BULLETIN DE LA S. M. F.

ED. MAILLET

Extension du théorème de Fermat sur les nombres polygones

Bulletin de la S. M. F., tome 23 (1895), p. 40-49

<http://www.numdam.org/item?id=BSMF_1895__23__40_1>

EXTENSION DU THÉORÈME DE FERMAT SUR LES NOMBRES POLYGONES;

Par M. Ed. Maillet.

I.

On sait que les nombres polygones d'ordre m sont de la forme

$$\frac{m}{2}(x^2 - x) + x,$$

où x est un entier quelconque.

Cauchy (1) a pu démontrer le théorème de Fermat sur les nombres polygones en s'appuyant sur le lemme suivant :

Lemme. — Soient k un nombre impair pris à volonté, et s un autre nombre impair compris entre les limites

$$(1) \qquad \sqrt{3k-2} - 1, \quad \sqrt{4k}.$$

On pourra toujours résoudre simultanément en nombres entiers

(1) *Exerc. de Math.*, t. I, p. 273, et *Mémoires de l'Institut.*

les deux équations

$$(2)\qquad \begin{cases} k = t^2 + u^2 + v^2 + w^2, \\ s = t + u + v + w. \end{cases}$$

Un lemme semblable (¹) a lieu quand k est impairement pair et s pair quelconque.

Legendre a conclu de ces deux lemmes quelques théorèmes (²) perfectionnant le théorème de Fermat.

On peut remarquer que, plus généralement, des théorèmes semblables ont lieu pour les nombres de la forme

$$\frac{\alpha}{2}x^2 + \frac{\beta}{2}x + \gamma,$$

où $\alpha > 0$, α, β, γ entiers, et où α et β n'ont d'autre diviseur commun que 1 ou 2 et sont à la fois pairs ou impairs. Il suffit évidemment de considérer les nombres

$$(3)\qquad \frac{\alpha}{2}x^2 + \frac{\beta}{2}x.$$

Les raisonnements étant de tous points semblables à ceux de Legendre, nous pourrons abréger.

Soit un nombre A qui soit la somme de quatre nombres (3)

$$\frac{\alpha}{2}t^2 + \frac{\beta}{2}t, \qquad \frac{\alpha}{2}u^2 + \frac{\beta}{2}u, \qquad \frac{\alpha}{2}v^2 + \frac{\beta}{2}v, \qquad \frac{\alpha}{2}w^2 + \frac{\beta}{2}w.$$

On aura

$$(4)\qquad A = \frac{\alpha}{2}k + \frac{\beta}{2}s.$$

Nous ne considérerons que les cas où k et s sont impairs; les cas où k est impairement pair et s pair quelconque se traiteraient de même.

Réciproquement, A étant un nombre donné, si l'on peut déterminer k et s de manière qu'ils soient impairs, et satisfassent à (4) et (1), l'application du lemme précité donnera au moins une décomposition de A en quatre nombres de la forme (3).

(¹) LEGENDRE, *Théorie des nombres*, 3ᵉ édit., t. II, p. 338.

(²) *Ibid.*, p. 351 et suiv., théorèmes V à IX.

Or les inégalités

$$\sqrt{3k-2}-1<s<\sqrt{4k}$$

donnent facilement si $A>2\alpha$

$$(5)\qquad \frac{-2\alpha-3\beta+\sqrt{(2\alpha+3\beta)^2-4\alpha(3\alpha-6A)}}{2\alpha}<s<\frac{-2\beta+2\sqrt{\beta^2+2A\alpha}}{\alpha}.$$

On pourra prendre A assez grand pour qu'on ait au moins λ valeurs de s impaires consécutives satisfaisant à (5), λ étant arbitraire; il est même facile de trouver une limite inférieure de A en fonction de λ.

Soient $s_1, s_2, \ldots, s_\lambda$ ces valeurs, $k_1, k_2, \ldots, k_\lambda$ les valeurs correspondantes de k, entières ou non, tirées de (4) :

$$(6)\qquad k_i=\frac{2A-\beta s_i}{\alpha}.$$

Considérons les nombres $2A-\beta s_i$.

1° α et β sont impairs.

Si l'on a

$$2A-\beta s_i\equiv 2A-\beta s_j \pmod{\alpha},$$

il faut, puisqu'ici α et β sont premiers entre eux par hypothèse,

$$s_i-s_j\equiv 0 \pmod{\alpha}.$$

Or, s_i et s_j étant impairs, s_i-s_j est pair; par suite

$$s_i-s_j\equiv 0 \pmod{2\alpha}.$$

Prenant alors

$$\lambda\geq\alpha,$$

on voit que α nombres consécutifs, pris parmi les nombres $s_1, s_2, \ldots, s_\lambda$, donnent des valeurs de $2A-\beta s_i$ incongrues (mod α), et par suite l'un d'eux, s', est tel que

$$2A-\beta s'\equiv 0 \pmod{\alpha}.$$

Mais $2A-\beta s'$ est évidemment impair, en sorte que

$$k'=\frac{2A-\beta s'}{\alpha}$$

est impair.

L'application du lemme précité à ces valeurs k', s' donnera une décomposition de A en une somme de quatre nombres de la forme voulue.

Ce procédé donnera évidemment autant de valeurs de k', s' qu'il y a d'unités dans $\frac{\lambda}{\alpha}$. Donc

THÉORÈME I. — *Si α et β sont impairs et premiers entre eux, tout nombre* A, *supérieur à une certaine limite fonction de α et β, est la somme de quatre nombres de la forme*

$$\frac{\alpha}{2}x^2 + \frac{\beta}{2}x \qquad (\alpha > 0).$$

On peut même assigner une limite inférieure de A *telle que cette décomposition ait lieu de ρ manières différentes, ρ étant arbitrairement choisi.*

Si $\alpha = \frac{m}{2}$, $\beta = \frac{-(m-2)}{2}$, on retrouve le théorème V de Legendre précité.

2° α est impairement pair, β est pair quelconque.

Par hypothèse α et β ont pour plus grand commun diviseur 2.

Si $s_i \equiv s_j \pmod{\alpha}$, $2A - \beta s_i$ et $2A - \beta s_j$ ont même résidu $(\mathrm{mod}\ \alpha)$.

Considérons parmi les nombres impairs $s_1, s_2, \ldots, s_\lambda$ où $\lambda \geq \frac{\alpha}{2}$, $\frac{\alpha}{2}$ nombres consécutifs et les nombres correspondants de la forme $2A - \beta s_i$. Ces nombres sont pairs et sont incongrus $(\mathrm{mod}\ \alpha)$, car

$$2A - \beta s_i \equiv 2A - \beta s_l \pmod{\alpha}$$

donne

$$\frac{\beta}{2}s_i \equiv \frac{\beta}{2}s_l \left(\mathrm{mod}\ \frac{\alpha}{2}\right)$$

et, puisque $\frac{\beta}{2}$ et $\frac{\alpha}{2}$ sont ici premiers entre eux,

$$s_i \equiv s_l \left(\mathrm{mod}\ \frac{\alpha}{2}\right),$$

ce qui est impossible, $s_i - s_l$ étant pair et $< \alpha$. Donc l'un de ces nombres $2A - \beta s'$ est $\equiv 0 \pmod{\alpha}$. α étant impairement pair,

$k' = \frac{2A - \beta s'}{\alpha}$ sera impair si $2A - \beta s'$ est impairement pair. Par suite

THÉORÈME II. — *On a un théorème semblable au théorème I, α étant impairement pair, quand* A *est impair et* β *pairement pair, et quand* A *est pair et* β *impairement pair* $\left(\frac{\alpha}{2}$ *et* $\frac{\beta}{2}$ *premiers entre eux*$\right)$.

L'un de ces deux résultats comporte une extension partielle du théorème VI de Legendre.

3° α est pairement pair, β est impairement pair.

Considérons encore parmi les nombres impairs $s_1, s_2, \ldots, s_\lambda$, où $\lambda \geqq \frac{\alpha}{2}$, $\frac{\alpha}{2}$ nombres consécutifs, et les nombres correspondants de la forme $2A - \beta s_i$. Les $\frac{\alpha}{4}$ premiers d'entre eux sont incongrus (mod α), car on aurait sans cela

$$\frac{\beta}{2}(s_i - s_l) \equiv 0 \quad \left(\mathrm{mod}\ \frac{\alpha}{2}\right),$$

d'où

$$s_i - s_l \equiv 0 \quad \left(\mathrm{mod}\ \frac{\alpha}{2}\right).$$

Dès lors, si ces $\frac{\alpha}{4}$ nombres sont tous $\equiv 0 \pmod 4$, ou si A est impair, l'un d'eux $2A - \beta s'$ est $\equiv 0 \pmod \alpha$, et

$$k' = \frac{2A - \beta s'}{\alpha}.$$

Si k' est impair on obtient une décomposition cherchée du nombre A. Si k' est pair on considérera

$$s'' = s' + \frac{\alpha}{2}$$

et

$$k'' = \frac{2A - \beta\left(s' + \frac{\alpha}{2}\right)}{\alpha} = \frac{2A - \beta s'}{\alpha} - \frac{\beta}{2} = k' - \frac{\beta}{2};$$

k'' sera impair et l'on obtiendra encore la décomposition cherchée. Donc :

THÉORÈME III. — *On a un théorème semblable au théorème I, quand* α *est pairement pair,* β *impairement pair et* A *impair* $\left(\frac{\alpha}{2}$ *et* $\frac{\beta}{2}$ *premiers entre eux*$\right)$.

Ce résultat, joint à l'un de ceux obtenus au théorème II, équivaut à une extension complète du théorème VI de Legendre.

Il nous suffira maintenant d'indiquer qu'en appliquant le second des lemmes précités on obtiendra par la même méthode des résultats du même genre comportant des extensions des théorèmes VII, VIII et IX de Legendre.

II.

Des résultats analogues peuvent s'obtenir pour les nombres de la forme

$$\frac{\alpha}{2}x^4+\frac{\beta}{2}x^2.$$

Il suffit de s'appuyer sur le théorème suivant (1), dû à Liouville :

THÉORÈME. — *Soit* $2n=x^2+y^2+z^2+t^2$; *si l'on pose*

$$(7)\qquad \begin{cases} 2x_1=x+y+z+t, & 2x_2=-x+y+z+t,\\ 2y_1=x+y-z-t, & 2y_2=-x+y-z-t,\\ 2z_1=x-y+z-t, & 2z_2=-x-y+z-t,\\ 2t_1=x-y-z+t, & 2t_2=-x-y-z+t, \end{cases}$$

les nombres

$$x_1,\quad y_1,\quad z_1,\quad t_1;\qquad x_2,\quad y_2,\quad z_2,\quad t_2$$

seront entiers aussi bien que x, y, z, t, *et l'on aura, en posant*

$$\Sigma x^2=x^2+y^2+z^2+t^2:$$

$$(8)\qquad \Sigma x^2=\Sigma x_1^2=\Sigma x_2^2,$$

$$(9)\qquad 6n^2=\Sigma x^4+\Sigma x_1^4+\Sigma x_2^4.$$

Liouville en a tiré ce corollaire :

---

(1) *Voir* LE BESGUE, *Exercices d'Analyse numérique*, librairie Leiber et Faraguet, Paris, 1859, p. 113.

Corollaire. — Tout nombre est la somme de δ bicarrés au plus ($\delta \leqq 53$).

En effet, soit $6k + r$, ($r \leqq 5$), un nombre quelconque; on sait qu'on a

$$k = f^2 + g^2 + h^2 + e^2, \tag{10}$$

et en remarquant que r est la somme d'au plus 5 bicarrés égaux à l'unité, et appliquant la formule (9), on obtient $6k + r$ sous la forme d'une somme d'au plus 53 bicarrés.

Mais l'on peut en tirer quelque chose de plus.

D'après (8) et (9), le théorème précédent donne

$$\begin{aligned} 6n^2 &= \Sigma x^4 + \Sigma x_1^4 + \Sigma x_2^4, \\ 6n &= \Sigma x^2 + \Sigma x_1^2 + \Sigma x_2^2 \end{aligned}$$

simultanément.

On aura donc simultanément

$$\left\{\begin{array}{ll} 6f^2 = \Sigma x^4 + \Sigma x_1^4 + \Sigma x_2^4, & 6f = \Sigma x^2 + \Sigma x_1^2 + \Sigma x_2^2, \\ 6g^2 = \Sigma x'^4 + \Sigma x_1'^4 + \Sigma x_2'^4, & 6g = \Sigma x'^2 + \Sigma x_1'^2 + \Sigma x_2'^2, \\ 6h^2 = \Sigma x''^4 + \Sigma x_1''^4 + \Sigma x_2''^4, & 6h = \Sigma x''^2 + \Sigma x_1''^2 + \Sigma x_2''^2, \\ 6e^2 = \Sigma x'''^4 + \Sigma x_1'''^4 + \Sigma x_2'''^4, & 6e = \Sigma x'''^2 + \Sigma x_1'''^2 + \Sigma x_2'''^2. \end{array}\right. \tag{11}$$

D'ailleurs, l'unité étant à la fois un bicarré et un carré, on voit que les deux nombres

$$6(f^2 + g^2 + h^2 + e^2) + r, \qquad 6(f + g + h + e) + r$$

seront respectivement la somme de δ bicarrés et carrés correspondants.

La forme de ces nombres suggère de suite l'idée d'appliquer les lemmes précités de Cauchy et Legendre : nous nous contenterons d'appliquer le lemme de Cauchy.

D'après ce lemme on peut déterminer f, g, h et e de façon que (10) ait lieu en même temps que

$$l = f + g + h + e, \tag{12}$$

k et l étant impairs, pourvu que

$$\sqrt{3k - 2} - 1 < l < \sqrt{4k}. \tag{13}$$

Dès lors, posant

$$(14)\qquad \begin{cases} 3A = \frac{\alpha}{2} 6k + \frac{\beta}{2} 6l \\ \text{ou} \\ A = \alpha k + \beta l \end{cases}$$

($\alpha > 0$ et β étant à la fois pairs ou impairs et n'ayant d'autre commun diviseur que 1 ou 2), si l'on peut déterminer k et l entiers impairs et satisfaisant à (13) et (14), le nombre 3A sera la somme de $\delta - 5$ nombres de la forme

$$(15)\qquad \frac{\alpha}{2} x^4 + \frac{\beta}{2} x^2$$

et, en posant

$$(16)\qquad r' = \frac{\alpha}{2} r + \frac{\beta}{2} r = r \frac{\alpha + \beta}{2},$$

le nombre $3A + r'$ sera la somme de $\delta - 5 + r$ nombres de la même forme (15).

D'abord on voit encore, par des inégalités analogues à (5), qu'on peut prendre A assez grand pour qu'on ait au moins λ valeurs impaires consécutives de l satisfaisant à (13), λ étant arbitrairement choisi.

Soient $l_1, l_2, \ldots, l_\lambda$ ces valeurs, $k_1, k_2, \ldots, k_\lambda$ les valeurs correspondantes de k, entières ou non, tirées de (14).

1° α et β sont impairs.

En prenant $\lambda \geqq \alpha$ et A pair, on trouve encore une valeur de k entière et impaire, telle que (14) ait lieu.

Tout nombre pair 3A est donc ici décomposable en $\delta - 5$ nombres de la forme (15). Les nombres $3A + r'$ (A pair) sont décomposables, d'après (16), en δ nombres au plus de la forme (15) et l'on peut dire :

Théorème V. — *Soient α et β entiers impairs et premiers entre eux; suivant que $\frac{\alpha + \beta}{2}$ aura avec 6 pour plus grand commun diviseur* 1, 2, 3 ou 6, *on peut prendre a' assez grand pour que tout nombre de la forme $6a + r''$, avec respectivement $a \geqq a'$,*

r'' égal à

0, 1, 2, 3, 4, 5
0, 2, 4
0, 3
0,

soit la somme d'au plus δ *nombres de la forme*

$$\frac{\alpha}{2}x^4+\frac{\beta}{2}x^2 \qquad (\delta\leqq 53).$$

2° α est impairement pair, β est pair.

A est pair; on pourra encore trouver l impair et tel que $A-\beta l\equiv 0 \pmod{\alpha}$. Alors

$$k=\frac{A-\beta l}{\alpha}$$

sera impair si $A-\beta l$ est impairement pair.

De plus, ici, $\frac{\alpha+\beta}{2}$ sera pair ou impair suivant que β sera impairement ou pairement pair.

Théorème V. — *Soient* α *impairement pair,* β *pair et* $\frac{\alpha}{2}$ *et* $\frac{\beta}{2}$ *premiers entre eux.*

Quand β *est pairement pair, suivant que* $\frac{\alpha+\beta}{2}$, *qui est impair, aura avec* 6 *le plus grand commun diviseur* 1 *ou* 3, *on peut prendre* a' *assez grand pour que tout nombre de la forme* $6a+r''$ *avec* $a\geqq a'$ *et respectivement* r'' *égal à*

0, 1, 2, 3, 4, 5
0, 3,

soit la somme d'au plus δ' *nombres de la forme*

$$\frac{\alpha}{2}x^4+\frac{\beta}{2}x^2 \qquad (\delta'\leqq 59).$$

Quand β *est impairement pair, suivant que* $\frac{\alpha+\beta}{2}$, *qui est pair, aura avec* 12 *le plus grand commun diviseur* 2, 4, 6 *ou* 12, *on peut prendre* a' *assez grand pour que tout nombre de la*

forme $2(6a + r'')$ *avec* $a \geqq a'$ *et respectivement* r'' *égal à*

0, 1, 2, 3, 4, 5
0, 2, 4
0, 3
0 ,

soit la somme d'au plus δ *nombres de la forme*

$$\frac{\alpha}{2} x^4 + \frac{\beta}{2} x^2, \qquad (\delta \leqq 53).$$

3° α pairement pair, β impairement pair.

On peut encore trouver l impair et tel que $A - \beta l \equiv 0 \pmod{\alpha}$, si A impairement pair. Si

$$k = \frac{A - \beta l}{\alpha}$$

n'était pas impair, en posant $l' = l + \frac{\alpha}{2}$,

$$k' = \frac{A - \beta l}{\alpha} - \frac{\beta}{2} = k - \frac{\beta}{2}$$

est impair.

Ici $\frac{\alpha + \beta}{2}$ est impair.

THÉORÈME VI. — *Soient* α *pairement pair,* β *impairement pair et* $\frac{\alpha}{2}$ *et* $\frac{\beta}{2}$ *premiers entre eux : suivant que* $\frac{\alpha + \beta}{2}$, *qui est impair, aura avec* 6 *le plus grand commun diviseur* 1 *ou* 3, *on peut prendre* a' *assez grand pour que tout nombre de la forme* $6a + r''$ *avec* $a \geqq a'$ *et respectivement* r'' *égal à*

0, 1, 2, 3, 4, 5
0, 3,

soit la somme d'au plus δ' *nombres de la forme*

$$\frac{\alpha}{2} x^4 + \frac{\beta}{2} x^2, \qquad (\delta' \leqq 59).$$
