2, 3, 5, Legendre: ±Trace Ratios in Families of Elliptic Curves

Nicholas M. Katz

CONTENTS

2000 AMS Subject Classification: 11G15, 11G20, 14G15, 14H52, 14K22

Keywords: Elliptic curve, finite field, trace of Frobenius, canonical lifting

For a given integer A and various families of elliptic curves over finite fields, we compare the number of occurrences of A with the number of occurrences of $-A$ as the trace of Frobenius in the family.

1. INTRODUCTION

The Legendre family of elliptic curves over the λ-line,

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

is one of the most familiar, and most studied, families of elliptic curves, often used for testing conjectures and for illustrating theorems. When we became interested in the Lang–Trotter conjecture [Lang and Trotter 76, p. 33] in the function-field case (cf. [Katz 09]), we turned to this family to do some computer experiments. This paper reports on an empirical discovery made in the course of those experiments, and on the theory that explains it. The explanation owes a great deal to Deligne, as will become clear below.

In the experiments, we took an odd prime p, and tabulated, for each $\lambda_0 \in \mathbb{F}_p \setminus \{0,1\}$, the "trace of Frobenius" $A(\lambda_0, \mathbb{F}_p) \in \mathbb{Z}$ for the elliptic curve E_{λ_0} over $\mathbb{F}_p$. Concretely, we have

$$\#E_{\lambda_0}(\mathbb{F}_p) = p + 1 - A(\lambda_0, \mathbb{F}_p).$$

We calculated the numbers $A(\lambda_0, \mathbb{F}_p)$ brutally, as the character sums

$$A(\lambda_0, \mathbb{F}_p) = -\sum_{x \in \mathbb{F}_p} \chi_2(x(x-1)(x-\lambda_0)).$$

Here $\chi_2 : \mathbb{F}_p \to \{0, \pm 1\}$ is the quadratic character of $\mathbb{F}_p^\times$, extended to all of $\mathbb{F}_p$ by $\chi_2(0) := 0$.

The original intention of the experiment was to see, for large primes p, which integers A occurred, and how often they occurred, as $A(\lambda_0, \mathbb{F}_p)$ for some $\lambda_0 \in \mathbb{F}_p \setminus \{0,1\}$.

1058-6458/2010 $ 0.50 per page

	$\mathbf{ord_2(p-1)}$							
$\mathbf{ord_2(p+1-A)}$	2	3	4	5	6	7	8	9
3	2	2	2	2	2	2	2	2
4	3	?	?	?	?	?	?	?
5	5	7/2	7/2	7/2	7/2	7/2	7/2	7/2
6	5	4	?	?	?	?	?	?
7	5	5	17/4	17/4	17/4	17/4	17/4	17/4
8	5	5	9/2	?	?	?	?	?
9	5	5	5	37/8	37/8	37/8	37/8	37/8
10	5	5	5	19/4	?	?	?	?
11	5	5	5	5	77/16	77/16	77/16	77/16
12	5	5	5	5	39/8	?	?	?
13	5	5	5	5	5	157/32	157/32	157/32
14	5	5	5	5	5	79/16	?	?

TABLE 1. Ratios as a function of $\mathrm{ord}_2(p-1)$ and $\mathrm{ord}_2(p+1-A)$.

There are two obvious constraints on which values of A can occur at all. The first is the Hasse bound

$$|A(\lambda_0, \mathbb{F}_p)| \leq 2\sqrt{p}.$$

The second is a congruence condition modulo 4. Recall that $E_{\lambda_0}(\mathbb{F}_p)$ has the structure of a (finite) abelian group, with the point at ∞ as the origin and with the three points $(0,0), (1,0), (\lambda_0, 0)$ as the nontrivial points of order 2. Thus the points of $E_{\lambda_0}(\mathbb{F}_p)$ of order dividing 2 form a subgroup of order 4, and hence $\#E_{\lambda_0}(\mathbb{F}_p) \equiv 0 \bmod 4$; in terms of $A(\lambda_0, \mathbb{F}_p)$ this gives the congruence

$$A(\lambda_0, \mathbb{F}_p) \equiv p + 1 \bmod 4.$$

So for primes $p \equiv -1 \bmod 4$, the only possible A's are those integers congruent to 0 modulo 4 that are at most $2\sqrt{p}$ in absolute value, while for $p \equiv 1 \bmod 4$, the only possible A's are those integers congruent to 2 modulo 4 that are at most $2\sqrt{p}$ in absolute value. Let us say that such A's are *unobstructed* for p. What will be essential in a moment is the observation that if A is unobstructed for p, then so is $-A$.

The experiments showed (empirically) that for a given odd p, any unobstructed A does in fact occur. This was not surprising, and had a simple explanation. The experiments also showed that when $p \equiv -1 \bmod 4$, A and $-A$ occur equally often. This, too, had a simple explanation.

But for $p \equiv 1 \bmod 4$, we found something quite unexpected. It was no longer the case that A and $-A$ occurred equally often: there was always a winner and a loser (in terms of which occurred more often). The winner was apparently determined by the following rule. Because $A \equiv 2 \bmod 4$, exactly one of A and $-A$ has $p + 1 - A \equiv 0 \bmod 8$, call it A, and for this choice, we have $p + 1 + A \equiv 4 \bmod 8$. Then A was the winner, and $-A$ the loser. In other words, among the curves in the Legendre family with a given value of $|A|$, the curves whose rational 2-power torsion consisted only of the four given points were less plentiful than those whose rational 2-power torsion subgroup had at least eight points.

We then examined the ratios of winners to losers in each unobstructed pair $(A, -A)$. We were astounded that for $p \equiv 5 \bmod 8$, this ratio was (empirically) always an integer, in fact, always one of the integers $2, 3, 5$. For example, here is the list, for $p = 277$, of all the pairs of the form (an unobstructed A, the number of times it occurs):

$$\begin{array}{llll} (-30, 4), & (30, 8), & (-26, 24), & (26, 8), \\ (-22, 8), & (22, 40), & (-18, 18), & (18, 9), \\ (-14, 8), & (14, 16), & (-10, 50), & (10, 10), \\ (-6, 6), & (6, 18), & (-2, 32), & (2, 16). \end{array}$$

Moreover, there was apparently a simple rule to determine the ratio, depending only on the power of 2 that divides $p + 1 - A$:

$$\begin{aligned} \mathrm{ord}_2(p + 1 - A) = 3 &\implies \text{ratio} = 2, \\ \mathrm{ord}_2(p + 1 - A) = 4 &\implies \text{ratio} = 3, \\ \mathrm{ord}_2(p + 1 - A) \geq 5 &\implies \text{ratio} = 5. \end{aligned}$$

For $p \equiv 1 \bmod 8$, the situation was more complicated. All the ratios were at least 2, some were 2, 3, or 5, but others were fractions with powers of 2 in their denominators, and occasionally 4 appeared. The data suggested the ratios listed in Table 1 as a function of $\mathrm{ord}_2(p-1)$, listed horizontally, and $\mathrm{ord}_2(p+1-A)$, listed vertically. For example, the first column of the table exhibits the $2,3,5$ ratio phenomenon for primes $p \equiv 5 \bmod 8$.

The entries with a question mark indicate that more than one ratio can occur for the given ord_2 values. For example, $p = 233$ has $\mathrm{ord}_2(p-1) = 3$, and each of $A = -6, 26$ has $\mathrm{ord}_2(p+1-A) = 4$. Yet their ratios are $7/4$ and $17/4$. Similarly, $p = 1993$ has $\mathrm{ord}_2(p-1) = 3$, and each of $A = -70, -38, -6, 26, 58$ has $\mathrm{ord}_2(p+1-A) = 4$, but their ratios are respectively $19/4, 7/2, 5, 7/2, 17/4$.

Deligne's contribution to the explanation of these phenomena was twofold. He pointed out that the Legendre family is isogenous to the universal family of elliptic curves endowed with a point of order four. He also gave a proof of the $2,3,5$ phenomenon for $p \equiv 5 \bmod 8$ by an argument working on the tree of $\mathrm{GL}(2, \mathbb{Q}_2)$: in his argument, the fundamental invariant determining the ratio was not $\mathrm{ord}_2(p+1-A)$ but rather the 2-adic behavior of the discriminant $A^2 - 4p$. Both of these ideas—working on the moduli problem $\Gamma_1(4)$ and paying attention to the 2-adic behavior of the discriminant—are crucial to the explanation we give below.

In the penultimate section, we discuss ± trace ratio phenomena for some other families. In the final section, we discuss some other sorts of ratio questions.

2. STATEMENT OF RESULTS

Although our computer experiments were done entirely over prime fields $\mathbb{F}_p$ for odd primes p, the same phenomena persist over all their finite extension fields $\mathbb{F}_q/\mathbb{F}_p$: for $\lambda_0 \in \mathbb{F}_q \setminus \{0,1\}$, we have the elliptic curve E_{λ_0} over $\mathbb{F}_q$ and the integer $A(\lambda_0, \mathbb{F}_q) \in \mathbb{Z}$ given by

$$\#E_{\lambda_0}(\mathbb{F}_q) = q + 1 - A(\lambda_0, \mathbb{F}_q).$$

There is, however, one difference between working only over $\mathbb{F}_p$ and working over general $\mathbb{F}_q/\mathbb{F}_p$, and that is the issue of supersingular elliptic curves. Recall that E_{λ_0} over $\mathbb{F}_q$ is called supersingular if $p \mid A(\lambda_0, \mathbb{F}_q)$, and that in that case, $A(\lambda_0, \mathbb{F}_q)$ is in fact divisible by $\sqrt{q}$ as an algebraic integer. In other words, if $q = p^{2k}$, then $p^k \mid A(\lambda_0, \mathbb{F}_q)$, while if $q = p^{2k+1}$, then $p^{k+1} \mid A(\lambda_0, \mathbb{F}_q)$.

Before we can analyze completely exactly which supersingular values of $A(\lambda_0, \mathbb{F}_q)$ can occur, we must introduce another family of elliptic curves closely related to the Legendre family, the family over the t-line, $t \neq 0, 1/4$, namely

$$y^2 = (x+t)(x^2+x+t).$$

The point $P_4 := (0,t)$ has order 4, and $2P_4$ is the point $P_2 := (-t, 0)$. One knows that this family with its P_4 is the universal curve given with a point of order 4, over any $\mathbb{Z}[1/2]$-scheme. In other words, the modular curve $\mathcal{M}_{\Gamma_1(4)}/\mathbb{Z}[1/2]$ is

$$\mathrm{Spec}(\mathbb{Z}[1/2][t][1/(t(1-4t))]),$$

with $y^2 = (x+t)(x^2+x+t), P_4$ the universal curve. We will call this the $\Gamma_1(4)$ family.

Its relation to the Legendre family is that under the 2-isogeny "divide by the $\mathbb{Z}/2Z$ generated by P_2," it becomes the Legendre family, with $\lambda = 1 - 4t$. Because isogenous elliptic curves over $\mathbb{F}_q$ have the same number of rational points, questions about the A's in the Legendre family are exactly the same as questions about the A's in the $\Gamma_1(4)$ family.

Lemma 2.1. *Let p be an odd prime.*

(1) *If $q = p^{2k+1}$ and if E_{λ_0} over $\mathbb{F}_q$ is supersingular, then $A(\lambda_0, \mathbb{F}_q) = 0$.*

(2) *If $q = p^{2k}$ and if E_{λ_0} over $\mathbb{F}_q$ is supersingular, then $A(\lambda_0, \mathbb{F}_q) = \epsilon 2p^k$, where $\epsilon = \pm 1$ is the choice of sign for which $\epsilon p^k \equiv 1 \bmod 4$.*

Proof. (1) Here $p^{k+1} \mid A(\lambda_0, \mathbb{F}_q)$. So if $A(\lambda_0, \mathbb{F}_q)$ were nonzero, its absolute value would be at least p^{k+1}. This exceeds the Weil bound $2\sqrt{q} = 2\sqrt{p}p^k$ for all $p \geq 5$. If $p = 3$, the two values $\pm p^{k+1}$ for $A(\lambda_0, \mathbb{F}_q)$ are allowed by the Weil bound, but they fail the congruence

$$q + 1 \equiv A(\lambda_0, \mathbb{F}_q) \bmod 4.$$

For (2), $p^k \mid A(\lambda_0, \mathbb{F}_q)$, so the nonzero values allowed by the Weil bound are $0, \pm p^k$, and $\pm 2p^k$. The congruence modulo 4 rules out both 0 and either choice of $\pm p^k$. Thus $A = \epsilon 2p^k$ for some choice of $\epsilon = \pm 1$. Then Frob_q, the characteristic polynomial of Frobenius, is $X^2 - AX + q = (X - \epsilon p^k)^2$, and hence $\mathrm{Frob}_q = \epsilon p^k$. But on a curve in the $\Gamma_1(4)$-family, we have a rational point of order 4, so fixed by $\mathrm{Frob}_q = \epsilon p^k$, and hence $\epsilon p^k \equiv 1 \bmod 4$. □

Remark 2.2. Thus when $q = p^{2k}$, the supersingular A's in the Legendre family are all the same choice of $\pm 2p^k$; the other choice never occurs in the Legendre family. So if we are to speak of ratios of A to $-A$, we must restrict to the ordinary members of the family, i.e., those whose A is prime to p. This was not an issue in working over $\mathbb{F}_p$, where the only possible supersingular A is 0.

We next explain the easy parts of what our experiments showed.

Lemma 2.3. *Suppose $q \equiv -1 \bmod 4$. Then A and $-A$ occur equally often in the Legendre family over $\mathbb{F}_q$.*

Proof. Denote by χ_2 the quadratic character of $\mathbb{F}_q$. Then $\chi_2(-1) = -1$. On the other hand,

$$A(\lambda_0, \mathbb{F}_q) = -\sum_{x \in \mathbb{F}_q} \chi_2(x(x-1)(x-\lambda_0)).$$

Elementary manipulation of this sum shows that

$$A(1-\lambda_0, \mathbb{F}_q) = \chi_2(-1)A(\lambda_0, \mathbb{F}_q).$$

Since $\chi_2(-1) = -1$, the involution $\lambda \mapsto 1-\lambda$ matches A's to $-A$'s, and shows that $A(1/2, \mathbb{F}_q) = 0$. □

In fact, as Deligne pointed out to me, this is a special case of the following general fact, of which the preceding lemma is the $N = 4$ case.

Lemma 2.4. *Let $\mathbb{F}_q$ be a finite field, $N \geq 4$ an integer invertible in $\mathbb{F}_q$, and consider the $\Gamma_1(N)$ family, i.e., the universal curve over the modular curve $\mathcal{M}_{\Gamma_1(N)}/\mathbb{F}_q$. Suppose $q \equiv -1 \bmod N$. Then A and $-A$ occur equally often as traces of Frobenius in the $\Gamma_1(N)$ family over $\mathbb{F}_q$.*

Proof. The Atkin–Lehner involution

$$(E, \mathbb{Z}/N\mathbb{Z} \hookrightarrow E) \mapsto (E/(\mathbb{Z}/N\mathbb{Z}), \text{ dual } \mu_N \hookrightarrow E)$$

is an A-preserving bijection from the $\Gamma_1(N)$ moduli problem of giving an inclusion of $\mathbb{Z}/N\mathbb{Z}$ to the $\Gamma_1(N)^{\text{arith}}$ moduli problem of giving an inclusion of μ_N. Since $q \equiv -1 \bmod N$, the quadratic twist of μ_N over $\mathbb{F}_q$ is $\mathbb{Z}/N\mathbb{Z}$, so forming the quadratic twist gives a bijection from the $\mathbb{F}_q$ points of the $\Gamma_1(N)^{\text{arith}}$ moduli problem back to the $\mathbb{F}_q$ points of the $\Gamma_1(N)$ moduli problem that reverses the sign of A.

The composition, attaching to an $\mathbb{F}_q$ point of the $\Gamma_1(N)$ family the quadratic twist of its Atkin–Lehner involute, is a sign-reversing involution. □

Lemma 2.5. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, $A \in \mathbb{Z}$ an integer prime to p with $|A| \leq 2\sqrt{q}$. If $A \equiv q + 1 \bmod 4$, there exists $\lambda_0 \in \mathbb{F}_q \backslash \{0, 1\}$ with $A(\lambda_0, \mathbb{F}_q) = A$.*

Proof. Translated into the same statement about the $\Gamma_1(4)$ family, this is a special case of [Katz 09, Lemma 4.3 (3)]. □

Remark 2.6. Indeed, for any $N \geq 4$ invertible in $\mathbb{F}_q$, any integer A prime to p with $|A| \leq 2\sqrt{q}$ and $A \equiv q + 1 \bmod N$ occurs as the trace at some $\mathbb{F}_q$-point of the $\Gamma_1(N)$ family; cf. [Katz 09, Lemma 4.3 (3)].

We now turn to the $2, 3, 5$ phenomenon when $q \equiv 5 \bmod 8$, and more generally to the ratios that occur when $q \equiv 1 \bmod 4$.

Suppose, for the rest of this section, that $q \equiv 1 \bmod 4$, and fix an integer A prime to p with $|A| < 2\sqrt{q}$ and $A \equiv 2 \bmod 4$. Replacing if necessary A by $-A$, we have

$$q + 1 - A \equiv 0 \bmod 8, \quad q + 1 + A \equiv 4 \bmod 8.$$

We are concerned with the ratio of occurrences of A to occurrences of $-A$ in the $\mathbb{F}_q$ points of the Legendre family, or equivalently in the $\mathbb{F}_q$ points of the $\Gamma_1(4)$ family. Write

$$\Delta := A^2 - 4q.$$

Deligne's explanation of the $2, 3, 5$ phenomenon is the following theorem.

Theorem 2.7. (Deligne.) *Suppose $q \equiv 5 \bmod 8$. Then $\text{ord}_2(\Delta) = 4$, and we have*

$$\begin{aligned} \Delta/16 \equiv 3 \text{ or } 7 \bmod 8 &\implies \textit{ratio} = 2, \\ \Delta/16 \equiv 5 \bmod 8, &\implies \textit{ratio} = 3, \\ \Delta/16 \equiv 1 \bmod 8, &\implies \textit{ratio} = 5. \end{aligned}$$

It is elementary that this is equivalent to the following theorem; see the explication just below.

Theorem 2.8. *Suppose $q \equiv 5 \bmod 8$. Then*

$$\begin{aligned} \text{ord}_2(q + 1 - A) = 3 &\implies \textit{ratio} = 2, \\ \text{ord}_2(q + 1 - A) = 4 &\implies \textit{ratio} = 3, \\ \text{ord}_2(q + 1 - A) \geq 5 &\implies \textit{ratio} = 5. \end{aligned}$$

Remark 2.9. In general, if we are told that $\text{ord}_2(q + 1 - A) = n \geq 3$, write $A = q + 1 + (\text{odd})2^n$. Then $A^2 = (q+1)^2 + (\text{odd})2^{n+2}$, and $\Delta := A^2 - 4q = (q-1)^2 + (\text{odd})2^{n+2}$. So if $\text{ord}_2(q-1) = m \geq 2$, then $q - 1 = (\text{odd})2^m$, and so $(q-1)^2 = 2^{2m}(\text{odd}^2)$. For $q \equiv 5 \bmod 8$, we have $\Delta = 16(\text{odd}^2) + (\text{odd})2^{n+2}$. Since $n \geq 3$, we have $\Delta/16 = \text{odd}^2 + 2^{n-2}(\text{odd})$. Now $\text{odd}^2 \equiv 1 \bmod 8$, so we have $\Delta/16 \equiv 1 + 2^{n-2}(\text{odd}) \bmod 8$. Thus $n = 3$ yields that $\Delta/16$ is $1 + 2(\text{odd})$ modulo 8, so 3 or 7; for $n = 4$, $\Delta/16$ is $1 + 4(\text{odd})$ modulo 8, so 5; and for $n \geq 5$, $\Delta/16$ is 1 modulo 8.

In fact, when $\text{ord}_2(q+1-A) = 3$, we have the following more general result.

Theorem 2.10. *Suppose* $q \equiv 1 \bmod 4$. *Then*

$$\operatorname{ord}_2(q+1-A) = 3 \implies \textit{ratio} = 2.$$

The remaining cases are covered by the following theorem.

Theorem 2.11. *Suppose that* $q \equiv 1 \bmod 8$, *and that* $\operatorname{ord}_2(q+1-A) \geq 4$. *Then* $\operatorname{ord}_2(\Delta) \geq 6$, *and we have the following results:*

(1) *Suppose* $\operatorname{ord}_2(\Delta) = 2k+1$, $k \geq 3$. *Then ratio* $= 5 - 3/2^{k-2}$.

(2) *Suppose* $\operatorname{ord}_2(\Delta) = 2k$, $k \geq 3$. *Then*

 (a) *if* $\Delta/2^{2k} \equiv 1 \bmod 8$, *then ratio* $= 5$,

 (b) *if* $\Delta/2^{2k} \equiv 3 \text{ or } 7 \bmod 8$, *then ratio* $= 5-3/2^{k-2}$,

 (c) *if* $\Delta/2^{2k} \equiv 5 \bmod 8$, *then ratio* $= 5 - 1/2^{k-3}$.

We can combine the statements of Theorems 2.7 and 2.11 (and the proof of Theorem 2.10) into one summarizing theorem. Observe that the $k = 2$ cases of assertions (2)(b) and (2)(c) produce the ratios 2 and 3, and that the $k = 3$ case of statement (2)(c) produces the ratio 4.

Theorem 2.12. *Suppose that* $q \equiv 1 \bmod 4$. *Then* $\operatorname{ord}_2(\Delta) \geq 4$, *and we have the following results:*

(1) *Suppose* $\operatorname{ord}_2(\Delta) = 2k+1$, $k \geq 2$. *Then ratio* $= 5 - 3/2^{k-2}$.

(2) *Suppose* $\operatorname{ord}_2(\Delta) = 2k$, $k \geq 2$. *Then*

 (a) *if* $\Delta/2^{2k} \equiv 1 \bmod 8$, *then ratio* $= 5$,

 (b) *if* $\Delta/2^{2k} \equiv 3 \text{ or } 7 \bmod 8$, *then ratio* $= 5-3/2^{k-2}$,

 (c) *if* $\Delta/2^{2k} \equiv 5 \bmod 8$, *then ratio* $= 5 - 1/2^{k-3}$.

In the same way that Theorem 2.7 implies Theorem 2.8, this Δ result implies the correctness of the table of ratios we were able to surmise when the ratio seemed to depend only on $\operatorname{ord}_2(q+1-A)$ and on $\operatorname{ord}_2(q-1)$.

Theorem 2.13. *Suppose that* $q \equiv 1 \bmod 4$. *Then we have the following results:*

(1) *If* $\operatorname{ord}_2(q+1-A) = 2k+1$ *and* $2 \leq \operatorname{ord}_2(q-1) \leq k$, *then ratio* $= 5$.

(2) *If* $\operatorname{ord}_2(q+1-A) = 2k+1$ *and* $\operatorname{ord}_2(q-1) \geq k+1$, *then ratio* $= 5 - 3/2^{k-1}$.

(3) *If* $\operatorname{ord}_2(q+1-A) = 2k$ *and* $2 \leq \operatorname{ord}_2(q-1) < k$, *then ratio* $= 5$.

(4) *If* $\operatorname{ord}_2(q+1-A) = 2k$ *and* $\operatorname{ord}_2(q-1) = k$, *then ratio* $= 5 - 1/2^{k-3}$.

3. BACKGROUND FOR THE PROOF

To prove the ratio theorems, we use Deuring-style class number formulas, which, for a given integer A that is prime to p, count the number of $\mathbb{F}_q$ points with given trace A on $\mathcal{M}_{\Gamma_1(4)}$. Our key (and only) insight is that while these formulas are each quite complicated, the *ratio* of the formula for A to that for $-A$ is quite simple.

Let us briefly recall how this works; cf. [Katz 09, Section 4]. Fix an integer A prime to p with $|A| < 2\sqrt{q}$. Then by Honda–Tate there exist elliptic curves $E/\mathbb{F}_q$ whose trace is A. Denote by $\mathbb{Z}[F]$ the ring

$$\mathbb{Z}[F] := \mathbb{Z}[X]/(X^2 - AX + q),$$

an order in the quadratic imaginary field $K := \mathbb{Q}[X]/(X^2 - AX + q)$, whose ring of integers we denote by $\mathcal{O}_K$. For each intermediate order

$$\mathbb{Z}[F] \subset R \subset \mathcal{O}_K,$$

we have its finite class group $\operatorname{Pic}(\operatorname{Spec}(R))$ of order denoted by $h(R)$, its finite unit group $R^\times$, and its "normalized" class number

$$h^\star(R) := h(R)/\#R^\times.$$

Now fix a complex embedding of the Witt vectors $W(\mathbb{F}_q) \subset \mathbb{C}$. By a fundamental result of Deligne, taking the first integer homology group of (the $\mathbb{C}$ points of) the canonical lifting $E^{\text{can}}/W(\mathbb{F}_q)$ of $E/\mathbb{F}_q$, we have that

$$E/\mathbb{F}_q \mapsto H(E) := H_1(E^{\text{can}}(\mathbb{C}), \mathbb{Z})$$

is an equivalence of categories between elliptic curves $E/\mathbb{F}_q$ whose trace is A and $\mathbb{Z}[F]$ modules that are $\mathbb{Z}$-free of rank 2. In this equivalence, the $\mathbb{Z}[F]$-linear endomorphisms of $H(E)$ are an order $\mathbb{Z}[F] \subset R \subset \mathcal{O}_K$, and $H(E)$ is an invertible module over this order R. (And by the equivalence, $R = \operatorname{End}_{\mathbb{F}_q}(E)$.)

Moreover, for any integer N prime to p, the group $E(\overline{\mathbb{F}_q})[N]$ as a $\operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ module, with generator of $\operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ taken to be the *arithmetic* Frobenius F, is $\mathbb{Z}[F]$-isomorphic to R/NR. Thus a $\Gamma_1(N)$ structure on

$E/\mathbb{F}_q$ is an F-fixed point of R/NR that has order N, a $\Gamma_0(N)$ structure is an F-stable subgroup of R/NR that is cyclic of order N, and an unoriented $\Gamma(N)$-structure is an F-fixed basis of R/NR as a $\mathbb{Z}/N\mathbb{Z}$ module.

So for any level-structure moduli problem $\mathcal{M}$, if $E/\mathbb{F}_q$ is an ordinary elliptic curve with trace A and endomorphism ring R, the number of $\mathcal{M}$-structures on $E/\mathbb{F}_q$ depends only on the data (A, q, R). We denote it by

$$\#\mathcal{M}(A, q, R).$$

For example, if $\mathcal{M} = \mathcal{M}_{\Gamma_1(4)}$, this number is the number of F-fixed points of order 4 in $R/4R$.

Putting this all together, we obtain a class number formula for $\#\mathcal{M}(A, q)$, the number of points on $\mathcal{M}(\mathbb{F}_q)$ with trace A:

$$\#\mathcal{M}(A, q) = \sum_{\text{orders } \mathbb{Z}[F] \subset R \subset \mathcal{O}_K} h^\star(R)\#\mathcal{M}(A, q, R).$$

In order to use this formula, we need to understand how both $h^\star(R)$ and $\#\mathcal{M}(A, q, R)$ vary as R runs over all the intermediate orders $\mathbb{Z}[F] \subset R \subset \mathcal{O}_K$.

Recall that orders in $\mathcal{O}_K$ are of the form $\mathbb{Z} + f\mathcal{O}_K$ for an integer $f = f_R \geq 1$, called the conductor of R; thus f_R is the order of the quotient additive group $\mathcal{O}_K/R$. Given two orders R and R_1 in $\mathcal{O}_K$, we have

$$R \subset R_1 \Longleftrightarrow f_{R_1} \mid f_R.$$

For an order $R \subset \mathcal{O}_K$, the normalized class numbers are related by an Euler-like ϕ_K function

$$\phi_K : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1},$$

defined as follows:

$$\begin{aligned} \phi_K(1) &= 1, \\ \phi_K(nm) &= \phi_K(n)\phi_K(m) \quad \text{if } \gcd(m, n) = 1, \\ \phi_K(\ell^n) &= \ell^{n-1}\phi_K(\ell) \quad \text{for primes } \ell, \end{aligned}$$

and

$$\phi_K(\ell) = \ell - 1,\ \ell, \text{ or } \ell + 1,$$

according to whether ℓ splits in K, ramifies in K, or is inert in K. In terms of ϕ_K we have the relation

$$h^\star(\mathbb{Z} + f\mathcal{O}_K) = \phi_K(f)h^\star(\mathcal{O}_K).$$

What about the numbers $\#\mathcal{M}(A, q, R)$? Let us take the case of $\mathcal{M}_{\Gamma_1(\ell^n)}$, for some prime $\ell \neq p$ with $\ell^n \geq 4$. Then we have the following elementary lemma, whose proof is left to the reader.

Lemma 3.1. *Let $\mathbb{Z}[F] \subset R \subset \mathcal{O}_K$ be an intermediate order, $\ell \neq p$ a prime, and $n \geq d \geq 0$ integers. The following conditions are equivalent:*

1. *The group of F-fixed points in $R/\ell^n R$ is abstractly isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^d\mathbb{Z}$;*
2. *$q + 1 - A \equiv 0 \bmod \ell^{n+d}$, and d is the largest integer $D \in [0, n]$ for which $(F - 1)/\ell^D \in R$.*

Lemma 3.2. *Let N be an integer prime to p. Then $(F - 1)/N \in \mathcal{O}_K$ if and only if the following two conditions are satisfied:*

1. *$q + 1 - A \equiv 0 \bmod N^2$;*
2. *$A \equiv 2 \bmod N$.*

If these conditions hold, then $q \equiv 1 \bmod N$.

Proof. The element $(F - 1)/N$ lies in the fraction field K, so it lies in $\mathcal{O}_K$ if and only its norm and trace lie in $\mathbb{Z}$. But its norm is $(q + 1 - A)/N^2$, and its trace is $(A - 2)/N$. The last assertion comes from comparing these two congruences for A modulo N. □

Lemma 3.3. *Let N be an integer prime to p such that $(F-1)/N \in \mathcal{O}_K$. Denote by f the conductor of $\mathbb{Z}[F]$. Then an intermediate order $\mathbb{Z}[F] \subset R \subset \mathcal{O}_K$, of conductor f_R, contains $(F - 1)/N$ if and only $f_R \mid (f/N)$.*

Proof. The order R contains $(F - 1)/N$ if and only if R contains the order $Z[(F - 1)/N]$, which is the order of conductor f/N, so if and only if $f_R \mid (f/N)$. □

Lemma 3.4. *The conductor f of $\mathbb{Z}[F]$ is related to the discriminant $\Delta := A^2 - 4q$ of $\mathbb{Z}[F]$ by the rule that f is the largest integer M such that $M^2 \mid \Delta$ and $\Delta/M^2 \equiv$* 0 or 1 mod 4.

Proof. Indeed, Δ/f^2 is the discriminant δ_K of $\mathcal{O}_K$. But δ_K is 0 or 1 modulo 4, and if $4 \mid \delta_K$, then $\delta_K/4$ is 2 or 3 modulo 4. □

With this background information, we will prove the ratio theorems, by computing the ratio

$$\#\mathcal{M}_{\Gamma_1(4)}(A, q)/\#\mathcal{M}_{\Gamma_1(4)}(-A, q).$$

We will, in fact, perform a more precise calculation. Denote by f the conductor of $\mathbb{Z}[F]$. Factor

$$f = 2^a f_0$$

with f_0 odd. For each divisor f_1 of f_0, we consider the corresponding f_1-packet, by which we mean the terms in the sum for $\#\mathcal{M}_{\Gamma_1(4)}(A,q)$ involving only those orders R whose conductor is $2^b f_1$ for some b:

$$\#\mathcal{M}_{\Gamma_1(4)}(A,q,f_1) := \sum_{\substack{\text{orders } \mathbb{Z}[F]\subset R\subset \mathcal{O}_K \\ \text{of conductor } 2^b f_1 \text{ for some } b}} h^\star(R)\#\mathcal{M}_{\Gamma_1(4)}(A,q,R).$$

We will compute the ratio

$$\#\mathcal{M}_{\Gamma_1(4)}(A,q,f_1)/\#\mathcal{M}_{\Gamma_1(4)}(-A,q,f_1)$$

for each f_1-packet separately.

For ease of notation, we define

$$R(2^b f_1) := \text{the order of conductor } 2^b f_1.$$

Thus

$$\#\mathcal{M}_{\Gamma_1(4)}(A,q,f_1) = \sum_{b=0}^{a} h^\star(R(2^b f_1))\#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^b f_1)),$$

and the same with A replaced by $-A$.

Our strategy is quite simple. We need to compute the numbers $\#\mathcal{M}_{\Gamma_1(4)}(\pm A,q,R(2^b f_1))$ and $\phi_K(2)$. Since f_1 is odd, we have the following lemma.

Lemma 3.5. *With notation as above, we have*

$$h^\star(R(2^b f_1)) = \phi_K(2^b)h^\star(R(f_1)) = 2^{b-1}\phi_K(2)h^\star(R(f_1)).$$

Lemma 3.6. *For $b < a$, we have $\#\mathcal{M}_{\Gamma_1(4)}(-A,q,R(2^b f_1)) = 0$, and for $b = a$, we have $\#\mathcal{M}_{\Gamma_1(4)}(-A,q,R(2^a f_1)) = 2$.*

Proof. By Lemma 3.2, $(-F-1)/2 = -F + (F-1)/2 \in \mathcal{O}_K$. Suppose first that $b < a$. Then $(-F-1)/2 \in R(2^b f_1)$ by Lemma 3.3. But if $E/\mathbb{F}_q$ is a point of $\mathcal{M}_{\Gamma_1(4)}(-A,q,f_1)$, it has only four rational points of 2-power torsion. Since it has a point of order 4, the group $E(\mathbb{F}_q)[4]$ is cyclic of order 4. Therefore $\mathrm{End}_{\mathbb{F}_q}(E)$ cannot contain $(-F-1)/2$. Thus any point of $\mathcal{M}_{\Gamma_1(4)}(-A,q,f_1)$ has $\mathrm{End}_{\mathbb{F}_q}(E) = R(2^a f_1)$, and has precisely two rational points of order 4. □

Corollary 3.7. *We have*

$$\#\mathcal{M}_{\Gamma_1(4)}(-A,q,f_1) = 2h^\star(R(2^a f_1)).$$

We now compute a, how 2 splits in K, and $\phi_K(2)$, as functions of Δ.

Lemma 3.8. *We have the following results:*

(1) *Suppose* $\mathrm{ord}_2(\Delta) = 2k+1$ *is odd. Then $a = k-1$, 2 ramifies in K, and $\phi_K(2) = 2$.*

(2) *Suppose* $\mathrm{ord}_2(\Delta) = 2k$ *is even. Then*

  (a) *If $\Delta/4^k \equiv 3$ or $7 \bmod 8$, then $a = k-1$, 2 ramifies in K, and $\phi_K(2) = 2$.*

  (b) *If $\Delta/4^k \equiv 1 \bmod 8$, then $a = k$, 2 splits in K, and $\phi_K(2) = 1$.*

  (c) *If $\Delta/4^k \equiv 5 \bmod 8$, then $a = k$, 2 is inert in K, and $\phi_K(2) = 3$.*

Proof. The computation of a, the power of 2 dividing the conductor, is immediate from Lemma 3.4. If $\mathrm{ord}_2(\Delta) = 2k+1$ is odd, then $K = \mathbb{Q}(\sqrt{\Delta})$ is obviously ramified at 2, and hence $\phi_K(2) = 2$. If $\mathrm{ord}_2(\Delta) = 2k$ is even, then $K = \mathbb{Q}(\sqrt{\Delta/4^k})$ is obtained by adjoining the square root of a 2-adic unit, namely $u = \Delta/4^k$. But one knows that for the 2-adic field $\mathbb{Q}_2$ and a unit $u \in \mathbb{Z}_2^\times$, the extension $\mathbb{Q}_2(\sqrt{u})/\mathbb{Q}_2$ depends only on u modulo 8: it is trivial when u is 1 modulo 8, it is the unramified extension $\mathbb{Q}_2(\zeta_3) = \mathbb{Q}_2(\sqrt{-3})$ when u is 5 modulo 8, and otherwise it is ramified. □

4. PROOF OF THEOREM 2.10

We now turn to Theorem 2.10. Thus q is 1 modulo 4, $\mathrm{ord}_2(q+1-A) = 3$, and $R := \mathrm{End}_{\mathbb{F}_q}(E)$ has conductor $2^b f_1$ for some $0 \le b \le a$. The group $E(\mathbb{F}_q)[4]$ is either cyclic or is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the second case occurs if and only if $(F-1)/2 \in R$. Since $(F-1)/2 \in \mathcal{O}_K$, it follows that $(F-1)/2 \in R$ if and only $2^b f_1 \mid f/2$, i.e., if and only if $0 \le b \le a-1$. Thus we have

$$\#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^a f_1)) = 2,$$
$$\#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^b f_1)) = 8-4 = 4 \quad \text{if } 0 \le b < a.$$

It remains to compute a in this case. We have $A = q+1+8(\text{odd})$, so $A^2 = (q+1)^2 + 32(\text{odd})$, and hence $\Delta = (q-1)^2 + 32(\text{odd})$. We must distinguish two cases. If q is 5 modulo 8, then $\Delta = 16(\text{odd})^2 + 32(\text{odd})$ and $\Delta/16$ is 3 or 7 modulo 8. So $a = 1$, 2 ramifies, and $\phi_K(2) = 2$. On the other hand, if q is 1 modulo 8, then $\Delta = 32(\text{odd})$, so again $a = 1$, 2 ramifies, and $\phi_K(2) = 2$. So in either case the numerator has two terms,

$$\#\mathcal{M}_{\Gamma_1(4)}(A,q,f_1) = 2h^\star(R(2f_1)) + 4h^\star(R(f_1)),$$

and the denominator only one,

$$\#\mathcal{M}_{\Gamma_1(4)}(-A,q,f_1) = 2h^\star(R(2f_1)).$$

Since $\phi_K(2) = 2$, we have $h^\star(R(2f_1)) = 2h^\star(R(f_1))$, and so the ratio is 2 in Theorem 2.10.

5. PROOF OF THEOREM 2.8

We now turn to Theorem 2.8. Thus q is 5 modulo 8. Theorem 2.10 treats the case $\mathrm{ord}_2(q+1-A) = 3$. So it remains to treat the case $\mathrm{ord}_2(q+1-A) \geq 4$. In this case, $(F-1)/4 \in \mathcal{O}_K$, so we have

$$\begin{aligned}\#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^af_1)) &= 2,\\ \#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^{a-1}f_1)) &= 8-4 = 4,\\ \#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^bf_1)) &= 16-4 = 12\\ &\qquad \text{if } 0 \leq b \leq a-2.\end{aligned}$$

Exactly as in the discussion following the statement of Theorem 2.8, $\Delta/16$ is 5 modulo 8 if $\mathrm{ord}_2(q+1-A) = 4$, and it is 1 modulo 8 if $\mathrm{ord}_2(q+1-A) \geq 5$. So we have $a = 2$ in both cases. In the first case, 2 is inert and $\phi_K(2) = 3$, while in the second, 2 splits and $\phi_K(2) = 1$.

The denominator is

$$2h^\star(R(2^2f_1)) = 4\phi_K(2)h^\star(R(f_1)).$$

The numerator is

$$\begin{aligned}&2h^\star(R(2^2f_1)) + 4h^\star(R(2f_1)) + 12h^\star(R(f_1))\\ &\quad = (4\phi_K(2) + 4\phi_K(2) + 12)h^\star(R(f_1)).\end{aligned}$$

When $\mathrm{ord}_2(q+1-A) = 4$, we have $\phi_K(2) = 3$, and so the ratio is 3. If $\mathrm{ord}_2(q+1-A) \geq 5$, then $\phi_K(2) = 1$, and the ratio is 5.

6. PROOF OF THEOREM 2.11

We now turn to the proof of Theorem 2.11. Thus q is 1 modulo 8, and $\mathrm{ord}_2(q+1-A) \geq 4$. Again in this case $(F-1)/4 \in \mathcal{O}_K$, so we have

$$\begin{aligned}\#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^af_1)) &= 2,\\ \#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^{a-1}f_1)) &= 8-4 = 4,\\ \#\mathcal{M}_{\Gamma_1(4)}(A,q,R(2^bf_1)) &= 16-4 = 12\\ &\qquad \text{if } 0 \leq b \leq a-2.\end{aligned}$$

So the denominator is

$$2h^\star(R(2^af_1)) = 2^a\phi_K(2)h^\star(R(f_1)).$$

The numerator is

$$\begin{aligned}&2h^\star(R(2^af_1)) + 4h^\star(R(2^{a-1}f_1)) + \sum_{b=0}^{a-2} 12h^\star(R(2^bf_1))\\ &\quad = \Big(2^a\phi_K(2) + 2^a\phi_K(2) + \sum_{b=1}^{a-2} 12 \times 2^{b-1}\phi_K(2) + 12\Big)\\ &\qquad \times h^\star(R(f_1)).\end{aligned}$$

The result now follows in completely straightforward fashion, using Lemma 3.8 to calculate both a and $\phi_K(2)$ as functions of Δ.

7. OTHER ±TRACE SITUATIONS

There are some other families in which, for q satisfying certain congruence conditions, if a trace A occurs, then $-A$ occurs as well. We will discuss these and the ratio phenomena to which they give rise. We fix two odd integers $N \geq 1$ and $M \geq 1$, with $\gcd(N,M) = 1$. We also fix a power $2^r \geq 4$ of 2. We take for $\mathcal{M}/\mathbb{Z}[1/2NM]$ the representable moduli problem

$$\mathcal{M} := \mathcal{M}_{\Gamma_1(2^rN)\cap\Gamma_0(M)}.$$

For an elliptic curve $E/S/\mathbb{Z}[1/2NM]$, a $\Gamma_1(2^rN) \cap \Gamma_0(M)$-structure on E/S is a point $P_{2^rN} \in E(S)[2^rN]$ that is, fiber by fiber, of order 2^rN, together with a cyclic subgroup G_M of order M in E/S.

Let $\mathbb{F}_q$ be a finite field, of characteristic p prime to $2NM$. The trace A at any point of $\mathcal{M}(\mathbb{F}_q)$ satisfies the congruence

$$A \equiv q+1 \bmod 2^rN,$$

and, if $M > 1$, the congruence condition that there exist some $\alpha \in (\mathbb{Z}/M\mathbb{Z})^\times$ that is a root modulo M of the polynomial $X^2 - AX + q$. This second condition is stable under $A \mapsto -A$; just replace α by its negative. But the first condition is stable under $A \mapsto -A$ if and only if

$$2(q+1) \equiv 0 \bmod 2^rN.$$

There are two ways this can happen. The first is that

$$q+1 \equiv 0 \bmod 2^rN,$$

in other words, $q \equiv -1 \bmod 2^rN$. In this case, the Atkin–Lehner involution "divide by the $\mathbb{Z}/2^rN\mathbb{Z}$ generated by P_{2^rN}," followed by quadratic twist, gives an involution of the finite set $\mathcal{M}(\mathbb{F}_q)$ that interchanges A and $-A$. So in this case we always have ratio 1: if A occurs, then $-A$ occurs equally often. And in this case, the only supersingular A is $A = 0$ (because q is -1 mod 4; cf. the proof of Lemma 2.1).

The other, and more interesting, case is

$$q \equiv 2^{r-1}N - 1 \bmod 2^r N.$$

Here there is a big difference between the case $2^r = 4$ and the case $2^r \geq 8$. Let us begin with the case $2^r = 4$.

So we are working with $\Gamma_1(4N) \cap \Gamma_0(M)$, and q is 1 modulo 4 and -1 modulo N. What can we say about supersingular A in this case?

Lemma 7.1. *With $\mathcal{M} = \mathcal{M}_{\Gamma_1(4N)\cap\Gamma_0(M)}$, suppose q is 1 modulo 4 and is -1 modulo N. If either q is an odd power of p or $N > 1$, there are no supersingular points in $\mathcal{M}(\mathbb{F}_q)$. If $q = p^{2k}$ and $N = 1$, then the supersingular points have $A = 2\epsilon p^k$ for the unique choice of* sign $\epsilon = \pm 1$ *for which ϵp^k is 1 modulo 4.*

Proof. Exactly as in the proof of Lemma 2.1, if q is an odd power of p, then 0 is the only possible supersingular value of A, but it is ruled out by the congruence modulo 4.

If $q = p^{2k}$, the only possible supersingular A is $2\epsilon p^k$ for the unique choice of sign $\epsilon = \pm 1$ for which ϵp^k is 1 modulo 4. But if $N > 1$, the congruence $A \equiv 0 \bmod N$ rules this out. If $N = 1$ and $q = p^{2k}$, the assertion is part (2) of Lemma 2.1. □

From [Katz 09, Lemma 4.3], we know exactly which ordinary A occur.

Lemma 7.2. *With $\mathcal{M} = \mathcal{M}_{\Gamma_1(4N)\cap\Gamma_0(M)}$, suppose q is 1 modulo 4 and is -1 modulo N. The ordinary A that occur as traces on $\mathcal{M}(\mathbb{F}_q)$ are those integers prime to p with $|A| < 2\sqrt{q}$ satisfying the congruence*

$$A \equiv q + 1 \bmod 2^r N,$$

and if $M > 1$, satisfying the congruence condition that there exist some $\alpha \in (\mathbb{Z}/M\mathbb{Z})^\times$ that is a root modulo M of the polynomial $X^2 - AX + q$.

Exactly as in the $\Gamma_1(4)$ discussion, we are concerned with the ratio of occurrences of A to occurrences of $-A$. Replacing if necessary A by $-A$, we have

$$q + 1 - A \equiv 0 \bmod 8, \quad q + 1 + A \equiv 4 \bmod 8.$$

The answer is exactly the same as it was in the $\Gamma_1(4)$ case.

Theorem 7.3. *With $\mathcal{M} = \mathcal{M}_{\Gamma_1(4N)\cap\Gamma_0(M)}$, suppose q is 1 modulo 4 and is -1 modulo N. Then the ratio is determined by the rules of Theorems 2.8, 2.10, and 2.11. In particular, when we have in addition that q is 5 modulo 8, the $2, 3, 5$ phenomenon persists.*

Proof. We prove this by writing the conductor f of $\mathbb{Z}[F]$ as $2^a f_0$ with f_0 odd. For each divisor f_1 of f_0, we will consider the corresponding f_1 packet.

There are two key observations. The first is that because q is -1 modulo N and N is odd, any $E/\mathbb{F}_q$ with trace A has $E(\mathbb{F}_q)[N]$ a cyclic group of order N. So whatever the f_1 packet, every member has exactly $\phi(N)$ $\Gamma_1(N)$-structures.

The second is that the inclusions

$$R(2^b f_1) \subset R(f_1)$$

induce isomorphisms

$$R(2^b f_1)/MR(2^b f_1) \cong R(f_1)/MR(f_1),$$

simply because M is odd. Therefore in the entire f_1 packet, the number of $\Gamma_0(M)$ structures carried by any of the $R(2^b f_1)$'s is independent of b, and is trivially invariant under changing F to $-F$. For some f_1 packets, there may be none, but we know [Katz 09, Lemma 4.3] that there are some for $\mathbb{Z}[F]$ itself, i.e., for the f_0 packet. So precisely the same f_1 packets enter in numerator and denominator.

For such an f_1 packet, denote by $c(f_1)$ the number of $\Gamma_0(M)$ structures carried by any of the $R(2^b f_1)$'s. For each term in a given f_1 packet that admits $\Gamma_0(M)$ structures, we have

$$\begin{aligned}&\#\mathcal{M}_{\Gamma_1(4N)\cap\Gamma_0(M)}(A, q, R(2^b f_1))\\ &\quad = \phi(N)c(f_1)\#\mathcal{M}_{\Gamma_1(4)}(A, q, R(2^b f_1)),\end{aligned}$$

and the same with A replaced by $-A$. So the theorem is reduced to the f_1 packet version of the ratio theorem for $\mathcal{M}_{\Gamma_1(4)}$ itself. □

We now turn to the case of $\Gamma_1(2^r N) \cap \Gamma_0(M)$ with $2^r \geq 8$, with q that is $2^{r-1} - 1$ modulo 2^r and -1 modulo N.

Lemma 7.4. *In this case there are no supersingular points in $\mathcal{M}(\mathbb{F}_q)$.*

Proof. If q is an odd power of p, then exactly as in Lemma 2.1, only $A = 0$ is possible, but it is ruled out by the modulo 2^r congruence $A \equiv q + 1 \equiv 2^{r-1} \bmod 2^r$. Since q is -1 modulo 4, it cannot be an even power of p. □

From [Katz 09, Lemma 4.3], we know exactly which A occur.

Lemma 7.5. *With $\mathcal{M} = \mathcal{M}_{\Gamma_1(2^r N)\cap\Gamma_0(M)}$, suppose q is $2^{r-1} - 1$ modulo 2^r and -1 modulo N. The ordinary A that occur as traces on $\mathcal{M}(\mathbb{F}_q)$ are those integers prime to p with $|A| < 2\sqrt{q}$ satisfying the congruence*

$$A \equiv q + 1 \bmod 2^r N,$$

and, if $M > 1$, satisfying the congruence condition that there exist some $\alpha \in (\mathbb{Z}/M\mathbb{Z})^\times$ that is a root modulo M of the polynomial $X^2 - AX + q$.

We are concerned with the ratio of occurrences of A to occurrences of $-A$. Replacing if necessary A by $-A$, we have

$$q + 1 - A \equiv 0 \bmod 2^{r+1}, \quad q + 1 + A \equiv 2^r \bmod 2^{r+1}.$$

Here every ratio is 3.

Theorem 7.6. *With $\mathcal{M} = \mathcal{M}_{\Gamma_1(2^r N)\cap\Gamma_0(M)}$, $r \geq 3$, suppose q is $2^{r-1} - 1$ modulo 2^r and -1 modulo N. Then the ratio is always 3.*

Proof. Exactly as in the proof of Theorem 7.3, we work with f_1 packets. Exactly as in that proof, we reduce to showing that for each f_1 packet, we have ratio 3 for the $\Gamma_1(2^r)$ problem itself, for any q that is $2^{r-1} - 1$ modulo 2^r. Here q is -1 modulo 4, so while $(F - 1)/2 \in \mathcal{O}_K$, $(F - 1)/4$ is not in $\mathcal{O}_K$.

So on the $-A$ side, $E(\mathbb{F}_q)[2^r]$ is cyclic, with 2^{r-1} choices of generator. On the A side this group either is cyclic, with 2^{r-1} choices of generator (the case $b = a$), or is $\mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with 2^r choices of generator (the case $0 \leq b \leq a - 1$). So the denominator is

$$\#\mathcal{M}_{\Gamma_1(2^r)}(-A, q, f_1) = 2^{r-1} h^\star(R(2^a f_1)),$$

and the numerator is

$$\begin{aligned}&\#\mathcal{M}_{\Gamma_1(2^r)}(A, q, f_1)\\ &\quad = 2^{r-1} h^\star(R(2^a f_1)) + \sum_{b=1}^{a-1} 2^r h^\star(R(2^b f_1))\\ &\qquad + 2^r h^\star(R(f_1)).\end{aligned}$$

So it remains to compute a and $\phi_K(2)$ in this case. Write $A = q + 1 + (2^{r+1})$. Then $A^2 = (q + 1)^2 + (2^{2r+1})$, because $q + 1$ is 2^{r-1}(odd). Then

$$\Delta = A^2 - 4q = (q - 1)^2 + (2^{2r+1}) = 4(\text{odd}^2) + (2^{2r+1}),$$

and $\Delta/4$ is $\text{odd}^2 + (2^{2r-1})$, which is 1 modulo 8. Thus $a = 1$, 2 splits in K, and $\phi_k(2) = 1$. So the denominator is

$$2^{r-1} h^\star(R(2f_1)) = 2^{r-1} h^\star(R(f_1)),$$

and the numerator is

$$\begin{aligned}&2^{r-1} h^\star(R(2f_1)) + 2^r h^\star(R(f_1))\\ &\quad = 2^{r-1} h^\star(R(f_1)) + 2^r h^\star(R(f_1)).\end{aligned}$$ □

8. RATIO COMPARISONS FOR CERTAIN PAIRS OF FAMILIES

There are many pairs of moduli problems, say $\mathcal{M}_1$ and $\mathcal{M}_2$, with the property that for every suitable finite field $\mathbb{F}_q$, the integers A prime to p that occur as traces in $\mathcal{M}_1(\mathbb{F}_q)$ are exactly the same as those that occur in $\mathcal{M}_2(\mathbb{F}_q)$. In any such situation, a natural ratio to consider is, for each such A,

$$\frac{\#\text{ of occurrences of } A \text{ in } \mathcal{M}_1(\mathbb{F}_q)}{\#\text{ of occurrences of } A \text{ in } \mathcal{M}_2(\mathbb{F}_q)}.$$

The simplest examples are these. Take an integer $N \geq 3$, and work over the cyclotomic ground ring $\mathbb{Z}[\zeta_N][1/N]$. Take the moduli problems $\Gamma_1(N^2)$ and (oriented) $\Gamma(N)$. Then for any finite field $\mathbb{F}_q$ with $q \equiv 1 \bmod N$, the integers A prime to p that occur are precisely those with $|A| < 2\sqrt{q}$ and

$$A \equiv q + 1 \bmod N^2.$$

Or take two integers $N \geq 2$ and $M \geq 3$ with $N \mid M$, and the following two moduli problems over the cyclotomic ground ring $\mathbb{Z}[\zeta_N][1/N]$. The first is $\Gamma_1(NM)$. The second, which we will denote by $\Gamma_1(N \times M)$, is the moduli problem that consists in giving a point P_N of order N and a point Q_M of order M such that the pair $(P_N, (M/N)Q_M)$ is an oriented $\Gamma(N)$ structure. Then for any finite field $\mathbb{F}_q$ with $q \equiv 1 \bmod N$, the integers A prime to p that occur are precisely those with $|A| < 2\sqrt{q}$ and

$$A \equiv q + 1 \bmod NM.$$

In any particular case, it is an exercise to work out the ratios in question, using the techniques developed above. Sometimes, however, the ratios are quite pleasingly simple, at least when q satisfies certain congruences.

This is the case when we compare the moduli problems $\Gamma_1(8)$ and $\Gamma_1(2\times 4)$, which both live over $\mathbb{Z}[1/2]$. We state the results below; their straightforward proofs are left to the reader. For a given integer A prime to p that occurs in both $\mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q)$ and in $\mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q)$, we will refer to

$$\frac{\#\text{ of occurrences of } A \text{ in } \mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q)}{\#\text{ of occurrences of } A \text{ in } \mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q)}$$

as "the ratio." The simplest statement is that for $q \equiv 5 \bmod 8$.

Theorem 8.1. *Suppose $q \equiv 5 \bmod 8$. The ratio is always 1.*

Theorem 8.2. *Suppose $q \equiv -1 \bmod 8$. Then we have the following results:*

(1) *In $\mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q)$, A and $-A$ occur equally often.*

(2) *In $\mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q)$, A and $-A$ occur equally often (cf. Lemma 2.4).*

(3) *If* $\mathrm{ord}_2(q+1-A) = 3$, *then ratio* $= 2$*; otherwise, ratio* $= 2/3$.

Theorem 8.3. *Suppose $q \equiv 3 \bmod 8$. Then we have the following results:*

(1) *In $\mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q)$, A and $-A$ occur equally often.*

(2) *In $\mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q)$, after possibly replacing A by $-A$, we have* $\mathrm{ord}_2(q+1+A) = 3$ *and* $\mathrm{ord}_2(q+1-A) \geq 4$*; A occurs three times as often as $-A$ (cf. Theorem 7.6).*

(3) *If* $\mathrm{ord}_2(q+1-A) = 3$, *then ratio* $= 2$*; otherwise, ratio* $= 2/3$.

(4) *The occurrences of*

$$\begin{aligned} -A &\in \mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q), \\ -A &\in \mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q), \\ A &\in \mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q), \\ A &\in \mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q), \end{aligned}$$

are in the proportion $1:2:2:3$.

Remark 8.4. When q is 3 or 5 modulo 8, there are no supersingular points on either $\mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q)$ or $\mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q)$. When q is -1 modulo 8, the supersingular points on both $\mathcal{M}_{\Gamma_1(8)}(\mathbb{F}_q)$ and $\mathcal{M}_{\Gamma_1(2\times 4)}(\mathbb{F}_q)$ all have $A = 0$.

In fact, Theorem 8.2 remains valid for $A = 0$, but a slightly different argument is required.

Indeed, suppose $q = p^{2k+1}$ is a fixed odd power of p with $p \equiv -1 \bmod 8$, and an elliptic curve $E/\mathbb{F}_q$ has $A = 0$. Then $R := \mathrm{End}_{\mathbb{F}_q}(E)$ is a quadratic imaginary order: it is either the order (of conductor 2) $\mathbb{Z}[F/(-p)^k] = \mathbb{Z}[X]/(X^2+p) = \mathbb{Z}[\sqrt{-p}]$ or the full ring of integers $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-p})/2]$; cf. [Waterhouse 69, Theorem 4.2 (3) and Theorem 4.5] and [Schoof 87, proof of Theorem 4.5].

Moreover, for each integer N prime to p, the R-module $E(\overline{\mathbb{F}_q})[N]$ is R-isomorphic to R/NR. And the set of isomorphism classes of $E/\mathbb{F}_q$ with $A = 0$ and given R is principal homogeneous under $\mathrm{Pic}(R)$. So for each of the two moduli problems $\mathcal{M}$ under consideration we get the class number formula

$$\#\mathcal{M}(0,q) = \sum_{\text{orders } \mathbb{Z}[F/(-p)^k] \subset R \subset \mathcal{O}_K} h^\star(R)\#\mathcal{M}(0,q,R),$$

and we can proceed exactly as in the ordinary case.

REFERENCES

[Cox 89] David Cox. *Primes of the Form x^2+ny^2*. New York: Wiley, 1989.

[Deligne 69] Pierre Deligne. "Variétés abéliennes ordinaires sur un corps fini." *Invent. Math.* 8 (1969), 238–243.

[Deuring 41] M. Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." *Abh. Math. Sem. Hansischen Univ.* 14 (1941), 197–272.

[Honda 68] T. Honda. "Isogeny Classes of Abelian Varieties over Finite Fields." *J. Math. Soc. Japan* 20 (1968), 83–95.

[Katz 09] Nicholas M. Katz. "Lang–Trotter Revisited." *Bull. Amer. Math. Soc. (N.S.)* 46:3 (2009), 413–457.

[Lang and Trotter 76] Serge Lang and Hale Trotter. *Frobenius Distributions in* GL_2*-Extensions*, Lecture Notes in Mathematics 504. New York: Springer, 1976.

[Schoof 87] René Schoof. "Nonsingular Plane Cubic Curves over Finite Fields." *J. Comb. Th., Series A* 46 (1987), 183–211.

[Waterhouse 69] William C. Waterhouse. "Abelian Varieties over Finite Fields." *Ann. Sci. de l'É.N.S. 4^e série* 2:4 (1969), 521–560.

Nicholas M. Katz, Department of Mathematics, Fine Hall, Princeton University, Princeton, NJ 08544-1000
(nmk@math.princeton.edu)

Received December 18, 2008; accepted June 18, 2009.