Invent. math. 72, 323-334 (1983)

Inventiones mathematicae
© Springer-Verlag 1983

A Classical Diophantine Problem and Modular Forms of Weight 3/2

J.B. Tunnell

Department of Mathematics, Fine Hall, Box 37, Princeton University,
Princeton, NJ 08540, USA

to S. Chowla

Introduction

It is a classical Diophantine problem to determine which integers are the area of some right triangle with rational sides. The main result of this paper is the following.

Theorem. *Let formal power series in the variable* q *be given by* $g=q\prod_1^\infty(1-q^{8n})(1-q^{16n})$ *and, for each positive integer* t, $\theta_t=\sum_{-\infty}^{\infty} q^{tn^2}$. *Set* $g\,\theta_2=\sum_1^\infty a(n)\,q^n$ *and* $g\,\theta_4=\sum_1^\infty b(n)\,q^n$.

(a) *If* $a(n)\neq 0$, *then* n *is not the area of any right triangle with rational sides.*

(b) *If* $b(n)\neq 0$, *then* $2n$ *is not the area of any right triangle with rational sides.*

The power series $g\,\theta_2$ and $g\,\theta_4$ are the q-expansions of certain modular forms of weight 3/2. It would follow from some current conjectures in the theory of elliptic curves that the converses of statements (a) and (b) are true for squarefree positive integers n (see Sect. 3).

In this introduction we will briefly recall the history of the problem and the connections to elliptic curves, as well as giving a description of the methods of the paper.

Let $\mathscr{C}$ be the set of areas of right triangles with rational sides. This is a subset of $(\mathbf{Q}^*)^+$, and consideration of similar triangles shows that it is a union of cosets of $(\mathbf{Q}^*)^2$. Classically, an integer in $\mathscr{C}$ was called a congruent number, and Dickson [9, Chap. XVI] traces the question of whether a given number is congruent back to Arab manuscripts and the Greeks prior to that. The positive integers not in $\mathscr{C}$ are called noncongruent numbers, a terminology we will use unless confusion with ideal theoretic congruence might result.

Partially supported by a grant from the National Science Foundation

From the Pythagorean formula it is clear that the rational number D is the area of a rational right triangle with hypotenuse h if and only if $(h/2)^2 \pm D$ are both rational squares. Hence D is in $\mathscr{C}$ if and only if the simultaneous Diophantine system

$$\begin{aligned} u^2 + D v^2 &= w^2 \\ u^2 - D v^2 &= z^2 \end{aligned} \tag{1}$$

has a rational solution (u, v, w, z) with $v \neq 0$. Geometrically, the two quadrics in $\mathbf{P}^3$ given by (1) intersect in a smooth quartic in $\mathbf{P}^3$ which contains the point $(1, 0, 1, 1)$. The intersection is thus an elliptic curve over $\mathbf{Q}$ and projection from $(u, v, w, z) = (1, 0, 1, 1)$ to the plane $z = 0$ gives a birational isomorphism with a plane cubic curve E^D having Weierstrass form $y^2 = x^3 - D^2 x$. The points on the space curve with $v = 0$ correspond to the points where $y = 0$ and the point at infinity on E^D. It is easy to see by reducing modulo primes that these points on $E^D(\mathbf{Q})$ are precisely those of finite order. Thus we arrive at the well-known result that D is the area of a rational right triangle if and only if the group $E^D(\mathbf{Q})$ of rational points on $y^2 = x^3 - D^2 x$ is infinite.

In making explicit the relation of the elliptic curve E^D to rational right triangles, D. Zagier has pointed out to me that it is more convenient to use the natural system of quadrics

$$\begin{aligned} a^2 + b^2 &= c^2 \\ a b &= 2 D t^2 \end{aligned} \tag{1'}$$

in place of (1). This leads directly to a plane cubic when the first equation is parameterized by $(a, b, c) = (c(1 - \lambda^2)/(1 + \lambda^2), 2c\lambda/(1 + \lambda^2), c)$ and these values are used in the second quadric. This yields $D(t(1 + \lambda^2)/c)^2 = \lambda - \lambda^3$, which upon multiplication by D^3 and setting $x = -D\lambda$ and $y = D^2 t(1 + \lambda^2)/c$ gives $y^2 = x^3 - D^2 x$. A rational solution (x, y) of this equation with $y \neq 0$, corresponds to a right triangle with sides $|(D^2 - x^2)/y|$, $|2Dx/y|$, $|(D^2 + x^2)/y|$.

There are several known criteria for an integer D to be noncongruent, all of which seem to be equivalent to proving by means of a 2-descent on E^D that the group of rational points is finite. References [1, 9, 12, and 15] contain samples of these results. For example, 1 and primes congruent to 3 modulo 8 are not the area of any rational right triangle. The smallest integer in $\mathscr{C}$ is 5; it is the area of the right triangle with sides 9/6, 40/6, 41/6 discovered by Fibonacci, among others. Investigations have been undertaken by making a computer search for solutions to the original Diophantine system and tabulating the results [1, 2]. The most recent tabulations and references can be found in [26]. Numerical evidence from such calculations suggested to the authors of [1] that all positive integers congruent to 5, 6, or 7 modulo 8 should be congruent numbers. Stephens [21] observed that this would follow from a weak form of the conjecture of Birch and Swinnerton-Dyer and asserted that the method of Heegner points could be applied to prove that primes congruent to 5 or 7 modulo 8 or twice primes congruent to 3 modulo 8 are in fact the areas of rational right triangles. B. Gross has informed me that refinements of these methods show that a positive integer with at most two prime factors which is congruent to 5, 6, or 7 modulo 8 is the area of a rational right triangle.

The fact that there exist modular forms of weight 3/2 such that the nonvanishing of the d^{th} Fourier coefficient implies that $E^d(\mathbf{Q})$ is finite follows from several recent theorems. First, the L-series of the elliptic curve E: $y^2=x^3-x$ is the Mellin transform of the image φ of some form of weight 3/2 (and in fact of several) under the correspondence of Shimura [18]. Second, the main theorem of Waldspurger [25] shows that the square of the n^{th} coefficient of a suitable form of this type is a multiple of $L(E^d, 1)$ for d equals n or $2n$. Finally, the result of Coates-Wiles [7] shows that if $L(E^d, 1)\neq 0$, then $E^d(\mathbf{Q})$ is finite.

When forms having the above properties are found, they provide an efficient way to prove that certain numbers are not areas of any rational right triangle. Conjecturally, it reduces the problem of determining if D is in $\mathscr{C}$ to an algebraic computation involving $O(D^{3/2})$ steps. For example, the coefficient $a(n)$ is the number of triples of integers (x, y, z) such that $2x^2+y^2+32z^2=n$ minus one-half the number of triples such that $2x^2+y^2+8z^2=n$.

The first section of the paper considers the Shimura correspondence and determines forms of weight 3/2 giving rise to the modular form ϕ with L-series $L(E, s)$. In the second section the calculations necessary to apply Waldspurger's results are carried out, and the values of $L(E^d, 1)$ are computed. This may be compared with the calculations of [3]. The third section applies these results to the problem of congruent numbers. A table of square free noncongruent integers less than 1000 is given. Conjecturally, any square free integer less than 1000 not in that table is the area of some rational right triangle. The comparison of the results here with the conjecture of Birch and Swinnerton-Dyer gives a formula for the conjectural order of the Tate-Shafarevitch group of E^d. The final section discusses the proof of some classical criteria for noncongruent numbers from the results of previous sections.

1. The Curve $y^2=x^3-D^2x$ and Forms of Weight 3/2

The elliptic curve E^D: $y^2=x^3-D^2x$ has complex multiplication by $\mathbf{Z}[i]$, and the L-function $L(E^1, s)$ is the Mellin transform of the unique normalized newform ϕ of weight 2, level 32 and trivial character. Thus the L-series of E^D is the Mellin transform of the form $\phi\otimes\chi_D$, where χ_D is the quadratic Dirichlet character corresponding to $\mathbf{Q}(\sqrt{D})$. The curve $E=E^1$ is the curve $32A$ of Table 1 of [4]. It is isogenous to $X_0(32)$, and $L(E, s)=\sum\chi(\mathfrak{a})N\mathfrak{a}^{-s}$ for a weight 1 Hecke character χ of $\mathbf{Q}(i)$. Some coefficients of the q-expansion of ϕ are tabulated in [4, Page 117]; they are easily computed from χ or by counting points over $\mathbf{F}_p$. The expansion begins $\phi=q-2q^5-3q^9+6q^{13}+2q^{17}+\dots$.

Shimura has shown in [18] that if f is a cusp form of weight $k/2$, for $k>1$ odd, which is an eigenform for Hecke operators $T(p^2)$ with eigenvalue λ_p, for all primes p, then there exists a form of weight $k-1$ which is an eigenform with eigenvalue λ_p for $T(p)$ for all p. This is called the Shimura map from cusp forms of half integer weight $k/2$ to forms of weight $k-1$. The effect of this map is to square the corresponding characters. From [10, § 5.3] we see that the form ϕ of weight 2 giving the L-series $L(E, s)$ is the image of at least one form of weight 3/2 with quadratic character χ. Further, it is established there that if

f is of weight 3/2 and is orthogonal to the forms of the type $\sum_{m=1}^{\infty} \psi(m)\, m\, q^{tm^2}$ which have the same level and character as f, then the image of f under the Shimura map is a cusp form. Contrary to the assertion of [10, Page 120], the modular form ϕ of level 32 is not the image of a form of weight 3/2, level 64 with quadratic character. For, from the dimension formulas of [8], we see that the space of such forms with trivial character is spanned by $\sum_{m=1}^{\infty} \psi(m)\, m\, q^{m^2}$ where ψ is of conductor 4, while the space of such forms with nontrivial quadratic character is zero. The situation is more favorable for forms of weight 3/2 and level 128. From [8] the dimension of the space of modular forms of weight 3/2, level 128 and fixed quadratic character is 3. This is the same as the dimension of the space of forms of weight 1/2 with level 128 and quadratic character, which suggests constructing such weight 3/2 forms by multiplying forms of weight 1/2 by a weight 1 form g. Let $\theta_t = \sum_{-\infty}^{\infty} q^{tm^2}$. This is a modular form of weight 1/2, level $4t$ and character χ_t. By the results of Serre-Stark [17], $\{\theta_2, \theta_8, \theta_{32}\}$ is a basis for forms of weight 1/2, level 128 and character χ_2. The set $\{\theta_1, \theta_4, \theta_{16}\}$ is a basis for the analogous space with trivial character. The next theorem gives a weight one form g of level 128 and character χ_{-2} which enables the weight 3/2, level 128 spaces to be analyzed completely. This method is computationally simpler than constructing the weight 3/2 forms via theta-functions of ternary quadratic forms.

Theorem 1. *There exists a unique normalized newform g of weight* 1, *level* 128 *and character χ_{-2}. The q-expansion of this form is*

$$g = \sum (-1)^{m+n} q^{(4m+1)^2 + 16n^2} = \sum (-1)^n q^{(4m+1)^2 + 8n^2}, \quad \textit{where } (m, n) \textit{ is in } \mathbf{Z} \times \mathbf{Z}.$$

Proof. Suppose that such a form g exists. Then g, $g \otimes \chi_2$, $g \otimes \chi_{-1}$, $g \otimes \chi_{-2}$ will also be normalized newforms of level 128 with the same character [19]. They are not all independent, for multiplication by θ_1 gives forms of weight 3/2 and level 128 with character χ_2, which lie in a space of dimension 3. Since the 4 newforms above are dependent, it must be true that $g = g \otimes \chi_t$ for some nontrivial quadratic character χ_t of conductor dividing 8. We wish to show that the Dirichlet series associated to g is the Artin-L-series of a two-dimensional irreducible Artin representation which is induced from a character of an index two subgroup. Then the problem of finding all such modular forms g will be reduced to a problem of Galois theory. It is a special case of a general result of Labesse and Langlands (L-indistinguishability for $SL(2)$, Canad. J. Math. XXXI (1979), 726–785; Proposition 6.5) that if $g = g \otimes \chi_t$, then g is as described above. Alternately, the theorem of Deligne and Serre (Formes modulaires de poids 1, Ann. Sc. de l'Ec. Norm. Sup., t 7 (1974), 507–530) shows that the L-series of g is the Artin L-series of some irreducible two-dimensional Artin representation σ of Artin conductor 128 and determinant χ_{-2}. Since $g = g \otimes \chi_t$, we have that $\sigma = \sigma \otimes \chi_t$, which implies by Frobenius reciprocity that σ is induced from an index two subgroup. It is easy to check that there is up to isomorphism only one such Artin representation with Artin conductor 128 and determinant the character χ_{-2}. It is in fact induced from any of the 3 quadratic extensions inside the field of 8th roots of unity. The L-series of g may be expressed in three ways as the Dirichlet L-series of a character of a quadratic extension K. When $K=\mathbf{Q}(i)$, η may be taken to be the character of the $(1+i)^5$-ideal classes which is trivial on $(1+2i)$ and -1 on (5) (these ideals generate the ideal class group in question, which has order 4). It is easy to see that $g=\sum \eta(\mathfrak{a})\, q^{N\mathfrak{a}}=\sum(-1)^{m+n} q^{(4m+1)^2+16n^2}$, the sum taken over all (m,n) in $\mathbf{Z}\times\mathbf{Z}$. A similar computation shows that when $K=\mathbf{Q}(\sqrt{-2})$, the Dirichlet character of this field may be taken to be the character η' of the 4-ideal class group which is trivial on (3) and takes value i on $(1+\sqrt{-2})$. Then $g=\sum \eta'(\mathfrak{b})\, q^{N\mathfrak{b}}=\sum(-1)^n q^{(4m+1)^2+8n^2}$. The expression coming from the field $\mathbf{Q}(\sqrt{2})$ will not be used in the sequel.

Remark. The form g has a long history. Jacobi noticed that $g=q\Pi(1-q^{8n})(1-q^{16n})$ and remarked on the two representations given in Theorem 1. A recent reference to this form is [13], a serendipitous one is H.J. Smith's Report on Number Theory [20], where he treats Jacobi's example in his article 128!

By Theorem 1 and the previous remarks, a basis for the space of cusp forms of weight 3/2, level 128 and trivial character is $\{g\theta_2, g\theta_8, g\theta_{32}\}$. Similarly, $\{g\theta_1, g\theta_4, g\theta_{16}\}$ is a basis for the weight 3/2 cusp forms of level 128 and character χ_8.

Theorem 2. *The modular forms $g\theta_2$, $g\theta_4$, $g\theta_8$ and $g\theta_{16}$ correspond to the weight two form ϕ (of level 32, trivial character) under Shimura's map from forms of weight 3/2 to forms of weight 2.*

Proof. The first few terms of the q-expansions of the forms of weight 3/2 with level 128 and trivial character are as follows:

$$\begin{aligned} g\theta_2 &= q+2q^3+q^9-2q^{11}-4q^{17}-2q^{19}-3q^{25}+4q^{33}-4q^{35}+\dots\\ g\theta_8 &= q+q^9-4q^{17}-3q^{25}+4q^{33}+\dots\\ g\theta_{32} &= q-q^9-2q^{17}+q^{25}+2q^{33}+\dots. \end{aligned}$$

The Hecke operators $T(p^2)$ preserve this space. Consideration of $T(3^2)$ and $T(5^2)$ shows that $g\theta_2, g\theta_8$ and $2g\theta_{32}-g\theta_8$ are eigenforms. The first two have eigenvalues $\lambda_3=0$, $\lambda_5=-2$, while it is clear that $2g\theta_{32}-g\theta_8=\sum_{-\infty}^{\infty}\psi(m)\, mq^{m^2}$, where ψ is the nontrivial quadratic character of conductor 4.

To derive that $g\theta_2$ and $g\theta_8$ are eigenforms for all $T(p^2)$, notice that they are orthogonal to $\sum\psi(m)\, m\, q^{m^2}$ since the eigenvalues of $T(3^2)$, $T(5^2)$ are different than on the latter form. Hence the span of $g\theta_2$ and $g\theta_8$ is $T(p^2)$ stable. The form $g(\theta_2-\theta_8)$ has q^n appearing with nonzero coefficient only when $n\equiv 3$ (8) (since $g=\sum c(n)\, q^n$ and $c(n)=0$ unless $n\equiv 1$ (8)). Similarly $g\theta_8$ has exponents in the q-expansion all congruent to 1 modulo 8. It is clear from the formula for the action of $T(p^2)$ [18, Theorem 1.7] that $T(p^2)(g(\theta_2-\theta_8))$ and $T(p^2)(g\theta_8)$ have the same properties with respect to exponents modulo 8 appearing in the

q-expansion. Since $T(p^2)$ acts on the span of $g(\theta_2-\theta_8)$ and $g\,\theta_8$, it must be that they are individually eigenforms for all $T(p^2)$.

Finally, from Shimura's theory there exist weight two forms ϕ_1, ϕ_2 of level at most 128 having $T(p)$ eigenvalues in agreement with those of $T(p^2)$ on $g(\theta_2-\theta_8)$ and $g\,\theta_8$ respectively. Since the eigenvalues for $p=3,5$ are known, it is easy to compare these values with the forms appearing in Table 3 of [4] of level dividing 128 to see that $\phi_1=\phi_2=\phi$ is the only possibility.

The case of the forms $g\,\theta_4$ and $g\,\theta_{14}$ with character χ_8 is analogous to the preceeding; we will not carry it out here.

For future reference write $g\,\theta_2=\sum a(n)\,q^n$ and $g\,\theta_4=\sum b(n)\,q^n$. Let the form of Theorem 1 be given by $g=\sum c(n)\,q^n$, with $c(n)=0$ for $n\leqq 0$. Then $a(n) = \sum\limits_{m=-\infty}^{\infty} c(n-2m^2)$ and $b(n)=\sum\limits_{m=-\infty}^{\infty} c(n-4m^2)$. Formulas for $a(n)$ and $b(n)$ may be given in terms of the characters η, η' of the proof of Theorem 1 and expressions of n by ternary quadratic forms. It is easy to see by using Theorem 1 that for n odd, $a(n)$ equals the number of triples of integers (x,y,z) such that $2x^2+y^2+32z^2=n$ minus one-half the number of (u,v,w) with $2u^2+v^2+8w^2=n$.

2. Waldspurger's Theorem on L-Series Values

We will specialize to our situation the following theorem of Waldspurger.

Theorem (Waldspurger [25, Theorem 1]). *Let ϕ be a newform of weight $k-1$ and character χ^2 which is the image of a form f of weight $k/2$ under Shimura's map. Assume further that 16 divides the level of ϕ. Then there exists a function $A(t)$ from square free integers to $\mathbf{C}$ such that*

(i) $A(t)^2\,\varepsilon(\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, 1/2)=2(2\pi)^{(1-k)/2}\,\Gamma((k-1)/2)\,L(\phi\,\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, (k-1)/2)$.

(ii) *For each positive integer N, there exists a finite set of explicitly described functions $c(n)$ such that $\sum A(n^{sf})\,c(n)\,q^n$ for $c(n)$ in this set spans the forms of weight $k/2$, level N, and character χ which correspond to ϕ via Shimura's map.*

Remark. The statement here is a special case of that of [25], which is sufficient for our purposes. The factor $\varepsilon(\eta, 1/2)$ for a Hecke character η is the one in [24]; Waldspurger uses the inverse in his statement. In particular, when η is quadratic $\varepsilon(\eta, 1/2)=1$ (since ε is inductive and $\varepsilon(1)=1$ [24]). The sets of functions $c(n)$ are given in the 11 equations of Sect. VIII.4 of [25]. They simplify immensely in the case of interest here.

Theorem 3. *Let $g\,\theta_2=\sum a(n)\,q^n$ and $g\,\theta_4=\sum b(n)\,q^n$ be modular forms of weight 3/2 and level 128 corresponding to the unique weight two normalized newform of level 32 and trivial character. For d a square-free odd positive integer we have*

$$L(E^d, 1)=a(d)^2\,\beta\,d^{-1/2}/4$$

$$L(E^{2d}, 1)=b(d)^2\,\beta(2d)^{-1/2}/2.$$

where

$$\beta=\int_1^{\infty} dx/(x^3-x)^{1/2}=2.62205\ldots \quad \textit{is the real period of } E.$$

Proof. We compare the forms constructed in Waldspurger's theorem with those constructed in Theorem 2. In this case, the possible functions are all of the form $c(n)=n^{1/4}\Pi\, c_p(n)$, where for p odd and n square-free, $c_p(n)=1$ [25, VIII.4.3]. The possible nonzero choices for $c_2(n)$ are the characteristic function of an odd residue class modulo 8 [25, VIII.4.1].

When χ is trivial, we apply Waldspurger's theorem to find that $\sum A(n^{sf})\,c(n)\,q^n$ for the four choices of the function $c(n)$ above span the same space as $g\,\theta_2, g\,\theta_8$. Since $g\,\theta_2$ and $g\,\theta_8$ have no terms q^n appearing with nonzero coefficient when n is not congruent to 1 or 3 modulo 8, it must be true that $A(n)=0$ for $n\equiv 5, 7$ (modulo 8). Choosing $c(n)$ to be respectively the characteristic functions of 1 and 3 modulo 8 shows that for n square-free $a(n)=\beta_1\,A(n)\,n^{1/4}$ and $a(n)=\beta_3\,A(n)\,n^{1/4}$. Thus we have

$$\begin{aligned}
a(n)^2&=\beta_1^2\,L(E^n,1)\,n^{1/2} && n\equiv 1 \quad (8),\\
a(n)^2&=\beta_3^2\,L(E^n,1)\,n^{1/2} && n\equiv 3 \quad (8),\\
a(n)^2&=0=A(n)^2=L(E^n,1) && n\equiv 5, 7 \ (8).
\end{aligned}$$

To compute β_1, β_3 we need to explicitly evaluate some L-series values. Let β be the period of E. It is shown in [3, Table 1] that $L(E^n,1)\,n^{1/2}/\beta$ is rational, and a table is given for certain n. In particular $L(E,1)/\beta=1/4$ and $L(E^3,1)\,3^{1/2}/\beta=1$. Since $a(1)=1$ and $a(3)=2$ this shows that $4/\beta=\beta_1^2=\beta_3^2$.

When $\chi=\chi_2$, Waldspurger's theorem again applies. In this case, $A(t)^2=L(\phi\,\chi_2\,\chi_t,1)=L(E^{2t},1)$. Comparing the Waldspurger basis with the basis $(g\,\theta_4-g\,\theta_{16})$, $g\,\theta_{16}$ gives in this case that $A(n)=0$ when $n\equiv 3, 7$ modulo 8 and that

$$\begin{aligned}
b(n)&=\gamma_1\,A(n)\,n^{1/4} && n\equiv 1 \ (8),\\
b(n)&=\gamma_5\,A(n)\,n^{1/4} && n\equiv 5 \ (8).
\end{aligned}$$

Using this to compute $L(E^{2n},1)$, and comparing with the tables of [3] to find $L(E^2,1)$ and $L(E^{10},1)$ verifies the theorem.

3. Applications

The previous results can be applied to prove that certain numbers are not the areas of rational right triangles by invoking the following theorem.

Theorem (Coates-Wiles [7]). *Let E be an elliptic curve over $\mathbf{Q}$ with complex multiplication by the ring of integers in a quadratic field of class number 1. If $L(E,1)\neq 0$, then $E(\mathbf{Q})$ is finite.*

From this and Theorem 3 we obtain immediately our main result. Recall that $g\,\theta_2=\sum a(n)\,q^n$ and $g\,\theta_4=\sum b(n)\,q^n$ are forms of weight 3/2, that $a(n)=0$ unless $n\equiv 1$ or 3 modulo 8 and $b(n)=0$ unless $n\equiv 1$ or 5 modulo 8. As a notational device, let $b(n/2)$ be zero if $n/2$ is not integral. Notice that $a(n)+b(n/2)$ is one of $a(n)$ or $b(n/2)$.

Theorem 4. *If $a(n)+b(n/2)\neq 0$ then n is not the area of a rational right triangle.*

Comparison with the conjecture of Birch and Swinnerton-Dyer [3], [22, § 8] leads to a sharp conjecture about congruent numbers. To frame their conjecture we need the basic conjecture that the L-series of an elliptic curve over Q has a meromorphic continuation to a function on the complex plane. Attached to such a curve is a cohomologically defined group $Ш$, the Tate-Shafarevitch group, which is conjectured to be finite. The conjecture of Birch and Swinnerton-Dyer relates the L-series value at 1 to the group of rational points of the elliptic curve and the conjectural order of $Ш$.

Conjecture (Birch and Swinnerton-Dyer). *Let A be an elliptic curve over $\mathbf{Q}$ and let $A(\mathbf{Q})$ be the group of rational points of A. Then*

(i) *$L(A,1)\neq 0$ if and only if $A(\mathbf{Q})$ is finite.*

(ii) *When $A(\mathbf{Q})$ is finite, $L(A,1)=\alpha|Ш|\,\Pi\, c_p/|A(\mathbf{Q})|^2$, where α is the integral of a minimal Néron differential over $A(\mathbf{R})$, $c_p=[A(Q_p)\colon A_0(Q_p)]$ and $|G|$ denotes the order of a group G.*

If this conjecture is valid for the curves E^d, then d is the area of a rational right triangle if and only if $L(E^d,1)=0$. Combining the above with Theorem 3 gives the following conjectural description of congruent numbers. Let $\sigma_0(n)$ be the number of positive divisors of n.

Conjecture. *Let d be a square-free positive integer. Then d is a congruent number if and only if $a(d)+b(d/2)=0$. If d is not congruent, the order $|Ш(E^d)|$ of the Tate-Shafarevitch group is $(a(d)/\sigma_0(d))^2$ when d is odd and $(b(d/2)/\sigma_0(d/2))^2$ when d is even.*

Remark. In order to derive the conjecture from that of Birch-Swinnerton-Dyer and Theorem 3, it is only necessary to apply the algorithm of [23] to check that $c_p=4$ when p is odd, $p|d$ and that $c_2=2$ or 4 according to d odd or even. The remaining $c_p=1$, and $E^d(\mathbf{Q})$ has order 4 in all cases.

Among other things, the conjecture predicts that $a(n)/\sigma_0(n)$ and $b(n/2)/\sigma_0(n/2)$ are integers, and gives an efficient algebraic criterion for deciding when a number is the area of a rational right triangle. Table 1 contains a list of all square-free positive integers n less than 1000 such that $a(n)+b(n/2)\neq 0$, By Theorem 4, these are all noncongruent, and conjecturally this list contains all noncongruent square-free positive integers less than 1000. The table contains several numbers left undecided in previous works [1, 2, 26]. The numbers are tabulated according to the value of $a(n)/\sigma_0(n)$ for n odd and $b(n/2)/\sigma_0(n/2)$ for n even; that is by the signed square root of the conjectural order of $Ш(E^n)$.

Table 1. Noncongruent square-free integers <1000

$a(N)/\sigma_0(N)$	N
1	1 3 33 51 57 59 83 139 177 187 209 211 267 321 339 345 379 385 411 451 489 499 515 555 587 595 649 659 665 681 707 803 811 827 835 899 921 969
-1	11 19 35 67 91 105 115 123 129 179 195 201 227 235 249 273 347 393 403 419 427 435 473 483 563 611 635 683 691 705 715 739 753 779 787 795 817 843 851 993
2	73 155 185 203 241 281 329 355 545 553 579 601 627 641 697 755 763 785 865 937
-2	17 89 97 193 217 233 259 305 377 401 449 481 497 617 667 713 745 769 897 929 955 977 979
3	43 131 163 417 491 537 571 619 849 913 923
-3	107 251 283 331 547 633 643 699 737 771 883
4	113 337 577 593 809 857 881 953
-4	409 521 569 939
5	307 859 971
-5	443 523 947
-6	433 673
-7	467
9	907

$b(N/2)/\sigma_0(N/2)$	N
1	2 10 58 74 114 122 130 170 258 290 314 346 354 362 370 402 474 506 586 610 618 642 714 730 746 786 826 906 922 946 962 970 986
-1	26 42 66 106 186 202 266 418 498.530 554 570 634 682 690 754 762 770 834 858 874 930
2	82 282 562 626 818 914
-2	146 178 274 322 466 938 994
3	298 778
-3	218 394 458 538 794 842 978
4	706 802
-4	482 898
5	698

4. Criteria for Noncongruent Numbers

There are several classical criteria which yield noncongruent numbers [1, 9, 15]. For example, it is known that if p and q are primes congruent to 5 modulo 8, then pq and $2p$ are not congruent numbers. This section will explain how such classical criteria may be derived from Theorems 1 and 4. I am indebted to K. Kramer for pointing out to me that all the classical criteria can be obtained by making a 2-descent on the curve E^d, or on an isogenous curve, to prove that $E^d(\mathbf{Q})$ is finite. He also provided an extensive list of criteria obtained in this fashion of which a few simple examples are treated here.

Proposition 5. *Let p be a prime congruent to* 3 *modulo* 8. *Then* $a(p) \equiv 2 \pmod 4$, *so that p is not a congruent number.*

Proof. It is easy to see from the proof of Theorem 1 and the definition that $a(n) = \sum \eta(x+iy)$ over all triples of integers (x, y, z) such that $x>0$ is odd, y is even and such that $n=x^2+y^2+2z^2$. When $n \equiv 3 \pmod 8$, z must be nonzero. There are two expressions $p=x^2+2z^2$, one with z the negative of the other. Since $\eta(x+iy)+\eta(x-iy)$ is even, the sum of $\eta(x+iy)$ over $p=x^2+y^2+2z^2$ with $x>0$ and odd and $y \neq 0$ is divisible by 4. Hence $a(p) \equiv 2\eta(a) \equiv 2 \pmod 4$ if $p=a^2+2b^2$.

For further applications it will necessary to count the number of representations of an integer as $2a^2+b^2+c^2$. This ternary quadratic form is in a genus with one class. It is well known that the number of representations of n by quadratic ternary forms in a genus is related to class numbers of quadratic fields. The following result, taken from [11, Page 194] will be sufficient for applications here. Let d be an odd square-free integer greater than 1. Let $N(d)$ be the number of triples of integers, modulo the action of unimodular integral matrices stabilizing the form $q(x, y, z)=x^2+y^2+2z^2$, such that $q(x, y, z)=d$. Then $N(d)=h(-2d)/2$, where $h(-2d)$ is the class number of $\mathbf{Q}(\sqrt{-2d})$.

Proposition 6. *Let* $p \equiv 1 \pmod 8$ *be a prime. Write $p=a^2+4b^2$ and suppose that* 16 *does not divide $p-1+4b$. Then* $a(p) \equiv 4 \pmod 8$, *and p is not congruent.*

Proof. There are unique expressions $p=a^2+4b^2=c^2+2d^2$ in positive integers. Hence, of the expressions of p as $x^2+y^2+2z^2$, exactly two are such that $xyz=0$. Of the $h(-2p)/2-2$ remaining expressions (x, y, z) and $(x, -y, -z)$ are counted together, since multiplying y by -1, z by -1 is a unimodular transformation preserving $x^2+y^2+2z^2$. In the sum these contribute $\eta(x+iy)+\eta(x-iy)=\pm 2$. The contributions of (x, y, z) and $(x, y, -z)$ are the same, showing that $a(p) \equiv 2(\eta(a+2bi)+\eta(c))+h(-2p)+4 \pmod 8$.

The hypothesis is equivalent to $h(-p) \equiv 4 \pmod 8$, since by [6], $h(-p) \equiv \frac{p-1}{2}+2b$. From Proposition 2 of [14], $h(-p)+h(-2p) \equiv \frac{p-1}{2} \pmod 8$. From the fact [5] that $p=r^2+2 \cdot 16s^2$ implies that $h(-p) \equiv 0 \pmod 8$ we see that $c \equiv \pm 3$ when $p \equiv 1 \pmod{16}$ and $c \equiv \pm 1$ when $p \equiv 9 \pmod{16}$. It is easy to see that $\eta(a+2bi)=-1$ in all cases. Thus, $a(p) \equiv 2(-1+\eta(c))+\frac{p-1}{2} \equiv 4 \pmod 8$.

The hypothesis of the previous theorem may be stated in several ways, which are equivalent to those considered by Razar in [16, Theorem 2].

Proposition 7. *Let p and q be primes congruent to* 5 *modulo* 8. *Then* $b(pq) \equiv 4 \pmod 8$, *so that $2pq$ is not the area of a rational right triangle.*

Proof. The alternate expression for g in terms of an ideal class character η' of $\mathbf{Q}(\sqrt{-2})$ in Theorem 1 may be used. Then $b(pq)=\sum \eta'(x+y\sqrt{-2})$ over all triples of integers (x, y, z) such that $pq=x^2+2y^2+z^2$ with $x>0$ and z even. Of the $h(-2pq)/2$ expressions of pq (up to unimodular automorphism stabilizing $x^2+2y^2+z^2$) there are 2 with $y=0$. In the remaining $(h(-2pq)/2-2)$, (x, y, z) and $(x, -y, -z)$ are counted once, but contribute $\eta(x+y\sqrt{-2})+\eta(x-y\sqrt{-2}) = \pm 2$ to the sum. Hence, $b(pq)\equiv 4+2(h(-2p)/2-2)\equiv h(-2p) \pmod 8$. From [14; Cor. 1, Prop. 5] $h(-2p)\equiv 4 \pmod 8$. This establishes the result.

Similar criteria are obtainable in other cases by expressing $a(n)$ or $b(n)$ in terms of a quadratic class number and computing modulo 8.

References

1. Alter, R., Curtz, T.B., Kubota, K.K.: Remarks and results on congruent numbers. Proc. Third Southeastern Conf. on Combinatorics, Graph Theory and Computing 1972, pp. 27–35
2. Alter, R.: The congruent number problem. Amer. Math. Monthly **87**, 43–45 (1980)
3. Birch, B.J., Swinnerton-Dyer, H.P.F.: Notes on elliptic curves II. J. reine angewandte Math. **218**, 79–108 (1965)
4. Birch, B.J., Kuyk, W.: Tables on elliptic curves. In: Modular functions of one variable IV. Lecture Notes in Mathematics, vol. 476, pp. 81–144. Berlin-Heidelberg-New York: Springer 1979
5. Barrucand, P., Cohn, H.: Note on primes of type x^2+32y^2, class number, and residuacity. J. reine angewandte Math. **238**, 67–70 (1969)
6. Brown, E.: The class number of $\mathbf{Q}(\sqrt{-p})$, for $p\equiv 1 \pmod 8$ a prime. Proc. Amer. Math. Soc. **31**, 381–383 (1972)
7. Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **39**, 223–251 (1977)
8. Cohen, H., Oesterlé, J.: Dimension des espaces de formes modulaires. In: Modular functions of one variable VI. Lecture Notes in Mathematics, vol. 627, pp. 69–78. Berlin-Heidelberg-New York: Springer 1977
9. Dickson, L.E.: History of the theory of numbers II. Carnegie Institution, Washington, DC (1920) (reprinted by Chelsea, 1966)
10. Flicker, Y.: Automorphic forms on covering groups of $GL(2)$. Invent. Math. **57**, 119–182 (1980)
11. Jones, B.W.: The arithmetic theory of quadratic forms. Math. Assoc. of Amer., Baltimore, MD 1950
12. Lagrange, J.: Thèse d'Etat de l'Université de Reims, 1976
13. Moreno, C.J.: The higher reciprocity laws: an example. J. Number Theory **12**, 57–70 (1980)
14. Pizer, A.: On the 2-part of the class number of imaginary quadratic number fields. J. Number Theory **8**, 184–192 (1976)
15. Razar, M.: The nonvanishing of $L(1)$ for certain elliptic curves with no first descents. Amer. J. Math. **96**, 104–126 (1974)
16. Razar, M.: A relation between the two-component of the Tate-Shafarevitch group and $L(1)$ for certain elliptic curves. Amer. J. Math. **96**, 127–144 (1974)
17. Serre, J-P., Stark, H.M.: Modular forms of weight 1/2. In: Modular functions of one variable VI. Lecture Notes in Mathematics, vol. 627, pp. 27–68. Berlin-Heidelberg-New York: Springer 1977
18. Shimura, G.: On modular forms of half-integral weight. Ann. of Math. **97**, 440–481 (1973)
19. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Iwanami Shoten and Princeton University Press 1971
20. Smith, H.J.: Collected Mathematical Papers, Volume 1, Oxford (1894). (reprinted by Chelsea, 1965)

21. Stephens, N.M.: Congruence Properties of Congruent numbers. Bull. London Math. Soc. pp. 182–184 (1975)

22. Tate, J.: The arithmetic of elliptic curves. Invent. Math. **23**, 179–206 (1974)

23. Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable IV. Lecture Notes in Mathematics, vol. 476, pp. 33–52. Berlin-Heidelberg-New York: Springer 1975

24. Tate, J.: Number theoretic background. In: Automorphic forms, representations, and *L*-functions. Proc. Symp. in Pure Math. XXXIII, Part 2, pp. 3–26 (1979)

25. Waldspurger, J.-L.: Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. de Math. pures et appliquées **60**, (4) 375–484 (1981)

26. Guy, R.K.: Unsolved problems. Amer. Math. Monthly **88**, 758–761 (1981)

Oblatum 22-I-1983