BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 58, Number 1, January 2021, Pages 45–56
https://doi.org/10.1090/bull/1707
Article electronically published on September 7, 2020

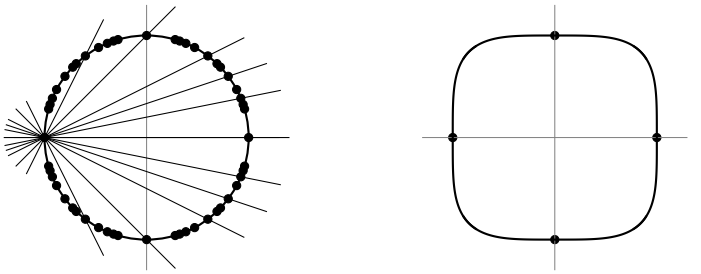
A p-ADIC APPROACH TO RATIONAL POINTS ON CURVES

BJORN POONEN

Abstract. In 1922 Mordell conjectured the striking statement that, for a polynomial equation $f(x, y) = 0$, if the topology of the set of complex number solutions is complicated enough, then the set of rational number solutions is finite. This was proved by Faltings in 1983 and again by a different method by Vojta in 1991. But neither proof provided a way to provably find all the rational solutions, so the search for other proofs has continued. Recently, Lawrence and Venkatesh found a third proof, relying on variation in families of p-adic Galois representations; this is the subject of the present exposition.

1. The Mordell conjecture

1.1. **Rational points on curves.** The equation $x^2 + y^2 = z^2$ has infinitely many solutions in integers satisfying $\gcd(x, y, z) = 1$. Equivalently, the circle $x^2 + y^2 = 1$ has infinitely many *rational* points ($(3/5, 4/5)$, $(5/13, 12/13)$, etc.). This can be understood geometrically: each line through $(-1, 0)$ with rational slope intersects the circle at one other point, which must have rational coordinates since finding its coordinates amounts to solving a quadratic equation over $\mathbb{Q}$ for which one rational root is already known; see Figure 1. The same argument shows that any nonsingular conic section defined by a polynomial with rational coefficients having one rational point has infinitely many.



$x^2 + y^2 = 1$ $\qquad$ $x^4 + y^4 = 1$

Figure 1

Received by the editors June 6, 2020.
2010 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G20, 14D07, 14D10, 14G05, 14H25.
Key words and phrases. Mordell conjecture, curve, rational point, genus, p-adic number, Galois representation.
This article is associated with a lecture given January 17, 2020, in the Current Events Bulletin at the 2020 Joint Mathematics Meetings in Denver. The writing of this article was supported in part by National Science Foundation grant DMS-1601946 and Simons Foundation grants #402472 (to Bjorn Poonen) and #550033.

In contrast, Fermat proved that the equation $x^4+y^4=z^4$ has no positive integer solutions. Equivalently, the set of rational points on the plane curve $x^4+y^4=1$ is $\{(\pm 1,0),(0,\pm 1)\}$. What about $x^4+y^4=17$? It turns out that it too has only finitely many rational points. (They are $(\pm 2,\pm 1)$ and $(\pm 1,\pm 2)$ [FW01].) More generally, for any fixed $d \geq 4$ and $a \in \mathbb{Q}^\times$, the curve $x^d+y^d=a$ has only finitely many rational points. All these finiteness claims are instances of the *Mordell conjecture*, which states that a "complicated enough" curve has only finitely many rational points, if any at all.

In the previous paragraph, the condition $d \geq 4$ is what made the curve "complicated enough". To state the Mordell conjecture fully, however, we need to consider also curves defined by several polynomials in higher-dimensional space and to introduce the notion of genus to measure their geometric complexity.

1.2. **Projective space.** Let k be a field and let $n \in \mathbb{Z}_{\geq 0}$. The set of k-points on n-dimensional *affine space* is $\mathbb{A}^n(k) := k^n$.

Define an equivalence relation $\sim$ on $k^{n+1}-\{\vec{0}\}$ by $(a_0,\ldots,a_n) \sim (\lambda a_0,\ldots,\lambda a_n)$ for all $\lambda \in k^\times$. Let $(a_0 : \cdots : a_n)$ denote the equivalence class of $(a_0,\ldots,a_n)$. The set of all such equivalence classes is the set

$$\mathbb{P}^n(k) := \frac{k^{n+1}-\{\vec{0}\}}{k^\times}$$

of k-points on n-dimensional *projective space*.

The points $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$ with $a_0 \neq 0$ have a unique representative of the form $(1, a_1, \ldots, a_n)$, so they form a copy of $\mathbb{A}^n(k)$. For each i, the same holds for the points with $a_i \neq 0$. Moreover, $\mathbb{P}^n(k)$ is the union of these $n+1$ overlapping copies of $\mathbb{A}^n(k)$.

One advantage of projective space over affine space is that $\mathbb{P}^n(\mathbb{R})$ is compact for the topology coming from the Euclidean topology on each $\mathbb{R}^n$; similarly, $\mathbb{P}^n(\mathbb{C})$ is compact. Related to this is that intersection theory works better in projective space: for example, two distinct lines in $\mathbb{P}^2(k)$ always meet in exactly one point.

1.3. **Projective varieties.** A finite list of polynomials $f_1,\ldots,f_m \in k[x_1,\ldots,x_n]$ defines an *affine variety*[1] $X \subset \mathbb{A}^n$ whose set of k-points is

$$X(k) := \{\vec{a} \in \mathbb{A}^n(k) : f_1(\vec{a}) = \cdots = f_m(\vec{a}) = 0\}.$$

But for a point $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$, a polynomial condition $f(\vec{a})=0$ does not necessarily make sense; to make sure that it is unchanged by scaling $\vec{a}$, we assume that f is *homogeneous*, a sum of monomials of the same total degree, such as $x_0^5x_1^2 - x_0^4x_1^3 + 9x_1^7$ of degree 7. A finite list of homogeneous polynomials $f_1,\ldots,f_m \in k[x_0,\ldots,x_n]$ defines a *projective variety* $X \subset \mathbb{P}^n$ whose set of k-points is

$$X(k) := \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(k) : f_1(\vec{a}) = \cdots = f_m(\vec{a}) = 0\}.$$

The decomposition of $\mathbb{P}^n$ as a union of $n+1$ copies of $\mathbb{A}^n$ restricts to express X as a union of $n+1$ affine varieties called *affine patches*. For each i, dehomogenizing $f_1,\ldots,f_m$ by setting x_i equal to 1 gives polynomials cutting out the ith affine patch in $\mathbb{A}^n$.

[1]Some people require a variety to satisfy additional conditions, such as not being a union of two strictly smaller such varieties.

1.4. **Smooth varieties.** If a variety $Y \subset \mathbb{A}^n$ is defined by $f_1, \dots, f_{n-r}$ such that for every field extension $L \supset k$ and point $\vec{a} \in Y(L)$, the matrix $\left(\left(\frac{\partial f_i}{\partial x_j}\right)(\vec{a})\right) \in \mathrm{M}_{n-r,n}(L)$ has rank $n-r$, then we call Y *obviously smooth of dimension* r; the rank condition is the same as the Jacobian criterion in the implicit function theorem. More generally, any affine or projective variety X is called *smooth of dimension* r if (in a sense we will not make precise) it can be covered by subvarieties isomorphic to obviously smooth varieties Y as above.

If X is smooth of dimension r over $\mathbb{R}$, then $X(\mathbb{R})$ is a smooth $\mathbb{R}$-manifold of dimension r. The same holds if $\mathbb{R}$ is replaced by $\mathbb{C}$ in all three places.

1.5. **Genus of a curve.** From now on, we consider a smooth projective curve X over $\mathbb{Q}$, that is, a projective variety over $\mathbb{Q}$ that is smooth of dimension 1. We assume, moreover, that X is *geometrically connected*, meaning that the variety defined by the same polynomials over an algebraically closed extension field (such as $\mathbb{C}$) is nonempty and not the disjoint union of two strictly smaller varieties. Then $X(\mathbb{C})$ is a compact connected one-dimensional $\mathbb{C}$-manifold, that is, a compact Riemann surface. Forgetting the complex structure, we find that $X(\mathbb{C})$ is a compact connected oriented two-dimensional real manifold; by the classification of such, $X(\mathbb{C})$ is homeomorphic to a g-holed torus for some $g \in \mathbb{Z}_{\geq 0}$. The integer g is called the *genus* of X. It measures the geometric complexity of X.

Remark 1.1. It turns out that g also equals the dimension of the space of holomorphic 1-forms on $X(\mathbb{C})$. One can also define g algebraically, either by using Kähler differentials in place of holomorphic forms or by computing the dimension of a sheaf cohomology group $\mathrm{H}^1(X, \mathscr{O}_X)$.

Example 1.2 (The Riemann sphere)**.** If $X = \mathbb{P}^1$, then the space $X(\mathbb{C}) = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ is homeomorphic to a sphere via (the inverse of) stereographic projection. Thus $g = 0$.

Example 1.3 (Plane curves)**.** If $X \subset \mathbb{P}^2$ is a smooth projective curve defined by a degree d homogeneous polynomial, then it turns out that $g = (d-1)(d-2)/2$.

Example 1.4 (Conic sections)**.** A nondegenerate conic section is a smooth curve of degree 2 in $\mathbb{P}^2$. By Example 1.3, it is of genus 0.

Example 1.5 (Elliptic curves)**.** An *elliptic curve* is a smooth degree 3 curve $y^2z - x^3 - Axz^2 - Bz^3 = 0$ in $\mathbb{P}^2$ for some numbers $A, B \in \mathbb{Q}$. (Dehomogenizing by setting $z = 1$ gives the equation $y^2 = x^3 + Ax + B$ for one affine patch.) By Example 1.3, an elliptic curve is of genus 1.

Example 1.6 (Hyperelliptic curves)**.** Let $f(x) \in \mathbb{Q}[x]$ be a nonconstant polynomial with no repeated factors. Then $y^2 = f(x)$ defines a smooth curve in $\mathbb{A}^2$. It is isomorphic to an affine patch of some smooth projective geometrically connected curve X. If f has degree $2g+1$ or $2g+2$, then the genus of X is g.

Remark 1.7. The problem of determining the rational points on a general curve can be reduced to the problem for a smooth projective geometrically connected curve (cf. [Poo17, Remark 2.3.27]). That is why it suffices to consider only the latter.

1.6. **The conjecture.**

Mordell conjecture ([Mor22], first proved in [Fal83])**.** *Let X be a smooth projective geometrically connected curve of genus g over $\mathbb{Q}$. If $g > 1$, then $X(\mathbb{Q})$ is finite.*

Remark 1.8. One can say qualitatively what happens for curves of genus 0 and 1 as well:

Genus g	$X(\mathbb{Q})$	Some examples
0	infinite, if nonempty	lines and conics[2]
1	can be finite or infinite	elliptic curves, ...
> 1	finite	plane curves of degree ≥ 4, ...

Several proofs of the Mordell conjecture are known, none of them easy:

- Faltings [Fal83] proved the conjecture in 1983 using methods from Arakelov theory, a kind of arithmetic intersection theory that combines number-theoretic data with complex-analytic data.
- Vojta [Voj91] gave a completely different proof based on diophantine approximation, a theory whose original goal was to quantify how closely irrational algebraic numbers such as $\sqrt[3]{2}$ could be approximated by rational numbers with denominator of at most a certain size. For a more elementary variant of Vojta's proof due to Bombieri, see [Bom90] or [HS00].
- Lawrence and Venkatesh [LV19] recently gave yet another proof. Their proof shares some ingredients with Faltings's but replaces the most difficult steps by arguments involving p-adic Hodge theory. The rest of this article is devoted to explaining some of the ideas underlying their proof.

Remark 1.9. All of these proofs generalize to the case of curves defined over number fields instead of just $\mathbb{Q}$. (A *number field* is a finite field extension over $\mathbb{Q}$, such as $\mathbb{Q}(\sqrt{5})$.)

Remark 1.10. Although the Lawrence–Venkatesh proof is the first *complete* proof of the Mordell conjecture using p-adic methods, older p-adic approaches have given partial results. Chabauty [Cha41] gave a proof for X satisfying an additional hypothesis, namely $\operatorname{rank} J(\mathbb{Q}) < g$ for a certain projective group variety J associated to X, the *Jacobian*. More recently, Kim [Kim05, Kim09] proposed a sophisticated extension of Chabauty's ideas, using the nilpotent fundamental group of X as a substitute for J. He proved that his approach combined with well-known conjectures would imply the Mordell conjecture. Kim's approach has already led to the explicit determination of $X(\mathbb{Q})$ for some X outside the reach of previous methods [BDMTV19], and it may be that Kim's approach succeeds for every X of genus > 1.

Remark 1.11. All the proofs so far are ineffective: they do not prove that there is an algorithm that takes as input the list of polynomials defining a curve X of genus > 1 and outputs the list of all rational points on X. At best they give a computable upper bound on $\#X(\mathbb{Q})$ in terms of X. See [Poo02] for more about the algorithmic problem.

[2]In fact, every genus 0 curve is isomorphic to one of these.

2. Overall strategy of the Lawrence–Venkatesh proof

Here let us outline the strategy of Lawrence and Venkatesh, while postponing definitions and details to later sections.

Let X be a smooth projective geometrically connected curve of genus > 1 over $\mathbb{Q}$. Lawrence and Venkatesh use two maps of sets

$$X(\mathbb{Q}) \xrightarrow{\mathrm{KP}} \{\text{curves}\} \xrightarrow{\mathrm{H}^1_{\mathrm{et}}} \{\mathbb{Q}_p\text{-representations of } G_{\mathbb{Q}}\}, \tag{1}$$

where each of the last two sets is really a set of isomorphism classes.

- The map KP sends a rational point $x \in X(\mathbb{Q})$ to a curve Y_x over $\mathbb{Q}$; the curves Y_x are the fibers of a surjective morphism $Y \to X$ for some *two-dimensional* variety Y defined in section 3. (*Fiber* means the inverse image of a point. KP stands for Kodaira and Parshin, who constructed certain $Y \to X$ for studying the Mordell conjecture [Par71].)
- The map $\mathrm{H}^1_{\mathrm{et}}$ sends each curve to its étale cohomology; see section 4.

Let $\mathscr{V}$ be the composition of the two maps. To complete the proof that $X(\mathbb{Q})$ is finite, Lawrence and Venkatesh prove that $\mathscr{V}$ has finite image and finite fibers; see section 5.

3. A family of curves

In this section, we construct the algebraic family of curves $Y \to X$.

3.1. **Fundamental group of a punctured Riemann surface.** For now, let X be a compact Riemann surface of genus g. Because X is homeomorphic to a $4g$-gon with edges glued appropriately, the Seifert–van Kampen theorem implies that the fundamental group of X (with respect to any basepoint) has a presentation

$$\pi_1(X) \simeq \left\langle a_1, b_1, \dots, a_g, b_g \;\middle|\; [a_1, b_1] \cdots [a_g, b_g] \right\rangle,$$

where $[a, b] := aba^{-1}b^{-1}$; that is, $\pi_1(X)$ is the quotient of a free group on $2g$ generators by the smallest normal subgroup containing the indicated product of g commutators. More generally, if B is a finite subset of X of size r, then

$$\pi_1(X - B) \simeq \left\langle a_1, b_1, \dots, a_g, b_g, c_1, \dots, c_r \;\middle|\; [a_1, b_1] \cdots [a_g, b_g] c_1 \cdots c_r \right\rangle.$$

3.2. **Analytic construction of a family of ramified covers.** Now fix X and a finite group G. Let $x \in X$. A surjective homomorphism $\pi_1(X - \{x\}) \overset{\alpha}{\twoheadrightarrow} G$ defines a finite covering space of $X - \{x\}$, and it can be completed to a finite *ramified* covering $Y_{x,\alpha} \to X$, with some branches possibly coming together above $x \in X$.

This covering depends on α, but there are only finitely many α since $\pi_1(X - \{x\})$ is finitely generated. To obtain a space not depending on a choice of any one α, define the finite disjoint union $Y_x := \coprod_\alpha Y_{x,\alpha}$, which is a disconnected ramified covering of X.[3] As x varies, the Y_x vary continuously in a family. The total space of this family is a two-dimensional compact complex manifold Y with a proper submersion $\phi\colon Y \to X$ such that $\phi^{-1}(x) = Y_x$ for each $x \in X$; see Figure 2.

[3]Lawrence and Venkatesh use a variant in which G has trivial center and the disjoint union is over *conjugacy classes* of surjective homomorphisms α; this makes sense since the isomorphism type of $Y_{x,\alpha}$ depends only on the conjugacy class.

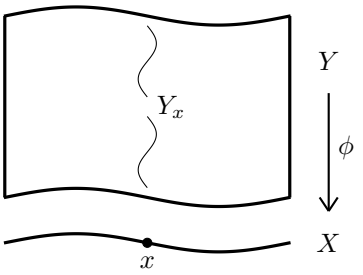


FIGURE 2

3.3. **An algebraic family of curves.** The constructions above can be made algebraic, in the following sense. Suppose that X is a smooth projective connected curve over $\mathbb{C}$. Then by the Riemann existence theorem, $Y_{x,\alpha} \to X$ arises from an algebraic morphism of algebraic curves. Moreover, there is a two-dimensional variety Y with a morphism $\phi\colon Y \to X$ whose fibers are the disconnected curves $Y_x = \coprod_\alpha Y_{x,\alpha}$.

Even better, the construction is canonical enough that if X is defined over $\mathbb{Q}$, then $\phi\colon Y \to X$ can be defined over $\mathbb{Q}$. This is called a *Kodaira–Parshin family*; see [LV19, §7] for details.

Remark 3.1. The curve X is playing two roles: it is the base of the family $Y \to X$, but also each fiber Y_x is a ramified covering of X.

4. Galois representations

The Lawrence–Venkatesh proof makes essential use of p-adic Galois representations. Therefore, in this section we define $\mathbb{Q}_p$, define the absolute Galois group of a field, and give examples and properties of $\mathbb{Q}_p$-representations of the absolute Galois group of $\mathbb{Q}$.

4.1. **The field of p-adic numbers.** Let p be a prime number. The *ring of p-adic integers* is the inverse limit $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Thus an element of $\mathbb{Z}_p$ is a sequence $(a_1, a_2, \ldots)$ where the elements $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ are compatible in the sense that the natural homomorphism $\mathbb{Z}/p^{n+1}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ maps a_{n+1} to a_n for each n. For example,

$$(3 \bmod 5,\ 13 \bmod 5^2,\ 38 \bmod 5^3,\ \ldots) \in \mathbb{Z}_5.$$

As a ring, $\mathbb{Z}_p$ is a domain of characteristic 0. Its fraction field, denoted $\mathbb{Q}_p$, is called the *field of p-adic numbers*.

For each $n \geq 1$, the homomorphism $\pi_n\colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ sending $(a_1, a_2, \ldots)$ to a_n is surjective with kernel $p^n\mathbb{Z}_p$. The kernel of $\pi_1\colon \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is the unique maximal ideal $p\mathbb{Z}_p$ of $\mathbb{Z}_p$. The collection of subsets $\pi_n^{-1}(a)$ for all $n \in \mathbb{Z}_{\geq 1}$ and $a \in \mathbb{Z}/p^n\mathbb{Z}$ is a basis of a topology on $\mathbb{Z}_p$. Equip $\mathbb{Q}_p$ with the unique topology making it a topological group having $\mathbb{Z}_p$ as an open subgroup.

Remark 4.1. Here we explain an alternative construction of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ and their topologies, producing the same results. The *p-adic absolute value on* $\mathbb{Q}$ is characterized by $\left|p^n \frac{a}{b}\right|_p := p^{-n}$ whenever $a, b, n \in \mathbb{Z}$ and $p \nmid a, b$; thus a rational number is p-adically small if its numerator is divisible by a large power of p. Define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to $|\ |_p$, just as $\mathbb{R}$ is the completion of $\mathbb{Q}$ with

respect to the standard absolute value. Then $|\ |_p$ extends to an absolute value on $\mathbb{Q}_p$. Define $\mathbb{Z}_p$ as the closed unit disk $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Finally, $|\ |_p$ induces a metric on $\mathbb{Q}_p$, which defines a topology on $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Working with $\mathbb{Z}_p$ or $\mathbb{Q}_p$ amounts to working with infinitely many congruences at once, but passing to the limit has advantages. One is that one can work over a domain or field of characteristic 0. Another is that some ideas from analysis over $\mathbb{R}$ have analogues for $\mathbb{Q}_p$.

Whereas number fields such as $\mathbb{Q}$ are examples of what are called *global fields*, $\mathbb{Q}_p$ is an example of a *local field*. For a more detailed introduction to p-adic numbers, see [Kob84].

4.2. **The absolute Galois group of $\mathbb{Q}$.** A complex number is *algebraic* over $\mathbb{Q}$ if it is a zero of some nonzero polynomial in $\mathbb{Q}[x]$. The set of all algebraic numbers is a subfield $\overline{\mathbb{Q}}$ of $\mathbb{C}$, called an *algebraic closure* of $\mathbb{Q}$.

Now let K be a subfield of $\overline{\mathbb{Q}}$. Call $K \supset \mathbb{Q}$ a *finite extension* if $\dim_{\mathbb{Q}} K$ is finite. Call $K \supset \mathbb{Q}$ a *Galois extension* if it is generated by the set of *all* zeros of some collection of polynomials in $\mathbb{Q}[x]$.[4] For example, $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$, but $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2}, e^{4\pi i/3}\sqrt[3]{2})$ is. The field $\overline{\mathbb{Q}}$ is the union of its finite Galois subextensions K.

For a Galois extension $K \supset \mathbb{Q}$, the *Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ is the set of automorphisms of K that fix $\mathbb{Q}$ pointwise.[5] The *absolute Galois group* of $\mathbb{Q}$ is $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Each automorphism of $\overline{\mathbb{Q}}$ restricts to give an automorphism of each finite Galois subextension K, and any compatible collection of such automorphisms defines an automorphism of $\overline{\mathbb{Q}}$, so

$$G_{\mathbb{Q}} \simeq \varprojlim_{\text{finite Galois } K \supset \mathbb{Q}} \mathrm{Gal}(K/\mathbb{Q}).$$

Just as the inverse limit $\mathbb{Z}_p$ had a topology, the inverse limit $G_{\mathbb{Q}}$ has a topology.

Remark 4.2. More generally, for any field F, one can construct a field $\overline{F}$ and topological group G_F.

4.3. **Global p-adic Galois representations.** Let V be a finite-dimensional $\mathbb{Q}_p$-vector space. If $\dim V = r$, then $\mathrm{Aut}\, V \simeq \mathrm{GL}_r(\mathbb{Q}_p)$, which has a topology coming from the topology of $\mathbb{Q}_p$. Call a $\mathbb{Q}_p$-linear action of $G_{\mathbb{Q}}$ on V *continuous* if the homomorphism $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}\, V$ defined by the action is continuous. By a *$\mathbb{Q}_p$-representation of $G_{\mathbb{Q}}$* we mean a finite-dimensional $\mathbb{Q}_p$-vector space V equipped with a continuous action of $G_{\mathbb{Q}}$. In the next few sections, we give examples of such representations arising in number theory and arithmetic geometry.

4.4. **The cyclotomic character.** Let m be a positive integer. Define

$$\mu_m := \{z \in \overline{\mathbb{Q}} : z^m = 1\},$$

which under multiplication is a cyclic group of order m. Thus μ_m is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 1. The group $G_{\mathbb{Q}}$ acts on the group μ_m.

Now fix a prime p, and let m range through the powers of p. Form the inverse limit

$$T := \varprojlim \mu_{p^n}$$

[4]For a definition that works over an arbitrary ground field k instead of $\mathbb{Q}$, one should require each polynomial to have distinct zeros in $\overline{k}$.

[5]Fixing $\mathbb{Q}$ pointwise is automatic; this condition becomes relevant only over other ground fields.

with respect to the homomorphisms $\mu_{p^{n+1}} \twoheadrightarrow \mu_{p^n}$ sending ζ to ζ^p. Then T is a free rank 1 module under the ring $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, and $G_{\mathbb{Q}}$ acts on T.

Next let

$$V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Then V is a one-dimensional $\mathbb{Q}_p$-vector space, and $G_{\mathbb{Q}}$ acts on V. It follows from the definitions that the action is continuous, so V is a one-dimensional $\mathbb{Q}_p$-representation of $G_{\mathbb{Q}}$; it is called the *cyclotomic character*.

4.5. **Galois representations associated to elliptic curves.** Let E be an elliptic curve over $\mathbb{Q}$. It turns out that E is a group variety; in particular, there is a map of varieties $E \times E \to E$ making $E(\overline{\mathbb{Q}})$ an abelian group. If $P \in E(\overline{\mathbb{Q}})$, we may use this group law to define $3P := P + P + P$ and so on. For each $m \geq 1$, it turns out that the *m-torsion subgroup*

$$E[m] := \{P \in E(\overline{\mathbb{Q}}) : mP = 0\}$$

is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2. Therefore the inverse limit

$$T_pE := \varprojlim E[p^n]$$

(with respect to the homomorphisms $E[p^{n+1}] \to E[p^n]$ sending P to pP) is a free $\mathbb{Z}_p$-module of rank 2, called a *Tate module*. Next,

$$V_pE := T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is a two-dimensional $\mathbb{Q}_p$-vector space. The continuous action of $G_{\mathbb{Q}}$ on $E(\overline{\mathbb{Q}})$ induces continuous actions on $E[p^n]$, T_pE, and V_pE. Thus V_pE is a two-dimensional $\mathbb{Q}_p$-representation of $G_{\mathbb{Q}}$.

4.6. **Galois representations associated to higher-genus curves.** Let X be a smooth projective geometrically connected curve of genus g over $\mathbb{Q}$. If $g \neq 1$, there is no group law $X \times X \to X$, but the Jacobian J of X does have a group law. The construction of V_pE generalizes to produce a $2g$-dimensional $\mathbb{Q}_p$-representation V_pJ of $G_{\mathbb{Q}}$.

4.7. **Galois representations from étale cohomology.** If X is a smooth projective variety over $\mathbb{Q}$ and $i \in \mathbb{Z}_{\geq 0}$, then the *étale cohomology group* $\mathrm{H}^i(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ (which we will not attempt to define here) is a $\mathbb{Q}_p$-representation of $G_{\mathbb{Q}}$.

Example 4.3. If E is an elliptic curve, then it turns out that $\mathrm{H}^1(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ is the dual of the representation V_pE. If X and J are as in section 4.6, then $\mathrm{H}^1(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ is the dual of V_pJ.

4.8. **Semisimple representations.** Let V be a $\mathbb{Q}_p$-representation of $G_{\mathbb{Q}}$. Call V *irreducible* if $V \neq 0$ and there is no $G_{\mathbb{Q}}$-invariant subspace W with $0 \subsetneq W \subsetneq V$. Call V *semisimple* if it is a direct sum of irreducible representations. Maschke's theorem [Ser77, §1.4, Theorem 2] states that any $\mathbb{C}$-representation of a finite group is semisimple, but this is not true for $\mathbb{F}_p$-representations of a finite group of order divisible by p, and $\mathbb{Q}_p$-representations of $G_{\mathbb{Q}}$ are more like the latter in this regard: they need not be semisimple.

Example 4.4. Let $\chi\colon G_{\mathbb{Q}} \to \mathbb{Q}_p^\times$ be the cyclotomic character. There is a homomorphism $\log_p\colon \mathbb{Q}_p^\times \to \mathbb{Q}_p$ from the multiplicative group to the additive group; see [Kob84, IV.2]. Composing these yields a nontrivial continuous homomorphism $\lambda\colon G_{\mathbb{Q}} \to \mathbb{Q}_p$. Let $V := \mathbb{Q}_p \oplus \mathbb{Q}_p$, viewed as a space of column vectors. Let each

$g \in G_{\mathbb{Q}}$ act as $\begin{pmatrix} 1 & \lambda(g) \\ 0 & 1 \end{pmatrix}$ on V. The only invariant subspace of V is $\mathbb{Q}_p \oplus 0$, so V is not semisimple.

4.9. **The absolute Galois group of $\mathbb{Q}_p$.** Let $\overline{\mathbb{Q}}_p$ denote an algebraic closure of $\mathbb{Q}_p$. The homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ extends uniquely to $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and nonuniquely to $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$; fix one such embedding. Define $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. It turns out that $\overline{\mathbb{Q}}_p$ is generated by its subfields $\overline{\mathbb{Q}}$ and $\mathbb{Q}_p$, so the homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ sending each σ to $\sigma|_{\overline{\mathbb{Q}}}$ is injective. Identify $G_{\mathbb{Q}_p}$ with its image, which is called a *decomposition group* of $G_{\mathbb{Q}}$.

The absolute value $|\ |_p$ on $\mathbb{Q}_p$ extends in a unique way to $\overline{\mathbb{Q}}_p$. Let $\overline{\mathbb{Z}}_p := \{x \in \overline{\mathbb{Q}}_p : |x|_p \leq 1\}$; it is a subring. The unique maximal ideal of $\overline{\mathbb{Z}}_p$ is $\mathfrak{m} := \{x \in \overline{\mathbb{Q}}_p : |x|_p < 1\}$, and the quotient $\overline{\mathbb{Z}}_p/\mathfrak{m}$ is an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Each element of $G_{\mathbb{Q}_p}$ preserves $|\ |_p$ and hence induces an automorphism of $\overline{\mathbb{Z}}_p/\mathfrak{m}$. Thus we obtain a homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$. It is surjective, and its kernel $I_p \subset G_{\mathbb{Q}_p} \subset G_{\mathbb{Q}}$ is called an *inertia group*. To summarize, we have a diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_p & \longrightarrow & G_{\mathbb{Q}_p} & \longrightarrow & G_{\mathbb{F}_p} & \longrightarrow & 1 \\ & & & & \downarrow & & & & \\ & & & & G_{\mathbb{Q}}. & & & & \end{array}$$

The *Frobenius automorphism* $\mathrm{Frob}_p \in G_{\mathbb{F}_p}$ is the automorphism $x \mapsto x^p$ of $\overline{\mathbb{F}}_p$; it generates a dense subgroup of $G_{\mathbb{F}_p}$ since it restricts to a generator of each finite quotient $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Write Frob_p also for any element of $G_{\mathbb{Q}_p}$ mapping to $\mathrm{Frob}_p \in G_{\mathbb{F}_p}$, or for the corresponding element of $G_{\mathbb{Q}}$.

4.10. **Local Galois representations.** Let p and q be primes. (Soon we will take $q = p$.) A *$\mathbb{Q}_p$-representation of $G_{\mathbb{Q}_q}$* is a finite-dimensional $\mathbb{Q}_p$-vector space V equipped with a continuous action of $G_{\mathbb{Q}_q}$. Call V *unramified* if I_q acts trivially on V; in that case the $G_{\mathbb{Q}_q}$-action can be described by one matrix, namely the automorphism $\mathrm{Frob}_q|_V \in \mathrm{GL}(V)$ given by the action of any $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$. Given $w \in \mathbb{Z}$, call such a V *pure of weight w* if the characteristic polynomial of $\mathrm{Frob}_q|_V$ is a polynomial in $\mathbb{Z}[x]$ whose complex zeros have absolute value $q^{w/2}$.

4.11. **Properties of representations coming from geometry.** Now return to a global representation V, a $\mathbb{Q}_p$-representation of $G_{\mathbb{Q}}$. For each prime q, restricting the $G_{\mathbb{Q}}$-action to the subgroup $G_{\mathbb{Q}_q}$ yields a local representation V_q. Let S be a finite set of primes. Call V *unramified outside S* if V_q is unramified for every $q \notin S$. For $w \in \mathbb{Z}$, call such a V *pure of weight w outside S* if, in addition, V_q is pure of weight w for every $q \notin S$. These properties were introduced because they hold for representations "coming from geometry":

Theorem 4.5. *Each representation $\mathrm{H}^i(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ as in section 4.7 is unramified outside S and is pure of weight i outside S, for a suitable finite set S (cf.* [Del74, Théorème 1.6]).

Remark 4.6. One can say more about S. The variety X can be defined by polynomials with coefficients in $\mathbb{Z}$. Reducing all the coefficients of the polynomials modulo ℓ produces polynomials defining a variety over $\mathbb{F}_\ell$. For most ℓ, this variety is again smooth; more precisely, this holds for all primes ℓ outside a finite set S_0. Then in Theorem 4.5 one may take $S = S_0 \cup \{p\}$.

4.12. **Faltings's finiteness theorem for global Galois representations.** Faltings cleverly combined a few classical facts from number theory (Hermite's finiteness theorem and the Chebotarev density theorem) to prove the following finiteness statement.

Theorem 4.7 (cf. [Fal83, proof of Satz 5])**.** *Fix a nonnegative integer d, a prime p, a finite set S of primes, and an integer w. Then the set of isomorphism classes of semisimple d-dimensional $\mathbb{Q}_p$-representations of $G_{\mathbb{Q}}$ that are unramified outside S and pure of weight w outside S is finite.*

5. The Lawrence–Venkatesh proof of the Mordell conjecture

We now flesh out the sketch we gave in section 2, though we will still have to gloss over many difficult arguments.

5.1. **From rational points to representations.** Let X be a smooth projective geometrically connected curve of genus > 1 over $\mathbb{Q}$. The goal is to prove that $X(\mathbb{Q})$ is finite.

Let G be a finite group. All the claims to be made in section 5.2 will be true if G is chosen suitably. (Lawrence and Venkatesh take G to be the semidirect product $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$ for a suitable large prime q.) Let $\phi\colon Y \to X$ be the Kodaira–Parshin family of curves over X defined using G; let KP be the map sending each $x \in X(\mathbb{Q})$ to the smooth projective curve $Y_x := \phi^{-1}(x)$ over $\mathbb{Q}$. Let $\mathrm{H}^1_{\mathrm{et}}$ denote the map sending each smooth projective curve C over $\mathbb{Q}$ to the global Galois representation $\mathrm{H}^1_{\mathrm{et}}(C_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$. The composition of these, as in (1), is a map of sets $\mathscr{V}$:

$$\begin{array}{ccccc} & & \overset{\mathscr{V}}{\frown} & & \\ X(\mathbb{Q}) & \xrightarrow{\mathrm{KP}} & \{\text{curves}\} & \xrightarrow{\mathrm{H}^1_{\mathrm{et}}} & \{\mathbb{Q}_p\text{-representations of } G_{\mathbb{Q}}\} \\ x & \longmapsto & Y_x & \longmapsto & V_x := \mathrm{H}^1_{\mathrm{et}}((Y_x)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p). \end{array}$$

Now it turns out that

- the representations V_x are all of the same dimension.
- they are semisimple.[6]
- they are unramified outside a set S that is independent of x, because one can choose a set S_0 as in Remark 4.6 that works for the whole family $Y \to X$.
- they are pure of weight 1 outside S.

That is, the representations V_x satisfy all the conditions of Faltings's finiteness theorem (Theorem 4.7), so

the map $\mathscr{V}$ has finite image!

To finish the proof that $X(\mathbb{Q})$ itself is finite, one needs to show that *every fiber of $\mathscr{V}$ is finite*, i.e., that the V_x vary enough that there are only finitely many $x \in X(\mathbb{Q})$ mapping to any given isomorphism class of representations.

[6]The semisimplicity is actually a difficult theorem, proved by Faltings in his paper on the Mordell conjecture. Lawrence and Venkatesh would be "cheating" if they used this, so instead they give an independent argument using Hodge–Tate weights to prove that V_x is semisimple for all but finitely many $x \in X(\mathbb{Q})$; that is sufficient for their proof of the Mordell conjecture.

5.2. **Variation in a p-adic family of local Galois representations.** The plan is to show that the global representations V_x vary enough by showing that even their restrictions to $G_{\mathbb{Q}_p}$ vary enough. These restrictions are local Galois representations indexed by $x \in X(\mathbb{Q})$, but to study them, we view them as members of a larger family of representations, indexed by $x \in X(\mathbb{Q}_p)$. Namely, for $x \in X(\mathbb{Q}_p)$, define the local Galois representation

$$V_x := \mathrm{H}^1_{\mathrm{et}}((Y_x)_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p).$$

Then $x \mapsto V_x$ defines the map $\mathscr{V}_p$ in the following commutative diagram of sets:

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\mathscr{V}} & \{\mathbb{Q}_p\text{-representations of } G_{\mathbb{Q}}\} \\ \downarrow & & \downarrow \text{restriction} \\ X(\mathbb{Q}_p) & \xrightarrow{\mathscr{V}_p} & \{\mathbb{Q}_p\text{-representations of } G_{\mathbb{Q}_p}\}. \end{array}$$

To prove that $\mathscr{V}$ has finite fibers, it suffices to prove that $\mathscr{V}_p$ has finite fibers. That is, loosely speaking, one must show that the local representation V_x varies enough as x ranges over $X(\mathbb{Q}_p)$; it is this claim that a large part of the Lawrence–Venkatesh article is devoted to. Its proof proceeds as follows:

- First, p-adic Hodge theory relates the variation of the étale cohomology groups V_x for $x \in X(\mathbb{Q}_p)$ to the variation of the Hodge filtration in the corresponding de Rham cohomology groups.
- The variation of the Hodge filtration is described by the Gauss–Manin connection, which in down-to-earth terms means that it is described by the solutions to a system of differential equations whose coefficients are algebraic functions on X over $\mathbb{Q}$.
- The same differential equations describe the variation of the Hodge filtration for the family $Y_{\mathbb{C}} \to X_{\mathbb{C}}$ of complex projective curves.
- A lower bound on that variation is given by the monodromy of the Kodaira–Parshin family over $\mathbb{C}$.
- An extensive calculation in topology (involving mapping class groups, Dehn twists, and the like) proves that indeed the monodromy group is large enough.

This completes the proof of the Mordell conjecture.

Remark 5.1. Lawrence and Venkatesh show that their approach has applications beyond rational points on curves. In particular, using recent work of Bakker and Tsimerman [BT19], they prove that certain affine varieties F of higher dimension (moduli spaces of smooth hypersurfaces in projective space) have few *integral* points, where "few" means that they are contained in a subvariety of F of lower dimension.

Acknowledgment

The author thanks Brian Lawrence for a comment.

About the author

Bjorn Poonen is the Distinguished Professor in Science at the Massachusetts Institute of Technology. He is the founding managing editor of *Algebra & Number Theory*. Twenty-five mathematicians have earned a PhD under his supervision.

References

[BT19] Benjamin Bakker and Jacob Tsimerman, *The Ax-Schanuel conjecture for variations of Hodge structures*, Invent. Math. **217** (2019), no. 1, 77–94, DOI 10.1007/s00222-019-00863-8. MR3958791 ↑55

[BDMTV19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, DOI 10.4007/annals.2019.189.3.6. MR3961086 ↑48

[Bom90] Enrico Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. MR1093712 ↑48

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité* (French), C. R. Acad. Sci. Paris **212** (1941), 882–885. MR4484 ↑48

[Del74] Pierre Deligne, *La conjecture de Weil. I* (French), Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307. MR340258 ↑53

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German), Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432. English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic Geometry* (Storrs, Conn., 1984), Springer, New York, 1986. MR718935 ↑48, 54

[FW01] E. Victor Flynn and Joseph L. Wetherell, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205, DOI 10.4064/aa98-2-9. MR1831612 ↑46

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. MR1745599 ↑48

[Kim05] Minhyong Kim, *The motivic fundamental group of* $\mathbf{P}^1\backslash\{0,1,\infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656, DOI 10.1007/s00222-004-0433-9. MR2181717 ↑48

[Kim09] Minhyong Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133, DOI 10.2977/prims/1234361156. MR2512779 ↑48

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003 ↑51, 52

[LV19] Brian Lawrence and Akshay Venkatesh, *Diophantine problems and p-adic period mappings*, Invent. Math. **221** (2020), no. 3, 893–999, DOI 10.1007/s00222-020-00966-7. MR4132959 ↑48, 50

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922), 179–192. ↑48

[Par71] A. N. Paršin, *Quelques conjectures de finitude en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Gauthier-Villars, Paris, 1971, pp. 467–471. MR0427323 ↑49

[Poo02] Bjorn Poonen, *Computing rational points on curves*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 149–172. MR1956273 ↑48

[Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR3729254 ↑47

[Ser77] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott; Graduate Texts in Mathematics, Vol. 42. MR0450380 ↑52

[Voj91] Paul Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548, DOI 10.2307/2944318. MR1109352 ↑48

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139-4307

Email address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/