EXPLICIT LOWER BOUNDS ON THE MODULAR DEGREE OF AN ELLIPTIC CURVE

MARK WATKINS

Abstract. We give explicit lower bounds on the modular degree of a rational elliptic curve. The technique is via a convolution-type formula involving the symmetric-square L-function, for which an analogue of "no Siegel zeros" is known due to a result of Goldfeld, Hoffstein, and Lieman; our main task is to determine an explicit constant for their bound. Combined with an easy bound on the Faltings height in terms of the discriminant, this gives an explicit lower bound on the modular degree that is $\gg \frac{N^{7/6}}{\log N\sqrt{\log\log N}}$ where N is the conductor. This improves previous explicit bounds that were linear in N. In an appendix, we calculate the Euler factors and local conductors for symmetric power L-functions of an elliptic curve, a topic of independent interest.

1. Introduction

Let E be a rational elliptic curve of conductor N; by the work of Wiles [38] and others [35, 12, 9, 2] it is known that there is a surjective map ϕ from $X_0(N)$ to E known as a modular parametrisation. Our aim in this paper is prove explicit lower bounds on the degree of this parametrisation. Our starting point is a formula of convolution type essentially due to Shimura [31] (see also [14]) which states that

$$\deg\phi = \frac{Nc^2}{2\pi\Omega}\cdot L(\mathrm{Sym}^2 E, 1)\cdot\prod_{p^2|N} U_p(1)^{-1},$$

where $L(\mathrm{Sym}^2 E, s)$ is the motivic symmetric-square L-function of E normalised so that $s = 1/2$ is the point of symmetry, Ω is the area of the fundamental parallelogram associated to the curve, c is the Manin constant which is known to be an integer (see [13] or [33, 1.6]), and the $U_p(1)$ are fudge factors (normalised differently than in [37]) that will be given explicitly. One of our goals is to show a bound of the type $\deg\phi \gg \frac{N^{7/6}}{\log N\sqrt{\log\log N}}$ as $N\to\infty$. This has been known in folklore (see [22, p. 16] or Papikian's work [25] on the function field analogue) since the time of the Goldfeld, Hoffstein, and Lieman appendix [16] to the work of Hoffstein and Lockhart [17], but herein we give a more detailed proof and compute explicit constants. It is routine to show that $1/\Omega \gg |\Delta|^{1/6} \geq N^{1/6}$ via computations with the arithmetic-geometric mean, and we can show via prime number theory that the contribution from U_p-product (in conjunction with the quotient $|\Delta|/N$) is $\gg 1/\sqrt{\log\log N}$. This leaves us to bound $L(\mathrm{Sym}^2 E, 1) \gg 1/\log N$, which follows from [16]. We assume that $N \geq 20000$ as else the tables of Cremona [10] can be used; thus we can bound the symmetric-square conductor as $N^{(2)} \geq 142$,

One can obtain explicit lower bounds on the modular degree in a couple of other ways. As N. Elkies pointed out to us, an idea of Ogg [24] can be used to show $d = \deg\phi \gg N/p$ where p is any prime not dividing N. Here is the argument.

Reduce the modular parametrisation map mod p, and consider it over $\mathbf{F}_{p^2}$. There are at least $N(p-1)/12$ supersingular points on $X_0(N)/\mathbf{F}_p$, all defined over $\mathbf{F}_{p^2}$ (see [36, 4.1.52]). The elliptic curve has at most $(p+1)^2$ points in $\mathbf{F}_{p^2}$ each of which has at most d preimages, and these preimages must include all the $\mathbf{F}_{p^2}$-rational points. The estimate $d \geq \frac{N}{12}\frac{p-1}{(p+1)^2}$ follows.

One can make a "characteristic zero" version of this argument by using lower bounds for the eigenvalues of the Laplacian on $X_0(N)$ instead of supersingular points. The technique for passing from an eigenvalue bound to a modular degree bound appears in a paper of Li and Yau [21]; this is then made explicit both by Yau [39] and Abramovich [1]. The result is equivalent to $\deg\phi \geq \lambda N/48$, where λ is a lower bound for the smallest eigenvalue. Selberg [27, p. 13] conjectures that $\lambda \geq 1/4$; the best known [20] is $\lambda \geq 66/289$.

In the next section we bound the area Ω of the fundamental parallelogram in terms of the discriminant. Then we derive an explicit zero-free region for $L(\mathrm{Sym}^2 E, s)$ and then pass to a lower bound on $L(\mathrm{Sym}^2 E, 1)$. From this, after a short consideration of effects from isogenies, quadratic twists, and Manin constants, we get our desired lower bounds on the modular degree. The paper concludes with an appendix on Euler factors and local conductors for symmetric power L-functions on elliptic curves.

2. Bounding the area of the fundamental parallelogram

Let E be an elliptic curve, which we write in the form $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$ in such a way that the discriminant is minimal away from 2. The polynomial on the right side of this equation is sometimes called the 2-torsion polynomial. We have that Ω is the real period multiplied by (the imaginary part of) the imaginary period, where the periods are defined by expressions involving the arithmetic-geometric mean of the square roots of differences of the roots of the 2-torsion polynomial.

Lemma 2.1. *Let E be an elliptic curve, Ω the area of its fundamental parallelogram, and D the absolute value of its discriminant. Then $1/\Omega \geq \frac{D^{1/6}}{14.045}$.*

Proof. The proof naturally divides into 2 cases, depending on whether $\Delta > 0$.

Case I: positive discriminant. When the discriminant is positive the 2-torsion polynomial has three real roots, which we order as $e_1 > e_2 > e_3$. We then have that (see for instance [7, Chapter 7]) the real period of E is $\pi/\mathrm{agm}(\sqrt{e_1 - e_2}, \sqrt{e_1 - e_3})$ and the imaginary period is $\pi i/\mathrm{agm}(\sqrt{e_2 - e_3}, \sqrt{e_1 - e_3})$, and we also have that $\sqrt{\Delta/16} = (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. Let $t = \frac{e_1 - e_2}{e_1 - e_3}$ so that $0 < t < 1$ and $(e_1 - e_3)\cdot[4t(1-t)]^{1/3} = \Delta^{1/6}$, and recall that $\mathrm{agm}(x, y) = x\cdot\mathrm{agm}(1, y/x)$, implying

$$\begin{aligned} 1/\Omega &= \frac{1}{\pi^2}(e_1 - e_3)\cdot\mathrm{agm}\big(1, \sqrt{t}\big)\cdot\mathrm{agm}\big(1, \sqrt{1-t}\big) \\ &\geq \frac{1}{\pi^2}(e_1 - e_3)\cdot[4t(1-t)]^{1/3}\cdot\mathrm{agm}\big(1, 1/\sqrt{2}\big)^2 = \frac{D^{1/6}}{\pi^2}\cdot\mathrm{agm}\big(1, 1/\sqrt{2}\big)^2, \end{aligned}$$

where the inequality follows from calculus, the relevant quotient function being minimised at $t = 1/2$.

Case II: negative discriminant. When the discriminant is negative we let r be the real root of the 2-torsion polynomial, and write $\tilde{r} = r + b_2/12$, so that $-\tilde{r}/2 \pm iZ$ are the other roots. The real period is now $2\pi/\mathrm{agm}(2\sqrt{B}, \sqrt{2B + A})$

and the (vertical part of the) imaginary period is $\pi i/\mathrm{agm}(2\sqrt{B}, \sqrt{2B-A})$ where $A = 3r + b_2/4 = 3\tilde{r}$ and $B = \sqrt{3r^2 + b_2 r/2 + b_4/2} = \sqrt{(3\tilde{r}/2)^2 + Z^2}$. Also note that $2ZB^2 = \sqrt{-\Delta/16}$. Write $c = \tilde{r}/Z$, so that $A = 3cZ$ and $B = Z\sqrt{1+9c^2/4}$, so that $D^{1/6} = 2Z(1+9c^2/4)^{1/3}$. Writing $M(x) = \mathrm{agm}(1,x)$, we have

$$\begin{aligned}
1/\Omega &= \frac{1}{2\pi^2}\cdot 2\sqrt{B}\cdot \mathrm{agm}\left(1, \sqrt{\frac{2B+A}{4B}}\right)\cdot 2\sqrt{B}\cdot \mathrm{agm}\left(1, \sqrt{\frac{2B-A}{4B}}\right)\\
&= \frac{1}{2\pi^2}\cdot 4Z\sqrt{1+9c^2/4}\cdot M\left(\sqrt{\frac{1}{2}+\frac{3c}{\sqrt{16+36c^2}}}\right)\cdot M\left(\sqrt{\frac{1}{2}-\frac{3c}{\sqrt{16+36c^2}}}\right)\\
&= \frac{D^{1/6}}{\pi^2}\cdot (1+9c^2/4)^{1/6}\cdot M\left(\sqrt{\frac{1}{2}+\frac{3c}{\sqrt{16+36c^2}}}\right)\cdot M\left(\sqrt{\frac{1}{2}-\frac{3c}{\sqrt{16+36c^2}}}\right)\\
&\geq \frac{D^{1/6}}{\pi^2}\cdot 4^{1/6}\cdot \mathrm{agm}\left(1, \sqrt{\frac{1}{2}+\frac{\sqrt{3}}{4}}\right)\cdot \mathrm{agm}\left(1, \sqrt{\frac{1}{2}-\frac{\sqrt{3}}{4}}\right),
\end{aligned}$$

as the function is minimised at $c = \pm\sqrt{4/3}$. In both cases we have $1/\Omega \geq \frac{D^{1/6}}{14.045}$. □

3. Zero-free regions and lower bounds for symmetric square L-functions

We next turn to making the argument of [16] explicit. We first derive a zero-free region for $L(\mathrm{Sym}^2 E, s)$, and then turn this into a lower bound for $L(\mathrm{Sym}^2 E, 1)$.

3.1. Zero-free regions for curves without complex multiplication.

Lemma 3.1. *Let E be a rational elliptic curve of symmetric-square conductor $N^{(2)} \geq 142$ that does not have complex multiplication, and let $L(\mathrm{Sym}^2 f_E, s)$ be the symmetric-square L-function of f_E, where f_E is the form associated to E. Then the function $L(\mathrm{Sym}^2 f_E, s)$ has no real zeros with $s \geq 1 - \delta/\log(N^{(2)}/C)$, where $\delta = 2(5-2\sqrt{6})/5 \approx 0.040408$ and $C = 96$.*

Proof. We follow the proof in the appendix [16] of [17], which uses the idea that a function possessing a double pole at $s=1$ cannot have a triple zero that is too close to this pole. The product L-function in question (see page 180) is given by

$$\begin{aligned}
\mathbf{L}(s) &= \zeta(s)\cdot L(F,s)^2\cdot L(F\times F, s) = \zeta(s)\cdot L(F,s)^3\cdot L(\mathrm{Sym}^2 F, s)\\
&= \zeta(s)^2\cdot L(\mathrm{Sym}^2 f_E, s)^3\cdot L(\mathrm{Sym}^4 f_E, s)
\end{aligned}$$

where $F = \mathrm{Sym}^2 f_E$ and all L-functions of symmetric powers are motivic. As that paper notes earlier in a slightly different context (see page 167, after the proof of Lemma 1.2), we have that the Dirichlet series $\mathbf{L}(s)$ has nonnegative coefficients at primes of good reduction, and, more important for our immediate purposes, by taking the logarithmic derivative we see that $(\mathbf{L}'/\mathbf{L})(s)$ has nonpositive coefficients at such primes. It is asserted in [17] that the Langlands correspondence implies the nonpositivity at bad primes, but we are unable to verify this. For our case of elliptic curves, the proper Euler factor at bad primes is worked out in the appendix, and it can be verified that we do indeed have the desired nonpositivity. Note that Dąbrowski [11] claims to compute the Euler factors at bad primes in Lemma 1.2.3 on page 63 of that paper, but the method used therein appears to be erroneous.

We also need to compute the factor at infinity and the (analytic) conductor of $\mathbf{L}(s)$. For the factor at infinity we use pages 60–61 of [11]: we have a factor of $\Gamma(s/2)/\pi^{s/2}$ for $\zeta(s)$, a factor of $\Gamma(s+1)\Gamma\bigl((s+1)/2\bigr)/(4\pi^3)^{s/2}$ for $L(\mathrm{Sym}^2 f_E, s)$, and a factor of $\Gamma(s+2)\Gamma(s+1)\Gamma(s/2)/(16\pi^5)^{s/2}$ for $L(\mathrm{Sym}^4 f_E, s)$. For the bad primes, we refer to the appendix; we should note that we can bound the symmetric-square conductor by the square of the conductor, that is, $N^{(2)} \le N^2$, and similarly the symmetric-fourth-power conductor is bounded by the square of the symmetric-square conductor, that is, $N^{(4)} \le (N^{(2)})^2$. This would also follow from [5]. Note that the symmetric-square conductor is actually a square, and so some authors (for instance [37]) define it to be the square root of our choice here.

So we claim that

$$\Phi(s) = \Gamma(s/2)^3\Gamma(s+1)^4\Gamma\bigl((s+1)/2\bigr)^3\Gamma(s+2)\left(\frac{{N^{(2)}}^3 N^{(4)}}{1024\pi^{16}}\right)^{s/2}\cdot \\ \cdot\, \zeta(s)^2\cdot L(\mathrm{Sym}^2 f_E, s)^3\cdot L(\mathrm{Sym}^4 f_E, s)$$

is meromorphic and symmetric under the map $s \to 1-s$. The asserted analytic properties follow from work of Gelbart and Jacquet [15] and Shimura [30] for the symmetric square, and later authors such as Kim and Shahidi [19] for higher symmetric powers; in particular, the arithmetic and analytic conductors are equal. By Bump and Ginzburg [4], when f_E is not a $GL(1)$-lift (when E does not have complex multiplication), $\Phi(s)$ has a double pole at $s = 1$ (see also the work of Kim [18]).

So the function $s^2(1-s)^2\Phi(s) = e^{A+Bs}\prod_\rho(1-s/\rho)e^{s/\rho}$ is entire of order 1. By taking the logarithmic derivative, evaluating at $s = 0$ and $s = 1$, and using the functional equation, we get $B+\sum_\rho 1/\rho = 0$, where the order of summation is taken over conjugate pairs of zeros of $\Phi(s)$ so that the sum is convergent. Thus we have that $\sum_\rho \frac{w_\rho}{s-\rho} = \frac{2}{s-1} + \frac{2}{s} + \frac{\Phi'}{\Phi}(s)$, where w_ρ is the multiplicity of the zero ρ.

Now assume that $L(\mathrm{Sym}^2 f_E, s)$ has a zero at $\beta \ge 1-2(5-2\sqrt{6})/5\log(N^{(2)}/C)$. Then $\Phi(s)$ has a triple zero at β, so that we have

$$\frac{3}{s-\beta}+\frac{3}{s-(1-\beta)}+\sum_\rho \frac{w_\rho}{s-\rho} = \\ \frac{2}{s-1}+\frac{2}{s}+\frac{3}{2}\log N^{(2)}+\frac{1}{2}\log N^{(4)}-\log 32\pi^8+ \\ +\frac{3}{2}\frac{\Gamma'}{\Gamma}(s/2)+4\frac{\Gamma'}{\Gamma}(s+1)+\frac{3}{2}\frac{\Gamma'}{\Gamma}((s+1)/2)+\frac{\Gamma'}{\Gamma}(s+2)+\frac{\mathbf{L}'}{\mathbf{L}}(s),$$

where the sum over ρ is over the non-Siegel zeros of $\Phi(s)$.

We let $C = 96$ and write $\delta = (1-\beta)\log(N^{(2)}/C)$ and evaluate the above displayed equation at $s = \sigma = 1+\eta\delta/\log(N^{(2)}/C)$ where $\eta = \frac{1}{10\delta}\bigl[(2-5\delta)-\sqrt{25\delta^2-100\delta+4}\bigr]$ is the smaller positive root of $\frac{5}{2}\delta x^2+(\frac{5}{2}\delta-1)x+2$. Note that both roots are real and positive when $0 < \delta \le 2(5-2\sqrt{6})/5$. We get a crude lower bound of zero for the ρ-sum by pairing conjugate roots, whilst $(\mathbf{L}'/\mathbf{L})(\sigma) \le 0$, and so

$$\frac{3}{\sigma-\beta} \le \frac{2}{\sigma-1}+\frac{2}{\sigma}-\frac{3}{\sigma-(1-\beta)}+\frac{5}{2}\log N^{(2)}-\log 32\pi^8+ \\ +\frac{3}{2}\frac{\Gamma'}{\Gamma}(\sigma/2)+4\frac{\Gamma'}{\Gamma}(\sigma+1)+\frac{3}{2}\frac{\Gamma'}{\Gamma}((\sigma+1)/2)+\frac{\Gamma'}{\Gamma}(\sigma+2).$$

From this we get that

$$\frac{3}{\eta+1}\frac{\log(N^{(2)}/C)}{\delta}\leq$$
$$\frac{2\log(N^{(2)}/C)}{\eta\delta}+\frac{2}{\sigma}-\frac{3}{\sigma-(1-\beta)}+\frac{5}{2}\log(N^{(2)}/C)-\log 32\pi^8+$$
$$+\frac{3}{2}\frac{\Gamma'}{\Gamma}(\sigma/2)+4\frac{\Gamma'}{\Gamma}(\sigma+1)+\frac{3}{2}\frac{\Gamma'}{\Gamma}((\sigma+1)/2)+\frac{\Gamma'}{\Gamma}(\sigma+2)+\frac{5}{2}\log C,$$

and here the terms with $\log(N^{(2)}/C)$ cancel due to the definition of η. So we have

$$0\leq\frac{2}{\sigma}-\frac{3}{\sigma-(1-\beta)}-\log 32\pi^8+$$
$$+\frac{3}{2}\frac{\Gamma'}{\Gamma}(\sigma/2)+4\frac{\Gamma'}{\Gamma}(\sigma+1)+\frac{3}{2}\frac{\Gamma'}{\Gamma}((\sigma+1)/2)+\frac{\Gamma'}{\Gamma}(\sigma+2)+\frac{5}{2}\log C,$$

Now $\eta\delta$ is maximised at the endpoint where $\delta=2(5-2\sqrt{6})/5$ and thus $\eta=2+\sqrt{6}$, giving us that $\sigma\leq 1+2(\sqrt{6}-2)/5\log(N^{(2)}/C)$. Under our assumption that $N^{(2)}\geq 142$ and definition of $C=96$, this gives that $\sigma\leq 1.46$, so that

$$\frac{3}{2}\frac{\Gamma'}{\Gamma}(\sigma/2)+4\frac{\Gamma'}{\Gamma}(\sigma+1)+\frac{3}{2}\frac{\Gamma'}{\Gamma}((\sigma+1)/2)+\frac{\Gamma'}{\Gamma}(\sigma+2)\leq 1.74.$$

We also have that

$$\frac{2}{\sigma}-\frac{3}{\sigma-1+\beta}=\frac{2}{1+\eta\delta/\log(N^{(2)}/C)}-\frac{3}{1+\delta(\eta-1)/\log(N^{(2)}/C)}$$
$$\leq\frac{2}{1+2(\sqrt{6}-2)/5\log(N^{(2)}/C)}-\frac{3}{1+2(-7+3\sqrt{6})/5\log(N^{(2)}/C)}\leq -0.84,$$

so that we get the contradiction that $0\leq -0.84-12.62+1.74+\frac{5}{2}\log C\leq -0.30$. Thus there are no zeros in the region indicated. ☐

Remark 3.2. The constant δ can be improved if we could lower-bound $\sum_\rho\frac{1}{s-\rho}$ less crudely as some constant times $\log(N^{(2)})$, which is likely feasible by zero-counting arguments. The constant C can be improved simply by requiring $N^{(2)}$ to be larger.

3.2. **Zero-free regions for curves with complex multiplication.**

Lemma 3.3. *Let E be a rational elliptic curve of symmetric-square conductor $N^{(2)}\geq 142$ with complex multiplication by an order in the complex quadratic field K. Then $L(\mathrm{Sym}^2 f_E,s)$ has no real zeros with $\sigma\geq 1-\delta/\log(N^{(2)}/C)$, where here we have $\delta=2^{1/2}+2-2^{7/4}\approx 0.050628$ and $C=64$.*

Proof. When E has complex multiplication by an order of K, the representation associated to f_E is dihedral, and so by [18] the fourth symmetric power L-function has a pole at $s=1$, so that the $\Phi(s)$ of above has a triple pole at $s=1$. However, as noted in [16], in this case we have that $L(\mathrm{Sym}^2 f_E,s)$ can be factored. Recall that there is some Hecke character ψ of K such that $L(f_E,s)=L(\psi,K,s)$ with $\psi(z)=\chi(z)(z/|z|)$ for some character χ defined on the ring of integers of K. Here χ has order at most 6, and is of order 1 or 2 unless K is $\mathbf{Q}(i)$ or $\mathbf{Q}(\zeta_3)$. We have the factorisation $L(\mathrm{Sym}^2 f_E,s)=L(\theta_K,s)L(\psi^2,K,s)$ where θ_K is the quadratic character of the imaginary quadratic field K. Here ψ^2 is the "motivic" square of ψ, so that if $\psi(z)=\chi(z)(z/|z|)$ for some quadratic character χ, we then have $\psi^2(z)=(z/|z|)^2$. Thus the square of χ is the trivial character on K and not the principal character of the same modulus as χ. The same convention shall apply to higher symmetric powers.

Similar to the above factorisation of the symmetric-square L-function, by comparison of Euler factors we find that $L(\mathrm{Sym}^4 f_E, s) = \zeta(s)L(\psi^2, K, s)L(\psi^4, K, s)$ and $L(\mathrm{Sym}^6 f_E, s) = L(\theta_K, s)L(\psi^2, K, s)L(\psi^4, K, s)L(\psi^6, K, s)$. Here we can note that $L(\mathrm{Sym}^4 f_E, s)$ has a pole at $s = 1$ but $L(\mathrm{Sym}^6 f_E, s)$ does not.

For the seven choices of K with $\mathrm{disc}(K) < -4$, we thus have only one function $L(\psi^2, K, s)$ to consider, and a direct computation establishes the indicated zero-free region. For $K = \mathbf{Q}(i)$ we need to consider quartic twists, and for $K = \mathbf{Q}(\zeta_3)$ we need to consider both cubic and sextic twists. Note that Theorem 2 of Murty [23] erroneously only considers quadratic twists, and thus the proof that the modular degree is at least $N^{3/2-\epsilon}$ for elliptic curves with complex multiplication is wrong. In fact, simply by taking sextic twists of $X_0(27)$ we can easily achieve a growth rate of only $N^{7/6+\epsilon}$.

Case I: Gaussian field. We first consider the case where $K = \mathbf{Q}(i)$. Using the above decomposition of the symmetric-square L-function, we get that the completed L-function that is symmetric under $s \to 1 - s$ is

$$\left(\frac{N^{(2)}/4}{4\pi^2}\right)^{s/2} \Gamma(s+1)L(\psi^2, K, s).$$

In order for the fourth symmetric power to work out, we see that

$$\left(\frac{4N^{(4)}/N^{(2)}}{4\pi^2}\right)^{s/2} \Gamma(s+2)L(\psi^4, K, s)$$

is symmetric under $s \to 1 - s$. Here we have $N^{(4)} = N^{(2)}$ from the appendix, due to the fact that the relevant inertia groups are all C_2, C_4, or Q_8.

The standard ingredient of proofs of a zero-free region for a Hecke L-function is a trigonometric polynomial that is always nonnegative. Here we take $(1+\sqrt{2}\cos\theta)^2 = 2 + 2\sqrt{2}\cos\theta + \cos 2\theta$. A better result might come about from using higher degree cosine polynomials, but the Γ-factors might be burdensome. Also note that the work of Coleman [8] could be used if we did not need to be explicit. Note that at bad primes we still have the desired nonnegativity since $2 \geq \cos 2\theta$ for all θ.

So we are led to consider the nonpositive sum

$$\frac{\mathbf{L}'}{\mathbf{L}}(s) = 2\frac{\zeta'}{\zeta}(s) + 2\sqrt{2}\frac{L'}{L}(\psi^2, K, s) + \frac{L'}{L}(\psi^4, K, s).$$

We assume that $L(\mathrm{Sym}^2 f_E, s)$ has a zero at at $\beta \geq 1-(2^{1/2}+2-2^{7/4})/\log(N^{(2)}/C)$, and upon noting that $L(\theta_K, s)$ has no positive real zeros, we see that this implies that $L(\psi^2, K, \beta) = 0$. Taking the logarithmic derivatives of the Hadamard products of $s(1-s)\zeta(s)$, $L(\psi^2, K, s)$, and $L(\psi^4, K, s)$ gives us that

$$\frac{2\sqrt{2}}{s-\beta}+\frac{2\sqrt{2}}{s-(1-\beta)} + \sum_\rho \frac{w_\rho}{s-\rho} =$$
$$\frac{2}{s-1} + \frac{2}{s} + 2\log(1/\sqrt{\pi}) + 2\sqrt{2}\log(\sqrt{N^{(2)}}/4\pi) + \log(2/2\pi) +$$
$$+ \frac{2}{2}\frac{\Gamma'}{\Gamma}(s/2) + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(s+1) + \frac{\Gamma'}{\Gamma}(s+2) + \frac{\mathbf{L}'}{\mathbf{L}}(s),$$

where, in the sum over non-Siegel zeros, w_ρ is an appropriate weight for the zero.

We define $C = 100$ and write $\delta = (1-\beta)\log(N^{(2)}/C)$ and proceed to evaluate the above displayed equation at $s = \sigma = 1 + \eta\delta/\log(N^{(2)}/C)$ where η is given by the smaller positive root of $\delta\sqrt{2}x^2 + (\delta\sqrt{2} - 2\sqrt{2} + 2)x + 2$. Note that both roots are real and positive when $0 < \delta \le 2^{1/2} + 2 - 2^{7/4}$.

We again get a crude lower bound of zero for the ρ-sum by pairing conjugate roots and have that $(\mathbf{L}'/\mathbf{L})(\sigma) \le 0$, and so

$$\begin{aligned}\frac{2\sqrt{2}}{\sigma-\beta} \le & \frac{2}{\sigma-1} + \frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma-(1-\beta)} + \log(1/\pi) + \sqrt{2}\log N^{(2)} + \\ & + 2\sqrt{2}\log(1/4\pi) + \log(1/\pi) + \frac{\Gamma'}{\Gamma}(\sigma/2) + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(\sigma+1) + \frac{\Gamma'}{\Gamma}(\sigma+2).\end{aligned}$$

From this we get that

$$\begin{aligned}\frac{2\sqrt{2}}{\eta+1}\frac{\log(N^{(2)}/C)}{\delta} \le \frac{2\log(N^{(2)}/C)}{\eta\delta} & + \frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma-(1-\beta)} + \sqrt{2}\log(N^{(2)}/C) + \\ & + 2\log(1/\pi) + 2\sqrt{2}\log(1/4\pi) + \frac{\Gamma'}{\Gamma}(\sigma/2) + \\ & + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(\sigma+1) + \frac{\Gamma'}{\Gamma}(\sigma+2) + \sqrt{2}\log C\end{aligned}$$

and here the terms with $\log(N^{(2)}/C)$ cancel due to the definition of η. So we have

$$\begin{aligned}0 \le \frac{2}{\sigma} - & \frac{2\sqrt{2}}{\sigma-(1-\beta)} + 2\log(1/\pi) + 2\sqrt{2}\log(1/4\pi) + \\ & + \frac{\Gamma'}{\Gamma}(\sigma/2) + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(\sigma+1) + \frac{\Gamma'}{\Gamma}(\sigma+2) + \sqrt{2}\log C.\end{aligned}$$

Now $\delta\eta$ is maximised as $\sqrt{2}(2^{1/4}-1)$ when $\delta = 2^{1/2} + 2 - 2^{7/4}$, and so under our assumption that $N^{(2)} \ge 142$ and $C = 100$ we have that $\sigma \le 1.8$, so that the Γ-terms contribute less than 2.821. We also have that

$$\begin{aligned}\frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma-1+\beta} &= \frac{2}{1+\eta\delta/\log(N^{(2)}/C)} - \frac{2\sqrt{2}}{1+\delta(\eta-1)/\log(N^{(2)}/C)} \\ &\le \frac{2}{1+\sqrt{2}(2^{1/4}-1)/\log(N^{(2)}/C)} - \frac{2\sqrt{2}}{1+(3\cdot 2^{3/4} - 2\sqrt{2} - 2)/\log(N^{(2)}/C)} \\ &\le -0.612,\end{aligned}$$

so that we get the contradiction that $0 \le -0.612 - 9.448 + 2.821 + \sqrt{2}\log C \le -0.726$.

Case II: Eisenstein field. Next we consider the other case where $K = \mathbf{Q}(\zeta_3)$. By examining the above functional equations for symmetric-power L-functions, we find that

$$\left(\frac{N^{(2)}/3}{4\pi^2}\right)^{s/2}\Gamma(s+1)L(\psi^2, K, s), \left(\frac{3N^{(4)}/N^{(2)}}{4\pi^2}\right)^{s/2}\Gamma(s+2)L(\psi^4, K, s),$$

$$\text{and} \quad \left(\frac{N^{(6)}/3N^{(4)}}{4\pi^2}\right)^{s/2}\Gamma(s+3)L(\psi^6, K, s)$$

are all invariant under $s \to 1-s$. Using the appendix, the fact that all the relevant inertia groups are C_3 or C_6 implies that we have that $N^{(6)} = N^{(4)} = (N^{(2)})^2$ except in the case when $3^3 \| N$, when the inertia group Φ_3 is the semi-direct product $C_3 \rtimes C_4$ and we have $N^{(6)} = 9N^{(4)} = (N^{(2)})^2$.

Here we choose a trigonometric polynomial of the form $(1+\cos\theta)(1+\beta\cos\theta)^2$. It turns out that the optimal choice of β for our purposes is twice the positive root of $x^5-25x^4-4x^3+30x^2+19x+3$, approximately 2.629152166, but we do not lose much by taking $\beta=5/2$, so that our nonnegative trigonometric polynomial is $\frac{1}{16}(106+171\cos\theta+90\cos 2\theta+25\cos 3\theta)$. So we consider the nonpositive sum

$$\frac{\mathbf{L}'}{\mathbf{L}}(s)=106\frac{\zeta'}{\zeta}(s)+171\frac{L'}{L}(\psi^2,K,s)+90\frac{L'}{L}(\psi^4,K,s)+25\frac{L'}{L}(\psi^6,K,s),$$

with the nonpositivity at bad primes following as before.

Assume there is a zero of $L(\psi^2,K,s)$ at $\beta\geq 1-(554-12\sqrt{2014})/261\log(N^{(2)}/C)$. As before, via taking the logarithmic derivative of Hadamard products we get that

$$\begin{aligned}\frac{171}{s-\beta}+\frac{171}{s-(1-\beta)}+\sum_\rho\frac{w_\rho}{s-\rho}=&\\ \frac{106}{s-1}+\frac{106}{s}+106\log(1/\sqrt{\pi})+\frac{171}{2}\log(N^{(2)}/12\pi^2)+&\\ +45\log(N^{(4)}/N^{(2)})+45\log(3/4\pi^2)+\frac{25}{2}\log(N^{(6)}/N^{(4)})+\frac{25}{2}\log(1/12\pi^2)+&\\ +53\frac{\Gamma'}{\Gamma}(s/2)+171\frac{\Gamma'}{\Gamma}(s+1)+90\frac{\Gamma'}{\Gamma}(s+2)+25\frac{\Gamma'}{\Gamma}(s+3)+\frac{\mathbf{L}'}{\mathbf{L}}(s).&\end{aligned}$$

We let $C=64$ and $\delta=(1-\beta)\log(N^{(2)}/C)$ and proceed to evaluate the above displayed equation at $s=\sigma=1+\eta\delta/\log(N^{(2)}/C)$ where η is given by the smaller positive root of $261\delta x^2+(261\delta-130)x+212$. Note that both roots are real and positive when $0<\delta\leq(554-12\sqrt{2014})/261$.

We again get a crude lower bound of zero for the ρ-sum by pairing conjugate roots and have that $(\mathbf{L}'/\mathbf{L})(\sigma)\leq 0$, and so

$$\begin{aligned}\frac{171}{\sigma-\beta}\leq\frac{106}{\sigma-1}+\frac{106}{\sigma}-\frac{171}{\sigma-(1-\beta)}+\frac{261}{2}\log N^{(2)}+&\\ +53\log(1/\pi)-171\log\sqrt{12}+171\log(1/\pi)+&\\ +45\log 3/4+90\log(1/\pi)-25\log\sqrt{12}+25\log(1/\pi)+&\\ +53\frac{\Gamma'}{\Gamma}(s/2)+171\frac{\Gamma'}{\Gamma}(s+1)+90\frac{\Gamma'}{\Gamma}(s+2)+25\frac{\Gamma'}{\Gamma}(s+3)&\end{aligned}$$

From this and the definition of η we get

$$\begin{aligned}0\leq\frac{106}{\sigma}-\frac{171}{\sigma-(1-\beta)}+339\log(1/\pi)-\log(3^{53}2^{286})+\frac{261}{2}\log C&\\ +53\frac{\Gamma'}{\Gamma}(s/2)+171\frac{\Gamma'}{\Gamma}(s+1)+90\frac{\Gamma'}{\Gamma}(s+2)+25\frac{\Gamma'}{\Gamma}(s+3)&\end{aligned}$$

Now $\delta\eta$ is maximised as $(6\sqrt{2014}-212)/261$ when $\delta=(554-12\sqrt{2014})/261$, and so under our assumption that $N^{(2)}\geq 142$ and $C=64$ we have that $\sigma\leq 1.28$, so that the above Γ-sum is less than 153. We thus get the contradiction that $0\leq -59-644+543+153$.

We conclude the proof by noting that $(554-12\sqrt{2014})/261\approx 0.059266911$ so that the δ for $\mathbf{Q}(i)$ is worse, while the value of $C=64$ obtained for $\mathbf{Q}(\zeta_3)$ is worse. Combining the worst cases we get the statement of the lemma. $\square$

3.3. **Lower bounds from zero-free regions.** We use these zero-free regions to lower bound $L(\mathrm{Sym}^2 f_E, 1)$.

Lemma 3.4. *Let E be a rational elliptic curve with whose symmetric-square conductor satisfies $N^{(2)} \geq 142$. Then $L(\mathrm{Sym}^2 f_E, 1) \geq \frac{0.057}{\log N^{(2)}}$.*

Proof. We use Rademacher's formulation [26] of the Phragmén–Lindelöf Theorem to bound $L(\mathrm{Sym}^2 f_E, s)$ on the critical line $s = 1/2 + it$. First we can note that $|L(\mathrm{Sym}^2 f_E, 3/2 + it)| \leq \zeta(3/2)^3$, and thus by the functional equation we have that

$$|L(\mathrm{Sym}^2 f_E, -1/2 + it)| =$$
$$\begin{aligned} &= (N^{(2)}/4\pi^3)\frac{|\Gamma(5/2+it)|\cdot|\Gamma(5/4+it/2)|}{|\Gamma(1/2+it)|\cdot|\Gamma(1/4+it/2)|}|L(\mathrm{Sym}^2 f_E, 3/2+it)| \\ &\leq \zeta(3/2)^3\frac{N^{(2)}}{4\pi^3}\cdot\left|\frac{3}{2}+it\right|\cdot\left|\frac{1}{2}+it\right|\cdot\left|\frac{1}{4}+\frac{it}{2}\right| \leq \zeta(3/2)^3\frac{N^{(2)}}{8\pi^3}\cdot\left|\frac{3}{2}+it\right|^3. \end{aligned}$$

So using the result of Rademacher with $Q = 2$, $a = -1/2$, $b = 3/2$, $\alpha = 3$, $\beta = 0$, $A = \zeta(3/2)^3(N^{(2)}/8\pi^3)$, and $B = \zeta(3/2)^3$, we get that

$$|L(\mathrm{Sym}^2 f_E, 1/2+it)| \leq (A|5/2+it|^3)^{1/2}B^{1/2} = \zeta(3/2)^3\cdot\sqrt{\frac{N^{(2)}}{8\pi^3}}|5/2+it|^{3/2},$$

not an optimal bound, but sufficient. We also have $|\zeta(1/2+it)| \leq (t^2+5)^{1/4}$.

Let $b = 1 - \frac{4/99}{\log N^{(2)}}$ so that the previous lemmata imply $\mathbf{L}(s) = L(\mathrm{Sym}^2 f_E, s)\zeta(s)$ has no zeros in $[b, 1)$, and thus $\mathbf{L}(b) < 0$. Note also that $b \geq 0.99$ due to our assumption that $N^{(2)} \geq 142$. We write $\mathbf{L}(s) = \sum_n a_n/n^s$ as a Dirichlet series, noting that a_n majorises the characteristic function of the squares. By the Mellin transform we have $\sum_n \frac{a_n}{n^b}e^{-n/X} = \int_{(2)} \Gamma(s)X^s\mathbf{L}(s+b)\frac{ds}{2\pi i}$.

Via moving the contour to where the real part of s is $1/2 - b$, we get that the integral is $RX^{1-b}\Gamma(1-b) + \mathbf{L}(b) + E(X)$ where $R = L(\mathrm{Sym}^2 f_E, 1)$ and the error term $E(X)$ is bounded by $\frac{1}{\pi}\int_0^\infty \big|\Gamma(1/2-b+it)X^{1/2-b}\mathbf{L}(1/2+it)\big|dt$. Using Lemma 3 in [26] with $Q = (1-b)/2$ and $s = b/2 + it$ we get

$$\begin{aligned} |\Gamma(1/2-b+it)| = &\frac{|\Gamma(3/2-b+it)|}{|1/2-b+it|} \leq \frac{|\Gamma(1/2+it)|\cdot|3/2+it|^{1-b}}{|1/2-b+it|} \\ &\leq \frac{|3/2+it|^{0.01}}{|0.49+it|}\cdot|\Gamma(1/2+it)| = \frac{(9/4+t^2)^{1/200}}{\sqrt{0.49^2+t^2}}\sqrt{\pi\mathrm{sech}\pi t} \end{aligned}$$

We compute that

$$\frac{\zeta(3/2)^3}{\sqrt{8\pi^3}}\int_0^\infty\left(\frac{25}{4}+t^2\right)^{3/4}\cdot(t^2+5)^{1/4}\cdot\frac{(9/4+t^2)^{1/200}}{\sqrt{0.49^2+t^2}}\sqrt{\pi\mathrm{sech}\pi t}\,dt < 15,$$

and so $|E(X)| \leq 5\sqrt{N^{(2)}}\cdot X^{1/2-b}$. Now $\mathbf{L}(b) \leq 0$ and a_n majorises the squares, so

$$\sum_m \frac{1}{m^2}e^{-m^2/X} \leq \sum_n \frac{a_n}{n^b}e^{-n/X} \leq RX^{1-b}\Gamma(1-b) + 5\sqrt{N^{(2)}}/X^{0.49}.$$

We take $X = (10^5 N^{(2)})^{50/49}$, so that $N^{(2)} \geq 142$ implies $X \geq 10^7$. The left-end of the display is $\int_{(2)} X^s\zeta(2s+2)\Gamma(s)\frac{ds}{2\pi i} \geq \zeta(2) + \Gamma(-1/2)/\sqrt{X} \geq 1.644$ and so $1.644 \leq RX^{1-b}\Gamma(1-b) + 0.016$. Noting that $\log X \leq 3.4\log N^{(2)}$, we see that $X^{1-b} \leq \exp\left(\frac{3.4}{99/4}\right) \leq 1.15$. By using $\Gamma(1-b) \leq \frac{99}{4}\log N^{(2)}$, we get $R \geq \frac{0.057}{\log N^{(2)}}$. □

4. Isogenous curves, Manin constants, and factors from twists and bad primes

Finally we can turn to the other objects in our formula for the modular degree. Using Shimura's formula, Lemma 3.4, and Lemma 2.1, we have that

$$\frac{\deg\phi}{c^2} \geq \frac{N}{2\pi\Omega}\frac{0.057}{\log N^{(2)}}\cdot\prod_{p^2|N}U_p(1)^{-1} \geq \frac{ND^{1/6}}{1550\log N^{(2)}}\cdot\prod_{p^2|N}U_p(1)^{-1}.$$

To bound the effects from the $U_p(1)^{-1}$, we recall their definition. First we assume that E is a quadratic minimal twist; this is like requiring that the model of E be minimal at every prime, except that now we further require that it be minimal when also considering quadratic twists. See the author's paper [37] for details. For a minimal twist we have that $U_p(s) = (1-\epsilon_p/p^s)^{-1}$ where $\epsilon_p = +1, 0, -1$, depending on certain properties of inertia groups (see [37]). In particular, we have that $\epsilon_p = +1$ for all primes congruent to 1 mod 12, and $\epsilon_p = -1$ for all primes congruent to 11 mod 12. When p is 5 mod 12 we have that $\epsilon_p = +1$ exactly when $p^2|c_6$ and $p\|c_4$, while these conditions imply that $\epsilon_p = -1$ for primes that are 7 mod 12. Note in particular that $U_p(1)^{-1}$ is greater than 1 for primes that are 11 mod 12. Also, when $U_p(1)^{-1}$ is less than 1 for primes that are 5 mod 12, we have that $p^3|D$ while $p^2\|N$. Writing N_p and D_p for the local conductor and discriminant at a prime p, we thus have $N_pD_p^{1/6}U_p(1)^{-1} \geq N_p^{7/6}p^{1/6}(1-1/p) \geq N_p^{7/6}$, with this being true for all primes $p\geq 5$ with $p\equiv 2 \pmod 3$. Finally we need to consider $p=2$ and $p=3$. Though we know that we can have $\epsilon_3 = +1$ only when $3^4\|N$, this does not help us much and there is not much to be done with $U_3(1)^{-1}$ except lower-bound it as $1-1/3 = 2/3$. In order for $\epsilon_2 = +1$ we need $2^8\|N$ and $2^9\|D$, so that $N_2D_2^{1/6}U_2(1)^{-1} \geq N_2^{7/6}2^{1/6}(1-1/2)$. Thus for a minimal twist we have

$$\frac{\deg\phi}{c^2} \geq \frac{N^{7/6}}{1550\log N^{(2)}}\cdot 2^{1/6}(1-1/2)\cdot(1-1/3)\cdot\prod_{\substack{p^2|N\\ p\equiv 1\,(3)}}(1-1/p).$$

We can estimate the product over primes using facts from prime number theory; for $N\geq 20000$ the logarithm of the product is bounded by

$$-\sum_{\substack{p^2|N\\ p\equiv 1\,(3)}}\frac{1}{p} - \sum_{p\equiv 1\,(3)}\frac{1/2p^2}{1-1/p} \geq (-0.5\log\log\log N + 0.22) - 0.02,$$

and so for every minimal twist we have that

$$(*)\qquad \frac{\deg\phi}{c^2} \geq \frac{N^{7/6}}{4150\log N^{(2)}}\frac{e^{1/5}}{\sqrt{\log\log N}} \geq \frac{N^{7/6}}{\log N^{(2)}}\frac{1/3400}{\sqrt{\log\log N}}.$$

We wish to compare what happens on each side of this inequality upon twisting our curve by an odd prime p, noting that the value of the motivic symmetric-square function $L(\mathrm{Sym}^2 E, 1)$ is invariant under quadratic twists. There are three cases, depending on the reduction type of the minimal twist F at p. If F has additive reduction, then the curves F and E have the $U_p(s)$, the conductor stays the same, and $1/\Omega$ increases by a factor of p. So Shimura's formula tells us that $\frac{\deg\phi}{c^2}$ goes up by p upon twisting, whilst the right side of the inequality stays the same, implying that $(*)$ is true for F. If F has multiplicative reduction at p, we have that $U_p(s)^{-1} = (1-1/p^{s+1})$. Here the conductor goes up by p upon twisting, as does $1/\Omega$, with $\frac{\deg\phi}{c^2}$ gaining a factor of $p\cdot p\cdot(1-1/p^2)=(p^2-1)$. This is bigger than the factor of $p^{7/6}$ that is an upper bound for the increase of the right side, so again $(*)$ is true for F. Finally, if the minimal twist F has good reduction at p we have that $U_p(1)^{-1}=(p-1)(p+1-a_p)(p+1+a_p)/p^3$ where a_p is the trace of Frobenius for F. The conductor goes up by p^2 and again $1/\Omega$ rises by a factor of p. So $\frac{\deg\phi}{c^2}$ goes up by $(p-1)(p+1-a_p)(p+1+a_p)$, which is bigger than the factor of $p^{7/3}$ that bounds the gain of the right side, even when $p=3$ and $a_p=\pm3$. So the above inequality is true for curves that are twist-minimal at 2.

Finally, we consider what happens upon twisting by -1 or 2. If $2^8|N$, the right side of $(*)$ stays the same upon twisting, while $\frac{\deg\phi}{c^2}$ stays the same or doubles. Otherwise, we have $U_2(1)^{-1}\geq(2-1)(2+1-2)(2+1+2)/2^3=5/8$ and get

$$\frac{\deg\phi}{c^2}\geq\frac{ND^{1/6}}{1550\log N^{(2)}}\cdot\frac{5}{8}\frac{2}{3}\cdot\frac{e^{1/5}}{\sqrt{\log\log N}}\geq\frac{N^{7/6}}{\log N^{(2)}}\frac{1/3050}{\sqrt{\log\log N}}.$$

So the above inequality $(*)$ is true for every rational elliptic curve.

5. Summary of results

We give a summary of the various lower bounds that we have obtained, recalling that from [13] we have $c^2\geq1$ for the Manin constant.

Theorem 5.1. *Suppose that E is a rational semistable elliptic curve. Then*

$$\deg\phi_E\geq\frac{N}{2\pi\Omega}\frac{0.057}{2\log N}\geq\frac{N^{7/6}}{3100\log N}.$$

Theorem 5.2. *Suppose that E is a rational elliptic curve. Then*

$$\deg\phi_E\geq\frac{N}{2\pi\Omega}\frac{0.057}{\log N^{(2)}}\cdot\prod_{p^2|N}U_p(1)^{-1}\geq\frac{N^{7/6}}{\log N}\cdot\frac{1/6800}{\sqrt{\log\log N}}.$$

Remark 5.3. Note we need $N\geq e^{84}$ in order to get $\deg\phi\geq N$ from Theorem 5.2. Also, one can improve the constant 6800 to 5100 by taking N sufficiently large in the various estimates.

Appendix A. Euler factors and conductors of symmetric power L-functions

In this appendix we compute the local conductors and Euler factors for the symmetric power L-functions of a rational elliptic curve. This was done for the symmetric square by Coates and Schmidt [6], and for the symmetric cube by Buhler, Schoen, and Top [3]. We stress that we are only computing the "arithmetic" conductors corresponding to l-adic representations, and make no claims about whether these conductors should occur in conjectured functional equations for the symmetric power L-functions. Note that Dąbrowski [11] claims to compute the Euler factors (Lemma 1.2.3), but the method appears to be erroneous.

A.1. **Notation for symmetric powers.** In our consideration of the conductors and Euler factors of symmetric powers, we follow the arguments of [3], page 123 and following, and [6], page 108–110 and appendices, recalling that in [37] we indicated a few minor errors in the latter. All of our L-functions shall be normalised so that $s=1/2$ is the point of symmetry in the functional equation; this is distinct from other works.

We let E be an elliptic curve, and write $\epsilon_p^{(m)}$ and $\delta_p^{(m)}$ for the tame and wild local conductors at p of the mth symmetric power of E, so that the global conductor of $\mathrm{Sym}^m E$ is $N^{(m)} = \prod_p p^{\delta_p^{(m)}+\epsilon_p^{(m)}}$. We can compute $\epsilon_p^{(1)}$ and $\delta_p^{(1)}$ from an algorithm of Tate [34], and can thus take those as given. For a given prime p, we take an auxiliary odd prime $l \neq p$. We write E_l for the l-division points of E and T_l for its Tate module and $V_l = T_l \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$, where each of these modules has a natural $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-structure. We define $H_l^1(E) = \mathrm{Hom}_{\mathbf{Q}_l}(V_l, \mathbf{Q}_l)$, and consider the l-adic representation $\rho_l^{(m)} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(\mathrm{Sym}^m(H_l^1(E)))$.

We now explain the standard manner to attach an Euler product to $\rho_l^{(m)}$. Let $\mathbf{G}_p \supseteq \Phi_p$ denote a decomposition group and its inertia group for p in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. We define the Euler factor at p by

$$P_p^{(m)}(X) = \det(\mathbf{1} - \rho_l^{(m)}(\mathrm{Frob}_p^{-1})X | \mathrm{Sym}^m(H_l^1(E))^{\Phi_p}).$$

The L-series of $\mathrm{Sym}^m E$ is then given by $L(\mathrm{Sym}^m E, s) = \prod_p P_p^{(m)}(p^{-s})^{-1}$. The tame part of the conductor of the mth symmetric power is given by the expression $\epsilon_p^{(m)} = (m+1) - \dim_{\mathbf{Q}_l}(\mathrm{Sym}^m(H_l^1(E))^{\Phi_p})$ and the wild part is

$$\delta_p^{(m)} = \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|} \dim_{\mathbf{F}_l}(M/M^{G_i})$$

where $M = \mathrm{Sym}^m E_l$ and $G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$ denote the series of higher ramification groups for the extension of local fields $\mathbf{Q}_p(E_l)/\mathbf{Q}_p$. We also write $\rho_p^{(m)} = m + 1 - \epsilon_p^{(m)} = \dim_{\mathbf{Q}_l}(\mathrm{Sym}^m(H_l^1(E))^{\Phi_p})$. Note that $\delta_p^{(m)} = 0$ for all m for $p \geq 5$, since there is no wild ramificiation in this case.

We also have notation for the Euler factors, writing $L(\mathrm{Sym}^m E, s) = \prod_p U_p^{(m)}(s)$. When E has multiplicative reduction at p we have that $U_p^{(1)}(s) = (1 - \kappa_p/p^{s+1/2})^{-1}$, where $\kappa_p = \pm 1$. Indeed, we have a quadratic extension $K/\mathbf{Q}_p$ such that E is isomorphic over K to the Tate curve E_t for a suitable $t \in \mathbf{Q}_p^{\times}$, and $\kappa_p = \hat{\kappa}(-1)$ where $\hat{\kappa}$ is the quadratic character of $K/\mathbf{Q}_p$. Similarly, when E has potential multiplicative reduction at p, we are still able to compute κ_p in this manner, though $U_p^{(1)}(s) \equiv 1$ as $\epsilon_p^{(1)} = 2$ in this case. By the Néron–Ogg–Safarevic criterion (see Silverman's book [32]) and Serre–Tate [29], when E has good or potentially good reduction at p, we have some complex number α_p (defined up to complex conjugacy) of unit modulus with $\det(\mathbf{1} - \rho_l(\mathrm{Frob}_p^{-1})X | H_l^1(E) \otimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l) = (1 - \alpha_p X)(1 - \bar{\alpha}_p X)$. When E has good reduction at p this gives us that $U_p^{(1)}(s) = (1 - \alpha_p/p^s)^{-1}(1 - \bar{\alpha}_p/p^s)^{-1}$, while we have $U_p^{(1)}(s) \equiv 1$ when E has potentially good reduction at p. So for every prime p we have either some α_p of unit modulus or $\kappa_p = \pm 1$ associated to it.

A.2. **Euler factors and local conductors.**

A.2.1. *Good and multiplicative reduction.* Now we compute the local conductors and Euler factors of the symmetric powers. When E has good reduction at p, we get that $\epsilon_p^{(m)} = \delta_p^{(m)} = 0$ for all m, as the associated representations are all trivial. The Euler factors are $U_p^{(m)}(s) = \prod_{i=0}^{m} (1 - \alpha_p^{m-2i}/p^s)^{-1}$. When E has multiplicative reduction at p, we get that $\epsilon_p^{(m)} = m$ and $\delta_p^{(m)} = 0$ for all m, using the filtration of [3]. From Lemma 1.2.4 of [11] we find that $U_p^{(m)}(s) = (1 - \kappa_p^m/p^{s+m/2})^{-1}$. Similarly, when E has potential multiplicative reduction at p, for m odd we have that $\epsilon_p^{(m)} = m+1$ and thus $U_p^{(m)}(s) \equiv 1$, while for m even, as with the multiplicative case we have $\epsilon_p^{(m)} = m$ and $U_p^{(m)}(s) = (1 - 1/p^{s+m/2})^{-1}$. Here we have that $\delta_2^{(m)} = \frac{m+1}{2}\delta_2^{(1)}$ for odd m and $\delta_2^{(m)} = 0$ for even m (see the $\Phi_2 = C_2$ case below), while $\delta_3^{(m)} = 0$ for all m.

A.2.2. *Potentially good reduction.* Finally there is the case of potentially good reduction. We write Φ_p for the (nontrivial) inertia subgroup of the extension $\mathbf{Q}_p(E_l)/\mathbf{Q}_p$, and $W_l = H_l^1(E) \otimes_{\mathbf{Q}_l} \bar{\mathbf{Q}}_l$, where Φ_p acts trivially on the second factor. From the work of Serre [28] we know that there are only a few possibilities for Φ_p: when $p \geq 5$ it is a cyclic group C_d for one of $d = 2, 3, 4, 6$; when $p = 2$ it can also be either the quaternion group Q_8 or $SL_2(\mathbf{F}_3)$; when $p = 3$ it can also be the semi-direct product $C_3 \rtimes C_4$.

A.2.3. *Potentially good reduction, cyclic inertia.* We first consider the case where Φ_p is cyclic of order d, so we can represent the action of it on W_l via the generating diagonal matrix $\tau_p = \begin{pmatrix} \zeta_d & 0 \\ 0 & \zeta_d^{-1} \end{pmatrix}$. From this, we readily see that the eigenvalues of the mth symmetric power are ζ_d^{j-k} for various nonnegative j and k with $j+k = m$. The invariant subspaces correspond to eigenvalues of $+1$, and so we compute the dimensions as indicated in Table 1 below, where the values of $\rho_p^{(m)}(\Phi_p)$ are listed; note that the values follow a pattern of period 12 in m and are independent of p.

Next we consider the Euler factors in this case. Let $\sigma_p \in \mathrm{Gal}(\mathbf{Q}_p(E_{l^\infty})/\mathbf{Q}_p)$ be such that it maps to the inverse of the Frobenius element of the Galois group of the residue fields. There are two possibilities for σ_p; when the decomposition group $\mathbf{G}_p$ is abelian we have that σ_p commutes with τ_p and so fixes the eigenspaces of W_l, and otherwise it swaps the eigenspaces. In the first case we get that the eigenvalues of σ_p restricted to the invariant subspace of the mth symmetric power of W_l are α_p^{j-k} for values of $j - k$ that are multiples of d. Since we have $k = m - j$, this is the same as requiring $d|(2j - m)$ where we still have $0 \leq j \leq m$. So we get that

$$U_p^{(m)}(s) = \prod_{\substack{0 \leq j \leq m \\ d|(2j-m)}} (1 - \alpha_p^{2j-m}/p^s)^{-1}.$$

Next suppose that $\mathbf{G}_p$ is nonabelian; as [6] points out on the top of page 110, this implies that $\sigma = \sigma_p$ swaps the eigenspaces of W_l. We claim that $\alpha = \alpha_p = \pm i$. Indeed, from [29] we have that $\det(I - \sigma X|W_l) = (1 - \alpha X)(1 - X/\alpha)$ while we have that $\sigma(u) = \alpha v$ and $\sigma(v) = -u/\alpha$ where u and v be basis elements for the eigenspaces. So the above determinant is $1 + X^2$, and thus the trace of σ is zero, implying that $\alpha = \pm i$ as claimed.

By basic properties of tensor products we can compute directly that σ maps $(u^{\otimes j} \otimes v^{\otimes k})_S \oplus \lambda(v^{\otimes j} \otimes u^{\otimes k})_S$ to $\lambda(-1)^j\alpha^{k-j}[(u^{\otimes j} \otimes v^{\otimes k})_S \oplus \frac{\alpha^{j-k}(-1)^k}{\lambda(-1)^j\alpha^{k-j}}(v^{\otimes j} \otimes u^{\otimes k})_S]$, so that $\lambda^2(-1)^{j-k}\alpha^{2k-2j} = 1$. Here the S-subscript denotes the symmetrization with respect to the ordering in the tensor product. Since $\alpha^2 = -1$, this implies that $\lambda^2 = 1$. The eigenvalue is $\lambda(-1)^j\alpha^{k-j}$. When m is odd we get a pair of eigenvalues $\pm i$ coming from taking $\lambda = \pm 1$, both of which correspond to an invariant subspace. Similarly, when m is even and $j \neq m/2$ we get a pair of eigenvalues ± 1. When $j = k = m/2$ we have $\lambda = +1$, and so the eigenvalue is $(-1)^j$. So in the case

Table 1. Values of $\rho_p^{(m)}$ for various inertia groups Φ_p; here $\tilde{m}$ is m modulo 12. The values for C_3 and C_6 are the same except when m is odd, in which case $\rho_p^{(m)}(C_6) = 0$ while $\rho_p^{(m)}(C_3)$ is as listed.

$\tilde{m}$	C_2	C_3, C_6	C_4	Q_8	$C_3 \rtimes C_4$	$SL_2(\mathbf{F}_3)$
0	$m+1$	$(m+3)/3$	$(m+2)/2$	$(m+4)/4$	$(m+6)/6$	$(m+12)/12$
1	0	$C_3 : (m-1)/3$	0	0	0	0
2	$m+1$	$(m+1)/3$	$m/2$	$(m-2)/4$	$(m-2)/6$	$(m-2)/12$
3	0	$C_3 : (m+3)/3$	0	0	0	0
4	$m+1$	$(m-1)/3$	$(m+2)/2$	$(m+4)/4$	$(m+2)/6$	$(m-4)/12$
5	0	$C_3 : (m+1)/3$	0	0	0	0
6	$m+1$	$(m+3)/3$	$m/2$	$(m-2)/4$	$m/6$	$(m+6)/12$
7	0	$C_3 : (m-1)/3$	0	0	0	0
8	$m+1$	$(m+1)/3$	$(m+2)/2$	$(m+4)/4$	$(m+4)/6$	$(m+4)/12$
9	0	$C_3 : (m+3)/3$	0	0	0	0
10	$m+1$	$(m-1)/3$	$m/2$	$(m-2)/4$	$(m-4)/6$	$(m-10)/12$
11	0	$C_3 : (m+1)/3$	0	0	0	0

that Φ_p is cyclic but $\mathbf{G}_p$ is nonabelian we get that $U_p(s) = (1+1/p^{2s})^{-\rho_p^{(m)}/2}$ for odd m and $U_p(s) = (1-1/p^{2s})^{-[\rho_p^{(m)}-1]/2}(1-(-1)^{m/2}/p^s)^{-1}$ for even m.

A.2.4. *Potentially good reduction, noncyclic inertia.* Now we turn to the cases of noncyclic Φ_p. It will be convenient to record the following trace formula for the symmetric powers of a representation ρ:

$$\mathrm{tr}(\rho^{\otimes m}) = \sum_{k=0}^{m/2} \binom{m-k}{k} \mathrm{tr}(\rho)^{m-2k}(-1)^k.$$

First we consider $\Phi_2 = Q_8$, where we have $\mathbf{G}_2 = SD_{16}$, that is, the semi-dihedral group of order 16, for the decomposition group. The character of the unique 2-dimensional faithful representation (of determinant 1 in a field of characteristic 0) of Q_8 sends the identity to 2, the order two element to -2, and everything else to 0. Now it is easy to use the above trace formula to compute the size of the invariant subspace of the symmetric powers (take the inner product of the mth power with the identity), getting that $\epsilon_2^{(m)}(Q_8)$ is $m+1$ for m odd, is $m+1-(m-2)/4$ for m congruent to 2 mod 4, and is $m+1-(m+4)/4$ when $4|m$. So $U_2^{(m)}(s) \equiv 1$ for m odd, and we need only consider m even when considering Euler factors. This Q_8-representation is generated by $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; we could also choose the off-diagonal matrix to be $\begin{pmatrix} 0 & \zeta_8^3 \\ \zeta_8 & 0 \end{pmatrix}$. In either case, we obtain SD_{16} by adjoining the matrix $\begin{pmatrix} \zeta_8^3 & 0 \\ 0 & \zeta_8 \end{pmatrix}$. Now the inverse Frobenius element image in SD_{16}/Q_8 can be taken so that it either fixes or swaps the eigenspaces of W_l. From the latter we have that $\alpha = \pm i$ as above. Denote by σ a representative of the inverse Frobenius in $\mathbf{G}_2$ that fixes the eigenspaces with $\sigma(u) = \alpha u$ and $\sigma(v) = v/\alpha$, where as before u and v are basis elements for the eigenspaces. The fixed eigenspaces of the mth symmetric power will be sums of spaces of the form $(u^{\otimes j} \otimes v^{\otimes k})_S \oplus \lambda(v^{\otimes j} \otimes u^{\otimes k})_S$,

TABLE 2. Values of $\epsilon_p^{(m)}$ for small m.

Φ_p	1	2	3	4	5	6	7	8	9	10	11	12
C_2	2	0	4	0	6	0	8	0	10	0	12	0
C_3	2	2	2	4	4	4	6	6	6	8	8	8
C_4	2	2	4	2	6	4	8	4	10	6	12	6
C_6	2	2	4	4	6	4	8	6	10	8	12	8
Q_8	2	3	4	3	6	6	8	6	10	9	12	9
$SL_2(\mathbf{F}_3)$	2	3	4	5	6	6	8	8	10	11	12	11
$C_3 \rtimes C_4$	2	3	4	4	6	6	8	7	10	10	12	10

where $j+k=m$ and the S-subscript again denotes symmetrization. By applying σ we get $\alpha^{j-k}[(u^{\otimes j}\otimes v^{\otimes k})_S \oplus \lambda\frac{\alpha^{k-j}}{\alpha^{j-k}}(v^{\otimes j}\otimes u^{\otimes k})_S]$ so that the eigenvalue is α^{j-k}. Now the (j,j) entry of the mth symmetric power of $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ must equal $+1$, and so we have $1 = i^j(-i)^k = i^{j-k} = \alpha^{j-k}$. Thus all the σ-eigenvalues are equal to $+1$ when m is even. So the Euler factor here is $U_2^{(m)}(s) = (1-1/2^s)^{-\rho_2^{(m)}(Q_8)}$.

Remark A.1. One can view this as saying that the invariant Q_8-eigenspaces are precisely the C_4-eigenspaces that have eigenvalue $+1$ under the action of σ.

Next we have the case where $\Phi_2 = SL_2(\mathbf{F}_3)$. Note that [6] erroneously claims on page 110 that there is a normal subgroup of order 3. The desired representation here is generated by $\begin{pmatrix} 1 & \zeta_6 \\ \zeta_6^2 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. One obtains $\mathbf{G}_2 = GL_2(\mathbf{F}_3)$ by adjoining $\begin{pmatrix} \zeta_8^3 & 0 \\ 0 & \zeta_8 \end{pmatrix}$, and again we can choose σ so that it either fixes or swaps the eigenspaces of W_l. By the above trace formula, we compute that $\epsilon_2^{(m)}(SL_2(\mathbf{F}_3))$ is $m+1$ when m is odd, and is as in Table 1 when m is even. As before the Euler factor is $(1-1/2^s)^{-\rho_2^{(m)}(SL_2(\mathbf{F}_3))}$.

Finally we consider $\Phi_3 = C_3 \rtimes C_4$. Here the representation is generated by $\begin{pmatrix} \zeta_6 & 0 \\ 0 & \zeta_6^5 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. One obtains the group $\mathbf{G}_3$ of order 24 by adjoining $\begin{pmatrix} \zeta_6 & 0 \\ 0 & \zeta_6^2 \end{pmatrix}$, and again we can choose σ so that it either fixes or swaps the eigenspaces of W_l. By the above trace formula, we compute that $\epsilon_3^{(m)}(C_3 \rtimes C_4)$ is $m+1$ when m is odd, and is as in the Table 1 when m is even. As before the Euler factor is $(1-1/3^s)^{-\rho_3^{(m)}(C_3\rtimes C_4)}$.

Remark A.2. As above with Q_8, one can view this as saying that the invariant $(C_3 \rtimes C_4)$-eigenspaces are precisely the C_3-eigenspaces that have eigenvalue $+1$ under the action of σ.

So now we have computed the values of $\epsilon_p^{(m)}$ (or equivalently those of $\rho_p^{(m)}$) and the Euler factors for all symmetric power L-functions of E. The only "unknown" is whether $\mathbf{G}_p$ is abelian, which can be computed via a congruence-based condition as in [37].

TABLE 3. Values of $\delta_3^{(m)}$ for small m.

Φ_3	t	1	2	3	4	5	6	7	8	9	10	11	12	formula
C_3	(1)	2	2	2	4	4	4	6	6	6	8	8	8	$\epsilon_3^{(m)}(C_3)$
C_6	(2)	2	2	2	4	4	4	6	6	6	8	8	8	$\epsilon_3^{(m)}(C_3)$
$C_3 \rtimes C_4$	(2)	1	1	1	2	2	2	3	3	3	4	4	4	$\epsilon_3^{(m)}(C_3)/2$
$C_3 \rtimes C_4$	(6)	3	3	3	6	6	6	9	9	9	12	12	12	$\frac{3}{2}\epsilon_3^{(m)}(C_3)$

A.3. **Computation of wild conductors.** We now conclude by computing the values of $\delta_p^{(m)}$ following the ideas of the appendix of [6]. Here we use the above formula for $\delta_p^{(m)}$, and plug in the values of the finitely many possibilities (derived from [6]) for the ramification sequence $\Phi_p = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$.

A.3.1. *At the prime 3.* When $\Phi_3 = C_3$, we have $G_1 = C_3$ and $G_2 = \mathrm{id}$. So we get that $\delta_3^{(m)}(C_3) = \epsilon_3^{(m)}(C_3)$. When $\Phi_3 = C_6$, we have $G_1 = G_2 = C_3$ and $G_3 = \mathrm{id}$. So we get that $\delta_3^{(m)}(C_6) = \epsilon_3^{(m)}(C_3)$. When $\Phi_3 = C_3 \rtimes C_4$ there are two cases; we have $G_1 = G_2 = C_3$ and $G_3 = \mathrm{id}$, or $G_1 = G_6 = C_3$ and $G_7 = \mathrm{id}$. In the first case we have $\delta_3^{(m)}(C_3 \rtimes C_4) = \frac{1}{2}\epsilon_3^{(m)}(C_3)$ and in the second case we have $\delta_3^{(m)}(C_3 \rtimes C_4) = \frac{3}{2}\epsilon_3^{(m)}(C_3)$.

TABLE 4. Values of $\delta_2^{(m)}$ for small m.

Φ_2	t	1	2	3	4	5	6	7	8	formula
C_2	(1)	2	0	4	0	6	0	8	0	$\epsilon_2^{(m)}(C_2)$
C_2	(2)	4	0	8	0	12	0	16	0	$2\epsilon_2^{(m)}(C_2)$
C_4	(2,2)	6	4	12	4	18	8	24	8	$2\epsilon_2^{(m)}(C_4) + \epsilon_2^{(m)}(C_2)$
C_6	(3)	2	0	4	0	6	0	8	0	$\epsilon_2^{(m)}(C_2)$
C_6	(6)	4	0	8	0	12	0	16	0	$2\epsilon_2^{(m)}(C_2)$
Q_8	(1,0,2)	3	3	6	3	9	6	12	6	$\epsilon_2^{(m)}(Q_8) + \frac{1}{2}\epsilon_2^{(m)}(C_2)$
Q_8	(1,0,4)	4	3	8	3	12	6	16	6	$\epsilon_2^{(m)}(Q_8) + \epsilon_2^{(m)}(C_2)$
Q_8	(1,2,4)	6	5	12	5	18	10	24	10	$\epsilon_2^{(m)}(Q_8)+\epsilon_2^{(m)}(C_4)+\epsilon_2^{(m)}(C_2)$
$SL_2(\mathbf{F}_3)$	(1,2)	1	1	2	1	3	2	4	2	$\frac{1}{3}\epsilon_2^{(m)}(Q_8) + \frac{1}{6}\epsilon_2^{(m)}(C_2)$
$SL_2(\mathbf{F}_3)$	(1,8)	2	1	4	1	6	2	8	2	$\frac{1}{3}\epsilon_2^{(m)}(Q_8) + \frac{2}{3}\epsilon_2^{(m)}(C_2)$
$SL_2(\mathbf{F}_3)$	(1,20)	4	1	8	1	12	2	16	2	$\frac{1}{3}\epsilon_2^{(m)}(Q_8) + \frac{5}{3}\epsilon_2^{(m)}(C_2)$
$SL_2(\mathbf{F}_3)$	(5,10)	5	5	10	5	15	10	20	10	$\frac{5}{3}\epsilon_2^{(m)}(Q_8) + \frac{5}{6}\epsilon_2^{(m)}(C_2)$

A.3.2. *At the prime 2.* When $\Phi_2 = C_2 = G_1$ there are two possibilities; either $G_2 = \mathrm{id}$ or $G_2 = C_2$ and $G_3 = \mathrm{id}$. In either case we have that $\delta_2^{(m)} = \frac{m+1}{2}\delta_2^{(1)}$ for odd m and $\delta_2^{(m)} = 0$ for even m. When $\Phi_2 = C_6$ there are two possibilities; either $G_1 = G_3 = C_2$ with $G_4 = \mathrm{id}$ or $G_1 = G_6 = C_2$ with $G_7 = \mathrm{id}$. In either case we have that $\delta_2^{(m)} = \frac{m+1}{2}\delta_2^{(1)}$ for odd m and $\delta_2^{(m)} = 0$ for even m. When $\Phi_2 = C_4$, we must have $G_1 = G_2 = C_4$, $G_3 = G_4 = C_2$, and $G_5 = \mathrm{id}$. We find that $\delta_2^{(m)}(C_2)$ is $2\epsilon_2^{(m)}(C_4)$ for even m and $2\epsilon_2^{(m)}(C_4) + \epsilon_2^{(m)}(C_2) = 3\epsilon_2^{(m)}(C_2)$ for odd m.

When $\Phi_2 = Q_8$ there are now three possibilities. First we can have $G_1 = Q_8$ and $G_2 = G_3 = C_2$ and $G_4 = \mathrm{id}$, in which case $\delta_2^{(m)} = \epsilon_2^{(m)}(Q_8) + \frac{1}{2}\epsilon_2^{(m)}(C_2)$. We denote this by $t = (1,0,2)$ to indicate that the ramification sequence contains one copy of Q_8, zero of C_4, and two of C_2. Secondly, we can have the case of $t = (1,0,4)$ where we have $G_1 = Q_8$ and $G_2 = G_5 = C_2$ with $G_6 = \mathrm{id}$, in which case we have $\delta_2^{(m)} = \epsilon_2^{(m)}(Q_8) + \epsilon_2^{(m)}(C_2)$. Finally, there is the case erroneously excluded by Coates-Schmidt, denoted by $t = (1,2,4)$, where we have $G_1 = Q_8$ and $G_2 = G_3 = C_4$ and $G_4 = G_7 = C_2$ and $G_8 = \mathrm{id}$, in which case our computation as above gives us that $\delta_2^{(m)} = \epsilon_2^{(m)}(Q_8) + \epsilon_2^{(m)}(C_4) + \epsilon_2^{(m)}(C_2)$.

Finally, when $\Phi_2 = SL_2(\mathbf{F}_3)$ there are four possibilities (see appendix to [6]). We can have $G_1 = Q_8$ and $G_2 = G_3 = C_2$ and $G_4 = \mathrm{id}$, in which case we get that $\delta_2^{(m)} = \frac{1}{3}\epsilon_2^{(m)}(Q_8) + \frac{1}{6}\epsilon_2^{(m)}(C_2)$. This is denoted by $t = (1,2)$ to indicate that there is one copy of Q_8 and two copies of C_2 in the ramification sequence. Secondly we can have $t = (1,8)$ for which $G_1 = Q_8$ and $G_2 = G_9 = C_2$ and $G_{10} = \mathrm{id}$, in which case $\delta_2^{(m)} = \frac{1}{3}\epsilon_2^{(m)}(Q_8) + \frac{2}{3}\epsilon_2^{(m)}(C_2)$. Thirdly we can have $t = (1,20)$ where $G_1 = Q_8$ and $G_2 = G_{21} = C_2$ and $G_{22} = \mathrm{id}$, in which case $\delta_2^{(m)} = \frac{1}{3}\epsilon_2^{(m)}(Q_8) + \frac{5}{3}\epsilon_2^{(m)}(C_2)$. Finally, we can have $t = (5,10)$ when $G_1 = G_5 = Q_8$ and $G_6 = G_{15} = C_2$ and $G_{16} = \mathrm{id}$, in which case $\delta_2^{(m)} = \frac{5}{3}\epsilon_2^{(m)}(Q_8) + \frac{5}{6}\epsilon_2^{(m)}(C_2)$.

In these cases (and also with the semi-direct product case for Φ_3), we can determine the ramification sequence already from knowledge of the (local) conductor of the elliptic curve, which can be computed via an algorithm of Tate [34]. Also, Serre [28] notes on page 312 that we can determine Φ_p for $p \geq 5$ via knowledge of the p-valuation of the discriminant; for $p = 2, 3$ a similar method can be used, in conjunction with information about the conductor. In Tables 3-4 we list the values of $\delta_p^{(m)}$ for various small m.

References

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves.* Internat. Math. Res. Notices 1996, no. 20, 1005–1011.

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises.* J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[3] J. Buhler, C. Schoen, J. Top, *Cycles, L-functions and triple products of elliptic curves.* J. Reine Angew. Math. **492** (1997), 93–133.

[4] D. Bump, D. Ginzburg, *Symmetric square L-functions on* $\mathrm{GL}(r)$. Ann. of Math. (2) **136** (1992), no. 1, 137–205.

[5] C. Bushnell, G. Henniart, *An upper bound on conductors for pairs.* J. Number Theory **65** (1997), no. 2, 183–196.

[6] J. Coates, C.-G. Schmidt, *Iwasawa theory for the symmetric square of an elliptic curve.* J. Reine Angew. Math. **375/376** (1987), 104–156.

[7] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics 138. Springer–Verlag, New York, 1993.

[8] M. D. Coleman, *A zero-free region for the Hecke L-functions.* Mathematika **37** (1990), no. 2, 287–304.

[9] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations.* J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[10] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1992. Second edition 1997. Data at `www.maths.nottingham.ac.uk/personal/jec/`

[11] A. Dąbrowski, *On the symmetric power of an elliptic curve.* Algebraic K-theory (Poznań, 1995), 59–82, Contemp. Math., 199, Amer. Math. Soc., Providence, RI, 1996.

[12] F. Diamond, *On deformation rings and Hecke rings.* Ann. of Math. (2) **144** (1996), no. 1, 137–166.

[13] B. Edixhoven, *On the Manin constants of modular elliptic curves.* In *Arithmetic algebraic geometry (Texel, 1989),* edited by G. van der Geer, F. Oort, and J. Steenbrink, 25–39, Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991.

[14] M. Flach, *On the degree of modular parametrizations.* In *Séminaire de Théorie des Nombres, Paris 1991–92,* edited by S. David, 23–36, Progr. Math., 116, Birkhäuser Boston, Boston, MA, 1993.

[15] S. Gelbart, H. Jacquet, *A relation between automorphic forms on* GL(2) *and* GL(3). Ann. Sci. École Norm. Sup. (4) **11** (1978), no. 4, 471–542.

[16] D. Goldfeld, J. Hoffstein, D. Lieman, appendix to [17].

[17] J. Hoffstein, P. Lockhart, *Coefficients of Maass forms and the Siegel zero.* With an appendix by D. Goldfeld, J. Hoffstein, and D. Lieman. Ann. of Math. (2) **140** (1994), no. 1, 161–181.

[18] H. H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2. J. Amer. Math. Soc. **16** (2003), no. 1, 139–183.

[19] H. H. Kim, F. Shahidi, *Cuspidality of symmetric powers with applications.* Duke Math. J. **112** (2002), no. 1, 177–197.

[20] H. H. Kim, F. Shahidi, *Functorial products for* $\mathrm{GL}_2 \times \mathrm{GL}_3$ *and the symmetric cube for* GL_2. With an appendix by C. J. Bushnell and G. Henniart. Ann. of Math. (2) **155** (2002), no. 3, 837–893.

[21] P. Li, S. T. Yau, *A new conformal invariant and its applications to the Willmore conjecture and the first eigenvalue of compact surfaces.* Inv. Math. **69** (1982), 269–291.

[22] B. Mazur, *Three Lectures about the Arithmetic of Elliptic Curves.* Notes from lectures given at the 1998 Arizona Winter School. URL: `swc.math.arizona.edu/notes/files/98MazurLN.ps`

[23] M. R. Murty, *Bounds for congruence primes,* in Automorphic Forms, Automorphic Representations and Arithmetic, edited by R. Doran, Ze-Li Dou and G. Gilbert, Proceedings of Symposia in Pure Mathematics, Vol. 66, Part 1, pp. 177-192, Amer. Math. Soc., 1999.

[24] A. P. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France **102** (1974), 449–462.

[25] M. Papikian, *On the degree of modular parametrizations over function fields.* J. Number Theory **97** (2002), no. 2, 317–349.

[26] H. Rademacher, *On the Phragmén-Lindelöf theorem and some applications.* Math. Z. **72** (1959/1960), 192–204.

[27] A. Selberg, *On the estimation of Fourier coefficients of modular forms.* Proc. Sympos. Pure Math., Vol. VIII, 1–15, Amer. Math. Soc., Providence, 1965.

[28] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* (French) [Galois properties of points of finite order of elliptic curves.] Invent. Math. **15** (1972), no. 4, 259–331.

[29] J.-P. Serre, J. Tate, *Good reduction of abelian varieties.* Ann. of Math. (2) **88** (1968), 492–517.

[30] G. Shimura, *On the holomorphy of certain Dirichlet series.* Proc. London Math. Soc. (3) 31 (1975), no. 1, 79–98.

[31] G. Shimura, *The special values of the zeta functions associated with cusp forms.* Comm. Pure Appl. Math **29** (1976), no. 6, 783–804.

[32] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer–Verlag, New York, 1986.

[33] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves.* Invent. Math. **98** (1989), no. 1, 75–106.

[34] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In *Modular functions of one variable IV*, edited by B. Birch and W. Kuyk, 33–52, Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.

[35] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[36] M. A. Tsfasman, S. G. Vlăduţ, *Algebraic-geometric codes.* Translated from the Russian by the authors. Mathematics and its Applications (Soviet Series), 58. Kluwer Academic Publishers Group, Dordrecht, 1991.

[37] M. Watkins, *Computing the modular degree of an elliptic curve.* Experiment. Math. **11** (2002), no. 4, 487–502 (2003).

[38] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[39] S. T. Yau, *An application of eigenvalue estimate to algebraic curves defined by congruence subgroups.* Math. Res. Lett. **3** (1996), no. 2, 167–172.