A Report on a Paper by Tunnell

Seyfi Turkelli

April 26, 2005

In 1983, Tunnell published a paper giving an almost complete answer to an ancient problem: determine a test whether or not a given positive integer D is the area of a right triangle with rational sides. His main result is :

Theorem. *Let* $g = q\prod_1^\infty(1-q^{8n})(1-q^{16n})$ *and for each positive* t, $\theta_t = \sum_{\mathbb{Z}} q^{tn^2}$. *Set* $g\theta_2 = \sum_1^\infty a(n)q^n$ *and* $g\theta_4 = \sum_1^\infty b(n)q^n$.

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

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

Classically, an integer is called *congruent* if it is the area of a right triangle with rational sides; Otherwise it is called *noncongruent*. One can show that D is a congruent number if and only if the group $E^d(\mathbb{Q})$ of rational points on the elliptic curve $E^d : y^2 = x^3 - d^2x$ is infinite [Ko, page 46]. (In fact, the explicit relation between the curve and congruent numbers is given in the paper in detail.)

The idea of the proof of the theorem is as follows: First $L-$series of the elliptic curve $E : y^2 = x^3 - x$ is the Mellin transform of the image of some forms of weight 3/2, namely $g\theta_2, g\theta_4, g\theta_8, g\theta_{16}$, under Shimura's correspondence [Sh]. Second, the main theorem of Waldspurger [Wa, Theorem 1] shows that the square of n^{th} coefficient of a suitable form of this type is a nonzero multiple of $L(E^d, 1)$ for $d = n$ or $d = 2n$. Finally, the result of Coates-Wiles [Co] shows that if $L(E^d, 1) \neq 0$ then $E^d(\mathbb{Q})$ is finite.

The paper mainly consists of three sections. In the first section, "suitable" forms weight 3/2 are determined. In the second section, Waldspurger's theorem is applied to relate the coefficients of these forms with $L(E^d, 1)$. In the final section, one applies these results to the *congruent number problem.*

One knows that the curve E^d has complex multiplication by $\mathbb{Z}[i]$ and $L-$function $L(E^d, s)$ is the Mellin transform of the form $\phi \otimes \chi_d$ where Φ is the unique normalized newform of weight 2, level 32, trivial character and χ_d is the quadratic Dirichlet character $(\frac{\bullet}{d})$ [Ko, page 81]. One also knows 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 eigenvalues λ_p for all primes p then there is a form of weight $k-1$ which is an eigenform for $T(p)$ with eigenvalue λ_p for all primes p, which is called the Shimura map from weight-$k/2$ cusp forms to weight-$k-1$ forms. This map squares the corresponding characters [Sh].

One has that the dimension of the forms of weight 3/2, level 128 and a fixed quadratic character is 3 which is the dimension of the forms of weight 1/2 of level 128 and quadratic character [Ch]. This suggests constructing such weight-3/2 forms by multiplying such weight-1/2 forms by weight-1 form g. By the results of Serre-Stark [Se], one can see that $\{g\theta_2, g\theta_8, g\theta_{32}\}$ forms a basis for the space of cusp forms of weight 3/2, level 128, trivial character, and $\{g\theta_1, g\theta_4, g\theta_{16}\}$ is a basis for the space of cusp forms of weight 3/2, level 128, character χ_8.

In the first section, it is proven that $g = \sum(-1)^{m+n}q^{(4m+1)^2+16n^2} = \sum(-1)^n q^{(4m+1)^2+8n^2}$ by considering its L-series as the Dirichlet L-series of a character of a quadratic extension $K/\mathbb{Q}$ where $K \subset \mathbb{Q}(\xi_8)$. The main result in this section is:

Theorem 1. *The weight-*$3/2$ *forms* $g\theta_2, g\theta_4, g\theta_8, g\theta_{16}$ *correspond to the unique normalized newform* ϕ *(of level* 32*, trivial character) under Shimura's map.*

One can summarize its proof as follows: First, one considers the space $\{g\theta_2, g\theta_8, g\theta_{32}\}$ which is preserved by the Hecke operators $T(p^2)$. One computes the eigenvalues of $g\theta_2, g\theta_8$ for $T(3^2), T(5^2)$, namely $\lambda_3 = 0, \lambda_5 = -2$ which is different than the ones of $2g\theta_2 - g\theta_8$. Therefore the spaces $< g\theta_2, g\theta_8 >$ and $< 2g\theta_2 - g\theta_8 >$ are orthogonal since the Hecke operators are normal. One can see that $g(\theta_2 - \theta_8)$ has q^n appearing only when $n \equiv 3 \pmod 8$ and $g\theta_8$ has q^n appearing only when $n \equiv 1 \pmod 8$. By the action of $T(p^2)$, it is clear that $T(p^2)g(\theta_2 - \theta_8)$ and $T(p^2)g\theta_8$ have the same properties. This implies that $g(\theta_2 - \theta_8)$ and $g\theta_8$ are individually eigenvalues. Finally, by Shimura correspondence, one has the forms ϕ_1 corresponding to $g(\theta_2 - \theta_8)$ and ϕ_2 corresponding $g\theta_8$ which have the same $T(p)$-eigenvalues with those of $T(p^2)$ on $g(\theta_2 - \theta_8)$ and $g\theta_8$, respectively. Knowing $\lambda_3 = 0$ and $\lambda_5 = -2$ and comparing these values with the table 3 of [Bi], one concludes that $\phi_1 = \phi_2 = \phi$ is the only possibility. For the forms $g\theta_4$ and $g\theta_{16}$, one proceeds n the same way.

In the second section, the main result relates the coefficients of our forms to $L(E^d, 1)$ as follows:

Theorem 2. *Let $g\theta_2 = \sum_1^\infty a(n)q^n$ and $g\theta_4 = \sum_1^\infty b(n)q^n$. For a square free odd positive integer d, one has*

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

and

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

where $\beta = \int_1^\infty dx/(x^3 - x)^{1/2} \approx 2.6$ is the real period of E.

The author's main tool to prove Theorem 2 is the following modified version of Waldspurger's theorem [Wa, Theorem 1]:

Lemma 3. *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 $\mathbb{C}$ such that*

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

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 $c(n)$ is the set spans the forms of weight $k/2$, level N, and character χ which correspond to ϕ via Shimura's map.

The factor $\epsilon(\eta, 1/2) = 1$ when η is quadratic [Ta]. One needs to determine the functions $c(n)$ in order to relate the coefficients $a(n)$ and $b(n)$ to $A(n)$ and so, to $L(E^d, 1)$. Luckily, they are explicitly given in section VIII.4 of [Wa]. By analyzing the tables in [Wa] and Table 1 in [Bs], one verifies the theorem.

In the third section, one concludes the proof of the theorem as an immediate corollary of theorem 2 and following result of Coates-Wiles [Co]:

Theorem 4. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by the ring of integers of a quadratic field with class number 1. If $L(E, 1) \neq 0$ then $E(\mathbb{Q})$ is finite.*

If Birch-Swinnerton-Dyer conjecture is valid for the curves E^d then it follows from the theorem that d is congruent if and only if $L(E^d, 1) = 0$. By putting $b(n/2) = 0$ if $n/2$ is not integral, one reformulates the result as:

If $a(n) + b(n/2) \neq 0$ then n is noncongruent.

The author combines this with Birch-Swinnerton-Dyer conjecture to give the following sharp conjecture:

Conjecture. *Let d be a square free integer. Then d is a congruent number if and only of $a(n) + b(n/2) = 0$. If d is noncongruent then the order of Tate-Shafarevich group $|\text{Ш}(E^d)|$ is $(a(d)/\sigma_0(d))^2$ when d is odd and $(b(d/2)/\sigma_0(d/2))^2$ when d is even, where $\sigma_0(d)$ is the number of positive divisors of d.*

He concludes his paper by proving some classical results on congruent number problem as applications of the theorem.

References

[Bs] B.J. Birch, H.P.F. Swinnerton-Dyer, Notes on Elliptic curves II. J. reine angewandte Math. **218**, 79-108 (1965)

[Bi] B.J. Birch, W. Kuyk, Tables on Elliptic Curves, Modular functions of one variable IV. Lecture notes in Mathematics, vol 476, pp. 81-144, Springer, Berlin-Heidelberg-Newyork, 1979

[Ch] H. Cohen, J. Osterle, Dimension des espaces des formes modulaires. Modular functions of one variable VI. Lecture notes in Mathematics, vol 627, pp. 69-78, Springer, Berlin-Heidelberg-Newyork, 1977

[Co] J. Coates, A. Wiles, On the conjeture of Birch and Swinnerton-Dyer. Invent. Math. **39**, 223-251 (1977)

[Ko] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, Newyork, 1984.

[Se] J.P. Serre, H.M. Stark, Modular Forms of weight 1/2. Modular functions of one variable VI. Lecture Notes in Mathematics, vol 627, pp. 27-68, Springer, Berlin-Heidelberg-Newyork, 1977

[Sh] Goro Shimura, On the modular forms of half integral weight. Annals of Mathematics **97**, 440-481 (1973)

[Ta] J. Tate, Number theoretic background. Automorphic forms, representations and L-functions, Proc. Symp. in Pure Math. XXXIII, Part 2, pp. 3-26 (1979)

[Tu] J.B. Tunnell, A classical diophantine problem and modular forms of weight 3/2. Invent. Math **72**, 323-334 (1983)

[Wa] J.L. Waldspurger, Sur les coefficients de Foruier des formes modularies de poids demi-entier. J. de Math. pures et appliquees **60**, (4) 375-484 (1981)