New issues, and expectations, in the study of rational points

Barry Mazur

Whatever is original in this survey lecture is joint with Karl Rubin

September 2, 2018

Abstract

Since Diophantus the question of rational solutions to polynomial equations has gripped the imagination of mathematicians, and yet we are—now in 2018—still attempting to understand the general lay of the land. There are questions we confront for which we still don't have the experience to conjecture their answer, let alone answer them. I will give an overview of this, as well as recent work on arithmetic statistics—i.e., the study of specific, or general families of curves or abelian varieties in terms of the statistical behavior of their Diophantine properties. This is largely due to Manjul Bhargava and his co-authors. I will discuss how this connects with, and sharpens, our more general expectations.

Introduction: The scarcity of rational points

1 Lang's (and Lang-type) Conjectures

By a **number field** we mean a subfield of finite degree over $\mathbf{Q}$ in the the field of algebraic numbers in $\mathbf{C}$—equivalently, a field generated over $\mathbf{Q}$ by a single algebraic number. Visibly, any curve defined over the field of algebraic numbers has plenty of algebraic points—these are dense in the locus of complex points of the curve, and it is striking how many different number fields are generated by the coordinates of the rational points of any one curve. Of

course, the algebraic points of $\mathbf{P}^1$ 'generate' all number fields; and the algebraic points of **hyperelliptic curves**—i.e., curves that are double covers of $\mathbf{P}^1$— generate selected quadratic extensions of all number fields.

Now fix a number field K. it was Serge Lang's firm belief that on the whole, algebraic varieties over K tend not to have all that many K-rational points unless either

- there is some specific algebraic geometric structure generating them, or
- a functional equation (proved, or conjectured) and a corresponding root number computation predicts the parity of the rank of a Mordell-Weil group (which in many cases allows one to expect the existence of more rational points than is in evidence without this prediction).[1]

But lacking either reason for rational points to be abundant, the sense is that they are scarce.

For example, consider the question of algebraic varieties possessing infinitely many rational points over number fields. It is easy to see that if V is an algebraic variety defined over $\bar{\mathbf{Q}}$, that admits a non-constant mapping $G \to V$ of where G is a connected positive dimensional algebraic group, then there is a number field K over which V is defined and possesses infinitely many K-rational points.

But an implication of one of Serge Lang's conjectures is that any algebraic variety V over $\bar{\mathbf{Q}}$ that does *not* contain a positive-dimensional image of an algebraic group (over $\bar{\mathbf{Q}}$) possesses only finitely many K-rational points over any number field K (over which it is defined)[2].

Following in this spirit, one might fix a number field K and ask if the following is true:

[1] Heegner points excepted, these two types of reasons don't seem to be available together. We rarely see an algebraic geometric mechanism explaining a parity prediction.

[2] A related question is the following: Let V be an algebraic variety possessing an automorphism α of infinite order (both variety and automorphism being defined over $\bar{\mathbf{Q}}$). Does V possess a non-periodic algebraic point? If so, then there will be a number field K over which V and α are defined, for which $V(K)$ is infinite. (An elementary argument shows that V does contain a non-periodic $\mathbf{C}$-valued point.)

Question 1. *Is it true that a variety V over K possesses infinitely many K-rational points if and only if there exists a connected (geometrically simple) algebraic group G over K possessing infinitely many K-rational points and a nonconstant mapping $G \to V$ defined over K?*

This lecture consists of three parts:

1. *Arithmetic Statistics.*

   Here, as in the introduction above, we will consider the general phenomenon of structure (scarcity or abundance; usually scarcity) of rational points, the average number of of rational points in certain families of curves, etc.

2. *Arithmetic Specifics.*

   In certain cases, one wants, explicitly, in contrast to general structure, the answer to some Diophantine problem, since that 'answer' tells us something we want to know about a particular mathematical issue. We might want to actually know the set of rational points on some particular curve, or a variety, because of the specific significance of each of those rational points. This happens most frequently when one is dealing with modular curves or varieties.

3. *Algorithmic issues in arithmetic.*

   Here the issues is solvability or unsolvability via algorithms, and the various modes of effectiveness.

I propose to touch on all these three facets of arithmetic.

Part I

Arithmetic Statistics

2 Hyperelliptic curves over Q

Thanks to the work of Manjul Bhargava, Benedict H. Gross, Bjorn Poonen, Arul Shankar, Michael Stoll, and Xiaoheng Wang,we are beginning to get a picture of the arithmetic statistics regarding rational points on hyperelliptic curves—i.e., curves that are double covers of curves of genus zero.

For example, consider curves C of the form $y^2 = f(x)$ where $f(x) \in \mathbf{Q}[X]$ is a polynomial with no multiple roots and of odd degree ($d \geq 5$) so C is of genus $g = (d-1)/2 > 1$. Any such curve has the property that the point at ∞ is a Weierstrass point, and—of course—then represents a rational point of the smooth projective curve C.

Here —as we shall presently see—is an *atypical family of such curves:*

$$C : y^2 = (x - a_1)(x - a_2) \dots (x - a_d) \ + \ c^2 \tag{1}$$

where the a_i are distinct rational numbers, and c is a nonzero rational number chosen such that C is smooth.There are (at least) $2d \sim 4g$ rational points on such curves C.

Fixing g and ordering isomorphism classes of hyperelliptic curves defined over $\mathbf{Q}$ by the discriminant of their defining polynomial $f(x)$, we may ask statistical questions about the set of all isomorphism classes of hyperelliptic curves:

Question 2. *Is it true that with probability* 1 *the rational point* ∞ *is the only* $\mathbf{Q}$*-rational point of* C*?*

- A theorem of Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang may be roughly interpreted as showing that most hyperelliptic curves of high genus have relatively few rational points ([B-G-W]).

- Bjorn Poonen and Michael Stoll [P-S] have shown that most odd degree hyperelliptic curves have only the one rational point ∞.
- More specifically, for $g \geq 3$ a positive portion of such curves have ∞ as their only rational point, and this proportion tends to 1 as g tends to infinity.
- Following these results, Arul Shankar and Wang show ([S-W]) that when $g \geq 9$, a positive proportion of hyperelliptic curves of genus g having *two* non-Weierstrass $\mathbf{Q}$-rational points curves have exactly those two rational points, and that this proportion tends to 1 as g tends to infinity.

This suggests that it might be interesting to frame more delicate questions making a triage in terms of numbers of rational points...

For elliptic curves, Jennifer Park, Bjorn Poonen, John Voight, and Melanie Wood have shored up some possible evidence (by a heuristic argument) for the remarkable guess (originally made by Honda for families of quadratic twists of a single elliptic curve) that there is a finite upper bound to the Mordell-Weil ranks of all elliptic curves over $\mathbf{Q}$. See [P-P-V-W]. Moroever, they conjecture that the maximal rank is quite small.

3 Uniformity Conjectures

Older results—based on conjectures—also imply that there's a striking paucity of K-rational points on curves (hyperelliptic or not) of genus > 1. For example, Lucia Caporaso, Joe Harris, and I conjecture the following (which itself is an implication of [SLC], the *Strong Lang Conjecture*):

Conjecture 1. *Let $g > 1$. There is a (finite) bound $N(g)$ with the property that for every number field K only finitely many curves of genus g defined over K have more than $N(g)$ K-rational points.*

For this, see [C-H-M] and note that there is an error in this article pointed out to us by Jakob Stix; a correction will be on archiv soon.

The curious point here is that $N(g)$ doesn't even depend on the field K. Of course, such a consequence of [SLC] might force one to have second thoughts about the likelihood of [SLC], and hence of Conjecture 1, being true. But let us continue this discussion supposing that Conjecture 1 does hold, and that the following limit is finite:

$$N(g) := \max_{K \subset \bar{\mathbf{Q}}} \quad \limsup_{C\text{: curves over } K \text{ of genus } g} |C(K)|. \tag{2}$$

By considering the curves given in Equation 1 alone, we see that $N(g) \geq 4g+4$ if $g > 1$, but not much more is known in the way of lower bounds; less, of course, is known in the way of upper bounds. The record lower bounds for genus 2 and 3, so far are: $N(2) \geq 226$ (cf: Genya Zaytman [Z]) and $N(3) \geq 100$ (cf: Noam Elkies [E]).

Can one find a lower bound for $N(4)$ that beats $4 \times 4 + 4 = 20$?

Defining $\nu := \limsup N(g)/g$ so that $4 \leq \nu \leq +\infty$ we might ask:

Question 3. *Is ν finite? Is it 4?*

Conjecture 1 implies that the 'average number of points' on a curve of genus $g > 1$ is bounded. That is, ordering the set $\mathcal{C}$ of K-isomorphism classes of (projective smooth) curves of genus g in any way:

$$\mathcal{C} = \{C_1, C_2, \dots\}$$

the Strong Lang Conjecture implies that the 'average number' is finite; i.e.,we have:

$$\lambda(g, K) := \limsup_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} |C_i(K)| \quad \leq \quad N(g) < +\infty.$$

To be sure, this 'average number', $\lambda(g, K)$, may depend on the ordering, so it would be only reasonable to ask such questions ordering the curves C_i in some natural way.

Question 4. *Might $\lambda(g, K)$ simply be 0?*

4 Diophantine Stability

Say that a variety V defined over K is **diophantine stable** (cf. [M-R]) 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.

Proposition 1. *Assume Conjecture 1. Let K be a number field and $g > 1$. Then for any Galois extension L/K with simple Galois group of sufficiently large order (i.e., of order $|\mathrm{Gal}(L/K)| \gg_K 0$) only finitely many curves of genus g defined over K are diophantine unstable for the extension L/K.*

We include the possibility that $\mathrm{Gal}(L/K)$ is cyclic of prime order.

Proof: Any nontrivial action of a simple group G on a set of cardinality n defines an embedding of G in the symmetric group on n letters, forcing $|G| \leq n!$. Assume SLC and therefore that $N(g)$, as in Equation 2 of Section 3. is finite. Let $G = \mathrm{Gal}(L/K)$ and assume that G is simple and $|G| > N(g)!$. Let C be any K-rational curve of genus g that is not diophantine stable for L/K. Any nontrivial orbit of G on $C(L)$ then contains more than $N(g)$ L-rational points, and therefore exhibits C as an L-outlier—that is, Under SLC there are only finitely many L-outliers. Consequently only finitely many curves of genus g defined over K are *diophantine unstable* for L/K.

Question 5. *Let K be a number field.*

1. *Are there Galois extensions L/K with simple Galois group of arbitrarily high order having the property that only finitely many elliptic curves defined over K of conductor prime to the discriminant of L are diophantine unstable for L/K ?*
2. *Are there Galois extensions L/K with simple Galois group of arbitrarily high order having the property that there are infinitely many elliptic curves defined over K that are diophantine unstable for L/K?*

5 Is a curve of genus g uniquely determined by its diophantine stability properties?

That diophantine instability relative to merely one such extension L/K cuts out—admittedly only conjecturally—a finite set of curves of any fixed genus $g > 1$, is suggestive to us that one might even single out a curve X unambiguously if one considers all extensions relative to which X is diophantine unstable.

More explicitly, let V be a variety over a number field K. We define, as in the paper with Karl Rubin [M-R], $\mathcal{L}(V)$ to be the set of number field extensions L/K contained in $\bar{K}/K$ which **belong to** V in the sense that there is an L-rational point of V that is rational over no proper intermediate field of the extension L/K. By the primitive element theorem any variety V over K containing a curve birationally isomorphic to $\mathbf{P}^1$ has the property that

(*) $\mathcal{L}(V)$ is the set of *all* finite field extensions of K.

One might ask about the converse:

Question 6. *If V is a geometrically irreducible smooth projective curve over a number field K, does $\mathcal{L}(V)$ determine V?*

Karl Rubin and I have at least proved ([M-R]) the following:

Theorem 2. *Let V be an irreducible projective curve over the number field K. Then every field extension L/K belongs to V if and only if V is birationally isomorphic (over K) to the projective line.*

Moreover, we show that for any curve of positive genus there are many extension fields do not belong to it:

Theorem 3. *Let X be an irreducible curve over a number field K whose normalization and completion is not of genus* 0*. Then there is a finite extension K'/K such that for any positive integer n, there are infinitely many primes ℓ where, for each of them, there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $X(K') = X(L)$.*

We show this by relating curves to abelian varieties, via their jacobians.

Our result was primarily a result about simple abelian varieties, from which we deduced the corresponding result for curves of genus ≥ 1. Suppose, then, that A is a simple abelian variety, and make a base change if necessary so that all endomorphisms of A are defined over K. For a prime power ℓ^n, let us order (by the size of the norm of their discriminant) the set of cyclic ℓ^n-extensions L/K (contained in $\bar{K}$).

We prove:

Theorem 4. *For a set of primes ℓ of positive density, and for any $n \geq 0$ there is a (positive, unfortunately) number $\alpha = \alpha(\ell)$ such that for N a positive number, among the 'first' N such cyclic extensions of K of degree ℓ^n the simple abelian variety A is diophantine stable for at least $N/\log(N)^\alpha$ of them if $N \gg 0$.*

In view of Theorem 1, a natural question to ask is:

Question 7. *Fixing a number field K Is there a bound $\ell(K, g)$ such that for any abelian variety A of dimension $\leq g$ over K and for any prime $\ell > \ell(K, g)$ there are only finitely many cyclic extensions L/K of degree ℓ with respect to which A is Diophantine Unstable?*

Examples show that—at the very least— $\ell(K, g) > g$.

Part II

Arithmetic Specifics: Rational points on modular curves

Aspects of the general problem (a variant of a problem initially posed by J.-P. Serre) regarding the action of Galois on torsion points of elliptic curves

over number fields has animated the study of *noncuspidal* K-rational points on modular curves for number fields K.

> **Question:** For a fixed number field K is there a finite bound $\ell_0(K)$ such that for every non-CM elliptic curve E over K the natural image of $\mathrm{Gal}(\bar{K}/K)$ to the automorphism group of $E[\ell]$, the kernel of multiplication by ℓ in $E(\bar{K})$, is **surjective** if ℓ is a prime $\geq \ell_0(K)$?

The issue then, has been to classify all instance of *nonsurjectivity* and specifically to classify instances where the action of Galois is contained in various subgroups of $GL_2(\mathbf{Z}/N\mathbf{Z})$. For example, to classify:

- K-rational points on the modular curve $X_1(N)$ corresponds to *pairs consisting of elliptic curves and points on them of order* N—defined over K;
- K-rational points on $X_0(N)$ correspond to *cyclic isogenies of elliptic curves* $E \to E'$ *of degree* N—defined over K.

Happily, for the ground-field $K = \mathbf{Q}$, classical theorems fully determine the answer to those two questions.

- The subtler question of $\mathbf{Q}$-rational points on

$$X_0(N)^+ = X_0(N)/\text{action of } w_N$$

  is currently tantalizing. Here w_N is the Atkin-Lehner involution.

  When N is ℓ^2, the square of a prime,

$$X_0(\ell^2)^+ = X_{\text{split Cartan}}(\ell) := X(\ell)/C_{\text{split}}(\ell),$$

  and so (noncuspidal) rational points on such a modular curve classify instances of elliptic curves over $\mathbf{Q}$ where the image of Galois is contained in a split Cartan subgroup $C_{\text{split}}(\ell)$ of $GL_2(\mathbf{Z}/\ell\mathbf{Z})$. Thanks to the results of Bilu-Parent-Rebolledo [B-P-R] who showed that there are *no* non-CM instances of this if $\ell > 7$ ($\ell \neq 13$); and thanks to Balakrishnan, Dogra, Müller, Tuitman and Vonk [B-D-M-T-V] who took care of the rather

subtle, last, case—i.e., $\ell = 13$, we have a complete understanding of the $\mathbf{Q}$-rational points of $X_{\text{split Cartan}}(\ell)$.

The question of $\mathbf{Q}$-rational points on $X_0(13)^+$ (and on $X_0(N)^+$ for other values of N *and especially in the cases where* $N = \ell$ *is prime*) is indeed subtler.

Definition 1. *A* $\mathbf{Q}$*-rational* **Galois-conjugate cyclic** N **isogeny** *for an elliptic curve* E *over a quadratic field* K *is given by a pair of isogenies*

$$\phi : E \to E'; \quad \phi' : E' \to E$$

where ϕ, ϕ' *are dual cyclic* N *isogenies defined over* K *and such that one is the Galois conjugate of the other under the Galois involution of* K*.*

The (noncuspidal) $\mathbf{Q}$-rational points on $X_0(N)^+$ are in *one-one correspondence* with $\mathbf{Q}$-rational Galois-conjugate cyclic N isogenies.[3]. Here we also allow the possibility that E, and even ϕ, be actually defined over $\mathbf{Q}$. In the latter case, no quadratic field K actually intervenes.

Remarks:

1. Note that if K is a quadratic imaginary field of class number one, and E an elliptic curve with CM by K, E will 'contribute to' $\mathbf{Q}$-rational points on $X_0(N)^+$ for infinitely many values of N—for example, for $\pi \in \mathcal{O}_K$ any prime element of degree 1 with $p := N_{K/\mathbf{Q}}(\pi)$ and

   $$\pi \in End_K(E) \subset \mathcal{O}_K,$$

   let $\phi : E \to E$ be multiplication by π; such points in $X_0(p)^+$ will be called 'CM-points.'
2. Visibly, a $\mathbf{Q}$-rational points on $X_0(N)^+$ is the image of some K-rational point on $X_0(N)$.

[3] Note that if E admits a $\mathbf{Q}$-rational Galois-conjugate cyclic N isogeny, then E itself is a quadratic elliptic $\mathbf{Q}$-curve in the following sense:

Definition 2. *An elliptic curve* E*—defined over a number field* K *that is Galois over* $\mathbf{Q}$*—is called an* **elliptic Q-curve** *if* E *is isogenous to all its Galois conjugates. It is called a* **quadratic elliptic Q-curve** *if it is defined over a quadratic field (and is isogenous to its Galois-conjugate)*

For discussion and information about elliptic $\mathbf{Q}$-curves, see, for example, [G-L].

For K ranging through quadratic number fields, here—at least roughly—is where we have stood for *the past two decades* regarding points of finite order and cyclic isogenies defined over K:

- *Regarding K-rational points on the modular curve $X_1(N)$:*

  Thanks to the work of Kenku, Momose and Kamienny, no elliptic curve over any quadratic field K has a K-rational point of prime order $p \geq 17$; for more precise information, see [K-M], [M1],[K-N].

  Theorem 5. *Let K be a quadratic field and E an elliptic curve over K. Then the torsion subgroup $E(K)_{tors}$ of $E(K)$ is isomorphic to one of the following 26 groups:*

  $\mathbf{Z}/m\mathbf{Z}$, *for* $1 \leq m \leq 18$, $m \neq 17$,
  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z}$, *for* $1 \leq m \leq 6$,
  $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3m\mathbf{Z}$, *for* $m = 1, 2$,
  $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

- *Regarding K-rational points on the modular curve $X_0(N)$:*

  Theorem 6. *Let K be a quadratic field not quadratic imaginary of class number one. Then for only finitely many primes p is there an elliptic curve over K admitting a p-isogeny defined over K.*

  (See [M2])

- *And regarding $\mathbf{Q}$-rational points on the modular curve $X_0(N)^+$:*

  Theorem 7. *Let N be a* **composite number.** *If N has a prime divisor p such that $p = 11$ or $p \neq 37$ and $p \geqq 17$, with the property that $J_0^-(p)(\mathbf{Q})$ is finite then the $\mathbf{Q}$-rational points of $X_0(N)^+$ consists of cusps and CM-points. (Here $J_0^-(p)$ is the quotient $J_0(p)/(1 + w_p)J_0(p)$ of the jacobian variety $J_0(p)$ of $X_0(p)$.)*

  See [M3], [M4].

But this still leaves open the question for general N and especially for prime values of N (in light of Theorem 7 above).

Definition 3. *By an* **unexpected Q-rational point on** $X_0(N)^+$ *let us mean a rational point that is not a cuspidal or CM (***Q****-rational) point, nor is it the image of such a point under a* **Q***-rational automorphism of* $X_0(N)^+$*.*

Question 8. *Is there a finite bound* N_o *such that for any* $N > N_o$ *the curve* $X_0(N)^+$ *has no unexpected* **Q***-rational points? For any* N *such that* $X_0(N)^+$ *is of genus* > 1*, find all unexpected* **Q***-rational points.*

(See also the discussion about this in [G].)

There has been recent exciting progress—see [B-B-C-C-E], [B-D], [B-D-M-T-V], [G]—in shaping algorithms for making Chabauty-Coleman explicit for computation, and developing the more recent methods of Chabauty-Coleman-Kim, to attack Question 8, the latter methods necessary especially for prime values of N. At a workshop this summer at Fondation des Treilles Alex Best, Francesca Bianchi, Nicholas Triantfillou, and Jan Vonk, following developed algorithms for the determination of rational points via the method of Chabauty-Coleman-Kim for—quite specifically—the six curves[4] $X_0(\ell)^+$ of genus 2, but with an eye toward shaping an effective usable and general algorithm. See their forthcoming paper *Les Treilles: Rational points on modular curves.*

Part III

Algorithmic questions about arithmetic

The fundamental starting point of such questions is "Hilbert's Tenth Problem," which can be posed for any (commutative) ring A:

Question 9. *Does there exist a finite algorithm to determine whether any finite system of polynomial equations in finitely many variables with coefficients in* A *has a solution in* A *or not?*

A basic theorem of B. Poonen and A. Shlapentokh connects Diophantine

[4] $\ell = 67, 73, 103, 107, 167, 191$

Stability for elliptic curves to issues of Diophantine *un*-solvability (cf. [P], [Shl1], [Shl2]):

Theorem 8. *(Poonen-Shlapentokh) If L/K is a finite extension of number fields and:*

- *Hilbert's Tenth Problem has a negative answer for $\mathcal{O}_K$, and*
- *there exists an elliptic curve E defined over K with positive Mordell-Weil rank (i.e., such that $E(K)$ is infinite) that is Diophantine Stable for the extension L/K,*

then Hilbert's Tenth Problem has a negative answer for $\mathcal{O}_L$.

Using this theorem (and the classical work of Julia Robinson/Davis/Putnam/ Matiyasevich) Karl Rubin and I showed that—conditional on the Shafarevich-Tate Conjecture—all number fields K (i.e., fields of finite degree over $\mathbf{Q}$) have the property that Hilbert's Tenth Problem has a negative answer for their rings of integers, $\mathcal{O}_K$. What, if anything, can one say about fields of algebraic numbers of infinite degree over $\mathbf{Q}$?

6 Rational points over large fields of algebraic numbers

Here are consequences of the results in our paper [M-R]:

Corollary 9. *Let A be any simple abelian variety over a number field K, such that all endomorphisms of A over $\bar{K}$ are defined over K. Then there are uncountably many algebraic extensions M/K, $M \subset \bar{K}$, that are Diophantine Stable for A.*

Corollary 10. *There are uncountably many fields of algebraic numbers $M \subset \bar{\mathbf{Q}}$, for which there does not exist an algorithm that determines whether or not a finite system of polynomial equations with coefficients in the ring of integers $\mathcal{O}_M$ has a solution over $\mathcal{O}_M$; that is, for which Hilbert's Tenth Problem has a negative answer.*

It is interesting to consider possible relations between the following conditions formulated for a (possibly large) subfield of algebraic numbers $M \subset \bar{\mathbf{Q}}$.

1. There exists an abelian variety A defined over M with $A(M)$ finitely generated and of positive rank.
2. There exists a finite degree extension W/M and an abelian variety A defined over W with $A(W)$ finitely generated and of positive rank.
3. There exists a variety V defined over a number field $K \subset M$ such that $V(K)$ is infinite and $V(K) = V(M)$.
4. There exists a finite degree extension W/M and a variety V defined over W such that for some a number field $K \subset W$ over which V is defined and $V(K)$ is infinite we have $V(K) = V(W)$.
5. There exists an infinite Diophantine subset of $\mathcal{O}_M$ that is also a Diophantine subset of the ring of integers in some number field contained in M.
6. Hilbert's Tenth Problem (HTP) has a negative answer for M.

Remarks:

- If (HTP) has a negative answer for a field of algebraic numbers W then it also has a negative answer for any subfield $M \subset W$ where $[W : M] < +\infty$. This follows from writing $\mathcal{O}_W$ as $\sum_{i=1}^{\nu} w_i \mathcal{O}_M$ so that any finite system of polynomial equations with coefficients in $\mathcal{O}_W$ can be converted into a finite system of polynomial equations with coefficients in $\mathcal{O}_M$. Therefore any finite algorithm to determine whether the latter system has solutions converts to a finite algorithm to determine whether the former system does. For essentially similar reasons, items (2) and (3) in Question 9 are equivalent, since if A an abelian variety over W as in (3), then the Weil Trace $B := Tr_{W/M} A$ is an abelian variety over M as in (2).
- Conditional on the Shafarevitch-Tate Conjecture, if (1) holds where A is an elliptic curve then (6) holds. It would be interesting to prove this implication in the more general case where A is an abelian variety of any dimension.

References

[B-D] J. Balakrishnan, N. Dogra, *Quadratic Chabauty and rational points I: p-adic heights:* arXiv:1601.00388v2 [math.NT]

[B-B-C-C-E] J. Balakrishnan, F.Bianchi, V. Cantoral-Farfán, M. Ciperiani, A. Etropolski, *Chabauty-Coleman experiments for genus* 3 *hyperelliptic curves*, `arXiv:1805.03361v1[math.NT]`

[B-D-M-T-V] J. Balakrishnan, N. Dogra, J. Müller, J. Tuitman, J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level* 13, `arxiv.org/abs/1711.05846v1`

[B-G-W] M. Bhargava, B. H. Gross, X. Wang, *Pencils of quadrics and the arithmetic of hyperelliptic curves*, http://arxiv.org/abs/1310.7692

[B-P-R] Y. Bilu, P. Parent, M. Rebolledo, *Rational points on* $X_0(p^r)^+$, Ann. Inst. Fourier, **63** (2013) 957-984

[C-H-M] L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc., **10** (1997) 1-5

[E] N. Elkies *Curves with many rational points*, `http://www.math.harvard.edu/~elkies/many_pts.pdf`

[G] S.D. Galbraith *Rational points on* $X_0^+(p)$, Experimental Math. **8** (1999) 311-318

[G-L] J. González, J-C. Lario, *Rational and Elliptic Parametrizations of* **Q***-Curves*, Journal of Number Theory **72** (1998) 13-31

[K-N] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields.*

[K-M] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields,* Nagoya Math. J. **109** (1988), 125-149

[M-R] B. Mazur, K. Rubin *Diophantine stability* (with an appendix by Michael Larsen), Amer. J. Math. **140** (2018) 571-616

[M1] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields,* Nagoya Math.J., **96** (1984), 139-165

[M2] F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995) 329-348

[M3] F. Momose *Rational points on the modular curves* $X_0(N)^+$, J. Math. Soc. Japan **39** (1987), no. 2, 269-286;

[M4] F. Momose, *Points on* $X_0(N)^+$ *over quadratic fields*, Acta Arith. **152** (2012), 159-173

[P-P-V-W] J. Park, B. Poonen, J. Voight, M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, arXiv:1602.01431v3 [math.NT]

[P] B. Poonen, *Using Elliptic Curves of Rank One towards the Undecidability of Hilbert's Tenth Problem over Rings of Algebraic Integers,* International Algorithmic Number Theory Symposium ANTS: Algorithmic Number Theory (2002) 33-42

[P-S] B. Poonen, M. Stoll, *Most odd degree hyperelliptic curves have only one rational point*, arXiv:1302.0061v3 [math.NT]

[S-W] A.Shankar, X. Wang, *Rational points on hyperelliptic curves having a marked non-Weierstrass point*, Compositio Math. **154** (2018). 188-222

[Shl1] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939- 962

[Shl2] A. Shlapentokh, *Hilbert's tenth problem over number fields, a survey* in: *Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 107- 137

[Z] G. Zaytman, *A genus* 2 *family with* 226 *sections*, arXiv:1110.0068v1 [math.NT]