Mathematics Faculty Scholarship

Mathematics

8-10-2004

Explicit Lower Bounds on the Modular Degree of an Elliptic Curve

Mark Watkins

Pennsylvania State University

EXPLICIT LOWER BOUNDS ON THE MODULAR DEGREE OF AN ELLIPTIC CURVE

MARK WATKINS

ABSTRACT. We derive an explicit zero-free region for symmetric square L-functions of elliptic curves, and use this to derive an explicit lower bound for the modular degree of rational elliptic curves. The techniques are similar to those used in the classical derivation of zero-free regions for Dirichlet L-functions, but here, due to the work of Goldfield-Hoffstein-Lieman, we know that there are no Siegel zeros, which leads to a strengthened result.

1. INTRODUCTION

Let E be a rational elliptic curve of conductor N; by the work of Wiles [24] and others, 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 to indicate sundry lower bounds on the modular degree of an elliptic curve. Our starting point is a formula of convolution type essentially due to Shimura [21] which states that we have

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

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 [8] or [22, 1.6]), and the $U_p(1)$ are fudge factors that can be given explicitly. From the above we have that

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

One of our goals is to show a bound of the type $\deg\phi \gg N^{7/6-\epsilon}$ as $N \to \infty$. Indeed, this has been known in folklore (see for instance the paper by Papikian [18] that deals with a functional field analogue) since the time of the Goldfeld-Hoffstein-Lieman [10] appendix to the work of Hoffstein-Lockhart [11], but herein we give a more complete proof and compute explicit constants. We shall assume that $N \geq 20000$, (and thus we have that the symmetric-square conductor $N^{(2)} \geq 142$), as else the tables of Cremona [6] can be used.

Previously, explicit bounds had been obtained in a couple of ways. As N. Elkies pointed out to us, one can use an idea of Ogg [17] to show that $d = \deg\phi \gg N/p$ where p is any prime of good reduction. Here is the argument. Reduce the modular parametrisation map mod p, and consider it over the field k of p^2 elements. Now $X_0(N)$ has about $pN/12$ supersingular points, all defined over k; whereas the elliptic curve has at most $(p+1)^2$ k-rational points. Since each of these has at most d

preimages, and these preimages must include all the k-rational points, the estimate $d \gg N/p$ follows, with a constant of $1/12$ as $N \to \infty$.

One can make a "characteristic zero" version of this argument by using lower bounds for the eigenvalues of the Laplacian on $X_0(N)$ in place of the supersingular points. This allows one to obtain a linear lower bound on the modular degree. Already in a paper of Li and Yau [14] there appears the technique for passing from an eigenvalue bound to a modular degree bound, and this is then made explicit by Abramovich [1] whose result is equivalent to $\deg \phi \geq 7N/1600$ which would improve to $\deg \phi \geq N/192$, upon assuming the Selberg eigenvalue conjecture. We shall see that these linear bounds are superior to ours unless N is quite large, as the constant in our bound will turn out to be rather small.

2. BOUNDING THE AREA OF THE FUNDAMENTAL PARALLELOGRAM

Let E be an elliptic curve, which we write in the form $y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$ 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. There are two natural cases depending on whether the discriminant is positive or negative. In either case we have that Ω is the real period multiplied by the imaginary part of the imaginary period. We have the following lower bound on $1/\Omega$.

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 Chapter 7 of Cohen [4]) 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 that we also have $\sqrt{\Delta/16} = (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. Let $t = \frac{e_1 - e_2}{e_1 - e_3}$ so that we have $t \in (0, 1)$ 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

$$1/\Omega = \frac{1}{\pi^2}(e_1 - e_3) \cdot \mathrm{agm}\left(1, \sqrt{t}\right) \cdot \mathrm{agm}\left(1, \sqrt{1-t}\right)$$

$$\geq \frac{1}{\pi^2}(e_1 - e_3) \cdot [4t(1-t)]^{1/3} \cdot \mathrm{agm}\left(1, 1/\sqrt{2}\right)^2 = \frac{D^{1/6}}{\pi^2} \cdot \mathrm{agm}\left(1, 1/\sqrt{2}\right)^2,$$

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

$$1/\Omega = \frac{1}{2\pi^2} \cdot 2\sqrt{B} \cdot \mathrm{agm}\left(1, \sqrt{\frac{2B+A}{4B}}\right) \cdot 2\sqrt{B} \cdot \mathrm{agm}\left(1, \sqrt{\frac{2B-A}{4B}}\right)$$

$$= \frac{1}{2\pi^2} \cdot 4Z\sqrt{1 + 9c^2/4} \cdot M\left(\sqrt{\frac{1}{2} + \frac{3c}{\sqrt{16 + 36c^2}}}\right) \cdot M\left(\sqrt{\frac{1}{2} - \frac{3c}{\sqrt{16 + 36c^2}}}\right)$$

$$= \frac{D^{1/6}}{\pi^2} \cdot (1 + 9c^2/4)^{1/6} \cdot M\left(\sqrt{\frac{1}{2} + \frac{3c}{\sqrt{16 + 36c^2}}}\right) \cdot M\left(\sqrt{\frac{1}{2} - \frac{3c}{\sqrt{16 + 36c^2}}}\right)$$

$$\geq \frac{D^{1/6}}{\pi^2} \cdot 4^{1/6} \cdot \mathrm{agm}\left(1, \sqrt{\frac{1}{2} + \frac{\sqrt{3}}{4}}\right) \cdot \mathrm{agm}\left(1, \sqrt{\frac{1}{2} - \frac{\sqrt{3}}{4}}\right),$$

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

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

We next turn to making the argument of [10] explicit. We first need to 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 $L(\mathrm{Sym}^2 f_E, s)$ be the symmetric-square L-function of f_E, where f_E is the form associated to a rational elliptic curve E that does not have complex multiplication. Then $L(\mathrm{Sym}^2 f_E, s)$ has no real zeros with $s \geq 1 - \delta/\log(N^{(2)}/C)$, where $\delta = 2(5 - 2\sqrt{6})/5 \approx 0.040408$, $C = 96$, and $N^{(2)} \geq 142$ is the symmetric-square conductor of E.*

Proof. We follow the proof in the appendix [10] of [11], which uses the idea that a function with a double pole at $s = 1$ cannot have a triple zero too close to this pole. The product L-function in question (see page 180) is $\mathbf{L}(s) = \zeta(s) \cdot L(F, s)^3 \cdot L(\mathrm{Sym}^2 F, s) = \zeta(s)^2 \cdot L(\mathrm{Sym}^2 f_E, s)^3 \cdot L(\mathrm{Sym}^4 f_E, s)$ 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 [11] that the Langlands correspondence implies the nonpositivity at bad primes. For our case of elliptic curves, the proper Euler factor at bad primes is worked out in the Sheffield dissertation of Phil Martin [15], and it can be verified directly that we do indeed have the desired nonpositivity. Note that Dąbrowski [7] 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; similarly the method in an appendix of a previous version of this paper failed to consider the cases of noncyclic inertia group correctly.

We also need to compute the factor at infinity and the conductor of $\mathbf{L}(s)$. For the factor at infinity, this is done on pages 60–61 of [7]: we have a factor of $\Gamma(s/2)/\pi^{s/2}$ for $\zeta(s)$, a factor of $\Gamma(s+1)\Gamma((s+1)/2)/(4\pi^3)^{s/2}$ 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 [15]; we should note that we can bound the symmetric-square conductor by the square of the conductor, that is, $N^{(2)} \leq N^2$, and similarly the symmetric-fourth-power conductor is bounded by the square of the symmetric-square conductor, that is, $N^{(4)} \leq (N^{(2)})^2$. This also follows from [3]. Note the symmetric-square conductor is actually a square, and so some authors (for instance [23]) define it to be the square root of our choice here.

So we claim that

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

is meromorphic and symmetric under the map $s \to 1 - s$. The asserted analytic properties follow from work of Gelbart and Jacquet [9] and Shimura [20] for the symmetric square, and later authors such as Kim and Shahidi for higher symmetric powers [13]. By Bump and Ginzburg [2], 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 [12]).

So the function $\Lambda(s) = s^2(1-s)^2 \Phi(s)$ is entire, and by taking the logarithmic derivative of its Hadamard product, we get that $\sum_\rho \frac{w_\rho}{s-\rho} = \frac{2}{s-1} + \frac{2}{s} + \frac{\Phi'}{\Phi}(s)$, where w_ρ is an appropriate weight for the zero and the order of summation is taken over conjugate pairs of zeros of $\Phi(s)$, and so is convergent. Now assume that $L(\mathrm{Sym}^2 f_E, s)$ has a zero at β. Then $\Phi(s)$ has a triple zero at β, so that we have

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

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

Now assume that $L(\mathrm{Sym}^2 f_E, s)$ has a zero at $\beta \geq 1 - 2(5 - 2\sqrt{6})/5 \log(N^{(2)}/C)$. 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 $\eta = \frac{1}{10\delta}\big[(2-5\delta) - \sqrt{25\delta^2 - 100\delta + 4}\big]$ 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 $0 < \delta \leq 2(5 - 2\sqrt{6})/5$. We get a crude lower bound of zero for the ρ-sum by pairing conjugate roots, and so

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

From this we get that

$$\frac{3}{\eta+1}\frac{\log(N^{(2)}/C)}{\delta} \leq$$

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

$$+ 3\frac{\Gamma'}{\Gamma}(\sigma/2) + 4\frac{\Gamma'}{\Gamma}(\sigma+1) + 3\frac{\Gamma'}{\Gamma}((\sigma+1)/2) + \frac{\Gamma'}{\Gamma}(\sigma+2) + \frac{5}{2}\log C,$$

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

$$0 \leq \frac{2}{\sigma} - \frac{3}{\sigma-(1-\beta)} - \log 32\pi^8 +$$

$$+ 3\frac{\Gamma'}{\Gamma}(\sigma/2) + 4\frac{\Gamma'}{\Gamma}(\sigma+1) + 3\frac{\Gamma'}{\Gamma}((\sigma+1)/2) + \frac{\Gamma'}{\Gamma}(\sigma+2) + \frac{5}{2}\log C,$$

Now $\eta\delta$ is maximised at the endpoint where $\delta = (5 - 2\sqrt{6})/5$, 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

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

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. $\square$

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 without complex multiplication.

Lemma 3.3. *Let E be a rational elliptic curve 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 $\delta = 2^{1/2} + 2 - 2^{7/4} \approx 0.050628$, $C = 64$, and $N^{(2)} \geq 142$ is the symmetric-square conductor of E.*

Proof. When E has complex multiplication by an order of K, the representation associated to f_E is dihedral, and so by [12] 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 by [10], 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 of 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 [16] 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: 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 [15], 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 [5] could be used if we did not need to be explicit. Note that at bad primes we still have the desired nonpositivity since $2 \geq \cos 2\theta$ for all θ.

So we are led to consider the nonpositive sum

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

Assume there is a zero of $L(\psi^2, K, s)$ at β. By the functional equation we get

$$\frac{2\sqrt{2}}{s-\beta} + \frac{2\sqrt{2}}{s-(1-\beta)} + \sum_\rho \frac{w_\rho}{s-\rho} =$$

$$\frac{2}{s-1} + \frac{2}{s} + 2\log(1/\sqrt{\pi}) + 2\sqrt{2}\log(\sqrt{N^{(2)}}/4\pi) + \log(2/2\pi) +$$

$$+ 2\frac{\Gamma'}{\Gamma}(s/2) + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(s+1) + \frac{\Gamma'}{\Gamma}(s+2) + \frac{\mathbf{L}'}{\mathbf{L}}(s),$$

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

Now we assume that the function $L(\mathrm{Sym}^2 f_E, s) = L(\theta_K, s)L(\psi^2, K, s)$ has a zero at $\beta \geq 1 - (2^{1/2} + 2 - 2^{7/4})/\log(N^{(2)}/C)$. 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

$$\frac{2\sqrt{2}}{\sigma - \beta} \le \frac{2}{\sigma - 1} + \frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma - (1 - \beta)} + \log(1/\pi) + \sqrt{2}\log N^{(2)} +$$

$$+ 2\sqrt{2}\log(1/4\pi) + \log(1/\pi) + +2\frac{\Gamma'}{\Gamma}(\sigma/2) + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(\sigma + 1) + \frac{\Gamma'}{\Gamma}(\sigma + 2).$$

From this we get that

$$\frac{2\sqrt{2}}{\eta + 1}\frac{\log(N^{(2)}/C)}{\delta} \le \frac{2\log(N^{(2)}/C)}{\eta\delta} + \frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma - (1 - \beta)} + \sqrt{2}\log(N^{(2)}/C) +$$

$$+ 2\log(1/\pi) + 2\sqrt{2}\log(1/4\pi) + +2\frac{\Gamma'}{\Gamma}(\sigma/2) +$$

$$+ 2\sqrt{2}\frac{\Gamma'}{\Gamma}(\sigma + 1) + \frac{\Gamma'}{\Gamma}(\sigma + 2) + \sqrt{2}\log C$$

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

$$0 \le \frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma - (1 - \beta)} + 2\log(1/\pi) + 2\sqrt{2}\log(1/4\pi) +$$

$$+ 2\frac{\Gamma'}{\Gamma}(\sigma/2) + 2\sqrt{2}\frac{\Gamma'}{\Gamma}(\sigma + 1) + \frac{\Gamma'}{\Gamma}(\sigma + 2) + \sqrt{2}\log C.$$

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

$$\frac{2}{\sigma} - \frac{2\sqrt{2}}{\sigma - 1 + \beta} = \frac{2}{1 + \eta\delta/\log(N^{(2)}/C)} - \frac{2\sqrt{2}}{1 + \delta(\eta - 1)/\log(N^{(2)}/C)}$$

$$\le \frac{2}{1 + \sqrt{2}(2^{1/4} - 1)/\log(N^{(2)}/C)} - \frac{2\sqrt{2}}{1 + (3 \cdot 2^{3/4} - 2\sqrt{2} - 2)/\log(N^{(2)}/C)}$$

$$\le -0.612,$$

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

Case II: 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

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

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

are all invariant under $s \to 1 - s$. Using [15], 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 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 β for our purposes is twice the positive root of the

polynomial $x^5 - 25x^4 - 4x^3 + 30x^2 + 19x + 3$, 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 are led to 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 β. By the functional equation we get

$$\frac{171}{s - \beta} + \frac{171}{s - (1 - \beta)} + \sum_\rho \frac{w_\rho}{s - \rho} =$$

$$\frac{106}{s - 1} + \frac{106}{s} + 106\log(1/\sqrt{\pi}) + \frac{171}{2}\log(N^{(2)}/12\pi^2) +$$

$$+ 45\log(N^{(4)}/N^{(2)}) + 45\log(3/4\pi^2) + \frac{25}{2}\log(N^{(6)}/N^{(4)}) + \frac{25}{2}\log(1/12\pi^2) +$$

$$+ 106\frac{\Gamma'}{\Gamma}(s/2) + 171\frac{\Gamma'}{\Gamma}(s + 1) + 90\frac{\Gamma'}{\Gamma}(s + 2) + 25\frac{\Gamma'}{\Gamma}(s + 3) + \frac{L'}{L}(s).$$

Now assume that $\beta \geq 1 - (554 - 12\sqrt{2014})/261\log(N^{(2)}/C)$. 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

$$\frac{171}{\sigma - \beta} \leq \frac{106}{\sigma - 1} + \frac{106}{\sigma} - \frac{171}{\sigma - (1 - \beta)} + \frac{261}{2}\log N^{(2)} +$$

$$+ 53\log(1/\pi) - 171\log\sqrt{12} + 171\log(1/\pi) +$$

$$+ 45\log 3/4 + 90\log(1/\pi) - 25\log\sqrt{12} + 25\log(1/\pi) +$$

$$+ 106\frac{\Gamma'}{\Gamma}(s/2) + 171\frac{\Gamma'}{\Gamma}(s + 1) + 90\frac{\Gamma'}{\Gamma}(s + 2) + 25\frac{\Gamma'}{\Gamma}(s + 3)$$

From this and the definition of η we get

$$0 \leq \frac{106}{\sigma} - \frac{171}{\sigma - (1 - \beta)} + 339\log(1/\pi) - \log(3^{53}2^{286}) + \frac{261}{2}\log C$$

$$+ 106\frac{\Gamma'}{\Gamma}(s/2) + 171\frac{\Gamma'}{\Gamma}(s + 1) + 90\frac{\Gamma'}{\Gamma}(s + 2) + 25\frac{\Gamma'}{\Gamma}(s + 3)$$

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 $0 \leq -59 - 644 + 543 + 153$. $\square$

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 $L(\mathrm{Sym}^2 f_E, 1) \geq \frac{0.033}{\log N^{(2)}}$.*

Proof. We use Rademacher's formulation [19] of the Phragmén–Lindelöf Theorem to bound $L(\mathrm{Sym}^2 f_E, s)$ and $\zeta(s)$. First note that by the Euler product we have $|L(\mathrm{Sym}^2 f_E, 3/2 + it)| \le \zeta(3/2)^3$, and so by the functional equation we get

$$|L(\mathrm{Sym}^2 f_E, -1/2 + it)| =$$

$$= (N^{(2)}/4\pi^3) \frac{|\Gamma(5/2 + it)| \cdot |\Gamma(5/4 + it/2)|}{|\Gamma(1/2 + it)| \cdot |\Gamma(1/4 + it/2)|} |L(\mathrm{Sym}^2 f_E, 3/2 + it)|$$

$$\le \zeta(3/2)^3 \frac{N^{(2)}}{4\pi^3} \cdot \left|\frac{3}{2} + it\right| \cdot \left|\frac{1}{2} + it\right| \cdot \left|\frac{1}{4} + \frac{it}{2}\right| \le \zeta(3/2)^3 \frac{N^{(2)}}{8\pi^3} \cdot \left|\frac{3}{2} + it\right|^3.$$

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

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

which is not anywhere near an optimal bound, but will suffice. Similarly we get that $|\zeta(1/2 + it)| \le \frac{\zeta(3/2)}{\sqrt{2\pi}} \sqrt{\frac{9}{4} + t^2}$.

Let $b = 1 - \frac{1}{25 \log N^{(2)}}$ so that $\mathbf{L}(s) = L(\mathrm{Sym}^2 f_E, s)\zeta(s)$ has no zeros in $[b, 1)$, so that $\mathbf{L}(b) < 0$. Note also that $b \ge 0.99$ due to our assumption that $N^{(2)} \ge 142$. Writing $\mathbf{L}(s) = \sum_n a_n/n^s$ as a Dirichlet series with nonnegative coefficients, by the Mellin transform we have that

$$\sum_n \frac{a_n}{n^b} e^{-n/X} = \int_{(2)} \Gamma(s) X^s \mathbf{L}(s + b) \frac{ds}{2\pi i}.$$

Via moving the contour to where the real part of s is $1/2 - b$, we get that the integral is $R X^{1-b} \Gamma(1 - b) + \mathbf{L}(\beta) + E(X)$ where $R = L(\mathrm{Sym}^2 f_E, 1)$ and the error term $E(X)$ is bounded by $\frac{1}{\pi} \int_0^\infty |\Gamma(1/2 - b + it) X^{1/2-b} \mathbf{L}(1/2 + it)| dt$. By another theorem in Rademacher [19] we have that

$$|\Gamma(1/2 - b + it)| \le |1/2 + it|^{1-b} \cdot |\Gamma(-1/2 + it)|$$

$$\le \frac{|1 + it|^{0.01}}{|1/2 + it|} |\Gamma(1/2 + it)| = \frac{2(1 + t^2)^{1/200}}{\sqrt{1 + 4t^2}} \sqrt{\pi \mathrm{sech}\pi t}$$

We compute that

$$\frac{\zeta(3/2)^4}{4\pi^2} \int_0^\infty \left(\frac{25}{4} + t^2\right)^{3/2} \sqrt{\frac{9}{4} + t^2} \cdot \frac{2(1 + t^2)^{1/200}}{\sqrt{1 + 4t^2}} \sqrt{\pi \mathrm{sech}\pi t} \, dt < 62,$$

so that $|E(X)| \le 20\sqrt{N^{(2)}} \cdot X^{1/2-b}$. Since $\mathbf{L}(\beta) \le 0$ we ge

$$\sum_n \frac{a_n}{n^b} e^{-n/X} \le R X^{1-b} \Gamma(1 - b) + 20\sqrt{N^{(2)}}/X^{0.49}.$$

Taking $X = (4000000 N^{(2)})^{50/49}$ and noting that $a_1 = 1$ with the other terms on the left side being nonnegative, this says that $e^{-1/10^6} \le R X^{1-b} \Gamma(1 - b) + 0.01$. Since we assume $N^{(2)} \ge 142$ we have $\log X \le 4.2 \log N^{(2)}$, and so we finally get that $X^{1-b} \le \exp(4.2/25) \le 1.19$. We also have $\Gamma(1 - b) \le 25 \log N^{(2)}$, and so we conclude that $R \ge \frac{0.033}{\log N^{(2)}}$. $\qquad\square$

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. For the Manin constant we simply use the fact that $c \geq 1$. So we have that

$$\deg \phi \geq \frac{N}{\Omega} \frac{0.033}{\log N^{(2)}} \cdot \prod_{p^2 | N} U_p(1)^{-1} \geq \frac{ND^{1/6}}{2675 \log N^{(2)}} \cdot \prod_{p^2 | N} U_p(1)^{-1}.$$

To bound the effects from the $U_p(1)^{-1}$, we recall its definition. First we assume that E is a global 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 [23] 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 [23]). 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 $U_p(1)^{-1} = 1 - 1/p$ for primes that are 5 mod 12, we have that $p^3 | D$ while $p^2 \| N$. For such primes we have that $N_p(D_p)^{1/6} U_p(1)^{-1} \geq N_p^{7/6} p^{1/6} (1 - 1/p) \geq N_p^{7/6}$. Finally we need to consider $p = 2$ and $p = 3$. There is not much to be done with $U_3(1)^{-1}$ except lower-bound it as $1 - 1/3 = 2/3$, whilst for $p = 2$ in order for $U_2(s)$ to equal $(1 - 1/2^s)^{-1}$ we need that $2^8 \| N$ and thus have $2^9 \| D$. So we have that $N_2(D_2)^{1/6} U_2(1)^{-1} \geq N_2^{7/6} 2^{1/6} (1 - 1/2)$. Thus for a global minimal twist we have that

$$\deg \phi \geq \frac{N^{7/6}}{7150 \log N^{(2)}} \cdot \prod_{\substack{p^2 | N \\ p \equiv 1 \, (3)}} (1 - 1/p).$$

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

$$\sum_{\substack{p^2 | N \\ p \equiv 1 \, (3)}} \frac{1}{p} + \sum_p \frac{1/2p^2}{1 - 1/p} \leq \sum_{\substack{p \leq 1.02 \log N \\ p \equiv 1 \, (3)}} \frac{1}{p} + 0.02 \leq 0.5 \log \log(1.02 \log N) - 0.33,$$

and so we have that

$$\deg \phi \geq \frac{N^{7/6}}{7150 \log N^{(2)}} \frac{e^{0.33}}{\sqrt{0.02 + \log \log N}} \geq \frac{N^{7/6}}{\log N^{(2)}} \frac{1/5150}{\sqrt{0.02 + \log \log N}}.$$

We wish to compare what happens on each side of this inequality upon twisting our curve by an odd prime p. There are three cases, depending on the reduction type of the minimal twist F at p. If it has additive reduction, we simply have the same $U_p(s)$ as above, and the conductor stays the same, with D increasing by a factor of p^6. The modular degree goes up by p upon twisting, whilst the right side of the inequality stays the same. If F has multiplicative reduction at p, we have that $U_p(s)^{-1} = (1 - 1/p^s)$. Here the conductor goes up by p and the discriminant by p^6 upon twisting, with the modular degree gaining a factor of $(p^2 - 1)$. This is bigger than the factor of $p^{7/6}$ by which the right side increases. Finally, if F has good reduction at p we have that $U_p(2)^{-1} = (p - 1)(p + 1 - a_p)(p + 1 + a_p)/p^3$ where a_p is the trace of Frobenius for F. The conductor goes up by p^2 and the

discriminant by p^6. The modular degree goes up by $(p-1)(p+1-a_p)(p+1+a_p)$, which is bigger than the factor of $p^{7/3}$ gained by the right side, even when $p = 3$ and $a_p = \pm 3$. So the above inequality is true for curves that are twist-minimal at 2.

Finally, we consider curves that are non-twist-minimal at 2. If $2^8|N$, the right side of our inequality stays the same upon twisting, while the left side does not diminish. When 256 does not divide the conductor, we can simply note that $U_2(1)^{-1} \geq (2-1)(2+1-2)(2+1+2)/2^3 = 5/8$ and so directly compute that

$$\deg \phi \geq \frac{ND^{1/6}}{2675 \log N^{(2)}} \cdot \frac{5}{8} \frac{2}{3} \cdot \frac{e^{0.33}}{\sqrt{0.02 + \log \log N}} \geq \frac{N^{7/6}}{\log N^{(2)}} \frac{1/5000}{\sqrt{0.02 + \log \log N}}.$$

5. SUMMARY OF RESULTS

We conclude this paper by giving a summary of the various lower bounds that can be obtained.

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

$$\deg \phi_E \geq \frac{N}{\Omega} \frac{0.033}{2 \log N} \geq \frac{N^{7/6}}{5350 \log N}.$$

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

$$\deg \phi_E \geq \frac{N}{\Omega} \frac{0.033}{\log N^{(2)}} \cdot \prod_{p^2|N} U_p(1)^{-1} \geq \frac{N^{7/6}}{7150 \log N^{(2)}} \cdot \prod_{\substack{p^2|N \\ p \equiv 1 \, (3)}} (1 - 1/p)$$

$$\geq \frac{N^{7/6}}{\log N} \cdot \frac{1/10300}{\sqrt{0.02 + \log \log N}}$$

Remark 5.3. Note that we need $N \geq e^{86.8}$ in order to derive that $\deg \phi \geq N$ from Theorem 2.

REFERENCES

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

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

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

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

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

[6] 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/`

[7] 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.

[8] 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.

[9] 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.

[10] D. Goldfeld, J. Hoffstein, D. Lieman, appendix to [11].

[11] J. Hoffstein, P. Lockhart, *Coefficients of Maass forms and the Siegel zero.* Ann. of Math. (2) 140 (1994), no. 1, 161–181.

[12] 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.

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

[14] 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.

[15] P. Martin, University of Sheffield dissertation under N. Dummigan.

[16] 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.

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

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

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

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

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

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

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

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

DEPARTMENT OF MATHEMATICS, MCALLISTER BUILDING, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA, 16802