Une forme générale de la conjecture *abc*

Nicolas Billerey (avec l'aide de
Manuel Pégourié-Gonnard)

6 août 2009

Dans [Lan99a], M. Langevin montre que la conjecture *abc* est équivalente à la conjecture suivante.

Conjecture 0.1 *Soient $F \in \mathbf{Z}[X,Y]$ une forme homogène séparable de degré ≥ 3 et ε un réel > 0. Il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que pour tout couple (a,b) d'entiers non nuls premiers entre eux, on a :*

$$\mathrm{rad}(F(a,b)) \geq C_{\varepsilon,F} \max(|a|,|b|)^{\deg(F)-2-\varepsilon},$$

où $\mathrm{rad}(n)$, $n \in \mathbf{N}^*$, désigne le produit de tous les nombres premiers divisant n.

Remarque. Par convention $\mathrm{rad}(0) = \infty$.

L'objectif ce cette *Note* est de démontrer le résultat de Langevin en suivant une méthode géométrique esquissée dans l'article de [GT02] (voir également [Hin08, pp.244-246]).

1 Le résultat de Langevin

On commence par rappeler l'énoncé de la conjecture *abc* sous sa forme classique.

Conjecture 1.1 (*abc*) *Soit ε un réel > 0. Il existe une constante $C(\varepsilon) > 0$ telle que pour tout triplet (a,b,c) d'entiers non nuls premiers entre eux vérifiant $a+b=c$, on ait*

$$\mathrm{rad}(abc) \geq C(\varepsilon) \max(|a|,|b|)^{1-\varepsilon}.$$

L'objectif de ce § est de démontrer la proposition suivante.

Proposition 1.2 *La conjecture* abc *est équivalente à la conjecture 0.1.*

La conjecture 0.1 implique la conjecture *abc* : il suffit de prendre

$$F(X,Y) = XY(X+Y).$$

Intéressons-nous donc à la réciproque. La démonstration requiert plusieurs étapes.

1.1 1. Le théorème de Mason

Notation. Étant donné un polynôme $f \in \mathbf{Z}[X]$, la notation $\{f = 0\}$ désigne l'ensemble des racines complexes de f. En particulier, $|\{f = 0\}|$ est le nombre de racines de f comptées sans multiplicité.

Théorème 1.3 (Mason) *Soient a, b et c trois polynômes de $\mathbf{Z}[t]$ non constants et premiers entre eux vérifiant :*

$$a(t) + b(t) = c(t).$$

Alors, on a :

$$\max(\deg(a), \deg(b), \deg(c)) \leq |\{abc = 0\}| - 1. \tag{1}$$

Démonstration. On considère a, b et c comme dans l'énoncé du théorème. L'application

$$\phi \ : t \mapsto \frac{a(t)}{c(t)}$$

est une application rationnelle $\mathbf{P}^1 \to \mathbf{P}^1$ non constante définie sur $\mathbf{Q}$. De plus, remarquons que

- si $\phi(\infty) \neq 0$, alors $\phi^{-1}(0) = \{a = 0\}$
- si $\phi(\infty) \neq \infty$, alors $\phi^{-1}(\infty) = \{c = 0\}$,
- si $\phi(\infty) \neq 1$, alors $\phi^{-1}(1) = \{b = 0\}$.

Par ailleurs, ∞ appartient à l'un, au plus, des ensembles $\phi^{-1}(\infty)$, $\phi^{-1}(1)$ et $\phi^{-1}(0)$. Appliquons à présent la formule de Riemann - Hurwitz à ϕ qui est de degré $d = \max(\deg(a), \deg(c))$. On a :

$$-2 = -2d + \sum_{y \in \mathbf{P}^1} \left(d - |\phi^{-1}(y)|\right).$$

Chacun des termes de la somme (finie) du membre de droite de l'égalité ci-dessus étant ≥ 0, on a la minoration suivante :

$$-2 \geq -2d + \sum_{y \in \{0,1,\infty\}} \left(d - |\phi^{-1}(y)|\right). \tag{2}$$

(Avec égalité si ϕ est non ramifiée hors de $\{0, 1, \infty\}$.) On en déduit

$$-2 \geq -2d + 3d - \left(|\phi^{-1}(0)| + |\phi^{-1}(1)| + |\phi^{-1}(\infty)|\right).$$

Soit encore

$$d \leq |\phi^{-1}(0)| + |\phi^{-1}(1)| + |\phi^{-1}(\infty)| - 2.$$

Or, les polynômes a, b et c étant premiers entre eux on a d'après ce qui précède :

$$|\phi^{-1}(0)| + |\phi^{-1}(1)| + |\phi^{-1}(\infty)| \leq |\{abc = 0\}| + 1. \tag{3}$$

(Avec égalité si $\phi(\{\infty\}) \subset \{0, 1, \infty\}$.) On en déduit l'inégalité

$$d \leq |\{abc = 0\}| - 1.$$

Comme par ailleurs, $b = c - a$, on a

$$\deg(b) \leq d$$

puis $d = \max(\deg(a), \deg(b), \deg(c))$. D'où le résultat.

1.2 2. Le théorème de Belyi

Adoptons la définition usuelle suivante.

Définition 1.4 *Soit S un ensemble fini de $\mathbf{P}^1(\overline{\mathbf{Q}})$. On appelle fonction de Belyi associée à S toute application rationnelle non constante $\phi : \mathbf{P}^1 \to \mathbf{P}^1$ définie sur $\mathbf{Q}$ vérifiant les propriétés suivantes :*

1. *la fonction ϕ est non ramifiée hors de 0, 1 et ∞ ;*
2. *on a $\phi(S) \subset \{0, 1, \infty\}$.*

Concernant l'existence de telles fonctions on a le résultat suivant (*cf.* [Ser97]).

Théorème 1.5 (Belyi) *Soit $S \subset \mathbf{P}^1(\overline{\mathbf{Q}})$ un ensemble fini. Alors, il existe une fonction de Belyi associée à S.*

Vu la démonstration du théorème de Mason donnée ci-dessus, on a le lemme suivant.

Lemme 1.6 *Soit ϕ une fonction de Belyi associée à $\{\infty\}$ et $a(t)$, $c(t)$ deux polynômes de $\mathbf{Z}[t]$ non constants et premiers entre eux tels que $\phi(t) = a(t)/c(t)$. Alors, on a l'égalité*

$$\max(\deg(a), \deg(b), \deg(c)) = |\{abc = 0\}| - 1,$$

où l'on a posé $b(t) = c(t) - a(t)$.

Démonstration. Dans la démonstration du théorème 1.3, on a deux inégalités dont résulte celle du théorème : (2) et (3). On a égalité dans (2) si ϕ est non ramifiée hors de $\{0, 1, \infty\}$. On a égalité dans (3) si $\phi(\{\infty\}) \subset \{0, 1, \infty\}$. Or c'est bien le cas par définition d'une fonction de Belyi. D'où le lemme.

1.3 3. Sur certains cas d'égalité dans le théorème de Mason

Proposition 1.7 *Soit $f \in \mathbf{Z}[t]$ un polynôme séparable. Alors, il existe $a(t)$, $b(t)$ et $c(t)$ trois polynômes non constants de $\mathbf{Z}[t]$ premiers entre eux tels que :*

1. *$a(t) + b(t) = c(t)$;*
2. *$\max(\deg(a), \deg(b), \deg(c)) = |\{abc = 0\}| - 1$;*
3. *deux des trois polynômes a, b et c sont de même degré et le troisième est de degré strictement plus petit ;*
4. *le polynôme f divise abc.*

Démonstration. Soit $S = \{f = 0\} \cup \{\infty\}$. C'est un sous-ensemble fini de $\mathbf{P}^1(\overline{\mathbf{Q}})$. D'après le théorème 1.5, il existe une fonction de Belyi ϕ associée à S. Posons, $\phi = a/c$, où a et c sont deux polynômes de $\mathbf{Z}[t]$ premiers entre eux et non constants, puis $b = c - a$. Comme $\{\infty\} \subset S$, l'application ϕ est en particulier une fonction de Belyi asscoiée à $\{\infty\}$. D'après le lemme 1.6, les polynômes a, b et c satisfont aux conditions 1 et 2.

Notons $d = \max(\deg(a), \deg(b), \deg(c))$. D'après la condition 1, les trois polynômes a, b et c ne sont pas tous de degrés différents. Il y en a donc au moins deux de même de degré, et c'est d. Par ailleurs, on a supposé que $\infty \in S$, et donc $\phi(\infty) = 0$, 1 ou ∞. Autrement dit, il y a au plus deux des trois polynômes a, b et c qui sont de même degré. Finalement, parmi les trois polynômes a, b et c, deux exactement sont de même degré d. C'est la condition 3.

Par ailleurs, soit $t \in \mathbf{P}^1(\overline{\mathbf{Q}})$ tel que $f(t) = 0$. Alors, par définition, on a $t \in S$. Comme ϕ est une fonction de Belyi pour S, on a $\phi(t) = 0$, 1 ou ∞. Autrement dit, t vérifie :

$$(abc)(t) = 0.$$

Le polynôme f étant séparable on en déduit qu'il divise le produit abc. Cela démontre la proposition.

1.4 4. Fin de la démonstration

On considère F comme dans la conjecture 0.1 et on pose $f(t) = F(t, 1)$. Le polynôme f est séparable de degré

$$\deg(f) \geq \deg(F) - 1. \tag{4}$$

Soient m et n deux entiers non nuls et premiers entre eux tels que $F(m, n) \neq 0$.

Quitte à changer $F(X, Y)$ en $F(Y, X)$, on peut supposer que l'on a $m \leq n$. De même, quitte à changer $F(X, Y)$ en $F(-X, Y)$, on peut supposer que l'on a $m > 0$. On suppose donc à partir de maintenant que l'on a

$$0 < m \leq n.$$

Le polynôme f étant séparable, il existe d'après la proposition 1.7, trois polynômes a, b et c non constants de $\mathbf{Z}[t]$ premiers entre eux tels que :

1. $a(t) + b(t) = c(t)$;
2. $\max(\deg(a), \deg(b), \deg(c)) = |\{abc = 0\}| - 1$;
3. deux des trois polynômes a, b et c sont de même degré et le troisième est de degré strictement plus petit ;
4. le polynôme f divise abc.

Posons $d = \max(\deg(a), \deg(b), \deg(c))$ et homogénéisons les polynômes a, b et c en degré d :

$$\begin{aligned} A(X, Y) &= Y^d a(X/Y), \\ B(X, Y) &= Y^d b(X/Y), \\ C(X, Y) &= Y^d c(X/Y). \end{aligned}$$

D'après la condition 1, on a

$$A(m, n) + B(m, n) = C(m, n).$$

Les entiers $A(m, n)$, $B(m, n)$ et $C(m, n)$ ne sont pas nécessairement premiers entre eux. Notons D leur pgcd.

Lemme 1.8 *L'entier D est majoré indépendamment de m et n.*

Démonstration. Quitte à échanger les polynômes a, b et c, on peut supposer (dans cette démonstration) que l'on a

$$\deg a = \deg b = d.$$

Posons alors

$$a(t) = a_0 t^d + \cdots + a_d \quad \text{et} \quad b(t) = b_0 t^d + \cdots + b_d.$$

Par définition, le résultant de a et b ([Bou81, A IV.71]), noté $\mathrm{Res}(a,b)$, est le déterminant de la matrice de Sylvester M de a et b (de taille $(2d)\times(2d)$) rappelée ci-dessous :

$$M = \begin{pmatrix} a_0 & \dots & \dots & \dots & a_d & & & 0 \\ 0 & a_0 & \dots & \dots & a_{d-1} & a_d & & \\ & & \ddots & & \vdots & & \ddots & \\ & & & a_0 & a_1 & \dots & \dots & a_d \\ b_0 & \dots & \dots & \dots & b_d & & & \\ 0 & b_0 & \dots & \dots & b_{d-1} & b_d & & \\ & & \ddots & & \vdots & & \ddots & \\ 0 & & & b_0 & b_1 & \dots & \dots & b_d \end{pmatrix}.$$

On note $\{C_i\}_{1\leq i\leq 2d}$ les colonnes de la matrice M. D'après les propriétés du déterminant, on a

$$X^{2d-1}\mathrm{Res}(a,b) = \det \begin{pmatrix} X^{2d-1}a_0 & \dots & \dots & \dots & a_d & & & 0 \\ 0 & a_0 & \dots & \dots & a_{d-1} & a_d & & \\ & & \ddots & & \vdots & & \ddots & \\ & & & a_0 & a_1 & \dots & \dots & a_d \\ X^{2d-1}b_0 & \dots & \dots & \dots & b_d & & & \\ 0 & b_0 & \dots & \dots & b_{d-1} & b_d & & \\ & & \ddots & & \vdots & & \ddots & \\ 0 & & & b_0 & b_1 & \dots & \dots & b_d \end{pmatrix}.$$

Puis, en ajoutant à la première colonne de la matrice ci-dessus $X^{2d-i}Y^{i-1}C_i$ pour tout $2 \leq i \leq 2d$, on ne modifie pas la valeur du déterminant, et on obtient ainsi

$$X^{2d-1}\mathrm{Res}(a,b) = \det \begin{pmatrix} X^{d-1}A(X,Y) & \dots & \dots & \dots & a_d & & & 0 \\ X^{d-2}YA(X,Y) & a_0 & \dots & \dots & a_{d-1} & a_d & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ Y^{d-1}A(X,Y) & & & a_0 & a_1 & \dots & \dots & a_d \\ X^{d-1}B(X,Y) & \dots & \dots & \dots & b_d & & & \\ X^{d-2}YB(X,Y) & b_0 & \dots & \dots & b_{d-1} & b_d & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ Y^{d-1}B(X,Y) & & & b_0 & b_1 & \dots & \dots & b_d \end{pmatrix}.$$

D'où, en développant le déterminant ci-dessus par rapport à la première colonne :

$$X^{2d-1}\mathrm{Res}(a,b) \in (A,B)\mathbf{Z}[X,Y].$$

En raisonnant comme ci-dessus (en remplaçant la colonne C_{2d} de la matrice M par $Y^{2d-1}C_{2d}$ et en ajoutant à celle-ci la somme des colonnes $X^{2d-i}Y^{i-1}C_i$ pour $1 \leq i \leq 2d-1$), on montre de même que l'on a

$$Y^{2d-1}\mathrm{Res}(a,b) \in (A,B)\mathbf{Z}[X,Y].$$

Or, le pgcd D de $A(m,n)$, $B(m,n)$ et $C(m,n)$ est le même que celui de $A(m,n)$ et $B(m,n)$. Donc, en spécialisant les relations ci-dessus, on a en particulier,

$$D \mid n^{2d-1}\mathrm{Res}(a,b) \quad \text{et} \quad D \mid m^{2d-1}\mathrm{Res}(a,b).$$

Les entiers m et n étant premiers entre eux, on en déduit que D divise le résultant de a et b. L'entier D est donc majoré indépendamment de m et n. D'où le lemme 1.8.

Quitte à interchanger a, b et c, on peut supposer que l'on a $A(m,n) \geq 0$, $B(m,n) \geq 0$ et $C(m,n) \geq 0$.

D'après le lemme précédent, on peut appliquer la conjecture *abc* aux entiers positifs, $A(m,n)$, $B(m,n)$ et $C(m,n)$. Pour $\varepsilon > 0$, on obtient :

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \gg_{\varepsilon,F} \max(A(m,n),B(m,n))^{1-\varepsilon}. \tag{5}$$

La fin de la démonstration de la proposition 1.2 consiste à minorer convenablement le membre de droite de l'inégalité ci-dessus et majorer celui de gauche.

Majoration. Étant donné un polynôme H de l'anneau (factoriel) $\mathbf{Z}[X,Y]$, on désigne par $\mathrm{rad}(H)$ le polynôme (bien défini au signe près)

$$\mathrm{rad}(H) = \prod_{P \mid H} P,$$

où le produit porte sur les éléments irréductibles P de $\mathbf{Z}[X,Y]$.

On aura besoin du lemme suivant.

Lemme 1.9 *Le polynôme* $F(X,Y)$ *divise* $\mathrm{rad}(A(X,Y)B(X,Y)C(X,Y))$.

Démonstration. Par construction, le polynôme f divise le produit *abc*. Posons

$$(abc)(t) = f(t)\cdot g(t), \quad \text{où } \deg(g) = \deg(abc) - \deg(f).$$

On a

$$\begin{aligned} A(X,Y)B(X,Y)C(X,Y) &= Y^{3d}a\Big(\frac{X}{Y}\Big)b\Big(\frac{X}{Y}\Big)c\Big(\frac{X}{Y}\Big) \\ &= Y^{3d}f\Big(\frac{X}{Y}\Big)g\Big(\frac{X}{Y}\Big) \\ &= Y^{3d-\deg(F)}F(X,Y)g\Big(\frac{X}{Y}\Big). \end{aligned}$$

Or, par construction, deux seulement des polynômes a, b et c sont de degré d et le troisième est de degré $< d$. Donc on a

$$3d - \deg(F) \geq \deg(abc) - \deg(F) + 1,$$

puis d'après la formule (4)

$$3d - \deg(F) \geq \deg(abc) - \deg(f) = \deg(g).$$

Autrement dit, le polynôme

$$Y^{3d-\deg(F)}g\Big(\frac{X}{Y}\Big) \in \mathbf{Z}[X,Y]$$

et F divise le produit ABC. Or, F est séparable par hypothèse, donc F divise $\mathrm{rad}(ABC)$. D'où le lemme 1.9.

D'après le lemme 1.9, posons :

$$\mathrm{rad}(ABC) = F \cdot G,$$

où $G \in \mathbf{Z}[X,Y]$. On en déduit

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \mid \mathrm{rad}(ABC)(m,n) = F(m,n)G(m,n),$$

puis

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \leq \mathrm{rad}(F(m,n))|G(m,n)|. \tag{6}$$

Or, l'un des trois polynômes a, b et c est de degré $< d$ et les deux autres sont de degré excatement d, d'où

$$\deg(\mathrm{rad}(ABC)) = |\{abc = 0\}| + 1.$$

Or, par construction $|\{abc = 0\}| = d + 1$. D'où :

$$\deg(\mathrm{rad}(ABC)) = d + 2.$$

On en déduit que G est de degré $d + 2 - \deg(F)$. D'où

$$|G(m,n)| \ll_F \max(|m|,|n|)^{d+2-\deg(F)}$$

et la majoration suivante d'après l'inégalité (6)

$$\mathrm{rad}(A(m,n)B(m,n)C(m,n)) \ll_F \mathrm{rad}(F(m,n)) \max(|m|,|n|)^{d+2-\deg(F)}. \tag{7}$$

Minoration. On rappelle que l'on s'est placé dans la situation où

$$0 < m \leq n \quad \text{et} \quad A(m,n),\ B(m,n) \text{ et } C(m,n) \geq 0.$$

On a alors

$$\begin{aligned}
\max\left(A(m,n), B(m,n)\right) &= n^d \max\left(a\left(\frac{m}{n}\right), b\left(\frac{m}{n}\right)\right) \\
&= \max(|m|,|n|)^d \max\left(a\left(\frac{m}{n}\right), b\left(\frac{m}{n}\right)\right) \\
&\geq \max(|m|,|n|)^d \inf_{t \in \mathbf{C}} \bigl(\max\left(|a(t)|, |b(t)|\right)\bigr).
\end{aligned}$$

Or les polynômes a et b étant premiers entre eux, on a, d'après un lemme de K. Mahler (*cf.* [Lan99b]) rappelé ci-dessous,

$$\inf_{t \in \mathbf{C}} \bigl(\max\left(|a(t)|, |b(t)|\right)\bigr) > 0.$$

On en déduit la minoration suivante

$$\max\left(A(m,n), B(m,n), C(m,n)\right) \gg_F \max(|m|,|n|)^d. \tag{8}$$

Lemme 1.10 (Mahler) *Soient P et Q deux polynômes complexes sans zéro commun. Alors,*

$$\inf_{z\in\mathbf{C}}\big(\max\left(|P(z)|,|Q(z)|\right)\big) > 0.$$

Démonstration. Posons

$$P(z) = a(z-x_1)\dots(z-x_p) \quad \text{et} \quad Q(z) = b(z-y_1)\dots(z-y_q).$$

Par hypothèse, $x_i \neq y_j$ pour tout i, j. Soit $z \in \mathbf{C}$. Supposons que l'on ait

$$\min_j |z-y_j| \geq \min_i |z-x_i|.$$

Soit alors i_0 tel que $|z-x_{i_0}| \leq \min_j |z-y_j|$. Alors, pour tout $1 \leq j \leq q$, on a d'après l'inégalité triangulaire

$$|x_{i_0}-y_j| \leq |x_{i_0}-z| + |z-y_j| \leq 2|z-y_j|.$$

D'où $|Q(z)| \geq 2^{-q}|Q(x_{i_0})|$ puis

$$|Q(z)| \geq \min_{i,j}\big(2^{-p}|P(y_j)|, 2^{-q}|Q(x_i)|\big).$$

Si $\min_j |z-y_j| < \min_i |z-x_i|$, on obtient de même

$$|P(z)| \geq \min_{i,j}\big(2^{-p}|P(y_j)|, 2^{-q}|Q(x_i)|\big).$$

D'où

$$\max\left(|P(z)|,|Q(z)|\right) \geq \min_{i,j}\big(2^{-p}|P(y_j)|, 2^{-q}|Q(x_i)|\big) > 0.$$

Cela démontre le lemme car l'infimum d'un ensemble est le plus grand de ses minorants.

Conclusion. En combinant les inégalités (7) et (8), on obtient

$$\operatorname{rad}(F(m,n))\max(|m|,|n|)^{d+2-\deg(F)} \gg_{\varepsilon,F} \max(|m|,|n|)^{d(1-\varepsilon)}.$$

D'où le résultat en remplaçant ε par ε/d dans (5). Cela achève la démonstration de la proposition 1.2.

Références

[Bou81] N. Bourbaki. *Éléments de mathématique*, volume 864 of *Lecture Notes in Mathematics*. Masson, Paris, 1981. Algèbre. Chapitres 4 à 7.

[GT02] A. Granville and T. Tucker. It's as easy as *abc*. *Notices Amer. Math. Soc.*, 49(10) :1224–1231, 2002.

[Hin08] M. Hindry. *Arithmétique*. Tableau Noir. Calvage & Mounet, 2008.

[Lan99a] M. Langevin. Imbrications entre le théorème de Mason, la descente de Belyi et les différentes formes de la conjecture (*abc*). *J. Théor. Nombres Bordeaux*, 11(1) :91–109, 1999. Les XXèmes Journées Arithmétiques (Limoges, 1997).

[Lan99b] M. Langevin. Liens entre le théorème de Mason et la conjecture (*abc*). In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 187–213. Amer. Math. Soc., Providence, RI, 1999.

[Ser97] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown.