An effective $p$-adic analogue of a theorem of Thue III

The diophantine equation $y^2 = x^3 + k$

by

J. COATES (Cambridge)

I. Introduction. The purpose of the present note is to apply the work of [5], [6] to the equation $y^2 = x^3 + k$, where $k$ is any non-zero integer. Let $p_1, \ldots, p_s$ be $s \geq 0$ prime numbers, and let $f$ be the largest integer, comprised solely of powers of $p_1, \ldots, p_s$, which divides $k$. We write $P$ for the maximum of $p_1, \ldots, p_s$; if no primes are specified, we take $P = 2$. Then our principal result is as follows:

**Theorem 1.** All solutions of the equation $y^2 = x^3 + k$ in integers $x, y$, with $(x, y, p_1 \ldots p_s) = 1$, satisfy

$$\max(|x|, |y|) < \exp \{2^{10^{7}+0.5^{2}} p^{10^{7}+0.5} |k/f|^{10^{7}+0.5} \}.$$ 

It will be observed that when $s = 0$, that is when no primes $p_1, \ldots, p_s$ are specified, Theorem 1 reduces to a slightly weaker form of the result in Baker's paper [1]. On the other hand, if $k$ is comprised solely of powers of $p_1, \ldots, p_s$ so that $|k/f| = 1$, then Theorem 1 implies that all solutions of the equation $y^2 = x^3 + k$ in integers $x, y$, with $(x, y, p_1 \ldots p_s) = 1$, satisfy

$$\max(|x|, |y|) < \exp \{2^{10^{7}+0.5^{2}} p^{10^{7}+0.5} \}.$$ 

(1)

The interest of this result lies in the fact that the number on the right does not depend on the exponents to which $p_1, \ldots, p_s$ divide $k$. In particular, it can be used to give the following explicit lower bound for the greatest prime factor of $x^2 - y^2$.

**Theorem 2.** If $x, y$ are integers, with $(x, y) = 1$, then the greatest prime factor of $x^2 - y^2$ exceeds

$$10^{-5} (\log \log X)^{1/4},$$

where $X = \max(|x|, |y|)$.

In order to deduce Theorem 2 from (1), we let $\Psi$ be either 1 or the greatest prime factor of $x^2 - y^2$, according as $|x^2 - y^2| = 1$ or $|x^2 - y^2| > 1$, and we let $p_1, \ldots, p_s$ be the primes not exceeding $\Psi$. 

References


Noting that \(s + 1 \leq 2N\) and \(P \leq 2N\), we conclude from (1) that
\[ X = \max(|x|, |y|) < \exp_{\exp_{(10^N)^{1/3}}}, \]
which is equivalent to the assertion of Theorem 2.

Theorem 1 can be expressed in a number of different ways. For example, an equivalent formulation is that
\[ |x^3 - y^2| \prod_{i=1}^{s} |y^3 - y^2|_{p} > 2^{-s(a+b)^2} p^{-a(b+1)} (\log x)^{3s - (a+b)n - 2}, \]
for all integers \(x, y\), with \((x, y, p_1, \ldots, p_s) = 1\) and \(x^3 - y^2 \neq 0\).

Theorem 1 has an application to the theory of elliptic curves. Let \(E\) be a curve of genus 1, with rational coefficients, and with a rational point. We say that \(E\) has a good reduction at a prime \(p\) if \(E\) is birationally equivalent to a curve defined by a cubic equation \(f(x, y) = 0\) with rational coefficients which are integral at \(p\), and which is such that the reduction \(\tilde{f}\) of \(f\) modulo \(p\) defines a non-singular cubic over the field \(\mathbb{F}_p\) with \(p\) elements. As before, let \(S = \{p_1, \ldots, p_s\}\) be a set of primes, which we assume, for simplicity, contains 2 and 3. Then, since 2 and 3 belong to \(S\), it is easily seen that \(E\) has a good reduction at all primes not in \(S\) if and only if its equation can be put in the form
\[ y^2 = 4x^3 - g_2x - g_3, \]
where \(g_2, g_3\) are integers which are not both divisible by the sixth power of any prime in \(S\), and where the discriminant
\[ A = g_2^3 - 27g_3^2 \]
of (2) is composed solely of powers of \(p_1, \ldots, p_s\) (cf. [4], p. 211). Thus, if \(E\) has a good reduction at the primes not in \(S\), it follows from Theorem 1, on rewriting (3) as
\[ 3^2 d = (3g_2)^3 - (3g_3)^2, \]
that
\[ \max(|g_2|, |g_3|) < \exp_{(2^{3(a+b)n+3} p^{2(a+b)n})}. \]

The application of Theorem 1 to (3) is valid, since we shall in fact establish Theorem 1 under the weaker hypothesis that \(x\) and \(y\) are not both divisible by the ninth power of any of \(p_1, \ldots, p_s\). We have therefore obtained in principle (1) an effective procedure for determining all elliptic curves having a good reduction at the primes not in \(S\). This means that we can determine all elliptic curves with a given conductor (cf. [8]), a fact which may be of interest in connexion with the verification of a conjecture of Weil [9] about these curves.

(1) By refining our methods, it may be possible to make this bound practically computable (cf. [2]).

The derivation of Theorem 1 from Theorem 1 of [8] is based on the treatment of the equation \(y^2 = x^3 + h\) given in [1], and is due originally to Mordell. However, we have found it necessary to generalize the classical reduction theory of binary cubic forms used in [1] so as to include a finite set of \(p\)-adic valuations as well as the ordinary absolute value, and § II is devoted to a proof of this generalization. It should also be noted that the results of this paper were first proven in a non-effective form by Mahler [7]. In fact, Mahler's general theorem, valid for any curve of genus 1, could be proven effectively by combining the work of [5], [6] with [3] but the results obtained would be much weaker than those established here.

II. The \(p\)-adic reduction of cubic forms. Let \(S = \{p_1, \ldots, p_s\}\) be an arbitrary set of \(s > 0\) prime numbers. The purpose of this section is to generalize the classical reduction theory of binary cubic forms (7) (cf. [1], p. 196) to include the valuations \(|_{p_1}, \ldots, |_{p_s}\) as well as the ordinary absolute value.

We first consider the \(p\)-adic reduction of binary quadratic forms. The result obtained will then be used to study cubic forms. By an \(S\)-integer, we shall mean a rational number whose denominator is composed solely of powers of \(p_1, \ldots, p_s\). Let \(Q(X, Y) = AX^2 + BX Y + CY^2\) be a binary quadratic form, whose coefficients \(A, B, C\) are \(S\)-integers, and whose discriminant \(D = 4AC - B^2\) is a rational integer divisible by \(4\).

Lemnma 1. By a substitution of the form \(X = rX' + sY', Y = tX' + uY', \) where \(r, s, t, u\) are \(S\)-integers with \(ru - qt = 1\), \(Q(X, Y)\) can be transformed into a quadratic form \(Q'(X', Y') = A'X'^2 + B'X'Y' + C'Y'^2\) with
\[ \max(|A'|_p, |B'|_p, |C'|_p) \leq p \quad \text{for all } p \in S. \]

Proof (4). By omitting certain primes from \(S\) if necessary, we can assume that, for each \(p\) in \(S\), the numerators of \(A, B, C\) are not all divisible by \(p\). We contend that, for each \(p\) in \(S\), there exist integers \(t_p, u_p\), with no common factor, such that
\[ |Q(t_p, u_p)|_p = \max(|A|_p, |B|_p, |C|_p). \]

For, if \(A\) denotes the least common multiple of the denominators of \(A, B, C\), then by assumption not all of \(AA, AB, AC\) are divisible by \(p\). The assertion is obvious if \(AA\) and \(AC\) are both divisible by \(p\) (take

(1) The arguments of [1] are plainly valid for an arbitrary binary cubic form.
(2) Here, and in subsequent arguments, a slightly weaker result is valid if \(D\) is not divisible by 4.
(4) I am indebted to Professor J.W.S. Cassels for the proof of this lemma.
LEMMA 2. By a substitution of the form \( X = sX' + qY', Y = tX' + uY' \), where \( v, q, t, u \) are \( S \)-integers with \( ru - qt = 1 \), \( F(X, Y) \) can be transformed into a cubic form

\[
F'(X', Y') = a'X'^3 + 3b'X'Y' + 3c'Y'^2 + \alpha'X'
\]

such that

\[
\max(|a'|, |b'|, |c'|, |\alpha'|) \leq p|D|^{-1/2} \quad \text{for all } p \in S.
\]

Proof. Let \( Q(X, Y) \) be the quadratic covariant of \( F(X, Y) \) defined by

\[
Q(X, Y) = \frac{1}{36} \left( \frac{\partial^2 F}{\partial X \partial Y} \right)^2 - \frac{\partial^2 F}{\partial X^2} \cdot \frac{\partial^2 F}{\partial Y^2} = AX^2 + BXY + CY^2.
\]

It is readily verified that

\[
A = v - au, \quad B = bu - av, \quad C = \alpha^2 - bd, \quad D = 4AD - B^2.
\]

Thus, as \( A, B, C \) are clearly \( S \)-integers and \( D \) is an integer divisible by 4, we can assume that

\[
\max(|A|, |B|, |C|) \leq p \quad \text{for all } p \in S;
\]

for Lemma 2 shows that this can be achieved by a transformation of the specified type.

Let \( \Delta \) be the least common multiple of the denominators of \( A, B, C, D \). By omitting certain primes from \( S \) if necessary, we can suppose that, for each \( p \in S \), not all of \( \Delta a, 3\Delta b, 3\Delta c, \Delta d \) are divisible by \( p \). In the following, we shall assume that both 2 and 3 belong to \( S \); a slightly simpler form of the subsequent argument is valid if this is not so.

We assert that, by means of a transformation of the specified type, we can ensure that

\[
\max(|A|, |B|, |C|, |D|) \leq p^2 \quad \text{for all } p \in S,
\]

and

\[
p^3|a| > \max(|a|, |b|, |c|, |d|), \quad |b| < p^{-2} \quad \text{for all } p \in S,
\]

with \( r \) any given positive integer. To prove this, we first observe that, for each \( p \in S \), there exist integers \( r_p, t_p \), with no common factor, such that

\[
|F(r_p, t_p)| = \max(|a|, |b|, |c|, |d|).
\]

This is obvious if either \( \Delta a \) or \( \Delta d \) is not divisible by \( p \) (take \( r_p, t_p \) to be 0 and 1 appropriately), and it is also obvious if both \( \Delta a, \Delta d \), and one of \( 3\Delta b, 3\Delta c \) is divisible by \( p \) (take \( r_p = 1, t_p = 1 \)). If \( p \neq 2,3 \) and neither

\( (p) \) If \( p \neq 2,3 \), this lemma can be replaced by \( p^3|D|^{-1/2} \).
of the previous two cases holds, so that \( A_0, A_d \) are divisible by \( p \) but
\( 3A_0, 3d \) are not, the assertion is still obvious (take \( r_1 = 1 \) and choose \( t \)
p so that \( p \) does not divide \( t_0 \) and \( 3A_0 + t_0 \cdot 3d \)). If \( p = 2 \), we can always
ensure that one of the previous two cases holds by means of a substitution
\( X = 2X', Y = 2^{-1}Y' \); but then the inequality (11) when \( p = 2 \)
must be replaced by (10). Next, applying (12), a similar argument to
that given in the proof of Lemma 1 shows that, by means of a substitution
\( X = rX' + qY', Y = rX' + uY' \), where \( r, q, t, u \) are integers with \( ru - gt = 1 \),
we can arrange that
\[
|a|_p = \max \{|a|_p, |b|_p, |3a|_p, |d|_p\} \quad \text{for all } p \in \mathcal{S}.
\]
Further, the covariant property of \( Q(X, Y) \) and the fact that \( r, q, t, u \)
are integers imply that (9) when \( p \neq 2 \), and (10) when \( p = 2 \), remain
valid. Having established (13), we assert that by means of a substitution
\( X = X' + \frac{1}{k} kY', Y = 2Y' \), where \( k \) is an integer, we can ensure that
the second inequality in (11) holds. For, if \( \lambda' \) denotes the least common
multiple of the denominators of \( a \) and \( 3b \) then, since \( |a|_p \geq |3b|_p \), for all \( p \)
in \( \mathcal{S} \), there exist integers \( j, k \) such that
\[
j\lambda' p_1^{j+1} \cdots p_s^{j+1} = 3\lambda' a = 3\lambda' b;
\]
the assertion is then plainly valid with \( h = k \), since the substitution
takes \( \lambda' \) into \( \lambda + 3b \). If \( p \neq 3 \), all the previous inequalities hold after
this last substitution has been made, and if \( p = 3 \) it is easily seen that
(10) holds in place of (9) and the first inequality in (11) holds in place of
(13). This completes the proof of (10) and (11).

We deduce from the identity \( A = b^2 - ac \) and (10), (11) that
\[
|ac|_p \leq p^3,
\]
whence by (11)
\[
|a|_p \leq p \quad \text{for all } p \in \mathcal{S}.
\]
This fact, together with the second inequality in (11), shows that \( |bc|_p \leq p^3 \),
and so we conclude from the identity \( B = bc - ad \) and (10), (11) that
\[
|d|_p \leq p \quad \text{for all } p \in \mathcal{S}.
\]

In the remainder of the proof, we need only consider those primes in
\( \mathcal{S} \) for which
\[
\max \{|a|_p, |d|_p\} < p^{-1} |D|_{p-1}^{1/2},
\]
since, for those primes in \( \mathcal{S} \) not satisfying this inequality, we conclude from
the identities \( A = b^2 - ac, B = bc - ad \) and (10), (11) that \( |a|_p \leq p^4 |D|_{p-1}^{1/2} \),
whence the assertion of Lemma 2 is valid for such primes.

Further, we need only consider the primes in \( \mathcal{S} \) satisfying
\[
|a|_p < p^{-3} |D|_p;
\]
for the identity \( B - Ac = Ca \) and (10), (11), (18) show that \( |a|_p \leq p^3 |D|_{p-1}^{1/2} \)
for those primes not satisfying (17), and so the assertion of Lemma 2
holds for those primes.

It is clear from (10) and (17) that, for those primes \( p \) still requiring
consideration, we have \( |4AC|_p < |D|_p \), whence we deduce from the identity
\( 4AC - B^2 = D \) that
\[
|B|_p = |D|_p^{1/2}.
\]
In particular, it follows from this last equation and (11) and (16) that
\( |B|_p > |bc|_p \); but then the identity \( B = bc - ad \) implies that
\[
|B|_p = |ad|_p.
\]
Now let \( v \) be the product of powers of \( p_1, \ldots, p_s \) such that
\[
|a|_p = |v|_p \quad \text{for all those primes } p \text{ in } \mathcal{S} \text{ still being considered. Then, as } v^2 a = ad/(d/v^2),
\]
we conclude from (18), (19), (20) that
\[
p^{-1} |D|_{p-1}^{1/2} \leq |v^2 a|_p \leq |D|_p^{1/2}.
\]
Further, we have \( c/v = v^2 ac/(ae^2) \), and so it follows from (21) and the
inequality \( |ac|_p \leq p^3 \) that
\[
|c|_p \leq p^{1/2} |D|_{p-1}^{1/2}.
\]
But now the substitution \( X = vX' + vY', Y = v^{-1} Y' \) is of the required
type, and transforms \( a, b, c, d \) into
\[
v^2 a, \quad v^2 a - v d, \quad v^2 a + 2v b + c/v, \quad v^2 a + 3v b + 3 c/v + d/v^2,
\]
respectively. By virtue of (11), (20), (21), (22), it is clear that the cubic
form, obtained after this substitution, satisfies all the assertions of Lemma 2.

We can now give our generalization of the classical reduction theory
of binary cubic forms. As before, let \( F(X, Y) = aX^3 + bX^2 Y + cX Y^2 + dY^3 \) be a binary cubic form, whose coefficients \( a, b, c, d \) are \( S \)-integers,
and whose discriminant \( D \), given by (8), is an integer divisible by 4.

**Theorem 3.** By a substitution of the form \( X = rX' + qY', Y = tX' + uY' \),
where \( r, q, t, u \) are \( S \)-integers with \( ru - qt = 1 \), \( F(X, Y) \) can be transformed into a cubic form
\( F'(X', Y') = a' X'^3 + b' X'^2 Y' + c' X' Y'^2 + d' Y'^3 \)
with
\[
\max \{|a'|_p, |b'|_p, |c'|_p, |d'|_p\} \leq p^3 |D|_{p-1}^{1/2} \quad \text{for all } p \in \mathcal{S},
\]
\[
\max \{|a'|_p, |b'|_p, |c'|_p, |d'|_p\} \leq 3^{1/2} (p_1 \cdots p_s)^{1/2} |D|.
\]
Proof. Lemma 2 shows that, by a substitution of the type specified in the theorem, we can ensure that the first set of inequalities is valid. Assuming this is so, let \( A \) be the least common multiple of the denominators of \( a, b, c, d; \) evidently

\[ A \leq \prod_{i=1}^{n} p_i^{|D_i|^{1/2}} \leq (p_1 \ldots p_n)^{|D|^{1/2}}. \]

The cubic form \( AF(X, Y) \) has integer coefficients and discriminant \( A^3 D \). Hence (cf. [1], p. 196), by means of a substitution \( X = rX' + qY', \ Y = sX + uY' \), where \( r, q, t, u \) are integers with \( ru - qt = \pm 1 \), \( AF(X, Y) \) can be transformed into a cubic form with the maximum of the absolute values of its coefficients at most \( |A|^3 \langle D \rangle^{1/2} \). Dividing this cubic form by \( A \), and noting (23), we have clearly proven Theorem 3.

III. Proof of Theorem 1. Let \( x, y \) be integers, which are not both divisible by the ninth power of any \( p_1, \ldots, p_s \), satisfying the equation \( y^3 = x^3 + k \). We first modify this equation. Recall that \( r \) is the largest integer, comprised solely of powers of \( p_1, \ldots, p_s \), which divides \( k \). Suppose that \( r = p_1^{e_1} \ldots p_s^{e_s} \), where \( e_1, e_2, \ldots, e_s, (1 \leq i \leq s) \) are non-negative integers such that \( 0 \leq e_i < 6 \). Then, if we put

\[ x' = x/(p_1^{e_1} \ldots p_s^{e_s}), \quad y' = y/(p_1^{e_1} \ldots p_s^{e_s}), \quad k' = k/(p_1^{e_1} \ldots p_s^{e_s}), \]

we have

\[ y'^3 = x'^3 + k'. \]

We denote by \( F(X, Y) \) the binary cubic form

\[ X^3 - 3x'XY^2 - 2y'Y^3. \]

By virtue of (24), the discriminant \( D \) of \( F(X, Y) \) is equal to \(-4k'\), and the coefficients of \( F(X, Y) \) are \( S \)-integers. We can therefore apply the reduction theory given in \( \S \) II. We conclude (cf. the proof of Theorem 3) that, by means of a substitution \( X = rX' + qY', \ Y = tX' + uY' \), where \( r, q, t, u \) are \( S \)-integers with \( ru - qt = \pm 1 \), \( F(X, Y) \) is transformed into a cubic form

\[ F'(X', Y') = aX'^3 + \beta X'^2 Y' + \gamma X' Y'^2 + \delta Y'^3 \]

with the property that, if \( A \) denotes the least common multiple of the denominators of \( a, \beta, \gamma, \delta \), then

\[ A \leq D^{1/2} \max(|Aa|, |A\beta|, |A\gamma|, |A\delta|) \leq 3^{1/5} D^{1/3}. \]

The argument now divides into two cases, according as \( F'(X', Y') \) is irreducible or not.

Suppose first that \( F'(X', Y') \) is irreducible. On equating the coefficient of \( X \) in the equation

\[ AF'(uX-qY, -tX+rY) = \pm A F(X, Y), \]

we obtain

\[ A \alpha u^3 - B \beta \nu^2 t + C \rho u t - D \delta \rho^2 = \pm A. \]

Since \( F'(X', Y') \) is irreducible, we can now apply Theorem 1 of [8] to (27). We take the primes specified in Theorem 1 to be the prime factors of the least common multiple \( \delta \) of the denominators of \( u \) and \( t \), and we take \( s = 6(s+1)+2 \). We deduce from Theorem 1 an upper bound for \( \max(|d|/|d| \}, \) whence, substituting this bound back into (27), we obtain an upper bound for the exponents to which \( p_1, \ldots, p_s \) divide \( \delta \). Noting that

\[ v < 31 \cdot 10^2 (s+1)^2, \quad \rho^2 < D^{2(s+1)} |D|^2, \quad A \leq D^{1/2} |D|^{1/2}, \]

we conclude that

\[ \max(|u|, |t|) < M, \quad \max(|u|/|d|, |t|/|d|) < M \quad (1 \leq i \leq s), \]

where

\[ M = \exp(2^{3(s+1)} 2^{1/3} |D|). \]

Now, on differentiating the identity

\[ F'(rX+qY, tX'+uY') = F'(X', Y') \]

with respect to \( X' \) and \( Y' \), and substituting \( X' = u, \ Y' = -t \), we obtain

\[ 3i = 3su^3 - 2\beta \nu^2 u + \gamma t^2, \quad 3q = -3\delta u^2 - 2\rho u t + \beta s, \]

respectively. It then follows from (25) and (28) that

\[ \max(|\gamma|, |\gamma|) < M^3, \quad \max(|\gamma|/|d|, |\gamma|/|d|) < M^3 \quad (1 \leq i \leq s). \]

Furthermore, equating the coefficients of \( X'Y' \) and \( Y'Y' \) in (28), we have

\[ 3x' = 3(\beta u^2 - \alpha q^2) + 2q^2(\beta s - \gamma t) + \beta t q^2 - \gamma u^2, \]

\[ 2y' = 2q^2 - 2\beta r q^2 + \gamma q^2 - \delta r^2. \]

Thus, by virtue of (25), (28), and (29),

\[ \max(|x'|, |y'|) < M^2, \quad \max(|x'|/|d|, |y'|/|d|) < M^2 \quad (1 \leq i \leq s). \]

But, as \( x' = x/(p_1^{e_1} \ldots p_s^{e_s}), y' = y/(p_1^{e_1} \ldots p_s^{e_s}), \) and \( x \) and \( y \) are not both divisible by the ninth power of any of \( p_1, \ldots, p_s \), this last inequality implies that

\[ \max(|x|, |y|) < M^{6(s+1)}. \]

Noting that \( |D| = d |d| \leq D^{1/2} |d| \), Theorem 1 follows immediately.

Acta Arithmetica XVI 6
Now assume that $F'(X', Y')$ is reducible. The estimate (28) remains valid in this case, but it does not seem possible to prove it by an elementary argument, as is done in the analogous situation in [1]. However, it can be established by modifying the work of § V of [5] and § IV of [6] so that it is applicable to reducible cubic forms with three distinct linear factors (*).

In the next paragraph, we shall indicate the significant changes that must be made in the arguments of § VI of [5], but we shall leave the detailed verification that (27) implies (28) to the reader. Note that $F'(X', Y')$ does indeed have three distinct linear factors, since its discriminant $D = -4k^2$ is not 0. It is also clear that, once we have established (28), the conclusion of Theorem 1 follows by the same reasoning as in the preceding paragraph.

In the notation of § VI of [5], we must therefore consider an equation of the form

$$\alpha_2 y' = \alpha_3 y'' (x' - a_1 y') (x' - a_2 y') = m',$$

where $a_1, a_2, a_3$ are distinct, and the field $K = K_{a_1, a_2, a_3}$ has degree $n < 2$. Here $x', y'$ are $S$-integers, and $m'$ is an integer satisfying $|m'|_{\nu_i} \gg p_i^{-1}$ ($1 \leq i \leq s$). As in § V of [5], we also use $S = \{ \lambda_1, \ldots, \lambda_s \}$ to denote the set of valuations of $K$ extending the valuations $|\nu_i|$, $\cdots$, $|\nu_s|$ of $Q$, and we let $\eta_1, \ldots, \eta_{s-1}$ denote $S$-units of $K$ satisfying (59) of [5]. Further, we signify by $\beta_i^{(j)} (1 \leq j \leq n)$ the field conjugates of an element $\beta_i$ of $K$ in $\Omega_1$, and by $N^{1/2} \beta_i$ the field norm of $\beta_i$. Put

$$\beta_i = x' - a_i y', \quad m'_i = N^{1/2} \beta_i, \quad \eta_i = \prod_{\nu_i} m'_{\nu_i}^{1/(\nu_i(\omega))}.$$

We deduce, as in § V of [5], that there exist integers $b_{i,1}, \ldots, b_{i,s-1}$ such that $\gamma_i = \beta_i b_{i,1}^{(1)} \cdots b_{i,s-1}^{(s-1)}$ satisfies

$$|\log(\gamma_i^{(1)})| |\beta_i|_{\nu_i} \leq C_{i} \quad (1 \leq i \leq s).$$

We let $H_i = \max |b_{i,j}|$, and we suppose that $H_q = \max H_i$. Then, for some pair of indices $i, j$, we have

$$\log(\gamma_i^{(1)}) |\beta_i|_{\nu_i} \leq -(C_i H_q - C_3)/(n \sigma - 1).$$

It follows from (30) that

$$|\beta_i^{(1)}|_{\nu_i} \gg C_i \sigma^{-1/2},$$

for some index $l \neq q$. Let $h$ be distinct from $l$ and $q$. From the identity

$$\alpha_1^{(1)} - \alpha_2^{(1)} \beta_i^{(1)} = (\alpha_1^{(1)} - \alpha_2^{(1)}) \beta_i^{(1)} = (\alpha_2^{(1)} - \alpha_3^{(1)}) \beta_i^{(1)},$$

we obtain

$$\eta_i^{(1)} \cdots \eta_i^{(s-1)} = \alpha = \omega,$$

where

$$b_k = b_{i,1} \cdots b_{i,s-1} \quad \alpha = \frac{(\alpha_1^{(1)} - \alpha_2^{(1)}) \beta_i^{(1)}}{(\alpha_1^{(1)} - \alpha_3^{(1)}) \beta_i^{(1)}}, \quad \omega = \frac{(\alpha_1^{(1)} - \alpha_3^{(1)}) \beta_i^{(1)}}{(\alpha_1^{(1)} - \alpha_2^{(1)}) \beta_i^{(1)}}.$$

Since now $|b_k| \leq 2H_q$, all the subsequent arguments of § V of [5] and § IV of [6] are valid without essential change, and (28) follows. This completes the proof of Theorem 1.

References


DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
Cambridge, England

Roy par la Rédaction le 25.0.699
A congruence for the second factor of the class number of a cyclotomic field (Corrigendum)

by

L. CARLITZ (Durham, N. C.)

Let $h$ denote the class number of the cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$, $p > 3$; also let $h_1, h_2$ denote the first and second factors, respectively, of the class number. It is proved in [1] that

$$h_2 G = \pm h_1 \pmod{p},$$

where

$$G = (-1)^{m+1} 2^{\nu+2} G_0^{-1} C \pmod{p}.$$ 

It has been pointed out by T. Metsänkylä [2] that $G_0$ is incorrectly defined in [1]. The error occurs in (2.9); it is easily seen that the left member should be multiplied by $\zeta^2$. Consequently the left members of (2.13), 2.14) and the formula at the top of p. 31 should all be multiplied by $\zeta^2$.

It follows that

$$G_0 = |g^{2m}| \quad (j = 0, 1, \ldots, m-2; \quad n = 1, 2, \ldots, m-1),$$

so that $G_0$ is the difference product of the quadratic residues $\neq 1$ of $p$.

The last paragraph of § 3 should be omitted.

On p. 28, line 8, $h_0$ should be replaced by $h$.

References
