UNIFORM BOUNDEDNESS FOR RATIONAL POINTS ON CURVES.

COLLOQUIUM DE GIORGI, SNS - DECEMBER 16, 2022

LUCIA CAPORASO

Contents

1. Rational points on curves

In this short survey, written for a general mathematician rather than a specialist, some progress about the distribution of rational points on algebraic varieties will be described by focusing on curves.

Algebraic varieties will always be defined over $\mathbb{Q}$, and hence over any field, F, in the following chain of extensions

$$\mathbb{Q} \subset \mathbb{Q}(a) \subset \overline{\mathbb{Q}} \subset \mathbb{C},$$

where $\mathbb{Q}(a)$, for some $a \in \overline{\mathbb{Q}}$, is a *number field*. Equivalently, a number field is a finite extension of $\mathbb{Q}$.

A (algebraic) variety, V, over F is a topological space endowed with a certain sheaf of functions with values in F. As F lies in $\mathbb{C}$ one can also view V over $\mathbb{C}$, as a complex variety with the standard analytic topology. A variety has thus an intrinsic double nature, an arithmetic one when considered over $\mathbb{Q}$, and a geometric one when considered over $\mathbb{C}$; the interplay between the two is a constant source of wonder.

Here V will always be projective, connected and smooth, this means that, as a complex variety, it is compact, connected, and its tangent space at every point is isomorphic to $\mathbb{C}^m$, for a fixed m equal to the dimension of V. If $m = 1$ then V is a *curve*.

The *set of F-rational points* of V is written $V(F)$. What is $V(F)$?

Suppose that V lies in some projective space $\mathbb{P}^n$, so that V is given "concretely" as the zero locus of some homogeneous polynomials in $\mathbb{Q}[x_0, \dots, x_n]$, and its points have $n + 1$ homogeneous coordinates (determined up to a nonzero multiplicative constant). Then $V(F)$ is the set of points of V

all of whose coordinates can be chosen in F; if $V = \mathbb{P}^n$ then $\mathbb{P}^n(F) = (F^{n+1} \smallsetminus \{0\})/\sim$.

Now suppose, instead, that V is given abstractly, not in any projective space. Notice first that, quite naturally, a "point over F" is a basic algebraic variety: its underlying topological space is a point, and its sheaf of functions is F; this variety is denoted by $\operatorname{Spec} F$. Now $V(F)$ is defined as the set of of morphisms of algebraic varieties from $\operatorname{Spec} F$ to V, i.e. $V(F) = \operatorname{Hom}(\operatorname{Spec} F, V)$; hence rational points can be studied from the abstract point of view. Of course, this is consistent with the previous definition: if V is realized concretely in some projective space by an embedding $\phi : V \hookrightarrow \mathbb{P}^n$, then $\phi(V(F)) = \phi(V)(F)$. One thinks of $\phi(V)$ as a "model" of the abstract variety V in projective space, and plenty of such models exist.

It is a fact that the set $V(\mathbb{Q})$ is often difficult to describe, even in the concrete, and seemingly easier, set up. Let us illustrate this phenomenon on a prominent example.

For any integer $d \geq 1$ consider the curve $C_d \subset \mathbb{P}^2$ given as the zero locus of the polynomial $x_0^d + x_1^d - x_2^d$. The set of $\mathbb{Q}$-rational points of C_d is, by definition,

$$C_d(\mathbb{Q}) = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{Q}) : \; x_0^d + x_1^d - x_2^d = 0\}.$$

It is clear that $C_d(\mathbb{Q})$ contains the two points $(1:0:1), (0:1:1)$, trivial zeroes of the polynomial defining C_d. If $d = 1$ the curve is a line, and it is easily seen to have infinitely many $\mathbb{Q}$-rational points. If $d = 2$, one easily checks that $C_2(\mathbb{Q})$ contains all the pythagorean triples, so it is, again, a countably infinite set. If $d \geq 3$ the trivial solutions turn out to be the only ones; this simple statement, however, has been surprisingly hard to prove. Indeed, P. Fermat claimed it in 1637, but a much celebrated proof was obtained only in 1995 by A. Wiles, using modern methodologies and ideas, partly in collaboration with R. Taylor; see [W95], [TW95]. Summarizing

Theorem 1. *(1) If $d = 1, 2$ then $C_d(\mathbb{Q})$ is infinite.*
(2) (Wiles) *If $d \geq 3$ then $\#C(\mathbb{Q}) = 2$.*

What about the geometric properties of C_d? The set $C_d(\mathbb{C})$ has the same cardinality of $\mathbb{C}$ for every $d \geq 1$. When C_d is viewed as a complex space with the standard topology, it turns out to be a compact, connected, orientable real surface (having dimension 1 over $\mathbb{C}$ it has dimension 2 over $\mathbb{R}$); its topological genus is equal to $(d-1)(d-2)/2$. Therefore, by Wiles Theorem, $C_d(\mathbb{Q})$ is infinite if and only if the genus of C_d is equal to zero. This is an instance of the interaction between geometry and arithmetic.

Let now C be an abstract curve. The associated curve over $\mathbb{C}$ is, again, a compact, connected, orientable real surface having a certain genus $g \geq 0$; the genus of C is then defined as $g(C) = g$. The genus of a curve is its most important geometric character. If C has a model as a plane curve of degree d, we have $g(C) = (d-1)(d-2)/2$, consistently with the previous example.

What can we say about the $\mathbb{Q}$-rational points of an arbitrary curve C? To have a more complete picture, we extend the question to any number field F; notice that, obviously, $C(\mathbb{Q}) \subset C(F)$. The following statement is an answer to our question and illustrates, again, the interplay between geometry and arithmetic.

Theorem 2. *Let C be a curve of genus g over $\mathbb{Q}$.*
(1) If $g = 0, 1$ then there exists a number field F such that $\#C(F) = \infty$.
(2) (Faltings) *If $g \geq 2$ then $\#C(F)$ is finite for any number field F .*

It is hard to over-estimate the importance of the second part, which is a famous Theorem of G. Faltings, known also as the Mordell Conjecture; see [F83]. After Faltings's original proof several methods have been applied in the search for an effective bound on the cardinality of $C(F)$. Among such methods, the approach of E. Bombieri and P. Vojta, [B90], [V91], will play a role later. The departure point here is to place the abstract curve C of genus $g \geq 2$ in a suitable ambient space, other than the projective space, where some extra structure can be used. Such an ambient space is provided by the *Jacobian variety*, J_C, of C. Set-theoretically, J_C can be defined as follows

$$J_C = \frac{\text{free abelian group generated by the points of } C}{\sim}$$

where "$\sim$" is the linear equivalence, generated by setting equivalent two linear combinations of points with positive coefficients if there exists a function on C having one as set of zeroes, and the other as sets of poles (the multiplicities of zeroes and poles are the coefficients in the linear combination). Hence $J_C(F)$ is the free abelian group over $C(F)$, modulo linear equivalence.

The curve C can be placed in J_C via an *Abel-Jacobi embedding*, as follows. Fix a point p_0 of C, then the Abel-Jacobi embedding, α^{p_0}, maps a point p of C to the class of $p - p_0$ in J_C,

$$\alpha^{p_0} : C \hookrightarrow J_C; \qquad p \longmapsto [p - p_0]$$

and this map is injective (as $g \geq 2$). Of course, if p and p_0 are F-rational points of C, the image of p is an F-rational point of J_C,

It is clear from the definition that J_C is an abelian group, it is less clear, but true, that it is a projective variety over $\mathbb{Q}$, whose associated complex variety has the form $\mathbb{C}^g/\mathbb{Z}^{2g}$. This type of projective variety is called an *abelian variety*. Its rich geometric structure (where arithmetic, algebraic and analytic properties are intertwined) has been studied extensively, and notable results have been obtained about its rational points. Among them is the famous theorem of Mordell-Weil (1921-1928), which establishes that, *for any number field F, the abelian group $J_C(F)$ has finite rank*, denoted by ρ_C, so that

$$J_C(F) \cong \mathbb{Z}^{\rho_C} \oplus \text{torsion subgroup}$$

and the torsion subgroup is finite. For more on these topics see [HS].

2. Moduli spaces and uniform boundedness

Faltings theorem is about all curves of genus $g \geq 2$. Now, the set of all such curves turns out to have, itself, a remarkably interesting geometry. There exists, in fact, a notable algebraic variety, the *moduli space of smooth cures of genus* g, denoted by M_g, whose $\overline{\mathbb{Q}}$-rational points are in bijection with curves of genus g over $\overline{\mathbb{Q}}$, up to isomorphism, and the same holds for its $\mathbb{C}$-rational points. Although the geometric structure of M_g is canonical, in that it is dictated by how curves vary in families, there is an issue that makes M_g not the best tool in some applications. Namely, it is not a *fine* moduli space.

To explain this point it is better to describe a fine moduli space which sometimes, as here, replaces M_g for practical purposes. This is the moduli space, M_g^ℓ, of curves of genus g, enriched by a "level-ℓ" structure, with ℓ some large integer. There is no need to define curves with level-ℓ structures, it suffices to know they have a fine moduli space, M_g^ℓ, defined over $\mathbb{Q}$. This means that there is a "universal family of curves", $u : \mathcal{C}_g \to M_g^\ell$, and a morphism onto M_g

$$\mathcal{C}_g \xrightarrow{u} M_g^\ell \xrightarrow{p} M_g,$$

such that the map p has finite, non-empty fibers, and the fiber of u over every point $x \in M_g^\ell(\mathbb{Q})$ is a curve, $C_x := u^{-1}(x)$, defined over $\mathbb{Q}$ and isomorphic to the curve over $\overline{\mathbb{Q}}$ corresponding to the point $p(x) \in M_g$. The morphism $u : \mathcal{C}_g \to M_g^\ell$ is called "universal family of curves" because every family of curves of genus g with level-ℓ structure can be reconstructed from it by base change. In particular, every curve of genus g over any field F appears as some fiber of $\mathcal{C}_g \to M_g^\ell$.

Over the original moduli space M_g there cannot possibly exist such a universal family, because some curves have non-trivial automorphisms (which disappear when adding a level-ℓ structure); this justifies the need to introduce M_g^ℓ.

Apart from its being a fine moduli space, M_g^ℓ is similar to M_g as algebraic variety: they are both connected (and irreducible), have dimension $3g-3$, and are not projective (not compact in the complex topology); but they admit a compactification which is itself a fine moduli space for curves with mild singularities. There is no need to further describe it here.

The general theory of moduli spaces provides also a "universal Jacobian variety", $v : \mathcal{J}_g \to M_g^\ell$, whose fiber over the point x is the Jacobian, J_{C_x}, of the fiber, C_x, of u over x. There is even a universal Abel-Jacobi mapping, expressed as follows

$$\alpha_g : \mathcal{C}_g \times_{M_g^\ell} \mathcal{C}_g \longrightarrow \mathcal{J}_g.$$

The morphism α_g glues together all the Abel-Jacobi maps of the single curves; in other words, if C_x is the fiber of u over the point x, and $p_0 \in C_x$, then the restriction of α_g

$$(\alpha_g)_{|p_0 \times C_x} : \{p_0\} \times C_x \longrightarrow J_{C_x}$$

is the Abel-Jacobi map, α^{p_0}, of the curve C_x with fixed point p_0, defined earlier. More details can be found in [GIT].

The fact that all curves of genus $g \geq 2$, over all our fields, are so well organized in a unique algebraic variety elicits the question on whether rational points on curves be also well organized. If F is a number field, by Faltings Theorem every such curve has only a finite set of F-rational points; if these sets were well organized, they might even have bounded cardinality. The following is a well known, open conjecture addressing this type of problems.

Conjecture 1 (Strong Uniformity Conjecture). *For every $g \geq 2$ there exists a number $N(g)$ such that, for every number field F,*

$$\#C(F) \leq N(g)$$

for all but finitely many curves C of genus g over F.

Notice that the conjecture will be trivially false without the last phrase allowing finitely many exceptions, which must depend on the field F.

The last years have seen important advances around these issues; see [G21] for a survey with an exhaustive bibliography. Most recently, some remarkable breakthroughs have been obtained by V. Dimitrov, Z. Gao, P. Habbegger and L. Khüne; see [DGH21] and [K21]. The next theorem summarizes them together.

Theorem 3 (Dimitrov-Gao-Habbegger, Khüne). *For every $g \geq 2$ there exists a number $c(g) \geq 1$ such that for every curve C of genus g over a number field F the set of its F-rational points satisfies*

$$\#C(F) \leq c(g)^{1+\rho_C},$$

where $\rho_C = \mathrm{rk} J_C(F)$.

The number $c(g)$ depends only on g. By the Mordell-Weil theorem, ρ_C is finite, but it may depend on F, or on the degree of F ove $\mathbb{Q}$. The proof is based on extending over the moduli spaces the approach described earlier to prove the Mordell conjecture. As illustrated, the theory of moduli spaces provides universal families of curves, universal Jacobians, and universal Abel-Jacobi maps, and hence a unified setting to treat rational points simultaneously for all curves of given genus, over any field. There is much more to the proof in terms of new tools and ideas which is not described here, an important example is the Betti map for abelian varieties, of [ACZ20]; a detailed expository account is in [G21].

3. Varieties of higher dimension and uniformity

Not much is known about rational points over number fields of varieties of higher dimension. But there is a connection between their distribution and their uniform boundedness on curves.

To be able to illustrate this connection, the property ensuring that a curve has only finitely many rational points, i.e. having genus at least 2, needs to be generalized to arbitrary dimension. This requires looking at the cotangent bundle of the variety V, a vector bundle of rank equal to the dimension of V; its determinant is a line bundle called (for good reasons) the canonical bundle of V.

A curve has genus at least 2 if and only if its canonical bundle is "big", in the sense that some high power has enough sections to realize a model of the curve in projective space. This concept can be defined for varieties of any dimension: a variety V is of *general type* if some high power of its canonical bundle has enough sections to realize a model for a dense open subset of V in projective space. A curve is of general type if and only if its genus is at least 2.

For example, projective spaces and abelian varieties are not of general type. On the other hand, if $V \subset \mathbb{P}^n$ is the zero locus of a polynomial of degree d, then V is of general type if and only if $d > n + 1$.

The topology of a variety V is the *Zariski topology*, where the closed subsets are exactly the algebraic subvarieties of V. The analytic topology is thus finer than the Zariski's, it has more closed subsets. On a curve, the only proper Zariski-closed subsets are the finite ones, so one may rephrase Faltings theorem by saying that *if a curve is of general type, then its set of F-rational points is not Zariski-dense, for any number field F.* In these terms it makes sense to ask whether the same holds for varieties of higher dimension, and conjecture that *the set of F-rational points on a variety of general type is not Zariski-dense, for any number field F.* This conjecture, attributed to E. Bombieri, S. Lang and P. Vojta, is open in all dimensions greater than 1, and so is the following, stronger conjecture

Conjecture 2 (Strong Lang Conjecture)**.** *Let V be a variety of general type over $\mathbb{Q}$. Then there exists a Zariski closed subset $Z \subsetneq V$ such that for any number field F the set of F-rational points of V not lying in Z is finite.*

The connection mentioned at the beginning can now be described. Loosely speaking, it is the fact that if rational points are not Zariski-dense in varieties of general type, then they are unformly bounded on curves of genus at least 2. More precisely, Conjecture 2 implies Conjecture 1, as stated in the following Theorem.

Theorem 4. *If the Strong Lang Conjecture holds, then for every $g \geq 2$ there exists a number $N(g)$ such that for every number field F, the set of of curves C of genus g over F such that $\#C(F) > N(g)$ is finite.*

This theorem is proved in [CHM97] and [CHM22], using, again, moduli spaces of curves. The first paper actually stated the theorem, but the proof only gave, as pointed out by J. Stix, the following weaker result. Assume the Strong Lang Conjecture, then for every $g \geq 2$ there exists a number $N(g)$ such that, for every number field F, the set of $\overline{\mathbb{Q}}$-isomorphism classes of curves of genus g having more that $N(g)$ F-rational points is finite. Now, two curves may be isomorphic over $\overline{\mathbb{Q}}$ but not over $\mathbb{Q}$ and, as illustrated, the rational points of the moduli spaces M_g and M_g^ℓ parametrize only $\overline{\mathbb{Q}}$-isomorphism classes. Therefore, in [CHM22], another type of moduli spaces of curves had to be introduced to account for this elusive arithmetic issue.

References

[ACZ20] Y. André, P. Corvaja, and U. Zannier. The Betti map associated to a section of an abelian scheme (with an appendix by Z. Gao). Inv. Math., 222:161-202, 2020.

[B90] E. Bombieri. The Mordell conjecture revisited. Annali della Scuola Normale Superiore di Pisa-Classe di Scienze, 17(4):615-640, 1990.

[CHM97] L. Caporaso, J. Harris, and B. Mazur. Uniformity of rational points. J. Amer. Math. Soc., 10(1):1-35, 1997.

[CHM22] L. Caporaso, J. Harris, and B. Mazur. Uniformity of rational points: an up-date and corrections. Tunisian J. Math. 4(1): 183-201 (2022).

[DGH21] V. Dimitrov, Z. Gao, and P. Habegger. Uniformity in Mordell-Lang for curves. Ann. of Math. 194 (1):237-298, 2021.

[F83] G. Faltings. Endlichkeitssätze für Abelsche Varietäten über Zahlkörpen. Invent. Math. 73 349-366, 1983.

[G21] Z. Gao. Recent developments of the Uniform Mordell-Lang Conjecture. Preprint arXiv: 2104.03431, 2021.

[HS] M. Hindry and J.H. Silverman. Diophantine Geometry An Introduction. Graduate Texts in Mathematics 201 Springer, 2000.

[K21] L. Kühne. Equidistribution in families of abelian varieties and uniformity. Preprint arXiv: 2101.10272, 2021.

[L86] S. Lang. Hyperbolic and diophantine analysis. Bull. Amer. Math. Soc. 14 , No. 2 p. 159-205, 1986.

[M86] B. Mazur. Arithmetic on curves. Bulletin of the AMS Volume 14, Number 2, 1986.

[GIT] D. Mumford, J. Forgarty, and F. Kirwan. Geometric Invariant Theory. Third edition Ergebnisse der Mathematik 34 Springer 1994.

[TW95] R. Taylor, A. Wiles. Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2) 141 (1995) no. 3, 553-572, 1995.

[V91] P. Vojta. Siegel's theorem in the compact case. Ann. of Math. (2), 133(3):509 - 548, 1991.

[W95] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. Ann. of Math. (2) 141 (1995), no. 3, 443-551.

(Caporaso) Dipartimento di Matematica e Fisica, Università Roma Tre, Largo San Leonardo Murialdo, I-00146 Roma, Italy

Email address: `caporaso@mat.uniroma3.it`