \text{ sont tous deux impairs.} \end{aligned}$$

Ces trois cas doivent être traités maintenant séparément.

I. — b pair.

Dans ce cas, de

$$p = a^2 - ab + b^2,$$

nous déduisons

$$\begin{aligned} 4p &= (2a - b)^2 + 3b^2, \\ p &= \left(a - \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2. \end{aligned}$$

Dans la relation (1), on peut donc prendre

$$c = -\left(a - \frac{b}{2}\right).$$

Il résulte alors de la relation (3)

$$c \equiv \frac{1}{2} \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p},$$

ou bien, puisque dans ce cas on a $2^n \equiv 1$,

$$(4^a) \quad c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p}.$$

De $a \equiv 2$, $b \equiv 0 \pmod{3}$, il résulte de plus

$$(5^a) \quad c \equiv 1 \pmod{3}.$$

II. — a pair.

Dans ce cas, au lieu de

$$p = a^2 - ab + b^2,$$

nous écrirons

$$16p = (2a - 4b)^2 + 3(2a)^2$$

ou

$$p = \left(\frac{a}{2} - b\right)^2 + 3\left(\frac{a}{2}\right)^2;$$

de sorte que nous pouvons prendre, dans la relation (1),

$$c = \frac{a}{2} - b.$$

Maintenant, on a

$$(6) \quad (a + bf)(1 + 2f) \equiv a - 2b + (2a - b)f \equiv -a - b - (2a - b)f^2 \pmod{p}$$

et

$$a + bf \equiv 0 \pmod{p},$$

donc

$$a - 2b \equiv -f(2a - b);$$

de sorte que, de la relation (3), résulte

$$a - 2b \equiv f \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n}$$

ou bien, puisqu'on a maintenant $f \equiv 2^n$,

$$(4^b) \quad c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p}.$$

De $a \equiv 2$, $b \equiv 0 \pmod{3}$, résulte de plus

$$(5^b) \quad c \equiv 1 \pmod{3}.$$

III. — a et b impairs.

Dans ce dernier cas, on remarque que l'on a

$$16p = (2a + 2b)^2 + 3(2a - 2b)^2$$

ou

$$p = \left(\frac{a+b}{2}\right)^2 + 3\left(\frac{a-b}{2}\right)^2;$$

de sorte que l'on peut prendre

$$c = \frac{a + b}{2}.$$

De la relation (6) résulte maintenant

$$a + b \equiv -f^2(2a - b);$$

donc, la relation (3) donne

$$a + b \equiv f^2 \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p}.$$

Comme on a, dans ce cas, $2^n \equiv f^2$, il vient

$$(4^c) \quad c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p},$$

tandis qu'on voit facilement que

$$(5^c) \quad c \equiv 1 \pmod{3}.$$

Des relations (4^a) , (4^b) , (4^c) , (5^a) , (5^b) , (5^c) , il résulte maintenant qu'on a, dans tous les cas,

$$(4) \quad c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots 2n}{1.2.3\dots n} \pmod{p},$$

$$(5) \quad c \equiv 1 \pmod{3},$$

ce qui donne alors le théorème énoncé ci-dessus.

On peut encore donner à la congruence (4) une autre forme; n étant pair, on écrira $2m$ à la place de n ; alors il vient

$$c \equiv 2^{2m-1} \frac{(2m+1)(2m+2)\dots 4m}{1.2.3\dots 2m}.$$

Maintenant, on a les relations

$$2m+1 \equiv -4m, \quad 2m+3 \equiv -(4m-2), \quad 2m+5 \equiv -(4m-4), \quad \dots,$$

à l'aide desquelles on trouve

$$c \equiv (-1)^m 2^{2m-1} \frac{[(2m+2)(2m+4)\dots 4m]^2}{1.2.3\dots 2m}$$

ou, après une petite transformation,

$$c \equiv (-1)^m 2^{4m-1} \frac{(m+1)(m+2)\dots 2m}{1.2.3\dots m}.$$

D.6 T.-J. STIELTJES. — DÉCOMPOSITION EN CARRÉS DES NOMBRES PREMIERS, ETC.

Maintenant, on a, de plus,

$$2^{3m} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{8}}$$

et

$$\frac{p^2-1}{8} = \frac{9m^2+3m}{2}.$$

En retranchant de cet exposant le nombre pair $\frac{8m^2+4m}{2}$, on peut écrire d'une façon plus simple

$$2^{3m} \equiv (-1)^{\frac{m^2-m}{2}},$$

et, comme conclusion,

$$(7) \quad c \equiv (-1)^{\frac{m^2+m}{2}} 2^{m-1} \frac{(m+1)(m+2)\dots 2m}{1.2.3\dots m} \pmod{p=6m+1}.$$

Cette dernière congruence déterminant c est donnée, sans démonstration et sans la définition plus précise, obtenue ici, du signe de c , par Oltramare dans le Tome LXXXVII des *Comptes rendus de l'Académie des Sciences*, p. 735, en même temps que d'autres du même genre.

