Q&A (mostly Q) about statistics regarding diophantine stability

B. Mazur— joint work with K. Rubin

October 9, 2017

These are skeletal notes describing what I talked about in the "Number Theorist's Lecture" that I gave on Friday October 6, 2017. I actually had also planned to display slides that Karl Rubin and I have that connect with statistics related to diophantine stability, but the discussion—Q&A—seemed complete enough that time being short, it made more sense not to display them but rather just offer them via a link on my web-page:

http://www.math.harvard.edu/~mazur/papers/For.N.T.Seminar.talk.pdf

1 Opening questions about Diophantine Stability

A variety V defined over K is **diophantine stable** for the field extension L/K if $V(L) = V(K)$; that is, if V acquires no *new* rational points when one extends the base field from K to L. We will be discussing theorems and conjectures that point to the prevalence of diophantine stability in a range of contexts.

For example, V is Diophantine **Un**-stable for any nontrivial field extension L/K *if and only if* V contains a curve over K isomorphic to a Zariski open in $\mathbf{P}^1$ (over K).

(If V/K contains a new rational point in the extension $K(t)/K$, then V *does* contains a curve that is the image of a Zariski open in $\mathbf{P}^1$; the proof in the other direction is clear.)

Question 1. *Do we have the same equivalence as above, when we restrict to number fields K and extensions L/K of finite degree?*

From now on, K will be a number field.

Karl Rubin and I proved a result—quite weak in comparison with the numerical phenomena, we think—which guarantees a certain amount of diophantine stability in the following context.

Let V be either a curve over K of genus $g \geq 1$, or an absolutely simple abelian variety.

Theorem 1. *Then there is a finite field extension K'/K for which there exists an arithmetic progression of prime numbers ℓ such that for each positive integer n there are infinitely many Galois cyclic field extensions L'/K' of degree $d := \ell^n$ that are Diophantine stable for V' (the base change of V from K to K').*

An interesting open question:

Question 2. *Is the same true if one drops the condition that the abelian variety be absolutely simple?*[1]

For simplicity, let's consider questions regarding diophantine stability restricted to cyclic extensions of K of prime degree ℓ, noting that class field theory gives us neat control of what we might denote $\mathcal{P}(K,\ell)_{\leq m}$, the set parametrizing all such extensions of a given number field K of conductor $\leq m$. If we pass to the limit, $\mathcal{P}(K,\ell) = \mathcal{P}(K,\ell)_{\leq m}$ we get an ind-system of finite dimensional projective spaces over $\mathbf{F}_\ell$ ordered by conductor m, so we have a natural way of formulating statistical questions about this.

Question 3. *Let A be an abelian variety over K. What can one say about the subset*

$$U(K,\ell,A) \subset \mathcal{P}(K,\ell)$$

consisting of those cyclic extensions of degree ℓ that are Diophantine **UN-***stable for A over K?*

Discuss the special case of $K = \mathbf{Q}$ and $A = E$, an elliptic curve:

Conjecture 2. *(This is equivalent—conditionally*[2]*—to an inspiring conjecture of David-Fearnley-Kisilevsky.) Let $K = \mathbf{Q}$ and $A = E$, an elliptic curve. Then $U(K,\ell,A)$ is infinite only if $\ell = 2, 3$, or 5.*

Note that there are indeed cases where we expect, or can prove, that $U(K,\ell,A)$ is infinite. I.e., we might have we can be called **root number** reasons to expect this—as in the above case when $\ell = 2$; or we might have **geometric** reasons—as in the above case—as we shall see below—for particular elliptic curves E over $\mathbf{Q}$ when $\ell = 3$; or at least for *one* case for an elliptic curve over a quadratic imaginary field when $\ell = 5$.

One of the many important viewpoints regarding algebraic geometry and number theory that the mathematician Serge Lang stressed is the following: for an algebraic variety to possess infinitely many rational points over a number field, there has to be, Lang felt, a good reason— best: a clear geometric reason. He conjectured, in fact, that this happens *only* if the variety contains the (nonconstant) image of a rational curve or an abelian variety. I imagine he would also be looking for similarly striking reasons for $U(K,\ell,A)$ to be infinite.

[1] It is tempting to offer this question as a possible graduate student project, but Karl and I think that it might be quite difficult.

[2] D-F-K make their conjecture about vanishing of central values of L-functions of elliptic curves over $\mathbf{Q}$ twisted by abelian characters, this being conjecturally equivalent to what is formulated here.

One possible geometric reason arises from the existence of what we'll call *ℓ-pencils*:

Let C be a smooth projective curve over K admitting an automorphism of (prime) degree ℓ (defined over K) such that the quotient of C by that automorphism is $\mathbf{P}^1$ over K. Then take A any abelian variety quotient of the jacobian of C, and note that the K-rational points of the "$\mathbf{P}^1$" quotient of C (except for the K-rational points of $\mathbf{P}^1$ that are in the image of $C(K)$—this being a finite set of points if the genus of C is > 1) parametrize cyclic extensions of K of degree ℓ that are Diophantine unstable for A.

Definition 1. *When we have such a C above with A an abelian variety quotient of its jacobian, say that A* **admits a pencil of Diophantine unstable extensions of degree ℓ over K.** *Or, for short:* **an ℓ-pencil**.

E.g., (*Exercise:*) Consider the case when $A = E$ is an elliptic curve and $\ell = 2$. Then *all* the points of $U(K, 2, E)$ come from the 'natural' pencil $C = E \to \mathbf{P}^1$ of degree 2.

Remark:

1. Such a pencil is (essentially) equivalent to a K-rational curve of genus 0 (with a K-rational point) in a fiber of the mapping

   $$E^\ell/\text{cyclic action} \quad \stackrel{\text{sum}}{\longrightarrow} \quad E.$$

   These are *interesting* $\ell - 1$-folds! Do they possess *any* $\bar{\mathbf{Q}}$-rational curves of genus 0 if $\ell \gg 0$?

2. For $\ell > 2$ and E an elliptic curve over K the following is—pretty much—all that's known (at least to Karl Rubin and me) so far.

   > Any elliptic curve E admits a pencil of Diophantine unstable extensions of degree 3 over some finite extension of K. Moreover, there are examples of elliptic curves over $\mathbf{Q}$ that admit a pencil of Diophantine unstable extensions of degree 3 over $\mathbf{Q}$. We know one example of *one* elliptic curve over $\mathbf{Q}$ (Cremona classification: 50a1) that admits a pencil of Diophantine unstable extensions of degree 5 over (appropriate) quadratic fields.

Question 4.

1. *For E an elliptic curve over $\mathbf{Q}$ is it true that there are no pencils of Diophantine unstable extensions of (prime) degree $\ell > 3$ over $\mathbf{Q}$?*
2. *For E an elliptic curve over a number field K are there any pencils of Diophantine unstable extensions of (prime) degree $\ell > 5$?*
3. *For any abelian variety A over K is there an upper bound $b(A, K)$ for the primes ℓ for which A admits a pencil of Diophantine unstable extensions of degree ℓ over K? Is there such a bound $b(n, d)$ that depends only on $n :=$ the dimension of A and $d :=$ the degree of K?*

An affirmative answer to (1) above would follow from the conjecture of David-Fearnley-Kisilevsky (which is the inspiration for our project).

As for (3), examples show that $b(n, d) \gg n^{alpha}$ with $\alpha = 1/2$ (of course, possibly: $b(n, d) = +\infty$).

Question 5. *Can one find examples that show $b(n,d) \gg n^{alpha}$ for some α strictly greater than 1/2?*

2 Pencils for $\ell = 3$

Here I discussed the K3 surface business related to $\ell = 3$, and here's an example over Q:

Take $E : y^2 = x^3 - 9x + 9$ over $\mathbf{Q}$. Putting $r(t) := 8(t^2 - 162t)/(t^2 + 8748)$ one computes to find that the points (x, y) on the curve E with $y = 3x + r(t)$ for rational values of t parametrize a pencil of cubic cyclic points on E.

3 A pencils for $\ell = 5$

The classical "Bring's Curve" $\mathcal{C}$ is defined over $\mathbf{Q}$ and will provide an example (e.g., over the field of Gaussian numbers $\mathbf{Q}[i]$) of a cyclic pencil of genus 4 for a certain elliptic curve $\mathcal{E}$. "Bring's curve" is the (smooth, projective) curve in $\mathbf{P}^4$ defined by three equations—in the five homogenous variables $(x_1, x_2, x_3, x_4, x_5)$:

$$\sum_i x_i^n = 0 \text{ for } n = 1, 2, 3. \tag{1}$$

Visibly $\mathcal{C}$ admits the symmetric group S_5 as group of automorphisms (all of this defined over $\mathbf{Z}$) the action being by permutation of the five variables. The group S_5 is the entire group of its automorphisms since $\mathcal{C}$ is a curve of genus 4. Also, $\mathcal{C}$ has no real points since its quadratic defining equation has none.

Let $\tau := (12345)$, and $\sigma := (1234)$ be the indicated 5- and 4- cycles, respective.

Proposition 1.

1. *There are exactly four fixed points of τ in $\mathcal{C}$. Namely: $\{(1, \zeta, \zeta^2, \zeta^3, \zeta^4)\}$ where ζ runs through the nontrivial fifth roots of 1. These are the only points of ramification for the mapping*

$$\mathcal{C} \to \mathcal{C}/\{\text{action of } \tau\}.$$

2. *There are exactly two ramified points for the mapping*

$$\mathcal{C} \to \mathcal{C}/\{\text{action of } \sigma\}.$$

Namely: $\{(1, \pm i, -1, \mp i, 0)\}$. These two points are all fixed points of σ; i.e., they are 'totally ramified.'

Proof. Taking the indices $1, 2, 3, 4, 5$ mod 5, for a ($\mathbf{C}$-valued) point $(x_1, x_2, x_3, x_4, x_5)$ to be a fixed point of τ we must have, for some $\lambda \in \mathbf{C}$ that $x_{k+1} = \lambda x_k$ for all $k \in \mathbf{Z}/5\mathbf{Z}$ which forces λ to be a fifth root of unity, and by the linear equation in 1 it must be a nontrivial fifth root of unity. For each such λ there is exactly one such point, proving (1).

For (2):

Lemma 1. *If $x = (x_1, x_2, x_3, x_4, x_5)$ is a fixed point of $\sigma^2 = (13)(24)$, then $x_5 = 0$.*

Proof. If x is such a fixed point, then there is a $\lambda \in \mathbf{C}$ such that $\sigma^2(x)_k = \lambda \cdot x_k$ for all five coordinates x_k. In particular,

$$x_3 = \lambda x_1;\ x_4 = \lambda x_2; x_5 = \lambda x_5.$$

By the latter equality (if $x_5 \neq 0$) it would follow that $\lambda = 1$. That is, $x = (a, b, a, b, c)$ for some a, b, c, with $c \neq 0$. The linear equation in 1 gives $c = -2(a + b)$ so a and b cannot both be zero. Without loss of generality, suppose that $a \neq 0$, and scale it so that $a = 1$. So, the linear equation in 1 gives

$$c = -2(b + 1) \tag{2}$$

and combined with the quadratic equation in 1,
i.e., $c^2 = -2(a^2 + b^2)$, we get that

$$b = \frac{5}{3} \text{ or } \frac{11}{3}. \tag{3}$$

Now comparing 2 with the cubic equation in 1 gives the relation $b^3 + 1 = 4(b + 1)^3$ and neither value in 3 satisfies this. □

Now let $x = (x_1, x_2, x_3, x_4, 0)$ be a fixed point of $\sigma^2 = (13)(24)$. Such a point satisfies the relations $x_3 = \lambda x_1$ and $x_4 = \lambda x_2$ for $\lambda \in \{\pm 1\}$. Again, without loss of generality we may suppose that $x_1 \neq 0$, and scaling suitably, $x_1 = 1$. So, putting $x_2 = b$, our point is of the form $x = (1, b, \lambda, \lambda b, 0)$. The linear equation in 1 then gives: $(1 + \lambda)(1 + b) = 0$; i.e., either $b = -1$ in which case the quadratic equation in 1 is violated, or else $\lambda = -1$ and the quadratic equation in 1 tells us that $b = \pm i$. Therefore $\{(1, \pm i, -1, \mp i, 0)\}$ are the only fixed points of $\sigma^2 = (13)(24)$.

Noting that $\{(1, \pm i, -1, \mp i, 0)\}$ are actually fixed under σ concludes the proof of Proposition 1. □

Corollary 3. *Let $\mathcal{P}$ (resp: $\mathcal{E}$) denote the quotient of $\mathcal{C}$ (over the field $\mathbf{Q}$) by the action of $\tau = (12345)$ (resp: $\sigma = (13)(24)$). Then $\mathcal{P}$ is of genus 0 and $\mathcal{E}$ is of genus 1.*

Proof. Recall that the Euler characteristic of Bring's curve is -6. If u and v denotes the Euler characteristics of $\mathcal{P}$ and $\mathcal{E}$ respectively, the Riemann-Hurwitz formula and Proposition 1 give:

$$-6 = 5u - 4 \cdot 4 \quad \text{and} -6 = 4v - 2 \cdot 3 \tag{4}$$

That is: $u = 2$ and $v = 0$. □

If K is a number field over which $\mathcal{C}$ has a K-rational point, then $\mathcal{P} \simeq \mathbf{P}^1$ (over K) and taking the image of that point in $\mathcal{E}$ as the 'origin' we view $\mathcal{E}$ as an elliptic curve over K. The structure

$$\mathcal{P} \xleftarrow[i]{} \mathcal{C} \xrightarrow{j} \mathcal{E} \ , \tag{5}$$

is a cyclic pencil of degree 5 (and genus 4) for the elliptic curve $\mathcal{E}$ over K.

Are there cyclic pencils of degree 5 (and genus 4) for other elliptic curves?

4 Framing a heuristic for Diophantine Stability from statistics of theta-elements

Here I discussed the extemely close connections between:

- Diophantine stability $\rightarrow$ (conjecturally)
- Special values of L-functions of abelian varieties twisted by abelian characters $\rightarrow$ (when $K = \mathbf{Q}$ and $A = E$) $\rightarrow$
- weighted sums of modular symbols $\rightarrow$
- the issue of θ-coefficients all being equal to a specific value.

One notes here that the first bullet is *arithmetic*, the second is *analytic*, the third is *essentially combinatorial,* and the fourth is *arithmetic again*—but with quite a different feel than the first bullet. The last two bullets are amenable to interesting statistical investigation, especially since the question of whether a collection of θ-coefficient *be all equal to a specific value* should be detectable—at least somewhat—from their general statistics. It seems to Karl and me that the statistics is worth exploring in depth for its own sake.

I felt, at this point that there wasn't time to display on the screen the statistics for modular symbols and theta-elements that connect to these questions, leaving this for another lecture and putting the 'slides' for this part of the talk on my web-page.