Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 128 (2008) 1847–1863

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Elliptic curves, modular forms, and sums of Hurwitz class numbers ☆

Brittany Brown [a], Neil J. Calkin [b], Timothy B. Flowers [b], Kevin James [b], Ethan Smith [b,*], Amy Stout [c]

[a] *5101 Connecticut Ave NW, Washington, DC 20008, USA*

[b] *Clemson University, Department of Mathematical Sciences, Box 340975, Clemson, SC 29634-0975, USA*

[c] *Department of Mathematics, LeConte College, 1523 Greene Street, University of South Carolina, Columbia, SC 29208, USA*

Received 20 March 2007; revised 28 September 2007

Available online 28 January 2008

Communicated by David Goss

Abstract

Let $H(N)$ denote the Hurwitz class number. It is known that if p is a prime, then

$$\sum_{|r|<2\sqrt{p}} H\left(4p-r^2\right)=2p.$$

In this paper, we investigate the behavior of this sum with the additional condition $r \equiv c \pmod{m}$. Three different methods will be explored for determining the values of such sums. First, we will count isomorphism classes of elliptic curves over finite fields. Second, we will express the sums as coefficients of modular forms. Third, we will manipulate the Eichler–Selberg trace formula for Hecke operators to obtain Hurwitz class number relations. The cases $m = 2, 3$ and 4 are treated in full. Partial results, as well as several conjectures, are given for $m = 5$ and 7.

☆ This work was partially funded by the NSF grant DMS: 0244001.

* Corresponding author.

E-mail addresses: brittyb586@yahoo.com (B. Brown), calkin@clemson.edu (N.J. Calkin), tflower@clemson.edu (T.B. Flowers), kevja@clemson.edu (K. James), ethans@math.clemson.edu (E. Smith), amycstout@hotmail.com (A. Stout).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.10.008

1. Introduction and statement of theorems

We begin by recalling the definition of the Hurwitz class number.

Definition 1. For an integer $N \geqslant 0$, the Hurwitz class number $H(N)$ is defined as follows. $H(0) = -1/12$. If $N \equiv 1$ or $2 \pmod 4$, then $H(N) = 0$. Otherwise, $H(N)$ is the number of classes of not necessarily primitive positive definite quadratic forms of discriminant $-N$, except that those classes which have a representative which is a multiple of the form $x^2 + y^2$ should be counted with weight $1/2$ and those which have a representative which is a multiple of the form $x^2 + xy + y^2$ should be counted with weight $1/3$.

Several nice identities are known for sums of Hurwitz class numbers. For example, it is known that if p is a prime, then

$$\sum_{|r|<2\sqrt{p}} H\left(4p - r^2\right) = 2p, \tag{1}$$

where the sum is over integers r (both positive, negative, and zero). See for example [3, p. 322] or [5, p. 154].

In this paper, we investigate the behavior of this sum with additional condition $r \equiv c \pmod m$. In particular, if we split the sum according to the parity of r, then we have

Theorem 1. *If p is an odd prime, then*

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod 2}} H\left(4p - r^2\right) = \begin{cases} \frac{4p-2}{3}, & \text{if } c = 0, \\ \frac{2p+2}{3}, & \text{if } c = 1. \end{cases}$$

Once we have the above result, we can use the ideas in its proof to quickly prove the next.

Theorem 2. *If p is an odd prime,*

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod 4}} H\left(4p - r^2\right) = \begin{cases} \frac{p+1}{3}, & c \equiv \pm 1 \pmod 4, \\ \frac{5p-7}{6}, & c \equiv p+1 \pmod 4, \\ \frac{p+1}{2}, & c \equiv p-1 \pmod 4. \end{cases}$$

We will also fully characterize the case $m = 3$ by proving the following formulae.

Theorem 3. *If p is prime, then*

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod 3}} H\left(4p - r^2\right) = \begin{cases} \frac{p+1}{2}, & \text{if } c \equiv 0 \pmod 3,\ p \equiv 1 \pmod 3, \\ p-1, & \text{if } c \equiv 0 \pmod 3,\ p \equiv 2 \pmod 3, \\ \frac{3p-1}{4}, & \text{if } c \equiv \pm 1 \pmod 3,\ p \equiv 1 \pmod 3, \\ \frac{p+1}{2}, & \text{if } c \equiv \pm 1 \pmod 3,\ p \equiv 2 \pmod 3. \end{cases}$$

We also have a partial characterization for the sum split according to the value of r modulo 5.

Theorem 4. *If p is prime, then*

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod 5}} H\left(4p-r^2\right) = \begin{cases} \frac{p-1}{2}, & \text{if } c \equiv \pm(p+1) \pmod 5,\ p \equiv \pm 2 \pmod 5, \\ \frac{p-3}{2}, & \text{if } c \equiv 0 \pmod 5,\ p \equiv 4 \pmod 5. \end{cases}$$

All of the above theorems may be proven by exploiting the relationship between Hurwitz class numbers and elliptic curves over finite fields. In Section 2, we will state this relationship and show how it is used to prove Theorem 1. We will then briefly sketch how to use the same method for the proof of Theorem 2 as well as several cases of Theorem 6 below.

In Section 3, we will use a result about the modularity of certain "partial" generating functions for the Hurwitz class number to prove Theorem 3. The interesting thing about this method is that it leads to a far more general result than what is obtainable by the method of Section 2. Out of this result, it is possible to extract a version of Theorem 3 for p not necessarily prime as well as the following.

Theorem 5. *If $(n,6)=1$ and there exists a prime $p \equiv 2 \pmod 3$ such that $\operatorname{ord}_p(n) \equiv 1 \pmod 2$, then*

$$\sum_{\substack{|r|<\sqrt{n} \\ r\equiv c_n \pmod 3}} H\left(n-r^2\right) = \frac{\sigma(n)}{12},$$

where we take $c_n = 0$ if $n \equiv 1 \pmod 3$, and $c_n = 1$ or 2 if $n \equiv 2 \pmod 3$.

A third method of proof will be discussed in Section 4, which uses the Eichler–Selberg trace formula. This method will allow us to prove the cases of the following result that remain unproven at the end of Section 2.

Theorem 6. *If p is prime, then*

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod 7}} H\left(4p-r^2\right) = \begin{cases} \frac{p+1}{3}, & c \equiv 0 \pmod 7,\ p \equiv 3,5 \pmod 7, \\ \frac{p-5}{3}, & c \equiv 0 \pmod 7,\ p \equiv 6 \pmod 7, \\ \frac{p-2}{3}, & c \equiv \pm(p+1) \pmod 7,\ p \equiv 2,3,4,5 \pmod 7, \\ \frac{p+1}{3}, & c \equiv \pm 2 \pmod 7,\ p \equiv 6 \pmod 7. \end{cases}$$

Finally, in Section 5, we list several conjectures, which are strongly supported by computational evidence. We also give a few partial results and discuss strategies for future work.

2. Elliptic curves and Hurwitz class numbers

The proofs we give in this section are combinatorial in nature and depend on the following, which is due to Deuring.

Theorem 7. *(See [4] or [12].) If r is an integer such that $|r| < 2\sqrt{p}$, then the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with exactly $p+1-r$ points is equal to the number of equivalence classes of binary quadratic forms with discriminant r^2-4p.*

Corollary 1. *For $|r| < 2\sqrt{p}$, the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with exactly $p+1-r$ points is given by $H(4p-r^2)+c_{r,p}$, where*

$$c_{r,p} = \begin{cases} 1/2, & \text{if } r^2-4p = -4\alpha^2 \text{ for some } \alpha \in \mathbb{Z}, \\ 2/3, & \text{if } r^2-4p = -3\alpha^2 \text{ for some } \alpha \in \mathbb{Z}, \\ 0, & \text{otherwise}. \end{cases} \tag{2}$$

Thus, the number of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ such that $m \mid \#E(\mathbb{F}_p)$ is equal to

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv p+1 \pmod m}} \big(H\big(4p-r^2\big)+c_{r,p}\big). \tag{3}$$

This is the main fact that we will exploit in this section. Another useful fact that we will exploit throughout the paper is the symmetry of our sums. In particular,

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod m}} H\big(4p-r^2\big) = \sum_{\substack{|r|<2\sqrt{p} \\ r\equiv -c \pmod m}} H\big(4p-r^2\big). \tag{4}$$

Proof of Theorem 1. For $p=3$, the identities may be checked by direct calculation. For the remainder of the proof, we will assume p is prime and strictly greater than 3.

Let $N_{2,p}$ denote the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ possessing 2-torsion, and recall that E has 2-torsion if and only if $2 \mid (p+1-r)$. Thus,

$$N_{2,p} = \sum_{\substack{|r|<2\sqrt{p} \\ r\equiv p+1 \pmod 2}} \big(H\big(4p-r^2\big)+c_{r,p}\big). \tag{5}$$

We will proceed by computing $N_{2,p}$, the number of isomorphism classes of elliptic curves possessing 2-torsion over $\mathbb{F}_p$. Then, we will compute the correction term, $\sum c_{r,p}$. In light of (1) and (5), Theorem 1 will follow.

We first recall the relevant background concerning elliptic curves with 2-torsion over $\mathbb{F}_p$. The reader is referred to [10] or [15] for more details. If E is an elliptic curve with 2-torsion then, we can move a point of order 2 to the origin in order to obtain a model for E of the form

$$E_{b,c}\colon y^2 = x^3 + bx^2 + cx. \tag{6}$$

The discriminant of such a curve is given by

$$\Delta = 16c^2\big(b^2-4c\big). \tag{7}$$

We will omit from consideration those pairs (b,c) for which the resulting curve has zero discriminant since these curves are singular.

Following [15, pp. 46–48], we take $c_4 = 16(b^2 - 3c)$ and $c_6 = 32b(9c - 2b^2)$. Then since $\mathrm{char}(\mathbb{F}_p) \neq 2, 3$, $E_{b,c}$ is isomorphic to the curve

$$E'\colon y^2 = x^3 - 27c_4x - 54c_6. \tag{8}$$

The curves in this form that are isomorphic to (8) are

$$y^2 = x^3 - 27u^4c_4x - 54u^6c_6, \quad u \neq 0. \tag{9}$$

Thus, given any elliptic curve, the number of $(A, B) \in \mathbb{F}_p^2$ for which the given curve is isomorphic to $E\colon y^2 = x^3 + Ax + B$ is

$$\begin{cases} \frac{p-1}{6}, & \text{if } A = 0 \text{ and } p \equiv 1 \pmod 3, \\ \frac{p-1}{4}, & \text{if } B = 0 \text{ and } p \equiv 1 \pmod 4, \\ \frac{p-1}{2}, & \text{otherwise.} \end{cases}$$

We are interested in how many curves $E_{b,c}$ give the same c_4 and c_6 coefficients. Given an elliptic curve $E\colon y^2 = x^3 + Ax + B$ with 2-torsion over $\mathbb{F}_p$, each choice of an order 2 point to be moved to the origin yields a different model $E_{b,c}$. Thus, the number of $E_{b,c}$ which have the same c_4 and c_6 coefficients is equal to the number of order 2 points possessed by the curves. This is either 1 or 3 depending on whether the curves have full or cyclic 2-torsion. Thus, the number of (b, c) for which $E_{b,c}$ is isomorphic to a given curve is

$$\begin{cases} \frac{p-1}{6}, & c_4 = 0,\ p \equiv 1 \pmod 3 \text{ and 2-torsion is cyclic}, \\ \frac{p-1}{4}, & c_6 = 0,\ p \equiv 1 \pmod 4 \text{ and 2-torsion is cyclic}, \\ \frac{p-1}{2}, & \text{otherwise with cyclic 2-torsion}, \\ \frac{p-1}{2}, & c_4 = 0,\ p \equiv 1 \pmod 3 \text{ and 2-torsion is full}, \\ \frac{3(p-1)}{4}, & c_6 = 0,\ p \equiv 1 \pmod 4 \text{ and 2-torsion is full}, \\ \frac{3(p-1)}{2}, & \text{otherwise with full 2-torsion.} \end{cases} \tag{10}$$

The proof of Theorem 1 will follow immediately from the following two propositions.

Proposition 1. *If $p > 3$ is prime, then the number of isomorphism classes of elliptic curves possessing 2-torsion over $\mathbb{F}_p$ is given by*

$$N_{2,p} = \begin{cases} \frac{4p+8}{3}, & \text{if } p \equiv 1 \pmod{12}, \\ \frac{4p+4}{3}, & \text{if } p \equiv 5 \pmod{12}, \\ \frac{4p+2}{3}, & \text{if } p \equiv 7 \pmod{12}, \\ \frac{4p-2}{3}, & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Proof. In view of (10), we want to count the number of curves $E_{b,c}$ that fall into each of six categories. Let A_1 denote the number of curves with cyclic 2-torsion and $c_4 = 0$, A_2 denote the number of curves with cyclic 2-torsion and $c_6 = 0$, A_3 denote the number of curves with cyclic

2-torsion and $c_4c_6 \neq 0$, A_4 denote the number of curves with full 2-torsion and $c_4 = 0$, A_5 denote the number of curves with full 2-torsion and $c_6 = 0$ and A_6 denote the number of curves with $c_4c_6 \neq 0$. Then $N_{2,p}$ can be computed by determining A_i for $i = 1, \ldots, 6$ and applying (10).

Now, an elliptic curve $E_{b,c}$ has full 2-torsion if and only if $b^2 - 4c$ is a square modulo p. Thus, the number of curves possessing full 2-torsion over $\mathbb{F}_p$ is given by

$$\sum_{\substack{b=0 \\ b^2 \neq 4c}}^{p-1} \sum_{c=1}^{p-1} \frac{1}{2}\left[\left(\frac{b^2-4c}{p}\right) + 1\right] = \frac{(p-1)(p-2)}{2}, \tag{11}$$

and the number of curves possessing cyclic 2-torsion over $\mathbb{F}_p$ is given by

$$\sum_{\substack{b=0 \\ b^2 \neq 4c}}^{p-1} \sum_{c=1}^{p-1} -\frac{1}{2}\left[\left(\frac{b^2-4c}{p}\right) - 1\right] = \frac{p(p-1)}{2}. \tag{12}$$

Note that if $c_4 = 0$, then $b^2 \equiv 3c \pmod{p}$ and hence $(\frac{c}{p}) = (\frac{3}{p})$. Thus, there are $p-1$ nonsingular curves (6) that give $c_4 = 0$. If a nonsingular curve $E_{b,c}$ possesses full 2-torsion and $c_4 = 0$, then $1 = (\frac{b^2-4c}{p}) = (\frac{-c}{p}) = (\frac{-3}{p}) = (\frac{p}{3})$. Thus, when $p \equiv 1 \pmod 3$, all $p-1$ nonsingular curves $E_{b,c}$ with $c_4 = 0$ will have full 2-torsion, and when $p \equiv 2 \pmod 3$, all will have cyclic 2-torsion. Thus,

$$A_1 = \begin{cases} 0, & p \equiv 1 \pmod 3, \\ p-1, & p \equiv 2 \pmod 3, \end{cases}$$

$$A_4 = \begin{cases} p-1, & p \equiv 1 \pmod 3, \\ 0, & p \equiv 2 \pmod 3. \end{cases}$$

Similar computations lead to

$$A_2 = \frac{p-1}{2},$$

$$A_5 = \frac{3(p-1)}{2}.$$

Finally, using (11) and (12), we see that

$$A_3 = \begin{cases} \frac{(p-1)^2}{2}, & p \equiv 1 \pmod 3, \\ \frac{(p-3)(p-1)}{2}, & p \equiv 2 \pmod 3, \end{cases}$$

$$A_6 = \begin{cases} \frac{(p-1)(p-7)}{2}, & p \equiv 1 \pmod 3, \\ \frac{(p-1)(p-5)}{2}, & p \equiv 2 \pmod 3. \end{cases}$$

Combining these with (10), the result follows. □

We now compute the correction term in (5).

Proposition 2. *The value of the correction term is given by*

$$\sum_{\substack{|r|<2\sqrt{p}\\ r\equiv 0 \pmod 2}} c_{r,p} = \begin{cases} 10/3, & p\equiv 1 \pmod{12},\\ 2, & p\equiv 5 \pmod{12},\\ 4/3, & p\equiv 7 \pmod{12},\\ 0, & p\equiv 11 \pmod{12}. \end{cases}$$

Proof. By (2), we see that each form proportional to x^2+xy+y^2 contributes $2/3$ to the sum while each form proportional to x^2+y^2 contributes $1/2$.

Forms proportional to x^2+xy+y^2 arise for those $r\equiv 0 \pmod 2$ for which there exists $\alpha\in\mathbb{Z}\backslash\{0\}$ such that $r^2-4p=-3\alpha^2$. Thus, $p=(\frac{r+\alpha i\sqrt{3}}{2})(\frac{r-\alpha i\sqrt{3}}{2})$. Recall that p factors in $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ if and only if $p\equiv 1 \pmod 3$. For each such p, there are 6 solutions to the above, but only 2 with r even. Thus, for $p\equiv 1 \pmod 3$, we must add $4/3$ to the correction term, and for $p\equiv 2 \pmod 3$, we add 0 to the correction term.

Forms proportional to x^2+y^2 arise for those $r\equiv 0 \pmod 2$ for which there exists $\alpha\in\mathbb{Z}\backslash\{0\}$ such that $r^2-4p=-4\alpha^2$. Thus, $p=\frac{r^2+4\alpha^2}{4}=(\frac{r}{2}+\alpha i)(\frac{r}{2}-\alpha i)$. Recall that p factors in $\mathbb{Z}[i]$ if and only if $p\equiv 1 \pmod 4$. Given a prime $p\equiv 1 \pmod 4$, there are 4 choices for $r/2$ and hence 4 choices for r. So, we have 4 forms and need to add 2 to the correction term. When $p\equiv 3 \pmod 4$ we add 0 to the correction term. □

Combining the results in Propositions 1 and 2, we have

$$\sum_{\substack{|r|<2\sqrt{p}\\ r\equiv 0 \pmod 2}} H\big(4p-r^2\big) = N_{2,p} - \sum_{\substack{|r|<2\sqrt{p}\\ r\equiv 0 \pmod 2}} c_{r,p} = \frac{4p-2}{3}.$$

Theorem 1 now follows from (1). □

We now give a sketch of the proof of Theorem 2. The proof uses some of computations from the proof of Theorem 1.

Proof sketch of Theorem 2. For $c\equiv\pm 1 \pmod 4$, the identities

$$\sum_{\substack{|r|<2\sqrt{p}\\ r\equiv c \pmod 2}} H\big(4p-r^2\big) = \frac{p+1}{3}$$

follow directly from Theorem 1 and (4).

By (3),

$$\sum_{\substack{|r|<2\sqrt{p}\\ r\equiv p+1 \pmod 4}} \big(H\big(4p-r^2\big)+c_{r,p}\big)$$

is equal to the number of isomorphism classes of elliptic curves over $E/\mathbb{F}_p$ with $4 \mid \#E(\mathbb{F}_p)$. This is equal to the number of classes of curves having full 2-torsion plus the number of classes having cyclic 4-torsion over $\mathbb{F}_p$.

As with the proof of Theorem 1, the identities may be checked directly for $p = 3$. So, we will assume that $p > 3$. From the proof of Proposition 1, we see that the number of isomorphism classes of curves having full 2-torsion over $\mathbb{F}_p$ is given by

$$\begin{cases} \frac{p+5}{3}, & p \equiv 1 \pmod{12}, \\ \frac{p+1}{3}, & p \equiv 5 \pmod{12}, \\ \frac{p+2}{3}, & p \equiv 7 \pmod{12}, \\ \frac{p-2}{3}, & p \equiv 11 \pmod{12}. \end{cases}$$

Following [10, pp. 145–147], we see that given any curve with 4-torsion over $\mathbb{F}_p$, we can move the point of order 4 to the origin and place the resulting curve into Tate normal to find a model for the curve of the form

$$E_b\colon y^2 + xy - by = x^3 - bx^2, \tag{13}$$

which has discriminant $\Delta_b = b^4(1 + 16b)$. Let $P = (0, 0)$ denote the point of order 4 on E_b. Thus, as b runs over all of $\mathbb{F}_p$, we see every class of elliptic curve possessing 4-torsion over $\mathbb{F}_p$. As before, we will omit $b = 0, 16^{-1}$ from consideration since these lead to singular curves.

Given a curve of the form (13), we note that both $P = (0, 0)$ and $-P$ have order 4. We see that moving $-P$ to origin and placing the resulting curve in Tate normal form gives us exactly the same normal form as before. Thus, there is exactly one way to represent each cyclic 4-torsion curve in the form (13).

We are only interested in counting the classes which have cyclic 4-torsion and not full 2-torsion (since these have already been counted above). Thus, given a curve (13), we move $2P$ to the origin and place the resulting curve in the form (6). Thus, we see that the curve has full 2-torsion if and only if $(\frac{16b+1}{p}) = 1$. Hence, we conclude that there are $(p-1)/2$ isomorphism classes of curves possessing cyclic 4-torsion but not possessing full 2-torsion over $\mathbb{F}_p$.

Finally, in a manner similar to the proof of Proposition 2, we check that

$$\sum_{\substack{|r|<2\sqrt{p} \\ r \equiv p+1 \pmod 4}} c_{r,p} = \begin{cases} 7/3, & p \equiv 1 \pmod{12}, \\ 1, & p \equiv 5 \pmod{12}, \\ 4/3, & p \equiv 7 \pmod{12}, \\ 0, & p \equiv 11 \pmod{12}. \end{cases}$$

Combining all the pieces, the result follows. □

For the remainder of this section, we will need the following result, which allows us to avoid the problem of detecting full m-torsion by requiring that our primes satisfy $p \not\equiv 1 \pmod m$.

Proposition 3. *If E is an elliptic curve possessing full m-torsion over $\mathbb{F}_p$, then $p \equiv 1 \pmod{m}$.*

Proof. Let G be the Galois group of $\mathbb{F}_p(E[m])/\mathbb{F}_p$. Then $G = \langle\phi\rangle$, where $\phi : \mathbb{F}_p(E[m]) \to \mathbb{F}_p(E[m])$ is the Frobenius automorphism. We have the representation

$$\rho_m : G \hookrightarrow \operatorname{Aut}\big(E[m]\big) \cong \operatorname{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

See [15, pp. 89–90].

Now, suppose that E has full m-torsion. Then $\mathbb{F}_p(E[m])/\mathbb{F}_p$ is a trivial extension. Whence, G is trivial and $\rho_m(\phi) = I \in \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Therefore, applying [15, Proposition V.2.3], we have $p \equiv \det(\rho_m(\phi)) \equiv 1 \pmod{m}$. □

We omit the proof of Theorem 4 since it is similar to, but less involved than the following cases of Theorem 6.

Proof sketch of Theorem 6 (Cases: $p \not\equiv 0, 1 \pmod 7$; $c \equiv \pm(p+1) \pmod 7$). If $p = 3$, the identities may be checked directly. We will assume that $p \neq 3, 7$ and prime. Since we also assume that $p \not\equiv 1 \pmod 7$, we know that no curve may have full 7-torsion over $\mathbb{F}_p$. Thus, if P is a point of order 7, $E[7](\mathbb{F}_p) = \langle P\rangle \cong \mathbb{Z}/7\mathbb{Z}$.

Now, suppose that E possesses 7-torsion, and let P be a point of order 7. In a manner similar to [10, pp. 145–147], we see that we can move P to the origin and put the resulting equation into Tate normal form to obtain a model for E of the form

$$E_s\colon y^2 + \big(1 - s^2 + s\big)xy - \big(s^3 - s^2\big)y = x^3 - \big(s^3 - s^2\big)x^2, \tag{14}$$

which has discriminant $\Delta_s = s^7(s-1)^7(s^3 - 8s^2 + 5s + 1)$.

First, we examine the discriminant. We note that $s = 0, 1$ both result in singular curves and so we omit these values from consideration. The cubic $s^3 - 8s^2 + 5s + 1$ has discriminant 7^4 and hence has Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (see [9, Corollary V.4.7]). Thus, the splitting field for the cubic is a degree 3 extension over $\mathbb{Q}$; and we see that the cubic will either be irreducible or split completely over $\mathbb{F}_p$. One can then check that the cubic splits over the cyclotomic field $\mathbb{Q}(\zeta_7)$, where ζ_7 is a primitive 7th root of unity. $\mathbb{Q}(\zeta_7)$ has a unique subfield which is cubic over $\mathbb{Q}$, namely $\mathbb{Q}(\zeta_7 + \zeta_7^6)$. Thus, $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ is the splitting field for the cubic $s^3 - 8s^2 + 5s + 1$. By examining the way that rational primes split in $\mathbb{Q}(\zeta_7)$, one can deduce that rational primes are inert in $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ unless $p \equiv \pm 1 \pmod 7$, in which case they split completely. Thus, we see that the cubic $s^3 - 8s^2 + 5s + 1$ has exactly 3 roots over $\mathbb{F}_p$ if $p \equiv \pm 1 \pmod 7$ and is irreducible otherwise. Hence, as s ranges over all of $\mathbb{F}_p$, we see $p - 5$ nonsingular curves (14) if $p \equiv \pm 1 \pmod 7$ and $p - 2$ nonsingular curves (14) otherwise.

Second, we check that the mapping $s \mapsto (1 - s^2 + s, -(s^3 - s^2))$ is a one to one mapping of $\mathbb{F}_p \backslash \{0, 1\}$ into $\mathbb{F}_p^2$. Hence, as s ranges over all of $\mathbb{F}_p \backslash \{0, 1\}$, we see $p - 2$ distinct equations of the form (14).

Next, we check that if we choose to move $-P$ to the origin instead of P, we will obtain exactly the same Tate normal form for E. Moving $2P$ or $3P$ to the origin each result in different normal forms unless $s = 0, 1$ or is a nontrivial cube root of -1, in which case both give exactly the same normal form as moving P to the origin. Note that by the above argument, moving $-2P$

to the origin will give the same normal form as $2P$ and moving $-3P$ to the origin will give the same normal form as $3P$. Now, $s = 0, 1$ both give singular curves; and nontrivial cube roots of -1 exists in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$, in which case there are exactly 2. Thus, the number of isomorphism classes of curves possessing 7-torsion over $\mathbb{F}_p$ is given by

$$\begin{cases} \frac{p+2}{3}, & p \not\equiv \pm 1 \pmod 7,\ p \equiv 1 \pmod 3, \\ \frac{p-1}{3}, & p \equiv 6 \pmod 7,\ p \equiv 1 \pmod 3, \\ \frac{p-2}{3}, & p \not\equiv \pm 1 \pmod 7,\ p \equiv 2 \pmod 3, \\ \frac{p-5}{3}, & p \equiv 6 \pmod 7,\ p \equiv 2 \pmod 3. \end{cases}$$

Finally, we check that, for $p \not\equiv 1 \pmod 7$,

$$\sum_{\substack{|r|<2\sqrt{p} \\ r \equiv p+1 \pmod 7}} c_{r,p} = \begin{cases} 4/3, & p \equiv 1 \pmod 3, \\ 0, & \text{otherwise.} \end{cases}$$

The result now follows for $c \equiv \pm(p+1) \pmod 7$ by (3) and (4). □

The remaining cases of Theorem 6 will be treated in Section 4.

3. Modular forms and Hurwitz class numbers

We do not give an exhaustive account of modular forms. Instead we refer the reader to Miyake's book [13] and Shimura's paper [14] for the details. Recall the definition of a modular form.

Definition 2. Let $f : \mathfrak{h} \to \mathbb{C}$ be holomorphic, let $k \in \frac{1}{2}\mathbb{Z}$, and let χ be a Dirichlet character modulo N. Then f is said to be a modular form of weight k, level N, and character χ if

(1) $f(\gamma z) = \begin{cases} \chi(d)(cz+d)^k f(z), & \text{if } k \in \mathbb{Z}, \\ \chi(d)(\frac{c}{d})(\frac{-4}{d})^{-k}(cz+d)^k f(z), & \text{if } k \in 1/2 + \mathbb{Z} \end{cases}$
for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$;

(2) f is holomorphic at the cusps of $\mathfrak{h}/\Gamma_0(N)$.

We denote this space by $\mathcal{M}_k(N, \chi)$. In the case that χ is trivial, we will omit the character. We also recall that the space is a finite-dimensional vector space over $\mathbb{C}$ and decomposes as

$$\mathcal{M}_k(N, \chi) = \mathcal{E}_k(N, \chi) \oplus \mathcal{S}_k(N, \chi),$$

where $\mathcal{S}_k(N, \chi)$ is the subspace of cusp forms and $\mathcal{E}_k(N, \chi)$ is the Eisenstein subspace.

For the remainder, we put $q := q(z) = e^{2\pi i z}$. It is well known that modular forms have natural representations as Fourier series. Here we will develop some notation and show how to construct

weight 2 Eisenstein series. Given two Dirichlet characters ψ_1, ψ_2 with conductors M_1 and M_2 respectively, put $M = M_1 M_2$; and put

$$E_2(z; \psi_1, \psi_2) := \sum_{n=0}^{\infty} a_n q^n,$$

where

$$a_0 = \begin{cases} 0, & \text{if } \psi_1 \text{ is nontrivial,} \\ \frac{M-1}{24}, & \text{if } \psi_1 \text{ and } \psi_2 \text{ are both trivial,} \\ -B_{k,(\psi_1\psi_2)}/4, & \text{otherwise,} \end{cases}$$

and, for $n \geqslant 1$,

$$a_n = \sum_{d|n} \psi_1(n/d)\psi_2(d)d.$$

Here $B_{k,\chi}$ denotes the kth generalized Bernoulli number associated to χ, whose generating function is $F_\chi(t) = \sum_{a=1}^{m} \frac{\chi(a)te^{at}}{e^{mt}-1}$, where m is the conductor of χ. Then, subject to a couple of technical conditions on ψ_1 and ψ_2, one can show $E_2(z; \psi_1, \psi_2) \in \mathcal{E}_2(M, \psi_1\psi_2)$. See [13, pp. 176–181].

When computing with modular forms, the following result allows us to work with only a finite number of coefficients.

Theorem 8. *(See Proposition 1.1 in [6].) Suppose that $k \in \mathbb{Z}$ and $f(z) = \sum a_n q^n \in \mathcal{M}_k(N, \chi)$. Put $m = \frac{k}{12} N \prod_{p|N}(1 + \frac{1}{p})$. Then $f(z)$ is uniquely determined by its Fourier coefficients $a_0, a_1, \ldots, a_{[m]}$.*

In [8, p. 90] ([16] also), Zagier defines a non-holomorphic q-series whose holomorphic part is the generating function for the Hurwitz class number, $H(N)$. He then shows that the series transforms like a modular form of weight $3/2$ on $\Gamma_0(4)$. In [1, Corollary 3.2], Cohen points out that a holomorphic form can be obtained by only summing over those N that fall into certain arithmetic progressions. He states without proof that the resulting series should be a form on $\Gamma_0(A)$, where he specifies A. However, using techniques similar to those found in [11, pp. 128–129], we were only able to prove the following version of this result.

Theorem 9. *If $-b$ is a quadratic nonresidue modulo a, then*

$$\mathcal{H}_1(z; a, b) := \sum_{N \equiv b \pmod{a}} H(N) q^N \in \mathcal{M}_{3/2}(G_a),$$

where

$$G_a = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(A) \colon \alpha^2 \equiv 1 \pmod{a} \right\},$$

and we take $A = a^2$ if $4 \mid a$ and $A = 4a^2$ otherwise.

We now turn to the proof of Theorem 3.

Proof of Theorem 3. It is well known that the classical theta series $\theta(z) := \sum_{s=-\infty}^{\infty} q^{s^2} \in \mathcal{M}_{1/2}(4)$. Applying Theorem 9, we see that $\mathcal{H}_1(z;3,1) = \sum_{N\equiv 1 \pmod 3} H(N)q^N \in \mathcal{M}_{3/2}(36)$. Note that in this case, $G_3 = \Gamma_0(36)$. Thus, we can check that product $\mathcal{H}_1(z;3,1)\theta(z) \in \mathcal{M}_2(36)$. Observe that the coefficients of the product bear a striking resemblance to the sums of interest. Indeed,

$$\begin{aligned}\mathcal{H}_1(z;3,1)\theta(z) &= \sum_{s=-\infty}^{\infty} \sum_{N\equiv 1 \pmod 3} H(N)q^{N+s^2} \\ &= \sum_{n\equiv 1 \pmod 3} \Bigg(\sum_{\substack{|s|<\sqrt{n} \\ s\equiv 0 \pmod 3}} H\big(n-s^2\big)\Bigg) q^n \\ &\quad + \sum_{n\equiv 2 \pmod 3} \Bigg(\sum_{\substack{|s|<\sqrt{n} \\ s\equiv \pm 1 \pmod 3}} H\big(n-s^2\big)\Bigg) q^n.\end{aligned}$$

We will prove Theorem 3 by expressing $\mathcal{H}_1(z;3,1)\theta(z)$ as a linear combination of basis forms with "nice" Fourier coefficients. Note that Theorem 8 says that we will only need to consider the first 13 coefficients in order to do this.

Let χ_0 denote the principal character of conductor 1, and let $\chi_{0,2}$ and $\chi_{0,3}$ denote the trivial characters modulo 2 and 3, respectively. Finally let $(\frac{\cdot}{3})$ denote the Legendre symbol modulo 3. Then one can show that $\mathcal{E}_2(36)$ has dimension 11 over $\mathbb{C}$ and is spanned by

$$\left\{ \begin{array}{lll} E_2(z;\chi_0,\chi_{0,2}), & E_2(z;\chi_0,\chi_{0,3}), & E_2(z;(\frac{\cdot}{3}),(\frac{\cdot}{3})), \\ E_2(2z;\chi_0,\chi_{0,2}), & E_2(3z;\chi_0,\chi_{0,2}), & E_2(9z;\chi_0,\chi_{0,2}), \\ E_2(6z;\chi_0,\chi_{0,2}), & E_2(18z;\chi_0,\chi_{0,2}), & E_2(3z;\chi_0,\chi_{0,3}), \\ E_2(2z;(\frac{\cdot}{3}),(\frac{\cdot}{3})), & E_2(4z;(\frac{\cdot}{3}),(\frac{\cdot}{3})) & \end{array} \right\}.$$

The cusp space $\mathcal{S}_2(36)$ is 1-dimensional and is spanned by the cusp form associated to the elliptic curve

$$E\colon y^2 = x^3 + 1,$$

which is the inverse Mellin transform of the L-series

$$\begin{aligned}L(E,s) &= \prod_{p\nmid 36} \big(1 - a(p)p^{-s} + p^{1-2s}\big)^{-1} = \sum_{(n,6)=1} \frac{a(n)}{n^s} \\ &= \sum_{(n,6)=1} \prod_{p\mid n} \Bigg[\sum_{\lceil \frac{\operatorname{ord}_p(n)}{2} \rceil \leqslant k \leqslant \operatorname{ord}_p(n)} \binom{k}{\operatorname{ord}_p(n)-k} a(p)^{2k-\operatorname{ord}_p(n)} (-p)^{\operatorname{ord}_p(n)-k} \Bigg] \frac{1}{n^s},\end{aligned}$$

where $a(p) := p + 1 - \#E(\mathbb{F}_p)$, and we take $a(p)^0 = 1$ even if $a(p) = 0$. We will denote this cusp form by $f_E(z)$.

One can verify computationally that

$$\begin{aligned}\mathcal{H}_1(z;3,1)\theta(z) = {} & \frac{-1}{16}E_2(z;\chi_0,\chi_{0,2}) + \frac{3}{16}E_2(z;\chi_0,\chi_{0,3}) + \frac{-1}{24}E_2\left(z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)\right)\\ & + \frac{-1}{2}E_2(2z;\chi_0,\chi_{0,2}) + \frac{1}{4}E_2(3z;\chi_0,\chi_{0,2}) + \frac{-3}{16}E_2(9z;\chi_0,\chi_{0,2})\\ & + 2E_2(6z;\chi_0,\chi_{0,2}) + \frac{-3}{2}E_2(18z;\chi_0,\chi_{0,2}) + \frac{-3}{16}E_2(3z;\chi_0,\chi_{0,3})\\ & + \frac{-1}{8}E_2\left(2z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)\right) + \frac{-1}{3}E_2\left(4z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)\right) + \frac{-1}{12}f_E(z).\end{aligned}$$

Let $\sigma(n) := \sigma_1(n) = \sum_{d|n} d$, and define the arithmetic functions

$$\begin{aligned}\mu_1(n) &:= \sum_{\substack{d|n\\ d\not\equiv 0 \pmod 2}} d,\\ \mu_2(n) &:= \sum_{\substack{d|n\\ d\not\equiv 0 \pmod 3}} d,\\ \mu_3(n) &:= \left(\frac{n}{3}\right)\sigma(n).\end{aligned}$$

Extend these to $\mathbb{Q}$ by setting $\mu_i(r) = 0$ for $r \in \mathbb{Q}\backslash\mathbb{Z}$ $(i = 1, 2, 3)$. Comparing nth coefficients, we have the following proposition.

Proposition 4.

$$\begin{aligned}\sum_{|s|<\sqrt{n}}^{*} H\left(n-s^2\right) = {} & -\frac{1}{16}\mu_1(n) + \frac{3}{16}\mu_2(n) - \frac{1}{24}\mu_3(n) - \frac{1}{2}\mu_1(n/2)\\ & + \frac{1}{4}\mu_1(n/3) - \frac{3}{16}\mu_1(n/9) + 2\mu_1(n/6) - \frac{3}{2}\mu_1(n/18)\\ & - \frac{3}{16}\mu_2(n/3) - \frac{1}{8}\mu_3(n/2) - \frac{1}{3}\mu_3(n/4) - \frac{1}{12}a(n),\end{aligned}$$

where the * *denotes the fact that if* $n \equiv 1 \pmod 3$*, we take the sum over all* $s \equiv 0 \pmod 3$*; if* $n \equiv 2 \pmod 3$*, we take the sum over all* $s \equiv \pm 1 \pmod 3$*.*

Using (4) and the fact that $a(n) = 0$ if $(n, 6) > 1$, we are able to extract the identities

$$\sum_{\substack{|r|<2\sqrt{p}\\ r\equiv c \pmod 3}} H\left(4p-r^2\right) = \begin{cases}\frac{p+1}{2}, & \text{if } p \equiv 1 \pmod 3,\ c = 0,\\ \frac{p+1}{2}, & \text{if } p \equiv 2 \pmod 3,\ c = 1 \text{ or } 2.\end{cases}$$

So, using (1), we are able to obtain Theorem 3 as a corollary.

At this point, we also note that there is a more general identity than (1), which is due to Hurwitz. See [2, p. 236]. In particular, if we let $\lambda(n) := \frac{1}{2}\sum_{d|n} \min(d, n/d)$, then

$$\sum_{|r|<2\sqrt{N}} H\left(4N - r^2\right) = 2\sigma(N) - 2\lambda(N).$$

So, this identity together with Proposition 4 makes it possible to generalize Theorem 3 for p not necessarily prime.

In addition, if we study the cusp form in our basis carefully, we can extract other nice formulae as well. For example, we can use the fact that $a(p) = 0$ if $p \equiv 2 \pmod 3$ to obtain Theorem 5. □

4. The Eichler–Selberg trace formula and Hurwitz class numbers

The Eichler–Selberg trace formula gives the value of the trace of the nth Hecke operator acting on $\mathcal{S}_k(N, \psi)$. The following gives a formula for computing the trace in a specific setting, which is useful for our purposes. The trace formula is, in fact, much more general and we refer the reader to [7, pp. 12–13] for more details.

Theorem 10. *Let p be a prime. The trace of the pth Hecke operator acting on $\mathcal{S}_2(N)$ is given by*

$$\operatorname{tr}_{2,N}(T_p) = p + 1 - \sum_{s\in H} \frac{1}{p-1} \sum_{f|t} \frac{1}{2}\phi\left(\left(s^2 - 4p\right)^{1/2}/f\right) \prod_{l|N} c(s, f, l)$$

$$- \sum_{s\in E_1\cup E_2} \frac{1}{2} \sum_{f|t} \frac{h((s^2-4p)/f^2)}{\omega((s^2-4p)/f^2)} \prod_{l|N} c(s, f, l),$$

where $H = \{s\colon s^2 - 4p = t^2\}$, $E_1 = \{s\colon s^2 - 4p = t^2 m,\ 0 > m \equiv 1 \pmod 4\}$, and $E_2 = \{s\colon s^2 - 4p = t^2 4m,\ 0 > m \equiv 2, 3 \pmod 4\}$.

Here, ϕ is the Euler ϕ-function. For $d < 0$, $h(d)$ is the class number of the order of $\mathbb{Q}(\sqrt{d})$ of discriminant d, and $\omega(d)$ is $1/2$ the cardinality of its unit group. For a prime $l \mid N$, $c(s, f, l)$ essentially counts the number of solutions to a certain system of congruences.

It is well known that if $s \in E_1 \cup E_2$, then

$$H\left(4p - s^2\right) = \sum_{f|t} \frac{h((s^2-4p)/f^2)}{\omega((s^2-4p)/f^2)}.$$

In fact, one may even define the Hurwitz class number in this way. See [3, p. 318]. So, if it is possible to control the $c(s, f, l)$—in particular, if it is possible to make them constant with respect to f, then there is hope that Hurwitz class number relations may be extracted from the trace formula. Indeed, if p is quadratic nonresidue modulo l for all primes l dividing N, then the computation of $c(s, f, l)$ is quite simple and does not depend on f.

For example, if we apply the trace formula to T_p acting on $\mathcal{S}_2(7) = \{0\}$ for $p \equiv 3, 5, 6 \pmod 7$,

$$c(s, f, l) = \begin{cases} 2, & p \equiv 3 \pmod 7,\ s \equiv 0, \pm 3, \\ 2, & p \equiv 5 \pmod 7,\ s \equiv 0, \pm 1, \\ 2, & p \equiv 6 \pmod 7,\ s \equiv 0, \pm 2, \\ 0, & \text{otherwise.} \end{cases}$$

The resulting Hurwitz class number relation is the following.

Proposition 5.

$$\sum_{|s|<2\sqrt{p}}^{*} H\left(4p - s^2\right) = p - 1,$$

where the * *denotes the fact that if* $p \equiv 3 \pmod 7$*, the sum is over all* $s \equiv 0, \pm 3 \pmod 7$*; if* $p \equiv 5 \pmod 7$*, the sum is over all* $s \equiv 0, \pm 1 \pmod 7$*; and if* $p \equiv 6 \pmod 7$*, the sum is over all* $s \equiv 0, \pm 2 \pmod 7$.

Combining the above proposition with the cases of Theorem 6 that were proven in Section 2, we are able to obtain the remaining formulae in the theorem.

5. Conjectures

For all primes p sufficiently large, Tables 1 and 2 give conjectured values for the sum

$$\sum_{\substack{|r|<2\sqrt{p} \\ r \equiv c \pmod m}} H\left(4p - r^2\right).$$

These values have been checked for primes $p < 1{,}000{,}000$. Where an entry is bold and marked by asterisks, the formula is handled by a theorem somewhere in this paper; where an entry is blank, we were not able to recognize any simple pattern from the computations.

We note that for $m = 5$ and 7, neither the curve counting method of Section 2 alone nor the basis of modular forms approach of Section 3 alone will be sufficient for a complete characterization of these sums. Rather a combination of the two methods should work.

For making further progress on Tables 1 and 2, it appears that the method of Section 3 will be most fruitful. The difficulty in using this method is that, in each case, the group G_m (defined in Theorem 9) is strictly contained in $\Gamma_0(4m^2)$. So, we will need a much larger basis of modular forms. Certainly a basis for $\mathcal{M}_2(\Gamma_1(4m^2))$ would be sufficient. However, to completely fill in the

Table 1
$m = 5$

	$c = 0$	$c = \pm 1$	$c = \pm 2$
$p \equiv 1 \pmod 5$	$\frac{(p+1)}{2}$	$\frac{(p+1)}{3}$	$\frac{(5p-7)}{12}$
$p \equiv 2 \pmod 5$	$\frac{(p+1)}{3}$	$\frac{(p+1)}{3}$	$*\mathbf{\frac{(p-1)}{2}}*$
$p \equiv 3 \pmod 5$	$\frac{(p+1)}{3}$	$*\mathbf{\frac{(p-1)}{2}}*$	$\frac{(p+1)}{3}$
$p \equiv 4 \pmod 5$	$*\mathbf{\frac{(p-3)}{2}}*$	$\frac{(5p+5)}{12}$	$\frac{(p+1)}{3}$

Table 2
$m = 7$

	$c = 0$	$c = \pm 1$	$c = \pm 2$	$c = \pm 3$
$p \equiv 1 \pmod 7$		$\frac{(p+1)}{3}$		
$p \equiv 2 \pmod 7$				$*\frac{(p-2)}{3}*$
$p \equiv 3 \pmod 7$	$*\frac{(p+1)}{3}*$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$*\frac{(p-2)}{3}*$
$p \equiv 4 \pmod 7$			$*\frac{(p-2)}{3}*$	
$p \equiv 5 \pmod 7$	$*\frac{(p+1)}{3}*$	$*\frac{(p-2)}{3}*$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$
$p \equiv 6 \pmod 7$	$*\frac{(p-5)}{3}*$	$\frac{(p+1)}{4}$	$*\frac{(p+1)}{3}*$	$\frac{(p+1)}{4}$

table, another method will be needed. Perhaps an adaptation of the curve counting method of Section 2 for $p \equiv 1 \pmod m$ would be best. The main obstacle to overcome is that one must deal with the presence of full m-torsion curves when $p \equiv 1 \pmod m$.

In general, for a prime m, we note that the curve counting method will give proofs for $c \equiv \pm(p+1) \pmod m$. We also note that, for primes $m \equiv 1 \pmod 4$, the basis of forms method will give proofs for the cases when $4p - c^2$ is not a square; and for primes $m \equiv 3 \pmod 4$, the basis of forms method will give proofs for the cases when $4p - c^2$ is a square. Thus, for a prime m, we will obtain half the cases from the basis of forms approach and we will obtain $2(m-1)+1$ more from the curve counting approach assuming that the case $p \equiv 1 \pmod m$ can be adequately handled. So, at least for primes greater than 7, a third method will be necessary to fully characterize how the sum splits.

Acknowledgments

The authors would like to thank Ken Ono for suggesting that we consider the Eichler–Selberg trace formula. The authors would also like to thank Robert Osburn for helpful conversation.

References

[1] Henri Cohen, Sums involving the values at negative integers of L-functions of quadratic characters, Math. Ann. 217 (3) (1975) 271–285.
[2] Henri Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, New York, 1996.
[3] David A. Cox, Primes of the Form $x^2 + ny^2$, Wiley–Interscience, New York, 1989.
[4] Max Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272.
[5] Martin Eichler, On the class of imaginary quadratic fields and the sums of divisors of natural numbers, J. Indian Math. Soc. (N.S.) 19 (1955) 153–180.
[6] Gerhard Frey, Construction and arithmetical applications of modular forms of low weight, in: Elliptic Curves and Related Topics, in: CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 1–21.
[7] Hiroaki Hijikata, Arnold K. Pizer, Thomas R. Shemanske, The basis problem for modular forms on $\Gamma_0(N)$, Mem. Amer. Math. Soc. 82 (418) (1989), vi+159 pp.
[8] F. Hirzebruch, D. Zagier, Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus, Invent. Math. 36 (1976) 57–113.
[9] Thomas W. Hungerford, Algebra, Springer-Verlag, New York, 1974.
[10] Anthony W. Knapp, Elliptic Curves, Princeton Univ. Press, Princeton, 1992.
[11] Neal Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1993.
[12] H.W. Lenstra Jr., Factoring integers with elliptic curves, Ann. of Math. (2) 126 (3) (1987) 649–673.
[13] Toshitsune Miyake, Modular Forms, Springer-Verlag, New York, 1989.

[14] Goro Shimura, On modular forms of half integral weight, Ann. of Math. (2) 97 (1973) 440–481.
[15] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.
[16] Don Zagier, Nombres de classes et formes modulaires de poids 3/2, C. R. Acad. Sci. Paris Sér. A–B 281 (21) (1975), Ai, A883–A886.