ELLIPTIC CURVES, RANK IN FAMILIES AND RANDOM MATRICES

E. KOWALSKI

This survey paper contains two parts. The first one is a written version of a lecture given at the "Random Matrix Theory and L-functions" workshop organized at the Newton Institute in July 2004. This was meant as a very concrete and down to earth introduction to elliptic curves with some description of how random matrices become a tool for the (conjectural) understanding of the rank of Mordell-Weil groups by means of the Birch and Swinnerton-Dyer Conjecture; the reader already acquainted with the basics of the theory of elliptic curves can certainly skip it. The second part was originally the write-up of a lecture given for a workshop on the Birch and Swinnerton-Dyer Conjecture itself, in November 2003 at Princeton University, dealing with what is known and expected about the variation of the rank in families of elliptic curves. Thus it is also a natural continuation of the first part. In comparison with the original text and in accordance with the focus of the first part, more details about the input and confirmations of Random Matrix Theory have been added.

Acknowledgments. I would like to thank the organizers of both workshops for inviting me to gives these lectures, and H. Helfgott, C. Hall, C. Delaunay, S. Miller, M. Young and M. Rubinstein for helpful remarks, in particular for informing me of work in process of publication or in progress that I was unaware at the time of the talks. In fact, since this paper was written, a number of other relevant preprints have appeared; among these we mention [Sn], [Mil2], with no claim to exhaustivity!

Notation. We use synonymously the two notation $f(x) = O(g(x))$ and $f(x) \ll g(x)$ for $x \in X$, where X is some set on which both f and $g \geqslant 0$ are defined; it means that for some "implied" constant $C \geqslant 0$ (which may depend on further parameters), we have $|f(x)| \leqslant Cg(x)$ for all $x \in X$. On the other hand, we use $f = o(g)$ as $x \to x_0$, for some limit point x_0, to mean that the limit of f/g exists and is 0 as $x \to x_0$, and similarly $f \sim g$ for $x \to x_0$ means $f/g \to 1$ as $x \to x_0$.

1. A concrete introduction to elliptic curves

Before embarking on our journey, we refer in general to Silverman's book [AEC] for a very good and readable discussion of the topics covered here, with complete proofs for all but the most advanced. Each subsection will include references to the parts of this book that corresponds, and other references if necessary.

1.1. Elliptic curves as algebraic curves, complex tori and the link between the two.

Elliptic curves can be seen in a number of different ways. We will present the two most geometric. First, an *affine plane cubic curve* over the field $\mathbf{C}$ of complex numbers is simply the set of complex solutions $(x, y) \in \mathbf{C} \times \mathbf{C}$ of an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

(called a *general Weierstrass equation*), where a_1, a_2, a_3, a_4 and a_6 are arbitrary complex numbers. If all the a_i are rational numbers, the curve is said to be *defined over* $\mathbf{Q}$. It is those curves which are most relevant for number theory, and especially

one is concerned with the basic diophantine question which is to find all rational solutions $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ to the equation (1).

For many reasons, it is usually more convenient to present the equation (1) in homogeneous form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2}$$

(which defines a *projective cubic curve*) and look for triplets of solutions (X, Y, Z) in the projective plane $\mathbf{P}_2(\mathbf{C})$ instead of the place $\mathbf{C}^2$, which means looking for non-zero solutions $(X, Y, Z) \neq (0, 0, 0)$ and identifying two solutions (X, Y, Z) and $(\alpha X, \alpha Y, \alpha Z)$ for any non-zero $\alpha \in \mathbf{C}^\times$.

If in a triplet (X, Y, Z) satisfying (2) we have $Z \neq 0$, then we can replace (X, Y, Z) by the equivalent solution $(X/Z, Y/Z, 1)$ and this satisfies (2) if and only if the pair $(x, y) = (X/Z, Y/Z)$ satisfies the original equation (1). So the homogeneous solutions with $Z \neq 0$ are in one-to-one correspondence with the points on the affine cubic curve. However, if $Z = 0$, the equation (2) gives $X = 0$, so the solutions are $(0, Y, 0)$ with $Y \neq 0$ arbitrary. All those are in fact equivalent to a single solution $(0, 1, 0)$, which is called the *point at infinity*, often denote ∞. Note in particular that this point always has rational coordinates.

Plane cubic curves provide the first "picture" of elliptic curves, that as algebraic curves. However, there is a necessary condition imposed on an equation (1) before it is said to be the equation of an elliptic curve, namely it must define a smooth curve in $\mathbf{C} \times \mathbf{C}$. This means that the partial derivatives

$$2y + a_1x + a_3 \quad \text{and} \quad a_1y - 3x^2 - 2a_2x - a_4$$

must not have a common zero (x, y) which is also a point on the cubic curve. There is an explicit "numeric" criterion for this to hold (see [AEC, p. 46]); in the slightly simpler case where $a_1 = a_3 = 0$ (we will see that one can reduce to this case in most situations), the smoothness expresses simply that the cubic polynomial $x^3 + a_2x^2 + a_4x + a_6$ has three distinct roots in $\mathbf{C}$, equivalently that the *discriminant* $\Delta = -16(4a_4^3 + 27a_6^2)$ is non-zero. Thus, this will be true for a "random" equation (1).

To summarize this definition: an elliptic curve, as an algebraic curve, is the set of projective solutions (X, Y, Z) to an equation (2) which defines a smooth curve.

Example 1.1. • The plane cubic curve with equation

$$y^2 = x^3$$

is not an elliptic curve: the point $(0, 0)$ is a singular point (the curve looks like a "cusp" in the neighborhood of $(0, 0)$).

• Similarly, the curve with equation

$$y^2 = x^3 + x^2$$

is not an elliptic curve; again $(0, 0)$ is singular, and the curve looks like a node in the neighborhood of $(0, 0)$.

• The curve with equation

$$y^2 = x^3 - x = x(x - 1)(x + 1)$$

is an elliptic curve, since the right-hand side has three distinct roots in $\mathbf{C}$. This curve is defined over $\mathbf{Q}$. It is often called the *congruent number* curve, for reasons we will explain below; it is also a so-called *CM curve*, and this terminology will also be explained.

• Let $\ell > 2$ be a prime number. *If* (a, b, c) were non-zero rationals such that $a^\ell + b^\ell = c^\ell$, then the cubic curve

$$y^2 = x(x - a^\ell)(x + b^\ell)$$

would be a very remarkable elliptic curve (defined over $\mathbf{Q}$), in fact so remarkable that it cannot possibly exist: this is the "highest level" summary of how Wiles proved Fermat's Great Theorem.

The other view of elliptic curves is more analytic in flavor, and identifies them with *complex tori*. Namely, let ω_1, ω_2 be non-zero complex numbers, with $\omega_1/\omega_2 \notin \mathbf{R}$. Let $\Lambda = \omega_1\mathbf{Z} \oplus \omega_2\mathbf{Z}$; this is an abelian subgroup of $\mathbf{C}$, and it generates $\mathbf{C}$ as an $\mathbf{R}$-vector space. Those two properties characterize the *lattices* in $\mathbf{C}$, and all of them are given as described.

Now consider the quotient group $X = \mathbf{C}/\Lambda$ which one views as a compact Riemann surface (it is compact because, for instance the compact set $\{a\omega_1 + b\omega_2 \mid (a, b) \in [0, 1] \times [0, 1]\}$ projects surjectively to X). Topologically, this is a torus, and as a group, this is $(\mathbf{R}/\mathbf{Z})^2$. Now the analytic definition of an elliptic curve is simply that it is one such quotient $\mathbf{C}/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}$. We will now discuss how this definition and that as smooth plane cubic curve are compatible. A small warning: although it is tempting to think so at first, taking ω_i with rational coordinates does not give the analogue of cubic curves defined over $\mathbf{Q}$! In fact, for a curve defined over $\mathbf{Q}$, the ratio ω_2/ω_1 is almost always transcendental, see e.g. [Ba, Ch. 6].

It is always natural to look for meromorphic functions defined on a Riemann surface (for instance, think that on a cubic curve we have two natural rational functions, $(x, y) \mapsto x$ and $(x, y) \mapsto y$ which are used to give the equation of the curve). Very concretely, this means we wish to consider meromorphic functions

$$f : \mathbf{C} \to \mathbf{C}$$

which are ω_1 and ω_2-periodic:

$$f(z + \omega_1) = f(z) \text{ and } f(z + \omega_2) = f(z).$$

Those f are called *elliptic functions*; this is where the history began in fact, since it was found, over a long period, that the arc-length on an ellipse can be expressed in terms of (inverses of) such functions (see [AEC, 168–170] for a sequence of exercises explaining this).

Now for a given Λ, one can construct an elliptic function $\wp$ which has a pole of order 2 at points of Λ and no other singularities, and satisfies the algebraic differential equation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

for some g_2, $g_3 \in \mathbf{C}$. In fact, this is the Weierstrass $\wp$-function of Λ which is given explicitly by the series

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big),$$

and g_2 and g_3 are the absolutely convergent series

$$g_2 = 60 \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^6}.$$

Sending $z \mapsto (2\wp(z), \sqrt{2}\wp'(z))$ gives points on the plane cubic

$$y^2 = x^3 - g_2x - 2g_3 \tag{3}$$

with $0 \mapsto \infty$ since $\wp$ has a pole at $z = 0$. One shows that this map is bijective, and that this cubic curve is smooth, hence is an elliptic curve "as plane curve". Moreover, one shows that all elliptic curves with $a_1 = a_3 = a_2 = 0$ arise in this manner,

and also that simple changes of variables can bring any Weierstrass equation (2) to the form (3).

References: [AEC, III.1,VI]

1.2. **The group law on elliptic curves and maps between elliptic curves.** The quotient $\mathbf{C}/\Lambda$ has a natural abelian group structure. So there must be a corresponding group structure for the points in the incarnation of the elliptic curve as a smooth plane cubic curve. This "group law" turns out to have a very nice geometric description, which is that if $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R = (x_3, y_3)$ are distinct points on the curve (i.e. distinct solutions to (1)), then we have $P+Q+R = 0$ for this group law if and only if P, Q and R are collinear.

Here is a quick sketch that this does indeed correspond, via the link presented in the previous section, to the addition on $\mathbf{C}/\Lambda$: the equation $F(x, y) = 0$ of the line joining P, Q and R gives an elliptic function $f(z) = F(\wp(z), \wp'(z))$ such that the *divisor* of f is $(p) + (q) + (r) - 3(0)$ where p, q, $r \in \mathbf{C}/\Lambda$ correspond respectively to P, Q, R by the analytic parameterization. (This means that f has three zeros p, q and r modulo Λ, and a triple pole at 0). By integrating zf'/f along the boundary of a fundamental parallelogram, one gets $p + q + r \in \Lambda$.

It is an essential fact that this group law can be expressed by algebraic formulae: for instance, one finds for $y^2 = x^3 + a_4x + a_6$ that $-(x, y) = (x, -y)$, and $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2, \tag{4}$$

$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) - y_1 \tag{5}$$

if $x_1 \neq x_2$. The case $x_1 = x_2$ is treated by a limit process (in other words, replace the line joining the two points by the tangent). It is in fact essential here to use the projective model (2) because the origin for the group law is the point at infinity.

This algebraic description shows that if the curve is defined over $\mathbf{Q}$, then the points with rational coordinates on an elliptic curve (those that we wish to determine as the basic diophantine question) form a subgroup of the group of complex-valued points.

In addition to considering a single elliptic curve, it is also important to study maps between elliptic curves (also called *morphisms* of elliptic curves). They are most easily described in the analytic description: given two lattices Λ_1 and Λ_2 in $\mathbf{C}$, we are looking for holomorphic maps $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$. It is easy to see that there exists complex numbers α and β such that $\alpha\Lambda_1 \subset \Lambda_2$ and $f(z) = \alpha z + \beta$ for $z \in \mathbf{C}/\Lambda_1$.

On the algebraic side, those maps become expressed by polynomials, or more often rational functions; thus it may be necessary to use two or more formulas to describe $f(x, y)$, depending on whether a certain expression is well-defined at (x, y), as we saw already for the case of the group law itself (the formula (4) is valid only for $x_1 \neq x_2$). So an algebraic map between two elliptic curves, seen as algebraic curves, is really a collection of applications defined by rational functions, one of which at least is valid at any given point (including at infinity), and which coincide in case there is more than one possibility. If all those rational functions can be chosen with coefficients in $\mathbf{Q}$, the map is said to be defined over $\mathbf{Q}$.

Example 1.2. Let E be an elliptic curve (2).

• For a fixed point $P_0 \in E$, defining $f(P) = P + P_0$, where $+$ is the group law defined above, gives a map $E \to E$.

• For any integer $n \in \mathbf{Z}$, the application

$$P \mapsto \underbrace{P + \cdots + P}_{n}$$

(again with + the group law on E) is a map $[n] : E \to E$. It is defined over $\mathbf{Q}$ if E itself is defined over $\mathbf{Q}$.

• Let a, b be complex numbers with $a^2 \neq 4b$. The map

$$\{y^2 = x^3 + ax^2 + bx\} \to \{w^2 = v^3 - 2av^2 + (a^2 - 4b)v\}$$
$$(x, y) \mapsto (\tfrac{y^2}{x^2}, \tfrac{y(b-x)^2}{x^2})$$

"is" a map between those two elliptic curves, with $(0, 0) \mapsto \infty$.

• Let $E : y^2 = x^3 - x$. Then $[i] : (x, y) \mapsto (-x, iy)$ is a map (not defined over $\mathbf{Q}$, but over $\mathbf{Q}(i)$, in an obvious sense).

As in the case of complex tori (and as it should be!), any map $E \to F$ between elliptic curves is of the form $f(x) = g(x) + x_0$ where g is a map that preserves the group law, i.e. $g(P + Q) = g(P) + g(Q)$. Such a map is called an *isogeny*.

The isogenies from a given curve to itself form a ring $\mathrm{End}(E)$, where the product is composition of maps and the addition is performed pointwise using the group law: $(f + g)(P) = f(P) + g(P)$. Similarly, if E is defined over $\mathbf{Q}$, the isogenies defined over $\mathbf{Q}$ form a subring $\mathrm{End}_{\mathbf{Q}}(E) \subset \mathrm{End}(E)$ which can be smaller than $\mathrm{End}(E)$, as the fourth example above illustrates.

Usually one has $\mathrm{End}(E) = \mathbf{Z}$, where $n \in \mathbf{Z}$ corresponds to the "multiplication by n" map. This is most easily seen using the analytic description: if a lattice Λ and $\alpha \in \mathbf{C}$ satisfy $\alpha\Lambda \subset \Lambda$, using a basis (ω_1, ω_2) of Λ one has for some integers n_i

$$\begin{cases} (n_1 - \alpha)\omega_1 + n_2\omega_2 = 0 \\ n_3\omega_1 + (n_4 - \alpha)\omega_2 = 0 \end{cases}$$

hence $(n_1 - \alpha)(n_4 - \alpha) - n_2n_3 = 0$, which shows that α is either an integer or the root of a quadratic polynomial; and by solving the system, if $\alpha \notin \mathbf{Z}$, one sees that ω_1/ω_2 is also a quadratic number, so the lattice is very special.

If $\mathrm{End}(E) \neq \mathbf{Z}$, one says that E has *complex multiplication*, abbreviated CM. For instance, the curve $y^2 = x^3 - x$ above is a CM curve since the map $[i]$ described in the example is not multiplication by n for any n.

One shows (again, it is obvious in the analytic description) that a non-zero isogeny $E_1 \to E_2$ is necessarily surjective. Its kernel $\ker f = \{x \in E_1 \mid f(x) = 0\}$ is a finite abelian group. For instance, for $f = [n]$ with $n \neq 0$, the kernel of f is called the group of n-torsion points on E, denoted $E[n]$. Using the group structure for a complex torus $\mathbf{C}/\Lambda \simeq (\mathbf{R}/\mathbf{Z})^2$, it is clear that $E[n] \simeq (\mathbf{Z}/n\mathbf{Z})^2$. All these facts can in fact be proved algebraically.

If the elliptic curve E is defined over $\mathbf{Q}$, the n-torsion points on E have the important property that their coordinates are algebraic numbers. One can think of those points as analogues of the classical roots of unity, since they are solutions to an equation $nx = 0$, similar to the equation $z^n = 1$ in the multiplicative group $\mathbf{C}^\times$. There are indeed numerous analogies from the arithmetic point of view.

Example 1.3. Let E have equation $y^2 = x^3 + a_4x + a_6$. Then

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

where e_i, $1 \leqslant i \leqslant 3$, are the distinct complex roots of $x_3 + a_4x + a_6 = 0$. The group structure on $E[2]$ is described by $(e_i, 0) + (e_j, 0) = (e_k, 0)$ if $i \neq j$, with k the element in $\{1, 2, 3\} - \{i, j\}$.

An isomorphism of elliptic curves is an isogeny f which is one-to-one, or equivalently with $\ker(f) = 0$. It is natural to try to classify all elliptic curves up to isomorphism.

Over $\mathbf{C}$, by simple changes of variable, any Weierstrass equation (1) can be brought to the form $y^2 = x^3 + c_4x + c_6$ for some c_4, c_6. As already mentioned, such equations define an elliptic curve if $\Delta = -16(4c_4^3 + 27c_4^2) \neq 0$. Two such equations can define isomorphic curves only if (with obvious notation) $c_4' = u^4c_4$ and $c_6' = u^6c_6$ for some $u \in \mathbf{C}^\times$. This shows easily that the so-called j-invariant $j = 1728(4c_4)^3/\Delta$ completely describes the isomorphism class of the elliptic curve. Moreover, the curves

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728} \text{ for } j \notin \{0, 1728\}$$
$$y^2 = x^3 - 1 \text{ for } j = 0$$
$$y^2 = x^3 - x \text{ for } j = 1728$$

show that every complex number is the j-invariant for some elliptic curve.

In arithmetic, it is also important to notice that elliptic curves E_1 and E_2 defined over $\mathbf{Q}$ might be isomorphic over $\mathbf{C}$ (i.e., have the same necessarily rational j-invariant) without being isomorphic over $\mathbf{Q}$, in which case E_1 and E_2 are called *twists* of each other. For instance, if $\alpha^2 \in \mathbf{Q}$, $(x, y) \mapsto (\alpha x, \alpha^{3/2}y)$ gives an isomorphism over $\mathbf{C}$ between $y^2 = x^3 - x$ and $y^2 = x^3 - \alpha^2 x$, and those two curves are not usually isomorphic over $\mathbf{Q}$, for instance because the elements of $E[2]$ are rational points on $y^2 = x^3 - x$, whereas they are not on $y^2 = x^3 - \alpha^2 x$ if α is not itself rational.

On the analytic side, where isomorphic tori correspond to homothetic lattices, one shows quite easily that any lattice $\omega_1\mathbf{Z} \oplus \omega_2\mathbf{Z} \subset \mathbf{C}$ can be brought by homothety to the form $\mathbf{Z} \oplus \tau\mathbf{Z}$ for some τ which can be chosen in the upper half-plane $\mathbf{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. Then two such lattices $\mathbf{Z} \oplus \tau\mathbf{Z}$ and $\mathbf{Z} \oplus \tau'\mathbf{Z}$ define isomorphic complex tori if and only if there exists some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$ such that

$$\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

The j-invariant can then be described as a holomorphic map $\mathbf{H} \to \mathbf{C}$ which is $SL(2, \mathbf{Z})$-invariant; it is the prototypical example of a modular function.

References: [AEC, III.2,3,9,VI.4,C.12]

1.3. **The arithmetic of elliptic curves: the Mordell-Weil group.** We now come to our main concern, which is the arithmetic properties of elliptic curves, and in particular the structure of the set of rational points. Let $E/\mathbf{Q}$ be an elliptic curve defined over $\mathbf{Q}$. As already mentioned, the fact that $a_i \in \mathbf{Q}$ implies immediately that the set of rational points on E, denoted $E(\mathbf{Q})$, is in fact a subgroup of E. It is called the *Mordell-Weil group* of E. The fundamental structure theorem is due to Mordell in this case.

Theorem 1.4. *For any elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})$ is a finitely generated abelian group.*

This means that one has an isomorphism

$$E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus F$$

for some integer $r \geqslant 0$, called the *rank* of E (over $\mathbf{Q}$), and some finite group F, which is simply the torsion subgroup of $E(\mathbf{Q})$, i.e., the subgroup of elements of finite order.

The current proof of the theorem is still much the same as Mordell's. It proceeds in two steps: in the first step, one shows that $E(\mathbf{Q})/mE(\mathbf{Q})$ is finite (for some integer $m \geqslant 2$, $m = 2$ gives quite elementary proofs). Then, given representatives for the finite group $E(\mathbf{Q})/mE(\mathbf{Q})$, one shows one to construct a finite set of generators of $E(\mathbf{Q})$.

From a diophantist's point of view, the problem with the proof is that the first part is *ineffective*: it does not provide (and no other argument is proved to yield) the representatives for $E(\mathbf{Q})/mE(\mathbf{Q})$ which are required for the second step (on the other hand, given the representatives, the second step is completely effective). More precisely, one does get an upper bound on r, but no bound for the "height" (i.e., the size) of elements filling up $E(\mathbf{Q})/mE(\mathbf{Q})$. (See below in Section 1.5 for the rigorous definition of the height; here you can think simply of the largest of the number of digits of the numerator and denominateur of the x-coordinate of a point on $E(\mathbf{Q})$).

On the other hand, the finite torsion group F can be computed efficiently, and in fact it has been possible to find a complete list of all finite abelian groups which arise in this way (this is due to Mazur). Here is an example of each torsion group (one can show that each arises for infinitely many elliptic curves over $\mathbf{Q}$):

- $y^2 = x^3 - 2$, torsion $= \{0\}$.
- $y^2 = x^3 + 8$, torsion $= \mathbf{Z}/2\mathbf{Z}$.
- $y^2 = x^3 + 4$, torsion $\simeq \mathbf{Z}/3\mathbf{Z}$.
- $y^2 = x^3 + 4x$, torsion $\simeq \mathbf{Z}/4\mathbf{Z}$.
- $y^2 - y = x^3 - x$, torsion $\simeq \mathbf{Z}/5\mathbf{Z}$.
- $y^2 = x^3 + 1$, torsion $\simeq \mathbf{Z}/6\mathbf{Z}$.
- $y^2 - xy - 4y = x^3 - x^2$, torsion $\simeq \mathbf{Z}/7\mathbf{Z}$.
- $y^2 + 7xy = x^3 + 16x$, torsion $\simeq \mathbf{Z}/8\mathbf{Z}$.
- $y^2 + xy + y = x^3 - x^2 - 14x + 29$, torsion $\simeq \mathbf{Z}/9\mathbf{Z}$.
- $y^2 + xy = x^3 - 45x + 81$, torsion $\simeq \mathbf{Z}/10\mathbf{Z}$.
- $y^2 + 43xy - 210y = x^3 - 210x^2$, torsion $\simeq \mathbf{Z}/12\mathbf{Z}$.
- $y^2 = x^3 - 4x$, torsion $\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
- $y^2 + xy - 5y = x^3 - 5x^2$, torsion $\simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
- $y^2 + 5xy - 6y = x^3 - 3x^2$, torsion $\simeq \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
- $y^2 + 17xy - 120y = x^3 - 60x^2$, torsion $\simeq \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Before continuing, here is a beautiful instance of the intrusion of elliptic curves in a very classical problem: what are the rationals (so-called *congruent numbers*) r such that there is a right-triangle with rational lengths a, b, c and area r.

Proposition 1.5. *A squarefree integer $n \geqslant 1$ is a congruent number if and only if the elliptic curve*

$$E_n \,:\, y^2 = x^3 - n^2 x$$

has rank $r_n \geqslant 1$.

The j-invariant of E_n is $j(E_n) = 1728$, which shows that all the curves E_n are isomorphic over $\mathbf{C}$ (not over $\mathbf{Q}$!), i.e., they are all twists of each other.

The arithmetic of elliptic curves has led J. Tunnell to a very simple algorithm for checking whether a given squarefree integer n is a congruent number; it is however still conditional on the Birch and Swinnerton-Dyer Conjecture described below.

Theorem 1.6 (Tunnell)**.** *If the Birch and Swinnerton-Dyer Conjecture holds, then (for odd squarefree n), n is a congruent number if and only if the number of triples of integers (x, y, z) such that $2x^2 + y^2 + 8z^2 = n$ is twice the number of triples such that $2x^2 + y^2 + 32z^2 = n$.*

Example 1.7. Let's check that $n = 41$ is congruent:

$$41 = \overbrace{2(\pm 4)^2 + (\pm 3)^2}^{4} = \overbrace{(\pm 3)^2 + 8(\pm 2)^2}^{4} = \overbrace{2(\pm 4)^2 + (\pm 1)^2 + 8(\pm 1)^2}^{8}$$
$$= \overbrace{2(\pm 2)^2 + (\pm 5)^2 + 8(\pm 1)^2}^{8} = \overbrace{2(\pm 2)^2 + (\pm 1)^2 + 8(\pm 2)^2}^{8}$$
$$41 = \overbrace{2(\pm 4)^2 + (\pm 3)^2}^{4} = \overbrace{(\pm 3)^2 + 32(\pm 1)^2}^{4} = c\overbrace{2(\pm 2)^2 + (\pm 1)^2 + 32(\pm 1)^2}^{8}$$

Note that Tunnell's theorem does not provide the lengths a, b, c of the right triangle with area 41, but they can be derived easily from the proof of the proposition, provided one knows a point with infinite order on E_n.

References: [AEC, VIII, X], [K].

1.4. **Reduction modulo primes and the Hasse-Weil L-function of an elliptic curve.** Let $E/\mathbf{Q}$ be an elliptic curve. By change of variable one can assume (i.e., E is isomorphic to a curve such) that the Weierstrass equation (1) has integral coefficients. For any prime p, one can reduce modulo p and look at solutions (x, y) in the finite field $\mathbf{Z}/p\mathbf{Z}$ of

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \,(\mathrm{mod}\, p). \tag{6}$$

For any prime p that does not divide the discriminant Δ_E, this equation, when one looks for solutions in an algebraic closure of $\mathbf{Z}/p\mathbf{Z}$, "defines" an elliptic curve over $\mathbf{Z}/p\mathbf{Z}$ (but we haven't really said what this means and this requires some care).

It is a simpler diophantine question to find the solutions to (6). In fact, there are certainly only a finite number of them in $(\mathbf{Z}/p\mathbf{Z})^2$, or in homogeneous coordinates in the projective plane over $\mathbf{Z}/p\mathbf{Z}$. The main fact is then the following result which says quite precisely how many solutions there can be:

Theorem 1.8 (Hasse)**.** *Let $p \nmid \Delta_E$. The number N_p of projective solutions modulo p to the equation defining E can be written $N_p = p + 1 - a_p$ with*

$$|a_p| \leqslant 2\sqrt{p}. \tag{7}$$

This is also called the Riemann Hypothesis for the curve E reduced modulo p.

Remark 1.9. If $a_1 = a_3 = 0$ then

$$a_p = -\sum_{x \,(\mathrm{mod}\, p)} \Big(\frac{x^3 + a_2x^2 + a_4x + a_6}{p}\Big) \tag{8}$$

with $(\frac{y}{p})$ the Legendre symbol, i.e., $(\frac{y}{p})$ is equal to 0 for $y = 0$, and otherwise is equal to 1 if y is a square modulo p and -1 is y is not a square modulo p; note that $1 + (\frac{y}{p})$ is the number of solutions to the equation $X^2 = y$ in $\mathbf{Z}/p\mathbf{Z}$, which gives quickly the formula stated from the definition $N_p = p + 1 - a_p$ and the fact that there is a single point at infinity.

It is reasonable to expect on probabilistic grounds that the size of this sum should be about $\sqrt{p}$, because there is about the same chance that the value of $x^3 + a_2x^2 + a_4x + a_6$ be a square as a non-square modulo p (for p odd, there are as many squares as non-squares among non-zero integers modulo p, namely $(p-1)/2$).

Example 1.10. In general, there is no simpler explicit formula for a_p. However, there is an elementary description if the curve has complex multiplication. For instance, let E be the congruent number curve with equation $y^2 = x^3 - x$, which has complex multiplication by i. We have $\Delta_E = 64$. Then a_p is given as follows: if

$p \equiv 3 \pmod 4$, then $a_p = 0$; if $p \equiv 1 \pmod 4$, then (Fermat) one can write $p = a^2+b^2$ with a odd, b even, and $a + b \equiv 1 \pmod 4$; then $a_p = 2a$.

For a few non-CM elliptic curves, one can give an "implicit" description. For instance, consider the curve

$$X_1(11) \,:\, y^2 + y = x^3 - x^2$$

with discriminant -11, then define $a(n)$ for $n \geqslant 1$ by the formal power series identity

$$\sum_{n\geqslant 1} a(n)q^n = q\prod_{n\geqslant 1}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots$$

Then the a_p for the curve $X_1(11)$ is the coefficient $a(p)$.

Finding the points on the curve modulo primes is fairly easy, and can provide information on the rational points (i.e., the Mordell-Weil group). However, using only one prime is clearly not sufficient (for instance, because there are usually many points modulo p which are not obtained by reduction of rational points). An important idea in number theory is to construct a "global" invariant that encompasses information obtained modulo all primes. In the case of elliptic curves, this takes the form of the so-called Hasse-Weil zeta function (or L-function) of an elliptic curve $E/\mathbf{Q}$.

We define first a naive version, namely

$$\ell(E,s) = \prod_{p\nmid \Delta_E} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where p runs over the primes not dividing the discriminant of E. This product converges absolutely for $\mathrm{Re}(s) > 3/2$ by Hasse's Theorem (the precise shape of the product may seem strange, but it is very well explained by looking at the points on the elliptic curve, not only after reduction modulo p, but also in finite extension fields of $\mathbf{Z}/p\mathbf{Z}$).

As a first statement indicating some kind of nice behavior of the various reductions modulo primes, having to do with the fact that they have a single "global" origin over $\mathbf{Q}$, Hasse conjectured that $\ell(E,s)$ has an analytic continuation to $\mathbf{C}$. This is now seen as an imprecise form of the *modularity* of elliptic curves over $\mathbf{Q}$, which was proved by Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor.

To explain the precise form, one must first refine the definition to obtain the "right" L-function. This requires the insertion in the product of correct factors at the primes $p \mid \Delta_E$.

First one may remark that because Δ_E is not an isomorphism-invariant of E, one can have $p \mid \Delta_E$ for some Weierstrass equation but not for another. So one defines the *conductor* of E, an integer $\mathfrak{f}(E) \geqslant 1$ such that $p \nmid \mathfrak{f}(E)$ if and only if E has a smooth reduction modulo p, possibly after some change of variable (isomorphism over $\mathbf{Q}$). For $p \mid \mathfrak{f}(E)$, the exponent f_p of p in $\mathfrak{f}(E)$ is dictated by the geometry of the singular reduction, in ways that can be quite complicated. But here are the simplest cases which are often sufficient:

- If the reduction of E modulo p has a node, then $f_p = 1$ ("multiplicative reduction").
- If $p > 3$ and the reduction of E modulo p has a cusp, then $f_p = 2$ ("additive reduction").
- If $p = 2$ or $p = 3$ and the reduction of E modulo p has a cusp, the definition of f_p is much more intricate. In all cases, one shows that $2 \leqslant f_p \leqslant 11$.

If $p \mid \mathfrak{f}(E)$, define

$$a_p = \begin{cases} 0 & \text{if } f_p \geqslant 2, \\ -1 & \text{if } f_p = 1, \text{ and the slopes of the node are in } \mathbf{Z}/p\mathbf{Z}, \\ 1 & \text{otherwise.} \end{cases}$$

(for the second case, the meaning is that a node can be such that the two "tangent directions" are either in $\mathbf{Z}/p\mathbf{Z}$ or generate a quadratic extension of $\mathbf{Z}/p\mathbf{Z}$; one speaks of *split* or *non-split* multiplicative reduction).

Example 1.11. • For the curve $X_1(11)$ or for the curve $y^2 + y = x^3 - x$, one has $\mathfrak{f}(E) = 11$. This is the smallest possible conductor for an elliptic curve $E/\mathbf{Q}$.

• If E is given by $y^2 = x^3 + ax + b$ and E_d is its *quadratic twist* given by $dy^2 = x^3 + ax + b$, where d is a squarefree integer, then $\mathfrak{f}(E_d)$ divides $d^2\,\mathfrak{f}(E)$, with equality if d is coprime with $\mathfrak{f}(E)$.

Using $\mathfrak{f}(E)$ and those a_p, the Hasse-Weil zeta function is defined by

$$L(E, s) = \prod_{p \mid \mathfrak{f}(E)} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \mathfrak{f}(E)} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

The meaning of the modularity of E can now be stated precisely. Denote by $a_E(n)$ the coefficients in the expansion of the Euler product $L(E, s)$ in Dirichlet series

$$L(E, s) = \sum_{n \geqslant 1} a_E(n) n^{-s}$$

and define

$$f(z) = \sum_{n \geqslant 1} a_E(n) e^{2\pi i n z} \text{ for } z \in \mathbf{H}, \text{i.e, } \mathrm{Im}(z) > 0.$$

The series converges absolutely and uniformly on compacts to define a holomorphic function $f : \mathbf{H} \to \mathbf{C}$. Then modularity of E means that we have

$$f\Big(\frac{az + b}{cz + d}\Big) = (cz + d)^2 f(z)$$

for all $a, b, c, d \in \mathbf{Z}$, $ad - bc = 1$, with $\mathfrak{f}(E) \mid c$, and moreover that $\mathrm{Im}(z)|f(z)|$ is bounded on $\mathbf{H}$ (those conditions express that f is a cusp form of weight 2 for the Hecke congruence subgroup $\Gamma_0(\mathfrak{f}(E))$).

From this one deduces that $L(E, s)$ has analytic continuation to an entire function by means of the formula

$$(2\pi)^{-s}\Gamma(s)L(E, s) = \int_0^\infty f(iy) y^{s-1} dy,$$

which is due to Hecke (and applies to all cusp forms of weight 2). Thus Hasse's Conjecture follows in this indirect manner.

The theory of Hecke gives more information, which is also very important: by means of the so-called Fricke involution and multiplicity one for Hecke operators, one shows that $L(E, s)$ also satisfies a functional equation

$$\Lambda(E, s) = w_E\, \mathfrak{f}(E)^{1-s} \Lambda(E, 2 - s) \tag{9}$$

for some $w_E \in \{\pm 1\}$ (called the sign of the functional equation), where

$$\Lambda(E, s) = (2\pi)^{-s}\Gamma(s)L(E, s).$$

In addition, one can prove that the sign w_E factorizes as a product over $p \mid \mathfrak{f}(E)$ of "local" signs $w_{E,p} \in \{\pm 1\}$. It is also important to know that w_E is effectively computable. For instance, if $\mathfrak{f}(E)$ is squarefree, one can show that

$$w_E = \mu(\mathfrak{f}(E)) a_E(\mathfrak{f}(E))$$

where $\mu(\mathfrak{f}(E))$ is the Möbius function, which is simply here $(-1)^k$, k being the number of distinct prime factors of $\mathfrak{f}(E)$.

Remark 1.12. When the curve $E/\mathbf{Q}$ happens to be a CM curve (for instance, the congruent number curve $y^2 = x^3 - x$), then one can give a much more elementary proof of the modularity of $L(E, s)$ than the general one provided by Wiles et al.

References: [AEC, V,C.16], [I2, 8], [K, II].

1.5. **The Birch and Swinnerton-Dyer conjecture.** Let E be an elliptic curve defined over $\mathbf{Q}$. Recall that the hope is still to solve, as much as possible, the diophantine question of finding the Mordell-Weil group of E. There is an intuition that the L-function of E, which has been built from "local" information about the various reductions of E modulo primes, should provide some help. It is not at all clear how to make this precise. However, there is a beautiful conjecture that provides a very clean link.

By modularity, we know that $L(E, s)$ is holomorphic, in particular defined at $s = 1$. Then the simplest form of the Birch and Swinnerton-Dyer Conjecture is

Conjecture 1.13. *We have*

$$\operatorname{rank} E(\mathbf{Q}) = \operatorname{ord}_{s=1} L(E, s),$$

i.e, $L(E, s)$ has a zero at $s = 1$ with order equal to the rank of the Mordell-Weil group of E.

Remark 1.14. To indicate the amazing consequences of such a statement, notice that if the sign w_E of the functional equation happens to be -1 (one often speaks of "odd" functional equation, or "odd" curve), then by (9) we find that $L(E, 1) = 0$, hence, under the Birch and Swinnerton-Dyer Conjecture, we have $\operatorname{rank} E(\mathbf{Q}) \geqslant 1$ in that case. However, the condition $w_E = -1$, as we have remarked, is a *local* condition, which in fact only involves the behavior of the curve at primes dividing $\mathfrak{f}(E)$ (primes of bad reduction). So this very simple-looking local condition should imply the global consequence that there is a non-trivial point of infinite order in $E(\mathbf{Q})$. The challenge is then to find a way to obtain concretely such a point; no algorithm is known to solve that problem.

There is also a more refined form of the conjecture, which takes the following form:

Conjecture 1.15. *We have*

$$L(E, s) \sim \alpha(s - 1)^r \text{ as } s \to 1,$$

where $r = \operatorname{rank} E(\mathbf{Q})$ and

$$\alpha = \frac{\Omega |Ш(E)| R(E) c}{|E(\mathbf{Q})_{tors}|^2} > 0, \tag{10}$$

the various terms Ω, $Ш(E)$, $R(E)$, c being all strictly positive real numbers which are described below.

Here are short descriptions of the unexplained quantities in this conjecture.

• $|E(\mathbf{Q})_{tors}|$ is the cardinality of the set of rational torsion points on E. As we have already mentioned, it is easy to compute, and in fact it is well-understood theoretically. (In particular, it takes only finitely many values).

• c (the *Tamagawa number*) is given by the product over primes of the local Tamagawa numbers $c_p = |E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)|$, where $E_0(\mathbf{Q}_p)$ is the set of points which have non-singular reduction modulo p. If E has good reduction at p, we have $c_p = 1$, so that the product really has only finitely many terms. There is an

efficient algorithm to compute c_p. This algorithm is described by K. Rubin in his paper in this volume.

• Ω is the *real period* of E, an elliptic integral of the type

$$\int_{E^0(\mathbf{R})} \frac{dx}{2y}$$

where $E^0(\mathbf{R})$ is the infinite component of the real points of the curve. It is also easily computable.

• $R(E)$ is the *elliptic regulator*: let $x_1, \dots, x_r$ be a basis for the free part of $E(\mathbf{Q})$. Then

$$R(E) = \det(\langle x_i, x_j \rangle)$$

where $\langle \cdot, \cdot \rangle$ is the *canonical height* on $E(\mathbf{Q})$, the bilinear form coming from the following quadratic form:

$$\|p\| = \lim_{n \to +\infty} 4^{-n} h([2^n]p)$$

where, for a point $p = (x, y) \in E(\mathbf{Q})$, the "naïve" height $h(p)$ is defined by

$$h(p) = h((x, y)) = \frac{1}{2} \log H(x)$$

with

$$H(x) = \max(|r|, |s|), \text{ if } x = \frac{r}{s} \text{ with } r, s \text{ integers and } (r, s) = 1.$$

The regulator R is hard to compute, since it involves finding a basis of the Mordell-Weil group, but because there are explicit and efficiently computable formulas for the height function, one can indeed compute it very quickly given the generators x_i. Note in particular that if $r = 0$, we have $R = 1$ by definition.

References: [AEC, VIII.7,8,9C.16]

1.6. **The Tate-Shafarevitch group.** There only remains to explain the term $Ш(E)$ in the refined Birch and Swinnerton-Dyer Conjecture. This is the so-called Tate-Shafarevitch group of E, which is in many ways the most mysterious component of the formula. For instance, although it is implicit in the statement that this must be a *finite* group, this is not known in general![1]

We will spend a few paragraphs trying to explain a bit more where this group comes from and why it is so elusive. We do this partly because it is quite a beautiful object in its own right, and partly from the belief that some progress could be made on its study (e.g., the finiteness conjecture) if more people, especially with an analytic frame of mind, looked at it more carefully...

First, here is a sketch explaining how the elements of $Ш(E)$ arise. Let $E/\mathbf{Q}$ be an elliptic curve, and assume its equation is of the type

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

with $e_i \in \mathbf{Q}$ (which means that the 2-torsion points $(0, e_i)$ are in $E(\mathbf{Q})$). We are looking for a way to find all rational solutions.

Let $(x, y) \in E(\mathbf{Q})$. Note that for $p \nmid \Delta_E$, the smoothness modulo p implies that at most one of the $x - e_i$ can be divisible by p. Since their product is the square y^2, we see that p occurs with an even exponent in the factorization of each $x - e_i$. This holds for all $p \nmid \Delta_E$, hence putting everything together, we can write

$$x - e_i = c_i w_i^2$$

[1] In fact, for elliptic curves over function fields over finite fields, the full Birch and Swinnerton-Dyer Conjecture is now a theorem of Kato and Trihan, *if* the Tate-Shafarevitch group is always finite.

for some $z_i \in \mathbf{Q}$, where the numerator and denominator of c_i are divisible only by primes dividing Δ_E. Now if a $p \mid \Delta_E$ has even exponent, we can change w_i and get a similar relation with c_i coprime with this p. If $p \mid \Delta_E$ has odd exponent (say $2k+1$), we can still "remove" similarly the p^{2k} part. Hence we have a relation

$$x - e_i = b_i z_i^2$$

with $z_i \in \mathbf{Q}$ and b_i is an integer which is product of some primes dividing Δ_E, each with exponent at most 1.

Obviously the set of choices for b_i is finite. We do not know which b_i actually occur, but we can make a list of all those which can conceivably arise from a rational point on E. Let us call T this finite, effectively computable, set of triples $b = (b_1, b_2, b_3)$ of non-zero squarefree integers (i.e., those where each prime divisor divides Δ_E). We have shown that given $(x, y) \in E(\mathbf{Q})$, there is some $b \in T$, and rationals z_1, z_2, z_3, such that

$$\begin{cases} y^2 = (x-e_1)(x-e_2)(x-e_3) \\ x - e_1 = b_1 z_1^2 \\ x - e_2 = b_2 z_2^2 \\ x - e_3 = b_3 z_3^2. \end{cases} \tag{11}$$

We now consider the set C_b of solutions to these equations for a fixed b; thus there are 5 variables (x, y, z_1, z_2, z_3). The set C_b is a curve in affine 5-space (since there are 4 relations). It is easy to see, by eliminating some unknowns, that C_b is isomorphic (over $\mathbf{Q}$) to the curve in 3-space with coordinates (z_1, z_2, z_3) given by the two equations

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) \\ b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1). \end{cases} \tag{12}$$

The crucial point is that for given $b \in T$ (recall that T is not simply the set of those (b_1, b_2, b_3) that actually arise from a rational point, but may be larger), the curve C_b may have a rational point or not. Certainly, if it does not, this particular b could not in fact arise from a rational point on E in the way described above. But conversely, if a rational point $(z_1, z_2, z_3) \in C_b(\mathbf{Q})$ exists, then using (11) one clearly gets at least one point in $E(\mathbf{Q})$. Now one shows (by further elementary algebraic manipulations for instance) that finding a rational point on each of the curves C_b (for which one exists) is tantamount to finding representatives of the quotient group $E(\mathbf{Q})/2E(\mathbf{Q})$. As the discussion of Mordell's Theorem recalled, it is then known how to find generators for $E(\mathbf{Q})$.

The above method of computing $E(\mathbf{Q})$ can indeed be implemented in many situations. However, in general it is confronted with the problem that there is no algorithm known to check whether the curves C_b have a rational point or not.

The common method of dealing with this has been to remark that one can, on the other hand, compute quite easily the subset $S \subset T$ of those b for which C_b has "locally" a point at all p (essentially, a point modulo p for all p), and a real-valued point. This is useful because, obviously, the set of b for which C_b has a rational point is a subset of S. (The S is for Selmer; this set can also be equipped with a group structure and is then called the 2-Selmer group of E).

However, there may be elements of S which still do not have a rational point (one says that the "Hasse principle" fails for C_b). Those elements "are" exactly the non-zero elements of order 2 in $Ш(E)$. Note that, as a subset of S, it is a finite set, but the point is that this is simply a subset of the full Tate-Shafarevitch group.

The full group is not as easy to define in concrete terms. Here is a more abstract definition, as a set (the group structure is not obvious): one says that a curve $C/\mathbf{Q}$

is a principal homogeneous space for $E/\mathbf{Q}$ if one can define an action of E on C, i.e. an algebraic map (denoted + here)

$$\begin{cases} E \times C \to C \\ (P, p) \mapsto p + P \end{cases}$$

such that $p+(P+Q) = (p+P)+Q$ and $p+P = q$ has a unique solution (denoted $q-p$) for all (p,q). (Note the similarity with the notion of an affine space with its associated vector space in elementary geometry). There is always a "trivial" homogeneous space, namely E itself with the action being given by the addition on E.

It is not quite obvious, but in fact the curves C_b with equations (12) are examples of homogeneous spaces for E. A definition of $Ш(E)$ is then as the set of all homogeneous spaces $C/\mathbf{Q}$ for which $C(\mathbf{R})$ and $C(\mathbf{Q}_p)$, for all p, are non-empty, modulo the relation of isomorphism as homogeneous spaces, which means that $C \sim C'$ if there exists an isomorphism $f : C \to C'$ defined over $\mathbf{Q}$ with $f(p+P) = p + f(P)$.

Once the group structure on $Ш(E)$ is defined, one sees that E is the identity element in $Ш(E)$. Then, to make the link with the previous curves C_b, notice that $C \in Ш(E)$ is trivial if and only if $C(\mathbf{Q}) \neq \emptyset$: first, if C is trivial, it is isomorphic to E, so has a rational point corresponding to the origin 0 of the group law of E. Conversely, if $p_0 \in C(\mathbf{Q})$ is a rational point, the map $p \mapsto p - p_0$ gives the required isomorphism $C \simeq E$.

There is no reason (and it often happens that this is not the case) that $Ш(E)$ should contain only the elements of order 2 which have already been described. One can show that $Ш(E)$ is a torsion group (i.e., every element is of finite order), and also that for any integer $n \geqslant 1$, the subgroup of n-torsion elements in $Ш(E)$ is finite (in ways at least similar in spirit to the case of $n = 2$). However, we have no a priori bound on the order of an element of $Ш(E)$; to have such a (finite) bound would be equivalent to proving that $Ш(E)$ is finite. This we state formally as a conjecture, due to Tate and Shafarevitch:

Conjecture 1.16. *For all $E/\mathbf{Q}$, the Tate-Shafarevich group $Ш(E)$ is a finite group.*

The refined form of the Birch and Swinnerton-Dyer Conjecture does not make sense without assuming this statement. For quite a long time, it was the case that not a *single* elliptic curve $E/\mathbf{Q}$ with $Ш(E)$ finite was known, but the work of Rubin, Kolyvagin and others have provided many examples in cases where the order of vanishing of the L-function of E is $\leqslant 1$.

A further useful known fact is that there is a (highly non-obvious!) symplectic pairing (due to Cassels)

$$Ш(E) \times Ш(E) \to \mathbf{Q}/\mathbf{Z} \tag{13}$$

which is perfect if $Ш(E)$ is finite; this gives information on the group structure.

Example 1.17. Let E be the elliptic curve $y^2 = x^3 - 24300$, $j = 0$. The rank is 0, the regulator is 1, the torsion group is trivial, the Tamagawa number is 1, we have

$$L(E, 1) = 4.061375813927\ldots$$
$$\Omega = 0.451263979325\ldots$$

and so $|Ш(E)| = 9$, which means (by the existence of the Cassels pairing) that $Ш(E) \simeq (\mathbf{Z}/3\mathbf{Z})^2$. In fact, the following are equations for all locally trivial homogeneous spaces under E:

$$\begin{aligned} C \simeq E \quad & x^3 + y^3 + 60x^3 = 0 \\ C_1 \quad & 3x^3 + 4y^3 + 5z^3 = 0 \\ C_2 \quad & 12x^3 + y^3 + 5z^3 = 0 \\ C_3 \quad & 15x^3 + 4y^3 + z^3 = 0 \\ C_4 \quad & 3x^3 + 20y^3 + z^3 = 0 \end{aligned}$$

(each of the four equations C_i above corresponds to two opposite elements of $Ш(E)$, equivalently to a line in $(\mathbf{Z}/3\mathbf{Z})^2$). See [Ma] for more details.

Remark 1.18. (1) Here is the cohomological definition of $Ш(E)$, which makes the group structure apparent, but gives little information related to finiteness:

$$Ш(E) = \ker\left\{ H^1(G_{\mathbf{Q}}, E) \to \prod_v H^1(G_{\mathbf{Q}_v}, E) \right\}.$$

Similarly the set called S above can be introduced more generally as the *Selmer group* for any prime ℓ

$$\mathrm{Sel}_\ell(E) = \ker\Big\{ H^1(G_{\mathbf{Q}}, E[\ell]) \to \prod_v H^1(G_{\mathbf{Q}_v}, E) \Big\}$$

and then the elementary computations that have been sketched correspond to the case $\ell = 2$ of the following short exact sequence:

$$0 \to E(\mathbf{Q})/\ell E(\mathbf{Q}) \to \mathrm{Sel}_\ell(E) \to Ш(E)[\ell] \to 0. \tag{14}$$

(2) The author believes that analytic number theory should be brought to bear on the finiteness conjecture for $Ш(E)$. Here is one reason for this: there is a well-known analogy between $Ш(E)$ and the class group of number fields, and in the latter case, the finiteness is known, but all proofs, in one way or another, depend on *inequalities*, whether from geometry of numbers or from the use of L-functions. Here is a wildly off-hand suggestion[2]: can one associate to a given $C \in Ш(E)$ some kind of holomorphic function f_C, in such a way that the f_C are linearly independent, but belong to a finite dimensional space? (Think of theta functions associated to ideal classes in an imaginary quadratic field, which are modular forms of a fixed type, hence live in a space that can be proved to be of finite dimension in a completely independent way...)

References: [AEC, X], see also the article by Swinnerton-Dyer [Sw] in this volume.

1.7. **Enter random matrices...** The Birch and Swinnerton-Dyer Conjecture is still unproved, but much evidence exists in its favor (certainly for the simple form), so that it is very reasonable to take it as an assumption if one wishes to study the "general" behavior of the rank of elliptic curves over $\mathbf{Q}$. One may expect it to help understand, for example, whether there are elliptic curves $E/\mathbf{Q}$ with arbitrarily large rank.[3]

The conjecture certainly helps explain why such curves, if they exist, are very hard to find: it is easy to show that if the Birch and Swinnerton-Dyer Conjecture

[2] Of course, the author *has* tried to make something out of it without success...

[3] In early May, 2006, N. Elkies announced having found a curve with rank $\geqslant 28$, improving the previous record of 24.

holds, there exists an absolute constant $c > 0$ such that for any $E/\mathbf{Q}$ with rank r we have

$$\mathfrak{f}(E) \geqslant e^{cr}; \tag{15}$$

this is obtained by bounding the order of vanishing of $L(E, s)$ at $s = 1$ by the number $N(E, 1)$ of zeros ρ of $L(E, s)$ with $|\operatorname{Im}(\rho)| \leqslant 1$ (counted with multiplicity), which is well-known to satisfy

$$\operatorname{ord}_{s=1} L(E, s) \leqslant N(E, 1) \ll \log \mathfrak{f}(E)$$

with an absolute implied constant. If one assumes the Generalized Riemann Hypothesis, there even exists $c > 0$ such that

$$\mathfrak{f}(E) \geqslant e^{cr \log r} \tag{16}$$

(for both facts, see e.g. [IK, 5.8]; the analogue of this inequality is known to be sharp over function fields, see [U1], and it may also be over $\mathbf{Q}$).

Unfortunately, at the present moment at least, our knowledge about L-functions and the distribution of their zeros is still quite limited, and we do not have very many unconditional results. It is worth mentioning one striking application of the Birch and Swinnerton-Dyer Conjecture, but one that goes the other way: Goldfeld showed how one could use an L-function with a zero at $s = 1$ of order $\geqslant 3$ to solve effectively the class number problem for imaginary quadratic fields, and thus, instead of using L-functions to study elliptic curves, it was elliptic curves which were used by Gross-Zagier to produce such an L-function in confirmation with Goldfeld's expectation.

However, for many questions, the recent development of Random Matrix Models for families of L-functions offers a new, unexpected, way of probing the diophantine mystery that is the Mordell-Weil group. As we will see in the second part, new phenomena and conjectures are appearing and it can be hoped that besides new insight, they will yield new ideas by comparison with the viewpoints of algebraic geometry.

2. Variation of the rank in families of elliptic curves

The purpose of this second part is to describe some of the known results concerning the variation of the rank of elliptic curves, mostly over $\mathbf{Q}$, when a large number of curves are taken together and considered as a whole, not as individuals. We discuss what analytic methods, especially based on L-functions (and hence on assuming the Birch and Swinnerton-Dyer conjecture), have been able to produce. Thus some other techniques (such as the use of sieve methods to produce twists with "large" rank) will not be considered, although they are certainly interesting.

It will be seen that even with quite deep assumptions, the outcome remains in some ways disappointing. It may be that currently the most remarkable achievements are the conjectures that arise out of the random matrix models concerning the order of vanishing of L-functions, hence conjecturally concerning the rank; this will be our second main topic.

For readers who skipped the first part, we recall some relevant notation: $\mathfrak{f}(E)$ is the conductor of an elliptic curve $E/\mathbf{Q}$, and $a_E(n)$ denotes the coefficients of its Hasse-Weil zeta function $L(E, s)$.

2.1. Families and invariants.

Although the term "family" has a number of well-defined and deep meanings in algebraic geometry and arithmetic, we will only need a very weak notion here, amounting to hardly more than walking through a (multi)set of elliptic curves with some indexing. (This is not the same definition discussed by D. Farmer in his paper [Fa] in this volume; it may be said that we exploit here some

concrete features of the specific L-functions of elliptic curves, or of modular forms, and benefit from the fact that for some problems, it is only necessary to have means of "comparing" two curves taken in the family, which is done efficiently using the Rankin-Selberg convolution; also, a useful survey of the case of function fields, to which we will make passing references, is contained in D. Ulmer's paper [U2]).

Precisely, a *family* $\mathcal{E}$ of elliptic curves over $\mathbf{Q}$ is the data, for any $T \geqslant 1$, of a finite (multi)set[4] $\mathcal{E}(T)$ of elliptic curves $E/\mathbf{Q}$, which we subject to the following simple conditions:

(a) There exist constants c_1, $c_2 \geqslant 0$ and $\alpha, \beta > 0$ such that

$$c_1 T^{\alpha} \leqslant |\mathcal{E}(T)| \leqslant c_2 T^{\beta} \tag{17}$$

for $T \geqslant 1$. (The curves are counted with their multiplicity in $|\mathcal{E}(T)|$, if one $E/\mathbf{Q}$ appears more than once in $\mathcal{E}(T)$.)

(b) There exist constants $c_3 \geqslant 0$ and $A \geqslant 0$ such that for any $T \geqslant 1$ and $E \in \mathcal{E}(T)$, we have

$$\mathfrak{f}(E) \leqslant c_3 T^{A}, \tag{18}$$

where $\mathfrak{f}(E)$ is the conductor of E.

We will now give several examples to indicate more precisely what we have in mind. For simplicity we often write $E \in \mathcal{E}$ to indicate that $E \in \mathcal{E}(T)$ for some T; similarly a map $f : \mathcal{E} \to X$ for any set X is a family of maps $f_T : \mathcal{E}(T) \to X$ (so if a curve E belongs to both $\mathcal{E}(T_1)$ and $\mathcal{E}(T_2)$, one may have $f_{T_1}(E) \neq f_{T_2}(E)$, e.g. if $f_T(E) = T$.)

(1) Algebraic families: Consider polynomials a_1, a_2, a_3, a_4, $a_6 \in \mathbf{Z}[t]$ and for any $t \in \mathbf{Z}$ let E_t be the curve given by the equation

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t). \tag{19}$$

If $\Delta(t)$, the discriminant of this curve, is not identically 0, there will be a finite set S of $t \in \mathbf{Z}$ such that E_t is an elliptic curve for $t \notin S$. If the j invariant $j(t)$ is also non-constant, then letting

$$\mathcal{E}(T) = \{E_t \mid |t| \leqslant T \text{ and } t \notin S\}$$

we get a family of elliptic curves; here there will be multiplicity if $E_t \simeq E_s$ for some $t \neq s$.

(2) Quadratic twists: This is partly a special case of the previous one. Fix an elliptic curve $E/\mathbf{Q}$ and for all quadratic fundamental discriminants d let E_d be the corresponding quadratic twist of E: if E is given by $y^2 = x^3 + a_4 x + a_6$, then E_d is the curve with equation

$$dy^2 = x^3 + a_4 x + a_6.$$

For any d, this is an elliptic curve and putting

$$\mathcal{E}_E(T) = \{E_d \mid |d| \leqslant T \text{ and } d \text{ is a fundamental quadratic discriminant}\}$$

gives an example of a family (recall $\mathfrak{f}(E_d) \mid d^2\,\mathfrak{f}(E)$, with equality if d is coprime to $\mathfrak{f}(E)$).

(3) All curves indexed by height: This was considered by Brumer [B]: for any integers a_4 and a_6 such that $4a_4^3 + 27a_6^2 \neq 0$ and such that $p^4 \mid a_4$ implies that $p^6 \nmid a_6$, let E_{a_4,a_6} be the curve

$$E_{a_4,a_6} : y^2 = x^3 + a_4 x + a_6,$$

given by the corresponding Weierstrass equation. Then let

$$\mathcal{E}_H(T) = \{E_{a_4,a_6} \mid |a_4|^3,\ |a_6|^2 \leqslant T\} \tag{20}$$

[4] We permit some of the curves to come "with multiplicity"; see the examples below, especially algebraic families.

This is a family. It is known that every elliptic curve over $\mathbf{Q}$ occurs exactly once among the E_{a_4,a_6}.

(4) All curves indexed by conductor: In this case we simply take

$$\mathcal{E}_c(T) = \{E/\mathbf{Q} \mid \mathfrak{f}(E) \leqslant T\}$$

A variant consists in taking only one representative in each isogeny class; in the corresponding family $\mathcal{E}'_c$, one can identify

$$\mathcal{E}'_c(T) = \{f \in S_2^*(q, \mathbf{Z}) \mid q \leqslant T\}$$

the set of primitive forms of weight 2 for $\Gamma_0(q)$, $q \leqslant T$, which have integral coefficients (this by modularity of elliptic curves over $\mathbf{Q}$ and the isogeny theorem).

(5) A counter-example: Here is a set of elliptic curves that (conjecturally) fails to define a family in our sense. For any $n \geqslant 0$, let $E_n/\mathbf{Q}$ be a curve (if it exists) with smallest conductor such that $\operatorname{rank} E_n(\mathbf{Q}) = n$ and $\mathcal{E}(T) = \{E_n \mid 0 \leqslant n \leqslant T\}$. Two things prevent this from being a family: either E_n does not exist for n large enough (although this is not currently expected to be the case); or even if it exists, then on B-SD we have (15) so the conductor grows exponentially, contradicting (18).

Obviously one can generalize the definitions above. Particularly, one could consider elliptic curves over an arbitrary global field, or abelian varieties over a global field. In the case of $\mathbf{Q}$ a narrower but very natural generalization is to consider arbitrary primitive modular forms (of weight 2) instead of those associated with Hasse-Weil L-functions of elliptic curves, or more geometrically (as described by Shimura) the isomorphism (or isogeny) classes of abelian varieties which are quotients of the jacobians $J_0(q)$ of the modular curves $X_0(q)$. We will only give the briefest remarks below about the "general" generalizations, but we will sometimes mention in more detail the case of the "family" $\mathcal{E}_0$ with $\mathcal{E}_0(q)$ the set of primitive weight 2 cusp-forms of level q (often restricted to primes for simplicity). Indeed much stronger analytic results have been obtained in this case, which can usefully serve as reference points in investigations of families elliptic curves.

For example it is worth mentioning (correcting slightly my remark quoted at the end of [U1]) that for an abelian variety $A/\mathbf{Q}$ of dimension $g \geqslant 1$, the analogue of (16), expressed in terms of the order of vanishing instead of the conductor, is that

$$\operatorname{ord}_{s=1} L(A, s) \ll \frac{\log \mathfrak{f}(A)}{\log \frac{1}{g} \log \mathfrak{f}(A)} \tag{21}$$

on GRH, the implied constant being absolute, if the conjectured analytic continuation and functional equation of $L(A, s)$ hold (note that $\mathfrak{f}(A) \geqslant 3^g$ also follows from the latter); see e.g. [IK, 5.14], [M]. The bound (21) is sharp because one can take $A = E^g$, $g \to +\infty$, for some elliptic curve $E/\mathbf{Q}$ of rank $\geqslant 1$. One may suspect that it is possible to improve (21) if A is simple. This is indeed the case for $J_0(q)$, q prime, for which $\log \mathfrak{f}(J_0(q)) \leqslant q \log q$,

$$\operatorname{ord}_{s=1} L(J_0(q), s) \geqslant \tfrac{q}{24} + o(q) \tag{22}$$

(by very easy sign considerations) and in fact

$$\operatorname{rank} J_0(q) \geqslant \tfrac{7q}{192} + o(q) \tag{23}$$

using Heegner points and fairly difficult non-vanishing results for L-functions [KM1].

Given a family $\mathcal{E}$, we are interested in the average behavior of various invariants related to the rank of the Mordell-Weil group of the curves $E \in \mathcal{E}$. For this we introduce the notation

$$A_{\mathcal{E}}(T, f) = \sum_{E \in \mathcal{E}(T)} f(E)$$

for any function $f : \mathcal{E} \to \mathbf{C}$. If $f = 1$ we denote simply $A_{\mathcal{E}}(T, 1) = A_{\mathcal{E}}(T)$, the number of elements in the family of "index" T (by (17), it grows polynomially). This is the natural comparison function with respect to which one can speak of "the average value" of f on $\mathcal{E}$: for instance, if f is real valued, this average value will be said to be $\leqslant M$ for some $M \in \mathbf{R}$ if

$$A_{\mathcal{E}}(T, f) \leqslant M A_{\mathcal{E}}(T) + o(A_{\mathcal{E}}(T))$$

for $T \to +\infty$, and similarly with $\geqslant M$, $= M$...

Among many interesting functions, we will mention the following:

(1) The rank, $\mathrm{rk}(E) = \mathrm{rank}\, E(\mathbf{Q})$.

(2) The "analytic rank", $\mathrm{ord}(E) = \mathrm{ord}_{s=1} L(E, s)$, well-defined since $E/\mathbf{Q}$ is always modular. The B-SD conjecture implies $\mathrm{rk}(E) = \mathrm{ord}(E)$.

(3) The special value, $L(E) = L(E, 1)$, and more generally the moments and derivatives: $L^{(k)}(E)^m = L^{(k)}(E, 1)^m$, or the characteristic functions $v^{(k)}$ of k-th order vanishing and $V^{(k)}$ of order of vanishing $\geqslant k$: $v^{(k)}(E) = 1$ if $\mathrm{ord}(E) = k$, and 0 otherwise, $V^{(k)}(E) = 1$ if $\mathrm{ord}(E) \geqslant k$ and 0 otherwise.

(4) The root number $w(E) = \pm 1$, i.e. the sign of the functional equation (9).

(5) The parity of the rank, $p(E) = (-1)^{\mathrm{rk}(E)}$; conjecturally $p(E) = w(E)$, and this is now known if the Tate-Shafarevitch group $Ш(E)$ is finite [N].

(6) For a prime ℓ, the order $m_\ell(E)$ of $E(\mathbf{Q})/\ell E(\mathbf{Q})$ or the order $s_\ell(E)$ of the ℓ-Selmer group $\mathrm{Sel}_\ell(E)$. One has $\ell^{\mathrm{rk}(E)} \leqslant m_\ell(E) \leqslant s_\ell(E)$, and if $E[\ell](\mathbf{Q}) = 0$, then $m_\ell(E) = \ell^{\mathrm{rk}(E)}$ (see (14)).

In addition to the relations already indicated, an important observation (going back to Shimura) is that $\mathrm{ord}(E) \geqslant \frac{1}{2}(1 - w(E))$: the functional equation (9) imposes $\mathrm{ord}(E) \geqslant 1$ if $w(E) = -1$, and otherwise $\mathrm{ord}(E) \geqslant 0$ (the latter is *not* a trivial fact: it needs modularity to be mentioned, and the fact that Hecke L-functions are entire). In particular we derive for a family $\mathcal{E}$

$$A_{\mathcal{E}}(T, \mathrm{ord}) \geqslant A_{\mathcal{E}}(T, \tfrac{1}{2}(1 - w)),$$

and on B-SD

$$A_{\mathcal{E}}(T, \mathrm{rk}) \geqslant A_{\mathcal{E}}(T, \tfrac{1}{2}(1 - w)),$$

which is one of the ways to get lower-bounds for the average rank. Without B-SD, recall that the Gross-Zagier formula and Kolyvagin's results give

$$A_{\mathcal{E}}(T, \mathrm{rk}) \geqslant A_{\mathcal{E}}(T, \tfrac{1}{2}(1 - w)v')$$

(this is the starting point towards (23) for instance.)

2.2. **Conjectures and heuristics.** Most of the current heuristics and conjectures on the variation of the rank involve assuming B-SD and then using some of the well-known (or emerging) conjectures about L-functions and the distribution of their zeros, a very extensively studied subject. One can also try to argue from the arguments leading to the proof of the Mordell-Weil theorem, but it is hard to make precise predictions because of the subtlety of issues involved.[5] (A third method is to make a guess, as in the conjecture that the rank of elliptic curves over $\mathbf{Q}$ is unbounded; neither from the point of view of L-functions and B-SD, nor from the Mordell-Weil theorem, does there appear convincing evidence at this time).

The basic heuristic about the order of vanishing of $L(E, s)$ at $s = 1$ has already been mentioned: it is that if $w(E) = -1$, then $\mathrm{ord}(E) \geqslant 1$, and that this should in general be the only way to produce an L-function vanishing at the central point, the order of vanishing being then the minimal compatible with $w(E)$, i.e. $L(E)$ should be non-zero if $w(E) = 1$ and $L'(E)$ should be non-zero if $w(E) = -1$. Note

[5] E.g. problems with class groups or ramification in the torsion fields of the curve.

that this heuristic can only be true in a suitable average sense since there certainly exist families of curves with $\mathrm{rk}(E) > 1$ for $E \in \mathcal{E}$.

To transform this principle into more precise predictions for the average rank, one needs another ingredient: namely, we are led to expect that in an "unbiased" family $\mathcal{E}$ one has

$$A_{\mathcal{E}}(T, \mathrm{ord}) \sim A_{\mathcal{E}}(T, \tfrac{1}{2}(1+w)) = \frac{A_{\mathcal{E}}(T)}{2} + \frac{A_{\mathcal{E}}(T, w)}{2},$$

and one has to treat the average of the root number. A second heuristic principle is that, again "in general", one should have about equal chance to have $w(E) = 1$ as $w(E) = -1$ in a family $\mathcal{E}$, leading to the vague conjecture:

Conjecture 2.1. *Let $\mathcal{E}$ be an "unbiased" family of elliptic curves over $\mathbf{Q}$. Then we have*

$$A_{\mathcal{E}}(T, w) = o(A_{\mathcal{E}}(T))$$
$$A_{\mathcal{E}}(T, \mathrm{rk}) = A_{\mathcal{E}}(T, \mathrm{ord}) \sim \tfrac{1}{2} A_{\mathcal{E}}(T)$$

as $T \to +\infty$.

It remains to find a better idea of what should be an unbiased family. For an algebraic family (Example 1 above), it is known that it is possible to find $\mathcal{E}$ such that $w(E)$, $E \in \mathcal{E}$, is constant. However the results of Helfgott [He] give a much clearer picture of the situation: in case the elliptic surface which "is the family" has at least one place v of multiplicative reduction (a generic situation), it shows that the even distribution of root numbers holds under some deep conjectures on the squarefree numbers represented by polynomials (and in fact are more or less equivalent with those), which are widely expected to hold – in particular, are consistent with general principles of cancellation in sums involving the Möbius function.

For the family $\mathcal{E}_E$ of quadratic twists of a given curve E, one has

$$w(E_d) = \chi_d(-\mathfrak{f}(E)) w(E) \tag{24}$$

for $(d, \mathfrak{f}(E)) = 1$, where $\chi_d = (\frac{d}{\cdot})$ is the Kronecker symbol associated with d. It follows that $w(E_d)$ takes the values ± 1 depending on $d \pmod{4\,\mathfrak{f}(E)}$, and does so asymptotically equally often. In this case, Conjecture 2.1 was formulated by Goldfeld.

Certainly the families $\mathcal{E}_H$ and $\mathcal{E}_c$ are expected to be unbiased. It is known that $w(E)$ is evenly distributed for $\mathcal{E}_H$, but it is not yet known for $\mathcal{E}_c$.

Remark 2.2. It is not necessarily the case that the family $J_0(q)$ is always simpler to deal with than families of elliptic curves. For instance consider the problem of averaging over q (prime) the root number $w(q)$ of $J_0(q)$. One finds using the Selberg trace formula and the formula for the dimension of the space of weight 2 cusp forms of level q that proving even distribution of ± 1 is equivalent to proving the even distribution of the value $h_{odd}(p) \pmod 4$ of the odd part of $h(\mathbf{Q}(\sqrt{-q}))$ modulo 4! This is a special case of Cohen-Lenstra predictions but is completely open. One also has

$$h_{odd}(p) \pmod 4 = \Gamma_p(\tfrac{1}{2}) \pmod 4$$

where Γ_p is the p-adic Gamma function and this makes sense because $\Gamma_p(\frac{1}{2})^2 = 1$. (This was remarked by H. Cohen who happened to be computing the right-hand side using GP exactly as I came in his office asking about the distribution of the left-hand side...)

2.3. **Random matrix models.** Quite recently, a deeper understanding of zeros of various L-functions has been obtained from Montgomery's first study of pair-correlation of zeros of the Riemann zeta function and the observed relation with the density of spacings of eigenvalues of random hermitian matrices of large rank, studied by Wigner for entirely different reasons. This has been set in a general framework by Katz and Sarnak [KS1], [KS2], who also gave very strong evidence by proving an analogue over function fields. Although the fundamental principle (that the distribution of zeros of "families"[6] of L-functions should be governed in some sense by the corresponding distributions of eigenvalues of large random matrices of some type, the latter being dictated by an hypothetical "symmetry group" of the family) remains entirely conjectural over number fields, a body of evidence exists, both numerical (see e.g. [O], [R1]), and theoretical: with certain restrictions, one has verified predictions based on this principle and a heuristic determination of the symmetry group, see e.g. [RoS] and [ILS] (the latter is significant because it treats situations where the type of symmetry group matters, and gets answers in perfect agreement). We will mention in Section 2.5 some similar results for families of elliptic curves.

There are more detailed surveys in the papers and books already mentioned. For us, it will be enough to state that by making various identifications of symmetry group (supported by the analogue cases over function fields, where this group is a well-defined monodromy group), Conjecture 2.1 appears as a very particular case of the Katz-Sarnak philosophy. But much more significantly, the random matrix models can make more precise predictions, such as when trying to estimate the number of curves in a family with rank at least 2. Being stronger, the resulting conjectures are easier to test for numerically. We will now describe a few examples.

Consider the subfamily $\mathcal{E}_{E,+}$ of the the family $\mathcal{E}_E$ of quadratic twists of $E/\mathbf{Q}$ such that $w(E_d) = 1$, and the average $A_{\mathcal{E}_E}(T, V'')$, which means that we count the number of twists with even order $\geqslant 2$. Using the Waldspurger formula for $L(E_d, 1)$, Sarnak conjectured that $A_{\mathcal{E}_{E,+}}(T, V'')$ should be of order $T^{3/4}$ (or equivalently $A_{\mathcal{E}_E}(T)^{3/4}$). Conrey, Keating, Rubinstein and Snaith [CKRS] use random matrix models to predict:

Conjecture 2.3. *There exist constants $c_+(E) > 0$ and $d_+(E) \in \mathbf{R}$, depending only on E, such that*

$$A_{\mathcal{E}_{E,+}}(T, V'') \sim c_+(E) A_{\mathcal{E}_E}(T)^{3/4} (\log T)^{d_+(E)}$$

as $T \to +\infty$.

(In this case, namely the twists with $w(E_d) = 1$, the suspected symmetry group is $SO(2N)$; for odd sign, it is in fact different, namely $SO(2N+1)$, so it is natural to distinguish between the two cases).

Although $d_+(E)$ can be predicted (not very easily), there is not yet a predicted value of the constant $c_+(E)$, which makes numerical tests of this conjecture not as convincing as it could be. However, another conjecture is proposed in [CKRS] which is easier to test. Namely, fix a prime p where E has good reduction, and split the family $\mathcal{E}_{E,+}$ in $\mathcal{E}_{E,s}$ and $\mathcal{E}_{E,i}$ where $E_d \in \mathcal{E}_{E,s}$ if $\chi_d(p) = 1$ and $E_d \in \mathcal{E}_{E,i}$ if $\chi_d(p) = -1$. Then

[6]There is not yet a compelling definition of this notion, beyond the kind of minimal assumptions we have postulated; however, see D. Farmer's article in this volume for a stronger set of analytic axioms which is sufficient to confidently make very strong predictions from Random Matrix Theory, but note that his "orthogonality" axiom is not usually sufficient to prove rigorously the expect asymptotic formulas.

Conjecture 2.4. *We have*

$$\lim_{T\to+\infty}\frac{A_{\mathcal{E}_{E,s}}(T,V'')}{A_{\mathcal{E}_{E,i}}(T,V'')}=\sqrt{\frac{p+1-a_E(p)}{p+1+a_E(p)}}.$$

The numerical evidence about this in [CKRS] is quite good. Note the interpretation of the limit as the ratio of $|E(\mathbf{Z}/p\mathbf{Z})|$ and $|E^t(\mathbf{Z}/p\mathbf{Z})|$, where E^t is the quadratic twist of the reduction of E modulo p. An arithmetic explanation for the appearance of such a constant would be quite interesting. This conjecture has been generalized by M. Young to the family of all elliptic curves indexed by height [Yo4].

Random Matrix models have also been used to study the behavior of the rank of the group of points on an elliptic curve $E/\mathbf{Q}$ which are defined in some extension field $K/\mathbf{Q}$. To do this, one uses the general form of the Birch and Swinnerton-Dyer conjecture that predicts that the rank of $E(K)$ be equal to the order of vanishing of the L-function $L_K(E,s)$ of E over the field K. If $K/\mathbf{Q}$ is a finite Galois extension with group G, there is a factorization

$$L_K(E,s)=\prod_{\chi}L(E\otimes\chi,s)$$

of $L_K(E,s)$ in terms of twists of E by irreducible characters of the group G. Although the analytic continuation and functional equation of these twists are not often known, there are conjectures and partial results if χ is of degree 1 or 2. In particular, the desired properties hold if $K/\mathbf{Q}$ is a cyclic extension of degree k.

David, Fearnley and Kisilevsky [DFK] used this approach to make in particular a conjecture on cyclic extensions $K/\mathbf{Q}$ for which the rank of $E(K)$ can be strictly larger than that of $E(\mathbf{Q})$; under the Birch and Swinnerton-Dyer Conjecture, this is the same as asking for what characters χ one of the values $L(E\otimes\chi,1)$ can vanish. They predict for instance that there should be only finitely many cyclic field of fixed prime degree $k\geqslant 7$ for which $\operatorname{rank}E(K)>\operatorname{rank}E(\mathbf{Q})$.

Another recent development has been the use by Delaunay [D2] of the general conjectures and principles about moments of L-functions of various type (due to Conrey, Farmer, Keating, Rubinstein and Snaith [CFKRS]) together with the conjecture of Birch and Swinnerton-Dyer to predict the leading order asymptotic for moments of all order of the order of the Tate-Shafarevitch groups in a family of quadratic twists. More precisely, one can define the analytic order $S(E)$ using (10), for a curve with $w(E)=1$, pretending that it has rank 0 (so $S(E)=0$ if $\operatorname{rank}E(\mathbf{Q})\geqslant 1$), and then predict the asymptotic of $S(E)^k$ by averaging $L(E,1)^k$. Similarly one can do the same with elements of the family with $w(E)=-1$, using the derivative $L'(E,1)$ to define an analytic order $S'(E)$. The expectation from Goldfeld's Conjecture is that summing both predicted heuristics for $S(E_d)^k$ and $S'(E_d)^k$, restricted each respectively to twists with $w(E_d)=1$ or $w(E_d)=-1$, one should get the correct asymptotic for $Ш(E)^k$ as higher rank twists, for which $S(E)=S'(E)=0$, should contribute less.

2.4. **Theoretical results.** We will now discuss some of the known theoretical results towards the problems and conjectures discussed in the previous sections. First, we should comment a little bit more on the relation between this kind of average consideration and the B-SD conjecture. Obviously we do not expect to prove the conjecture by this method, even in special cases. One could envision that, if it fails very badly, this could be proved by averaging the rank and the order of vanishing for a family and noting a discrepancy (e.g., if an algebraic family $\mathcal{E}$ built so that $\operatorname{rk}(E)\geqslant 11$ for all $E\in\mathcal{E}$, as in [M], happened to be such that $\operatorname{ord}(E)=9$ or 10 for $E\in\mathcal{E}$, where one would expect that $A_{\mathcal{E}}(T,L^{(9)})$ would be comparable to $A_{\mathcal{E}}(T)$...), but that is of course highly unlikely for many reasons.

More seriously, even without B-SD it is certainly an interesting problem (requiring no special justification) to study the average of special values of L-functions, and we can hope to provide some evidence for B-SD by giving examples where the rank and the order of vanishing are of comparable size, on average. This is an appealing problem, but (to the author's knowledge), there is no known "non-obvious" family $\mathcal{E}$ for which we can prove unconditionally that

$$\alpha \leqslant \frac{A_{\mathcal{E}}(T, \mathrm{rk})}{A_{\mathcal{E}}(T, \mathrm{ord})} \leqslant \beta$$

for some constants α, $\beta > 0$ and all T large enough (with the convention $0/0 = 1$ which is natural here). Even in the case of $J_0(q)$, q prime, one can prove

$$\mathrm{ord}(J_0(q)) \leqslant 0.1q + o(q)$$

(see [KM2], [KMV]) in addition to (22) and (23), but there is no known upper bound for $\mathrm{rk}(J_0(q))$ of the right order of magnitude.

Another way that average studies could be useful would be if they yielded some insight into why the B-SD conjecture is true: what exactly makes this local-global principle operate?

The best understood case is that of the family $\mathcal{E}_E$ of twists of a given E. In fact, Heath-Brown has proved very precise unconditional results on the distribution of the order s_2 of the 2-Selmer group of twists of the congruent number curve. Precisely let $\mathcal{E}$ be the family of curves E_d of type

$$E_d \,:\, y^2 = x^3 - d^2 x$$

for d odd and squarefree. Heath-Brown proves [H1], [H2] the following results on the distribution of s_2.

Theorem 2.5. *Let $\mathcal{E}$ be the family above.*

(1) *For any $k \geqslant 0$ we have*

$$A_{\mathcal{E}}(T, s_2^k) \sim d_k A_{\mathcal{E}}(T)$$

as $T \to +\infty$, where

$$d_k = \prod_{j=1}^{k} (1 + 2^j).$$

(2) *For any $r \geqslant 0$, let χ_r be the characteristic function of $s_2(E) = 2^{r+2}$. We have*

$$A_{\mathcal{E}}(T, \chi_r) \sim \tfrac{1}{2} e_r A_{\mathcal{E}}(T) \tag{25}$$

as $T \to +\infty$, where

$$e_r = 2^r \prod_{j=1}^{r} (2^j - 1)^{-1} \prod_{j \geqslant 0} (1 - 2^{-2j-1}).$$

(3) *In particular for $T \geqslant 2$ we have*

$$\alpha A_{\mathcal{E}}(T) \leqslant A_{\mathcal{E}}(T, \mathrm{rk}) \leqslant \beta A_{\mathcal{E}}(T)$$

for some constants α, $\beta > 0$ and

$$A_{\mathcal{E}}(T, v) \gg A_{\mathcal{E}}(T).$$

(3) *For $k \geqslant 0$, let $r_k(E)$ be the characteristic function of the condition $\mathrm{rk}(E) = k$. We have*

$$A_{\mathcal{E}}(T, r_k) \leqslant 1.742^{-(k^2-k)/2} A_{\mathcal{E}}(T)$$

for T large enough.

As discussed below, we only know about the order of vanishing ord in this family that

$$(\tfrac{1}{2}+o(1))A_{\mathcal{E}}(T)\leqslant A_{\mathcal{E}}(T,\mathrm{ord})\text{ and }A_{\mathcal{E}}(T,\mathrm{ord})=o(T\log T)$$

as $T\to+\infty$. (On GRH, we do get a bounded order of vanishing on average).

We can only say a few words about the strategy of the proof, since it is very different from the other cases we will discuss below, and is independent of L-functions (see Heath-Brown's short note in this volume [H4]). The main fact is (1), from which the rest follows quite directly. For instance, (3) follows using the fact that $4\mid s_2(E_d)$ since the 2-torsion points are rational, and $s_2(E_d)=4$ (resp. $=8$) implies that $\mathrm{rk}(E_d)=0$ (resp. $=1$) by the standard exact sequence (14) for $\ell=2$ and the ensuing formula

$$\mathrm{rk}(E_d)=\dim_{\mathbf{Z}/2\mathbf{Z}}\mathrm{Sel}_2(E_d)-\dim_{\mathbf{Z}/2\mathbf{Z}}(Ш(E_d)[2])-2,$$

together with the fact that the last two terms are even (by the existence of Cassels's pairing (13)).

By the classical descent theory that we sketched in Section 1.6, the elements of the 2-Selmer group of E_d are identified with quadruplets (D_1,D_2,D_3,D_4) of integers $\geqslant 1$ such that $d=D_1D_2D_3D_4$ and the system

$$D_1X^2+D_4W^2=D_2Y^2\text{ and }D_1X^2-D_4W^2=D_3Z^2$$

has solutions modulo p for all primes p (it automatically has real solutions); compare with (12). This condition need be checked only at $p\mid d$, and leads to a formula for $s_2(E_d)$ as a fairly involved sum of quadratic residue symbols. Then one needs to take the k-th power of this expression and perform the average: this is a very impressive analytic feat, which can not be summarized here.

Remark 2.6. Although the presence of the Tate-Shafarevitch group means that we can not confirm Conjecture 2.1 using this result, interesting evidence comes from confronting it with the heuristics for the order of $Ш(E)$ proposed by Delaunay (see [D1] and his article in this volume [D3]), on the Cohen-Lenstra model. Indeed, his heuristics suggest that for $r\geqslant 0$, the proportion of d for which E_d has rank 0 and $Ш(E_d)[2]\simeq(\mathbf{Z}/2\mathbf{Z})^{2r}$ should be

$$f_r=2^{-r(2r-1)}\prod_{j=1}^{r}\Big(1-\frac{1}{4^j}\Big)\prod_{j\geqslant r+1}(1-2^{-2j+1})$$

(we use the fact that if $Ш(E)$ is finite, then $Ш(E)[2]\simeq Ш(E)/2Ш(E)$, which is the group really considered by Delaunay.)

A simple computation reveals that $f_r=e_{2r}$ in (25), therefore all twists with $\dim_{\mathbf{Z}/2\mathbf{Z}}\mathrm{Sel}_2(E_d)=r+2$ (even) are accounted for by curves of rank 0 if this heuristic is correct. Or, to state it another way: if Conjecture 2.1 holds, the heuristic for the 2-rank of $Ш(E_d)$ is correct. Obviously, such consistency is quite convincing. Note that for curves of rank 1 and r odd, one needs to alter a little bit the proposed heuristic of Delaunay (specifically, replace $M_u(f)=M^s_{u/2}(f)$ by $M_u(f)=M^s_u(f)$ in [D1, p. 195, Heuristic Assumption]) to get agreement, but this seems a reasonable change (the $u/2$ does not carry great evidence towards it).

When seeing this, Delaunay also noticed that Heath-Brown proved in [H1] that the average of $s_2(E_d)/4$ is equal to 3, both over curves with even rank and over curves with odd rank (note that the parity conjecture is proved by Monsky in the Appendix to [H2] for this family, so having even or odd rank translates to a congruence modulo 8 for d). Assuming Conjecture 2.1 in this case, this translates to statements on the average of $|Ш(E_d)[2]|$, namely it should be $=3$ for rank 0 and $3/2$ for rank 1. This agrees with [D1, Example 7], again using M_u instead of $M_{u/2}$.

The methods of Heath-Brown have been partly generalized to the family of quadratic twists for a curve E with the 2-torsion points rational [Y2], but not in full generality. One can however study the order of vanishing using analytic techniques. The best results are due to Perelli and Pomykala [PP]. They prove the following:

Theorem 2.7. *Let $E/\mathbf{Q}$ be a fixed elliptic curve and consider the family $\mathcal{E}_E$ of quadratic twists by d coprime with $\mathfrak{f}(E)$. For any $\varepsilon > 0$ we have*

$$A_{\mathcal{E}_E}(T, \mathrm{rk}) \geqslant A_{\mathcal{E}_E}(T, v') \gg A_{\mathcal{E}_E}(T)^{1-\varepsilon} \tag{26}$$

for $T \geqslant 2$, and any $\varepsilon > 0$, the implied constant depending only on E and ε. Moreover we have

$$A_{\mathcal{E}_E}(T, \mathrm{ord}) = o(T \log T) \text{ as } T \to +\infty. \tag{27}$$

Recall that (21) gives the trivial upper bound

$$A_{\mathcal{E}}(T, \mathrm{ord}) \ll (A+1) A_{\mathcal{E}}(T)(\log T)$$

for any family $\mathcal{E}$ and $T \geqslant 2$, the implied constant depending on the family, so the gain in (27) is quite small. It seems very hard to improve this however, as it depends on a difficult large-sieve type inequality of Heath-Brown for real characters.

On GRH, Goldfeld [G] has proved that the order of vanishing is bounded on average. Also, Ono [On] currently has the best lower bound on the proportion of twists with $L(E_d) \neq 0$ (hence of twists with $\mathrm{rk}(E_d) = 0$):

$$A_{\mathcal{E}_E}(T, v) \gg A_{\mathcal{E}_E}(T)(\log T)^{c(E)-1}$$

for $T \geqslant 2$ and some constant $c(E) \geqslant 0$, the implied constant depending only on E. In some cases this has been improved to a positive proportion (see e.g. [Y1]).

The method of proof for (26) is based on computing the first and second moments ($A_{\mathcal{E}_E}(T, L')$ and $A_{\mathcal{E}_E}(T, |L'|^2)$) of $L'(E_d)$: Cauchy's inequality gives

$$A_{\mathcal{E}_E}(T, v') \geqslant \frac{A_{\mathcal{E}_E}(T, L')^2}{A_{\mathcal{E}_E}(T, |L'|^2)} \tag{28}$$

so it suffices to give a lower bound for the first moment $A_{\mathcal{E}_E}(T, L')$ and an upper bound for the second moment $A_{\mathcal{E}_E}(T, |L'|^2)$; this is done (as is the case for (27)) using the methods sketched in the next section. Note that the moment conjectures for mollified families of L-functions, if applicable in this case, immediately imply that the order of vanishing of the twists is bounded on average.

Consider now the case of an algebraic family $\mathcal{E}$. Basically the same methods used for quadratic twists are available, but the averaging is much more difficult to perform in general and currently the only non-trivial results are known under the additional assumption of the Generalized Riemann Hypothesis to study the L-functions. Then one can prove the following result:

Theorem 2.8. *Let $\mathcal{E}$ be an algebraic family of elliptic curves over $\mathbf{Q}$. Assume GRH and the Tate conjecture for the elliptic surface associated to $\mathcal{E}/\mathbf{Q}$. Then we have*

$$A_{\mathcal{E}}(T, \mathrm{ord}) \leqslant (\mathrm{rank}\, \mathcal{E}(\mathbf{Q}(t)) + \deg N_{\mathcal{E}} + \tfrac{1}{2})(1 + o(1)) A_{\mathcal{E}}(T)$$

as $T \to +\infty$, where $\mathrm{rank}\, \mathcal{E}(\mathbf{Q}(t))$ is the rank of $\mathcal{E}$ as an elliptic curve over $\mathbf{Q}(t)$ and $N_{\mathcal{E}}$ is the conductor polynomial defined by

$$N_{\mathcal{E}} = \prod_{\Delta(t)=0} (X - t) \prod_{c_4(t)=c_6(t)=0} (X - t) \in \mathbf{Z}[X], \tag{29}$$

$c_4(t)$ and $c_6(t)$ being the usual invariants for the curves (19).

We will describe more precisely below the particular case of Tate's conjecture which is required. The theorem as stated is due to Silverman [S], building on earlier work of Fouvry and Pomykala [FP] and Michel [Mi] which established weaker or slightly different inequalities, all with the conclusion that the average order of vanishing of $\mathcal{E}$ is bounded, hence also the rank on B-SD. (Note however that the generic rank of $\mathcal{E}(\mathbf{Q}(t))$ arises in the bound independently of B-SD).

This average boundedness of the rank was also proved by Brumer [B] for the family $\mathcal{E}_H$ of all elliptic curves ordered by height. The best known result is due to M. Young [Yo1, Yo3]:

Theorem 2.9. *Let $\mathcal{E}_H$ be the family* (20)*. Assume GRH for L-functions of elliptic curves. Then we have*

$$A_{\mathcal{E}_H}(T, \mathrm{ord}) \leqslant (\tfrac{25}{14} + o(1))A_{\mathcal{E}_H}(T)$$

as $T \to +\infty$.

Brumer had the constant 2.3 instead of 25/14, which had been improved to 2 by Heath-Brown [H3]. Young's result is significant because a constant which is strictly smaller than 2 implies that a positive proportion of the curves must have rank either 0 or 1.

2.5. **Basic analytic tools.** The analytic investigations of the L-functions of elliptic curves are based on two quite general formulas which go back in principle to Riemann and other early investigators of the Riemann zeta function. The first, called somewhat misleadingly "the approximate functional equation", is a convenient expression for L-functions in the critical strip where the Dirichlet series is not convergent. Here is one of many variants, which we state for modular forms, since it is not in any way specific to elliptic curves.

Proposition 2.10. *Let f be a primitive cusp form of weight 2 and conductor q with Fourier coefficients $\lambda_f(n)$ and root number $w(f)$. We have for $X \geqslant 1$*

$$L(f,1) = \sum_n \frac{\lambda_f(n)}{n} \exp\Big(-\frac{2\pi n}{X\sqrt{q}}\Big) + w(f) \sum_n \frac{\overline{\lambda_f}(n)}{n} \exp\Big(-\frac{2\pi n X}{\sqrt{q}}\Big).$$

In particular if $E/\mathbf{Q}$ is an elliptic curve we have for any $X \geqslant 1$

$$L(E,1) = \sum_n \frac{a_E(n)}{n} \exp\Big(-\frac{2\pi n}{X\sqrt{\mathfrak{f}(E)}}\Big) + w(E) \sum_n \frac{a_E(n)}{n} \exp\Big(-\frac{2\pi n X}{\sqrt{\mathfrak{f}(E)}}\Big).$$

For a proof see e.g. [IK, 5.2].

The second principle is of the same type, but applies to the logarithmic derivative of the L-function instead. It is (also misleadingly) called the "explicit formula". To state one of its variants, let f be again a modular form and define $\Lambda_f(n)$ by the Dirichlet series expansion

$$-\frac{L'}{L}(f,s) = \sum_{n \geqslant 1} \Lambda_f(n) n^{-s}$$

for $\sigma > 3/2$, so that Λ_f is supported on prime powers and

$$\Lambda_f(p^k) = (\alpha_p^k + \beta_p^k)(\log p)$$

where $\alpha_p\beta_p = p$ and $\alpha_p + \beta_p = \lambda_f(p)$ (at least for $(p,q) = 1$). In particular note that for $(p,q) = 1$ we have

$$\Lambda_f(p) = a_E(p)(\log p), \quad \Lambda_f(p^2) = (a_E(p^2) - 2p)(\log p). \tag{30}$$

Proposition 2.11. *Let f be a primitive cusp form of weight 2 and conductor q with Fourier coefficients $\lambda_f(n)$, and let η be a sufficiently smooth function on $]0,+\infty[$ with compact support such that $\eta(x^{-1})=\eta(x)$. We have*

$$2\sum_{n\geqslant 1}\frac{\Lambda_f(n)}{n}\eta(n)=\eta(1)\log q-\sum_{\rho}\hat{\eta}(\rho-1)+\frac{1}{2i\pi}\int_{(1/2)}\Big(\frac{\Gamma'}{\Gamma}(s)+\frac{\Gamma'}{\Gamma}(1-s)\Big)\hat{\eta}(s)ds$$

where ρ runs over zeros of $L(f,s)$ and $\hat{\eta}$ is the Mellin transform of η. In particular if $E/\mathbf{Q}$ is an elliptic curve we have

$$2\sum_{n\geqslant 1}\frac{\Lambda_E(n)}{n}\eta(n)=\eta(1)\log \mathfrak{f}(E)-\mathrm{ord}(E)\hat{\eta}(0)-\sum_{\rho\neq 1}\hat{\eta}(\rho-1)+\frac{1}{2i\pi}\int_{(1/2)}\Big(\frac{\Gamma'}{\Gamma}(s)+\frac{\Gamma'}{\Gamma}(1-s)\Big)\hat{\eta}(s)ds.$$

For a proof, see e.g. [IK, 5.5]; note that in the second formula we have isolated the (possible) zero at $s=1$ from the others.

Before going further, here are a few remarks on these two formulas. In the first one, a standard choice of the parameter X is $X=1$, in which case the effective length of summation is essentially $n\leqslant\sqrt{\mathfrak{f}(E)}$ for both sums, after which the tails are very small. However, taking $X=\sqrt{\mathfrak{f}(E)}$ is also useful because, although it lengthens the first sum to $n\leqslant\mathfrak{f}(E)$ – which can make it unmanageable –, it gets rid of the second sum involving the root number. The latter can be very much of a problem. There are similar formulas for all moments $L^{(k)}(E)^m$ of all derivatives, with $a_E(n)$ replaced by the coefficients of the corresponding Dirichlet series, and the "length" becoming $\mathfrak{f}(E)^{m/2}$.

The second formula does not involve the root number, and partly for this reason it has been the most commonly used. But because it requires a certain control of the zeros of $L(E,s)$, in applications it has usually been used on the assumption that GRH holds. In this case, we have $\mathrm{Re}(\rho-1)=0$ and it is easy to choose a simple test function η for which $\hat{\eta}(s)\geqslant 0$ for all s with $\mathrm{Re}(s)=0$. Because of the sign, this makes it suitable for *upper bounds* for $\mathrm{ord}(E)$, but not for lower bounds. As we'll see, in applications the support of η is such that n appears up to $\mathfrak{f}(E)^{\kappa}$ for some $\kappa>0$ (a small κ can still be useful).

2.6. **The Delta-symbol for a family.** In any case, for both formulas, if one wishes to use them for families, performing the average over $E\in\mathcal{E}$ yields expressions for $A_{\mathcal{E}}(T,L)$ or $A_{\mathcal{E}}(T,\mathrm{ord})$ in terms of the following fundamental averages, called the Delta-symbols, or twisted Delta-symbols, of the family:

$$\Delta_T(n,m)=A_{\mathcal{E}}(T,a_E(n)a_E(m))=\sum_{E\in\mathcal{E}(T)}a_E(n)a_E(m), \tag{31}$$

$$\Delta_T^w(n,m)=A_{\mathcal{E}}(T,w(E)a_E(n)a_E(m))=\sum_{E\in\mathcal{E}(T)}w(E)a_E(n)a_E(m). \tag{32}$$

Precisely, for $A_{\mathcal{E}}(T,L)$, one gets $\Delta_T(n,1)$ and $\Delta_T^w(n,1)$, and for $A_{\mathcal{E}}(T,\mathrm{ord})$, one gets combinations of $\Delta_T(p^k,1)$. The second parameter m is potentially significant if one could involve a mollifier (as has been done with $J_0(q)$); it can be dispensed

with using the formula

$$a_E(n)a_E(m) = \sum_{\substack{d|(n,m)\\(d,\mathfrak{f}(E))=1}} d a_E\Big(\frac{nm}{d^2}\Big),$$

but this is not necessarily the best arrangement.

The reason of the terminology is the heuristic that, for $n = m$, there is no cancellation in the sum and $\Delta_T(n,m)$ should be large. In fact, recalling the Hasse bound $|a_E(n)| \leqslant d(n)\sqrt{n}$ and $w(E) = \pm 1$, we see that

$$|\Delta_T(n,m)| \leqslant \tau(n)\tau(m)\sqrt{nm}A_{\mathcal{E}}(T), \tag{33}$$

$$|\Delta_T^w(n,m)| \leqslant \tau(n)\tau(m)\sqrt{nm}A_{\mathcal{E}}(T), \tag{34}$$

and one would expect that $\Delta_T(n,n)$ is roughly of the order of magnitude of the bound above, from the Sato-Tate conjecture. On the other hand, if $n \neq m$ one can expect random sign changes in $a_E(n)a_E(m)$, $E \in \mathcal{E}$, that make the sum smaller than this trivial bound. This leads to expect some kind of approximate orthogonality, at least in certain ranges of n and m. Similar effects are easy to see for the analogue case of Dirichlet characters modulo q, where we have

$$\sum_{\chi \,(\mathrm{mod}\, q)} \chi(n)\overline{\chi(m)} = \varphi(q)\delta_q(n,m),$$

where $\delta_q(n,m) = 1$ if $n \equiv m \,(\mathrm{mod}\, q)$ and $(nm,q) = 1$, and $\delta_q(n,m) = 0$ otherwise, in particular if $n \neq m$ and $n, m \leqslant q$. Similarly, but not so easily, for the variety $J_0(q)$ one has the following easy consequence of the Petersson formula:

$$\sum_f \omega_f \lambda_f(n)\lambda_f(m) = \sqrt{mn}\delta(m,n) + O(mn(m,n,q)q^{-3/2})$$

(see e.g. [IK, 14]), where f runs over an orthogonal basis of the space of weight 2 cusp forms of level q, and $\omega_f^{-1} = 4\pi\langle f, f\rangle$, the Petersson norm of f, which is of size about q. Alternately, one can use the Selberg Trace Formula for the Delta symbol in this case (see [V]), with a slightly weaker estimate on the error term.

The simplest case for families of elliptic curves is that of the family $\mathcal{E}_E$ of quadratic twists E_d (with $(d, \mathfrak{f}(E)) = 1$) of a given E. In this case $a_{E_d}(n) = (\frac{d}{n})a_E(n)$ and $w(E_d)$ is given by (24) so

$$\Delta_T(n,m) = a_E(n)a_E(m) \sum_{|d|\leqslant T}^{\flat} \Big(\frac{d}{nm}\Big),$$

$$\Delta_T^w(n,m) = w(E)a_E(n)a_E(m) \sum_{|d|\leqslant T}^{\flat} \Big(\frac{-d\,\mathfrak{f}(E)}{nm}\Big)$$

where $\sum^{\flat}$ is the sum over the relevant d. Since $d \mapsto (\frac{d}{nm})$ is a Dirichlet character modulo nm which is trivial if and only if nm is a square, it is not hard to derive better individual bounds than (33), (34). However (partly because of the restrictions on d) to prove an asymptotic formula for, say, $A_{\mathcal{E}_E}(T, L')$, it is necessary to keep the Delta symbol in non-estimated form and perform some transformations in the ensuing sum over n. See [I1] for the details, which yield for instance

$$A_{\mathcal{E}_E}(T, L') = \alpha_1 A_{\mathcal{E}_E}(T)(\log T) + \alpha_2 A_{\mathcal{E}_E}(T) + O(T^{27/28})$$

as $T \to +\infty$, for some constants $\alpha_1 > 0$ and $\alpha_2 \geqslant 0$. This gives the lower bound required in (28).

In this situation, it is unimportant (for analytic purposes) that we are dealing with elliptic curves: all the necessary estimates are in fact valid for arbitrary primitive cusp forms of weight 2.

2.7. **Sketch of proof of Theorem 2.8.** We consider the situation of an algebraic family. In this case one uses the explicit formula for a test function of the type $\eta_\lambda(x) = \eta(x^{\lambda^{-1}})$, the parameter $\lambda \geqslant 1$ allowing to "localize" optimally the sum. The fixed test function η is compactly supported in $[e^{-1}, e]$, and such that $\eta(it) \geqslant 0$ for all $t \in \mathbf{R}$, so the sum over zeros is $\geqslant 0$ under GRH. (For instance, the triangle function $\eta(x) = \max(1 - |\log x|, 0)$ is commonly used.) Since $\hat{\eta}_\lambda(s) = \lambda\hat{\eta}(\lambda s)$, by positivity one derives from Proposition 2.11 that

$$\lambda \operatorname{ord}(E)\hat{\eta}(0) \leqslant \eta(1)\log \mathfrak{f}(E) - 2\sum_n \frac{\Lambda_E(n)}{n}\eta(n^{\lambda^{-1}}) + (\text{arch}),$$

where (arch) designates the archimedean contribution of the Gamma function, which is easily handled because it is independent of t. Hence

$$\lambda\hat{\eta}(0)A_{\mathcal{E}}(T, \operatorname{ord}) \leqslant \eta(1)A_{\mathcal{E}}(T, \mathfrak{f}) - 2\sum_n \eta(n^{\lambda^{-1}})A_{\mathcal{E}}\Big(T, \frac{\Lambda_E(n)}{n}\Big) + O(A_{\mathcal{E}}(T)) \tag{35}$$

for $T \geqslant 2$, the implied constant depending on the family. The average of the conductor is easily handled by (18) which holds with $A = \deg \Delta$, where Δ is the discriminant polynomial, or with $A = \deg N_{\mathcal{E}}$ where $N_{\mathcal{E}}$ is the conductor polynomial (29):

$$A_{\mathcal{E}}(T, \mathfrak{f}) \leqslant (\deg N_{\mathcal{E}})A_{\mathcal{E}}(T)(\log T)(1 + o(1))$$

as $T \to +\infty$

The last sum can be expressed in terms of the Delta symbols for $n = p^k$. Those are given by

$$\Delta_T(p^k, 1) = \sum_{|t| \leqslant T} a_{E_t}(p^k).$$

The individual Hasse bound is sufficient to treat all $k \geqslant 3$ to show that for $T \geqslant 2$ we have

$$\sum_{\substack{n = p^k \\ k \geqslant 3}} \Lambda_E(n) n^{-1} \eta(n^{\lambda^{-1}}) \ll A_{\mathcal{E}}(T).$$

For the remaining values of k, the main observation is that $t \mapsto a_{E_t}(p^k)$ is periodic of period p, except for some innocuous problems when $p \mid \Delta(t)$. Thus one is led to study the local average

$$\mathcal{A}_{\mathcal{E}}^k(p) = \frac{1}{p}\sum_{\substack{t \,(\mathrm{mod}\, p) \\ \Delta(t) \neq 0}} a_{E_t}(p^k), \tag{36}$$

and apart from boundary terms and those t where $p \mid \Delta(t)$ we have

$$\Delta_T(p^k, 1) \simeq \mathcal{A}_{\mathcal{E}}^k(p)A_{\mathcal{E}}(T). \tag{37}$$

The treatments of Fouvry-Pomykala, Michel and Silverman diverge at this point. Before going further, we remark that this shows that (except if $\mathcal{A}_{\mathcal{E}}^k(p) = 0$) there is in fact no cancellation in $\Delta_T(p^k, 1)$ as T grows, for fixed p and k. (Contrast with the Petersson formula). So improving the results below require a non-trivial treatment of the sum over p afterwards, which is quite difficult (Young [Yo1], for instance, did succeed in exploiting this sum over p).

Chronologically, Fouvry and Pomykala used the trivial bound for $k = 2$, with a contribution of size about $\lambda A_{\mathcal{E}}(T)(1 + o(1))$ to (35). For $k = 1$ they use the character sum expression (8) for $a_E(p)$ (if E has good reduction at $p \geqslant 5$)

$$a_E(p) = -\sum_{x \,(\mathrm{mod}\, p)} \Big(\frac{f_t(x)}{p}\Big)$$

if E_t is put in Weierstrass form

$$E_t \,:\, y^2 = x^3 - 27c_4(t)x - 54c_6(t) = f_t(x),$$

yielding an expression for $\mathcal{A}_{\mathcal{E}}(p) = \mathcal{A}^1_{\mathcal{E}}(p)$ as a two-variable character sum

$$\mathcal{A}_{\mathcal{E}}(p) = -\frac{1}{p}\sum_{x,t}\sum \Big(\frac{x^3 - 27c_4(t)x - 54c_6(t)}{p}\Big).$$

One expects, at least generically, square-root cancellation in this sum, i.e. that this expression should be bounded. Fouvry and Pomykala prove this under some genericity assumptions by invoking general bounds of Adolphson and Sperber.

On the other hand, Michel sees the estimation of $\mathcal{A}_{\mathcal{E}}(p)$ as a problem about a one-variable sum of local traces of Frobenius acting on the ℓ-adic sheaf $\mathcal{F}$ of rank 2 whose local traces at a point of $U = \{t \in \mathbf{Z}/p\mathbf{Z} \mid \Delta(t) \neq 0\}$ are $a_{E_t}(p)$, namely

$$\mathcal{F} = R_1\pi_!\mathbf{Q}_\ell$$

where $\pi : \mathcal{E} \to \mathbf{P}^1$ is the morphism defining the algebraic surface $\mathcal{E}$ (modulo p). Estimating $\mathcal{A}_{\mathcal{E}}(p)$ reduces to the computation of the cohomology groups of $\mathcal{F}$, and Michel treats this with the same kind of arguments that Katz [K] used to prove (for instance) the vertical Sato-Tate distribution for Kloosterman sums. The only assumption on $\mathcal{E}$ that remains necessary (in order that the required monodromy group be as large as possible) is that the family be non-constant, i.e. the polynomial $j(t)$ is not constant (modulo p), which excludes only finitely many p if $j(t) \in \mathbf{Z}[t]$ is not constant, and the estimate obtained is:

Proposition 2.12. *Let $\mathcal{E}$ be a non-constant algebraic family of elliptic curves modulo p. We have*

$$|\mathcal{A}^k_{\mathcal{E}}(p)| \leqslant (k+1)(\deg \Delta(t) - 1)p^{(k-1)/2}.$$

and if $k = 1$ one can replace $2(\deg \Delta(t) - 1)$ by $\deg N_{\mathcal{E}}$.

Finally, Silverman handles the case $k = 2$ as Michel did, except that he shows that the bound he obtained remains valid for a constant family (using Rankin-Selberg convolution). For $k = 1$, he does not use character sums to handle $\mathcal{A}_{\mathcal{E}}(p)$ but instead a formula conjectured by Nagao and proved by Rosen and himself [RoS], namely

$$\sum_{p \leqslant x} \mathcal{A}_{\mathcal{E}}(p)(\log p) \sim -\operatorname{rank} \mathcal{E}(\mathbf{Q}(t))x,$$

as $x \to +\infty$, under the assumption that the Tate Conjecture holds for $\mathcal{E}/\mathbf{Q}$, i.e. that the order of the pole at $s = 2$ (on the edge of the region of absolute convergence) of the L-function attached to $H^2(\mathcal{E}/\bar{\mathbf{Q}}, \mathbf{Q}_\ell)$ is equal to the rank of the Néron-Severi group of $\mathcal{E}/\mathbf{Q}$. Thus, summing the contribution of $n = p$ in (35) yields a contribution which is

$$-\frac{\lambda}{2}(1 + o(1))(\operatorname{rank} \mathcal{E}(\mathbf{Q}(t)))A_{\mathcal{E}}(T)$$

by summation by parts (using the fact that $p \leqslant e^\lambda$).

The outcome of all this (and a correct treatment of boundary terms) is the estimate

$$\lambda\hat{\eta}(0)A_{\mathcal{E}}(T,\mathrm{ord}) \leqslant (1+o(1))A_{\mathcal{E}}(T)\Big\{(\deg N_{\mathcal{E}})(\log T) + \frac{\lambda}{2}(\mathrm{rank}\,\mathcal{E}(\mathbf{Q}(t))) + \frac{\lambda}{2} + O(1) + O(\lambda e^{\lambda})\Big\}.$$

Taking λ slightly smaller than $\log T$ gives the desired average bound.

An interesting point is that the periodicity of $t \mapsto a_{E_t}(p)$ means that in fact the family can be restricted to certain parameters t as long as they are very well-distributed in arithmetic progressions. For instance, one checks easily that using

$$\pi(x;q,a) = \frac{\mathrm{li}(x)}{\varphi(q)} + O(x^{1/2}(\log x))$$

which follows from GRH for Dirichlet L-functions, one can deduce that the average rank is still bounded for the family $\mathcal{E}_p$ which restricts t to prime values:

$$\mathcal{E}_p(T) = \{E_t \mid 1 \leqslant t \leqslant T \text{ and } t \text{ is prime}\}.$$

There are (at least) two interesting problems arising out of this proof. The first is to remove the dependence on GRH; this has been done for quadratic twists, but at the cost of getting only (27) instead of boundedness of the average rank. No other instance is known. (Even Brumer's family of curves indexed by height, which seems the most accessible, remains out of reach; see however the recent work of Young [Yo2] concerning the proportion of non-vanishing). It should be noted that in the case of $J_0(q)$, this removal requires much more delicate analysis in the form of density theorems for the possible zeros of L-functions close to the critical line, see [KM2].

The other possibility is to improve on the average rank. The argument shows that the only possible way to do so is to treat non-trivially the sum over the zeros in the explicit formula to get some cancellation with the other terms (especially with the $\Lambda_E(p^2)$ contributions). This is closely related with the issues surrounding the predictions of random matrix theory discussed previously, and has been done quite successfully by Iwaniec, Luo and Sarnak [ILS] for $J_0(q)$ and other families of automorphic L-functions. Some results for algebraic families are due to M. Rubinstein [R2], S. Miller [Mil1] and M. Young [Yo1], confirming the 1-level and 2-level densities (the latter does distinguish between various symmetry groups).

2.8. **Some discussion of numerical evidence.** Due to the large choice of well-documented and well-implemented algorithms for computing with elliptic curves[7], particularly over $\mathbf{Q}$, many of the conjectures concerning them can be put to the test, and in particular those concerning the rank. This has led to the controversial problem of "excess rank", as a number of experiments with seemingly innocuous families revealed a fairly large proportion of curves with rank $\geqslant 2$ (see e.g. [KZ], [Fe] or [B, 1st paragraph]). Since an occurrence of excess rank for an infinite family (not chosen in a special way to have large rank) would put into question the general Katz-Sarnak philosophy, there is a certain agreement that the data available simply reflects a problem with the size of the sample.

The most convincing theoretical argument against excess rank maybe follows by doing the numerical experiments with the 2-rank of the Selmer group for the congruence number curves, and comparing with the results of Heath-Brown, since those are unconditional. Of course, the Selmer group could have a very different behavior, but as explained in [H2, p. 336], small tests tend to reveal an "excess

[7] For instance with the Pari/GP system [Pari].

rank" in this case too, which has to disappear in the long run... Moreover, discussing his proof, Heath-Brown indicates one possible explanation for a very slow convergence towards the limiting distribution: in his arguments, the k-th moment of $s_2(E_d)$ must be averaged over numbers having at least 16^k prime factors before it gets close to the asymptotic value!

Another very simple type of experiments which has not been widely performed is that of computing the Delta symbols for some families of elliptic curves. This is much faster, of course, than computing the rank exactly, but it can in theory be quite useful if one compares the results for two families, one of which is – if possible – well-understood. As indicated in Section 2.5, for a number of analytical arguments it is the quasi-orthogonality of $\Delta_T(m,n)$ which is at the heart of a successful average study of special values of L-functions. Even if one family is inaccessible, a behavior of the Delta symbol similar to that of another would be good indication that the rank might also behave in a similar way.

With this in mind, we performed the computation for the most mysterious family $\mathcal{E}_c$, that of elliptic curves indexed by the conductor. For this we used Cremona's table, which currently lists all 845960 elliptic curves over $\mathbf{Q}$ with conductor $< T = 130000$, up to isomorphism. (The table also contains the rank, for which the distribution is: rank 0, 340655 curves, rank 1, 427012 curves, rank 2, 77357 curves, rank 3, 936 curves, and no rank $\geqslant 4$). We limited the computation to $\Delta(p,1)$ where p is a prime $p \leqslant \sqrt{T}(\log T) < 4246$, since according to the approximate functional equation those are sufficient to recover $L(E,1)$, and we also computing the twisted Delta-symbols $\Delta_T^w(p,1)$ as well as the sum $\frac{1}{2}(\Delta_T(p,1)+\Delta_T^w(p,1))$.

The following graphs show for instance the Delta symbols for $p=61$ and $p=797$; the horizontal axis is the number of curves counted up to x, i.e. $A_{\mathcal{E}_c}(x)$, $x \leqslant T$.

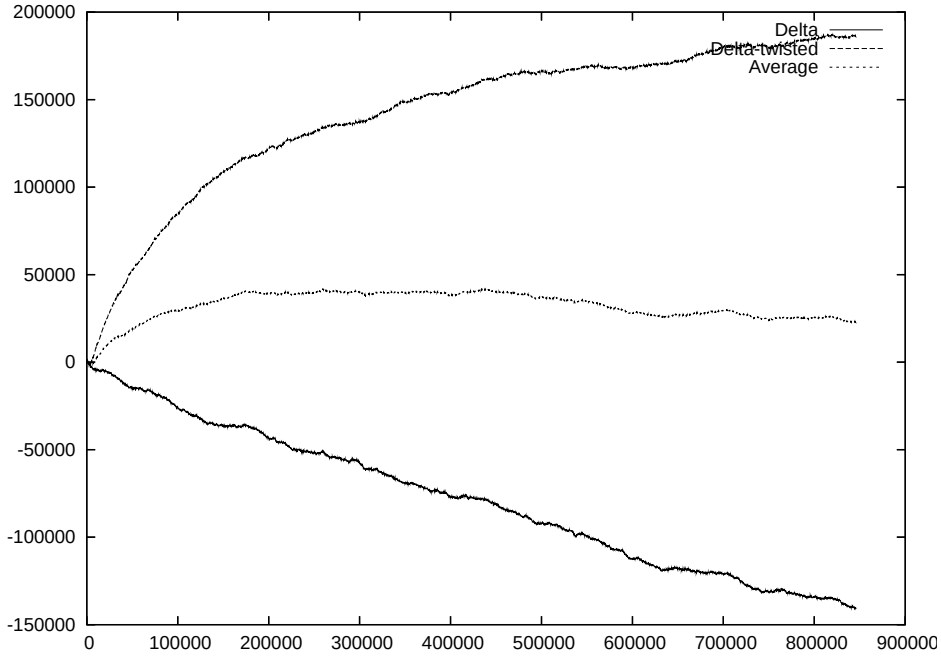

FIGURE 1. Delta symbols for $p=61$

Notice that, as far as $\Delta_T(p,1)$ is concerned, in the first case ($p=61$) one has a curve very close to linear, which suggests strongly an effect of periodicity like the one

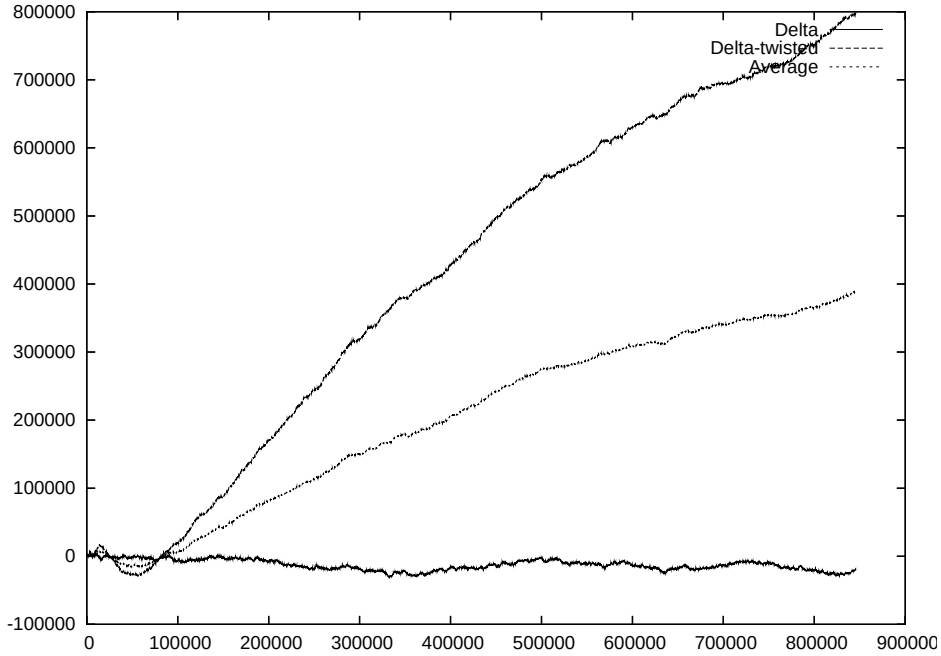

FIGURE 2. Delta symbols for $p = 797$

that does happen for the Delta symbol of an algebraic family of elliptic curves. This might seem natural and taken to be the reflection of an equidistribution statement for the reductions of curves $E \in \mathcal{E}_c(T)$ modulo p as $T \to +\infty$, among the elliptic curves modulo p, except that the natural linear factor to expect for $\Delta_T(p, 1)$ would be (compare (36) and (37))

$$\mathcal{A}_c(p) = \frac{1}{p} \sum_{E \,(\mathrm{mod}\, p)} a_E(p) = 0,$$

where the sum is over all elliptic curves modulo p, so quadratic twists with a_p, $-a_p$ cancel out. This does not fit the data available at all!

On the other hand, for $p = 797$, the Delta symbol behaves much more randomly. It should be mentioned that those are the two most common aspects of the graphs for the primes considered, with the first case being most common, and maybe more significantly, with the "linear" curves having negative slopes. Note this means a tendency to have $a_E(p) < 0$, which increases the number of points modulo p, something which is often an indication of a larger rank.

In both cases, however (again this is typical) the introduction of the root number changes the picture completely: in the first case, there seems to be a correlation between $a_E(p)$ negative and $w(E) = -1$ (not too surprising in fact, by the above remark), so that the twisted Delta symbol seems to be increasing (the curve does not look quite as linear). For $p = 797$, the twisted symbol first seems to oscillate, but then has a marked tendency to increase.

All in all, these graphs look very mysterious to me. I think however that the Delta symbol deserves better scrutiny, both numerical and theoretical.

REFERENCES

[Ba] A. Baker: *Transcendental number theory*, Cambridge Math. Library, Cambridge Univ. Press (1975).

[B] A. Brumer: *The average rank of elliptic curves, I*, Invent. math. 109 (1992), 445–472.

[CFKRS] B. Conrey, D. Farmer, J.P. Keating, M. Rubinstein and N. Snaith: *Integral moments of L-functions*, Proc. Lond. Math. Soc., 91 (2005), 33–104.

[CKRS] B. Conrey, J.P. Keating, M. Rubinstein and N. Snaith: *On the frequency of vanishing of quadratic twists of modular L-functions*, in Number theory for the millennium, I (Urbana, IL, 2000), 301–315, A K Peters (2002).

[DFK] C. David, J. Fearnley and H. Kisilevsky: *Vanishing of L-functions of elliptic curves over number fields*, in this volume.

[D1] C. Delaunay: *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbf{Q}$, Exper. Math. 10 (2001), 191–196.

[D2] C. Delaunay: *Moments of the orders of Tate-Shafarevitch groups*, International J. of Number Theory, Vol. 1, No. 2 (2005) 243–264.

[D3] C. Delaunay: *Heuristics on class groups and on Tate-Shafarevich groups*, in this volume.

[Fa] D. Farmer: *Modeling families of L-functions*, in this volume.

[Fe] S. Fermigier: *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbf{Q}$, Exper. Math. 5 (1996), 119–130.

[FP] É. Fouvry and J. Pomykala: *Rang des courbes elliptiques et sommes d'exponentielles*, Mh. Math. 116 (1993), 111–125.

[G] D. Goldfeld: *Conjectures on elliptic curves over quadratic fields*, Number Theory (Carbondale 1979), Springer Lecture Notes Math. 751 (1979), 108–118.

[H1] D.R. Heath-Brown: *The size of the Selmer group for the congruent number problem, I*, Invent. math. 111 (1993), 171–195.

[H2] D.R. Heath-Brown: *The size of the Selmer group for the congruent number problem, II*, Invent. math. 118 (1994), 331–370.

[H3] D.R. Heath-Brown: *The average analytic rank of elliptic curves*, Duke Math. J. 122 (2004), no. 3, 591–623.

[H4] D.R. Heath-Brown: *A Note on the 2-Part of* Ш *for the Congruent Number Curves*, in this volume.

[He] H.A. Helfgott: *Root numbers and the parity problem*, PhD thesis, Princeton University (2003).

[I1] H. Iwaniec: *On the order of vanishing of modular L-functions at the critical point*, Sém. Théor. Nombres Bordeaux 2 (1990), 365–376.

[I2] H. Iwaniec: *Topics in classical automorphic forms*, Grad. Studies in Math. 17, A.M.S (1997).

[IK] H. Iwaniec and E. Kowalski: *Analytic Number Theory*, A.M.S Colloquium Publications, vol 53 (2004).

[ILS] H. Iwaniec, W. Luo and P. Sarnak: *Low -lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. 91 (2001), 55–131.

[K] N. Katz: *Gauss sums, Kloosterman sums and monodromy groups*, Princeton Univ. Press (1988).

[KS1] N. Katz and P. Sarnak: *Random matrices, Frobenius eigenvalues, and monodromy*, A.M.S Colloquium Publications, vol. 45 (1999).

[KS2] N. Katz and P. Sarnak: *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. 36 (1999), 1–26.

[K] N. Koblitz: *Introduction to elliptic curves and modular forms*, G.T.M 97.

[KM1] E. Kowalski and P. Michel: *A lower bound for the rank of* $J_0(q)$, Acta Arith. 94 (2000), 303–343.

[KM2] E. Kowalski and P. Michel: *The analytic rank of* $J_0(q)$ *and zeros of automorphic L-functions*, Duke Math. J. 100 (1999), 503–542.

[KMV] E. Kowalski, P. Michel and J. VanderKam: *Non-vanishing of high derivatives of automorphic L-functions at the center of the critical strip*, J. reine angew. Math. 526 (2000), 1–34.

[KZ] G. Kramarz and D. Zagier: *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc., New Ser. 52 (1987), 51–60.

[Ma] B. Mazur: *On the passage from local to global in number theory*, Bull. A.M.S 29 (1993), 14–50.

[M] J-F. Mestre: *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. 58 (1986), 209–232.

[Mi] P. Michel: *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Mh. Math. 120 (1995), 127–136.

[Mil1] S. Miller: 1- *and* 2-*Level Densities for Rational Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, Compositio Math. 140 (2004), 952–992.

[Mil2] S. Miller: *Investigations of zeros near the central point of elliptic curve L-functions*, preprint (2005), `arXiv:math.NT/0508150`

[N] J. Nekovàr: *On the parity of ranks of Selmer groups, II*, C. R. Acad. Sci. Paris Sér. I Math. 332 (2001), 99–104.

[O] A. Odlyzko: *The* 10^{20}*-th zero of the Riemann zeta function and* 70 *million of its neighbors*, ATT Bell Laboratories preprint, 1989.

[On] K. Ono: *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. reine angew. Math. 533 (2001), 81–97.

[Pari] PARI/GP, version `2.2.?`, Bordeaux, 2005, `http://pari.math.u-bordeaux.fr/`.

[PP] A. Perelli and J. Pomykala: *Averages over twisted elliptic L-functions*, Acta Arith. 80 (1997), 149–163.

[RoS] M. Rosen and J. Silverman: *On the rank of an elliptic surface*, Invent. math. 133 (1998), 43–67.

[R1] M. Rubinstein: *Evidence for a spectral interpretation of the zeros of L-functions*, PhD thesis, Princeton University (1998).

[R2] M. Rubinstein: *Low-lying zeros of L-functions and random matrix theory*, Duke Math. J. 109 (2001), 147–181.

[RS] Z. Rudnick and P. Sarnak: *Zeros of principal L-functions and random matrix theory*, Duke Math. J. 81 (1996), 269–322.

[AEC] J. Silverman: *The arithmetic of elliptic curves*, Grad. Texts in Math 106, Springer Verlag (1986).

[S] J. Silverman: *The average rank of an algebraic family of elliptic curves*, J. reine angew. Math. 504 (1998), 227–236.

[Sn] N. Snaith: *Derivatives of random matrix characteristic polynomials with applications to elliptic curves*, preprint (2005), `arXiv:math.NT/0508256`.

[Sw] P. Swinnerton-Dyer: *2-Descent Through the Ages*, in this volume.

[U1] D. Ulmer: *Elliptic curves with large rank over function fields*, Ann. of Math. (2) 155 (2002), 295–315.

[U2] D. Ulmer: *Functions fields and random matrices*, in this volume.

[V] J. VanderKam: *The rank of quotients of* $J_0(N)$, Duke Math. J. 97 (1999), 545–577.

[Yo1] M. Young: *Low-lying zeros of families of elliptic curves*, Journal of the A. M. S., to appear (posted on September 7, 2005, PII S0894-0347(05)00503-5).

[Yo2] M. Young: *On the non-vanishing of elliptic curve L-functions at the central point*, to appear in Proc. London Math. Soc.

[Yo3] M. Young: *Analytic number theory and ranks of elliptic curves*, in this volume.

[Yo4] M. Young: *Moments of the critical values of families of elliptic curves, with applications*, preprint (2005).

[Y1] G. Yu: *Rank* 0 *Quadratic Twists of a Family of Elliptic Curves*, Compositio Mathematica 135 (2003), 331–356.

[Y2] G. Yu: *On the quadratic twists of a family of elliptic curves*, preprint.

Université Bordeaux I - A2X
351, cours de la Libération
33405 Talence Cedex
France

emmanuel.kowalski@math.u-bordeaux1.fr