CONGRUENCE CLASS BIAS AND THE LANG-TROTTER CONJECTURE FOR FAMILIES OF ELLIPTIC CURVES

S. JAROV, A. KHADRA, N. WALJI

ABSTRACT. For various families of elliptic curves over the integers, we obtain distribution results towards the Lang–Trotter conjecture on average. We demonstrate the existence of a congruence class bias in this context, and then investigate this further computationally.

1. INTRODUCTION

Let $E = E(a,b)$, for some (suitable) $a, b \in \mathbb{Z}$, be an elliptic curve with Weierstrass equation $y^2 = x^3 + a + b$, where the discriminant is $\Delta(a,b) = 4a^3 + 27b^2 \neq 0$. If p is a prime of good reduction, then the reduction modulo p of E is an elliptic curve over $\mathbb{F}_p$. For such a p, we define $a_p(E) := p+1-|E(\mathbb{F}_p)|$. The statistical properties of the sequences $(a_p(E))_p$ have been studied extensively from various perspectives. Our particular interest lies in the Lang–Trotter conjecture, which predicts that, for any integer r,

$$\pi(x, E(a,b), r) := \#\{p \leq x : a_p(E) = r\} \sim C_E \frac{\sqrt{x}}{\log x},$$

for some suitable constant C_E.

This was shown [4,5] to hold on average for families of elliptic curves of the form

$$\{E(a,b) : |a| \leq A, |b| \leq B, a, b \in \mathbb{Z}, \Delta(a,b) \neq 0\},$$
$$\{E(a,b) \in \mathcal{F}_{A,B} : E(a,b) \text{ minimal in its isomorphism class}\}.$$

Further averaging results were obtained through the perspective of different families, for example with the work of James [7] on 3-torsion elliptic curves (which form a subset of density zero in the families above) and many further results [1,3,6,8,13,14,16].

In this work, we explore a direction involving thin families determined by a combination of polynomial and exponential functions (see also Section 4.2 of [6]), and show that the Lang–Trotter conjecture holds on average for these new families over various specified congruence classes of primes. We also exhibit the existence of a congruence class bias in this context.

First let us define, for any subset of primes P and polynomials f, g,

$$\pi(x, E(a,b), r, P) := \#\{p \leq x : p \in P, a_p(E) = r\}$$

and

$$\mathcal{F}_{A,B}(f,g) := \{E(f(a), g(b)) : |a| \leq A, |b| \leq B, a, b \in \mathbb{Z}, \Delta(f(a), g(b)) \neq 0\}.$$

Theorem 1.1. *For positive integers k_1, k_2, a_1, a_2, let $f_{k_i,a_i}(n) := n^{k_i} a_i^n$ for all $n \in \mathbb{N}$.*

(a) *Fix $a_i = -1$ and let P be the set of all primes p such that $p \equiv -1 \pmod{2k_1}$, $p \equiv -1 \pmod{2k_2}$, and if k_i is divisible by 4, then one can also weaken the corresponding condition to $p \equiv -1 \pmod{k_i}$. If k_1, k_2 are both odd, then we instead set $P = \{p : (k_i, p-1) = 1, i = 1, 2\}$. Then, given any integer r, for $A, B > x^{1+\epsilon}$, we have*

$$|\mathcal{F}_{A,B}(f_{k_1,a_1}, f_{k_2,a_2})|^{-1} \sum_{|a| \le A, |b| \le B} \pi\left(x, E(f_{k_1,a_1}(a), f_{k_2,a_2}(b)), r, P\right) \sim C_{k_1,k_2,r} \frac{\sqrt{x}}{\log x},$$

as $x \to \infty$, for some specified constant $C_{k_1,k_2,r}$.

(b) *Fix $k_i = 2$, and let $P = \left\{p : \left(\frac{a_i}{p}\right) = -1\right\}$. Then given any integer r, for $A, B > x^{2+\epsilon}$, we have*

$$|\mathcal{F}_{A,B}(f_{k_1,a_1}, f_{k_2,a_2})|^{-1} \sum_{|a| \le A, |b| \le B} \pi\left(x, E(f_{k_1,a_1}(a), f_{k_2,a_2}(b)), r, P\right) \sim C'_{a_1,a_2,r} \frac{\sqrt{x}}{\log x},$$

as $x \to \infty$, for some specified constant $C'_{a_1,a_2,r}$.

We will also prove:

Theorem 1.2. *Let $g_i(n) = n^{k_i}(a_i^n + b_i^n)$, with $i = 1, 2$, for positive integers a_i, b_i and odd k_i. Let $P := \{p : (k, p-1) = 1, p \nmid a, b\}$. Then for $A, B > x^{2+\epsilon}$ and any integer r,*

$$|\mathcal{F}_{A,B}(g_1, g_2)|^{-1} \sum_{|a| \le A, |b| \le B} \pi\left(x, E(g_1(a), g_2(b)), r, P\right) \ge C \frac{\sqrt{x}}{\log x} + o\left(\frac{\sqrt{x}}{\log x}\right)$$

as $x \to \infty$, where the bound C depends on a_i, b_i, k_i.

In special cases, we will describe the constant in Theorem 1.1 explicitly in Section 2.4 (in particular, see equation (25)). In examining these constants, one can determine the existence of a congruence class bias in terms of the occurrence of primes p such that $a_p = r$, which depends on the congruence conditions used to determine P. This provides further evidence of the bias observed in [15].

Our paper is structured as follows. In Section 2, we establish modulo p reduction properties for the families from our theorems. Then we make use of a variant of the Lang–Trotter conjecture on average under congruence conditions (see earlier work in [7, 8]), the main aspects of this proof are described for the convenience of the reader. In Section 3, we examine the implications of our theorems for congruence class bias on average. In Section 4, we obtain some computations to examine congruence class bias for individual elliptic curves.

2. Proof

2.1. **Equidistribution of certain functions.**

We begin our proof with some equidistribution results. We say that $f : C \to D$ is an *m-to-one function* if the preimage of each element of D has order m.

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

(a) *For any positive integer k, let $f_k : \mathbb{Z} \to \mathbb{F}_p$ be the function $n \mapsto a^n n^k \pmod{p}$. For any integer c, let $S_c := \{c, c+1, \ldots, c + (2p-1)\}$.*

(i) *For* $a = -1$*, if* k *is even and* $p \equiv -1 \pmod{2k}$*, then* $f_k|_{S_c}$ *is a two-to-one function for any integer* c*.*

(ii) *For* $a = -1$*, if* k *is a multiple of 4 and* $p \equiv k-1 \pmod{2k}$*, then* $f_k|_{S_c}$ *is a two-to-one function for any* c*.*

(iii) *For any integer* a*, if* $(k, p-1) = 1$*, then* $f_k|_{S_c}$ *is a two-to-one function for any* c*.*

(b) *Define* $T_c := \{c, c+1, \ldots, c+p(p-1)-1\}$ *for any integer* c*. For any integer* a*, if* $k = 2$ *and* $\left(\frac{a}{p}\right) = -1$*, then* $f_k|_{T_c}$ *is a* $(p-1)$*-to-one function.*

(c) *Given positive distinct integers* a, b *and odd integer* $k \geq 3$*, let* $g_k : \mathbb{Z} \to \mathbb{F}_p$ *be the function* $n \mapsto n^k(a^n + b^n)$*. For an odd prime* p *such that* $(k, p-1) = 1$ *and* $p \nmid a, b$*, we have, for any integer* c*,*

$$|\left(g_k|_{T_c}\right)^{-1}(u)| \geq \frac{p-1}{2},$$

for all $u \in \mathbb{F}_p$*.*

Proof of (a)(i). We first note that 0 is in the image of f_k. Given $c \in \mathbb{F}_p^\times$, choose any integer d such that

$$d \equiv c^{(p+1)/2k} (\text{mod } p).$$

Then $f_k(d) \equiv (-1)^d c^{(p+1)/2} \pmod{p}$.

We have $c^{p+1} \equiv c^2 (\text{mod } p)$ by Fermat's little theorem. Since the polynomial $x^2 - c^2 \equiv 0 \pmod{p}$ has exactly two solutions $\pm c$, we have that $c^{(p+1)/2} \equiv \pm c \pmod{p}$. Since

$$f_k(d) \equiv -f_k(d+p) \pmod{p},$$

either

$$f_k(d) \equiv c \pmod{p} \quad \text{or} \quad f_k(d+p) \equiv c \pmod{p}.$$

Therefore c is in the image of f_k. We conclude that f_k is surjective.

If furthermore we choose d above in $\{0, \ldots, p-1\}$, then $\{d, d+p\} \subset S$ maps to $\{c, -c\} \subset \mathbb{F}_p$ under the function f_k, given the construction above. Therefore, $f_k|_S$ is a two-to-one function. □

Proof of (a)(ii). Note that the squares are in the image of f_k. Indeed, given $c \in \mathbb{F}_p^\times$, choose an integer d such that $d \equiv c^{(p+1)/k} \pmod{p}$. Then

$$(c^{(p+1)/k})^k \equiv c^{p+1} \equiv c^2 \pmod{p}.$$

Since k is even, $p \equiv k-1 \pmod{2k} \Rightarrow p \equiv k-1 \pmod{4}$. If k is a multiple of 4, this means $p \equiv 3 \pmod{4}$, and so -1 is not a square in mod p.

As above, we now note that $f_k(d) \equiv -f_k(d+p) \pmod{p}$, so

$$\{f_k(d), f_k(d+p)\} = \{c^2, -c^2\}.$$

Therefore, f_k is surjective.

Using a similar argument to that in the proof of the previous lemma, we also obtain that $f_k|_S$ is a two-to-one function. □

Proof of part (a)(iii). This follows using similar ideas to above. □

Proof of part (b). For integers ℓ, j note that $f(\ell + j(p-1)) \equiv (\ell - j)^2 a^\ell \pmod{p}$. Under our assumption that a is not a quadratic residue in mod p, we consider the following multiset over $\mathbb{F}_p$: For odd ℓ, $\{(\ell-j)^2 a^\ell | j \in \{0, \ldots, p-1\}\}$ is exactly the multiset of each quadratic non-residue occurring twice, along with the element 0 occurring once. For even ℓ, it is the multiset of each non-zero quadratic residue occurring twice, along with the element 0 occurring once. Since $\{\ell + j(p-1) \mid \ell \in \{0, \ldots, p-2\}, j \in \{0, \ldots, p-1\}\} = T_0$, this shows that $f_2 \mid_{T_0}$ is a $(p-1)$-to-one function. The cases for other T_c follow in a similar way. □

Proof of part (c). First, we note that for any n we cannot have $a^n + b^n \equiv a^{n+1} + b^{n+1} \equiv 0 \pmod{p}$. Otherwise, we would have

$$a^{n+1} + ab^n \equiv 0 \equiv a^{n+1} + b^{n+1} \pmod{p}$$

which implies $a \equiv b \pmod{p}$ and so $2a^n \equiv 0 \pmod{p}$, contradicting our assumptions. Therefore, $a^n + b^n \not\equiv 0 \pmod{p}$ for at least half of the elements $n \in T_0$.

Given $t \in T_0$ with $a^t + b^t \not\equiv 0 \pmod{p}$, consider the following (as a subset of $\mathbb{F}_p$)

$$\begin{aligned} &\left\{n^k(a^n + b^n) \mid n = t + j(p-1), j \in \{0, \ldots, p-1\}\right\} \\ =&\left\{(t-j)^k(a^t + b^t) \mid j \in \{0, \ldots, p-1\}\right\} \\ =&\,\mathbb{F}_p. \end{aligned}$$

Since at least half the elements $t \in T_0$ have $a^t + b^t \not\equiv 0 \pmod{p}$, we conclude that $|\left(g_k \mid_{T_0}\right)^{-1}(u)| \geq (p-1)/2$, for all $u \in \mathbb{F}_p$. The proof follows in a similar way for other cases of T_c. □

2.2. **Averaging results.** The proof now proceeds in a standard way by following David–Pappalardi [4], in a similar way to James [7] (see also [8] and [6] for related work), and applying Proposition 2.1. We present some of the details for the benefit of the reader, focusing on the special case where r is odd and m is prime.

Let r be an odd integer, and set $B(r) = \max\left(3, r, \frac{r^2}{4}\right)$. Let m be a prime number and c an integer coprime to m. Let $d := (r^2 - 4p)/f^2$, $h(d)$ be the class number of the order of discriminant d, $w(d)$ the number of units in this order, and let

$$H(r^2 - 4p) = 2 \sum_{\substack{f^2 | r^2 - 4p \\ d \equiv 0,1 \bmod 4}} h(d)/w(d)$$

be the Kronecker class number, which gives the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with $p + 1 - r$ points (for $r \leq 2\sqrt{p}$). Note that f in the sum takes positive integer values only.

Given an elliptic curve $E(a,b)/\mathbb{F}_p$ represented by the equation $y^2 = x^3 + ax + b$, outside of certain special cases requiring either a or b to be 0, the number of elliptic curves in the $\mathbb{F}_p$-isomorphism class of E is $(p-1)/2$. This means that the number of elliptic curves $E(a,b)$ where $0 \leq a, b < p$ are integers and $a_p(E(a,b)) = r$ is $H(r^2 - 4p)(p-1)/2 + O(p)$ (see Birch [2]).

Let $\mathcal{F}_{f,g}(A,B) := \{E(f(a), g(b)) \mid |a| \leq A, |b| \leq B\}$, where f and g are a pair of functions. Using the notation from earlier, let $\pi(x, E, r, \{p \equiv c \pmod{m}\})$ denote the number of primes $p \leq x$ such that $p \equiv c \pmod{m}$ and such that $a_p(E) = r$. We also define $\pi_{1/2}(x) = \int_2^x dt/(2\sqrt{t}\log t)$ (see [9]).

For the proof of Theorem 1.1(a), we let f, g be a pair of functions described in the theorem statement, and we begin with

$$\begin{aligned}&\frac{1}{4AB}\sum_{E\in\mathcal{F}_{f.g}(A,B)}\pi(x,E,r,\{p\equiv c \pmod m\})\\ =&\frac{1}{4AB}\sum_{\substack{p\le x\\ p\equiv c \pmod m}}\#\{|a|\le A,|b|\le B: a_p(E(a,b))=r\}\\ =&\frac{1}{4AB}\sum_{\substack{p\le x\\ p\equiv c \pmod m}}\left(\frac{2A}{p}+O(1)\right)\left(\frac{2B}{p}+O(1)\right)\left(\frac{pH(r^2-4p)}{2}+O(p)\right)\end{aligned}$$

applying Proposition 2.1(a) and Birch [2]. We write the above as

$$\frac{1}{2}\sum_{\substack{p\le x\\ p\equiv c \pmod m}}\frac{H(r^2-4p)}{p}+O\left(\sum_{\substack{p\le x\\ p\equiv c \pmod m}}H(r^2-4p)\left(\frac{1}{A}+\frac{1}{B}+\frac{p}{AB}\right)\right)+O\left(\sum_{\substack{p\le x\\ p\equiv c \pmod m}}\frac{1}{p}\right).$$

The proof of Theorem 1.1(b) begins similarly, but with larger error terms. We have (applying Proposition 2.1(b) and Birch [2]),

$$\begin{aligned}&\frac{1}{4AB}\sum_{E\in\mathcal{F}_{f.g}(A,B)}\pi(x,E,r,\{p\equiv c \pmod m\})\\ =&\frac{1}{4AB}\sum_{\substack{p\le x\\ p\equiv c \pmod m}}\left(\frac{2A}{p}+O(p)\right)\left(\frac{2B}{p}+O(p)\right)\left(\frac{pH(r^2-4p)}{2}+O(p)\right).\\ =&\frac{1}{2}\sum_{\substack{p\le x\\ p\equiv c \pmod m}}\frac{H(r^2-4p)}{p}+O\left(\sum_{\substack{p\le x\\ p\equiv c \pmod m}}H(r^2-4p)\left(\frac{p}{A}+\frac{p}{B}+\frac{p^3}{AB}\right)\right) \qquad (1)\end{aligned}$$

This demonstrates the need for stronger bounds on A and B in Theorem 1.1(b), where we require $A, B > x^{2+\epsilon}$.

In the case of Theorem 1.2, let us denote the expression in equation line (1) above as $M(x, A, B)$. Then given Proposition 2.1(c), we have

$$\frac{1}{4AB}\sum_{E\in\mathcal{F}_{f.g}(A,B)}\pi(x,E,r,\{p\equiv c \pmod m\})\ge\frac{1}{2}M(x,A,B).$$

The remainder of the proofs follow in the same way for each theorem, which we will continue below.

Following [4], we obtain

$$\frac{1}{2}\sum_{\substack{p\in S_f(x)\\ p\equiv c \pmod{m}}}\frac{H(r^2-4p)}{p}=\frac{2}{\pi}K_r(c,m)\cdot\pi_{\frac{1}{2}}(x)+O\left(\frac{\sqrt{x}}{\log^2 x}\right). \tag{2}$$

where

$$K_r(c,m)=\sum_{\substack{f=1\\(f,2r)=1}}^{\infty}\sum_{n=1}^{\infty}\frac{\lambda_f^r(n;c,m)}{fn\phi\left([m,nf^2]\right)}, \tag{3}$$

with

$$\lambda_f^r(n;c,m)=\sum_{\substack{a \pmod{4n}^*\\ a\equiv 1 \pmod 4\\ (r^2-af^2,4n)=4\\ \frac{r^2-af^2}{4}\equiv c \pmod{(nf^2,m)}}}\left(\frac{a}{n}\right), \tag{4}$$

where $\sum_{a \pmod{4n}^*}$ is the sum over all invertible residues modulo $4n$ and

$$S_f(x)=\left\{B(r)<p\le x\,\middle|\,4p\equiv r^2 \pmod{f^2},\text{ and } d=\frac{r^2-4p}{f^2}\equiv 0,1 \pmod 4\right\}.$$

Note that $p>B(r)$ implies that $|r|\le 2\sqrt{p}$.

2.3. **An Auxiliary lemma.** We determine the constant that will arise in our asymptotic expression. We begin by proving various properties of

$$\lambda_f^r(n;c,m):=\sum_{\substack{a \pmod{4n}^*\\ a\equiv 1 \pmod 4\\ (r^2-af^2,4n)=4\\ \frac{r^2-af^2}{4}\equiv c \pmod{(nf^2,m)}}}\left(\frac{a}{n}\right), \tag{5}$$

for $(c,m)=1$. First we define $\kappa(n)$ to be the multiplicative function such that

$$\kappa(\ell^\alpha)=\begin{cases}\ell & \text{if } \alpha \text{ is odd,}\\ 1 & \text{if } \alpha \text{ is even.}\end{cases} \tag{6}$$

for positive integer α and prime ℓ.

Lemma 2.2. *We show*

(a) When n is odd,

$$\lambda_f^r(n;c,m)=\sum_{\substack{a \pmod{n}^*\\ (r^2-af^2,n)=1\\ r^2-af^2\equiv 4c \pmod{(nf^2,m)}}}\left(\frac{a}{n}\right).$$

(b) Let p_1,p_2 be odd, distinct primes, then $\lambda_f^r(p_1p_2;c,m)=\lambda_f^r(p_1;c,m)\lambda_f^r(p_2;c,m)$.

(c) For a prime ℓ,

$$\lambda_f^r(\ell^\alpha;c,m)=\sum_{\substack{a \pmod{4\ell^\alpha}^*\\ a\equiv 1 \pmod 4\\ (r^2-af^2,4\ell^\alpha)=4\\ \frac{r^2-af^2}{4}\equiv c \pmod{(\ell^\alpha f^2,m)}}}\left(\frac{a}{\ell}\right)^\alpha,$$

for cases of ℓ, m, f, where $(c,m)=1$ and m is prime.

(d) *If $\alpha \geq 1$ and m is odd, then $\lambda_1^r(2^\alpha; c, m) = \frac{(-2)^\alpha}{2}$.*
If $\alpha \geq 1$ and m is even, then $\lambda_1^r(2^\alpha; c, m) = \frac{(-2)^\alpha}{2^{min(\alpha,\beta)}}$.

(e) *For an odd prime $\ell \nmid m$,*

$$\lambda_1^r(\ell^\alpha; c, m) = \ell^{\alpha-1} \cdot \begin{cases} \ell - 1 - \left(\frac{r^2}{\ell}\right) & \text{if } \alpha \text{ is even,} \\ -\left(\frac{r^2}{\ell}\right) & \text{if } \alpha \text{ is odd.} \end{cases}$$

For $\ell | m$,

$$\lambda_1^r(\ell^\alpha; c, m) = \ell^{\alpha - min(\alpha,\beta)} \cdot \left(\frac{r^2-4c}{\ell}\right)^\alpha.$$

(f) *For an odd prime $\ell \nmid r$ with $(\ell^{\alpha+2}, m) \neq 1$, we have*

$$\frac{\lambda_\ell^r(\ell^\alpha; c, m)}{\ell^{\alpha-1}} = \begin{cases} 0 & \text{if } \alpha \text{ is odd or } r^2 \not\equiv 4c \pmod{m}, \\ \ell - 1 & \text{if } \alpha \text{ is even and } r^2 \equiv 4c \pmod{m}. \end{cases}$$

(g) *For all positive integers n, $|\lambda_f^r(n; c, m)| \leq n/\kappa(n)$.*

Proof.

Part (a): Since n and f are odd, we apply the Chinese remainder theorem, to get that $r^2 - af^2 \equiv 4c \pmod{4 \cdot (nf^2, m)}$ implies

$$r^2 - af^2 \equiv 0 \pmod{4}, \quad \text{and} \quad r^2 - af^2 \equiv 4c \pmod{(nf^2, m)}. \tag{7}$$

We have that $(r^2 - af^2, 4n) = 4$ implies $(r^2 - af^2, 4) = 4$ and $(r^2 - af^2, n) = 1$. Let a_1 and a_2 be the images of a under the projections $(\mathbb{Z}/4n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/4n\mathbb{Z})^* \to (\mathbb{Z}/4\mathbb{Z})^*$, respectively. Therefore we can break up the condition $(r^2 - af^2, 4n) = 4$ into $(r^2 - a_2f^2, 4) = 4$, and $(r^2 - a_1f^2, n) = 1$. Finally, since n is odd so the shape of the Kronecker symbol does not change. The result follows.

Part (b): Since p_1p_2 is odd, we apply Lemma 2.2 (a)

$$\lambda_f^r(p_1p_2; c, m) = \sum_{\substack{a \pmod{p_1p_2}^* \\ (r^2-af^2, p_1p_2)=1 \\ r^2-af^2 \equiv 4c \pmod{(p_1p_2f^2, m)}}} \left(\frac{a}{p_1p_2}\right). \tag{8}$$

As $(p_1, p_2) = 1$, we apply the Chinese Remainder Theorem and let a_1 and a_2 be the images of a under the projections $(\mathbb{Z}/p_1p_2\mathbb{Z})^* \to (\mathbb{Z}/p_1\mathbb{Z})^*$ and $(\mathbb{Z}/p_1p_2\mathbb{Z})^* \to (\mathbb{Z}/p_2\mathbb{Z})^*$, respectively. It follows that $(r^2 - a_1f^2, p_1) = 1$ and $(r^2 - a_2f^2, p_2) = 1$. The third condition on the sum in equation (8) implies that $r^2 - af^2 \equiv 4c \pmod{N}$, for any $N | (p_1p_2f^2, m)$. Since $(p_1f^2, m), (p_2f^2, m) | (p_1p_2f^2, m)$, we can write

$$r^2 - af^2 \equiv 4c \pmod{(p_1f^2, m)} \text{ and } r^2 - af^2 \equiv 4c \pmod{(p_2f^2, m)}.$$

We obtain

$$\begin{aligned} \lambda_f^r(p_1p_2; c, m) &= \sum_{\substack{a_1 \pmod{p_1}^* \\ (r^2-a_1f^2, p_1)=1 \\ r^2-a_1f^2 \equiv 4c \pmod{(p_1f^2, m)}}} \left(\frac{a_1}{p_1}\right) \sum_{\substack{a_2 \pmod{p_2}^* \\ (r^2-a_2f^2, p_2)=1 \\ r^2-a_2f^2 \equiv 4c \pmod{(p_2f^2, m)}}} \left(\frac{a_2}{p_2}\right) \\ &= \lambda_f^r(p_1; c, m) \cdot \lambda_f^r(p_2; c, m). \end{aligned}$$

Part (c): Consider the case when $(\ell^\alpha, m) = \ell$ and $(f, \ell) = \ell$:

Using $(\ell,4)=1$, we apply the Chinese remainder theorem to obtain,

$$r^2 - af^2 \equiv 4c \pmod{\ell} \tag{9}$$

$$r^2 - af^2 \equiv 0 \pmod{4}. \tag{10}$$

But (10) is true since $(r^2-af^2, 4\ell^\alpha)=4$, so we can drop this condition. Since f contains a factor of ℓ, (9) can be rewritten as $r^2 \equiv 4c \pmod{\ell}$ and we are left with,

$$\lambda_f^r(\ell^\alpha; c, m) = \sum_{\substack{a \pmod{4\ell^\alpha)^*} \\ a\equiv 1 \pmod 4 \\ (r^2-af^2, 4\ell^\alpha)=4 \\ r^2 \equiv 4c \pmod{\ell}}} \left(\frac{a}{\ell}\right)^\alpha .$$

We have $m=\ell$ since $(m,\ell)=1$ and m,ℓ are prime. So if $r^2 \equiv 4c \pmod{m}$, then addressing $\lambda_f^r(\ell^\alpha; c, m)$ reduces to a case from [4]; otherwise, it is zero.

The other cases follow using similar approaches.

Part (d): We are considering

$$\lambda_1^r(2^\alpha; c, m) = \sum_{\substack{a \pmod{4\cdot 2^\alpha)^*} \\ a\equiv 1 \pmod 4 \\ (r^2-a, 4\cdot 2^\alpha)=4 \\ \frac{r^2-a}{4} \equiv c \pmod{(2^\alpha, m)}}} \left(\frac{a}{2^\alpha}\right) = \sum_{\substack{a \pmod{2^{\alpha+2})^*} \\ a\equiv 1 \pmod 4 \\ (r^2-a, 4\cdot 2^\alpha)=4 \\ \frac{r^2-a}{4} \equiv c \pmod{(2^\alpha, m)}}} \left(\frac{a}{2}\right)^\alpha . \tag{11}$$

If m is odd: $(2^\alpha, m)=1$ and so the last condition on the sum of equation (11) is trivial. Using earlier work, we obtain

$$\lambda_1^r(2^\alpha; c, m) = c_1^r(2^\alpha) = (-2)^\alpha/2.$$

If m is even: We write $m = 2^\beta m'$, where $2 \nmid m'$ and $\beta \geq 1$. Then we have $(2^\alpha, m) = 2^{\min(\alpha,\beta)}$ and

$$\frac{r^2-a}{4} \equiv c \pmod{(2^\alpha, m)} \implies r^2 - a \equiv 4c \pmod{2^{\min(\alpha,\beta)+2}}.$$

Equation 11 simplifies to

$$\lambda_1^r(2^\alpha; c, m) = \sum_{\substack{a \pmod{2^{\alpha+2})^*} \\ (r^2-a, 4\cdot 2)=4 \\ r^2-a \equiv 4c \pmod{2^{\min(\alpha,\beta)+2}}}} \left(\frac{a}{2}\right)^\alpha .$$

Next, we use the projection

$$(\mathbb{Z}/4\cdot 2^\alpha \mathbb{Z})^* \to (\mathbb{Z}/4\cdot 2^{\min(\alpha,\beta)}\mathbb{Z})^*$$

for the first condition on the sum in equation (11), which gives

$$\lambda_1^r(2^\alpha; c, m) = 2^{\alpha-\min(\alpha,\beta)} \sum_{\substack{a \pmod{2^{\min(\alpha,\beta)+2})^*} \\ (r^2-a, 4\cdot 2)=4 \\ r^2-a \equiv 4c \pmod{4\cdot 2^{\min(\alpha,\beta)}}}} \left(\frac{a}{2}\right)^\alpha .$$

Since m is even and $(c,m)=1$, c is odd. So the third condition on the sum above implies that $(r^2-a, 4\cdot 2)=4$. We also see that $r^2 - a \equiv 4c \pmod{4\cdot 2^{\min(\alpha,\beta)}}$ implies that there is one value of a which satisfies it (as c, r are fixed). Moreover, the value of the Kronecker symbol here only depends on the congruence class of a in mod 8. Thus the first and third conditions can be rewritten in mod 8 instead. The third condition reduces to $r^2 - a \equiv 4c \pmod 8$, but r and c are odd so we have $r^2 \equiv 1 \pmod 8$ and $4c \equiv 4 \pmod 8$. Putting this together we get $a \equiv 5 \pmod 8$. Leaving us with

$$\begin{aligned}\lambda_1^r(2^\alpha; c, m) &= 2^{\alpha - \min(\alpha,\beta)} \sum_{a \equiv 5 \pmod 8} \left(\frac{a}{2}\right)^\alpha \\ &= 2^{\alpha - \min(\alpha,\beta)} (-1)^\alpha \\ &= \frac{(-2)^\alpha}{2^{\min(\alpha,\beta)}}.\end{aligned}$$

Part (e): If $l \nmid m$, $4 \cdot (l^\alpha, m) = 1$ so $r^2 - a \equiv 4c \pmod 4 \equiv 0 \pmod 4$. Which is already implied by the third condition on our sum, $(r^2 - a, 4l^\alpha) = 4$. So, we end up with

$$\lambda_1^r(l^\alpha; c, m) = \sum_{\substack{a \pmod{4l^\alpha}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - a, 4l^\alpha) = 4}} \left(\frac{a}{l}\right)^\alpha = c_1^r(l^\alpha) = l^{\alpha - 1} \cdot \begin{cases} l - 1 - \left(\frac{r^2}{l}\right) & \text{if } \alpha \text{ is even,} \\ -\left(\frac{r^2}{l}\right) & \text{if } \alpha \text{ is odd.} \end{cases}$$

If $l | m$, we let $m = l^\beta m'$ where $l \nmid m'$ and $\beta \geq 1$. Then $(l^\alpha, m) = l^{\min(\alpha,\beta)}$, so

$$\lambda_1^r(l^\alpha; c, m) = \sum_{\substack{a \pmod{4l^\alpha}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - a, 4 \cdot l^{\min(\alpha,\beta)}) = 4 \\ r^2 - a \equiv 4c \pmod{4 \cdot l^{\min(\alpha,\beta)}}}} \left(\frac{a}{l}\right)^\alpha. \tag{12}$$

Consider the map $\mathbb{Z}/4 \cdot l^\alpha \mathbb{Z} \to \mathbb{Z}/4 \cdot l^{\min(\alpha,\beta)}\mathbb{Z}$. We use this with respect to the first condition on our sum in equation (12) to get

$$\lambda_1^r(l^\alpha; c, m) = l^{\alpha - \min(\alpha,\beta)} \sum_{\substack{a \pmod{4 \cdot l^{\min(\alpha,\beta)}}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - a, 4 \cdot l^{\min(\alpha,\beta)}) = 4 \\ r^2 - a \equiv 4c \pmod{4 \cdot l^{\min(\alpha,\beta)}}}} \left(\frac{a}{l}\right)^\alpha. \tag{13}$$

Now, the third condition in the sum above can be broken up into $(r^2 - a, 4) = 4$ and $(r^2 - a, l) = 1$. The fourth condition in (12) then implies

$$r^2 - a \equiv 4c \pmod 4 \equiv 0 \pmod 4 \implies (r^2 - a, 4) = 4,$$

using the fact that $(c, l) = 1$ since $(c, m) = 1$. We also get, $r^2 - a \equiv 4c \pmod l \implies (r^2 - a, l) = 1$. By the definition of the Kronecker symbol, we are only concerned with a reduced modulo l. Since l is odd we obtain

$$\lambda_1^r(l^\alpha; c, m) = l^{\alpha - \min(\alpha,\beta)} \cdot \left(\frac{r^2 - 4c}{l}\right)^\alpha.$$

Part (f): Note that if $(l^{\alpha+2}, m) = 1$, then our expression is identical to $c_l^r(l^\alpha)$ from David-Pappalardi and can be treated the same. Otherwise, we have

$$\lambda_l^r(l^\alpha; c, m) = \sum_{\substack{a \pmod{l^\alpha}^* \\ (r^2 - al^2, l^\alpha) = 1 \\ r^2 - al^2 \equiv 4c \pmod{(l^{\alpha+2}, m)}}} \left(\frac{a}{l}\right)^\alpha. \tag{14}$$

The second condition in the sum above tells us $(r^2 - al^2, l) = 1$. But this is always true since $al^2 \equiv 0 \pmod{l}$ and we have $l \nmid r$. So our third condition on the sum in equation (14) becomes $r^2 - al^2 \equiv 4c \pmod{m}$ which implies $r^2 \equiv 4c \pmod{m}$. Since $(l^{\alpha+2}, m) \neq 1$, we have that l and m are prime. So we have

$$\lambda_l^r(l^\alpha; c, m) = \sum_{\substack{a \pmod{l^\alpha}^* \\ r^2 \equiv 4c \pmod{m}}} \left(\frac{a}{l}\right)^\alpha,$$

and the result follows.

Part (g): This follows from applying results of parts (c) and (d) and using [4]. □

2.4. Determining the constant.

We will now express our constant as a product over primes. Recall that m is an odd prime and c is not divisible by m. We assume that r is an odd integer; later we will also specify that $(m, r) = 1$.

Lemma 2.3. *Let*

$$K_r(c, m) = \sum_{\substack{f=1 \\ (f,2r)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{\lambda_f^r(n; c, m)}{fn\phi\left([m, nf^2]\right)}, \tag{15}$$

where

$$\lambda_f^r(n; c, m) = \sum_{\substack{a \pmod{4n}^* \\ a \equiv 1 \pmod{4} \\ (r^2 - af^2, 4n) = 4 \\ \frac{r^2 - af^2}{4} \equiv c \pmod{(nf^2, m)}}} \left(\frac{a}{n}\right). \tag{16}$$

Then

$$K_r(c, m) = \frac{1}{\phi(m)} g(c, m) \prod_{\substack{\ell \mid r \\ \ell \nmid m}} \left(1 - \ell^{-2}\right)^{-1} \prod_{\substack{\ell \nmid r \\ \ell \nmid m}} \left(\frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)}\right),$$

where

$$g(c, m) = \begin{cases} \frac{m^2}{m^2 - 1}, & \text{if } \left(\frac{r^2 - 4c}{m}\right) = 0 \\ \frac{m}{m - 1}, & \text{if } \left(\frac{r^2 - 4c}{m}\right) = +1 \\ \frac{m}{m + 1}, & \text{if } \left(\frac{r^2 - 4c}{m}\right) = -1. \end{cases}$$

Proof. We write

$$K_r(c, m) = \sum_{\substack{f=1 \\ (f,2r)=1 \\ (f,m)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,m)=1}}^{\infty} \frac{\lambda_f^r(n; c, m)}{fn\phi\left([m, nf^2]\right)} + \sum_{\substack{f=1 \\ (f,2r)=1 \\ (f,m)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,m)>1}}^{\infty} \frac{\lambda_f^r(n; c, m)}{fn\phi\left([m, nf^2]\right)}$$

$$+\sum_{\substack{f=1\\(f,2r)=1\\(f,m)>1}}^{\infty}\sum_{n=1}^{\infty}\frac{\lambda_f^r(n;c,m)}{fn\phi\left([m,nf^2]\right)}.$$

Notation: We denote the first double sum as $K_r^{(1)}$, the second as $K_r^{(2)}$, and the third as $K_r^{(3)}$. Accordingly, we consider three cases.

Case 1: Assume $(m,nf^2)=1$. Then $\phi([m,nf^2])=\phi(m)\phi(nf^2)$. As $(m,nf^2)=1$,

$$\frac{r^2-af^2}{4}\equiv c \pmod{(nf^2,m)}\equiv c \pmod{1}.$$

which is already implied by $(r^2-af^2,4n)=4$. So,

$$\lambda_f^r(n;c,m)=c_f^r(n):=\sum_{\substack{a(4n)^*\\(r^2-af^2,4n)=4}}\left(\frac{a}{n}\right).$$

So we have

$$K_r^{(1)}=\sum_{\substack{f=1\\(f,2r)=1\\(f,m)=1}}^{\infty}\sum_{\substack{n=1\\(n,m)=1}}^{\infty}\frac{\lambda_f^r(n;c,m)}{fn\phi(nf^2)\phi(m)}=\frac{1}{\phi(m)}\sum_{\substack{f=1\\(f,2r)=1\\(f,m)=1}}^{\infty}\sum_{\substack{n=1\\(n,m)=1}}^{\infty}\frac{c_f^r(n)}{fn\phi(nf^2)}. \tag{17}$$

Consider $(n\phi(nf^2))^{-1}$ from the inner sum of (17). Replacing n by ℓ^α for some prime ℓ, we have

$$\frac{1}{\ell^\alpha\phi(\ell^\alpha f^2)}=\frac{1}{\ell^\alpha\phi(f^2)\phi(\ell^\alpha)}\frac{\phi((f^2,\ell^\alpha))}{(f^2,\ell^\alpha)}.$$

This allows us to write the inner sum in (17) as

$$\frac{1}{f\phi(f^2)}\sum_{\substack{n=1\\(n,m)=1}}^{\infty}\frac{c_f^r(n)}{n\phi(n)}\frac{\phi((f^2,n))}{(f^2,n)}.$$

Using Lemma 2.2 (b),

$$K_r^{(1)}=\frac{1}{\phi(m)}\sum_{\substack{f=1\\(f,2r)=1\\(f,m)=1}}^{\infty}\frac{1}{f\phi(f^2)}\prod_{\ell\nmid m}\left(\sum_{\alpha\geq 0}\frac{c_f^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}\frac{\phi((f^2,\ell^\alpha))}{(f^2,\ell^\alpha)}\right). \tag{18}$$

For the product in the equation above, we note that

$$\prod_{\ell\nmid m}\left(\sum_{\alpha\geq 0}\frac{c_f^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}\frac{\phi((f^2,\ell^\alpha))}{(f^2,\ell^\alpha)}\right)=\prod_{\ell\nmid m}\left(\sum_{\alpha\geq 0}\frac{c_1^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}\right)\prod_{\substack{\ell\nmid m\\ \ell\mid f}}\left(\frac{\sum_{\alpha\geq 0}\frac{c_f^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}\frac{\phi((f^2,\ell^\alpha))}{(f^2,\ell^\alpha)}}{\sum_{\alpha\geq 0}\frac{c_1^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}}\right).$$

We can then substitute this back into (18) and use multiplicativity to express the sum using products over primes.

$$K_r^{(1)}=\frac{1}{\phi(m)}\prod_{\ell\nmid m}\left(\sum_{\alpha\geq 0}\frac{c_1^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}\right)\prod_{\substack{p\nmid 2r\\ p\nmid m}}\left(\sum_{\beta\geq 0}\frac{1}{p^\beta\phi(p^{2\beta})}\right)\prod_{\substack{\ell\nmid m\\ \ell\mid p}}\left(\frac{\sum_{\alpha\geq 0}\frac{c_{p^\beta}^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}\frac{\phi((p^{2\beta},\ell^\alpha))}{(p^{2\beta},\ell^\alpha)}}{\sum_{\alpha\geq 0}\frac{c_1^r(\ell^\alpha)}{\ell^\alpha\phi(\ell^\alpha)}}\right)$$

$$= \frac{1}{\phi(m)} \prod_{\ell \nmid m} \left(\sum_{\alpha \geq 0} \frac{c_1^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} \right) \prod_{\substack{\ell \nmid 2r \\ \ell \nmid m}} \left(1 + \sum_{\beta \geq 1} \frac{1}{\ell^\beta \phi(\ell^{2\beta})} \frac{\sum_{\alpha \geq 0} \frac{c_\ell^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} \frac{\phi((\ell^{2\beta}, \ell^\alpha))}{(\ell^{2\beta}, \ell^\alpha)}}{\sum_{\alpha \geq 0} \frac{c_1^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)}} \right)$$

$$= \frac{1}{\phi(m)} \prod_{\substack{\ell \nmid m \\ \ell | 2r}} \left(\sum_{\alpha \geq 0} \frac{c_1^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} \right) \prod_{\substack{\ell \nmid 2r \\ \ell \nmid m}} \left(\sum_{\alpha \geq 0} \frac{c_1^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} + \sum_{\beta \geq 1} \frac{1}{\ell^\beta (\ell - 1) \ell^{2\beta - 1}} \left(1 + \sum_{\alpha \geq 1} \frac{c_\ell^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} \frac{\phi(\ell^\gamma)}{\ell^\gamma} \right) \right)$$

where $\gamma = \min\{2\beta, \alpha\}$,

$$= \frac{1}{\phi(m)} \prod_{\substack{\ell \nmid m \\ \ell | 2r}} \left(1 + \sum_{\alpha \geq 1} \frac{c_1^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} \right) \prod_{\substack{\ell \nmid 2r \\ \ell \nmid m}} \left(1 + \sum_{\alpha \geq 1} \frac{c_1^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} + \frac{1}{(\ell - 1)} \frac{\ell}{\ell^3 - 1} \left(1 + \sum_{\alpha \geq 1} \frac{c_\ell^r(\ell^\alpha)}{\ell^{2\alpha}} \right) \right).$$

Applying page 180 of [4], we obtain

$$K_r^{(1)} = \frac{1}{\phi(m)} \prod_{\substack{\ell | r \\ \ell \nmid m}} (1 - \ell^{-2})^{-1} \prod_{\substack{\ell \nmid r \\ \ell \nmid m}} \left(\frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)} \right). \tag{19}$$

Case 2: Assume $(m, f) = 1$ and $(m, n) > 1$. Then $[m, nf^2] = nf^2$. We consider

$$K_r^{(2)} = \sum_{\substack{f=1 \\ (f,2r)=1 \\ (m,f)=1}}^{\infty} \sum_{\substack{n=1 \\ (m,n)=m}}^{\infty} \frac{\lambda_f^r(n; c, m)}{fn\phi(nf^2)}, \tag{20}$$

where (since $(m, nf^2) = m$),

$$\lambda_f^r(n; c, m) = \sum_{\substack{a \pmod{4n}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - af^2, 4n) = 4 \\ \frac{r^2 - af^2}{4} \equiv c \pmod m}} \left(\frac{a}{n} \right) = \sum_{\substack{a \pmod{4n}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - af^2, 4n) = 4 \\ r^2 - af^2 \equiv 4c \pmod m}} \left(\frac{a}{n} \right).$$

as m is odd.

Since $\lambda_f^r(n; c, m)$ is a multiplicative function, given Lemma 2.2 (b), we can rewrite the inner sum of (20) as products over primes.

$$K_r^{(2)} = \sum_{\substack{f=1 \\ (f,2r)=1 \\ (m,f)=1}}^{\infty} \frac{1}{f\phi(f^2)} \prod_{\ell \nmid m} \left(\sum_{\alpha \geq 0} \frac{\lambda_f^r(\ell^\alpha; c, m)}{\ell^\alpha \phi(\ell^\alpha)} \frac{\phi((f^2, \ell^\alpha))}{(f^2, \ell^\alpha)} \right) \tag{21}$$

$$\cdot \prod_{\ell = m} \left(\sum_{\alpha \geq 1} \frac{\lambda_f^r(\ell^\alpha; c, m)}{\ell^\alpha \phi(\ell^\alpha)} \frac{\phi((f^2, \ell^\alpha))}{(f^2, \ell^\alpha)} \right)$$

Note that if $(\ell, m) = 1$, then $\lambda_f^r(\ell^\alpha; c, m) = c_f^r(\ell^\alpha)$. If $(\ell, m) > 1$ (and so $\ell = m$), then Lemma 2.2 (c) gives that $\lambda_f^r(\ell^\alpha; c, m) = \ell^{\alpha - 1} \left(\frac{r^2 - 4c}{\ell} \right)^\alpha$. So we get

$$K_r^{(2)} = \sum_{\substack{f=1 \\ (f,2r)=1 \\ (m,f)=1}}^{\infty} \frac{1}{f\phi(f^2)} \prod_{\ell \nmid m} \left(\sum_{\alpha \geq 0} \frac{c_f^r(\ell^\alpha)}{\ell^\alpha \phi(\ell^\alpha)} \frac{\phi((f^2, \ell^\alpha))}{(f^2, \ell^\alpha)} \right)$$

$$\cdot \prod_{\ell = m} \left(\sum_{\alpha \geq 1} \frac{\ell^{\alpha-1} \left(\frac{r^2-4c}{\ell}\right)^{\alpha}}{\ell^{\alpha}\phi(\ell^{\alpha})} \frac{\phi((f^2,\ell^{\alpha}))}{(f^2,\ell^{\alpha})} \right)$$

We simplify the final product of the expression above to get

$$\prod_{\ell = m} \left(\frac{1}{\ell - 1} \sum_{\alpha \geq 1} \frac{\left(\frac{r^2-4c}{\ell}\right)^{\alpha}}{\ell^{\alpha}} \right) = \frac{1}{\phi(m)} \sum_{\alpha \geq 1} \frac{\left(\frac{r^2-4c}{m}\right)^{\alpha}}{m^{\alpha}}.$$

Following [4], we eventually get

$$\prod_{\substack{\ell \mid 2r \\ \ell \nmid m}} \left(\sum_{\alpha \geq 0} \frac{c_1^r(\ell^{\alpha})}{\ell^{\alpha}\phi(\ell^{\alpha})} \right) \prod_{\substack{\ell \nmid 2r \\ \ell \nmid m}} \left(1 + \sum_{\alpha \geq 1} \frac{c_1^r(\ell^{\alpha})}{\ell^{\alpha}\phi(\ell^{\alpha})} + \frac{1}{(\ell-1)} \frac{\ell}{\ell^3 - 1} \left(1 + \sum_{\alpha \geq 1} \frac{c_\ell^r(\ell^{\alpha})}{\ell^{2\alpha}} \right) \right)$$

$$\cdot \frac{1}{\phi(m)} \sum_{\alpha \geq 1} \frac{\left(\frac{r^2-4c}{m}\right)^{\alpha}}{m^{\alpha}}$$

which gives

$$K_r^{(2)} = \frac{1}{\phi(m)} \prod_{\substack{\ell \mid r \\ \ell \nmid m}} \left(1 - \ell^{-2}\right)^{-1} \prod_{\substack{\ell \nmid r \\ \ell \nmid m}} \left(\frac{\ell(\ell^2 - \ell - 1)}{(\ell-1)(\ell^2-1)} \right) \cdot f(m), \tag{22}$$

where

$$f(m) := \sum_{\alpha \geq 1} \frac{\left(\frac{r^2-4c}{m}\right)^{\alpha}}{m^{\alpha}} = \begin{cases} 0, & \text{if } r^2 \equiv 4c \pmod{m} \\ \frac{1}{m-1}, & \text{if } \left(\frac{r^2-4c}{m}\right) = +1 \\ \frac{-1}{m+1}, & \text{if } \left(\frac{r^2-4c}{m}\right) = -1. \end{cases}$$

Case 3: Assume $(m, f) > 1$. Then $[m, nf^2] = nf^2$. We consider

$$K_r^{(3)} = \sum_{\substack{f=1 \\ (f,2r)=1 \\ (f,m)=m}}^{\infty} \sum_{n=1}^{\infty} \frac{\lambda_f^r(n; c, m)}{fn\phi(nf^2)}, \tag{23}$$

where (since $(m, nf^2) = m$),

$$\lambda_f^r(n; c, m) = \sum_{\substack{a \pmod{4n}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - af^2, 4n) = 4 \\ \frac{r^2-af^2}{4} \equiv c \pmod m}} \left(\frac{a}{n}\right) = \sum_{\substack{a \pmod{4n}^* \\ a \equiv 1 \pmod 4 \\ (r^2 - af^2, 4n) = 4 \\ r^2 \equiv 4c \pmod m}} \left(\frac{a}{n}\right).$$

Again following [4], this eventually leads to:

If $r^2 \equiv 4c \pmod{m}$,

$$K_r^{(3)} = \frac{1}{\phi(m)} \prod_{\substack{\ell \mid r \\ \ell \nmid m}} \left(1 - \ell^{-2}\right)^{-1} \prod_{\substack{\ell \nmid r \\ \ell \nmid m}} \left(\frac{\ell(\ell^2 - \ell - 1)}{(\ell-1)(\ell^2-1)} \right) \cdot \frac{1}{m^2 - 1}, \tag{24}$$

If $r^2 \not\equiv 4c \pmod{m}$, $K_r^{(3)} = 0$.

Summing cases: We sum the equations (19), (22), and (24), we get

$$\begin{aligned} K_r(c,m) &= K_r^{(1)} + K_r^{(2)} + K_r^{(3)} \\ &= \frac{1}{\phi(m)} g_r(c,m) \prod_{\substack{\ell \mid r \\ \ell \nmid m}} \left(1-\ell^{-2}\right)^{-1} \prod_{\substack{\ell \nmid r \\ \ell \nmid m}} \left(\frac{\ell(\ell^2-\ell-1)}{(\ell-1)(\ell^2-1)} \right), \end{aligned} \tag{25}$$

where

$$g_r(c,m) = \begin{cases} 1 + 0 + \frac{1}{m^2-1} &= \frac{m^2}{m^2-1}, \text{ if } \left(\frac{r^2-4c}{m}\right) = 0 \\ 1 + \frac{1}{m-1} + 0 &= \frac{m}{m-1}, \text{ if } \left(\frac{r^2-4c}{m}\right) = +1 \\ 1 + \frac{-1}{m+1} + 0 &= \frac{m}{m+1}, \text{ if } \left(\frac{r^2-4c}{m}\right) = -1. \end{cases}$$

□

3. Congruence class bias

In [16], we observed that, given some positive integer m, the distribution of supersingular primes on average was not evenly distributed over the invertible congruence classes of m. For example, on average there are twice as many supersingular primes congruent to $2 \pmod 3$ as there are congruent to $1 \pmod 3$. More generally, we observed that if m is an odd prime, the ratio of supersingular primes congruent to a quadratic residue of m, versus those congruent to a quadratic non-residue of m, is

$$\frac{m+1}{m-1}.$$

For an individual non-CM elliptic curve E, we recall that for sufficiently large primes p we have $E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow E(\mathbb{F}_p)$. For example, if 5 divides the order of $E(\mathbb{Q})_{\mathrm{tors}}$, then for a sufficiently large p, $a_p(E) \equiv p + 1 - |E(\mathbb{F}_p)| \equiv p + 1 \pmod 5$, and so if p is supersingular for E, then we must have $p \equiv 4 \pmod 5$.

One can conjecture that for any individual non-CM elliptic curve, if there is no obstruction arising from torsion, that there exists a congruence class bias for the distribution of supersingular primes, in accordance with the displayed formula above. (In Section 4, we briefly explore this conjecture computationally for a few elliptic curves.)

In this section, we take the opportunity to extend the above observations to non-supersingular cases, using equation (25) from Section 2. We use the notation from Section 2.2 (see equations (2) and (3)). We first observe that, for any odd $r \neq 3$, we have

$$K_r(1,3)/K_r(2,3) = 3/2.$$

This lies in contrast to the supersingular case, where $K_0(2,3)/K_0(1,3) = 2$. Note in particular that the direction of the bias has changed and that the strength of the bias has decreased.

In the case of $m = 5$ with odd $r \neq 5$, there are two possibilities:

$$K_r(1,5)/K_r(2,5) = \begin{cases} 1, & \text{for } r \equiv 1 \text{ or } 4 \bmod 5 \\ 5/6, & \text{for } r \equiv 2 \text{ or } 3 \bmod 5. \end{cases}$$

We again contrast this with the supersingular case, where $K_0(1,5)/K_0(2,5) = 3/2$, and note that the strength of the bias has decreased.

We lastly discuss the case of $m = 7$ with odd $r \neq 7$. There are three possibilities:

$$K_r(1,7)/K_r(2,7) = \begin{cases} 8/7, & \text{for } r \equiv 1 \text{ or } 6 \bmod 7 \\ 7/6, & \text{for } r \equiv 2 \text{ or } 5 \bmod 7 \\ 3/4, & \text{for } r \equiv 3 \text{ or } 4 \bmod 7. \end{cases}$$

This has a stronger bias compared to the supersingular case, which simply has $K_0(1,7)/K_0(2,7) = 1$ (the difference in outcome compared to the $m = 3$ and 5 cases is due to both 1 and 2 being quadratic residues mod 7). Even if we instead consider the ratio $K_0(1,7)/K_0(3,7) = 4/3$, we note that the bias is no stronger than in the odd $r \equiv 3, 4 \pmod 7$ case above.

In general, given equation (25), we observe that the possible biases for odd prime m with coprime odd r are of the form

$$1, \frac{m+1}{m}, \frac{m}{m-1}, \frac{m+1}{m-1},$$

or their inverses.

4. Computations

The biases demonstrated in Section 3 are on average over a family of infinite size. This means that we do not obtain information about any individual elliptic curve in the context of congruence class bias for the Lang–Trotter conjecture.

In this section we consider individual elliptic curves and examine whether the predictions from [16] seem to be consistent with our computational evidence.

We selected six elliptic curves, all without Complex Multiplication, and chosen to have varied ranks and torsion subgroups, from the LMFDB [10]. A table of these is presented below, using the LMFDB label of the curve. The torsion subgroup column refers to the isomorphism class of $E(\mathbb{Q})_{\text{tors}}$.

Elliptic curve	Conductor	Rank	Torsion subgroup
21.a1	21	0	$\mathbb{Z}/2\mathbb{Z}$
38.b2	38	0	$\mathbb{Z}/5\mathbb{Z}$
53.a1	53	1	trivial
55.a1	55	0	$\mathbb{Z}/4\mathbb{Z}$
65.a2	65	1	$\mathbb{Z}/2\mathbb{Z}$
83.a1	83	1	trivial

For each elliptic curve we used SAGE [12] to obtain a list of all supersingular primes less than 4×10^8. We then used Python [11] to partition these lists according to certain congruence classes. The overall run time on a standard laptop was 4 hours or more for each curve.

The first graph below finds, for each elliptic curve, the ratio of the number of supersingular primes less than x that are 2 mod 3 versus 1 mod 3. One can compare this to the result on average [16] which gives a ratio of 2.

Note that for all three graphs, the x-axes are labelled in increments of 10^8 and that the graphs have points plotted every 0.25×10^8 units, which are connected with straight lines.

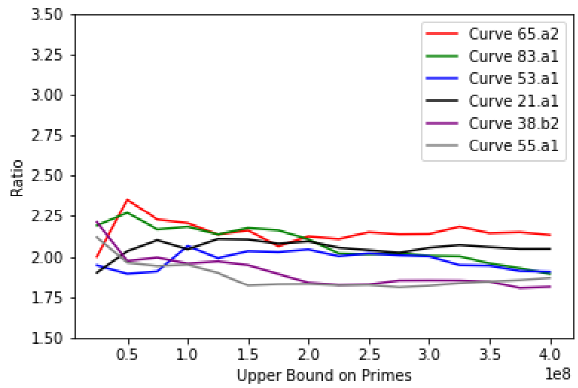

Figure 1: Ratio of supersingular primes that are 2 mod 3 versus 1 mod 3.

The next graph finds, for five of the six elliptic curves, the ratio of the number of supersingular primes less than x that are 1 mod 5 versus 2 mod 5. The ratio from the averaging result was 3/2.

Note that the curve 38.b2 was excluded from the graph below because it has 5-torsion. Recall that for sufficiently large p, we have $E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_p)$. So for curve 38.b2 we have $5 \mid \#E(\mathbb{F}_p)$ and therefore $a_p(E) = p + 1 - \#E(\mathbb{F}_p) \equiv p + 1 \pmod 5$. So if p is supersingular, then $p \equiv 4 \pmod 5$.

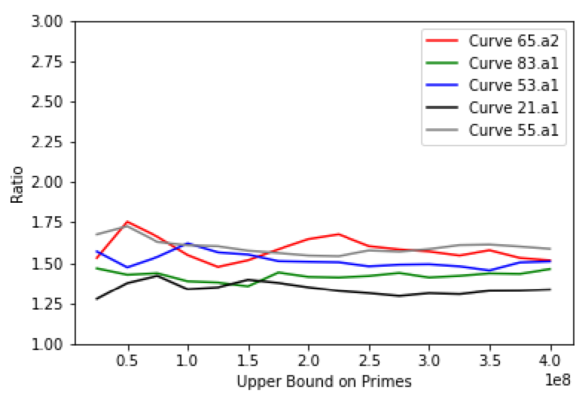

Figure 2: Ratio of supersingular primes that are 1 mod 5 versus 2 mod 5.

This final graph plots the ratio of the number of supersingular primes less than x that are 1 mod 7 versus 3 mod 7. (We did not consider the case of 1 mod 7 versus 2 mod 7 since no bias is predicted for that case.) The ratio from the averaging result was 4/3.

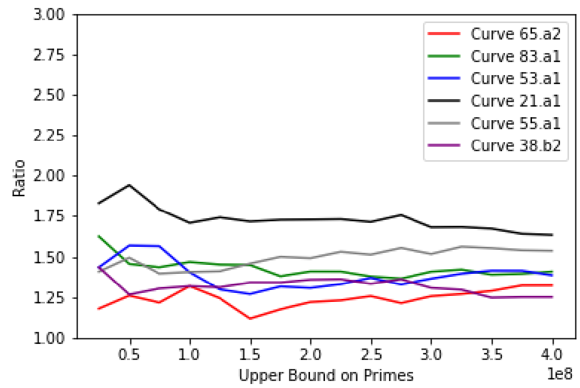

Figure 3: Ratio of supersingular primes that are 1 mod 7 versus 3 mod 7.

References

[1] Battista, J., Bayless, J., Ivanov, D., James, K. *Average Frobenius distributions for elliptic curves with nontrivial rational torsion.* Acta Arithmetica (2005) 119.1:81-91.

[2] B. J. Birch, How the number of points of an elliptic curve over a fixed prime field varies, J. London Math. Soc. 43 (1968), 57-60.

[3] Cojocaru, A., Shparlinski, I. *Distribution of Farey Fractions in Residue Classes and Lang-Trotter Conjectures on Average.* Proceedings of the American Mathematical Society (2008) 136.6:1977-1986.

[4] David, C., Pappalardi, F. *Average Frobenius Distributions of Elliptic Curves.* International Mathematics Research Notes (1999) 4:165-183.

[5] Fouvry, É., Murty, R. *On the Distribution of Supersingular Primes.* Canadian Journal of Mathematics (1996) 48.1:81-104.

[6] Fugleberg, N., Walji, N. *On the distribution of traces of Frobenius for families of elliptic curves and the Lang–Trotter conjecture on average.* Preprint. arXiv:2109.05661.

[7] James, K. *Average frobenius distributions for elliptic curves with 3-torsion.* Journal of Number Theory (2004) 109:278-298.

[8] James, K. *Averaging Special Values of Dirichlet L-Series.* The Ramanujan Journal (2005) 10:75–87.

[9] Lang, S., Trotter, H. *Frobenius Distributions in GL_2-Extensions.* Lecture Notes in Mathematics. Springer-Verlag, 1976.

[10] The LMFDB Collaboration, The L-functions and modular forms database, 2021.

[11] Python Software Foundation. Python Language Reference, version 3.11.

[12] SageMath, the Sage Mathematics Software System (Version 9.3), The Sage Developers, 2021.

[13] Sha, M., Shparlinski, I. *Lang-Trotter and Sato-Tate distributions in single and double parametric families of elliptic curves.* Acta Arithmetica 170: 299-325 (2015).

[14] Shparlinski, I. *On the Lang-Trotter and Sato-Tate Conjectures on Average for Polynomial Families of Elliptic Curves.* Michigan Mathematical Journal (2013) 62.3:491-505.

[15] Walji, N., *Supersingular distribution on average for congruence classes of primes.* Acta Arithmetica, 142: 387-400 (2010).

[16] Walji, N. *Supersingular distribution, congruence class bias, and a refinement of strong multiplicity one.* ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–California Institute of Technology.

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2, Canada