ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

SEQUENCES OF FIELDS WITH MANY SOLUTIONS TO THE UNIT EQUATION

DAVID GRANT

Dedicated to Wolfgang Schmidt on the occasion of his 60th birthday

Let K be a number field of degree δ over the rationals $\mathbf{Q}$ and S a finite set of places of K containing the archimedean places M_∞. Let U_S denote the group of S-units of K and U the group of units. Let $s = \#S$. Then, for $\alpha, \beta \in K^\times$, the (two variable) S-unit equation is

$$(1) \qquad \alpha x + \beta y = 1, \qquad x, y \in U_S.$$

In its simplest form, $\alpha = \beta = 1$ and $S = M_\infty$; we call the resulting equation

$$(2) \qquad x + y = 1, \qquad x, y \in U,$$

the "unit equation." For a general reference to S-unit equations, see [**4**]. Evertse has shown that the number of solutions to (1) is at most $3 \times 7^{\delta+2s}$ [**3**]. The dependence of the bound on s is interesting. An equivalence relation on S-unit equations is given in [**5**], and it is shown there that for fixed K and S, there are only finitely-many equivalence classes of S-unit equations with more than two solutions. Yet, it is shown in [**6**] that with $K = \mathbf{Q}$, $\alpha = \beta = 1$, (1) can have more than $\exp(Cs^{1/2}/\log(s))$ solutions, for some constant $C > 0$. (A conjecture for the correct dependence on s of the number of solutions to (1) with $K = \mathbf{Q}$ and $\alpha = \beta = 1$ is also given in [**6**].)

On the other hand, it is unknown how the number of solutions to (2) should depend on δ. Nagell has shown that, for any $\delta \geq 5$, there are infinitely many number fields K of degree δ over $\mathbf{Q}$ with at least $6(2\delta-3)$ solutions to (2) [**8**]. (This bound is twice what Nagell stated, but Nagell did not distinguish between the solutions $(\varepsilon_1, \varepsilon_2)$ and $(\varepsilon_2, \varepsilon_1)$ to (2).) There is considerable room between Evertse's and Nagell's bounds; the purpose of this paper is to produce sequences of number fields where

Received by the editors on June 13, 1995, and in revised form on February 29, 1996.
Partially supported by NSF grant DMS-9303220.

the number of solutions to (2) grows quadratically in δ. Our examples come from cyclotomic and elliptic units, and we use mainly only well-known facts about these units. The first example of such a sequence of fields comes from:

Theorem 1. *Let p be an odd prime and ζ a primitive pth root of* 1. *Let $K = \mathbf{Q}(\zeta)$ and $\delta_p = [\mathbf{Q}(\zeta) : \mathbf{Q}] = p-1$. If m_p is the number of solutions to* (2) *in K, then*

$$m_p \geq \delta_p^2/2.$$

Proof. The proof follows easily from classical facts about cyclotomic units (see [**11**]). Let $1 \leq i,\ g \leq p-1$ with $i \neq g$. Note that $v_{ig} = (1-\zeta^i)/(\zeta^g - \zeta^i)$ is a cyclotomic unit, so

$$\frac{1-\zeta^i}{\zeta^g-\zeta^i} + \frac{1-\zeta^g}{\zeta^i-\zeta^g} = 1$$

gives the solution (v_{ig}, v_{gi}) to (2). Now let $1 \leq k,\ l \leq p-1$, with $k \neq l$. We want to show that $v_{ig} = v_{kl}$ if and only if $(i,g) = (k,l)$.

Let $\lambda = 1-\zeta$, which generates the lone prime in $\mathbf{Z}[\zeta]$ above p. Let $\mathbf{Z}[\zeta]_\lambda$ denote the completion of $\mathbf{Z}[\zeta]$ at λ. We can compute the first two terms in the λ-adic expansion of v_{ig} by

$$\begin{aligned} v_{ig} &= \frac{(1-\zeta^i)/(1-\zeta)}{(1-\zeta^i)/(1-\zeta) - (1-\zeta^g)/(1-\zeta)} \\ &= \frac{\sum_{m=0}^{i-1}\zeta^m}{\sum_{m=g}^{i-1}\zeta^m} \quad \text{or} \quad \frac{\sum_{m=0}^{i-1}\zeta^m}{-\sum_{m=i}^{g-1}\zeta^m}, \end{aligned}$$

depending on whether $i > g$ or $i < g$. So

$$v_{ig} = \frac{\sum_{m=0}^{i-1}(1-\lambda)^m}{\sum_{m=g}^{i-1}(1-\lambda)^m} \quad \text{or} \quad \frac{\sum_{m=0}^{i-1}(1-\lambda)^m}{-\sum_{m=i}^{g-1}(1-\lambda)^m}.$$

In either case,

$$\begin{aligned} v_{ig} &= \frac{i - i(i-1)\lambda/2 + O(\lambda^2)}{i-g-(i(i-1)/2 - g(g-1)/2)\lambda + O(\lambda^2)} \\ &= \frac{i(1-(i-1)\lambda/2) + O(\lambda^2)}{(i-g)(1-(i+g-1)\lambda/2) + O(\lambda^2)} \\ &= \left(\frac{i}{i-g}\right)(1+g\lambda/2) + O(\lambda^2), \end{aligned}$$

where $O(\lambda^2)$ denotes an element in $\lambda^2\mathbf{Z}[\zeta]_\lambda$.

Suppose that $v_{ig} = v_{kl}$. Then

$$\left(\frac{i}{i-g}\right)\left(1+\frac{g}{2}\lambda\right) \equiv \left(\frac{k}{k-l}\right)\left(1+\frac{l}{2}\lambda\right) \bmod \lambda^2.$$

So if we let a bar denote reduction mod$p$, then $\bar{i}/(\bar{i}-\bar{g}) = \bar{k}/(\bar{k}-\bar{l})$, and since $(p)\mathbf{Z}[\zeta] = (\lambda)^{p-1}$, $p-1 \geq 2$, we also have that $\bar{g}/2 = \bar{l}/2$. Therefore, $\bar{g} = \bar{l}$ and hence $\bar{i} = \bar{k}$. So $(i,g) = (k,l)$.

Therefore the solutions (v_{ig}, v_{gi}) to (2) are distinct, and we can conclude that the number of solutions m_p to (2) in K is at least

$$(p-1)(p-2) = \delta_p(\delta_p - 1) \geq \delta_p^2/2. \qquad \square$$

We can get a similar result for towers of fields generated by torsion points on elliptic curves with complex multiplication. We refer the reader to [**9**] and [**10**] for the following facts about elliptic curves and the theory of complex multiplication of elliptic curves. Let K be any field. Recall that an elliptic curve E over K can always be defined by a Weierstrass model

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K. \tag{3}$$

The discriminant of the model is nonzero and is given by

$$\Delta(C) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

The j-invariant j and invariant differential ω of E are given by

$$j = \frac{(b_2^2 - 24b_4)^3}{\Delta(C)}, \qquad \omega = \frac{dx}{2y + a_1x + a_3}.$$

Fixing the point at infinity, the choice of Weierstrass model over K is unique up to transformations of the form

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t, \qquad r, s, t \in K,\ u \in K^\times. \tag{4}$$

If C' is the resulting Weierstrass model relating x' and y', then

$$\Delta(C') = u^{-12}\Delta(C). \tag{5}$$

Over a field of characteristic not 2 or 3, E has a model of the form

$$y^2 = x^3 + ax + b, \qquad a, b \in K,$$

and the j-invariant of E is zero if and only if $a = 0$. Now let K be a number field and O_K its ring of integers. Let $\mathfrak{p}$ be a prime of O_K, $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$, and $R_\mathfrak{p}$ the integers of $K_\mathfrak{p}$. We will let $\mathfrak{p}$ also denote the maximal ideal of $R_\mathfrak{p}$. We say that a model C of E over $K_\mathfrak{p}$ with coefficients in $R_\mathfrak{p}$ is a model defined over $R_\mathfrak{p}$, and that it has good reduction if the reduced equation mod$\mathfrak{p}$ defines an elliptic curve over $R_\mathfrak{p}/\mathfrak{p}$. This happens if and only if $\Delta(C)$ is a unit in $R_\mathfrak{p}$. We say that E has good reduction at $\mathfrak{p}$ if it has a model over $R_\mathfrak{p}$ which has good reduction. If such a model exists it can always be obtained from a given Weierstrass model via a transformation as in (4). We say that E has potential good reduction at $\mathfrak{p}$ if there is a finite extension field N of $K_\mathfrak{p}$, whose maximal ideal of its ring of integers we denote by $\mathfrak{P}$, such that E obtains good reduction at $\mathfrak{P}$ over N. Any elliptic curve over a number field K has only finitely many primes at which it does not have good reduction.

Let K be an imaginary quadratic field, O_K its ring of integers and h its class number. We will let $\mathfrak{a}^\rho$ denote the complex conjugate of an ideal $\mathfrak{a}$ of O_K. Let H be the Hilbert class field of K, so $[H : K] = h$. Then there exists an elliptic curve E defined over H with complex multiplication by O_K, i.e., there exists an injection

$$i : O_K \to \mathrm{End}\,(E). \tag{6}$$

(Indeed, there are h many isomorphism classes of such E over an algebraic closure of $\mathbf{Q}$.) We write $[\alpha] = i(\alpha)$. We can (and will) always assume the injection is normalized by $[\alpha]^*\omega = \alpha\omega$ for all $\alpha \in O_K$, where $[\alpha]^*\omega$ denotes the pullback of ω under the action of $[\alpha]$. The complex multiplication forces E to have everywhere potentially good reduction, which occurs precisely when the j-invariant of E is an algebraic integer. Let O denote the origin on E. Let $\mathfrak{p}$ be a prime ideal of O_K. Then we let $E[\mathfrak{p}]$ denote the elements $x \in E$ such that $[\alpha]x = O$ for all $\alpha \in \mathfrak{p}$. We let $E[\mathfrak{p}]'$ denote $E[\mathfrak{p}] - O$. We let $H(E[\mathfrak{p}])$ be the field generated over H by the x– and y–coordinates of all the points of $E[\mathfrak{p}]$.

We will let $M = H(x(E[\mathfrak{p}]))$ denote the field generated over H by all the x-coordinates of points in $E[\mathfrak{p}]$ (which is the field generated over H by all even functions of points in $E[\mathfrak{p}]$). A major result of the theory of complex multiplication is that M is the ray class field over K of modulus $\mathfrak{p}$, so long as K is not $\mathbf{Q}(\sqrt{-3})$ (in which case $j = 0$), or $\mathbf{Q}(\sqrt{-1})$ (in which case $j = 1728$) [**10**, p. 135].

Theorem 2. *Let $K \neq \mathbf{Q}(\sqrt{-3})$ be an imaginary quadratic field of class number h, and let O_K be its ring of integers. Let H be the Hilbert class field of K and E an elliptic curve defined over H with complex multiplication by O_K, so then the j-invariant j of E is a nonzero algebraic integer. Let $\mathfrak{p}$ be a prime ideal of O_K, prime to j, with $N\mathfrak{p} > 12$ (hence $\mathfrak{p}$ is prime to 6), such that E has good reduction at all primes of H above $\mathfrak{p}$. Then if $M = H(x(E[\mathfrak{p}]))$ and $m_{\mathfrak{p}}$ is the number of solutions to (2) in M, then $\delta_{\mathfrak{p}} = [M : \mathbf{Q}] = h(N\mathfrak{p} - 1)$, and*

$$m_{\mathfrak{p}} \geq \frac{1}{2^4 h^2}\delta_{\mathfrak{p}}^2,$$

where $N\mathfrak{p}$ denotes the norm of $\mathfrak{p}$ from K to $\mathbf{Q}$.

Note that all but finitely many primes $\mathfrak{p}$ of O_K satisfy the conditions of the theorem. For the proof we will use the following lemma.

Lemma. *Let $K, \mathfrak{p}, H, E$ and M be as in the statement of Theorem 2. Let E be given by a model (3) over H and $u \in E[\mathfrak{p}]'$. Let $\mathcal{C} \subset O_K$ denote a fixed reduced residue system* $\bmod \mathfrak{p}$. *Then for any $i, g, k \in \mathcal{C}$, with $g \neq \pm i \bmod \mathfrak{p}$ and $k \neq \pm i \bmod \mathfrak{p}$,*

$$w_{igk} = \frac{x([k]u) - x([i]u)}{x([g]u) - x([i]u)} \tag{7}$$

is a unit in the ring of integers of M.

Proof of Lemma. We give two proofs. The first follows easily from the work of Kubert and Lang. First note that w_{igk} is independent of transformations (4) of a model as in (3). In particular, we can take E to be defined by the model

$$y^2 = x^3 - (g_2/4)x - (g_3/4), \qquad g_2, g_3 \in H.$$

To this model we can standardly assign a complex period τ, so that the complex points (x, y) of E are parameterized by $(\wp(z,\tau), (1/2)\wp'(z,\tau))$ for $z \in \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$, where $\wp$ is the Weierstrass $\wp$-function. Now let T be a variable in the upper-half complex plane and $L = \mathbf{Z} + \mathbf{Z}T$. Let p be the rational prime below $\mathfrak{p}$. Kubert and Lang [**7**, Chapter 2, Section 6] have shown that if r, s, t are in $(1/p)L/L$ but not in L, and if $r \neq \pm s$, $r \neq \pm t \bmod L$, then

$$\frac{\wp(t,T) - \wp(r,T)}{\wp(s,T) - \wp(r,T)}$$

is a unit in the integral closure of $\mathbf{Z}[J(T)]$ in the field of modular function of level p, where $J(T)$ is 1728 times Klein's modular J-function (see [**1**]). Specializing T to τ, J becomes the j invariant of E, which is an algebraic integer; therefore, taking $t = [k]u$, $s = [g]u$, and $r = [i]u$, we get that w_{igk} is a unit.

For what follows, it makes sense to give a second proof, which is a modification of an argument given by de Shalit [**2**, pp. 53–54]. Note that, by (5), the expression

$$\varepsilon_{ki} = \frac{(x([k]u) - x([i]u))^6}{\Delta(C)}$$

is independent of transformations (4) of models as in (3). Let q be any prime of M not over $\mathfrak{p}$ and M_q the localization of M at q. Since E has potentially good reduction at q, we can find a finite extension N of M_q over which E has a transformed Weierstrass model C' (with coordinates x' and y') with good reduction at the maximal ideal Q of the ring of integers of N. Hence $\Delta(C')$ is unit at Q. Furthermore, $x'([k]u)$ and $x'([i]u)$ are integral at Q, and noncongruent $\bmod Q$, since the $\mathfrak{p}$-torsion injects when reduced $\bmod Q$, and $k \neq \pm i \bmod \mathfrak{p}$. Note that the $\mathfrak{p}$-torsion injects if Q does not lie over $\mathfrak{p}^\rho$ because then the characteristic of the residue field at Q is prime to p, and if Q lies over $\mathfrak{p}^\rho$ and $\mathfrak{p}^\rho \neq \mathfrak{p}$, then the $\mathfrak{p}$-torsion injects anyway since the reduction of E at any prime over $\mathfrak{p}^\rho$ is ordinary (the normalization of (6) shows that if $\alpha \in O_K$ is prime to $\mathfrak{p}$, then $[\alpha]$ is étale). Hence

$$\frac{(x'([k]u) - x'([i]u))^6}{\Delta(C')} = \varepsilon_{ki}$$

is a unit at Q. We conclude that w_{igk}, being a sixth root of $\varepsilon_{ki}/\varepsilon_{gi}$, is a unit at all primes q not lying over $\mathfrak{p}$.

Now let $\mathcal{P}$ be any prime of $H(E[\mathfrak{p}])$ above $\mathfrak{p}$ and $\mathfrak{P}$ its restriction to H. Let $R_{\mathfrak{P}}$ and $R_{\mathcal{P}}$ be the rings of integers in the completions $H_{\mathfrak{P}}$ and $H(E[\mathfrak{p}])_{\mathcal{P}}$ of H at $\mathfrak{P}$ and $H(E[\mathfrak{p}])$ at $\mathcal{P}$, respectively. By abuse of notation, we denote their maximal ideals by $\mathfrak{P}$ and $\mathcal{P}$, respectively.

Since E has good reduction at $\mathfrak{P}$, and the residue characteristic of $\mathfrak{P}$ is not 2 or 3, there is a model for E of the form

$$y^2 = x^3 + ax + b, \qquad a, b \in R_{\mathfrak{P}}, \tag{8}$$

which has good reduction at $\mathfrak{P}$. Since we took $K \neq \mathbf{Q}(\sqrt{-3})$, we have $a \neq 0$ in $R_{\mathfrak{P}}$, but since we also took $\mathfrak{p}$ prime to j, a is not 0 mod $\mathfrak{P}$ as well.

Note that, by our normalization of (6), $E[\mathfrak{p}]$ is contained in E_1, the $H(E[\mathfrak{p}])_{\mathcal{P}}$-points of E which reduce to the origin mod$\mathcal{P}$. The points in E_1 can be parameterized by the points in a formal group. Using the model (8) for E, $t = -x/y$ is a local parameter at the origin, and we have expansions

$$x = \frac{1}{t^2} - at^2 + (d^o \geq 4), \qquad y = -\frac{1}{t^3} + at + (d^o \geq 3), \tag{9}$$

where $(d^o \geq n)$ denotes a formal power series with coefficients in $R_{\mathfrak{P}}$, all of whose terms have total degree at least n. If v_1 and v_2 are independent generic points of E and v_3 is the sum of v_1 and v_2 under the group morphism of E, then setting $t_i = t(v_i)$, we have

$$t_3 = \mathcal{F}(t_1, t_2),$$

where $\mathcal{F}$ is a formal power series in two variables with coefficients in $R_{\mathfrak{P}}$. Now $\mathcal{F}$ defines a formal group over $R_{\mathfrak{P}}$, and the map $u \to t(u)$ defines an isomorphism

$$E_1 \cong \mathcal{F}(\mathcal{P}), \tag{10}$$

from the $H(E[\mathfrak{p}])_{\mathcal{P}}$-points of E in the kernel of reduction $\bmod \mathcal{P}$ to the points of $\mathcal{F}$ which lie in $\mathcal{P}$.

Let $\alpha \in O_K$. From our normalization of (6), we have

$$[\alpha]t = \alpha t + (d^o \geq 2), \tag{11}$$

where $[\alpha]t$ denotes the pullback of t under the action of $[\alpha]$. Note that $[\alpha]t$ has coefficients in $R_{\mathfrak{P}}$ since (8) has good reduction at $\mathfrak{P}$. So if π is a uniformizer for $\mathfrak{p}$ in O_K, then $E[\mathfrak{p}]$ corresponds via (10) to the zeros of $[\pi]t$. By the $\mathfrak{P}$-adic Weierstrass preparation theorem [**11**, p. 115], we can write

$$[\pi]t = \Pi^n f(t)u(t),$$

where u is a unit power series over $R_{\mathfrak{P}}$, Π is a uniformizer in $R_{\mathfrak{P}}$ for $\mathfrak{P}$, $n \geq 0$, and $f \in R_{\mathfrak{P}}[t]$ is a distinguished polynomial, i.e., $f \equiv t^d \bmod \mathfrak{P}$, where d is the degree of f. Since our model for E has good reduction at $\mathfrak{P}$, $[\pi]$ has finite height $\bmod \mathfrak{P}$ so $n = 0$. Hence $E[\mathfrak{p}]$ corresponds to the zeros of f, and we have $d = \#E[\mathfrak{p}] = N\mathfrak{p}$. Since $\operatorname{ord}_{\mathfrak{p}}\pi = 1$ and $\mathfrak{p}$ is unramified in H, $f(t)/t$ is an Eisenstein polynomial over $R_{\mathfrak{P}}$. Therefore, if $u \in E[\mathfrak{p}]'$, $t(u)$ is a uniformizer for $\mathcal{P}$ in $R_{\mathcal{P}}$. By (11), for $\alpha \in (O_K/\mathfrak{p}O_K)^{\times}$,

$$\frac{t([\alpha]u)}{t(u)} \equiv \alpha \bmod \mathcal{P}.$$

Hence, by (7), the lead term in the $t(u)$-adic expansion of w_{igk} is

$$\frac{1/(k^2 t(u)^2) - 1/(i^2 t(u)^2)}{1/(g^2 t(u)^2) - 1/(i^2 t(u)^2)} = \frac{(i^2 - k^2)g^2}{(i^2 - g^2)k^2}.$$

So w_{igk} is a unit at $\mathcal{P}$ as well, so is a unit in $H(E[\mathfrak{p}])$, and hence in M. $\square$

Proof of Theorem. We will maintain the notation as in the proof of the lemma. First of all, since $f(t)/t$ has degree $N\mathfrak{p} - 1$, and is irreducible by Eisenstein's criterion, we have $[H(E[\mathfrak{p}]) : H] \geq N\mathfrak{p} - 1$. On the other hand, if G is the Galois group of $H(E[\mathfrak{p}])/H$, then we have an injection $G \to (O_K/\mathfrak{p}O_K)^\times$, given by $\sigma \to \alpha$ if $\sigma(u) = [\alpha]u$ for any $u \in E[\mathfrak{p}]'$. Hence $[H(E[\mathfrak{p}]) : H] = N\mathfrak{p} - 1$, and $H(E[\mathfrak{p}])/H$ is totally ramified at any prime over $\mathfrak{p}$. Since M is the fixed subfield of $\langle -1 \rangle \subseteq G$, $[M : H] = (1/2)(N\mathfrak{p} - 1)$, and so $\delta_\mathfrak{p} = h(N\mathfrak{p} - 1)$, and M/H is totally ramified at any prime over $\mathfrak{p}$ (which all also follows from class field theory if $j \neq 1728$).

Fix $u \in E[\mathfrak{p}]'$. Let $i, g \in \mathcal{C}$ with $i, g \not\equiv \pm 1 \bmod \mathfrak{p}$ and $g \not\equiv \pm i \bmod \mathfrak{p}$. Then from the lemma, we have that

$$w_{ig} = \frac{x(u) - x([i]u)}{x([g]u) - x([i]u)}, \qquad w_{gi} = \frac{x(u) - x([g]u)}{x([i]u) - x([g]u)}$$

are units in M, so

$$w_{ig} + w_{gi} = 1$$

gives the solution (w_{ig}, w_{gi}) to (2). (For other diophantine applications of this solution to the unit equation, see [**7**, Chapter 8]). We will show that, for $k, l \in \mathcal{C}$, $k, l \not\equiv \pm 1 \bmod \mathfrak{p}$, $l \not\equiv \pm k \bmod \mathfrak{p}$, then if $w_{ig} = w_{kl}$, then either $(k^2, l^2) \equiv (i^2, g^2) \bmod \mathfrak{p}$ or $(k^2, l^2) \equiv (1 - g^2, 1 - i^2) \bmod \mathfrak{p}$. As in the proof of Theorem 1, we want to compute the first two nontrivial terms in the $\mathcal{P}$-adic expansion of w_{ig} using $t(u)$ as a uniformizer.

Let E be defined by a model as in (8). Continuing the computation of $\mathcal{F}$ as in [**9**, p. 114], we get

$$\mathcal{F}(t_1, t_2) = t_1 + t_2 - 2at_1t_2(t_1 + t_2)(t_1^2 + t_1t_2 + t_2^2) + (d^o \geq 7). \tag{12}$$

A simple induction using (12) shows that, for all $n \in \mathbf{Z}$,

$$[n]t = nt - 2a\left(\frac{n^5 - n}{5}\right)t^5 + (d^o \geq 7). \tag{13}$$

It is an easy, if somewhat painful, exercise to show that (13) holds for all $n \in O_K$. (One notes that the n for which (13) holds form a ring containing $\mathbf{Z}$, so one needs only to verify that (13) holds for $n = \eta = \sqrt{d}$ or $n = \eta = (1 + \sqrt{d})/2$, whichever η generates O_K over $\mathbf{Z}$ for some $d \in \mathbf{Z}$. To show that η satisfies (13), we first show that $\sqrt{d}$

satisfies (13) using $[\sqrt{d}][\sqrt{d}] = [d]$. Then (13) also holds for $1+\sqrt{d}$ and 2, so one deduces that if $\eta = (1+\sqrt{d})/2$, then (13) holds for η by using $[2][\eta] = [1+\sqrt{d}]$.)

The first two nontrivial terms of the $t(u)$-adic expansion of w_{ig} can be read off from

$$\begin{aligned}&\frac{(1/t(u)^2 - at(u)^2) - (1/t([i]u)^2 - at([i]u)^2) + O(t(u)^4)}{(1/t([g]u)^2 - at([g]u)^2) - (1/t([i]u)^2 - at([i]u)^2) + O(t(u)^4)},\\ &\qquad = \frac{(i^2-1)g^2}{i^2-g^2}\left(1 + \frac{a}{5}i^2(1-g^2)t(u)^4 + O(t(u)^6)\right),\end{aligned}$$

which follows from (9), (13), and a Mathematica calculation. Here $O(t(u))^n$ denotes an element of $t(u)^n\mathbf{R}_{\mathcal{P}}$. Let a bar denote reduction mod $\mathfrak{p}$. Let $\alpha = i^2$ and $\beta = g^2$, so if $w_{ig} = w_{kl}$, with $\gamma = k^2$ and $\delta = l^2$, then we get

$$(\bar{\alpha}-1)\bar{\beta}/(\bar{\alpha}-\bar{\beta}) = (\bar{\gamma}-1)\bar{\delta}/(\bar{\gamma}-\bar{\delta}).$$

Now since a is not $0 \bmod \mathfrak{P}$, and since $H(E[\mathfrak{p}])/H$ is totally ramified over $\mathfrak{P}$, we have $\operatorname{ord}_{\mathcal{P}}\mathfrak{p} = N\mathfrak{p} - 1 > 4$, so we also get

$$\bar{\alpha}(1-\bar{\beta}) = \bar{\gamma}(1-\bar{\delta}).$$

Solving, we get $(\bar{\gamma}, \bar{\delta}) = (\bar{\alpha}, \bar{\beta})$ or $(\bar{\gamma}, \bar{\delta}) = (1-\bar{\beta}, 1-\bar{\alpha})$, so we get $(k^2, l^2) \equiv (i^2, g^2) \bmod \mathfrak{p}$ or $(k^2, l^2) \equiv (1-g^2, 1-i^2) \bmod \mathfrak{p}$. Hence there are at most eight pairs (k, l) so that $w_{ig} = w_{kl}$. Hence the number of solutions $m_{\mathfrak{p}}$ of (2) in M is at least

$$\begin{aligned}\frac{1}{8}(\#\mathcal{C}-2)(\#\mathcal{C}-4) &= \frac{1}{8}(N\mathfrak{p}-3)(N\mathfrak{p}-5)\\ &> \frac{1}{16}(N\mathfrak{p}-1)^2\end{aligned}$$

since $N\mathfrak{p} > 12$. Since $\delta_{\mathfrak{p}} = h(N\mathfrak{p}-1)$, we have

$$m_{\mathfrak{p}} > \frac{1}{2^4h^2}\delta_{\mathfrak{p}}^2. \qquad \square$$

Remarks. 1) The conditions $K \neq \mathbf{Q}(\sqrt{-3})$ and $\mathfrak{p}$ prime to j can presumedly be dropped. Without these conditions the degree 7 terms in the expansion of $\mathcal{F}$ would have to be investigated.

2) I do not know if $w_{ig} = w_{kl}$ ever occurs without $(k,l) \equiv (\pm i, \pm g) \bmod \mathfrak{p}$. The extra possibility $(\gamma, \delta) \equiv (1-\beta, \alpha) \bmod \mathfrak{p}$ may just be an artifact of the proof. Certainly, if $i^2 + g^2 \equiv 1 \bmod \mathfrak{p}$, the eight possibilities coalesce into four.

Corollary. *Let $\varepsilon > 0$, and $c(\varepsilon) > 0$ be an arbitrary constant. Then there are infinitely many imaginary quadratic fields K_i, each with infinitely many extensions M_{ig}, such that if m_{ig} is the number of solutions to* (2) *in M_{ig} and $\delta_{ig} = [M_{ig} : \mathbf{Q}]$, then*

$$m_{ig} > c(\varepsilon)\delta_{ig}^{2-\varepsilon}.$$

These M_{ig} can be chosen to be distinct.

Proof. Let $K_i \neq \mathbf{Q}(\sqrt{-3}), \mathbf{Q}(\sqrt{-1})$ for $i \in \mathbf{N}$ be some ordering of the (all but two) imaginary quadratic number fields. Let O_{K_i} be the ring of integers of K_i, H_i the Hilbert class field of K_i, and h_i the class number of K_i. Let E_i be an elliptic curve defined over H_i with normalized complex multiplication by O_{K_i}. Let $\mathfrak{p}_{ig}$, $g \in \mathbf{N}$, be some ordering of the prime ideals of O_{K_i} which satisfy the conditions of Theorem 2, with the additional conditions that $\mathfrak{p}_{ig}$ not be ramified over $\mathbf{Q}$, and that $N\mathfrak{p}_{ig} - 1 > (c(\varepsilon)2^4 h_i^2)^{1/\varepsilon}/h_i$. These include all but finitely many primes of O_{K_i}. Then if $M_{ig} = H_i(x(E_i[\mathfrak{p}_{ig}]))$, Theorem 2 implies that

$$m_{ig} > \frac{1}{2^4 h_i^2}\delta_{ig}^{2-\varepsilon}(h_i(N\mathfrak{p}_{ig} - 1))^{\varepsilon} > c(\varepsilon)\delta_{ig}^{2-\varepsilon},$$

where m_{ig} is the number of solutions to (2) in M_{ig} and $\delta_{ig} = [M_{ig} : \mathbf{Q}]$.

For the last part of the corollary, we first note that $M_{ig} = M_{ik}$ implies that $g = k$, for if $\mathfrak{p}_{ig} \neq \mathfrak{p}_{ik}$, then $\mathfrak{p}_{ig}$ ramifies in M_{ig} but not in M_{ik}. Suppose now that $M_{ig} = M_{kl}$. Since M_{ig} is the ray class field over K_i of modulus $\mathfrak{p}_{ig}$, the only primes of H_i which ramify in M_{ig} are the primes above $\mathfrak{p}_{ig}$, which do so totally, so have a ramification index of $(1/2)(N\mathfrak{p}_{ig} - 1) > 2$ over H_i. Since H_i/K_i is unramified, the only primes in M_{ig} not above $\mathfrak{p}_{ig}$ which are ramified over $\mathbf{Q}$ have a ramification index of at most $[K_i : \mathbf{Q}] = 2$. Therefore, in M_{ig}, there is a distinguished set of primes with a ramification index over $\mathbf{Q}$ greater than 2 (namely the primes above $\mathfrak{p}_{ig}$), and we can recover H_i from M_{ig}

as the inertial subfield in the Galois closure of M_{ij} over $\mathbf{Q}$ of any of these primes, since $\mathfrak{p}_{ig}$ is unramified over $\mathbf{Q}$. And since H_i/K_i is unramified, the discriminant D_{H_i} of H_i over $\mathbf{Q}$ uniquely determines the absolute value of the discriminant D_{K_i} of K_i over $\mathbf{Q}$, via $D_{H_i} = D_{K_i}^{[H_i:\mathbf{Q}]/2}$. Since an imaginary quadratic field is uniquely determined by the absolute value of its discriminant, we can conclude that if $M_{ig} = M_{kl}$, then $k = i$ and we have already noted that this forces $l = g$. $\square$

Remarks. Since there are only finitely many imaginary quadratic fields of given class number, for a given δ, there are only finitely many of the M_{ig} with $[M_{ig} : \mathbf{Q}] \leq \delta$.

Acknowledgment. I would like to thank E.B. Burger for useful discussions on this material.

REFERENCES

1. T. Apostol, *Modular functions and Dirichlet series in number theory*, 2nd edition, Springer-Verlag, New York, 1990.

2. E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication,* Academic Press, Orlando, 1987.

3. J-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561–584.

4. J-H. Evertse, K. Györy, C.L. Stewart and R. Tidjeman, *S-unit equations and their applications*, in *New advances in transcendence theory*, Cambridge, 1988.

5. ———, *On S-unit equations in two unknowns*, Invent. Math. **92** (1988), 461–477.

6. P. Erdös, C.L. Stewart and R. Tidjeman, *Some diophantine equations with many solutions*, Comp. Math. **66** (1988), 37–56.

7. D.S. Kubert and S. Lang, *Modular units*, Springer Verlag, New York, 1981.

8. T. Nagell, *Quelques problèmes relatif aux unités algébriques*, Ark. Math. **8** (1969), 115–127.

9. J.H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, New York, 1986.

10. ———, *Advanced topics in the arithmetic of elliptic curves*, Springer Verlag, New York, 1994.

11. L. Washington, *Introduction to cyclotomic fields*, Springer Verlag, New York, 1982.

Department of Mathematics, Campus Box 395, University of Colorado at Boulder, Boulder, Colorado 80309-0395
E-mail address: grant@boulder.colorado.edu