ELLIPTIC CURVES AND THEIR STATISTICS

Rough notes for my Basic Notions Talk, Feb 28 2012

B. Mazur

Part I. Densities

1. Aggregates

It is curious how *aggregates* rather than *single instances* creep into our subject even when we aren't looking for statistical trouble.

Here is an example. In the Erdös spirit, I'll offer a \$5 prize for anyone who can manage to provide a proof of the fact that

- *every* linear form $aX+b$ with $a, b \in \mathbf{Z}$ relatively prime represents at least one prime number; and yet
- the proof doesn't actually show that it represents *infinitely many* primes.

I think my \$5 is safe, but the point I want to make is that a certain amount of our work is—whether we want it or not—inescapably about "aggregates."

The statement in the first bullet above is true[1], and Dirichlet proved it in 1837 by showing, more precisely, that there is a *positive density* of primes in any arithmetic progression with $g.c.d.(a, b) = 1$.

Specifically,

[1]An analogous statement is conjectured to be true for any polynomial with integer coefficients that satisfies some natural requirements (as would follow from Schinzel's Conjecture).

$$\lim_{X\to\infty} \frac{\#\{p \text{ a prime number of the form } p = \ an+b \le X\}}{\pi(X)} \ = \ \frac{1}{\Phi(a)},$$

where $\pi(X)$ is the total number of primes $\le X$; and $\Phi(a)$ is Euler's Φ-function.

$$\Phi(a) = |(\mathbf{Z}/a\mathbf{Z})^*|.$$

There are a number of existence theorems for specific objects in mathematics that would be interesting enough if we even knew the existence of *one* of those desired objects; and yet our existence proof works by, in fact, guaranteeing large numbers of them—usually positive densities of them!

Dirichlet's Theorem, quoted above, has generalized into one of the most successful and most-often-used techniques for finding prime number with specific properties. Namely: Cebotarev's Theorem[2], which I'll state only for $\mathbf{Q}$, but the analogous theorem is true over any number field:

2. Cebotarev Classes

Recall that if K/Q is a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$ and discriminant Δ, then for every prime number p not dividing Δ (i.e., unramified in the extension $K/\mathbf{Q}$) there is a unique conjugacy class of elements $\mathcal{C}(p) \subset G$ (called the *Frobenius conjugacy class attached to* p) that is defined by reducing mod p an appropriate polynomial equation for a primitive element generating K to get a separable polynomial over $\mathbf{F}_p$, and studying the Galois extension of $\mathbf{F}_p$ that it generates[3]. From this conjugacy class $\mathcal{C}(p)$, for example, you can read off how many primes of K lie above p, and (equivalently) the degree of the field extension of $\mathbf{F}_p$ generated by that polynomial equation.

Now let $\mathcal{C} \subset G$ be a conjugacy class of elements in G, and define

$$\mathcal{P}_{\mathcal{C}}(X) := \text{ unramified primes } p \le X \text{ such that } \mathcal{C}(p) = \mathcal{C}.$$

Put

$$\mathcal{P}_{\mathcal{C}} \ = \ \cup_X \mathcal{P}_{\mathcal{C}}(X).$$

[2]proved in his Phd thesis in 1922

[3]connecting it appropriately to the initial Galois extension K/Q

By a **Cebotarev class of primes defined by** $K/\mathbf{Q}$ let us mean a union of these $\mathcal{P}_{\mathcal{C}}$'s, give or take a finite set. By a **Cebotarev class of primes** let us mean such a set of primes defined by some finite Galois extension.

The most famous kind of "Cebotarev classes" are arithmetic progression $an + b$ with (a, b) relatively prime. These are defined by the cyclotomic field extensions $K/\mathbf{Q} = \mathbf{Q}(e^{2\pi i/a})/\mathbf{Q}$. The Galois group, $G = \mathrm{Gal}(K/\mathbf{Q})$ is canonically isomorphic to $(\mathbf{Z}/a\mathbf{Z})^*$, and Dirichlet's theorem is a special case of the general result that tells us that Cebotarev classes have computable densities; specifically:

Theorem 2.1. (Cebotarev) Let $\mathcal{C} \subset G$ be a conjugacy class of elements in $G = \mathrm{Gal}(K/\mathbf{Q})$. Then

$$\lim_{X\to\infty} \frac{\#\{\mathcal{P}_{\mathcal{C}}(X)\}}{\pi(X)} \quad = \quad \frac{|\mathcal{C}|}{|G|}.$$

So for $K = \mathbf{Q}(e^{2\pi i/a})$ the Galois group G is abelian and in fact of order $\Phi(a)$, so the densities are given by $1/\Phi(a)$ as described above.

Any "good" error term, by the way, giving the rate of this convergence seems to depends on GRH; if you want "unconditional error terms," they're not all that good. More about that later.

Cebotarev classes will enter—in a big way—into the statistical study of the arithmetic of elliptic curves, but also... some less familiar classes will be part of our story as well.

3. Spin Classes

Joint work with J. Friedlander, H. Iwaniec, and K. Rubin: see our paper "The spin of prime ideals" on ArXiv.

I'll try to explain this notion by an example. Let

$$K := \mathbf{Q}(e^{2\pi i/7} + e^{-2\pi i/7}) = \mathbf{Q}(\cos 2\pi i/7),$$

i.e., K is the maximal total real subfield in the cyclotomic field obtained by adjoining a primitive 7-th root of unity to $\mathbf{Q}$. The field extension $K/\mathbf{Q}$ is the unique cyclic extension of $\mathbf{Q}$ of degree 3 ramified only at the prime 7. The primes p congruent to ± 1 mod 7 split (into the product of three primes in K).

The further basic facts about $K/\mathbf{Q}$ are these:

- K has class number 1.
- There are units in (the ring of integers of) K with arbitrary (i.e., all eight possible) signs for the three real embeddings of K.

It follows from these facts that the totally positive units in K are squares, and also that (modulo squares) there is a unique totally positive generator of any [nonzero] ideal in $\mathcal{O}_K$. Fix a generator $\sigma \in G := \mathrm{Gal}(K/\mathbf{Q})$.

Definition 3.1. By the **spin** of a prime ideal P in $\mathcal{O}_K$ we mean the "Legendre symbol"

$$spin(\sigma; P) := \left(\frac{\pi}{P^\sigma}\right).$$

Here $\pi \in P$ is a choice of totally positive generator of P. The symbol is defined to be zero if $P^\sigma = P$, and is ± 1 depending on whether π is or is not a square modulo P^σ.

Spin, then, is a kind of incestuous quadratic residue.

Since totally positive elements are stable under Galois action we have:

$$spin(\sigma; P) = \left(\frac{\pi}{P^\sigma}\right) = \left(\frac{\pi^\gamma}{(P^\sigma)^\gamma}\right) = \left(\frac{\pi^\gamma}{P^{\gamma\sigma}}\right) = spin(\sigma; P^\gamma)$$

so we can define the *spin* of any rational prime p to be:

$$spin(K/\mathbf{Q}, \sigma; p) := spin(\sigma; P)$$

for any prime P of K lying above p. Of course, this is uninteresting (i.e., 0) unless p splits completely in K; i.e., $p \equiv \pm 1 \bmod 7$.

An exercise is to see that quadratic reciprocity gives us a relation between $spin(K/\mathbf{Q}, \sigma; p)$ and $spin(K/\mathbf{Q}, \sigma^{-1}; p)$ (the product is a product of local Hilbert symbols at places dividing 2).

We (i.e., John Friedlander, Henryk Iwaniec, Karl Rubin and I) prove a general theorem about cubic cyclic fields (including all those satisfying the above two bullets[4]) which for our example K gives us:

[4]We don't need class number 1, though: the simplest modification that preserves the statement is to restrict to primes p that split into principal prime ideals, or ideals that are of odd order in the ideal class group of K.

Theorem 3.2. For $a \equiv \pm 1 \mod 7$ we have

$$\sum_{p \leq X;\ p \equiv a \mod 7} spin(K/\mathbf{Q}, \sigma; p) << X^{1-\nu+\epsilon}$$

Here $\nu = \frac{1}{10{,}656}$ (independent of the cubic cyclic field K satisfying the bullets above) and any $\epsilon > 0$; the implied constants depend on K and ϵ.

Note that this means that the classes

$$\mathcal{P}^{\pm}(a) := \{\text{primes } p \equiv a \mod 7 \mid spin(K/\mathbf{Q}, \sigma; p) = \pm 1\}$$

occur with equal density. Call these subsets of primes $\mathcal{P}^{\pm}(a)$ **spin classes**.

Since we have such a good convergence rate (i.e., ν is positive!) and since our method is surely *not* giving zero-free strips within the critical strip for L-functions, we are morally (but not logically) certain that $\mathcal{P}^{\pm}$ are *not* Cebotarev classes! In any event,

Conjecture 3.3. Spin classes are not Cebotarev classes.

Regarding Cebotarev classes, one has a recent result of Hershy Kisilevsky and Mike Rubinstein guaranteeing that certain classes are not Cebotarev:

Theorem 3.4. (Kisilevsky, Rubinstein) Let $\mathcal{P}$ be a class of primes and $r \in \mathbf{Q}$, with $0 \leq r \leq 1$. Then $\mathcal{P}$ is *not* a Cebotarev class of density r if either

- $\mathcal{P}(X) - r \cdot \pi(X) << \sqrt{X}/\log X$, or
- $\mathcal{P}(X) - r \cdot Li(X) << \sqrt{X}/\log X$.

Here, as usual,

$$\mathcal{P}(X) := \{p \in \mathcal{P} \mid p \leq X\}.$$

Our method for the proof of Theorem 3.2 uses Burgess's bounds giving estimates for incomplete sums of characters. Discuss.

Conjecture 3.5. Let $n \geq 3$, $Q \geq 3$, $N \leq Q^{1/n}$. Then for any real nontrivial Dirichlet character χ of modulus $q \leq Q$ we have

$$\sum_{M < a \leq N} \chi(a) << Q^{\frac{1-\delta}{n}+\epsilon}$$

with some fixed $\delta = \delta(n) > 0$ and any $\epsilon > 0$, the implied constant depending (only) on ϵ and n.

Burgess proves this for $n = 3$; and this is what we use. We have good use for any further progress made with the above conjecture, so we urge people to take a look at it.

We have been discussing densities of *sets of prime numbers* and there is no difficult ordering prime numbers (by size, of course)[5]. But when we compute statistic of other mathematical objects, there may be some question as to what is the "natural way to order them." So, since this is a basic notions seminar about density, it is reasonable to devote a digression to this issue, and ask:

4. What do we mean by density?

There are sophisticated notions of density, but for this hour when we talk about densities, we will have fixed some specific (infinite) collection of objects $\mathcal{U}$, together with a choice of *size function* $s : \mathcal{U} \to \mathbf{R}_{\geq 0}$, where a size function means that for every $X \in \mathbf{R}_{\geq 0}$, the number of objects in $\mathcal{O}$ of size less than or equal to X is finite. We'll say that some property P occurs with density r in $\mathcal{U}$ if:

$$\lim_{X \to \infty} \frac{\#\{u \in \mathcal{U} \mid u \text{ has property } P \text{ and } s(u) \leq X\}}{\#\{u \in \mathcal{U} \mid s(u) \leq X\}} = r.$$

Now if you are estimating quantities of prime numbers, there is not much choice of the size function, but often for other arithmetic objects one has multiple choices, with density results that change with the choice. For example:

5. The case of Quartic Number Fields

One must be careful when choosing the coefficients of a fourth degree polynomial, if you want a root of that polynomial to generate anything other than a field whose Galois group is other than S_4. Hilbert's irreducibility theorem provides corroboration of this with a proof that if you rank algebraic numbers of degree 4 by the size of the coefficients of their minimal polynomial (monic, over $\mathbf{Q}$) then 100% of them have Galois group S_4. But let us count quartic fields (rather than algebraic numbers that generate them) nested by the size (absolute value) of their discriminant. Dick's Basic Notions talk two weeks ago mentioned the classical theorem of Hermite that there are only a finite number of different algebraic number fields with absolute value of discriminant

[5]Although, even here, there is the alternate notion of "Dirichlet density."

$\leq X$, so it makes sense to compute densities with respect to this size function. Counting field extensions of a given field with a fixed Galois group (i.e., Galois group of their Galois closure) has been the subject of a number of precise conjectures (initially: [**?**], and then successively refined in [**?**, **?**]). Barghava's remarkable paper [**?**], which is further evidence for these conjectures, proves that when you count quartic fields, nested by discriminant, you do not get 100% of them having Galois group S_4.

Bhargava thinks of the problem of counting quartic fields as a problem purely in the Geometry of Numbers, and *proves* the following theorem:

Theorem 5.1 (Bhargava)**.** When ordered by absolute discriminant, *a positive proporition* (approximately 0.09356) of quartic fields have associated Galois group D_4. The remaining approximately 0.90644 of quartic fields have Galois group S_4.

All this was an introduction meant to lead to elliptic curves and to hint that we will be paying special attention their arithmetic statistics. And to point out that when one asks questions like:

> *What is the probability that a cubic plane curve with rational coefficients has infinitely many rational points?*

one should be clear about how one is ordering this infinite collection.

Part II. Elliptic curve statistics

6. Elliptic curves

An **elliptic curve** E over a field K is a curve of genus one *with a chosen K-rational point, called the "origin"*. It is a theorem (essentially a corollary of the Riemann-Roch theorem) that allows you to represent any elliptic curve over K as a cubic plane curve (over K, of course) with its origin being its only point (even over the algebraic closure $\bar{K}$) at infinity.

This already is a beautiful piece of mathematics and if you haven't seen it before here is a hint about how you get such a representation, each of these statements being directly obtainable from Riemann-Roch

together with the sole fact that the curve we are dealing with has genus one:

- there is only one rational function on E (up to scalars) that has at worst a single pole at one point on E, namely the constant function 1;
- there are two independent rational functions on E having at worst a double pole at the origin and no poles elsewhere: call a choice of the 'new' (i.e., nonconstant) function x;
- there are three independent rational functions on E having at worst a double pole at the origin and no poles elsewhere: call a choice of the 'new' function with an actual triple pole at the origin y;
- *and* there is a linear relation satisfied by the seven functions

$$1, x, y, x^2, xy, x^3, y^2,$$

all these having at worst poles of order six at the origin and none elsewhere.

In particular we get a mapping of our E onto a plane cubic in x and y and this turns out to be an isomorphism).

Even more explicitly, when K is a number field (our main focus here), letting $\mathcal{O}_K$ denote the ring of integers of K, we can choose our functions x and y judiciously so that any such E can be given in an affine plane by a cubic equation

$$(*) \qquad y^2 = x^3 + ax + b$$

for constant $a, b \in \mathcal{O}_K$, with its discriminant, $\Delta(a, b) = -4a^3 - 27b^2$, different from zero (this guarantees that E is a *smooth curve*).

Different pairs (a, b) may give rise to isomorphic elliptic curves; for instance, for any element $u \in \mathcal{O}_K$ setting $Y = u^3 y$ and $X = u^2 x$ gives, after clearing terms in the displayed equation, the new cubic equation

$$Y^2 = X^3 + Ax + B$$

where $(A, B) = (u^4 a, u^6 b)$. Here $\Delta(A, B) = u^{12}\Delta(a, b)$.

It is natural then to represent an elliptic curve E by such an affine model **(*)** with a and b *not divisible* by u^4 and u^6 respectively, for any nonunit $u \in \mathcal{O}_K$; equivalently, with minimal absolute value of the norm of its discriminant, among all affine models **(*)** representing E.

For number theory it is quite a good thing that we can represent elliptic curves over a number field K, i.e., *curves of genus one over* K

having a K-rational point, in such a clean way. This is not it at all the case if you don't require the curve of genus one to have a K-rational point: it may well be that the only representation of such a curve that is rational over the field K in question is as a curve of very high degree in a projective space (and therefore any projection of such a curve to the plane will represent it only birationally as a curve of high degree with a large singularity locus. This issue will be what is behind the deep questions having to do with what I'll be calling the *companions* to elliptic curves—later in this lecture.

7. The statistical questions, for three kinds of families of elliptic curves over a given number field K

These are the families:

(1) The full family of *all* elliptic curves over a fixed number field.

(2) The family of all quadratic twists of a given elliptic curve over a given number field. That is, fixing $a, b \in \mathcal{O}_K$ and varying $d \in \mathcal{O}_K - \{0\}$ consider the family

$$dy^2 = x^3 + ax + b,$$

or—tucking the d into the left-hand side of the equation, one gets the same elliptic curve from

$$y^2 = x^3 + ad^2x + bd^3.$$

(3) The family of quadratic twists by all characters of prime conductor of a given elliptic curve over $\mathbf{Q}$. That is, fixing $a, b \in \mathbf{Z}$ and varying prime number p consider the family

$$py^2 = x^3 + ax + b.$$

Any family of type (3) is of density zero (for any natural ordering) in the family of type (2) that contains it, and those families of type (2) are of density zero in the all-encompassing family of type (1). So, there is no a priori reason to expect that the statistics of these three "types" to bear any relationship to one another.

This is what we mean by their "statistics":

We are, of course, interested in it arithmetic statistics in the fullest possible sense, related each of the three families that have just been introduced. But today we will be focusing on just these:

- The relative densities of members of each of these families with a given Mordell-Weil rank. E.g., what is the proportion of each family that has finitely many rational points? What is the average rank?

- The relative densities of p-Selmer ranks (we will be discussing this notion below; more specifically, when $p = 2$). E.g., what is the proportion of each family that has trivial 2-Selmer rank? More generally what proportion has 2-Selmer rank $0, 1, 2, 3, \ldots$?

8. Current Guesses, and Theorems, about Mordell-Weil rank density

We are mainly interested, in this talk, about the second bullet at the end of the previous section; namely 2-Selmer rank statistics. But here, by way of digression, is a discussion of what we expect regarding Mordell-Weil ranks, for the family of Type (1) when ordered in the 'natural way,' i.e. by size of absolute value of the norm of the conductor.

We expect that 50% of the family of all elliptic curves over K (ordered by any of the standard size-functions) to have Mordell-Weil rank 0 and 50% to have rank 1. This was first conjectured by Goldfeld in 1979 at least for $K = \mathbf{Q}$ and families of "Type (2)," i.e., for families of quadratic twists over $\mathbf{Q}$. In later years this fit in with the various heuristic viewpoints, e.g., that of Katz-Sarnak, and also, with precise conjectural bounds on rates of convergence for quadratic twist families (Conrey, Keating, Rubinstein, and Snaith) coming from random matrix heuristics; and similar conjectures for all elliptic curves over $\mathbf{Q}$ (Mark Watkins). This has been referred to as the *minimalist conjecture*[6]. In the terminology of the previous section then, the "minimalist conjecture" is that $\rho(K, r) = 1/2$ if $r = 0, 1$ and $\rho(K, r) = 0$ if $r \geq 2$. As hinted in the introduction above, this conjecture is widely believed for the family of Type (1)-and yet it is difficult to get numerical data that firmly support it! The reason for this is in the nature of the error term that is also predicted (coming from random matrix heuristics).

[6]The reason for the term "minimalist" is that—from the point of view of densities, these are the smallest possible densities that are compatible with the expected *parity* of Mordell-Weil ranks: i.e., 0 is the smallest even number and 1 the smallest odd.

The form that this type of error term takes (it will be slightly different in different contexts) if X is the number of instances counted) is

$$aX^b \log^c(X)$$

for specific numbers $b < 1$ (but b close to 1). It is diabolic how the graphs of such functions are so very indistinguishable (to the eye) from the linear function aX, but —of course—from the point of view of densities the difference between $aX^b \log^c(X)$ (for any $b < 1$) and aX is major! This is one of the perils of prediction of qualitative behavior from too little data.

What can be proved?

If the minimalist conjecture is true, then the *average Mordell-Weil rank* when compiled for *all* elliptic curves would be $1/2$. This, therefore, is the goal. In 1992 Armand Brumer showed (by analytic means, and conditional on standard conjectures) that the average rank of elliptic curves over $\mathbf{Q}$ is bounded by 2.3.

The most striking recent results are due to Manjul Bhargava together with his students and co-authors. They have been developing extremely precise methods for counting appropriate orbits of certain arithmetic groups acting on integral points on certain lattices. This approach follows and significantly refines the classical Methods in the Geometry of Numbers (as had pursued by Gauss, Minkowski, Siegel, and others). Manjul Bhargava and Aren Shankar have established (unconditionally) that the "average rank"[7] over $\mathbf{Q}$ is ≤ 0.99. The method here is via what might be called the "geometry of arithmetic orbits in linear representations of reductive groups." Manjul has hopes that these methods might work not only over $\mathbf{Q}$ but also over any fixed number field K.

But for now, over $\mathbf{Q}$ they prove that:

$$\rho(K;0) \geq 0.075$$

and

$$\rho(K;0) + \rho(K;1) \geq 0.80.$$

A striking further result that Bhargava obtained with Wei Ho is that among elliptic curves possessing one point of infinite order, a subset of

[7]The quotation-marks here are meant to signal that the *in*-equalities regarding averages that we will be discussing will always mean the $\limsup_{X\to\infty}$ (for upper bounds) or the $\liminf_{X\to\infty}$ (for lower bounds) and if these upper and lower bounds are not equal, no claim is being made that the $\lim_{X\to\infty}$ actually exists.

positive density has Mordell-Weil rank one (at present this result is only for elliptic curves only over $\mathbf{Q}$).

9. Back to 2-Selmer rank statistics

As a preview of what we will be discussing, here is a table giving a hint of the differences in the statistics for our three types of families.

Table 1. Statistical differences

Family Type	1	2	3
Ordering	by Conductor	Skew-Box	by Conductor
Heuristics	Poonen-Rains	Poonen-Rains modified by "Disparity"	"Equal odds"
Methods	Geom. of Nos.	Cebotarev	Cebotarev & Spin

10. Ordering the aggregate of elliptic curves:

We have a natural way of counting the curves!

Theorem 10.1. For any real number X there are only finitely many isomorphism classes (over K) of elliptic curves (over K) with a representation as above such that the absolute value of the norm of its discriminant is less than X; i.e.,

$$|N_{K/\mathbf{Q}}\Delta(a,b)| \ < \ X.$$

That is, we can order the collection of these mathematical objects, in terms of the size of the norms of the discriminants of their "smallest" representations as above[8]

The proof of this finiteness already requires significant results in the arithmetic of elliptic curves: for each (rational) integer $N \neq 0$ let $\mathcal{N}$ denote a finite collection of integers in $\mathcal{O}_K$ such that every integer in $\mathcal{O}_K$ with norm equal to N is a twelfth power (of an integer in $\mathcal{O}_K$) times an element of $\mathcal{N}$. We are—in effect—counting the number of integral

[8]There are some slightly different competing ways of ordering the array of elliptic curves. For example by *conductor*, or as in Manjul Bhargava's work by the size of a natural "height-type" function $H(E) := \max\{|N_{K/\mathbf{Q}}a|^3, |N_{K/\mathbf{Q}}b|^2\}$.

solutions to the following finite collection of diophantine equations in α and β:

$$-4\alpha^3 - 27\beta^2 = \nu$$

for ν running through the finite set $\mathcal{N}$. Each of these equations are again integral models of *elliptic curves* parametrized by the variables α and β. They have only finitely many integral solutions in $\mathcal{O}_K$.

Moral: the integral solutions over K of these particular elliptic curves "count" the totality of all elliptic curves over K. It's an example of elliptic curves "knowing" other elliptic curves.

That these affine models of elliptic curves have only finitely many integral solutions in $\mathcal{O}_K$, was shown by Siegel (using methods that were ineffective[9] ; effective solutions to this were provided later by Baker; and Faltings famous proof of Mordell-Conjecture also bears on this problem.

The rough number of such elliptic curves is—for X sufficiently large—squeezed between $X^{5/6-\epsilon}$ and $X^{5/6+\epsilon}$ (any $\epsilon > 0$ but presumably starting at larger and larger X).[10]

11. Families of "type (1)": *all* elliptic curves over a given number field

We have discussed, in section above, the work of Manjul Bhargava and Aren Shankar and co-authors regarding Mordell-Weil statistics. Their results are related to thestudy of the average *size* of the 2-Selmer rank of elliptic curves (again over $\mathbf{Q}$ —and when they are ordered in any of the standard ways). They show that the average size is *three*[11] For any prime number p the *reduced p-Selmer rank of an elliptic curve over a number field*[12] has this important property: it is finite (!), computable (!) (at least in principle), and is an upper bound for the rank of the Mordell-Weil group of the elliptic curve over the number field. If the Shafarevich-Tate conjecture holds, then for all but finitely many primes p, the reduced p-Selmer rank would be equal to that Mordell-Weil rank.

[9]these methods being related to the Mordell-Weil rank of these elliptic curves, a notion which we'll discuss later

[10]More fun would be to get a precise asymptotic estimate with an error term; this is what Bhargava gets for the ordering of elliptic curves via the size of the function $E \mapsto H(E)$.

[11]Of course no 2-Selmer group can have such a size: these 2-Selmer groups are then all either above or below average.

[12]This is the dimension of the so-called p-Selmer group minus the rank of rational p-torsion of the elliptic curve over the number field.

So it is natural, as in the results of Bhargava and co-authors alluded to above, to expect that the statistics of p-Selmer ranks (e.g., even when restricted to $p = 2$) contribute to our understanding of Mordell-Weil ranks. More recent advances concern 3-Selmer,and 5-Selmer.

12. Families of "type (2)": Elliptic curves that are quadratic twists of a given elliptic curve

The elliptic curves in this family are all isomorphic over $\mathbf{C}$; they are quadratic twists of one another (in various senses, but most directly:) in the sense that any two of them become isomorphic over some quadratic extension of the base field K.

If

$$E: \quad y^2 = x^3 + ax + b$$

is the initial elliptic curve and

$$E^{(d)}: \quad dy^2 = x^3 + ax + b$$

is a general member of the family, note that modifying d by multiplying by a square in $\mathcal{O}_K$ does change the isomorphism type of the elliptic curve so what is really at issue is a class of elliptic curves indexed by elements in $\mathcal{O}_K - \{0\}$ mod squares. It is natural, then, to denote $E^{(d)}$ as E^χ where χ is the (quadratic) Dirichlet character over K that cuts out the quadratic Galois extensions $K(\sqrt{d})$. There is also a natural ordering of the members of this family. For brevity, if I is a prime ideal in a number field, by $|I|$, the **size** of I, let us mean $|I| := |N_{K/\mathbf{Q}} I|$; i.e, the absolute value of the norm to $\mathbf{Q}$ of the ideal I.

Now, for a character χ, let

$$|\chi| := \max\{|P|;\ P \text{ a } \textit{prime} \text{ ideal dividing the conductor of } \chi\}.$$

The type of question we will examine has it roots in a famous result of Heath-Brown on the statistics of 2-Selmer ranks of a specific family of CM elliptic curves over $\mathbf{Q}$ related to the congruent number problem[13]. This is the family

$$E_D: \quad Dy^2 = x^3 - x$$

for positive square-free integers D. The arithmetic of this family answers the question of whether or not D can be the common difference of an arithmetic progressions of squares of rational numbers.

[13]D.R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Inv. Math. **111** (1993), 171-195; see also *The size of Selmer groups for the congruent number problem, II.*

We shall be dealing with Selmer ranks, which—for the moment—can just be thought of as useful numbers. More specifically, It is convenient to define something that might be called the *reduced Selmer rank*.

Definition 12.1. If E is an elliptic curve over K, by $r(E;K)$, the **reduced 2-Selmer rank** of E over K, we mean:

$$r(E;K) := \{\text{the } 2-\text{Selmer rank of } E \text{ over } K\} \quad - \quad \dim_{\mathbf{F}_2} E(K)[2].$$

Among the many uses of this number $r(E,K)$ is that it is computable, it is an upper bound for the Mordell-Weil rank of E over K, and conjecturally it has the same parity as that Mordell-Weil rank.

13. Disparity

It is conjectured that ordering the family of all elliptic curves over a given number field by the absolute value of the norm of the conductor, there are "asymtotically as many elliptic curves having odd 2-Selmer rank[14] as there are having even rank." We don't know this yet[15] This is *not* the case for families of Type (2).

Here I will be discussing results due to Zev Klagsbrun, Karl Rubin and myself coming from our article *Selmer ranks of quadratic twists of elliptic curves* which is posted on ArXiv.

Theorem 13.1. The ratio

$$\frac{|\{|\chi| < X;\ r(E^\chi;K)\ \text{ is odd}\}|}{|\{|\chi| < X\}|}$$

is constant for large enough X.

Note: Here is the format of how this is proved: Let Σ be the set of all places of K dividing $2 \cdot \infty$ or the conductor of E. Let $C(K)$ be the group of quadratic characters of K, and consider the set-theoretic mapping:

$$C(K) \longrightarrow \{\text{even},\ \text{odd}\}$$

[14](and therefore, conjecturally having odd Mordell-Weil rank, and p-Selmer rank for any p)

[15]We do know that the odd and even 2-Selmer ranks both have positive density, though.

which says whether the reduced 2-Selmer rank of E^χ over K is even or odd. This mapping is constant on cosets of the kernel of the homomorphism

$$h : C(K) \longrightarrow \Gamma := \prod_{v\in\Sigma} C(K_v)$$

that sends χ to the product of its local restrictions χ_v for $v \in \Sigma$.

More specifically, given E over K, one can define a function

$$C(K_v) \xrightarrow{f_v} \{\pm 1\}$$

(for $v \in \Sigma$) which is a slightly modified "arithmetic ratio of epsilon-factors" whose definition I omit to give here, but which has the effect that for every quadratic character χ of K, the ranks of the 2-Selmer groups of E^χ and E have the same parity if and only if

$$\prod_{v\in\Sigma} f_v(\chi_v) \;=\; 1 \;\in \{\pm 1\}.$$

Define

$$f : \Gamma \to \{\pm 1\}$$

to be the product:

$$f(\gamma) := \prod_{v\in\Sigma} f_v(\gamma_v)$$

where $\gamma = (\dots, \gamma_v, \dots)$.

Let $C(K, X) \subset C(K)$ be the (finite) subgroup consisting of characters such that the absolute values of the norms of primes dividing their conductors are $< X$. So

$$C(K) = \cup_X C(K, X).$$

Since the target group Γ is finite, once X is large enough, $h(C(K, X)) = h(C(K))$. The limit stabilizes to the ratio

$$\frac{|\{\gamma \in \Gamma; f(\gamma) = \pm 1|}{|\{|\Gamma|}$$

for such values of X (where the sign ± 1 depends—in the evident way—on whether or not the rank of E over K is even or odd).

Define, then,

$$\delta(E, K, \text{odd}) := \frac{1}{2} - \lim_{X\to\infty} \frac{|\{|\chi| < X;\ r(E^\chi; K)\ \text{ is odd}\}|}{|\{|\chi| < X\}|}.$$

and its colleague:

$$\delta(E,K,\text{odd}) := \frac{1}{2} - \lim_{X\to\infty} \frac{|\{|\chi| < X;\ r(E^\chi;K)\ \text{ is even}\}|}{|\{|\chi| < X\}|}.$$

these being called the *odd* and *even* disparities of E over K. Of course:

$$\delta(E,K,\text{odd}) + \delta(E,K,\text{even}) = 0.$$

Definition 13.2. By the *disparity*,

$$0 \le \delta(E,K) := |\delta(E,K,\text{odd})| = |\delta(E,K,\text{even})| \le \frac{1}{2},$$

we mean the absolute value of either of the above.

Whatever the disparity is—i.e., the relative frequency of odd to even ranks of the 2-Selmer groups of twists—if the Shafarevich-Tate Conjecture holds we would be getting exactly the same disparity relating odd to even ranks of the Mordell-Weil groups of twists.
If $\delta(E,K) = 0$ we "have parity" in the sense that there are statistically as many odd ranks as even; and if $\delta(E,K) = \frac{1}{2}$ all ranks are odd, or all ranks are even. Either of these endpoints occur; for example, we show that if K has at least one real place, we "have parity." And it is not hard to find more interesting disparities[16].

Here is a random example of what Zev, Karl, and I show, regarding disparity, in the course of studying full rank statistics of 2-Selmer groups.

Let L be a finite number field extension of $\mathbf{Q}$ of degree d, in which 2 splits completely and 5 is unramified. Form the infinite sequence of number fields $K_n := L(\mu_{2^n})$ for $n = 3,4,5,\ldots$, and view the elliptic curve E

$$(50A1) \quad y^2 = x^3 - 675x - 79650$$

over each K_n.

Theorem 13.3.

$$\delta(E,K_n) = \frac{\left(1 - 2^{-(2^{n-1}+1)}\right)^d}{2}.$$

In particular, just dealing with these examples yields a set of achieved disparities that is dense in the full range of possibilities, $[0,\frac{1}{2}]$.

[16]For example we show that if K has no real place, and E is semistable over K then we never "have parity."

14. Modified Poonen-Rains heuristic

The Poonen-Rains heuristic offers conjectures for the relative averages of p-Selmer ranks of twists of a general elliptic curve E over a general number field K. The idea is to view the Selmer group conditions as given by the intersection of two Langrangian subspaces in a quadratic space. The heuristic comes, then, from the densities of ranks of the intersection of two "random Lagrangians." This range of densities can also be achieved as an equilibrium distribution of a certain Markov system, assuming "parity." In the case of families of Type (2), as we've discussed, there can be disparity, yet, curiously the Markov process model still provides what is, in fact, provable.

Here give description of the Markov Process...

The function

$$\mathcal{D}(Z) := \sum_{n\geq 0} \mathcal{D}_n Z^n \ = \prod_{i=0}^{\infty} \frac{1+2^{-i}Z}{1+2^{-i}}$$

had already come up in the work of Heath-Brown, and later in that of Swinnerton-Dyer specifically as defining the stationary distribution for Markov process we've just described; it also shows up in our work.

The coefficients $\mathcal{D}_n$ are all positive numbers and, setting $Z = 1$ we get that

$$\sum_n \mathcal{D}_n = 1$$

so $\mathcal{D}$ is a probability density (a positive measure with mass equal to 1) on the set of natural numbers. Setting $Z = -1$ we get $\sum_n (-1)^n \mathcal{D}_n = 0$ which gives us an equal balance of odd and even densities:

$$\sum_{n \text{ odd}} \mathcal{D}_n = \sum_{n \text{ even}} \mathcal{D}_n = \frac{1}{2}.$$

While we are on this topic, looking ahead, if you evaluate at $Z = 2$ and $Z = -2$ you get:

$$\sum_n 2^n \mathcal{D}_n = \prod_{i=0}^{\infty} \frac{1+2^{-i}2}{1+2^{-i}} = \prod_{i=0}^{\infty} \frac{1+2^{1-i}}{1+2^{-i}} = 3$$

and

$$\sum_n (-2)^n \mathcal{D}_n = \prod_{i=0}^{\infty} \frac{1+2^{-i}2}{1+2^{-i}} = \prod_{i=0}^{\infty} \frac{1+2^{1-i}}{1+2^{-i}} = 0,$$

respectively. This gives us that

$$\sum_{n \text{ odd}} 2^n \mathcal{D}_n = \sum_{n \text{ even}} 2^n \mathcal{D}_n = \frac{3}{2}$$

which eventually will be linked to "average sizes of 2-Selmer groups of odd and of even rank." The derivative of $\mathcal{D}(Z)$ evaluated at $Z = \pm 1$ will eventually be linked to the "average 2-Selmer (even and odd) rank."

15. Digression: p-Selmer for general primes p

There is a corresponding Markov Process[17] related to p-Selmer,

$$\sum_{n \text{ even}} \mathcal{D}_n^{(p)} \cdot p^n = \sum_{n \text{ odd}} \mathcal{D}_n^{(p)} \cdot p^n \quad = \quad p+1,$$

suggesting the following amazing conjecture.

Conjecture: Let K be a number field. The average "size" of the p-Selmer groups in the collection of all elliptic curves over K is $p+1$, for any prime number p. More generally the average "size" of the N-Selmer group is $\sigma(N) := \sum_{d \mid N} 1$.

Even more amazing is that Bhargava and Shankar prove that this is the case for the family of all elliptic curves over $K = \mathbf{Q}$ and $N = 2, 3, 4, 5$.

16. Returning to quadratic twist families and reduced 2-Selmer ranks

Here is a conjecture, closely related to the result we actually proved. (For the exact statement, see Theorem 19.2 of section 19 in the Appendix.

Conjecture 16.1. Let E be an elliptic curve over a number field, and assume that E has "full Galois action on its 2-torsion." That is, the natural mapping of the absolute Galois group of K to $\mathrm{Aut}(E[2]) \approx \mathrm{GL}_2(\mathbf{F}_2) = S_3$ is surjective.

(1) Let $n \geq 0$, and let

$$\epsilon = \text{ "even," or "odd"}$$

according to the parity of n. Then the limit described the formula below exists and the formula holds:

[17] See section 18 in the Appendix.

$$\big(\frac{1}{2} - \delta(E,K;\epsilon)\big)\cdot \mathcal{D}_n \;=\; \lim_{X\to\infty} \frac{|\{|\chi| < X;\ r(E^\chi,K) = n\}|}{|\{|\chi| < X\}|}.$$

As corollaries of this conjecture (following the discussion above) one would have

Corollary 16.2. Let E be an elliptic curve over K. With the same ordering of χ's as in the statement of Conjecture 16.1 it follows—if that conjecture holds—that the average size of the reduced 2-Selmer groups of quadratic twists of E is 3 (independent of the disparity). Moreover, there is a finite upper bound to the average 2-Selmer rank, and Mordell-Weil rank, of quadratic twists of E.

We cannot yet manage to prove these limits, when we order the quadratic twists χ by increasing absolute value of norm of conductor as described above. We do prove the theorem above, though, in a less satisfactory way: that is, when we use what we call *skew-box ordering* described in section 19 of the appendix below.

Here are some further qualitative comments about our general methods.

(1) We use only standard methods: class field theory, global duality, an effective Cebotarev theorem (in either of the standard two strengths: the unconditionally proved theorem, but also if we want to improve some bounds, we formulate results using the conditional estimate based on GRH) and basic arithmetic of elliptic curves.
(2) More specifically, the actual densities we obtain all derive from an understanding of the relative densities of certain "Cebotarev classes" of places in various finite extension fields of K.
(3) For example, of use to us, in the context in which we work, are three distinct Cebotarev classes of "good" places of K related to the S_3-extension that is the splitting field of 2-torsion in E; we call these classes *types* $0, 1$, and 2 below according as $Frob_v$ is of order 3, 2, or 1.
(4) Now, averaging over *many* type 0 places has the effect of smoothing things out a lot, and this is a major piece of our machinery, thanks to which we avoided a certain interesting side-question[18].

[18]Zev suggested this successful way of skirting such (side-)questions.

17. Families of "type (3)": Elliptic curves that are quadratic twists of a given elliptic curve by a character of prime conductor

Let E for example be the elliptic curve

$$y^2 = x^3 + x^2 - 16x - 29 \ ,$$

which has conductor $784 = 2^4 \cdot 7^2$. Let K be the maximal real subfield of the field $\mathbf{Q}(\mu_7)$ of 7-th roots of unity as in section 3. Then, K is a cyclic extension of $\mathbf{Q}$ of degree 3, and $K = \mathbf{Q}(\mathbf{E}[\mathbf{2}])$, the field generated by the coordinates of the points of order 2 on E.

Suppose p is a rational prime congruent to $\pm 1 \pmod 7$, so p splits into 3 distinct primes in K. Let P be one of the primes above p. If P has a totally positive generator that is congruent to 1 (mod 8), then the 2-Selmer group $\mathrm{Sel}_2(E^{(p)}/\mathbf{Q})$ of the quadratic twist of E by p has dimension

$$\dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^{(p)}/\mathbf{Q}) = \begin{cases} 3 & \text{if } spin(P) = 1, \\ 1 & \text{if } spin(P) = -1. \end{cases}$$

The condition that p have a generator congruent to 1 modulo 8 is equivalent to asking that p split completely in the ray class field of K modulo 8. Hence, the set of such p has positive density. Moreover, K has class number 1. Thus, thanks to theorems generalizing Theorem 3.2 (see our paper "The spin of prime ideals" on ArXiv) shows that, within that set of twists, the Selmer rank is equal to 1 half of the time and 3 half of the time. As one might expect, this holds more generally.

Appendix

18. Markov Combinatorics

Fix p a prime number and define the following operator $\mathcal{M} = \mathcal{M}_p$ $(d \mapsto \mathcal{M}_p d)$ on the convex set Ω of mass densities:

$$\mathcal{M}_p d(n) := (1 - p^{-1-n})d(n+1) + p^{1-n}d(n-1).$$

So, $\mathcal{M}_p d(0) := (1 - p^{-1})d(1)$.

The following lemma is evident.

Lemma 18.1. (1) The linear operator $\mathcal{M}_p$ preserves Ω;

(2) $\mathcal{M}_p$ preserves mass; e.g., If D is a probability density, so is $\mathcal{M}_p D$.

(3) $\mathcal{M}_p$ sends even mass densities to odd ones and odd to even; e.g., $\mathcal{M}_p$ "flips" disparity, in that if d is a nontrivial mass density, then

$$\epsilon_{\text{even}}(\mathcal{M}_p d) = \epsilon_{\text{odd}}(d),$$

and

$$\epsilon_{\text{odd}}(\mathcal{M}_p d) = \epsilon_{\text{even}}(d).$$

The operator $\mathcal{M}_p$ has a not-quite-unique equilibrium density in the following sense: Consider the following mass density (it *is* in fact a probability distribution having parity) predicted by the Poonen-Rains heuristic, as discussed in Part I above:

$$\mathcal{D}_p(n) := \prod_{j=1}^{\infty}(1+p^j)^{-1}\prod_{j=1}^{n}\frac{p}{p^j-1}.$$

NOTE: We have the following infinite-product generating function for the $\mathcal{D}_p(n)$'s:

$$G(Z) := \sum_{n\geq 0}\mathcal{D}_p(n)Z^n \ = \prod_{i=0}^{\infty}\frac{1+p^{-i}Z}{1+p^{-i}}.$$

Theorem 18.2. (1) $2\mathcal{D}_{p,\text{odd}}$ and $2\mathcal{D}_{p,\text{even}}$ are probability densities,
(2) $\mathcal{M}_p\mathcal{D}_{p,\text{odd}} = \mathcal{D}_{p,\text{even}}$ and $\mathcal{M}_p\mathcal{D}_{p,\text{even}} = \mathcal{D}_{p,\text{odd}}$.

Proof: These are direct computation.

Theorem 18.3. For any nontrivial mass density d we have the limits:

$$\lim_{k\to\infty}\mathcal{M}_p^{2k}d = 2\mu(d)\cdot\big(\epsilon_{\text{odd}}(d)\cdot\mathcal{D}_{p,\text{odd}} + \epsilon_{\text{even}}(d)\cdot\mathcal{D}_{p,\text{even}}\big).$$

NOTE: When we prove this theorem (e.g., by quoting something) we should also give error terms

Corollary 18.4. We also have the limits:

$$\lim_{k\to\infty} \mathcal{M}_p^{2k+1} d = 2\mu(d) \cdot \big(\epsilon_{\text{odd}}(d) \cdot \mathcal{D}_{\text{even}} + \epsilon_{\text{even}}(d) \cdot \mathcal{D}_{\text{odd}}\big).$$

We have the evident corollary:

Corollary 18.5. *The "Poonen-Rains Heuristic" Statistics gives the stationary distribution for the Markov process M^2 applied to distributions having parity:*
For any nontrivial probability density d having parity,

$$\lim_{k\to\infty} M_p^{2k} d = \mathcal{D}_p.$$

NOTE: We should also give the formulas for average size and—in fact— all moments—for even and odd ranks

19. Skew-box ordering

By a **skew-box ordering** of our family we mean the following.

(1) First, for integers $1, 2, 3, \dots \nu, \dots$ we give positive-real-valued monotonically increasing functions $\alpha_\nu(X)$ of a positive real variable X; we assume further that for each ν $\alpha_\nu(X)$ tends to infinity with X.

(2) If $\chi \in C(K)$ let $d(\chi)$ be its conductor, and write it as follows:

$$d(\chi) = d_\Sigma(\chi) d_0(\chi) d_1(\chi) d_2(\chi),$$

where we have factored $d(\chi)$ into the part involving places in Σ and the places (outside Σ) of types $0, 1$ and 2.

Definition 19.1. For positive integers j, k define **the skew-box $B_{j,k}(K, X)$ with sides $\{\alpha_\nu\}_\nu$ and cut-off X** to be the finite subset of the group $C(K)$ of quadratic characters where

(a) $d_1(\chi) = q_1 q_2 \dots q_{j'}$ is a product of j' places, where $j' \le j$ and the absolute value of the norm of q_i is $< \alpha_i(X)$, for $i = 1, 2, \dots j'$, and where

(b) $d_2(\chi) = q_{j'+1}q_{j'+2}\dots q_{j'+k'}$ is a product of k' places, where $k' \le k$ and the absolute value of the norm of q_i is $< \alpha_i(X)$, for

$$i = j'+1, j'+2, \dots j'+k',$$

(c) (in contrast to the requirement that we bound the norms of each of the places of types 1 and 2, and take account of how many places of those types there are) we require that the absolute value of the norm of $d_0(\chi)$ is $< \alpha_{j'+k'+1}(X)$.

Note that $C(K)$ is the union of the finite "skew-boxes" $B_{j,k}(K,X)$ as X, j, and k tend to infinity.

Here is our theorem:

Theorem 19.2. Let E be an elliptic curve over K with full Galois action on 2-torsion; that is, the natural homomorphism

$$\mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}\big(E(\bar{K})[2]\big)$$

is surjective. For integers

$$1, 2, 3, \dots \nu, \dots$$

there are explicit positive-real-valued monotonically increasing functions[19] $\alpha_\nu(X)$ of a positive real variable X, each tending to infinity with X, such that defining skew-boxes $B_{j,k}(K,X)$ with sides given by those $\{\alpha_\nu\}_\nu$, we have:

(1) Let $n \ge 0$, and let

$$\epsilon = \text{ "even," or "odd"}$$

according to the parity of n. Then the limit described the formula below exists and the formula holds:

[19]These functions depend on E and K. I won't give the formulas here, but just mention that these are defined "recursively" and come from successively applying the effective Cebotarev Theorem; we have unconditional bounds, and also better bounds conditional on GRH.

$$\big(\frac{1}{2}-\delta(E,K;\epsilon)\big)\cdot\mathcal{D}_n \;=\; \lim_{j+k\to\infty}\lim_{X\to\infty}\frac{|\{\chi\in B_{j,k}(K,X);\ r(E^\chi,K)=n\}|}{|B_{j,k}(K,X)|}$$

where X, j, and k all go to infinity.

As discussed in the context of Conjecture 16.1 a series of corollaries follow:

Corollary 19.3. Let E be an elliptic curve over K with full Galois action on 2-torsion. With the same skew-box ordering of χ's as in the statement of Theorem 19.2 the average size of the reduced 2-Selmer groups of quadratic twists of E is 3 (independent of the disparity). Moreover, there is a finite upper bound to the average 2-Selmer rank, and Mordell-Weil rank, of quadratic twists of E.