SQUAREFREE VALUES OF POLYNOMIALS AND THE ABC-CONJECTURE

J. Browkin, M. Filaseta, G. Greaves and A. Schinzel

Dedicated to Professor Christopher Hooley, F.R.S.

§1. *Introduction.* The well-known *abc*-conjecture of Masser and Oesterlé states:

Given $\epsilon > 0$, there is a number $C(\epsilon)$ such that for any relatively prime positive integers a, b, c with $a + b = c$, we have

$$c < C(\epsilon)\big(Q(abc)\big)^{1+\epsilon}, \tag{1.1}$$

where $Q(k) = \prod_{p|k} p$ denotes the product of the distinct primes dividing k.

See e.g. [11] for a discussion of the history and implications of the conjecture. It can of course be expressed in terms of not necessarily positive integers a, b, c (which may be taken to satisfy $a+b+c = 0$ if we prefer) in which case the bound is asserted for $\max\{|a|, |b|, |c|\}$.

The inequality (1.1) can be rewritten in the form

$$\log(a + b) < (1 + \epsilon) \log Q\big(ab(a + b)\big) + \log C(\epsilon).$$

Denote

$$L_{a,b} = \frac{\log(a + b)}{\log Q\big(ab(a + b)\big)}, \tag{1.2}$$

and let $(L_{a,b})$ denote a sequence whose values are these numbers $L_{a,b}$, taken in some fixed order. In this notation the conjecture asserts

$(L_{a,b})$ *is a bounded sequence whose greatest limit point does not exceed* 1.

On the other hand, there exist infinitely many examples of $L_{a,b}$ which are larger than 1 (see [13]). Currently, the greatest known, discovered by E. Reyssat (see [14] or [2]) is $1.62991\ldots$, arising from taking $a = 2$, $b = 3^{10} \times 109$, $c = 23^5$.

If the *abc*-conjecture holds, the greatest limit point of $(L_{a,b})$ would in fact equal 1. To see this, take $a = 1$, $b = 2^n - 1$. Then

$$Q\big(ab(a + b)\big) \;=\; 2 \prod_{p|2^n-1} p \;<\; 2^{n+1},$$

so $L_{a,b} > n/(n + 1) \to 1$ as $n \to \infty$. So we can reformulate the *abc*-conjecture as

$(L_{a,b})$ *is a bounded sequence with its greatest limit point equal to* 1.

Now let

$$\mathcal{L} = \{L_{a,b} : a \geq 1,\, b \geq 1,\, (a, b) = 1)\}$$

be the set of (distinct) values of $(L_{a,b})$, and let $\mathcal{L}'$ be the "derived" set of limit points of $\mathcal{L}$. We are interested in seeing what can be actually proved about $\mathcal{L}'$. By use of a sieve method we obtain the following theorem.

Theorem 1. *The set $\mathcal{L}'$ of limit points of $\mathcal{L}$ contains the interval $\left[\frac{1}{3}, \frac{15}{16}\right]$.*

The entry $\frac{1}{3}$ here is the best possible because $\log(a+b) \geq \frac{1}{3}\log\big(ab(a+b)\big) \geq \frac{1}{3}\log Q\big(ab(a+b)\big)$ in (1.2). On the other hand, we will show in Theorem 4 that if the *abc*-conjecture holds then $\frac{15}{16}$ may be replaced by 1 in Theorem 1.

One might also enquire about the limit points of

$$\mathcal{M} = \left\{ \frac{\log a}{\log Q\big(ab(a+b)\big)} : 1 \leq a \leq b,\ (a,b) = 1 \right\}$$

in addition to those of $\mathcal{L}$. As will be seen, our methods show that

$$\left[0, \tfrac{3}{4}\right] \subseteq \mathcal{M}', \tag{1.3}$$

so that the set of combined limit points of $\mathcal{L}$ and $\mathcal{M}$ contains $\left[0, \frac{15}{16}\right]$.

Our proof of Theorem 1 rests on the following result about squarefree values of binary forms.

Theorem 2. (a) *Let $1 \leq Y \leq X$, where X is sufficiently large, and let $f(x,y) \in \mathbb{Z}[x,y]$ be a binary form whose irreducible factors f_i are distinct and all have degrees not exceeding μ. Let D denote the largest fixed divisor of $f(x,y)$, and let $S = D/\big(\prod_{p|D} p\big)$. Let $N(X,Y)$ denote the number of pairs $\langle x,y\rangle$ with*

$$X < x \leq 2X,\ Y < y \leq 2Y \tag{1.4}$$

for which $f(x,y)/S$ is squarefree. Suppose for some $\epsilon > 0$

$$X^{\mu} < (XY)^{3-\epsilon},\ Y > X^{\epsilon}. \tag{1.5}$$

Then

$$N(X,Y) = C_f XY \left\{ 1 + O\left(\frac{1}{\log X}\right)\right\}, \tag{1.6}$$

where the constant $C_f > 0$ depends only on f as in (3.6) below, and the O-constant depends only on ϵ.

(b) *In part (a), set $X = Y^{\alpha}$, where $\alpha > 1$ is fixed. Then (1.6) holds*

$$\begin{aligned} &\textit{for any } \alpha \textit{ when } \mu \leq 3\\ &\textit{if } \alpha < 3 \textit{ when } \mu = 4\\ &\textit{if } \alpha < \tfrac{3}{2} \textit{ when } \mu = 5. \end{aligned}$$

In this theorem, the first inequality in (1.5) implies $Y > X^{\epsilon/3}$ when $\mu \geq 3$; for all μ we assume $Y > X^{\epsilon}$, for our convenience. In particular we will take advantage of the implication $1/\log Y \ll 1/\log X$. As a consequence, when f is quadratic our theorem does not embody even the result of Nagell [12] in which $Y = 1$. It would be possible to refine Theorem 2 into a result holding uniformly for $1 < Y \leq X$, but at the cost of introducing technicalities into the treatment that are not necessary for our purpose here.

Observe that Theorem 2 also marginally fails to include the results of Hooley [9], where $Y = 1$, $\mu = 3$, and of one of the present authors [8], where $X = Y$, $\mu = 6$, and may thus be regarded as a somewhat imperfect bridge between them. The imperfection stems from our use in the proof of Lemma 2 of the estimate $d(n) \ll n^\epsilon$ for the divisor function. There is therefore no need to take extra care about other factors that also contribute no worse than X^ϵ to our requirements in (1.5).

The treatment in [8] was arranged on the assumption $X = Y$, and it is necessary to modify the treatment to obtain part (a) of Theorem 2. For part (b), which is what we actually use, we have only to observe that the given conditions are sufficient for (1.5).

Denote the n-th cyclotomic polynomial by $\Phi_n(x)$. In §6 we establish the following theorem.

Theorem 3. *Assume the abc-conjecture holds. Then, for every positive integer n, there exist infinitely many integers m for which $\Phi_n(m)$ is squarefree.*

As we indicate in §6, the same method suffices to show that (assuming the *abc*-conjecture) for all positive integers n the polynomial $(x^n - 1)/(x - 1)$ takes infinitely many squarefree values.

Unconditionally, it has not been shown that there exists an irreducible $f(x) \in \mathbb{Z}[x]$ of degree ≥ 4 having the property that $f(m)$ is squarefree for infinitely many integers m. Before the stronger result of Hooley [9] mentioned earlier Erdős [4] had established that all irreducible cubics with largest fixed divisor equal to 1 possess this property.

Finally, and also in §6, we point out what is conjectured to be true in the direction of our Theorem 1.

Theorem 4. *Assume the abc-conjecture holds. Then the set of limit points of $\mathcal{L}$ is precisely the interval $[\frac{1}{3}, 1]$.*

By the same method an analogous result can be obtained about $\mathcal{M}'$, as described in (1.3):

Assume the abc-conjecture holds. Then the set of limit points of $\mathcal{M}$ is precisely the interval $[0, 1]$.

Throughout this article the symbol p denotes a prime. The arbitrarily small real number $\epsilon > 0$ need not be the same on each occurrence.

§2. *The treatment of Theorem 1.* We describe here how Theorem 1 follows once Theorem 2 has been established.

First we use the following construction, which in conjunction with a simpler version of Theorem 2 leads to the weaker form of our Theorem 1 in which the right-hand end-point $\frac{15}{16}$ is replaced by $\frac{6}{7}$. Take

$$a = y^\nu,\ b = x^\nu - y^\nu.$$

Thus $c = a+b = x^\nu$. We will specify $\nu = 1$, 2, 4, or 6. Fix an exponent $\alpha > 1$ and consider

$$X = Y^\alpha,\ X < x \le 2X,\ Y < y \le 2Y, \tag{2.1}$$

as in Theorem 2. For the specified values of ν the irreducible factors of $x^\nu - y^\nu$ are of degree at most 2. It is then a relatively easy case of Theorem 2 that we can, for any $\alpha \ge 1$, find x, y satisfying (2.1) so that $xy(x^\nu - y^\nu)$ is squarefree.

For $L_{a,b}$, as defined in (1.2), this construction gives $Q\big(ab(a+b)\big) = xy(x^\nu - y^\nu)$, $(a,b) = 1$, and

$$L_{a,b} = \frac{\log x^\nu}{\log\big(xy(x^\nu - y^\nu)\big)} = \frac{\nu\alpha}{(\nu+1)\alpha+1} + O\left(\frac{1}{\log X}\right).$$

The limit points of these $L_{a,b}$ cover the interval $\big(\nu/(\nu+2), \nu/(\nu+1)\big)$. On taking the union of these for $\nu = 1$, 2, 4, 6 we cover $(\frac13, \frac67) \setminus \{\frac12, \frac23\}$, whence

$$\left[\tfrac13, \tfrac67\right] \subseteq \mathcal{L}', \tag{2.2}$$

since the set $\mathcal{L}'$ contains the derived set of the set of limit points of the sequence $(L_{a,b})$.

The construction with $\nu = 6$ also gives

$$\frac{\log a}{\log Q\big(ab(a+b)\big)} = \frac{\nu}{(\nu+1)\alpha+1} + O\left(\frac{1}{\log X}\right),$$

which leads in a similar way to the assertion (1.3) about $\mathcal{M}'$.

Next, we show how Theorem 2 can further be used to obtain that $[\frac67, \frac{12}{13}] \subseteq \mathcal{L}'$. We invoke the polynomial identity

$$y^3(2x+y) + (x+y)^3(x-y) = x^3(x+2y).$$

We replace the pair $\langle x, y\rangle$ by $\langle x^3, y^3\rangle$ and set

$$a = y^9(2x^3+y^3),\ b = (x^3+y^3)^3(x^3-y^3).$$

Thus $a+b = x^9(x^3+2y^3)$. We apply Theorem 2 to

$$f(x,y) = xy(x^3+2y^3)(2x^3+y^3)(x^3+y^3)(x^3-y^3).$$

One easily checks that $S = 2$. We deduce that $Q\big(ab(a+b)\big) = f(a,b)/2$ provided this last expression is squarefree. Since the irreducible factors of $f(x,y)$ have degree at most 3, we obtain from Theorem 2 that we can arrange this for any α in (2.1). Proceeding as earlier we obtain

$$L_{a,b} = \frac{12\alpha}{13\alpha+1} + O\left(\frac{1}{\log X}\right),$$

whence $\left[\frac67, \frac{12}{13}\right] \subseteq \mathcal{L}'$.

To complete the inference of Theorem 1 from Theorem 2, we describe now how to obtain $[\frac{12}{13}, \frac{15}{16}] \subseteq \mathcal{L}'$. As above, we make use of a certain polynomial identity, namely

$$(x+y)^7(x-y)(x^2-xy+y^2)+y^7(2x+y)(3x^2+3xy+y^2)=x^7(x+2y)(x^2+3xy+3y^2).$$

These polynomial identities were obtained by considering special cases of the identities described by Lemma 3 in [5]. For example, this last identity follows from considering $k=7$, $s=3$ there. Such identities were explicitly given earlier by Huxley and Nair in [10], but they also go back even further as part of the general theory of Padé approximants (cf. [1]).

In the above identity, we replace $\langle x, y\rangle$ with $\langle x^2, y^2\rangle$. Set

$$a=(x^2+y^2)^7(x^2-y^2)(x^4-x^2y^2+y^4), \quad b=y^{14}(2x^2+y^2)(3x^4+3x^2y^2+y^4).$$

We apply Theorem 2 with $\mu=4$ and

$$\begin{aligned} f(x,y) = {} & xy(x+y)(x-y)(x^2+y^2)(2x^2+y^2)(x^2+2y^2) \\ & \times (x^4-x^2y^2+y^4)(3x^4+3x^2y^2+y^4)(x^4+3x^2y^2+3y^4). \end{aligned}$$

Here, $S=6$. We deduce that $Q\big(ab(a+b)\big)=f(a,b)/6$ for infinitely many pairs $\langle a, b\rangle$ defined as above with $x\in(X,2X]$, $y\in(Y,2Y]$, and $X=Y^\alpha$, where α can be an arbitrary number from the interval $(1,3)$. Proceeding as before, the result $[\frac{12}{13}, \frac{15}{16}] \subseteq \mathcal{L}'$ easily follows, completing the proof that Theorem 1 is a consequence of Theorem 2.

§3. *The treatment of Theorem 2.* In this section we reduce the proof of Theorem 2 to that of Lemmas 1 and 2 below. The general structure of the argument resembles that in [9], [7] and [8], where some points are discussed at greater length than below.

Let $N'(X,Y)$ denote the number of pairs $\langle x, y\rangle$ of integers satisfying (1.4) such that

$$f(x,y)/S \not\equiv 0, \bmod p^2 \text{ for all } p\le\xi=\tfrac{1}{3}\log Y, \tag{3.1}$$

this providing the definition of ξ. Then

$$N(X,Y)=N'(X,Y)+O\big(E(X,Y)\big), \tag{3.2}$$

where

$$E(X,Y)=\sum_{\substack{X<x\le 2X,\, Y<y\le 2Y \\ p^2|f(x,y) \text{ for some } p>\xi}} 1. \tag{3.3}$$

The Inclusion-Exclusion Principle suffices to estimate N'. We obtain

$$\begin{aligned} N'(X,Y) &= \sum_{X<x\le 2X,\, Y<y\le 2Y} \ \sum_{\substack{\ell^2|f(x,y)/S \\ p|\ell\Rightarrow p\le\xi}} \mu(\ell) \\ &= \sum_{\substack{\ell \\ p|\ell\Rightarrow p\le\xi}} \mu(\ell) \sum_{\substack{1\le u\le S\ell^2,\ 1\le v\le S\ell^2 \\ f(u,v)\equiv 0, \bmod S\ell^2}} \ \sum_{\substack{X<x\le 2X,\, Y<y\le 2Y \\ x\equiv u, y\equiv v, \bmod S\ell^2}} 1 \\ &= \sum_{\substack{\ell \\ p|\ell\Rightarrow p\le\xi}} \mu(\ell) \sum_{\substack{1\le u\le S\ell^2,\ 1\le v\le S\ell^2 \\ f(u,v)\equiv 0, \bmod S\ell^2}} \left\{\frac{X}{S\ell^2}+O(1)\right\}\left\{\frac{Y}{S\ell^2}+O(1)\right\}. \end{aligned}$$

Denote

$$\rho(r) = \sum_{\substack{1 \le u \le r,\ 1 \le v \le r \\ f(u,v) \equiv 0, \bmod r}} 1. \tag{3.4}$$

When ℓ is squarefree and Y sufficiently large the condition $p \mid \ell \Rightarrow p \le \xi$ gives $\ell \le \prod_{p \le \xi} p = \exp\left(\sum_{p \le \xi} \log p\right) \le e^{9\xi/8} = Y^{3/8}$, since ξ is as defined in (3.1). Thus $Y/(S\ell^2) \gg 1$ and it follows that

$$\begin{aligned} N'(X,Y) &= XY \sum_{\substack{\ell \\ p \mid \ell \Rightarrow p \le \xi}} \frac{\mu(\ell)\rho(S\ell^2)}{S^2\ell^4} + O\Bigg(X \sum_{\ell \le Y^{3/8}} \frac{\rho(S\ell^2)}{\ell^2}\Bigg) \\ &= C_f XY \left\{1 + O\left(\frac{1}{\log Y}\right)\right\}, \end{aligned} \tag{3.5}$$

where

$$C_f = \prod_p \left\{1 - \frac{\rho(p^{\sigma+2})}{p^{2\sigma+4}}\right\} > 0, \tag{3.6}$$

the exponent $\sigma = \sigma(p)$ being defined by $p^\sigma \parallel S$. The properties of the function ρ needed to support (3.5), in particular $\rho(p^2) \ll p^2$, can be obtained as in [7]. The definition of S given in Theorem 2 implies that $\rho(p^{\sigma+2}) < p^{2\sigma+4}$ for all p, so that $C_f > 0$.

Because of (3.2), (3.5) and (3.6) the proof of the main assertion (1.6) of Theorem 2 will be complete when we have shown

$$E(X,Y) \ll \frac{XY}{\log Y}. \tag{3.7}$$

The irreducible factors f_i of the form f are all distinct, so the discriminant Δ of f is non-zero. If Y is large enough, as the theorem allows, then $p > \xi$ implies that p does not divide Δ or any non-zero coefficient of any f_i. If $p \nmid (x,y)$ in (3.3) then $p^2 \mid f_i(x,y)$ for some i (since $p \nmid \Delta$). Except when $f_i(x,y)$ is x or y this implies $p \nmid xy$. So we can write

$$E(X,Y) \ll E^{(0)}(X,Y) + \sum_i E_i^{(1)}(X,Y) + \sum_i E_i^{(2)}(X,Y), \tag{3.8}$$

where

$$E^{(0)}(X,Y) = \sum_{\substack{X < x \le 2X,\ Y < y \le 2Y,\ p > \xi \\ p^2 \mid xy}} 1,$$

$$E_i^{(1)}(X,Y) = \sum_{\substack{X < x \le 2X,\ Y < y \le 2Y,\ \xi < p \le XY\eta \\ f_i(x,y) = kp^2,\ p \nmid xy}} 1, \tag{3.9}$$

$$E_i^{(2)}(X,Y) = \sum_{\substack{X < x \le 2X,\ Y < y \le 2Y,\ p > XY\eta \\ f_i(x,y) = kp^2 \ne 0,\ p \nmid xy}} 1, \tag{3.10}$$

We may suppose $f_i(x,y)\neq 0$ in (3.10) since otherwise the contribution to $E(X,Y)$ of the pair $\langle x,y\rangle$ would already have been counted in (3.9). We will specify

$$\eta = 1/\log X, \tag{3.11}$$

although a smaller choice, even $1/X^{\epsilon}$, would be satisfactory for our purposes.

When $Z=X$ or $Z=Y$ the number of multiples of d in $(Z,2Z]$ does not exceed the number in $(0,2Z]$, which is $\ll Z/d$. Hence

$$E^{(0)}(X,Y) \ll \sum_{p>\xi} \frac{XY}{p^2} \ll \frac{XY}{\xi} \ll \frac{XY}{\log Y}, \tag{3.12}$$

since we specified $\xi = \frac{1}{3}\log Y$ in (3.1).

The proof of Theorem 2 will be completed via the following two lemmas, which we give in a form that is uniform in X, Y, ξ, η.

Lemma 1. *Suppose $1\le Y\le X$ and $\eta \le \log X$. Let f_i be any one of the irreducible factors of the form f, as described in Theorem 2. Then the expression $E_i^{(1)}(X,Y)$ given in* (3.9) *satisfies*

$$E_i^{(1)}(X,Y) \ll \frac{XY\sqrt{\eta}}{\sqrt{\log X}} + \frac{XY}{\xi}.$$

When ξ, η are as in (3.1), (3.11), and $Y > X^{\epsilon}$ as in Theorem 2, this estimate reduces to $E_i^{(1)}(X,Y) \ll XY/\log X$, which is what is needed for Theorem 2. Observe in particular that the corresponding estimate obtained in [8], namely $X^2/\log X$, is not adequate in the present context.

Lemma 2. *Suppose $1<Y\le X$, and let f be a form with no linear factors over $\mathbb{Z}$. Define*

$$S(X,Y,K) = \sum_{|k|\le K} \sum_{\substack{X<x\le 2X,\, Y<y\le 2Y\\ f(x,y)=kp^2,\, p\nmid xy}} 1.$$

Then

$$S(X,Y,K) \ll X^{\epsilon/5}\big(X\sqrt{Y} + K^{\frac14}(XY)^{\frac34}\big).$$

In (3.10) the form f_i is irreducible. We can suppose it is not linear, for if so then the sum (3.10) would be empty. In this sum, the variable k satisfies $|k|\le K$, where $K \ll X^{\mu}/p^2$ and $p > XY\eta$. Under the condition (1.5) of Theorem 2 this gives $K \ll (XY)^{1-\epsilon}/\eta^2$, where η is as in (3.11). Thus Lemma 2 gives

$$E_i^{(2)}(X,Y) \ll X^{\epsilon/5}\left(X\sqrt{Y} + \frac{(XY)^{1-\epsilon/4}}{\sqrt{\eta}}\right) \ll \frac{XY}{\log Y}.$$

With (3.12) and (3.8) these estimates for $E_i^{(1)}(X,Y)$ and $E_i^{(2)}(X,Y)$ establish (3.7) and hence Theorem 2.

In [8] a weaker form of Lemma 2 was obtained (in the case $X=Y$) using Selberg's sieve method. The procedure could be adapted to the context $X\neq Y$ to yield a result useful for the same range of K as is Lemma 2. We use the two-dimensional Large Sieve to obtain the sharper version stated.

§4. *Lemmas on linear congruences.* In the proofs of Lemmas 1 and 2 we will need the following results relating to the solutions of a congruence $ax + by \equiv 0$, $\bmod\, m$, that lie in a box $X < x \le 2X$, $Y < y \le 2Y$. It is here that we introduce the rescaling of the procedures used in [8] that is essential in the context $X \ne Y$. In the case $X = Y$ Lemma 3 and part (a) of Lemma 4 reduce to Lemmas 1 and 2 in [8].

We will consider the points $\langle x, y\rangle$ for which

$$x \equiv \omega y, \bmod r, \tag{4.1}$$

where $r > 0$. In the language of the Geometry of Numbers, the solutions of (4.1) form a lattice Λ_ω, given by

$$\langle x, y\rangle = \ell\langle \omega, 1\rangle + m\langle r, 0\rangle.$$

This lattice has (positive, by convention) determinant r.

We use the maximum norm $|\langle x, y\rangle| = \max\{|x|, |y|\}$, although the Euclidean norm, or any other equivalent one, could be employed.

Consider the modified lattice λ_ω consisting of non-integral vectors

$$\mathbf{z} = \langle z_1, z_2\rangle = \left\langle \frac{x}{X}, \frac{y}{Y}\right\rangle, \tag{4.2}$$

where x, y satisfy (4.1). This has determinant

$$\Delta = \frac{r}{XY}. \tag{4.3}$$

Choose a basis $\mathbf{a}, \mathbf{b}$ for this modified lattice (Minkowski-reduced with respect to the norm $|\cdot|$) as follows: let $|\mathbf{a}|$ be minimal so that $\mathbf{a} \ne \mathbf{0}$, and let $|\mathbf{b}|$ be minimal so that $\mathbf{b}$ is independent of $\mathbf{a}$. Then

$$\Delta \ll |\mathbf{a}||\mathbf{b}| \ll \Delta,$$

where Δ is the determinant described in (4.3), the implied constants being absolute. These inequalities go back at least to Minkowski (see, for example, chapter 8 of [3]), but were derived *ab initio* (for the case $X = Y$) in [8]. (They are also immediately accessible to geometrical intuition; one can see, when $|\cdot|$ is the Euclidean norm, that the angle between $\mathbf{a}$ and $\mathbf{b}$ is not less than $\pi/3$.)

The region $X < x \le 2X$, $Y < y \le 2Y$ becomes the square $1 < z_1 \le 2$, $1 < z_2 \le 2$ in $\mathbf{z}$-space. Write $\mathbf{z} = \ell\mathbf{a} + m\mathbf{b}$. Then $|\ell| = |b_2 z_1 - b_1 z_2|/\Delta$, $|m| = |a_2 z_1 - a_1 z_2|/\Delta$. Since $|z_i| \le 2$ in (4.2), this gives

$$|\ell| \ll L = \frac{|\mathbf{b}|}{\Delta},\ |m| \ll M = \frac{|\mathbf{a}|}{\Delta},\ M \le L,\ LM = \frac{|\mathbf{a}||\mathbf{b}|}{\Delta^2} \ll \frac{1}{\Delta}. \tag{4.4}$$

Thus the integer vector $\langle \ell, m\rangle$ is confined to a parallelogram with area $\ll XY/r$ and perimeter $\ll L \ll 1/(\Delta M) = 1/|\mathbf{a}|$. This proves Lemma 3, as follows.

Lemma 3. *The number $N_\omega(X, Y, r)$ of solutions of* (4.1) *for which $X < x \le 2X$, $Y < y \le 2Y$ satisfies*

$$N_\omega(X, Y, r) \ll \frac{XY}{r} + \frac{1}{|\mathbf{a}|},$$

where $\mathbf{a} = \mathbf{a}(\omega, r)$ *is, as above, the shortest non-zero vector in the lattice* $\lambda_\omega = \lambda_\omega(r)$ *given by* (4.2).

We will need to average the error term $1/|\mathbf{a}|$ appearing in Lemma 3 over certain values of r and of ω, $\bmod r$. Since it causes little extra trouble, we establish Lemma 4 in a form uniform in y, η.

Lemma 4. *Suppose* ω, $\bmod r$ *runs over the roots of a congruence* $g(\omega, 1) \equiv 0$, mod r, *where* g *is a form with no linear factors over* $\mathbb{Z}[x, y]$. *Let* $\mathbf{a}$ *be as in Lemma 3. Suppose* $1 \le Y \le X$, $0 < \eta \le \log X$, *and that* X *is sufficiently large.*

(a) *Denote*

$$\Sigma^{(2)}(X, Y, \eta) = \sum_{X < p \le XY\eta} \sum_{\omega, \bmod p^2} \frac{1}{|\mathbf{a}(\omega, p)|},$$

where the sum is over primes p. *Then*

$$\Sigma^{(2)}(X, Y, \eta) \ll \frac{XY\sqrt{\eta}}{\sqrt{\log X}}.$$

(b) *Denote*

$$\Sigma^{(3)}(R, X, Y) = \sum_{1 \le r \le R} \sum_{\omega, \bmod r} \frac{1}{\sqrt{r|\mathbf{a}|}}.$$

Then

$$\Sigma^{(3)}(R, X, Y) \ll R^\epsilon\left(\sqrt{X} + (XYR)^{\frac{1}{4}}\right).$$

From (4.2) we can express $\mathbf{a}$ as $\mathbf{a} = \langle u_1/X,\ u_2/Y\rangle$, where u_1, u_2 are integers, not both 0. Then

$$|\mathbf{a}| = \max\{|u_1|/X, |u_2|/Y\} > 0.$$

Here $\mathbf{a}$ is in the lattice λ_ω, so

$$u_1 \equiv \omega u_2, \bmod r, \tag{4.5}$$

so that in Lemma 4 we have

$$g(u_1, u_2) \equiv 0, \bmod r. \tag{4.6}$$

In part (a) of the Lemma, where $r = p^2$ and $p > X$, consider first those p, ω for which $u_1 u_2 = 0$. If $u_2 = 0$, so that $u_1 \ne 0$, then (4.5) gives $p^2 \,|\, u_1$, so that in particular $|u_1| \ge p^2$. Hence

$$p^2 \le \frac{p^4}{X^2} \le \frac{|u_1|^2}{X^2} \le |\mathbf{a}|^2 \le |\mathbf{a}||\mathbf{b}| \ll \Delta = \frac{p^2}{XY},$$

which is impossible for large X. Hence $u_2 \ne 0$. Similarly we deduce $u_1 \ne 0$, unless $\omega \equiv 0$, $\bmod p$, which does not arise as soon as X exceeds the coefficients of g. So in establishing part (a) we may now suppose $u_1 u_2 \ne 0$.

The terms where $|\mathbf{a}| \ge \sqrt{\eta}/\sqrt{\log X}$, i.e. where

$$\min\left\{\frac{X}{|u_1|}, \frac{Y}{|u_2|}\right\} \le \frac{\sqrt{\log X}}{\sqrt{\eta}}, \tag{4.7}$$

contribute to $\Sigma^{(2)}$ an amount

$$\ll \sum_{X<p\le XY\eta} \sum_{\omega, \bmod p^2} \frac{\sqrt{\log X}}{\sqrt{\eta}} \ll \frac{XY\sqrt{\eta}}{\sqrt{\log X}},$$

since there are only $O(1)$ roots $\omega, \bmod p^2$.

The remaining contribution to $\Sigma^{(2)}$ is from p, ω with $p > X, u_1 \neq 0, u_2 \neq 0$ and where (4.7) is false. The minimality of $|\mathbf{a}|$ and X sufficiently large imply that $|u_i| \le p^2 \le (XY\eta)^2 \ll X^5$. The terms with $X/|u_1| < Y/|u_2|$ contribute

$$\ll \sum_{u_1,u_2}{}' \sum_{p>X} \sum_{\substack{\omega, \bmod p^2 \\ p^2 | u_1 - \omega u_2}} \frac{X}{|u_1|},$$

where $\sum'$ denotes a sum over all u_1 and u_2 satisfying $0 < |u_i| \ll X^5$ and $\sqrt{\log X}/\sqrt{\eta} < X/|u_1| < Y/|u_2|$. The condition $p^2 \mid u_1 - \omega u_2$ is (4.5), which implies $p^2 \mid g(u_1, u_2)$, as in (4.6). Here $g(u_1, u_2) \neq 0$ because the form g has no linear factors over $\mathbb{Z}$. Since $|u_i| \ll X^5$, this divisibility condition occurs for only finitely many primes exceeding X. Since the value $u_2 = 0$ does not occur the number of values of u_2 for given u_1 is at most $2Y|u_1|/X$. Thus this contribution to $\Sigma^{(2)}$ is at most

$$\ll \sum_{|u_1| < \frac{X\sqrt{\eta}}{\sqrt{\log X}}} \frac{X}{|u_1|} \frac{Y}{X} |u_1| \ll \frac{XY\sqrt{\eta}}{\sqrt{\log X}}.$$

The contribution from terms with $Y/|u_2| \le X/|u_1|$ is estimated similarly. This completes the proof of part (a) of Lemma 4.

We argue along the same general lines for part (b). Deal first with

$$\sum_{P<r\le 2P} \sum_{\omega, \bmod r} \frac{1}{\sqrt{r}} \min\left\{ \sqrt{\frac{X}{|u_1|}}, \sqrt{\frac{Y}{|u_2|}} \right\}, \tag{4.8}$$

where if u_1 or u_2 equals 0 then the minimum is the expression involving the non-zero u_i. We will take

$$P = \frac{R}{2^\alpha} : \ 1 \le \alpha \ll \log R. \tag{4.9}$$

First consider those pairs r, ω for which

$$\min\left\{ \frac{X}{|u_1|}, \frac{Y}{|u_2|} \right\} \le \frac{1}{\psi}, \tag{4.10}$$

where ψ will be specified below. The contribution to (4.8) from these pairs is

$$\sum_{P<r\le 2P} \sum_{\omega, \bmod r} \frac{1}{\sqrt{r\psi}} \ll \frac{P^{\frac{1}{2}+\epsilon}}{\sqrt{\psi}}, \tag{4.11}$$

since there are $\ll r^\epsilon$ values of ω for each r.

There remains the contribution to (4.8) from those pairs r, ω for which (4.10) is false. It is not necessary to attempt to deal with the terms where $u_1 u_2 = 0$ with the same care as in part (a). The terms where $X/|u_1| < Y/|u_2|$ (possibly with $u_2 = 0$) contribute

$$\sum_{\frac{1}{\psi} < \frac{X}{|u_1|} < \frac{Y}{|u_2|}} \sum_{P \le r \le 2P} \sum_{\substack{\omega, \mathrm{mod}\ r \\ r | u_1 - \omega u_2}} \frac{1}{\sqrt{r}} \sqrt{\frac{X}{u_1}}. \tag{4.12}$$

As in part (a) the divisibility condition implies $r \,|\, g(u_1, u_2)$, where $g(u_1, u_2) \neq 0$, whence the number of such r is $\ll g(u_1, u_2)^\epsilon \ll (X\psi)^\epsilon \ll P^\epsilon$, when $\psi \le P/X$ as specified below. The number of $\omega, \mathrm{mod}\, r$ is also $\ll P^\epsilon$, so the contribution (4.12) is at most

$$\begin{aligned} \sum_{|u_1| < X\psi} \sum_{|u_2| < Y|u_1|/X} P^\epsilon \sqrt{\frac{X}{|u_1| P}} &\ll \sum_{|u_1| < X\psi} P^\epsilon \sqrt{\frac{X}{|u_1| P}} \left\{ 1 + \frac{Y|u_1|}{X} \right\} \\ &\ll \frac{1}{P^{\frac{1}{2} - \epsilon}} \left\{ X\sqrt{\psi} + XY\psi^{\frac{3}{2}} \right\}, \end{aligned} \tag{4.13}$$

and since $Y < X$ the similar contribution from the terms where $X/|u_1| > Y/|u_2|$ is not larger.

This contribution (4.13) has to be added to the entry (4.11). Of these, (4.13) will not be larger than (4.11) if we choose $\psi = \min\left\{P/X, \sqrt{P/(XY)}\right\}$, in which case (4.11), and therefore (4.8), is $\ll P^\epsilon\left(\sqrt{X} + (XYP)^{1/4}\right)$.

On summing over the values of P indicated in (4.9) we obtain the estimate for $\Sigma^{(3)}(R, X, Y)$ stated in Lemma 4.

§5. *The sifting argument.* We complete the proof of Theorem 2 by establishing Lemmas 1 and 2, as enunciated earlier.

In proving Lemma 1 we may suppose that X is as large as desired, since otherwise the Lemma is trivial.

In the notations of Lemmas 3 and 4 we have from (3.9)

$$E_i^{(1)}(X, Y) \le \sum_{\xi < p \le XY\eta} \sum_{\substack{1 \le \omega \le p^2 \\ f_i(\omega, 1) \equiv 0, \mathrm{mod}\ p^2}} N_\omega(X, Y, p^2). \tag{5.1}$$

When $p \ll X$ we do not use Lemma 3, but make a separate estimate for each y. The contribution of these p to $E_i^{(1)}(X, Y)$, as defined in (3.9), is

$$\begin{aligned} &\ll \sum_{\xi < p \ll X} \sum_{\substack{Y < y \le 2Y \\ p \nmid y}} \sum_{\substack{1 \le \psi \le p^2 \\ f_i(\psi, y) \equiv 0, \mathrm{mod}\ p^2}} \sum_{\substack{X < x \le 2X \\ x \equiv \psi, \mathrm{mod}\ p^2}} 1 \\ &\ll \sum_{\xi < p \ll X} \sum_{Y < y \le 2Y} \left\{ \frac{X}{p^2} + O(1) \right\} \ll \frac{XY}{\xi}, \end{aligned}$$

since there are at most $O(1)$ values of ψ for each p when $p \nmid y$.

In particular, if the irreducible form f_i is of degree 1 or 2 then all primes p in (3.9) for which $E_i^{(1)}(X,Y) \neq 0$ satisfy $p \ll X$, so that the proof of Lemma 1 is already complete. Accordingly to prove Lemma 1 we may suppose in particular that f_i has no linear factor over $\mathbb{Z}$, so that Lemma 4 may be applied.

Lemma 3 gives

$$N_\omega(X,Y,p^2) \leq \frac{XY}{p^2} + O\left(\frac{1}{|\mathbf{a}|}\right).$$

The contribution to (5.1) from the summand XY/p^2 is

$$\sum_{\xi < p \leq XY\eta} \sum_{\omega, \bmod p} \frac{XY}{p^2} \ll \frac{XY}{\xi}.$$

The contribution from the other summand $1/|\mathbf{a}|$ is estimated in part (a) of Lemma 4. This completes the proof of Lemma 1.

Proceed to the proof of Lemma 2, in which we may suppose $K \leq X^\mu$, where μ is the degree of f. A certain amount of removal of common factors is necessary, as in [8]. Thus we first set

$$(x,y) = d, \; x = dx_1, \; y = dy_1, \; X = dX_1, \; Y = dY_1. \tag{5.2}$$

Then $(d,p) = 1$, so we obtain $d^\mu \,|\, k$ and

$$\begin{gathered} k = d^\mu k_1, \; f(x_1,y_1) = p^2 k_1, \; (x_1,y_1) = 1, \\ X_1 < x_1 \leq 2X_1, \; Y_1 < y_1 \leq 2Y_1, \; |k_1| \leq K/d^\mu. \end{gathered}$$

Second, set $\delta = (y_1, k_1)$, so that

$$\delta \,|\, c_0 \neq 0, \tag{5.3}$$

where c_0 is the coefficient of x^μ in f ; $c_0 \neq 0$ because f has no linear factors over $\mathbb{Z}$. Write

$$y_1 = \delta y_2, \; x_1 = x_2, \; k_1 = \delta r, \; X_2 = X_1, \; Y_2 = Y_1/\delta. \tag{5.4}$$

Then

$$f(x_1,y_1) = \delta g(x_2,y_2),$$

where $g(x,y)$ is again a binary form having no linear factors over $\mathbb{Z}$. Thus, in Lemma 2, $S(X,Y,K)$ does not exceed the number of solutions of

$$\left.\begin{aligned} g(x_2,y_2) = p^2 r, \; (y_2, x_2 r) = 1, \; \delta \,|\, c_0, \\ X_2 < x_2 \leq 2X_2, \; Y_2 < y_2 \leq 2Y_2, \; r \leq R, \end{aligned}\right\} \tag{5.5}$$

where

$$R = \frac{K}{d^\mu \delta} \ll X^\mu. \tag{5.6}$$

Since $(y_2, r) = 1$ we can define ω, mod r by

$$x_2 \equiv \omega y_2, \bmod r. \tag{5.7}$$

Then $g(\omega, 1) \equiv 0$, mod r. We deal with this using the lattice structure described in §4, where X, Y have to be replaced by X_2, Y_2. Thus we write $\mathbf{z} = \ell\mathbf{a} + m\mathbf{b}$, where L, M satisfy (4.4), with

$$\Delta = \frac{r}{X_2 Y_2}. \tag{5.8}$$

Write $\mathbf{a} = \langle u_1/X_2, u_2/Y_2\rangle$, $\mathbf{b} = \langle v_1/X_2, v_2/Y_2\rangle$, the notation for $\mathbf{a}$ being as in Lemma 4. In this situation we obtain

$$p^2 r = g(x_2, y_2) = g(\ell u_1 + m v_1, \ell u_2 + m v_2) = G(\ell, m),$$

say, divisible by r for all $\langle \ell, m\rangle$.

Now let q denote a "sifting" prime, which will satisfy $q \le Q$, $q \nmid r$, where Q is to be specified. The sifting condition in the ensuing argument is that $G(\ell, m)/r$ is either a quadratic residue ϖ or is 0, mod q. Denote by $\psi(q)$ the number of pairs $\langle \ell, m\rangle$, mod q that satisfy this condition. Thus $\psi(q) \le q^2$.

We can estimate $\psi(q)$ as on p. 56 of [8]. When $(m, q) = 1$ set $\ell \equiv \beta m$, mod q. Then the congruence $\varpi r \equiv m^\mu G(\beta, 1)$, mod q has $\frac{1}{2}q + O(\sqrt{q})$ solutions for $\langle \beta, \varpi\rangle$, mod q (in fact, half as many as there are solutions $\langle \beta, \gamma\rangle$ of $m^\mu G(\beta, 1) \equiv r\gamma^2$, mod q). In this way we obtain $\psi(q) = \frac{1}{2}q^2 + O\big(q^{3/2}\big)$.

Define $\psi^*(q) = q^2 - \psi(q)$, so that $\psi^*(q) \ge 0$, and make ψ, ψ^* multiplicative. We need an estimate for

$$\Sigma = \sum_{1 \le n \le Q,\ (n,r)=1} |\mu(n)| \frac{\psi(n)}{\psi^*(n)},$$

with the trivial interpretation $\Sigma = +\infty$ if some $\psi^*(n)$ were 0, in which case the quantity to be estimated in Lemma 5 below is also 0. Estimating Σ can be accomplished, with sufficient accuracy for our purposes, much more simply than in [8]. For our convenience define $\psi(q) = \frac{1}{2}q^2$ when $q \,|\, r$. Then

$$\Sigma \prod_{p|r} \left\{1 + \frac{\psi(p)}{\psi^*(p)}\right\} \ge \sum_{n \le Q} |\mu(n)| \frac{\psi(n)}{\psi^*(n)} \ge \sum_{p \le Q} \frac{\psi(p)}{\psi^*(p)} \gg \frac{Q}{\log Q},$$

so that

$$\Sigma \gg \frac{Q}{(Qr)^\epsilon}.$$

The sum Σ occurs both in Selberg's sieve and in the Large Sieve method, either of which we might employ at this point. We will use the following two-dimensional version of the arithmetic formulation of the Large Sieve inequality. Lemma 5 was established by Gallagher [6] (whose account is restricted to the case where the numbers N_i are all equal).

Lemma 5. *Suppose* $c(\mathbf{n}) = 0$ *if* $\mathbf{n} = \langle \ell, m\rangle$ *is in any one of a certain set of* $\psi(q)$ *"forbidden" residue classes,* $\mathrm{mod}\, q$*, for each prime* $q \le Q$*. Let* $\mathcal{B}$ *denote the box given by the inequalities* $M_1 \le \ell \le M_1 + N_1$*,* $M_2 \le m \le M_2 + N_2$*. Then*

$$\left| \sum_{\mathbf{n}\in\mathcal{B}} c(\mathbf{n}) \right|^2 \ll \frac{\Pi}{\Sigma} \sum_{\mathbf{n}\in\mathcal{B}} |c(\mathbf{n})|^2$$

where $\Pi = (N_1 + Q^2)(N_2 + Q^2)$ *and* Σ *is as above.*

Now let $\Sigma(d, \delta, r, \omega)$ denote the number of solutions of (5.5), for given d, δ, r, X_2, Y_2, ω satisfying (5.2), (5.3), (5.4), (5.7), so that in Lemma 2

$$S(X, Y, K) = \sum_{1\le d\le X, \delta | c_0} \sum_{1\le r\le R} \sum_{g(\omega,1)\equiv 0, \mathrm{mod}\ r} \Sigma(d, \delta, r, \omega),$$

R being as in (5.6). Then Lemma 5 gives the estimate

$$\Sigma(d, \delta, r, \omega) \ll \frac{(L + Q^2)(M + Q^2)(rQ)^\epsilon}{Q}.$$

Here $M = |\mathbf{a}|/\Delta \le L$, $LM \ll 1/\Delta = X_2Y_2/r$, as in (4.4) and (5.8). So we choose $Q = \sqrt{M}$, and we obtain

$$\Sigma(d, \delta, r, \omega) \ll \frac{LMX^\epsilon}{\sqrt{M}} \ll \frac{X^\epsilon}{\Delta\sqrt{M}} \ll \frac{X^\epsilon}{\sqrt{\Delta|\mathbf{a}|}} = \frac{X^\epsilon\sqrt{X_2Y_2}}{\sqrt{r|\mathbf{a}|}}.$$

We can apply part (b) of Lemma 4, in which we replace X, Y by X_2, Y_2. Using (5.6) we obtain

$$\sum_{1\le r\le R} \sum_{g(\omega,1)\equiv 0, \mathrm{mod}\ r} \Sigma(d, \delta, r, \omega) \ll X^\epsilon\big(X_2\sqrt{Y_2} + (X_2Y_2)^{\frac{3}{4}}R^{\frac{1}{4}}\big),$$

where we may replace ϵ by $\epsilon/5$. Since (5.4), (5.2), (5.3) give $X_2 = X/d$, $Y_2 = Y/(d\delta)$, $\delta\,|\,c_0$, where $c_0 \ne 0$ is a constant, summing this estimate over d, δ gives the estimate stated in Lemma 2.

This completes the proof of Theorem 2.

§6. *The proofs of Theorem 3 and Theorem 4.* We begin with Theorem 3. We make use of our approach to establishing (2.2), where we took $a = y^v$, $b = x^v - y^v$. We will simplify matters here by considering $y = 1$.

We suppose, as we may, that $n > 1$. We consider $F(x) = x\big(x^{n^2} - 1\big)$. Let X be sufficiently large. Fix N so that if $p > N$ then p does not divide the discriminant of $F(x)$, and so that

$$\sum_{p>N} \frac{n^2+1}{p^2} < \tfrac{1}{2}.$$

Let

$$P = \prod_{p \le N} p. \tag{6.1}$$

Set $G(s) = F\big(P^2 s - P\big)$. Observe that $G(s)$ has no roots modulo p^2 if $p \le N$. Also, if $p > N$, then $G(s)$ has at most $n^2 + 1$ roots modulo p^2. Therefore, the number of integers $s \in (X/P^2, 2X/P^2]$ for which $G(s)$ is divisible by p^2 for some prime $p \le 2X$ is bounded above by

$$\sum_{N<p\le 2X} (n^2+1)\left(\frac{X/P^2}{p^2}+1\right) \le \left(\sum_{p>N} \frac{n^2+1}{p^2}\right)\frac{X}{P^2} + (n^2+1)\pi(2X) \le \frac{3X}{4P^2}.$$

By letting X vary, we deduce that there are infinitely many integers t having the property that if p is a prime $\le t$ then $p^2 \nmid F(t)$. We show now that if t is a sufficiently large integer with this property, then either $\Phi_n(t)$ or $\Phi_{n^2}(t)$ must be squarefree, so that Theorem 3 will then follow since $\Phi_{n^2}(x) = \Phi_n(x^n)$. Suppose that neither are squarefree. Let $a = 1$, $b = t^{n^2} - 1$. Note that there is a $g(x) \in \mathbb{Z}[x]$ such that $F(x) = \Phi_n(x)\Phi_{n^2}(x)g(x)$. By our assumption, we deduce that there are primes p_1, p_2, not necessarily distinct, satisfying $p_1^2 p_2^2 \,|\, F(t)$. Since $p^2 \nmid F(t)$ for every prime $p \le t$, we deduce that p_1 and p_2 are $> t$. Hence

$$Q\big(ab(a+b)\big) = Q\big(F(t)\big) < F(t)/t^2 < t^{n^2-1},$$

and we obtain

$$L_{a,b} > \frac{n^2}{n^2-1}.$$

By our assumption that the *abc*-conjecture holds, there can be only finitely many such pairs (a,b). This implies as desired that if t is sufficiently large then either $\Phi_n(t)$ or $\Phi_{n^2}(t)$ is squarefree. This completes the proof of Theorem 3.

As was remarked in §1, a similar approach leads to the slightly stronger result that the polynomial

$$f_n(x) = \frac{x^n - 1}{x - 1}$$

is infinitely often squarefree. To show this one would observe

$$F(x) = x(x-1)f_n(x)f_n(x^n),$$

where $F(x)$ is as before, and argue as above to show that either $f_n(t)$ or $f_n(t^n)$ is squarefree when t is large.

We follow a similar approach in proving Theorem 4, but do not take $y = 1$. Set

$$F(x,y) = xy(x^{2n} - y^{2n}) \text{ for } n = 1, 2, \ldots.$$

With N sufficiently large and P as in (6.1) take $G(s,t) = F(x,y)$, where

$$x = P^2 s - P,\ y = Pt - 1. \tag{6.2}$$

If $p^2 \,|\, G(s,t)$ then $p > N$, because $G(s,t) \equiv -P, \bmod p^2$ when $p \le N$.

Let $C(X,Y,p^2)$ denote the number of $\langle x,y\rangle$ such that (6.2) holds and

$$F(x,y) \equiv 0, \bmod p^2, \;\; X < x \le 2X, \;\; Y < y \le 2Y, \tag{6.3}$$

where we will take $X = Y^\alpha$ with $\alpha > 1$, as elsewhere in this paper. We wish to estimate

$$\sum_{N<p\le 2X} C(X,Y,p^2) \tag{6.4}$$

from above. It will not be necessary to use the arguments from §4.

For the terms with $p \nmid y$ observe that t takes at most $Y/P+1$ values and for each of these the integer s lies in at most $2n+1$ residue classes mod p^2, in each of which there are at most $X/(Pp)^2+1$ values of s for which $X < x \le 2X$. Thus the contribution to (6.4) from such terms does not exceed

$$\sum_{N<p\le 2X} (2n+1)\left(\frac{Y}{P}+1\right)\left(\frac{X/P^2}{p^2}+1\right).$$

When $p \,\|\, y$ the congruence in (6.3) gives $p \,|\, x$, so the contribution from these terms does not exceed

$$\sum_{N<p\le 2X} \left(\frac{Y/P}{p}+1\right)\left(\frac{X/P^2}{p}+1\right).$$

When $p^2 \,|\, y$ (6.3) gives $p \le \sqrt{2Y}$, so the contribution from these terms does not exceed

$$\sum_{N<p\le \sqrt{2Y}} \left(\frac{Y/P}{p^2}+1\right)\left(\frac{X}{P^2}+1\right).$$

We will choose N (and hence P) sufficiently large, and then take X, Y sufficiently large (in terms of N). Since $X^\epsilon < Y < X$ all the contributions to (6.4) are

$$\ll \frac{XY}{NP^3} + \frac{Y}{P}\pi(2X) + \left(\frac{X}{P^2}+\frac{Y}{P}\right)\log\log X + \frac{X}{P^2}\pi(\sqrt{2Y}\,),$$

and we obtain

$$\sum_{N<p\le 2X} C(X,Y,p^2) < \frac{3XY}{4P^3}$$

when N, X, Y are large enough.

But the total number of pairs $\langle x,y\rangle$ such that (6.2) holds and $X < x \le 2X$, $Y < y \le 2Y$ is asymptotic to XY/P^3. Hence there exists such a pair $\langle x,y\rangle$ with the property that $p^2 \nmid F(x,y)$ for every $p \le 2X$. Now by letting X vary we obtain infinitely many pairs $\langle x,y\rangle$ for which there exists an X such that

$$X < x \le 2X, \;\; X^\alpha < y \le 2X^\alpha, \;\; p^2 \,|\, F(x,y) \Rightarrow p > 2X, \tag{6.5}$$

so that in particular x and y are squarefree.

From this we can deduce, using the abc-conjecture, that for infinitely many of these pairs $\langle x, y\rangle$ at least one of the numbers $xy\big(x^n + y^n\big)$, $xy\big(x^n - y^n\big)$ is squarefree. For if $p_1^2 \mid xy\big(x^n + y^n\big)$, $p_2^2 \mid xy\big(x^n - y^n\big)$ we would obtain $p_1 > 2X$, $p_2 > 2X$, so that actually $p_1 \nmid xy$, $p_2 \nmid xy$. Take $a = y^{2n}$, $b = x^{2n} - y^{2n}$. Then

$$Q\big(ab(a+b)\big) = Q\big(xy(x^{2n} - y^{2n})\big) \le \frac{xy(x^{2n} - y^{2n})}{p_1 p_2} < 2^{2n} Y^{(2n-1)\alpha+1}.$$

Consequently

$$\begin{aligned} L_{a,b} &> \frac{\log x^{2n}}{\log\big(2^{2n} Y^{(2n-1)\alpha+1}\big)} > \frac{2n\alpha \log Y}{2n\log 2 + \big((2n-1)\alpha + 1\big)\log Y} \\ &\to \frac{2n\alpha}{(2n-1)\alpha+1} > 1 \text{ as } Y \to \infty, \end{aligned}$$

since $\alpha > 1$. This contradicts the $abc-$conjecture.

We can now complete the proof of Theorem 4. If $xy\big(x^n - y^n\big)$ is squarefree for infinitely many pairs $\langle x, y\rangle$ appearing in (6.5), then put $a = y^n$, $b = x^n - y^n$. Then $Q\big(ab(a+b)\big) = xy(x^n - y^n)$. Otherwise $xy\big(x^n + y^n\big)$ is squarefree infinitely often, and we take $a = y^n$, $b = x^n$, so that $Q\big(ab(a+b)\big) = xy(x^n + y^n)$. In either case, we obtain

$$L_{a,b} = \frac{n\alpha}{(n+1)\alpha + 1} + O_n\left(\frac{1}{\log Y}\right).$$

With α fixed, let $Y \to \infty$. Then let α vary over $(1, \infty)$. Since the set of limit points is closed, we get that all points of the interval $[n/(n+2), n/(n+1)]$ are limit points, and Theorem 4 now follows using

$$\bigcup_{n=1}^{\infty} \left[\frac{n}{n+2}, \frac{n}{n+1}\right] = [\tfrac{1}{3}, 1),$$

together with the observation made in the introduction that the abc-conjecture implies that there are no limit points of $\mathcal{L}$ outside $[\frac{1}{3}, 1]$.

References

1 G.A. Baker and P. Graves-Morris : Padé Approximants, Part I: Basic Theory (Encyclopedia of Mathematics, Volume 13), Addison-Wesley Publ. Co., Reading, MA, 1981.

2 J. Browkin and J. Brzezinski : Some remarks on the *abc*-conjecture, Math. Comp. 62 (1994), 931–939.

3 J.W.S. Cassels : An Introduction to the Geometry of Numbers, Springer, Berlin, 1959.

4 P. Erdős : Arithmetical Properties of Polynomials, J. London Math. Soc. 28 (1953), 416–425.

5 M. Filaseta : Short Interval Results for k-free Values of Irreducible Polynomials, Acta Arith. 64 (1993), 249–270.
6 P.X. Gallagher : The Large Sieve and Probabilistic Galois Theory, Amer. Math. Soc. Proc. Sympos. Pure Math. 24 (1973), 91–101.
7 F. Gouvêa and B. Mazur : The Square-free Sieve and the Rank of Elliptic Curves, J. Amer. Math. Soc. 4 (1991), 1–23.
8 G. Greaves : Power-free Values of Binary Forms, Quart. J. Math. Oxford (2) 43 (1992), 45–65.
9 C. Hooley : On the Power Free Values of Polynomials, Mathematika 14 (1967), 21–26.
10 M.N. Huxley and M. Nair : Power Free Values of Polynomials III, Proc. London Math. Soc., 41 (1980), 66–82.
11 S. Lang : Old and New Conjectured Diophantine Inequalities, Bull. Amer. Math. Soc. 23 (1990), 37–75.
12 T. Nagell : Zur Arithmetik der Polynome, Abh. Math. Sem. Hamburg Univ. 1 (1922), 179–184.
13 C.L. Stewart and R. Tijdeman : On the Oesterlé-Masser Conjecture, Monatsh. Math. 102 (1986), 251–257.
14 B.M.M. de Weger : Algorithms for Diophantine Equations, C.W.I. Tract 65 (1989), Amsterdam, p. 126.

Authors' addresses :

J. Browkin
Institute of Mathematics
University of Warsaw
ul. Banacha 2
PL-02-097 Warsaw
Poland

M. Filaseta
Dept. of Mathematics
University of South Carolina
Columbia
South Carolina 29208
U.S.A.

G.R.H. Greaves
School of Mathematics
University of Wales, Cardiff
23, Senghennydd Road
P.O. Box 926
Cardiff CF2 4YH
Wales, U.K.

A. Schinzel
Mathematics Institute
Polish Academy of Sciences
P.O. Box 137
PL-00-950 Warsaw
Poland

MSC 1991 : 11N25