have no solution in integers $(x_1, x_2, y) \neq (0, 0, 0)$. Since $f(\nu)$ tends to 1, this shows that form (b) of Dirichlet's theorem cannot be improved for (α, β).

Hence if form (a) cannot be improved, then form (b) cannot be improved. The implication in the opposite direction may be shown in an entirely analogous manner.

References

[1] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer Grundlehren 99 (1959).

[2] H. Davenport and W. M. Schmidt, *Dirichlet's theorem on diophantine approximation*, Rendiconti convegno di Teoria dei numeri, Roma 1968. (To appear).

[3] O. H. Keller, *Geometrie der Zahlen*, Enzyklop. der math. Wiss. I. 2, Heft 11, 1954.

[4] A. Ya. Khintchine, *Systems of regular linear equations and a general problem of Čebyšev* (Russian), Izv. Akad. Nauk SSSR (ser. mat.) 12 (1948), pp. 249–259.

[5] K. Mahler, *On lattice points in n-dimensional star bodies, I. Existence theorems*, Proc. Roy. Soc. Lond. A (187) (1946), pp. 151–187.

TRINITY COLLEGE
Cambridge, England

UNIVERSITY OF COLORADO
Boulder, Colorado

Reçu par la Rédaction le 7. 6. 1969

ACTA ARITHMETICA
XVI (1970)

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 $s \geqslant 0$ prime numbers, and let $\mathfrak{k}$ 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*

$$\max(|x|, |y|) < \exp\{2^{10^7(s+1)^4} P^{10^9(s+1)^3} |k/\mathfrak{k}|^{10^6(s+1)^2}\}.$$

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 $|k/\mathfrak{k}| = 1$, 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

$$\max(|x|, |y|) < \exp\{2^{10^7(s+1)^4} P^{10^9(s+1)^3}\}. \tag{1}$$

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^3-y^2.

Theorem 2. *If x, y are integers, with $(x, y) = 1$, then the greatest prime factor of x^3-y^2 exceeds*

$$10^{-3}(\log\log X)^{1/4},$$

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

In order to deduce Theorem 2 from (1), we let $\mathfrak{P}$ be either 1 or the greatest prime factor of x^3-y^2, according as $|x^3-y^2| = 1$ or $|x^3-y^2| > 1$, and we let $p_1, \ldots, p_s$ be the primes not exceeding $\mathfrak{P}$.

Noting that $s+1 \leqslant 2\mathfrak{P}$ and $P \leqslant 2\mathfrak{P}$, we conclude from (1) that

$$X = \max(|x|, |y|) < \exp\exp\{10^{12}\mathfrak{P}^4\},$$

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

$$|x^3-y^2| \prod_{j=1}^{s} |x^3-y^2|_{p_j} > 2^{-10(s+1)^2} P^{-10^3(s+1)} (\log X)^{10^{-6}(s+1)^{-2}},$$

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 $\bar{f}$ of f modulo p defines a non-singular cubic over the field 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

$$y^2 = 4x^3 - g_2 x - g_3, \tag{2}$$

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

$$\Delta = g_2^3 - 27g_3^2 \tag{3}$$

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 $3^3\Delta = (3g_2)^3 - (3^3 g_3)^2$, that

$$\max(|g_2|, |g_3|) < \exp\{2^{10^7(s+1)^4} P^{10^9(s+1)^3}\}.$$

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 [6] is based on the treatment of the equation $y^2 = x^3+k$ 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 $s \geqslant 0$ prime numbers. The purpose of this section is to generalize the classical reduction theory of binary cubic forms (2) (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 $Q(X, Y) = AX^2+BXY+CY^2$ 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 (3).

LEMMA 1. *By a substitution of the form* $X = rX'+qY'$, $Y = tX'+uY'$, *where* r, q, 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*

$$\max(|A'|_p, |B'|_p, |C'|_p) \leqslant p \quad \textit{for all } p \textit{ in } S.$$

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 r_p, t_p, with no common factor, such that

$$|Q(r_p, t_p)|_p = \max(|A|_p, |B|_p, |C|_p). \tag{4}$$

For, if Δ denotes the least common multiple of the denominators of A, B, C, then by assumption not all of $\Delta A, \Delta B, \Delta C$ are divisible by p. The assertion is obvious if ΔA and ΔC are both divisible by p (take

(2) The arguments of [1] are plainly valid for an arbitrary binary cubic form.

(3) 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.

$r_p = 1$, $t_p = 1$), and it is also obvious if either ΔA or ΔC is not divisible by p (take r_p and t_p to be 0 and 1 appropriately). By the Chinese remainder theorem, there exist integers r, t such that

$$|r-r_p|_p < 1, \quad |t-t_p|_p < 1 \quad \text{for all } p \text{ in } S. \tag{5}$$

It follows from (4) and (5) that

$$|Q(r,t)|_p = \max(|A|_p, |B|_p, |C|_p) \quad \text{for all } p \text{ in } S. \tag{6}$$

Since r_p and t_p have no common factor, the greatest common factor of r and t is not divisible by any prime in S, and so we can clearly suppose that this greatest common factor is 1. Hence there exist integers q, u such that $ru-qt = 1$. It is then plain from (6) that, by means of the substitution $X = rX'+qY'$, $Y = tX'+uY'$, we can ensure that

$$|A|_p = \max(|A|_p, |B|_p, |C|_p) \quad \text{for all } p \text{ in } S.$$

Now assume that 2 does not belong to S; it will be clear that a slightly simpler form of the subsequent argument is valid if this is not so. We assert that by means of a substitution $X = X'+\frac{1}{2}hY'$, $Y = Y'$, where h is an integer, we can ensure that [5]

$$|B|_p \leqslant 1/p \quad \text{for all } p \text{ in } S. \tag{7}$$

For, if Δ' denotes the least common multiple of the denominators of A and B, then, since $|A|_p \geqslant |B|_p$ for all p in S, there exist integers j, k such that $j\Delta' p_1 \ldots p_s - k\Delta' A = \Delta' B$; it is therefore plain that the above assertion is valid with $h = k$, since the substitution changes B into $hA+B$. But now, since $D = 4AC-B^2$ is an integer divisible by 4, we conclude from (7) that $|AC|_p \leqslant 1$ for all p in S. Thus, by a substitution $X = p_1^{j_1}\ldots p_s^{j_s}X'$, $Y = p_1^{-j_1}\ldots p_s^{-j_s}Y'$, we can arrange that

$$\max(|A|_p, |C|_p) \leqslant p \quad \text{for all } p \text{ in } S.$$

This inequality, together with (7), completes the proof of Lemma 1.

We next establish an analogue of Lemma 1 for binary cubic forms. Let $F(X, Y) = aX^3+3bX^2Y+3cXY^2+dY^3$ be a binary cubic form, whose coefficients a, b, c, d are S-integers, and whose discriminant [6]

$$D = 3b^2c^2 - a^2d^2 - 4ac^3 - 4b^3d + 6abcd \tag{8}$$

is a rational integer divisible by 4.

[5] Note that by taking powers of $p_1, \ldots, p_s$, we can in fact make $|B|_p$ arbitrarily small.

[6] Note that this definition of the discriminant differs from the usual one by a factor of 27.

Lemma 2. *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*

$$F'(X', Y') = a'X'^3+3b'X'^2Y'+3c'X'Y'^2+d'Y'^3$$

such that

$$\max(|a'|_p, |b'|_p, |c'|_p, |d'|_p) \leqslant p^5|D|_p^{-1/2} \quad \textit{for all } p \textit{ in } S \text{ [7]}.$$

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

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

It is readily verified that

$$A = b^2-ac, \quad B = bc-ad, \quad C = c^2-bd, \quad D = 4AC-B^2.$$

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

$$\max(|A|_p, |B|_p, |C|_p) \leqslant p \quad \text{for all } p \text{ in } S; \tag{9}$$

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

Let Δ be the least common multiple of the denominators of a, $3b$, $3c$, d. By omitting certain primes from S if necessary, we can suppose that, for each p in S, not all of Δa, $3\Delta b$, $3\Delta c$, Δd 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

$$\max(|A|_p, |B|_p, |C|_p) \leqslant p^3 \quad \text{for all } p \text{ in } S, \tag{10}$$

and

$$p^3|a|_p \geqslant \max(|a|_p, |b|_p, |c|_p, |d|_p), \quad |b|_p \leqslant p^{-\nu} \quad \text{for all } p \text{ in } S, \tag{11}$$

with ν 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

$$|F(r_p, t_p)|_p = \max(|a|_p, |3b|_p, |3c|_p, |d|_p). \tag{12}$$

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

[7] If $p \neq 2, 3$, this bound can be replaced by $p^2|D|_p^{-1/2}$.

of the previous two cases holds, so that Δa, Δd are divisible by p but $3\Delta b$, $3\Delta c$ are not, the assertion is still obvious (take $r_p = 1$ and choose t_p so that p does not divide t_p and $3\Delta b + t_p 3\Delta c$). 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 (9) 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 $X = rX' + qY'$, $Y = tX' + uY'$, where r, q, t, u are integers with $ru - qt = 1$, we can arrange that

$$(13)\qquad |a|_p = \max(|a|_p, |3b|_p, |3c|_p, |d|_p) \quad \text{for all } p \text{ in } S.$$

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 $X = X' + \frac{1}{3}hY'$, $Y = Y'$, where h is an integer, we can ensure that the second inequality in (11) holds. For, if Δ' denotes the least common multiple of the denominators of a and $3b$, then since $|a|_p \geqslant |3b|_p$ for all p in S, there exist integers j, k such that

$$j\Delta' p_1^{v+1} \ldots p_s^{v+1} - k\Delta' a = 3\Delta' b;$$

the assertion is then plainly valid with $h = k$, since the substitution changes $3b$ into $ha + 3b$. 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 $|ac|_p \leqslant p^3$, whence by (11)

$$(14)\qquad |c|_p \leqslant p^3 \quad \text{for all } p \text{ in } S.$$

This fact, together with the second inequality in (11), shows that $|bc|_p \leqslant p^3$, and so we conclude from the identity $B = bc - ad$ and (10), (11) that

$$(15)\qquad |d|_p \leqslant p^3 \quad \text{for all } p \text{ in } S.$$

In the remainder of the proof, we need only consider those primes in S for which

$$(16)\qquad \max(|c|_p, |d|_p) < p^{-1}|D|_p^{1/2},$$

since, for those primes in S not satisfying this inequality, we conclude from the identities $A = b^2 - ac$, $B = bc - ad$ and (10), (11) that $|a|_p \leqslant p^4 |D|_p^{-1/2}$, whence the assertion of Lemma 2 is valid for such primes. Further, we need only consider the primes in S satisfying

$$(17)\qquad |C|_p < p^{-3}|D|_p;$$

for the identity $Bb - Ac = Ca$ and (10), (11), (16) show that $|a|_p \leqslant p^5 |D|_p^{-1/2}$ for those primes not satisfying (17), and so the assertion of Lemma 2 holds for these 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

$$(18)\qquad |B|_p = |D|_p^{1/2}.$$

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

$$(19)\qquad |B|_p = |ad|_p.$$

Now let v be the product of powers of $p_1, \ldots, p_s$ such that

$$(20)\qquad p^{-1} \leqslant |d/v^3|_p \leqslant p$$

for all those primes p in S still being considered. Then, as $v^3 a = ad/(d/v^3)$, we conclude from (18), (19), (20) that

$$(21)\qquad p^{-1}|D|_p^{1/2} \leqslant |v^3 a|_p \leqslant p|D|_p^{1/2}.$$

Further, we have $c/v = v^2 ac/(av^3)$, and so it follows from (21) and the inequality $|ac|_p \leqslant p^3$ that

$$(22)\qquad |c/v|_p \leqslant p^4 |D|_p^{-1/2}.$$

But now the substitution $X = vX' + vY'$, $Y = v^{-1}Y'$ is of the required type, and transforms a, b, c, d into

$$v^3 a, \quad v^3 a + bv, \quad v^3 a + 2bv + c/v, \quad v^3 a + 3bv + 3c/v + d/v^3,$$

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 $F(X, Y) = aX^3 + 3bX^2Y + 3cXY^2 + dY^3$ 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 $ru - qt = \pm 1$, $F(X, Y)$ can be transformed into a cubic form*

$$F'(X', Y') = a'X'^3 + 3b'X'^2Y' + 3c'X'Y'^2 + d'Y'^3$$

with

$$\max(|a'|_p, |b'|_p, |c'|_p, |d'|_p) \leqslant p^5 |D|_p^{-1/2} \quad \textit{for all } p \textit{ in } S,$$

$$\max(|a'|, |b'|, |c'|, |d'|) \leqslant 3^{3/2}(p_1 \ldots p_s)^5 |D|.$$

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 Δ be the least common multiple of the denominators of a, b, c, d; evidently

$$(23) \qquad \Delta \leqslant \prod_{j=1}^{s} p_j^5 |D|_{p_j}^{-1/2} \leqslant (p_1 \ldots p_s)^5 |D|^{1/2}.$$

The cubic form $\Delta F(X, Y)$ has integer coefficients and discriminant $\Delta^4 D$. Hence (cf. [1], p. 196), by means of a substitution $X = rX'+qY'$, $Y = tX'+uY'$, where r, q, t, u are integers with $ru-qt = \pm 1$, $\Delta F(X, Y)$ can be transformed into a cubic form with the maximum of the absolute values of its coefficients at most $|3^3\Delta^4 D|^{1/2}$. Dividing this cubic form by Δ, 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 of $p_1, \ldots, p_s$, satisfying the equation $y^2 = x^3+k$. We first modify this equation. Recall that $\mathfrak{k}$ is the largest integer, comprised solely of powers of $p_1, \ldots, p_s$, which divides k. Suppose that $\mathfrak{k} = p_1^{6e_1+d_1} \ldots p_s^{6e_s+d_s}$, where d_i, e_i $(1 \leqslant i \leqslant s)$ are non-negative integers such that $0 \leqslant d_i < 6$. Thus, if we put

$$x' = x/(p_1^{2e_1} \ldots p_s^{2e_s}), \quad y' = y/(p_1^{3e_1} \ldots p_s^{3e_s}), \quad k' = k/(p_1^{6e_1} \ldots p_s^{6e_s}),$$

we have

$$(24) \qquad y'^2 = x'^3+k'.$$

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 § 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

$$F'(X', Y') = \alpha X'^3+\beta X'^2Y'+\gamma X'Y'^2+\delta Y'^3$$

with the property that, if Δ denotes the least common multiple of the denominators of $\alpha, \beta, \gamma, \delta$, then

$$(25) \qquad \Delta \leqslant P^{5s}|D|^{1/2}, \quad \max(|\Delta\alpha|, |\Delta\beta|, |\Delta\gamma|, |\Delta\delta|) \leqslant 3^{3/2}P^{10s}|D|^{3/2}.$$

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

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

$$(26) \qquad \Delta F'(uX-qY, -tX+rY) = \pm\Delta F(X, Y),$$

we obtain

$$(27) \qquad \Delta\alpha u^3-\Delta\beta u^2t+\Delta\gamma ut^2-\Delta\delta t^3 = \pm\Delta.$$

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

$$\nu \leqslant 31\cdot 10^2(s+1)^2, \quad \mathfrak{F}^2 \leqslant P^{20(s+1)}|D|^3, \quad \Delta \leqslant P^{5s}|D|^{1/2},$$

we conclude that

$$(28) \qquad \max(|u|, |t|) < M, \quad \max(|u|_{p_i}, |t|_{p_i}) < M \quad (1 \leqslant i \leqslant s),$$

where

$$M = \exp\{2^{10^7(s+1)^4}P^{10^8(s+1)^3}|D|^{10^6(s+1)^2}\}.$$

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

$$3r = 3\alpha u^2-2\beta ut+\gamma t^2, \quad 3q = -3\delta t^2-2\gamma ut+\beta u^2,$$

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

$$(29) \qquad \max(|r|, |q|) < M^3, \quad \max(|r|_{p_i}, |q|_{p_i}) < M^3 \quad (1 \leqslant i \leqslant s).$$

Further, equating the coefficients of XY^2 and Y^3 in (26), we have

$$\pm 3x' = 3(\delta tr^2-\alpha uq^2)+2qr(\beta u-\gamma t)+\beta tq^2-\gamma ur^2,$$
$$\pm 2y' = \alpha q^3-\beta rq^2+\gamma r^2q-\delta r^3.$$

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

$$\max(|x'|, |y'|) < M^{10}, \quad \max(|x'|_{p_i}, |y'|_{p_i}) < M^{10} \quad (1 \leqslant i \leqslant s).$$

But, as $x' = x/(p_1^{2e_1} \ldots p_s^{2e_s})$, $y' = y/(p_1^{3e_1} \ldots p_s^{3e_s})$, 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

$$\max(|x|, |y|) < M^{18(s+1)}.$$

Noting that $|D| = 4|k'| \leqslant P^{5(s+1)}|k/\mathfrak{k}|$, Theorem 1 follows immediately.

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 ([8]). In the next paragraph, we shall indicate the significant changes that must be made in the arguments of § V 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 $D = -4k'$ 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 § V of [5], we must therefore consider an equation of the form

$$(x'-a_1y')(x'-a_2y')(x'-a_3y') = m', \tag{30}$$

where a_1, a_2, a_3 are distinct, and the field $K = Q(a_1, a_2, a_3)$ has degree $n \leqslant 2$. Here x', y' are S-integers, and m' is an integer satisfying $|m'|_{p_i} \geqslant p_i^{-2}$ $(1 \leqslant i \leqslant s)$. As in § V of [5], we also use $S = \{| \ |_{\mathfrak{P}_1}, \ldots, | \ |_{\mathfrak{P}_\varrho}\}$ to denote the set of valuations of K extending the valuations $| \ |_{r_1}, \ldots, | \ |_{r_\sigma}$ of Q, and we let $\eta_1, \ldots, \eta_{\varrho-1}$ denote S-units of K satisfying (39) of [5]. Further, we signify by $\xi_i^{(j)}$ $(1 \leqslant j \leqslant n)$ the field conjugates of an element ξ of K in Ω_{r_i}, and by $N\xi$ the field norm of ξ. Put

$$\beta_l = x'-a_ly', \quad m_l' = N\beta_l, \quad \varphi_l = \Big\{\prod_{i=1}^{\sigma} |m'|_{r_i}\Big\}^{1/(n\sigma)}.$$

We deduce, as in § V of [5], that there exist integers $b_{l1}, \ldots, b_{l,\varrho-1}$ such that $\gamma_l = \beta_l\eta_1^{b_{l1}}\ldots\eta_{\varrho-1}^{b_{l\varrho-1}}$ satisfies

$$|\log(\varphi_l^{-1}|\gamma_l|_{\mathfrak{P}_i})| \leqslant C_3 \quad (1 \leqslant i \leqslant \varrho).$$

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

$$\log(\varphi_q^{-1}|\beta_{qi}^{(j)}|_{r_i}) \leqslant -(C_5H_q - C_3)/(n\sigma-1).$$

It follows from (30) that

$$|\beta_{li}^{(j)}|_{r_i} \geqslant C_6\varphi_q^{-1/2},$$

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

$$(a_{li}^{(j)}-a_{qi}^{(j)})\beta_{hi}^{(j)} - (a_{hi}^{(j)}-a_{qi}^{(j)})\beta_{li}^{(j)} = (a_{li}^{(j)}-a_{hi}^{(j)})\beta_{qi}^{(j)},$$

[8] More generally, this work can be modified so as to be valid for any binary form with at least three distinct linear factors, cf. [3].

we obtain

$$\eta_{1i}^{(j)b_1}\ldots\eta_{\varrho-1,i}^{(j)b_{\varrho-1}} - a = \omega,$$

where

$$b_k = b_{lk} - b_{hk}, \quad a = \frac{(a_{hi}^{(j)}-a_{qi}^{(j)})\gamma_{li}^{(j)}}{(a_{li}^{(j)}-a_{qi}^{(j)})\gamma_{hi}^{(j)}}, \quad \omega = \frac{(a_{li}^{(j)}-a_{hi}^{(j)})\beta_{qi}^{(j)}\gamma_{li}^{(j)}}{(a_{li}^{(j)}-a_{qi}^{(j)})\beta_{li}^{(j)}\gamma_{hi}^{(j)}}.$$

Since now $|b_k| \leqslant 2H_q$, 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

[1] A. Baker, *Contributions to the theory of Diophantine equations II. The Diophantine equation $y^2 = x^3+k$*, Phil. Trans. Royal Soc. London, Series A, 263 (1968), pp. 193–208.

[2] — *Linear forms in the logarithms of algebraic numbers (IV)*, Mathematika 15 (1968), pp. 204–216.

[3] — and J. Coates, *Integer points on curves of genus 1*, to appear in Proc. Camb. Phil. Soc.

[4] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), pp. 193–291.

[5] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), pp. 279–305.

[6] — *An effective p-adic analogue of a theorem of Thue II. The greatest prime factor of a binary form*, Acta Arith., this volume, pp. 399–412.

[7] K. Mahler, *Ueber die rationalen Punkte auf Kurven von Geschlecht 1*, J. reine angew. Math. 170 (1933), pp. 168–178.

[8] A. Ogg, *Abelian curves of small conductor*, J. reine angew. Math. 226 (1967), pp. 204–215.

[9] A. Weil, *Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. 168 (1967), pp. 149–156.

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
Cambridge, England

Reçu par la Rédaction le 25. 6. 1969

ACTA ARITHMETICA
XVI (1970)

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 $Q(\zeta)$, wher- $\zeta = e^{2\pi i/p}$, $p > 3$; also let h_1, h_2 denote the first and second factors, rese pectively, of the class number. It is proved in [1] that

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

where

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

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 ζ^g. Consequently the left members of (2.13), 2.14) and the formula at the top of p. 31 should all be multiplied by ζ^g. It follows that

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

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_2 should be replaced by h.

References

[1] L. Carlitz, *A congruence for the second factor of the class number of a cyclotomic field*, Acta Arith. 14 (1968), pp. 27–34.

[2] T. Metsänkylä, *Congruences modulo 2 for class number factors in cyclotomic fields*, Annales Academiae Scientarium Fennicae Series A, I. Mathematica 453 (1969), pp. 1–11.