Some Polynomial Identities related to the *abc*-Conjecture

George Greaves and Abderrahmane Nitaj

To Andrzej Schinzel on the occasion of his 60th birthday

Abstract. Let $L_{a,b} = \log c \,/\, \log Q(abc)$ when positive coprime integers a, b, c satisfy $a + b = c$ and $Q(n)$ denotes the product of the distinct primes that divide n. Then the set of limit points of the distinct values of $L_{a,b}$ contains the interval $\left[\frac{1}{3}, \frac{36}{37}\right]$.

1991 Mathematics Subject Classification: 11D75

1. Introduction

Suppose a, b, c are positive integers with $a + b = c$ and highest common factor $(a, b) = 1$. In collaboration with J. Browkin, M. Filaseta and one of the present authors, Andrzej Schinzel [2] considered the quotient

$$L_{a,b} = \frac{\log(a+b)}{\log Q\big(ab(a+b)\big)}\ , \tag{1.1}$$

where $Q(k)$ denotes the product of the distinct prime factors of k. Let $(L_{a,b})$ denote a sequence consisting of these numbers $L_{a,b}$ taken in some fixed order. In [2] the well-known abc-conjecture of Masser and Oesterlé was reformulated as

$L_{a,b}$ is a bounded sequence with greatest limit point 1.

The objective in [2] was to see what could be proved about the limit points of the sequence $(L_{a,b})$. In fact the principal result of [2] related to the limit points of the set $\mathcal{L}$ of distinct values of $(L_{a,b})$. In this note the result in [2] is improved as follows. Let $\mathcal{L}'$ denote the set of limit points of $\mathcal{L}$.

Theorem 1. *The set $\mathcal{L}'$ contains the interval $\left[\frac{1}{3}, \frac{36}{37}\right]$.*

The corresponding result in [2] referred to the shorter interval $\left[\frac{1}{3}, \frac{15}{16}\right]$. One may conjecture that this interval ought to be replaceable by $[\frac{1}{3}, 1]$. Indeed, one of the results in [2] is that this would follow from the abc-conjecture. There appears,

---

A. Nitaj was supported by the TMR programme of the European Community under contract ERBFMBICT960848.

however, to be no particular prospect of establishing such an improvement within the framework of our current ideas.

The proof in [2] consisted of two main components: a suitable collection of polynomial identities, and a sieve result about squarefree values of binary forms. We have nothing new to say about the sieve result in [2], but we have found some new polynomial identities which lead to the improved result recorded in Theorem 1.

These identities have the shape

$$a(x,y)+b(x,y)=c(x,y)\ , \tag{1.2}$$

where $a=a(x,y)$, $b=b(x,y)$, $c=c(x,y)$ are binary forms. We will write

$$P(x,y)=a(x,y)b(x,y)c(x,y)\ . \tag{1.3}$$

A simple example, which we will refer to again later, is

$$a=(x-y)(x+y)^3\ , \qquad b=y^3(y+2x)\ , \qquad c=x^3(x+2y)\ . \tag{1.4}$$

Then it is easily verified that $a+b=c$. Fix a number $\alpha>1$, and use (1.4) when

$$X<x\le 2X\ , \quad Y<y\le 2Y\ , \qquad \text{where} \quad X=Y^\alpha\ , \tag{1.5}$$

and Y is sufficiently large. With a, b, c as in (1.4) the quotient $L_{a,b}$ defined in (1.1) becomes

$$L_{a,b}=\frac{\log c}{\log\big(Q(P(x,y))\big)}\ . \tag{1.6}$$

where $c=x^3(x+2y)$ and $Q\big(P(x,y)\big)=xy(x+2y)(y+2x)(x+y)(x-y)$. Here $Q\big(P(x,y)\big)$ has a fixed square factor $S=4$, but it would be easy to show directly (and it follows from Theorem 2 below) that for any α and large Y there exist x, y satisfying (1.5) for which $P(x,y)/S$ is squarefree. Then

$$L_{a,b}\sim\frac{4\alpha}{5\alpha+1} \quad \text{as} \quad Y\to\infty \tag{1.7}$$

for any $\alpha>1$, and it follows that $\big(\frac{2}{3},\frac{4}{5}\big)\subseteq\mathcal{L}'$.

The treatment in [2] used a collection of polynomial identities $a+b=c$ of this type, of which the simplest was given by $a=x$, $b=y$, $c=x+y$, leading to $\big(\frac{1}{3},\frac{1}{2}\big)\subseteq\mathcal{L}'$. The equation $a+b=c$ given by (1.4) was not used directly, but one of the identities that was used was the result of the substitutions $x\mapsto x^3$, $y\mapsto y^3$ in (1.4). This leads to (1.6) with

$$c=x^9\big(x^3+2y^3\big)\ , \quad Q\big(P(x,y)\big)=xy\big(x^3+2y^3\big)\big(y^3+2x^3\big)\big(x^3+y^3\big)\big(x^3-y^3\big)\ .$$

Because of Theorem 2 below, this leads in place of (1.7) to

$$L_{a,b}\sim\frac{\nu\alpha}{(\nu+1)\alpha+1} \quad \text{as} \quad Y\to\infty \tag{1.8}$$

where currently $\nu=12$ and $\alpha>1$ is arbitrary. Hence $\big(\frac{6}{7},\frac{12}{13}\big)\subseteq\mathcal{L}'$.

Let $\sigma(P)$ denote the sum of the degrees of the distinct irreducible factors of $P(x,1)$. The fact that the coefficient of α in the denominator of (1.8) is no larger than $\nu+1$, where ν is the degree of the polynomials a, b, c, reflects the fact that

$$\sigma(P) = \nu + 1. \tag{1.9}$$

By Mason's abc-theorem for polynomials [4] (or see [3], for example) this value $\nu+1$ is actually the smallest obtainable. It is important to the quality of the results that the identities $a+b=c$ employed should be optimal with respect to Mason's theorem in this way.

2. Squarefree values of binary forms

We need the following result, which was used and proved in [2].

Theorem 2. *Let $f(x,y)$ be a binary form over the integers whose irreducible factors are distinct and have degrees not exceeding μ. Let S denote the largest square divisor of $f(x,y)$. Let $N(X,Y)$ denote the number of pairs $\langle x,y\rangle$ satisfying* (1.5) *for which $f(x,y)/S$ is squarefree. Let X, Y also be as in* (1.5)*, and suppose α satisfies*

$$\begin{aligned} \alpha > 1 &\quad \text{when} \quad \mu \le 3 \\ 1 < \alpha < 3 &\quad \text{when} \quad \mu = 4 \\ 1 < \alpha < \tfrac{3}{2} &\quad \text{when} \quad \mu = 5\,. \end{aligned}$$

Then

$$N(X,Y) = C_f XY \left\{ 1 + O\left(\frac{1}{\log X}\right)\right\},$$

where the constant $C_f > 0$ depends only on f and the O-constant depends only on α.

The inference (1.8) is justified by the case $\mu = 3$ of Theorem 2. In the remainder of this paper we will need to refer only to the case $\mu = 4$, that is to say when the irreducible factors of our polynomials a, b, c are at worst quartic.

The weaker version of Theorem 1 proved in [2] was obtained via an identity (1.2) of degree $\nu = 20$ where (1.9) applied. The theorem of this paper will follow by exhibiting identities of degrees $\nu = 24$, $\nu = 32$ and $\nu = 48$ which also share these properties $\mu = 4$, $\sigma = \nu + 1$. Since Theorem 2 then allows the choice $1 < \alpha < 3$ the relation (1.8) gives

$$\left(\tfrac{12}{13}, \tfrac{18}{19}\right) \subseteq \mathcal{L}', \qquad \left(\tfrac{16}{17}, \tfrac{24}{25}\right) \subseteq \mathcal{L}', \qquad \left(\tfrac{24}{25}, \tfrac{36}{37}\right) \subseteq \mathcal{L}'\,,$$

which taken with the version in [2] will complete the proof of Theorem 1 since the set of limit points of the set $\mathcal{L}$ is closed.

The restriction on the degrees in Theorem 2 is regrettable but is typical of the current state of knowledge. For example it is not known whether n^4+1 represents infinitely many squarefree numbers, because it seems difficult to rule out the suggestion that for all large n it might be divisible by p^2 for some prime p between n and $n^{3/2}$.

3. The polynomial identities

The identities $a + b = c$ which complete the proof of Theorem 1 are as follows. First, set

$$\begin{aligned} a &= \left(2x^4 - y^4\right)^6 \left(2x^4 - 4x^2y^2 - y^4\right) \left(2x^4 + 4x^2y^2 - y^4\right) \\ b &= 2^{10}x^{12}y^{12} \left(2x^4 - 2x^2y^2 - y^4\right) \left(2x^4 + 2x^2y^2 - y^4\right) \\ c &= \left(2x^4 + y^4\right)^2 \left(2x^4 + 4x^2y^2 + y^4\right)^3 \left(2x^4 - 4x^2y^2 + y^4\right)^3 . \end{aligned} \tag{3.1}$$

Then $a + b = c$. Moreover, a, b, c will be positive when (1.5) holds and Y is large enough. This is our identity of degree $\nu = 32$. Second, set

$$\begin{aligned} A &= \left(x^2 + 3y^2\right) \left(x^4 - 18x^2y^2 + 9y^4\right) \\ B &= 4xy\left(x^2 - 3y^2\right) \left(3x^4 + 2x^2y^2 + 3y^4\right) \left(x^4 + 6x^2y^2 + 81y^4\right) \\ C &= \left(x^4 + 30x^2y^2 + 9y^4\right) \left(x^4 - 2x^2y^2 + 9y^4\right) , \end{aligned} \tag{3.2}$$

and, further, set $a_1 = A^4$, $b_1 = B^2$, $c_1 = C^3$. Then $a_1 + b_1 = c_1$. Note that this provides a solution of $A^4 + B^2 = C^3$, but gives an identity of degree only 24. However, it turns out that $D = A^4 - B^2$ factorises in the following spectacular way:

$$D = f_1(x, y) f_1(x, -y) f_2(x, y) f_2(x, -y) f_3(x, y) f_3(x, -y) , \tag{3.3}$$

where

$$\begin{aligned} f_1(x, y) &= x^4 + 12x^3y - 30x^2y^2 + 36xy^3 - 27y^4 \\ f_2(x, y) &= x^4 - 4x^3y + 10x^2y^2 - 12xy^3 - 3y^4 \\ f_3(x, y) &= x^4 + 4x^3y + 6x^2y^2 - 12xy^3 + 9y^4 . \end{aligned} \tag{3.4}$$

Then $A^8 - B^4 = C^3D$, so we take

$$a = C^3D , \quad b = B^4 , \quad c = A^8 \tag{3.5}$$

to obtain $a + b = c$, again with a, b, c positive for large Y. This is our identity of degree $\nu = 48$.

It is immediately verifiable that in the identities given by (3.1), (3.2) and (3.5) the irreducible factors of $a = a(x, y)$, $b = b(x, y)$, $c = c(x, y)$ are of degree at most $\mu = 4$. Moreover, the sum $\sigma(P)$ of the degrees of the irreducible factors of $P(x, 1)$ (where $P = abc$ as in (1.3)) takes its minimum possible value $\nu + 1$ requested in (1.9). Thus these identities will complete the proof of Theorem 1 in the way described in §2, and it only remains to verify that they are in fact valid identities.

A modern computer algebra system would confirm these identities very quickly, but we will give a self-contained description here, partly because this will give some insight into their structure.

Identities of degree 32

As in §1 (and in [2]) begin from the identity given by (1.4), but do not merely replace x, y by powers. Rather, first set $2x = u^2$, $y = -v^2$. This leads to

$$u^6\left(u^2-4v^2\right)+16v^6\left(u^2-v^2\right)=\left(u^2+2v^2\right)\left(u^2-2v^2\right)^3 . \tag{3.6}$$

The substitution was chosen so that two of the quadratics that arise reduce over the integers. Next, set

$$u = 2w^2 - z^2 , \quad v = 2wz . \tag{3.7}$$

Then the irreducible quadratics in (3.6) become

$$\begin{aligned} u^2+2v^2 &= 4w^4+4w^2z^2+z^4 = \left(2w^2+z^2\right)^2 \\ u^2-2v^2 &= 4w^4+4w^2z^2+z^4-16w^2z^2 \\ &= \left(2w^2+4wz+z^2\right)\left(2w^2-4wz+z^2\right) . \end{aligned} \tag{3.8}$$

If we now substitute $w = x^2$, $z = y^2$ the identity (3.6) gives the identity of degree 32 described by (3.1). In this process, it was important not only that the quartics in (3.8) reduced but that one of them was a square, to ensure that the sum $\sigma(P)$ of the degrees of irreducible factors attained the value described in (1.9).

The substitution (3.7) satisfies the following criterion, which was drawn to the attention of one of the authors by M.N. Huxley. We want to make $u^2 + kv^2$ reduce after a quadratic substitution

$$u = p_1w^2 + q_1wz + r_1z^2 , \quad v = p_2w^2 + q_2wz + r_2z^2 . \tag{3.9}$$

Let $\theta^2 + k = 0$. The criterion is that the quadratic in w, z given by $u - \theta v$ should have its discriminant a square in the field $\mathbb{Q}(\theta)$:

$$(q_1-\theta q_2)^2 - 4(p_1-\theta p_2)(r_1-\theta r_2) = (f-g\theta)^2 . \tag{3.10}$$

For one of the values $k = \pm 2$ we would like this square to be zero.

Denote the invariants of the pair (3.9) of quadratics by

$$P = q_1^2 - 4p_1r_1 , \quad Q = q_1q_2 - 2(p_1r_2 + p_2r_1) , \quad R = q_2^2 - 4p_2r_2 .$$

Then (3.10) says

$$\left(P-f^2\right) - 2\theta(Q-fg) + \theta^2\left(R-g^2\right) = 0 .$$

Since this is not to differ essentially from $\theta^2 + k = 0$, and this is to be done for $k = \pm 2$, the invariants P, Q, R should satisfy

$$\begin{aligned} P &= 2l + a^2 = -2m + c^2 \\ Q &= \quad ab \quad = \quad cd \\ R &= \ l + b^2 = \quad m + d^2 , \end{aligned}$$

which we want either with $a = b = 0$ or with $c = d = 0$. This can be done as in (3.7). There are different ways, for example by taking $u = 2w^2 - z^2$, $v = 2w^2 + 2wz + z^2$

in place of (3.7) (essentially different in that the quartic factors in the resulting identity do not occur to the same multiplicities as those in (3.1)).

An alternative identity of a rather different type can also be obtained from (3.6). Make $u + v\sqrt{-2} = (x + y\sqrt{-2}\,)^4$, so that $u^2 + 2v^2 = (x^2 + 2y^2)^4$ with

$$u = x^4 - 12x^2y^2 + 4y^4\ , \quad v = 4xy(x^2 - 2y^2)\ ,$$

and actually $u = (x^2 + 4xy + 2y^2)(x^2 - 4xy + 2y^2)$. Then

$$\begin{aligned} u^2 - 2v^2 &= (u^2 + 2v^2) - 4v^2 = (x^2 + 2y^2)^4 - 4v^2 \\ &= \left((x^2 + 2y^2)^2 - 2v\right)\left((x^2 + 2y^2)^2 + 2v\right)\ . \end{aligned}$$

Now (3.6) gives $a + b = c$ with

$$\begin{aligned} a &= (x^2 + 4xy + 2y^2)^6 (x^2 - 4xy + 2y^2)^6 \alpha(x, y)\alpha(x, -y) \\ b &= 2^{16}x^6y^6(x^2 - 2y^2)^6 \beta(x, y)\beta(x, -y) \\ c &= (x^2 + 2y^2)^4 \gamma^3(x, y)\gamma^3(x, -y)\ , \end{aligned}$$

where

$$\begin{aligned} \alpha(x, y) &= x^4 + 8x^3y - 12x^2y^2 - 16xy^3 + 4y^4 \\ \beta(x, y) &= x^4 + 4x^3y - 12x^2y^2 - 8xy^3 + 4y^4 \\ \gamma(x, y) &= x^4 + 8x^3y + 4x^2y^2 - 16xy^3 + 4y^4\ . \end{aligned}$$

This identity $a + b = c$ also satisfies the criterion (1.9), as well as having $\mu = 4$ in the notation of Theorem 2.

The identity of degree 48

We described earlier how this identity, given by (3.5), is based on the solution of $A^4 + B^2 = C^3$ given by (3.2). This in turn can be reached in the following way.

The method described in Chapter 25 of Mordell's book [5] was used to find polynomials X, Y, Z with degrees 4, 4, 6 respectively such that $X^3 + Y^3 = 2Z^2$. Next, use a "duplication" procedure (different from that used to obtain (3.5)): from an identity $a + b = c$ we find $(a - b)^2 + 4ab = c^2$, which will also satisfy the criterion (1.9) if the previous one did. This process leads to an identity of degree 24:

$$4Z^4 - (X^3 - Y^3)^2 = 4X^3Y^3\ .$$

For our purposes it is essential that the irreducible factors of $Z(X^3 - Y^3)$ have degrees not exceeding 4 in the variables x, y.

There are at least two identities satisfying the last condition. Of these, one is given by

$$\begin{aligned} X &= (x^2 + 2xy + 3y^2)(x^2 - 6xy + 3y^2) \\ Y &= (x^2 - 2xy + 3y^2)(x^2 + 6xy + 3y^2) \\ Z &= (x^2 - 3y^2)(x^4 + 18x^2y^2 + 9y^4)\ . \end{aligned}$$

After a substitution $y \mapsto iy$, where $i^2 = -1$, this leads to the solution (3.2) of the equation $A^4 + B^2 = C^3$. The other is the identity (3.11) below, which is of the shape $A^4 - B^2 = 4C^3$ and arises from

$$\begin{aligned} X &= 8xy\big(x^2 - 3xy + 3y^2\big) \\ Y &= 2(x-3y)(x-y)\big(x^2+3y^2\big) \\ Z &= 2\big(x^2-3y^2\big)\big(x^4 - 6x^3y + 18x^2y^2 - 18xy^3 + 9y^4\big) \ . \end{aligned}$$

The solution (3.2) has been noted elsewhere: in a paper to appear F. Beukers [1] gives a set of four polynomial solutions found by D. Zagier, which together give all integer solutions of the equation. Of these, the solution (3.2) is the only one which meets our condition that the irreducible factors have degree at most 4. The complete solution of $X^3 + Y^3 = 2Z^2$ has also been found by Rodeja [6].

On the other hand, if we only seek one polynomial solution then an alternative approach is possible. Since $(a+ib)^3 = a^3 - 3ab^2 + i\big(3a^2b - b^3\big)$, where $i^2 = -1$, we obtain $u^2 + B^2 = C^3$ when

$$u = a\big(a^2 - 3b^2\big) \ , \quad B = b\big(3a^2 - b^2\big) \ , \quad C = a^2 + b^2 \ .$$

We can make $u = A^2$ by arranging $a = f^2$, $f^4 - 3b^2 = d^2$, and setting $A = fd$. Do this by making

$$f = x^2 + 3y^2 = \big(x + y\sqrt{-3}\big)\big(x - y\sqrt{-3}\big) \ ,$$

so that a solution $d = x^4 - 18x^2y^2 + 9y^4$, $b = 4\big(x^3y - 3xy^3\big)$ is provided by the expansion of $\big(x + y\sqrt{-3}\big)^4$. Now we have $A^4 + B^2 = C^3$, and it can be verified that the solution we have found is exactly (3.2).

This derivation makes the factorisation of $3a^2 - b^2$ into the pair of quartics recorded in (3.2) seem fortuitous (but note $3C = 3\big(a^2 + b^2\big) = 4f^4 - d^2$). Similarly, we do not offer any discussion of why the factorisation of $A^4 - B^2 = D$ recorded in (3.3) could be expected to occur. On the other hand (3.3), *once found*, can be verified by hand without excessive pain. It would nevertheless be tedious to set out the details of every step, so we merely give a set of directions. First write $F_i(x,y) = f_i(x,y)f_i(x,-y)$ and proceed from (3.5), (3.4) and (3.2). Only even powers of x, y occur, so we can substitute $x^2 = u$, $3y^2 = v$. Next, set $r = u + v$, $s = u - v$. From this point work with the product F_1F_2 rather than with F_1, F_2 separately. It will now be found that only even powers of r, s occur, so set $r^2 = r_2$, $s^2 = s_2$. Then set $r_2 = r_3$, $r_2 - 2s_2 = s_3$. Again, only even powers of r_3, s_3 are involved, so set $r_3^2 = r_4$, $s_3^2 = s_4$. By this stage the identities $a + b = c$, $a - b = F_1F_2F_3$ (the first of which is known for other reasons) are now of degree only 3 and immediate to verify.

Other identities

We conclude by recording some other interesting polynomial identities of the type we have been discussing, which are however not needed for our primary objective of establishing Theorem 1.

First, the identity of degree 24 alluded to above is given by

$$\begin{aligned} A =&\left(x^2-3y^2\right)\left(x^4-6x^3y+18x^2y^2-18xy^3+9y^4\right) \\ B =&\left(x^2-6xy+3y^2\right)\left(x^2-2xy+3y^2\right)\left(x^4-4x^3y+4x^2y^2+3y^4\right) \\ &\times\left(x^4+12x^2y^2-36xy^3+27y^4\right) \\ C =&2^2xy(x-y)(x-3y)\left(x^2-3xy+3y^2\right)\left(x^2+3y^2\right)\ , \end{aligned} \tag{3.11}$$

where $A^4-B^2=4C^3$.

There is an identity of degree 30 which can be reached as follows. Let k be an integer. Set $\varepsilon = x+y\sqrt{k}$ and $\overline{\varepsilon}=x-y\sqrt{k}$. Then

$$\left(\frac{\varepsilon^{15}+\overline{\varepsilon}^{15}}{2}\right)^2-k\left(\frac{\varepsilon^{15}-\overline{\varepsilon}^{15}}{2\sqrt{k}}\right)^2=\left(x^2-ky^2\right)^{15}\ .$$

If $k=-3$, then we find

$$\begin{aligned} \left(\varepsilon^{15}+\overline{\varepsilon}^{15}\right)/2 &= x\left(x^2-9y^2\right)\left(x^4-30x^2y^2+45y^4\right)\alpha(x,y)\alpha(x,-y) \\ \left(\varepsilon^{15}-\overline{\varepsilon}^{15}\right)/\left(2\sqrt{k}\,\right) &= 3y\left(x^2-y^2\right)\left(5x^4-30x^2y^2+9y^4\right)\beta(x,y)\beta(x,-y)\ , \end{aligned}$$

where

$$\begin{aligned} \alpha(x,y) &= x^4+18x^3y+24x^2y^2-18xy^3-9y^4 \\ \beta(x,y) &= x^4+\ \ 6x^3y-24x^2y^2-54xy^3-9y^4\ . \end{aligned}$$

There is another similar identity obtained by taking $k=-15$.

References

[1] Beukers, F. The diophantine equation $Ax^p+By^q=Cz^r$. Duke Math. J., to appear

[2] Browkin, J., Filaseta, M., Greaves, G., Schinzel, A., Squarefree Values of Polynomials and the *abc*-Conjecture. In: Sieve Methods, Exponential Sums, and their Applications in Number Theory (London Math. Soc. Lecture Notes 237) (ed. by G. R. H. Greaves, G. Harman, M.N. Huxley), 65–85. Cambridge University Press, Cambridge-New York-Melbourne 1997

[3] Lang, S., Old and new conjectured diophantine inequalities. Bull. Amer. Math. Soc. 23 (1990), 37–75

[4] Mason, R.C., Equations over Function Fields. In: Number Theory, Noordwijkerhout 1983 (Lecture Notes in Mathematics 1068), 149–157. Springer-Verlag, Berlin-New York 1984

[5] Mordell, L.J., Diophantine Equations. Academic Press, London-New York 1969

[6] Rodeja, F.E.G., On the diophantine equation $x^3+y^3=2z^2$. Rivista Math. Hisp. Am. (1953), 4–13, 229–240

Authors' addresses:

George Greaves
University of Wales, Cardiff
School of Mathematics
23 Senghennydd Road
P.O.Box 926
Cardiff CF2 4YH
Great Britain
e-mail: Greaves@cardiff.ac.uk

Abderrahmane Nitaj
Universität des Saarlandes
Fb9, Mathematik
Postfach 151150
D-66041 Saarbrücken
Germany
e-mail: nitaj@diana.math.uni-sb.de