JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Mark WATKINS

On elliptic curves and random matrix theory

Tome 20, n° 3 (2008), p. 829-845.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_3_829_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 829-845

On elliptic curves and random matrix theory

par Mark WATKINS

To Henri Cohen on the occasion of his 60th birthday

Résumé. Rubinstein a accumulé une masse de données concernant les tordues quadratiques paires d'une courbe elliptique fixée, et comparé les résultats aux prédictions venues du modèle des matrices aléatoires. Nous utilisons la méthode des points de Heegner pour obtenir des données comparables (en nombre plus faible) pour les tordues impaires. Nous constatons de nouveau qu'au moins une des principales prédictions de la théorie des matrices aléatoires est confortée par les données.

Abstract. Rubinstein has produced a substantial amount of data about the even parity quadratic twists of various elliptic curves, and compared the results to predictions from random matrix theory. We use the method of Heegner points to obtain a comparable (yet smaller) amount of data for the case of odd parity. We again see that at least one of the principal predictions of random matrix theory is well-evidenced by the data.

1. Introduction and motivation

Let E be an elliptic curve $E : y^2 = f(x)$ with f a cubic rational polynomial. How many twists $E_d : dy^2 = f(x)$ have higher (analytic) rank than is forced by the sign of the functional equation? It is an early conjecture of Goldfeld [19] that the average rank in a quadratic twist family is 1/2, with rank 0 and rank 1 each asymptotically occurring 50% of the time. In particular, introducing the counting functions

$$C_e(D) = \{|d| \le D,\ d \text{ squarefree, parity of } E_d \text{ even, and } L(E_d,1) = 0\} \text{ and}$$
$$C_o(D) = \{|d| \le D,\ d \text{ squarefree, parity of } E_d \text{ odd, and } L'(E_d,1) = 0\},$$

Goldfeld's conjecture says that both $C_e(D)$ and $C_o(D)$ are $o(D)$ as $D \to \infty$.

1.1. The case of even parity. A folklore conjecture of Sarnak, derived from the Ramanujan-Petersson conjecture [34] for weight 3/2 forms in concert with Waldspurger's theorem [43], says that

Conjecture 1.1.1. *We have* $\log C_e(D) \sim \frac{3}{4} \log D$ *as* $D \to \infty$.

Manuscrit reçu le 16 janvier 2008.

Via the use of random matrix theory, this is refined in [7, Conjecture 1]. We briefly describe the method. We first get asymptotics for the moments of $L(E_d,1)$ from analogies with random matrices, and Mellin inversion is then applied to get a distribution function for $L(E_d,1)$. Namely, we expect there to be a constant $\alpha(E)$ depending upon the arithmetic of the curve E such that

$$\lim_{t\to 0}\lim_{D\to\infty}\frac{\#\{|d|\le D,\ E_d\text{ even}, L(E_d,1)<t\}}{\#\{|d|\le D,\ E_d\text{ even}\}\cdot t^{1/2}(\log D)^{3/8}}=\alpha(E), \tag{1}$$

where the exponent of 3/8 here is $\binom{-1/2}{2}$ and is derived from the symmetry type of the random matrices (orthogonal in this case). A discretisation process involving the conjecture of Birch and Swinnerton-Dyer [2] is then used to assert that sufficiently small values of $L(E_d,1)$ must in fact correspond to $L(E_d,1)=0$ — the idea here is that the quotient

$$S(d)=\frac{L(E_d,1)}{\Omega_{\mathrm{re}}(E_d)}\frac{\#\mathrm{Tors}(E_d)^2}{\prod_p c_p(d)} \tag{2}$$

is a nonnegative integer, and thus we must have $S(d)\ge 1$ when $S(d)\ne 0$. By re-arranging, this is the same as saying that

$$L(E_d,1)<\frac{\Omega_{\mathrm{re}}(E_d)\cdot\prod_p c_p(d)}{\#\mathrm{Tors}(E_d)^2}\quad\text{implies}\quad L(E_d,1)=0.$$

Ignoring fine details and taking $d>0$ for simplicity, we essentially have $\Omega_{\mathrm{re}}(E_d)=\Omega_{\mathrm{re}}(E)/\sqrt{d}$ and $\#\mathrm{Tors}(E_d)=\#\mathrm{Tors}(E)$, while the variation of the Tamagawa product $\prod_p c_p(d)$ behaves somewhat like a divisor function; in particular, it is sensitive to the number of prime divisors of d.

1.1.2. ***Asymptotic predictions.*** In the specific case where we restrict $|d|$ to be prime, we obtain Conjecture 1 of [7], which says that $c_E D^{3/4}(\log D)^{3/8-1}$ of such twists should have a vanishing central L-value. Here the exponent on the logarithm is decreased by 1 from that in (1) due to the Prime Number Theorem [21, 42], while the primary exponent of $\frac{3}{4}$ comes from considering $t=\frac{\Omega_{\mathrm{re}(E)}}{\sqrt{|d|}}\cdot\frac{\prod_p c_p}{\#\mathrm{Tors}(E)^2}$ in (1) and summing over d. However, in this restricted case of twists by primes, it is possible that $c_E=0$, as noted in [12, Corollary 2]. The analysis given in [8, §6] of the data [37] of Rubinstein provides evidence for this asymptotic. Without the primality restriction the heuristic analysis is trickier, but the work of [15] computes a suitable average for the Tamagawa product. This leads to the prediction

$$C_e(D)\sim c'_E D^{3/4}(\log D)^{b_E} \tag{3}$$

where $c'_E\ne 0$, while b_E is related to the Galois group of the defining cubic polynomial $f(x)$ and takes on four possible values. We discuss the concordance of this with the data of Rubinstein [37] in Section 3.1.2 below.

1.1.3. ***A conjecture about ratios.*** As noted already in [7], we can eliminate some of unknowns in (3) by restricting d to various congruence classes. The effect of such a restriction should only be to modify the constant factor (and by a computable amount), so that we can eliminate the exponents by considering different congruence classes and taking a ratio. Phrased slightly differently, when restricting to d in arithmetic progressions modulo a prime q, the moments (and thus value distributions) differ by a factor depending on the trace of Frobenius a_q, and from this we obtain Conjecture 2 of [7]. In particular, we have

Conjecture 1.1.4. [7, Conjecture 2]. *For a prime $q \geq 5$ of good reduction we have (twisting by d that are squarefree)*

$$\lim_{D\to\infty} \frac{\#\{|d| \leq D : E_d \text{ even}, L(E_d,1)=0, \left(\frac{d}{q}\right)=+1\}}{\#\{|d| \leq D : E_d \text{ even}, L(E_d,1)=0, \left(\frac{d}{q}\right)=-1\}} = \left(\frac{q+1+a_q}{q+1-a_q}\right)^{-1/2}.$$

Here the $-1/2$ exponent is the same as in the above value distribution (1). In Section 3.1.1 below, we analyse the data of Rubinstein concerning this.

1.2. Odd parity. We investigate the analogues of the above conjectures when considering twists of odd parity. In particular, the behaviour for the L'-value distribution in the analogy of (1) is now expected [41, Eq. 2.9ff] to be like $t^{3/2}$ rather than $t^{1/2}$, and so we get

Suspicion 1.2.1. *For a prime $q \geq 5$ of good reduction we have*

$$\lim_{D\to\infty} \frac{\#\{|d| \leq D : E_d \text{ odd}, L'(E_d,1)=0, \left(\frac{d}{q}\right)=+1\}}{\#\{|d| \leq D : E_d \text{ odd}, L'(E_d,1)=0, \left(\frac{d}{q}\right)=-1\}} = \left(\frac{q+1+a_q}{q+1-a_q}\right)^{-3/2}.$$

An analysis of our data in Section 3.2 will show close conformity with this prediction. On the other hand, we are unable to say too much about the analogue of Conjecture 1.1.1, and indeed, there is no real agreement about what such an analogue should actually predict (see [10, §§2,3]). In Section 3.2.1, we do however present some evidence that the constant 3/4 might be too large for odd parity, suggesting that there are many fewer rank 3 quadratic twists when compared to the number that have rank 2.

1.3. Overview of data. We give a brief overview of our data, comparing it to that of Rubinstein [37] for the case of even parity twists. We fix an elliptic curve E of rank 0 and conductor N. For each suitable d, we use the method of Heegner points to determine (with high confidence) whether $L'(E_d,1)=0$. We require that $-d<0$ is fundamental and that $-d$ is a square modulo $4N$, with an additional technical condition when $\gcd(d,N)\neq 1$. For each d our computations take time essentially proportional to the size of the class group of $\mathbf{Q}(\sqrt{-d})$, and thus about $\sqrt{d}$ on average. Our data set consists of 76 curves E with $N \leq 100$ and all $d \leq 10^8$ satisfying the above constraints. We obtain a total of 638147 twists of rank 3 or more. Comparatively, the relevant data of Rubinstein contain 2379 rank 0 elliptic curves for which the vanishing of $L(E_d, 1)$ was considered for $d \leq 10^8$, with a condition concerning d modulo $4N$ similar to that of our case. This data set contains a total of 283172426 twists of rank 2 or more.

1.3.1. ***Comparison of complexity.*** Although the data of Rubinstein contain more curves by a factor of 30, for each curve we consider about the same number of twists. In fact, both algorithms have the same asymptotic complexity, taking time $D^{3/2}$ to consider all twists up to D. We briefly describe the method used to compute the data in [37]. Given $E/\mathbf{Q}$, there is an associated modular form (a Shintani lift [39]) of weight 3/2 whose coefficients yield the $S(d)$ of (2) via the Waldspurger correspondence. These lifts were computed by Tornaría using Brandt matrices, and written as a linear combination of Θ-series of ternary quadratic forms. Rubinstein then computed the first D coefficients via enumerating lattice points in ellipisoids. Without the use of convolution (which we discuss in Section 2.5), this takes time $D^{3/2}$, though the implicit constant factor here is quite small. In constrast, although we obtain the same $D^{3/2}$ complexity, our implicit constant is dominated by reducing binary quadratic forms, and is somewhat larger.

1.4. Related work. The work of Elkies [16] considers odd parity twists up to 10^7 for the congruent number curve, and some data about the odd parity twists up to 10^6 for the first four elliptic curves appears in [10, §4].[1] Other related papers include work of Delaunay and Duquesne [13] which takes a family of curves with odd parity and considers when the rank is more than 1, and the works of Delaunay [11] with Roblot [14] which consider the distribution of the height of the generator for rank 1 quadratic twists.

2. Computational method and experiment

2.1. Heegner points. We review the method of Heegner points; a partial description is given in [45], so we accent the nuances in our case of quadratic twists. Let $E/\mathbf{Q}$ be an elliptic curve of conductor N with $L(E, 1) \neq 0$. Let $-d$ be a negative fundamental discriminant that is square modulo $4N$ with the additional requirement that for all $p | \gcd(d, N)$ the local root number $\epsilon_p(E_{-d})$ is equal to $+1$. Such restrictions on d are our Heegner hypothesis for E, and we denote the set of d that satisfy this by $\mathcal{H}_o(E)$. Below we will construct a canonically-defined point T_d that is on $E_{-d}/\mathbf{Q}$. Denoting the height function by $\hat{h}$, it is a conjecture of Gross and Hayashi [22] that

[1] The aim in this latter paper was to consider the distribution of $L'(E_d, 1)$ — our goal here is less broad in scope, as we only care if this value is nonzero. It should also be noted that some L'-values in [10, §4] were wrongly thought to be nonzero due to an improper stopping criterion.

Conjecture 2.1.1. *For $d \in \mathcal{H}_o(E)$ as above, we have*

$$\hat{h}(T_d) = \frac{\sqrt{d}}{4\Omega_{\text{vol}}} L(E,1)L'(E_{-d},1) \times 2^{\omega(\gcd(d,N))}\left(\frac{w(-d)}{2}\right)^2. \tag{4}$$

Here $\omega(n)$ is the number of distinct prime factors of n, while $w(-d)$ is the number of units in $\mathbf{Q}(\sqrt{-d})$. The Gross-Zagier theorem [20] applies in the case where $-d \neq -3$ is odd with $\gcd(d,N) = 1$. Recent work of Conrad [6] has reinterpreted much of the proof of [20], but it is still unclear whether the above Conjecture can be proven simply by an increase in care to detail. In our case where $L(E,1) \neq 0$, equation (4) tells us that $L'(E_d,1)$ vanishes precisely when $\hat{h}(T_d) = 0$, that is, when T_d is a torsion point.

2.1.2. ***Heights of Heegner points.*** There is some theoretical work regarding the heights of Heegner points in a family of quadratic twists. In particular, in the case that E has rank 0, Ricotta and Vidick show [35, Corollaire 3.2] that the average height of T_d is of size $c\sqrt{d}\log d$, with the leading constant c being given explicitly in terms of a special value of the symmetric square L-function of E. However, our computational method is somewhat useless in this regard, as we do not compute the height of T_d. Rather, we approximate T_d on the complex torus representation of E, and measure how close it is to the nearest (rational) torsion point. This metric is much more convenient in our computations (we only care if T_d is torsion), but its lack of arithmetic content renders it impotent for questions about heights.

2.1.3. ***Twisted traces.*** Before describing how to compute T_d, as an aside we mention that using twisted traces could diminish the stringency of the requirement that $-d$ be square modulo $4N$, with again a conjectural Gross-Zagier extension relating $\hat{h}(T_d)$ to $L'(E_d,1)$. This was indicated to us[2] by H. Darmon and G. Tornaría, and a similar idea can be used in the case of even parity [27]. The idea is that the Hilbert class field of $\mathbf{Q}(\sqrt{-dl})$ contains that of $\mathbf{Q}(\sqrt{-d})$, and if we construct a point in the former, then tracing by the genus character χ_l gives a point in $\mathbf{Q}(\sqrt{-d})$. An explicit example is to take 76A: $y^2 = x^3 - x^2 - 21x - 31$ where $-d = -3$ is not a square modulo $304 = 4 \cdot 76$, but $-dl = -15$ is (where $l = 5$). Anticipating the notation of below, the forms $\tilde{f} = (76, 17, 1)$ and $\tilde{g} = (152, 169, 47)$ generate the class group of $\mathbf{Q}(\sqrt{-15})$, and adding $\phi(\tau_{\tilde{f}}) + \phi(\tau_{\tilde{g}})$ gives the point $(-\frac{8}{5}, \frac{13}{25}\sqrt{-15})$ in $\mathbf{Q}(\sqrt{-15})$. If we twist by the genus character χ_5, we get that $\chi_5(76)\phi(\tau_{\tilde{f}}) + \chi_5(152)\phi(\tau_{\tilde{g}})$ yields the point $(-4, 3\sqrt{-3})$ in $\mathbf{Q}(\sqrt{-3})$.

[2] B. J. Birch informs us that his early experiments [1] with N. M. Stephens also made use of twisted traces, as else the data set they obtained would have been quite small.

2.2. Computing the Heegner point. We now describe how to compute the above point T_d. This is canonical up to sign and possible translation by a 2-torsion point. We fix a square root β of $-d \pmod{4N}$, and define $S_\beta(-d, N)$ to be the set of positive definite binary quadratic forms (A, B, C) of discriminant $-d$ having $N|A$ and $B \equiv \beta \pmod{2N}$. Our goal is to take each form g in the class group of $\mathbf{Q}(\sqrt{-d})$ and replace it by an $\mathrm{SL}_2(\mathbf{Z})$-equivalent form $\tilde{g} = (A, B, C) \in S_\beta(-d, N)$. To do this, we take the particular form $h_\beta = (N, \beta, \gamma)$ (with γ defined by the condition $\mathrm{disc}(h_\beta) = -d$), and form the composition $\hat{g} = h_\beta^{-1} \circ g$. Then, possibly after reducing $\hat{g}$, we find some (small) integer t with $\gcd(t, N) = 1$ that is represented by it, and transform $\hat{g} \to (t, b, c)$ for some b, c. Finally, we compose (t, b, c) with h_β (without reducing), which yields a form $\tilde{g} = (A, B, C) \in S_\beta(-d, N)$.

2.2.1. ***Optimising our representatives.*** However, it will be important to minimise the size of A. We can note that $S_\beta(-d, N)$ is $\Gamma_0(N)$-invariant, and so we can apply the $\Gamma_0(N)$-reduction given in [5, Subalgorithm 8.6.13]. In practise, we actually use a variant that takes into consideration the continued fraction expansion of the quantity $u = -B/(2A/N)$ so as to lessen the time spent in the "Loop on c" in Step #2. We pay the very small cost of not strictly minimising A in a few cases. If desired, we can additionally consider the effect of Atkin-Lehner transformations (using the trick of Delaunay mentioned in [45, §3.1]) to try to reduce the size of A even further: we compose $(A, B, C) \circ w_N h_{-\beta}^{-1}$, find a small t with $\gcd(t, N) = 1$ that this represents, transform to (t, b, c), and apply Subalgorithm 8.6.13 to the composition $h_{-\beta} \circ (t, b, c)$. If this yields a form with smaller leading coefficient, we use it instead (noting that w_N flips the sign of the modular parametrisation in our case). It is possible to consider the involutions w_Q in a similar manner, but we did not do this in practise, as the time spent with Subalgorithm 8.6.13 was often more than the time spent computing the modular parametrisation. Similarly, we saw no need to utilise the extra automorphisms $z \to z + 1/k$ when $k|24$ and $k^2|N$ (as used in [16]).

2.2.2. ***Applying the modular parametrisation.*** We wish to apply the modular parametrisation $\phi : X_0(N) \to E$ to each form (A, B, C) obtained above. We can identify $X_0(N)$ with the completed upper half plane modulo $\Gamma_0(N)$, and similarly E with $\mathbf{C}/\Lambda$ for a canonical lattice Λ corresponding to the minimal model.[3] For each form (A, B, C) we take the associated quadratic surd $\tau = \frac{-B+\sqrt{-d}}{2A}$ in the upper half plane, and evaluate $\phi(\tau) = \sum_n \frac{a_n}{n} e^{2\pi i n \tau}$ to a given precision. Due to the exponential decay, it is easy to determine when the tail of this series contributes no more than 10^{-16} (this is essentially our machine precision), with the smallness of A

[3] In all cases, we choose the strong Weil curve in the isogeny class of E, and it follows that we expect that the Manin constant of E is 1, this being checkable in any individual case.

ensuring that the series will converge sufficiently rapidly. Additionally, we compute the Fourier coefficients a_n only once for each E, and reuse them for various d.

Using the modularity (over $\mathbf{Q}$) of elliptic curves [46, 4], it is a theorem due to Shimura [38, §6.8] that applying the Weierstrass $\wp$-function to $\phi(\tau)$ gives a point on E defined over the Hilbert class field of $\mathbf{Q}(\sqrt{-d})$. The points corresponding to $\phi(\tau)$ also satisfy a reciprocity law with the Artin map, and by summing the $\phi(\tau)$ we obtain a trace u_d, which yields a point $U_d = \mathcal{P}(u_d)$ on E over $\mathbf{Q}(\sqrt{-d})$, where here the map $\mathcal{P}$ sends s to the point $\bigl(\wp(s), \wp'(s)\bigr)$. To descend down to $E_{-d}(\mathbf{Q})$ we take $U_d - \overline{U_d}$ which gives a point $T_d \in E_{-d}(\mathbf{Q})$ via the Galois action; alternatively, from the complex standpoint we consider $t_d = u_d - \overline{u_d} = 2i \cdot \mathrm{Im}(u_d)$. Of course, in practise we only have approximations $\dot{u}_d$ and $\dot{t}_d$.

2.3. Detecting torsion. We must now give a method for deciding if $\dot{t}_d$ corresponds to a torsion point of $E_{-d}(\mathbf{Q})$. We have canonical periods ω_{re} and ω_{im} for the lattice Λ, with ω_{re} real. When $\Delta_E < 0$ we take Λ_{im} to be the (integral) multiples of $\mathrm{Im}(\omega_{\mathrm{im}})$, while when $\Delta_E > 0$ we take Λ_{im} as the multiples of $\omega_{\mathrm{im}}/2$ — the division by 2 takes care of the possibility that T_d is a torsion point on the nonidentity component of the real locus (the so-called egg). Since t_d is imaginary, for T_d to be torsion we must[4] have that $t_d \in \Lambda_{\mathrm{im}}$, and in our experiment we declare $T_d = \mathcal{P}(t_d)$ to be torsion if the distance from $\dot{t}_d$ to Λ_{im}, denoted by $\|\dot{t}_d\|$, is sufficiently small.

2.3.1. ***A consistency check.*** We also claim that $2 \cdot \mathrm{Re}(u_d)$ must always correspond to a torsion point on $E(\mathbf{Q})$, which gives us a consistency check. To see this, we note that $\mathcal{P}(u_d)$ is defined over $\mathbf{Q}(\sqrt{-d})$, and thus we get that both $\mathcal{P}(2u_d) = \mathcal{P}(u_d) + \mathcal{P}(u_d)$ and $\mathcal{P}(t_d) = \mathcal{P}(u_d) - \mathcal{P}(\overline{u_d})$ are also defined over $\mathbf{Q}(\sqrt{-d})$. Their difference $\mathcal{P}\bigl(2 \cdot \mathrm{Re}(u_d)\bigr)$ is in both $E\bigl(\mathbf{Q}(\sqrt{-d})\bigr)$ and $E(\mathbf{R})$; since $E/\mathbf{Q}$ has rank 0, the only $\mathbf{Q}(\sqrt{-d})$-points in the real locus are torsion, verifying our claim. This torsion condition provides a useful check on our computations.

We let e be the exponent[5] of the torsion subgroup of $E(\mathbf{Q})$, and let $\Lambda_{\mathrm{re}}^{T}$ be the multiples of ω_{re}/e. Our machine precision was 53 bits, which corresponds to about 16 digits. We raised an error condition if $2 \cdot \mathrm{Re}(\dot{u}_d)$ was not within $2 \cdot 10^{-10}$ of $\Lambda_{\mathrm{re}}^{T}$. This is, in some sense, the overall precision we expect from doing each individual operation at machine precision. However, it is not a rigourous bound, and we obtained the above cutoff of $2 \cdot 10^{-10}$ by examining the observed numerical variation for the first few curves. In any event, our experiment yielded no errors from this consistency check.

[4] This is a bit imprecise, as $E/\mathbf{Q}\bigl(\sqrt{-d}\bigr)$ could have a larger torsion group than $E/\mathbf{Q}$ — however, this rarely happens, and for a given E, the finitely many d for which it might occur can be readily determined from consideration of the isogeny structure of $E/\mathbf{Q}$.

[5] This suffices, and we did not worry about making any improvements.

2.4. Our experiment. We took the 76 isogeny classes of rank 0 elliptic curves with conductor not more than 100, and considered all imaginary quadratic twists by fundamental discriminants up to 10^8 that satisfied our Heegner hypothesis.

We declared the Heegner point T_d to be torsion if $\|\dot{t}_d\| \leq 10^{-9}$. As a guide to size, for the T_d that we declared to be non-torsion, we obtained only 6 values[6] of $\|\dot{t}_d\|$ between 10^{-8} and 10^{-9}, the smallest of these being $3.31 \cdot 10^{-9}$ for 90C1 and $-d = -41817839$. Even in this extremal case, this is 10 times as large as the above "overall precision" for our computation, and so we have fair confidence that the Heegner point really is non-torsion in all cases where we have declared this to be the case.

In the other direction, for T_d that we declared to be torsion, the largest value of $\|\dot{t}_d\|$ was $3.11 \cdot 10^{-10}$ for the curve 67A1 and $-d = -88543415$. This is of the same magnitude as the "overall precision" mentioned above, and so presumably can be attributed to accumulated round-off error. The smallest non-torsion $\|\dot{t}_d\|$ for this curve was $1.00 \cdot 10^{-7}$ for $-d = -50506727$; indeed, for each of our 76 curves, the observed ratio between the smallest non-torsion $\|\dot{t}_d\|$ and largest torsion $\|\dot{t}_d\|$ was always 300-to-1 or more, which is good evidence of numerical robustness. This should persuade that our lists of d with $L'(E_{-d}, 1) = 0$ are correct.

2.4.1. ***The computer programme.*** We wrote a `C` programme to implement the above algorithm. To generate the various class groups, we looped through all $b \leq \sqrt{d/3}$ and factored $(b^2 + d)/4$ into ac using a table as in [44, §5]. This enumeration is quite fast, but the process of finding suitable representatives $(A, B, C) \in S_\beta(-d, N)$ is comparatively quite time-consuming.[7] We borrowed the code for periods, conductors, root numbers, and Fourier coefficients from the SYMPOW package of [28], while the torsion was a command-line option to the programme. The composition of forms would often yield coefficients with more than 32 bits, and so it was useful to have a 64-bit processor. A typical run took 4 days using a 2.6 GHz Opteron 852. Our memory requirements were quite modest: we stored the Fourier coefficients a_n for $n \leq 10^7$, but only a few curves needed more than 10^6; this used about 80 megabytes, while the factor table had about $10^8/6$ entries, and so was of similar size.

2.5. An alternative method. With the permission of N. D. Elkies, we now describe an alternative method which again should give high certainty regarding whether the Heegner point T_d constructed above is torsion. The idea is to compute the Heegner point modulo p for many primes p; if the

[6] I know of no independent interest for these small values — this is about the number that would be expected upon assuming that $\|t_d\|/\omega_{\text{im}}$ is randomly distributed in a suitable interval.

[7] The $\Gamma_0(N)$-reduction is somewhat analogous to continued fractions, but I was unable to find a trick that would evade real number computations.

reduction of T_d mod p is always the same as the reduction of a global torsion point, we then suspect that T_d is itself torsion. We have not implemented this method but it has some interesting features. First, in this same probabilistic manner we should be able to predict whether the Heegner point is s-divisible, which would then lead us to expect that s^2 divides the order of the Shafarevich-Tate group if Tamagawa numbers do not interfere. Furthermore, by additionally considering higher powers of primes, there could be relations with p-adic modular forms of weight 3/2 and conjectures of Jochnowitz [24]. Finally, there is the possibility of reducing the running time (of considering all d up to D) to be essentially linear using convolution; this can also presumably be done with the ternary quadratic forms in the even parity case, but it seems that it is not used in practise.

2.5.1. ***Some details.*** We take an elliptic curve $E/\mathbf{Q}$ and run over small primes p that are coprime to N. For each d up to D we want to consider many inert primes p, so "small" might be $p \leq (\log D)^2$. For each d (satisfying the Heegner hypothesis) such that p is inert, we have that the Heegner point mod p is a sum of CM points that are supersingular mod p. We then list the E-images of the supersingular points Q of $X_0(N)$; the computation of the map $X_0(N) \to E$ need be done only once per curve, and should be feasible, at least for small N. The multiplicity in the Heegner sum of these images is the number of embeddings of $\mathbf{Q}(\sqrt{-d})$ in the endomorphism ring $\mathrm{End}(Q)$, and the number of such embeddings is itself a Fourier coefficient of a Θ-function of a rank 3 lattice-translate. We can then compute these Θ-functions via various methods. To use convolution, we would write the Θ-series as a (short) linear combination of products of Θ-series from lattices of lesser dimension, with the products then computed using convolution in essentially linear time.[8] However, this would additionally require memory linear in D, and it is not clear that the constant factors would allow it to be practical in any case. Indeed, one reason that Rubinstein is able to produce significantly more data in the case of even parity is that the constant-time step of enumeration of lattice points in an ellipisoid is much faster than the computations with quadratic forms that occur in our odd parity case — as noted above, the time spent trying to apply $\Gamma_0(N)$-reduction was often time-dominant for us.

3. Data analysis

In this section, we give an analysis of the data we obtained from our experiment. We begin by first giving a similar analysis for the data of Rubinstein in the case of even parity, so as to form a basis of comparison.

[8] We mention in passing that recent improvements due to Van Buskirk [26] might give a small speed-up compared to the older split-radix methods.

3.1. Even parity. The relevant data of Rubinstein consist of 2379 rank 0 curves, and for each curve, we can test the above Conjecture 1.1.4 for a large selection of primes. We chose to consider good primes q up to 1000. For a given curve E, we write

$$S_q^{\pm}(D) = \#\{d \in \mathcal{H}_e(E) : d \leq D, L(E_{-d}, 1) = 0, \left(\tfrac{d}{q}\right) = \pm 1\},$$

where $\mathcal{H}_e(E)$ is the set of discriminants satisfying the Heegner constraints in the even parity experiment. We then have a set of about $166 \cdot 2379$ pairs, with each pair given by $\left(\frac{q+1+a_q}{q+1-a_q}, \frac{S_q^+(D)}{S_q^-(D)}\right)$, where we omit the curve from the notation. We can then take this set of nearly 400000 pairs, and use a least-squares regression (see [18, Liber II, Sectio III] and [25]) to compute the best-fit exponent. If Suspicion 1.2.1 is indeed correct, we should expect a result of -0.5 — however, we obtain -0.612.

3.1.1. ***Effect of the secondary term.*** To solve this paradox, it was noted to us by M. O. Rubinstein that, at least in our data range, a secondary term (as computed in [9]) should be included on the right side of Conjecture 1.1.4. Indeed, for large q, the main term is given by $\left(\frac{q+1+a_q}{q+1-a_q}\right)^{-1/2} \sim -\frac{1}{2}\frac{2a_q}{q}$, while the secondary term is computed to be $-\frac{3/4}{\log D}\frac{a_q(q-1)\log q}{(q+1)^2-a_q^2} \sim -\frac{3}{4}\frac{a_q}{q}\frac{\log q}{\log D}$. For $D = 10^8$ and $q \approx 10^3$ this secondary term is thus $9/32$ as large as the main term (and in the same direction). We choose to ignore further secondary terms, though it is not clear that they need be negligible.

We can exemplify the above paragraph by stratifying our data. For each of the 166 primes q with $5 \leq q \leq 1000$, we consider the 2379 curves (excluding those for which q is bad) and, as above, assume a power law and compute the best-fit exponent from the resulting 2379 data points. We should expect to get a result that is something like $-\frac{1}{2} - \frac{3}{8}\frac{\log q}{\log 10^8}$. In Figure 1 we plot the resulting 166 best-fit exponents with q on a logarithmic scale, and see that secondary terms do indeed appear to give a correction whose dominant contribution is linear in $\log q$.

3.1.2. ***Asymptotic behaviour.*** The 2379 curves of Rubinstein fall in three[9] natural b-classes for the expected asymptotic $C_e(D) \sim c_E D^{3/4}(\log D)^b$ depending on the maximal 2-torsion for a curve in the isogeny class. To be pedantic, we do not compute $C_e(D)$ due to various Heegner restrictions on d, but we expect a similar asymptotic to hold (with a different value of c_E) for our counting function, which we denote by $C_e^{\#}(D)$. Borrowing

[9] The fourth class, where the discriminant is square but there is no rational 2-torsion, can only occur when the conductor is not squarefree (see [29]). However, the data of Rubinstein only have curves of squarefree conductor — the theoretical difficulties in this regard have been overcome in recent work of Pacetti and Tornaría [32].

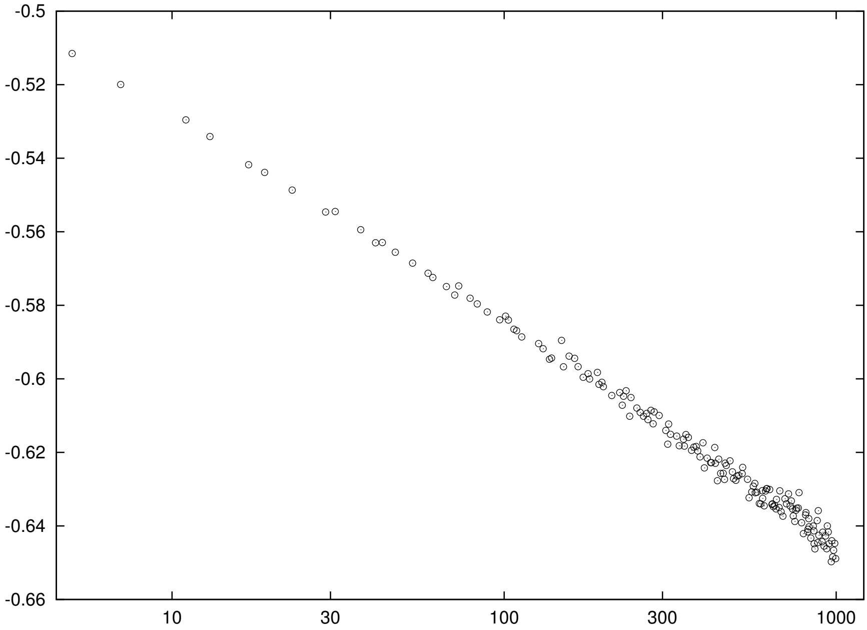

FIGURE 1. Plot of best-fit exponent for each prime $5 \le q \le 1000$.

an idea from theoretical physics as explained in [30, §4.3.1], we can "amalgamate" the data for which we expect the same value of b — the idea is that the crude behaviour of the counting functions is the same, and any obtrusive effect from the amalgamation would only be seen in the constant in front. For each of these three b-classes, we can fit the amalgamated data as $C_e^{\#}(D) \sim e^c D^a (\log D)^b$ for the parameters (a, b, c). This fitting process is exactly analogous to doing a least squares fit, except now we have three linear equations rather than two. For the amalgamation of the 1385 curves with no 2-torsion, we get a best-fit pair of $(a, b) = (0.746, 1.27)$, while for the 661 curves with a single 2-torsion point we get $(a, b) = (0.760, 1.40)$, and for the 333 cases of full 2-torsion we obtain $(a, b) = (0.768, 1.52)$. As can be seen, the prediction of $a = 3/4$ is quite commensurate with the data. However, the expected values of b, respectively 0.749, 1.082, and 1.375, are less indicated, possibly due to the fact that the expected convergence should be quite slow, as we need to consider d with many prime factors before the asymptotic behaviour becomes manifest. Furthermore, we might expect that the $e^c D^a (\log D)^b$ asymptotic is the start of a series expansion in $1/\log D$, and secondary terms might be non-negligible at $D = 10^8$.

3.2. Odd parity. We attempted to analyse our odd parity data in the same manner. For each curve, we tested Suspicion 1.2.1 by using the 143 primes q between 100 and 1000. This is the opposite stratification compared to the above, as here we fix E and vary the prime. Nonetheless, by writing

$$\tilde{S}_q^{\pm}(D) = \#\{d \in \mathcal{H}_o(E) : d \leq D, L'(E_{-d}, 1) = 0, \left(\tfrac{d}{q}\right) = \pm 1\},$$

we might still expect a power law in Suspicion 1.2.1, and the obtained best-fit exponents for each of the 76 curves (each using 143 data points) all lie between -1.41 and -1.55, signifying that -1.5 is reasonable. We can also compute the best-fit exponent upon amalgamating all $76 \cdot 143$ data points, which gives -1.47. A log-log scatter plot of these 10868 data points appears in Figure 2, and we can notice a reasonable spread of data centered about the line of slope $-3/2$. The effects from secondary terms do not appear to be too large here; the analogy of Figure 1 shows a general downward trend (from -1.4 to -1.6) as q increases, but does not resemble a straight line.

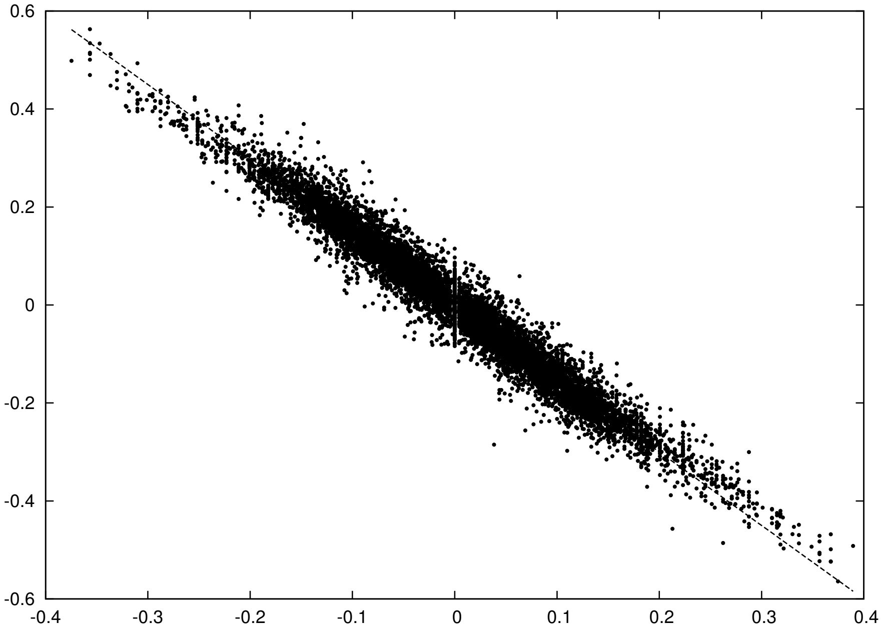

FIGURE 2. Log-log scatter plot of 10868 pairs of $\left(\frac{q+1+a_q}{q+1-a_q}, \frac{\tilde{S}_q^{+}(10^8)}{\tilde{S}_q^{-}(10^8)}\right)$.

3.2.1. ***Asymptotic behaviour.*** The situation is murkier when considering the asymptotic behaviour for the number of rank 3 quadratic twists. Again we would have three b-classes for amalgamation when considering a putative $C_o^{\#}(D) \sim e^c D^a (\log D)^b$ asymptotic, but the relative sparseness of the data seems to preclude us from making any strong conclusion in any event. For this reason, we simply amalgamated the data from all 76 curves (this is a total of 638147 data points), and via the above fitting methodology determined $(a, b) = (0.43, 5.75)$ to be the best-fit pair. In particular, the value of a is noticeably smaller when compared to the case of even parity.

Furthermore, the guess of $a = \frac{3}{4}$ in the asymptotic for $C_o^{\#}(D)$ is contraindicated by other evidence. For instance, if we simply fit $C_o^{\#}(D) \sim e^{\tilde{c}} D^{\tilde{a}}$, we should expect $\tilde{a} \geq a$ to hold and $\tilde{a}$ to decrease as D increases, both effects due to the influence of the logarithm. However, for the curves 37B and 67A, the value of $\tilde{a}$ has already dropped below $\frac{3}{4}$ at $D = 10^8$. Indeed, amalgamating all 76 curves gives a best-fit $\tilde{a}$ of 0.848 at $D = 10^7$ and 0.793 at $D = 10^8$, and $\tilde{a}$ might drop below $\frac{3}{4}$ upon extending the data to $D = 10^9$.

3.3. Extended data for the congruent number curve. The data of Elkies [16] only considered the two curves 32A and 64A. Part of this limited focus was due to the simplifications that come about in these cases, but it is also notable that these curves possess an immediate relation to the congruent number problem, and thus to Pythagorean triangles.[10] Because of this interest, we extended our data for 32A and 64A up to 10^9. For 32A, we obtained 79917 odd twists with $L'(E_d, 1) = 0$, while 64A gave 94602 such twists. Computing the best-fit pairs for $C_o^{\#}(D) \sim e^c D^a (\log D)^b$ yields respectively $(a, b) = (0.44, 5.91)$ and $(0.55, 3.58)$. The twists we considered correspond to the curves $y^2 = x^3 - d^2 x$ with $d \equiv 7 \pmod 8$ for 32A and to $d \equiv 14 \pmod{16}$ for 64A — we did not use "mock" Heegner points (described in [31]) to handle the other d, as our aim was somewhat different than that in [16]. With the help of T. A. Fisher, we were able to extend[11] the result of [16] to say that all such (odd) twists up to 10^9 have positive rank. This was done simply by finding a non-torsion point on each twist whose Heegner point was torsion. Additionally, Elkies has post-processed our data, and thus found that $d = 48272239$ gives a curve $y^2 = x^3 - d^2 x$ of rank 5, which surpasses the previous record (see [36]) for the smallest such d; changing the metric slightly, Elkies finds that $d = 51604646$ yields the smallest known conductor for a (quadratic) twist of 32A of rank 5.

4. Concluding comments

We have given data for twists of rank 3 (or more) for various elliptic curves. This supplements the data [37] of Rubinstein for rank 2. One could ask about data for rank 4, but this looks difficult. We took the 374974 positive rank twists of even parity of 11A listed by Rubinstein and used the `ellQ.gp` programme [40] of D. Simon (written in GP/PARI [33]) to compute the 2-Selmer rank of each (taking a total of about a day), and this yielded 4147 twists with 2-Selmer rank of 4. However, the use of `FourDescent` in Magma [3] found that only 554 of these have 4-Selmer

[10] In his typically eccentric style, Heegner [23] preferred to call these triangles *Harpedonapten*, which seems similar to *Seilspanner* (a cable-wrench or a rope-tensioning device), and were presumably used by the ancient Egyptians in construction work.

[11] Lists of data are currently available from `www.dpmms.cam.ac.uk/~taf1000/LIST.32A.9.pts` and `www.dpmms.cam.ac.uk/~taf1000/LIST.64A.9.pts`

rank of 4, and further computations of T. A. Fisher (using descent by 5-isogeny [17]) showed that only 444 have rank 4. Extending the data of Rubinstein to 10^{10} for a few selected curves should be feasible, and a pruning as above might then yield a sufficient amount of data regarding twists of rank 4. In particular, the analogue of Suspicion 1.2.1 should have $-5/2$ as the exponent, which could show a dramatic effect in the data.

4.1. Acknowledgements. The author was partially supported during this work by Engineering and Physical Sciences Research Council (EPSRC) grant GR/T00658/01, and thanks the Magma Computer Algebra Group at the University of Sydney for the use of their quad Opterons in carrying out the computations described here. He also thanks D. B. Zagier for comments regarding curve fitting, and K. Belabas for help with translation.

4.1.1. ***Availability of data.*** Our experimental data regarding odd parity twists with rank 3 (or more) are available for download from the website `magma.maths.usyd.edu.au/~watkins/ALL.tar` and our code is available from `magma.maths.usyd.edu.au/~watkins/HEEGcode.tar` currently.

References

[1] B. J. Birch, N. M. Stephens, *Computation of Heegner points.* In *Modular forms (Durham, 1983).* Papers from the symposium held at the University of Durham, Durham, June 30 to July 10, 1983. Edited by R. A. Rankin. Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Ellis Horwood Ltd., Chichester; Halsted Press [John Wiley & Sons, Inc.], New York (1984), 13–41.

[2] B. J. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I. II.* J. reine angew. Math. **212** (1963), 7–25, **218** (1965), 79–108. Available online from the Göttinger Digitalisierungszentrum via `resolver.sub.uni-goettingen.de/purl?GDZPPN002180022` and `resolver.sub.uni-goettingen.de/purl?GDZPPN002181169`

[3] W. Bosma, C. Playoust, J. Cannon, *The Magma algebra system. I. The user language.* In *Computational algebra and number theory.* Proceedings of the 1st MAGMA Conference held at Queen Mary and Westfield College, London, August 23–27, 1993. Edited by J. Cannon and D. Holt, Elsevier Science B.V., Amsterdam (1997), 235–265. Cross-referenced as J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Possibly available from `sciencedirect.com` through `dx.doi.org/10.1006/jsco.1996.0125`

[4] 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. Online from `ams.org` through `dx.doi.org/10.1090/S0894-0347-01-00370-8`

[5] H. Cohen, *Number Theory. (Part I: Tools, and Part II: Diophantine Equations).* Graduate Texts in Mathematics **239**, Springer, 2007.

[6] B. Conrad, *Gross–Zagier revisited.* With an appendix by W. R. Mann. In *Heegner points and Rankin L-series.* Papers from the Workshop on Special Values of Rankin L-Series held in Berkeley, CA, December 2001. Edited by H. Darmon and S.-W. Zhang. Mathematical Sciences Research Institute Publ. **49**, Cambridge University Press, Cambridge (2004), 67–163. Available online from `msri.org/communications/books/Book49/files/05conrad.pdf`

[7] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions.* In *Number theory for the millennium, I* (Urbana, IL, 2000). Papers from the conference held at the University of Illinois at Urbana–Champaign, Urbana, IL, May 21–26, 2000. Edited by M. A. Bennett, B. C. Berndt, N. Boston, H. G. Diamond, A. J. Hildebrand and W. Philipp. Published by A K Peters, Ltd., Natick, MA (2002), 301–315. Preprint at `arxiv.org/math/0012043`

[8] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *Random Matrix Theory and the Fourier Coefficients of Half-Integral Weight Forms*, Exper. Math. **15** (2006), no. 1, 67–82. For data see [37]. Preprint available online from `arxiv.org/math/0412083` and paper at `expmath.org/expmath/volumes/15/15.1/Conrey.pdf`

[9] J. B. Conrey, A. Pokharel, M. O. Rubinstein, and M. Watkins, *Secondary terms in the number of vanishings of quadratic twists of elliptic curve L-functions.* In *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341**, Cambridge University Press (2007), 215–232. Preprint at `arxiv.org/math/0509059`

[10] J. B. Conrey, M. O. Rubinstein, N. C. Snaith, M. Watkins, *Discretisation for odd quadratic twists.* In *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341**, Cambridge University Press (2007), 201–214. Preprint online at `arxiv.org/math/0509428`

[11] C. Delaunay, *Moments of the orders of Tate-Shafarevich groups.* Int. J. Number Theory **1** (2005), no. 2, 243–264. Possibly available online from `www.worldscinet.com` via `dx.doi.org/10.1142/S1793042105000133`

[12] C. Delaunay, *Note on the frequency of vanishing of L-functions of elliptic curves in a family of quadratic twists.* In *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341**, Cambridge University Press (2007), 195–200.

[13] C. Delaunay, S. Duquesne, *Numerical investigations related to the derivatives of the L-series of certain elliptic curves.* Exper. Math. **12** (2003), no. 3, 311–317. Online at `expmath.org/expmath/volumes/12/12.3/DelauneyDuquesne.pdf` (sic)

[14] C. Delaunay, X.-F. Roblot, *Regulators of rank one quadratic twists.* Preprint (2007), online at `arxiv.org/0707.0772`

[15] C. Delaunay, M. Watkins, *The powers of logarithm for quadratic twists.* In *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341**, Cambridge University Press (2007), 189–193.

[16] N. D. Elkies, *Heegner point computations.* In *Algorithmic Number Theory.* Proceedings of the First International Symposium (ANTS-I) held at Cornell University, Ithaca, New York, May 6–9, 1994, edited by L. M. Adleman and M.-D. Huang, Lecture Notes in Computer Science **877**, Springer-Verlag, Berlin (1994), 122–133.

• N. D. Elkies, *Curves $Dy^2 = x^3 - x$ of odd analytic rank.* In *Algorithmic number theory.* Proceedings of the 5th International Symposium (ANTS-V) held at the University of Sydney, Sydney, July 7–12, 2002, edited by C. Fieker and D. R. Kohel, Lecture Notes in Computer Science **2369**, Springer-Verlag, Berlin (2002), 244–251. Preprint available online from `arxiv.org/math/0208056` and possibly the paper from `springerlink.com` via `dx.doi.org/10.1007/10.1007/3-540-45455-1_20`

◇ The data are available online from `www.math.harvard.edu/~elkies/cong_r3_7b.html` and `www.math.harvard.edu/~elkies/cong_r3_6b.html`

[17] T. Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\boldsymbol{Q}$*.* J. Eur. Math. Soc. (JEMS) **3** (2001), no. 2, 169–201. Possibly available from `springerlink.com` via `dx.doi.org/10.1007/s100970100030`

[18] C. F. Gauss, *Theoria motus corporum coelestium in sectionibus conicis solem ambientium.* (Latin) [Theory of motion of celestial bodies revolving about the sun in conic sections]. Published in 1809, with priority for least squares claimed from 1795 in §186. A modern English translation is *Theory of the Motions of the Heavenly Bodies Moving about the Sun in Conic Sections*, Dover, 2004. Original available online from the the Göttinger Digitalisierungszentrum via `resolver.sub.uni-goettingen.de/purl?PPN236008730`

[19] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields.* In *Number theory, Carbondale 1979* (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), M. B. Nathanson, ed., Lecture Notes in Math. **751**, Springer-Verlag, Berlin (1979), 108–118.

[20] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), no. 2, 225–320. Available online from the Göttinger Digitalisierungszentrum (digital library) via `resolver.sub.uni-goettingen.de/purl?GDZPPN002102773` or possibly from `springerlink.com` through `dx.doi.org/10.1007/BF01388809`

[21] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques.* (French) [On the distribution of zeros of the function $\zeta(s)$ and its arithmetic consequences]. Bull. Soc. Math. France **24** (1896), 199–220. Available online from `www.numdam.org/item?id=BSMF_1896__24__199_1`

[22] Y. Hayashi, *Die Rankinsche L-Funktion und Heegner-Punkte für allgemeine Diskriminanten.* (German) [The Rankin L-function and Heegner points for general discriminants]. Dissertation, Rheinische Friedrich-Wilhelms-Universität Bonn, Bonn, 1993. Bonner Mathematische Schriften **259**, Universität Bonn, Mathematisches Institut, Bonn, 1994, viii+157pp.

• Y. Hayashi, *The Rankin's L-function and Heegner points for general discriminants.* Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), no. 2, 30–32. Available online from `projecteuclid.org` at `projecteuclid.org/euclid.pja/1195510808`

[23] K. Heegner, *Diophantische Analysis und Modulfunktionen.* (German) [Diophantine analysis and modular functions]. Math. Z. **56** (1952), 227–253. Available online from the Göttinger Digitalisierungszentrum via `resolver.sub.uni-goettingen.de/purl?GDZPPN002382962` or possibly from `springerlink.com` via `dx.doi.org/10.1007/BF01174749`

[24] N. Jochnowitz, *A p-adic conjecture about derivatives of L-series attached to modular forms.* In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture.* Papers from the workshop held at Boston University, Boston, Massachusetts, August 12–16, 1991, edited by B. Mazur and G. Stevens, Contemporary Mathematics **165**, American Mathematical Society, Providence, RI (1994), 239–263.

[25] A. M. Legendre, *Nouvelles méthodes pour la détermination des orbites des comètes*; avec un appendice: *Sur la Méthode des moindres quarrés.* (French) [New methods for the determination of the orbits of comets; with an appendix: On the method of least squares]. Published in 1805. Available online from `num-scd-ulp.u-strasbg.fr:8080/327`

• M. Legendre, *Sur la méthode moindres quarrés, et sur l'attraction des ellipsoïdes homogènes.* (French) [On the method of least squares, and the attraction of homogeneous ellipsoids]. Republication of relevant parts of above in Mem. Acad., 1811. Available online from `gallica.bnf.fr/ark:/12148/bpt6k62641x`

[26] T. Lundy, J. Van Buskirk, *A new matrix approach to real FFTs and convolutions of length 2^k.* Computing **80** (2007), no. 1, 23–45. Possibly available from `springerlink.com` via `dx.doi.org/10.1007/s00607-007-0222-6`

[27] Z. Mao, F. Rodriguez-Villegas, G. Tornaría, *Computation of the central value of quadratic twists of modular L-functions.* In *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341**, Cambridge University Press (2007), 273–288. Preprint available from `arxiv.org/math/0606762`

[28] P. Martin, M. Watkins, *Symmetric powers of elliptic curve L-functions.* In *Algorithmic Number Theory.* Proceedings of the 7th International Symposium (ANTS-VII) held at the Technische Universität Berlin, Berlin, July 23–28, 2006, edited by F. Hess, S. Pauli, and M. Pohst, Lecture Notes in Computer Science **4076**, Springer, Berlin (2006), 377–392. Preprint available at `arxiv.org/math/0604095` and possibly the paper from `springerlink.com` via `dx.doi.org/10.1007/117920861_27`

[29] J.-F. Mestre, J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième.* (French) [Semi-stable Weil curves of discriminant an m-th power]. J. Reine Angew. Math. **400** (1989), 173–184. Online from the Göttinger Digitalisierungszentrum via `resolver.sub.uni-goettingen.de/purl?GDZPPN002206943`

[30] S. J. Miller, *Investigations of Zeros near the Central Point of Elliptic Curve L-functions.* Exper. Math. **15** (2006), no. 3, 257–279. Preprint available at `arxiv.org/math/0508150`

[31] P. Monsky, *Mock Heegner points and congruent numbers.* Math. Z. **204** (1990), no. 1, 45–67. Online via `resolver.sub.uni-goettingen.de/purl?PPN266833020_0204` and possibly from `springerlink.com` via `dx.doi.org/10.1007/BF02570859`

•

P. Monsky, *Three constructions of rational points on $Y^2 = X^3 \pm NX$.* Math. Z. **209** (1992), no. 3, 445–462. Available online from the Göttinger Digitalisierungszentrum via `resolver.sub.uni-goettingen.de/purl?GDZPPN002440016` and also possibly from `springerlink.com` via `dx.doi.org/10.1007/BF02570844`

◇ P. Monsky, *Errata: "Three constructions of rational points on $Y^2 = X^3 \pm NX$."* Math. Z. **212** (1993), no. 1, 141. Corrects Lemma 4.7 and Theorem 4.8. Online from `resolver.sub.uni-goettingen.de/purl?GDZPPN00244108X` and also possibly available from `springerlink.com` via `dx.doi.org/10.1007/BF02571645`

[32] A. Pacetti, G. Tornaría, *Computing central values of twisted L-series: the case of composite levels.* To appear in Exper. Math. Preprint available at `arxiv.org/math/0607008`

[33] PARI/GP, version `2.4.2-1896`, Bordeaux, Oct. 2007. See `pari.math.u-bordeaux.fr`

[34] H. Petersson, *Konstrucktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung. II.* (German) [Construction of all the solution of a Riemannian functional equation by Dirichlet series with an Euler product development, II]. Math. Ann. **117** (1939), 39–64. Online from the Göttinger Digitalisierungszentrum via `resolver.sub.uni-goettingen.de/purl?GDZPPN002280426` or possibly from `springerlink.com` via `dx.doi.org/10.1007/BF01450007`

[35] G. Ricotta, T. Vidick, *Hauteur asymptotique des points de Heegner.* (French) [Asymptotic height of Heegner points]. To appear in Canadian Journal of Mathematics. Preprint online from `arxiv.org/math/0511439`

[36] N. F. Rogers, *Rank Computations for the Congruent Number Elliptic Curves.* Exper. Math. **9** (2000), no. 4, 591–594, `expmath.org/restricted/9/9.4/rogers.ps`

[37] M. O. Rubinstein, University of Waterloo, data and code for L-functions, available online from `pmmac03.math.uwaterloo.ca/~mrubinst/L_function_public/VALUES` in the directory `DEGREE_2/ELLIPTIC/QUADRATIC_TWISTS/WEIGHT_THREE_HALVES/COEFFICIENTS`

[38] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Kanô Memorial Lectures, No. 1, Publications of the Math. Soc. of Japan, No. 11, Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971.

[39] T. Shintani, *On construction of holomorphic cusp forms of half integral weight.* Nagoya Math. J. **58** (1975), 83–126. Online from `projecteuclid.org/euclid.nmj/1118795445`

[40] D. Simon, *Computing the rank of elliptic curves over number fields.* LMS J. Comput. Math. **5** (2002), 7–17. Online at `www.lms.ac.uk/jcm/5/lms2000-006` and programme available from `www.math.unicaen.fr/~simon/ellQ.gp`

[41] N. C. Snaith, *The derivative of $SO(2N+1)$ characteristic polynomials and rank 3 elliptic curves.* In *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341**, Cambridge University Press (2007), 93–107.

[42] C.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers.* (French) [Analytic investigations in the theory of prime numbers]. Ann. Soc. scient. Bruxelles **20** (1896), 183–256.

[43] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier.* (French) [On the Fourier coefficients of modular forms of half-integral weight]. J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484.

[44] M. Watkins, *Real zeros of real odd Dirichlet L-functions*, Math. Comp. **73** (2004), no. 245, 415–423. Online from `ams.org` via `dx.doi.org/10.1090/S0025-5718-03-01537-0`

[45] M. Watkins, *Some remarks on Heegner point computations*, notes from a short course at the Institut Henri Poincaré, see `arxiv.org/math/0506325`

[46] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551. Possibly online from `jstor.org` through `dx.doi.org/10.2307/2118559`

Mark Watkins
MAGMA Computer Algebra Group
Department of Mathematics, Carslaw Building
University of Sydney, Sydney, Australia
E-mail: `watkins@maths.usyd.edu.au`