TATE-SHAFAREVICH GROUPS OF THE CONGRUENT NUMBER ELLIPTIC CURVES

Ken Ono

Abstract. Using elliptic modular functions, Kronecker proved a number of recurrence relations for suitable class numbers of positive binary quadratic forms. For instance if $F(N)$ denotes the number of uneven classes of positive binary quadratic forms with determinant $-N$, then

$$F(2m) + 2\sum_{k=1}^{\infty}(-1)^k F(2m-k^2) = -\sigma(m),$$

where $\sigma(m) := \sum_{2d+1|m} \chi_{-1}(2d+1)$ (see [p. 108, (III),D]). In this note we derive similar relations, assuming the Birch and Swinnerton-Dyer Conjecture, for the orders of Tate-Shafarevich groups of the congruent number elliptic curves

$$E_N: \quad y^2 = x^3 - N^2x.$$

Assuming the Birch and Swinnerton-Dyer Conjecture, if E_N has rank 0, then $\sqrt{|Ш(E_N)|}$ is a simple explicit finite linear combination of $\sqrt{|Ш(E_{N'})|}$ where $1 \le N' < N$.

The relations.

If $N \ge 1$ is an odd square-free integer, then let $E_1(N)$ and $E_2(N)$ denote the elliptic curves over $\mathbb{Q}$

$$E_i(N): \quad y^2 = x^3 - 4^{i-1}N^2x,$$

and let $r_i(N)$ denote the rank of $E_i(N)$. Similarly let $Ш_i(N)$ denote the Tate-Shafarevich group $Ш(E_i(N))$. If $q := e^{2\pi iz}$, $\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$, and $\Theta(z) := \sum_{n\in\mathbb{Z}} q^{n^2}$, then let $f_1(z) \in S_{\frac{3}{2}}(128, \chi_0)$ and $f_2(z) \in S_{\frac{3}{2}}(128, \chi_2)$ be eigenforms given by

$$f_1(z) := \eta(8z)\eta(16z)\Theta(2z) = \sum_{n=1}^{\infty} a_1(n)q^n.$$

$$f_2(z) := \eta(8z)\eta(16z)\Theta(4z) := \sum_{n=1}^{\infty} a_2(n)q^n.$$

Throughout $\chi_t := \left(\frac{t}{\cdot}\right)$ shall denote Kronecker's character for $\mathbb{Q}(\sqrt{t})$. Both forms lift, via the Shimura correspondence, to the cusp form associated to the curve $y^2 = x^3 - x$

$$\sum_{n=1}^{\infty} a(n)q^n := \eta^2(4z)\eta^2(8z) = q\prod_{n=1}^{\infty}(1-q^{4n})^2(1-q^{8n})^2.$$

1991 *Mathematics Subject Classification.* Primary 11G40.
The author is supported by NSF grants DMS-9508976 and DMS-9304580.

Consequently we obtain the following multiplicative formulae for square-free $t \geq 1$:

$$a_1(tm^2) = a_1(t)\sum_{d|m}\chi_{-1}(d)\mu(d)\left(\frac{t}{d}\right)a(m/d),$$

$$a_2(tm^2) = a_2(t)\sum_{d|m}\chi_{-2}(d)\mu(d)\left(\frac{t}{d}\right)a(m/d). \tag{1}$$

Given $a_i(t)$, the integers $a_i(tm^2)$ follow immediately from (1) since

$$a(N) = \sum_{\substack{x\in\mathbb{Z},\, y\geq 0\\ 4x^2+(2y+1)^2=N}} (-1)^{x+y}(2y+1). \tag{2}$$

This can be deduced by explicitly computing the Hecke Grössencharacter of $y^2 = x^3 - x$, or by computing the relevant Jacobstahl sums [Ch. 6, B-E-W], or by classical $q-$series identities [Th. 3,M-O].

Tunnell [T] proved that if $N \geq 1$ is an odd square-free integer, then

$$L(E_i(N), 1) = \frac{2^{i-1}\cdot\Omega\cdot a_i(N)^2}{4\sqrt{2^{i-1}N}}, \tag{3}$$

where $\Omega := \displaystyle\int_{x=1}^{\infty}\frac{1}{\sqrt{x^3-x}}dx \sim 2.622\cdots$. Therefore assuming the Birch and Swinnerton-Dyer Conjecture, $E_i(N)$ has rank 0 if and only if $a_i(N) \neq 0$. In addition if $a_i(N) \neq 0$, then

$$\sqrt{|Ш_i(N)|} = \frac{|a_i(N)|}{\tau(N)} \tag{4}$$

where $\tau(N)$ denotes the number of divisors of N. If the functions $\mathfrak{T}_i(t,m)$ are defined by

$$\mathfrak{T}_1(t,m) := \begin{cases} \mathrm{sign}(a_1(t))\tau(t)\sum_{d|m}\chi_{-1}(d)\mu(d)\left(\frac{t}{d}\right)a(m/d) & \text{if } a_1(t)\neq 0\\ 0 & \text{if } a_1(t)=0, \end{cases} \tag{5}$$

$$\mathfrak{T}_2(t,m) := \begin{cases} \mathrm{sign}(a_2(t))\tau(t)\sum_{d|m}\chi_{-2}(d)\mu(d)\left(\frac{t}{d}\right)a(m/d) & \text{if } \ a_2(t)\neq 0,\\ 0 & \text{if } a_2(t)=0, \end{cases} \tag{6}$$

then by $(1), (4), (5)$, and (6), if $t \geq 1$ is an odd square-free integer, then

$$a_i(tm^2) = \mathfrak{T}_i(t,m)\sqrt{|Ш_i(t)|}. \tag{7}$$

For convenience we define the sets $\mathfrak{S}_1(N)$ and $\mathfrak{F}(N)$, the indices for the first explicit Kronecker relation:

$$\mathfrak{S}_1(N) := \left\{(m,k)\in\mathbb{Z}_+^2 \mid k\geq 3 \text{ odd},\ \frac{2N-k^2}{m^2}\in\mathbb{Z}_+ \text{ square-free},\ r_1\left(\frac{2N-k^2}{m^2}\right)=0\right\}$$

$$\mathfrak{F}(N) := \left\{(x,y) \mid x\in\mathbb{Z},\ y\geq 0,\ \text{and } 4x^2+(2y+1)^2=N\right\}.$$

Theorem 1. *If N is a positive integer, then*

$$a_1(N-1)+\sum_{k=1}^{\infty} a_1(N-(2k+1)^2)$$

$$= \sum_{\substack{x\in\mathbb{Z},y\geq 0\\ 8x^2+2(2y+1)^2=N}} (-1)^y(2y+1) + 2 \sum_{\substack{x\in\mathbb{Z},y\geq 0,\\ 16x^2+4(2y+1)^2=N}} (-1)^{x+y}(2y+1).$$

Proof Theorem 1. If $F_1(z) := \sum_{n=1}^{\infty} A_1(n)q^n := \eta(4z)\eta(8z)\Theta(z)\cdot\sum_{k=0}^{\infty} q^{\frac{(2k+1)^2}{2}}$, then it turns out that

$$F_1(z) = C_1(z) + 2\eta^2(8z)\eta^2(16z)$$

where $C_1(z) = \sum_{n=1}^{\infty} b(n)q^n$ is the newform associated to the elliptic curve

$$y^2 = x^3 + x.$$

In particular all three forms are in $S_2(64)$ and the identity follows from the standard dimension counting argument. In this case checking the identity for the first 9 terms suffice. Therefore we find that $A_1(N) = b(N) + 2a(N/2)$. Using [Ch. 6, B-E-W], or [Th. 3, M-O], it turns out that

$$b(N) = \sum_{(x,y)\in\mathfrak{F}(N)} (-1)^y(2y+1).$$

Assuming the Birch and Swinnerton-Dyer Conjecture, $E_1(t)$ for $t \geq 1$ odd and square-free, has rank 0 if and only if $a_1(t) \neq 0$. The proof now follows immediately from (2) and (7). □

Using the previous discussion we obtain the following immediate corollary.

Corollary 1. *Assuming the Birch and Swinnerton-Dyer Conjecture, if $2N-1$ is a positive square-free integer for which $E_1(2N-1)$ has rank 0, then*

$$\mathfrak{T}_1(2N-1,1)\sqrt{|Ш_1(2N-1)|} + \sum_{(m,k)\in\mathfrak{S}_1(N)} \mathfrak{T}_1\left(\frac{2N-k^2}{m^2}, m\right)\sqrt{\left|Ш_1\left(\frac{2N-k^2}{m^2}\right)\right|}$$

$$= \sum_{(x,y)\in\mathfrak{F}(N)} (-1)^y(2y+1) + 2\sum_{(x,y)\in\mathfrak{F}(N/2)} (-1)^{x+y}(2y+1).$$

Corollary 2. *Assuming the Birch and Swinnerton-Dyer Conjecture, if $2N-1$ is a positive square-free integer for which $E_1(2N-1)$ has rank 0 and $\mathrm{ord}_p(N)$ is odd for some prime $p \equiv 3 \pmod 4$, then*

$$|Ш_1(2N-1)| = \frac{1}{\tau(2N-1)^2}\left(\sum_{(m,k)\in\mathfrak{S}_1(N)} \mathfrak{T}_1\left(\frac{2N-k^2}{m^2}, m\right)\sqrt{\left|Ш_1\left(\frac{2N-k^2}{m^2}\right)\right|}\right)^2.$$

We now define the index sets $\mathfrak{S}_2(N), \mathfrak{H}(N)$, and $\mathfrak{I}(N)$ for the second Kronecker relation:

$$\mathfrak{S}_2(N) := \left\{(m,k)\in\mathbb{Z}_+^2 \mid \frac{N-4k^2}{m^2}\in\mathbb{Z}_+ \text{ square-free, } r_2\left(\frac{N-k^2}{m^2}\right) = 0\right\},$$

$$\mathfrak{H}(N) := \left\{(x,y) \mid x\in\mathbb{Z}, y\geq 0, \text{ and } 16x^2+(2y+1)^2 = N\right\},$$

$$\mathfrak{I}(N) := \left\{(x,y) \mid x,y\geq 0, \text{ and } 4(2x+1)^2+(2y+1)^2 = N\right\}.$$

Theorem 2. *If N is a positive integer, then*

$$a_2(N)+2\sum_{k=1}^{\infty}a_2(N-4k^2)$$

$$=\sum_{\substack{x\in\mathbb{Z},y\geq 0\\ 16x^2+(2y+1)^2=N}}(-1)^{x+y}\chi_2(2y+1)(2y+1)-4\sum_{\substack{x,y\geq 0\\ 4(2x+1)^2+(2y+1)^2=N}}(-1)^{x+1}\chi_2(2y+1)(2x+1).$$

Proof Theorem 2. If $F_2(z)=\sum_{n=1}^{\infty}A_2(n)q^n:=f_2(z)\Theta(4z)$, then it is easy to deduce that

$$F^*(z):=\sum_{n\equiv 1,3,7,11,13,15 \pmod{16}}A_2(n)q^n-\sum_{n\equiv 5,9 \pmod{16}}A_2(n)q^n$$

is the newform associated to the elliptic curve

$$y^2=x^3-2x.$$

The proof now follows from the explicit Jacobstahl sums $\sum_{x=0}^{p-1}\left(\frac{x^3-2x}{p}\right)$ which can be found in [6.1.2, 6.2.1, B-E-W]. □

As immediate corollaries we obtain:

Corollary 3. *Assuming the Birch and Swinnerton-Dyer Conjecture, if $N\geq 1$ is an odd square-free integer for which $E_2(N)$ has rank 0, then*

$$\mathfrak{T}_2(N,1)\sqrt{|Ш_2(N)|}+2\sum_{(m,k)\in\mathfrak{S}_2(N)}\mathfrak{T}_2\left(\frac{N-4k^2}{m^2},m\right)\sqrt{\left|Ш_2\left(\frac{N-4k^2}{m^2}\right)\right|}$$

$$=\sum_{(x,y)\in\mathfrak{H}(N)}(-1)^{x+y}\chi_2(2y+1)(2y+1)-4\sum_{(x,y)\in\mathfrak{I}(N)}(-1)^{x+1}\chi_2(2y+1)(2x+1).$$

Corollary 4. *Assuming the Birch and Swinnerton-Dyer Conjecture, if N is a positive odd square-free integer for which $E_2(N)$ has rank 0 and $ord_p(N)=1$ for some prime $p\equiv 3 \pmod 4$, then*

$$|Ш_2(N))|=\frac{4}{\tau(N)^2}\left(\sum_{(m,k)\in\mathfrak{S}_2(N)}\mathfrak{T}_2\left(\frac{N-4k^2}{m^2},m\right)\sqrt{\left|Ш_2\left(\frac{N-4k^2}{m^2}\right)\right|}\right)^2.$$

We conclude with an application to the following question due to Kolyvagin.

Kolyvagin's question. *If $E/\mathbb{Q}$ is an elliptic curve and p is prime, are there infinitely many quadratic twists E_D for which*

$$|Ш(E_D)|\not\equiv 0 \pmod p?$$

Corollary 5. *If p is prime, then there are infinitely many square-free integers N and M for which*

$$r_1(N)=0 \quad\text{and}\quad |Ш_1(N)|\not\equiv 0 \pmod p,$$
$$r_2(M)=0 \quad\text{and}\quad |Ш_2(M)|\not\equiv 0 \pmod p.$$

Proof. If $p=2$, then this is a standard application of 2−descents. By Rubin's theorem, if p is odd and p divides $|Ш_i(N)|$ when $a_i(N)\neq 0$, then $p|a_i(N)$. The result now follows easily from the unconditional recurrences for $a_i(N)$ in Theorems 1 and 2.

□

Remarks

Using the fact that $|Ш_1(1)| = |Ш_2(1)| = 1$ (i.e. via Rubins' theorem [R] and (4)), Corollaries 1 and 3 conditionally capture the orders of all the Tate-Shafarevich groups of rank 0 congruent number curves. The only feature that may appear to be a mystery are the signs of $a_i(t)$ which are part of $\mathfrak{T}_i(t, m)$. However one can easily deduce these signs from the recurrence relations since $\sqrt{Ш_i(N)}$ is always a positive integer. Therefore these relations are closed in the sense that no additional information is required apart from the fact that $a_i(1) = 1$.

The existence of these Kronecker-type formulae is not necessary for obtaining Corollary 5. In a forthcoming paper, the author and C. Skinner [O-S] show how to obtain such results, in a more general setting, in the absence of Kronecker-type formulae. N. Jochnowitz [J] also obtains such results via a completely different argument.

The Kronecker relations presented here have the pleasant property that they are explicit and only depend on the traces of Frobenius of the elliptic curves

$$y^2 = x^3 - x, \quad y^2 = x^3 + x, \quad y^2 = x^3 - 2x.$$

In particular the $E_1(N)$ and $E_2(N)$ are simply twists of these special curves. It is of some interest to classify those *rare* elliptic curves E for which one can obtain Kronecker formulae for orders of Tate-Shafarevich groups of families of twists, especially those formulae which only depend on the Frobenius of special twists of E.

References

[B-E-W] B.C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Wiley Publ., (to appear).

[C] J.E. Cremona, *Algorithms for elliptic curves*, Cambridge Univ. Press, 1992.

[D] L. E. Dickson, *History of the theory of numbers, Vol. 3*, G. E. Strechert & Co., 1934.

[M-O] Y. Martin and K. Ono, *Eta-quotients and elliptic curves*, Proc. Amer. Math. Soc., (to appear).

[J] N. Jochnowitz, *Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves,* (preprint).

[O-S] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms mod ℓ*, (preprint).

[R] K. Rubin, *Tate-Shafarevich groups and $L-$functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560.

[S] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

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

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: ono@math.ias.edu

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail address: ono@math.psu.edu