SUR UNE CONJECTURE D'ABEL

par Abdoulaye IDE SALEY

Ce présent travail a pour but de donner une généralisation et une démonstration très élémentaire des formules de Barlow-Abel en rapport avec le dernier théorème de Fermat. Ce qui nous permettra de donner une démonstration très simple de la plupart des résultats obtenus sur la conjecture d'Abel et de généraliser le théorème de Sophie Germain aux entiers sans facteur carré.

PROPOSITION 1. — *Soient a, b et c des entiers relativement premiers entre eux et non nuls vérifiant : $a^n + b^n = c^n$ avec $a < b < c$ et n un entier positif impair sans facteur carré (i.e. p premier et $p/n \Rightarrow p^2 \nmid n$).*

Alors pour tout diviseur premier p de $c-a$, on a p/b ; posons $\alpha = \mathrm{ord}_p(c-a)$ et $\beta = \mathrm{ord}_p(b)$ alors $\alpha = \beta n$ si $p \nmid n$ (resp. $\alpha = \beta n - 1$ si p/n).

Preuve. — Posons $c - a = d \geq 2$. Alors $c^n = a^n + \sum_{n=1}^{n} \binom{n}{r} d^r \cdot a^{n-r} = a^n + b^n$. Donc $b^n = d^n + td$ avec

$$t = na^{n-1} + \binom{n}{2} da^{n-2} + \cdots + nd^{n-2}a\,.$$

Soit p un diviseur premier de d. Alors p/b^n donc p/b. Écrivons

$$d = p^{\alpha} d' \text{ avec } (d', p) = 1 \text{ et } b = p^{\beta} b' \text{ avec } (b', p) = 1\,.$$

On a alors $\alpha, \beta \geq 1$ et

$$p^{\beta n - \alpha} b'^n = p^{\alpha(n-1)} d'^n + d' t$$

d'où en particulier $\alpha \leq \beta n$. De plus, n étant impair $n - 1 \geq 2$.

Supposons que $\beta n \geq \alpha + 2$. Alors $p^2/d't$ donc p^2/t car $(d', p) = 1$. Ainsi p/t. Mais $t = na^{n-1} + d(\cdots)$. Donc p/na^{n-1}. On en déduit que p/n car $(a, b) = 1$.

Or $\binom{n}{2} = \frac{n(n-1)}{2}$ donc $p/\binom{n}{2}$. Mais

$$t = na^{n-1} + \binom{n}{2} da^{n-2} + d^2(\cdots)$$

Mots-clés : théorème de Fermat, formules de Barlow et d'Abel.
Classification math. : 11D41, 11A99.

et donc

$$t = na^{n-1} + p^2(\cdots)$$

Comme p^2/t, on a p^2/na^{n-1} ; autrement dit p^2/n. Ce qui contredit n est sans facteur carré.

Par conséquent, $\beta n < \alpha + 2$ or $\beta n \geq \alpha$. On en déduit que : $\alpha = \beta n$ ou $\alpha = \beta n - 1$. Mais si $\alpha = \beta n - 1$ on en déduit aussi que p/n d'après le raisonnement précédent.

Réciproquement si p/n alors p/t. Donc $p/p^{\beta n-\alpha}b'^n$, soit $p/p^{\beta n-\alpha}$; on en déduit que $\alpha = \beta n - 1$. Ainsi p/n si et seulment si $\alpha = \beta n - 1$. Ce qui achève la preuve de la proposition 1. ∎

Corollaire 1. — *Soit n un entier impair sans facteur carré. Si $a^n + b^n = c^n$ avec $a < b < c$ et a, b, c des entiers positifs non nuls relativement premiers entre eux alors :*

1) Il existe des nombres premiers distincts $p_1, \ldots, p_s$ tels que :

$$c - a = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \text{ avec } p_i/b, \forall i$$

avec

$$\alpha_i = n \operatorname{ord} p_i(b), \text{ si } p_i \not\asymp n$$

ou

$$\alpha_i = n \operatorname{ord} p_i(b) - 1, \text{ si } p_i/n$$

2) Il existe des nombres premiers distincts $q_1, \ldots, q_r$ tels que :

$$a + b = q_1^{\beta_1} \cdots q_r^{\beta_r} \text{ avec } q_i/c, \forall i$$

avec

$$\beta_i = n \operatorname{ord} q_i(c), \text{ si } q_i \not\asymp n$$

ou

$$\beta_i = n \operatorname{ord} q_i(c) - 1, \text{ si } q_i/n\,.$$

3) On a une décomposition du même type pour $c - b$ si $c - b \neq 1$.

Preuve du corollaire 1.

1) On applique la proposition 1 à tous les diviseurs premiers de $c - a$;

2) Il suffit d'écrire $(-b)^n = a^n + (-c)^n$ et de remarquer que la proposition 1 s'applique aux entiers négatifs.

3) On raisonne comme pour *1)*, en échangeant les rôles de a et b.

Corollaire 2. — *Soit n un nombre premier supérieur à 3 et soient a, b, c des entiers positifs non nuls relativement premiers entre eux vérifiant : $a^n + b^n = c^n$. Alors :*

1) **Formules de Barlow** *(1810).*

Si $(n, abc) = 1$ *alors il existe des entiers* $r, s, t \geq 1$ *tels que :*

$$\begin{cases} c - a = r^n \\ a + b = s^n \quad \text{avec } r/b,\ s/c \text{ et } t/a \\ c - b = t^n \quad \text{et } (\frac{a}{t}, t) = (\frac{b}{r}, r) = (\frac{c}{s}, s) = 1. \end{cases}$$

2) **Formules d'Abel** *(1823).*

Si n/c *alors :*

$$a + b = n^{\beta n - 1} t^n \text{ où } \beta = \mathrm{ord}_n(c)$$
$$(t, n) = 1, \quad t/c\,.$$

De plus, il existe des entiers $r, s \geq 1$ *tels que :*

$$\begin{cases} c - a = r^n \\ c - b = s^n \quad \text{avec } r/b,\ s/a \text{ et } (\frac{a}{s}, s) = (\frac{b}{r}, r) = 1. \end{cases}$$

Preuve du corollaire 2. — Elle est immédiate d'après le corollaire 1.

Remarque. — D'après le corollaire 1, l'affirmation ci-dessus de Barlow est encore vraie lorsque n est un entier impair sans facteurs carrés.

Corollaire 3. — *Soient* n *un entier impair sans facteur carré et* a, b, c *des entiers (non nuls) positifs, relativement premiers entre eux vérifiant* $a^n + b^n = c^n$ *avec* $a < b < c$.

Alors :

1) b *et* c *admettent au moins deux facteurs premiers distincts (Lucas 1891).*

2) Si a *admet un seul diviseur premier alors* $c - b = 1$ *(Jonquières 1884).*

3) Si $c - b \neq 1$ *alors* a *admet au moins deux facteurs premiers distincts.*

Ces résultats 1), 2) et 3) sont une conséquence du théorème de Möller (1955).

4) Plus généralement :

i) Si $c - a$ *admet* r *diviseurs premiers distincts alors* b *admet au moins* $r + 1$ *diviseurs premiers distincts.*

ii) Si $c - b \neq 1$ *et si* $c - b$ *admet* r *diviseurs premiers distincts alors* a *admet au moins* $r + 1$ *diviseurs premiers distincts.*

Tous ces résultats peuvent s'établir directement à partir du théorème de Zsigmondy (1892) sur les facteurs premiers primitifs.

Preuve du corollaire 3.

1) Supposons $b = p^\beta$ où p est premier et $\beta \geq 1$.

1$^{\text{er}}$ **cas** : $p \nmid n$

Alors $c-a = p^{n\beta}$ et $c^n = (a+p^{n\beta})^n = a^n + p^{n\beta}$. Soit : $p^{n\beta} = p^{n^2\beta} + (\text{termes} > 0)$. Ce qui est impossible.

2^e cas : p/n

Alors $c-a = p^{n\beta-1}$ et $c^n = a^n + p^{(n\beta-1)n} + (\cdots)$. Soit : $p^{n\beta} = p^{(n\beta-1)n} + (\text{termes} > 0)$ or $(n\beta-1)n = n\beta\left(n - \frac{1}{\beta}\right) > n\beta$. Donc l'avant dernière égalité est impossible.

2) De même, supposons $c = p^\beta$

1^er cas : $p \not> n$

Alors $a + b = p^{n\beta}$ et

$$\begin{aligned} c^n = p^{\beta n} &= a + b \cdot \frac{a^n + b^n}{a+b} \\ &= p^{\beta n} \cdot \frac{a^n + b^n}{a+b} \,. \end{aligned}$$

Ce qui est impossible car $\frac{a^n+b^n}{a+b} > 1$.

2^e cas : p/n

Alors $a + b = p^{\beta n-1}$. Et $c^n = p^{\beta n} = p^{\beta n-1} \cdot \frac{a^n+b^n}{a+b}$, or $\frac{a^n+b^n}{a+b} > n$. En effet :

$$\begin{aligned} a^n + b^n - na - nb &= a(a^{n-1} - n) + b(b^{n-1} - n) \\ &> 2^{n-1} - n + 2^{n-1} - n > 0 \,. \end{aligned}$$

Par suite, l'égalité $p^{\beta n} = p^{\beta n-1} \cdot \frac{a^n+b^n}{a+b}$ est impossible.

3) est la contraposée de *2)* et *3)* s'établit de la même manière que le *1)*.

4)

i) Supposons que b et $c-a$ ont mêmes diviseurs premiers.

D'après le corollaire 1,

$$c - a = (p_1^{\alpha_1} \cdots p_r^{\alpha_r})^n q_1^{\beta_1 n-1} \cdots q_t^{\beta_t n-1}$$

et

$$b = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_t^{\beta_t}$$

où les p_j et q_i sont des nombres premiers distincts et $q_i/n, \forall i$.

Alors $b^n \leq (c-a) \cdot n$. Or $(c-a)(a^{n-1} + a^{n-2} - c + \cdots c^{n-1}) = b^n$. Par conséquent

$$(c-a)(a^{n-1} + a^{n-2}c + \cdots + c^{n-1}) \leq (c-a)n \,.$$

Ce qui est absurde, car $0 < a < c$.

ii) Le raisonnement est identique au cas précédent.

PROPOSITION 2 (généralisation du théorème de Legendre aux entiers impairs positifs sans facteur carré). — *Soient n un entier positif impair sans facteur carré et p un nombre premier distinct de n tels que les conditions suivantes soient vérifiées :*

1) n n'est pas congru à une puissance $n^{\text{ième}}$ d'un entier modulo p.

2) Si $a^n + b^n \equiv c^n$ modulo (p) alors p divise a, b ou c.

Alors il n'existe pas d'entiers positifs non nuls, relativement premiers entre eux a, b, c tels que $a^n + b^n = c^n$ et $(n, abc) = 1$.

Preuve. — Supposons qu'il existe un tel couple d'entiers a, b, c.

D'après *2)*, on a p/a, b ou c.

Supposons p/a. Alors d'après la remarque suivant le corollaire 2, il existe des entiers $r, s, t \geq 1$ tels que :

$$-r^n + s^n + t^n = 2a \equiv 0 \mod p\,.$$

Donc d'après *2)* le premier p divise r, s ou t (r, s, t vérifient les propriétés de l'hypothèse *2)* ci-dessus). On en déduit que p/t. On a :

$$c \equiv b \mod p$$
$$s_1^n \equiv b^{n-1} \mod p \text{ où } s_1 = \frac{c}{s} \text{ car } (a+b)s_1^n = a^n + b^n$$
$$t_1^n \equiv n s_1^n \mod p \text{ où } t_1 = \frac{a}{t} \text{ car } t_1^n = \frac{c^n - b^n}{c-b} \equiv n b^{n-1} \equiv n s_1^n \mod p\,.$$

Comme $p \nmid s_1$ choisissons s_1' tel que $s_1 s_1' \equiv 1 \mod p$ (ce qui est possible d'après le théorème de Bezout).

Alors $(s' t_1)^n \equiv n \mod p$. Ce qui contredit l'hypothèse *1)*.

PROPOSITION 3 (généralisation du théorème de Sophie Germain aux entiers impairs positifs sans facteur carré). — *Soit n un entier positif impair sans facteur carré. Si $2n+1$ est premier alors il n'existe pas d'entiers positifs non nuls relativement premiers entre eux a, b, c tels que $a^n + b^n = c^n$ et $(n, abc) = 1$.*

Preuve. — Il suffit de montrer que n et $p = 2n+1$ vérifient les conditions *1)* et *2)* de la proposition 2.

1) Si $n \equiv a^n \pmod p$ alors :

$$\pm 1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^n \equiv n \pmod p\,.$$

Ainsi

$$n \equiv \pm 1 \mod p\,.$$

Ce qui est impossible car $n < p$.

Donc l'hypothèse *1)* de la proposition 2 est vérifiée pour n et p.

2) Supposons $a^n + b^n \equiv c^n \mod p$ et $p \nmid a \cdot b \cdot c$. Comme $n = \frac{p-1}{2}$ on a d'après le petit théorème de Fermat :

$$a^n \equiv \pm 1 \pmod p$$
$$b^n \equiv \pm 1 \pmod p$$
$$c^n \equiv \pm 1 \pmod p .$$

Ainsi $0 = a^n + b^n - c^n \equiv \pm 1 \pm 1 \pm 1 \mod(p)$. Ce qui est impossible.

Ains l'hypothèse *2)* de la proposition 2 est aussi vérifiée pour n et p.

Ce qui achève la preuve de la proposition 3. ■

– ◊ –

Université de Grenoble I
Institut Fourier
UMR 5582
UFR de Mathématiques
B.P. 74
38402 ST MARTIN D'HÈRES Cedex (France)

(28 janvier 1998)