THE S-INTEGRAL POINTS ON THE PROJECTIVE LINE MINUS THREE POINTS VIA FINITE COVERS AND SKOLEM'S METHOD

BJORN POONEN

ABSTRACT. We describe a p-adic proof of the finiteness of $(\mathbb{P}^1 - \{0,1,\infty\})(\mathbb{Z}[S^{-1}])$ using only Skolem's method applied to finite covers.

1. Introduction

Let S be a finite set of primes of $\mathbb{Q}$. Let $R = \mathbb{Z}[S^{-1}]$. Let $X = \mathbb{P}^1_R - \{0,1,\infty\} = \operatorname{Spec} R[x, x^{-1}, (1-x)^{-1}]$. The set $X(R)$ is in bijection with $\{(x,y) \in R^\times \times R^\times : x + y = 1\}$.

Siegel [Sie26] proved that $X(R)$ is finite. Kim [Kim05] gave a new, p-adic proof of this fact, as an application of his nonabelian analogue of the Skolem–Chabauty method. Inspired by Kim's proof, we give a different p-adic proof, using only Skolem's method applied to finite covers. (In fact, the proof we present dates from an April 23, 2005 email to Kim following a talk he gave on his method, but we have not published our proof before now.)

2. Review of the Skolem–Chabauty method

Let k be a finite extension of $\mathbb{Q}$. Let S be a finite set of places of k containing all the archimedean places. The ring of S-integers in k is $R := \{x \in k : v(x) \geq 0 \text{ for all } v \notin S\}$.

Skolem devised a method that, in modern terms, for some subvarieties X in an algebraic torus over R, could prove finiteness of $X(R)$ or even determine it explicitly [Sko34]. His method was generalized by Chabauty [Cha38], who also adapted Skolem's method to study rational points on a curve X in an abelian variety [Cha41]; see [MP12] for an introduction to the latter. Although we need only the torus case, it is not much extra work to describe the method in a more general setting, so we will do so.

A semiabelian variety J is a commutative group variety fitting in an exact sequence $1 \to T \to J \to A \to 1$ with T a torus and A an abelian variety.

Proposition 2.1. *Let R be a ring of S-integers in a number field k. Let J be a finite-type group scheme over R whose generic fiber J_k is a semiabelian variety. Then the abelian group $J(R)$ is finitely generated.*

Proof. By replacing k by a finite extension and enlarging S, we may assume that J fits in an exact sequence of R-group schemes

$$1 \longrightarrow \mathbb{G}_m^n \longrightarrow J \longrightarrow A \longrightarrow 1$$

Date: December 23, 2020.

2020 *Mathematics Subject Classification.* Primary 11G30.

Key words and phrases. S-unit equation, Siegel's theorem, integral points, Skolem's method.

This research was supported in part by National Science Foundation grant DMS-1601946 and Simons Foundation grants #402472 (to Bjorn Poonen) and #550033.

for some $n \geq 0$ and abelian scheme A over R. Taking R-points yields an exact sequence

$$1 \longrightarrow (R^\times)^n \longrightarrow J(R) \longrightarrow A(R). \tag{1}$$

The group $R^\times$ is finitely generated by the Dirichlet S-unit theorem. By the valuative criterion for properness, $A(R) = A(K)$, which is finitely generated by the Mordell–Weil theorem. Now (1) shows that $J(R)$ is finitely generated. $\square$

For a group variety J over a field, say that a subvariety $X \subset J$ **generates** J if, for some n, the addition morphism $X^n \to J$ is surjective (which amounts to requiring that it gives a surjective map on points over an algebraically closed field).

Proposition 2.2. *Let J be a semiabelian variety over $\mathbb{Q}_p$. Equip $J(\mathbb{Q}_p)$ with the p-adic topology. Let Γ be a finitely generated subgroup of a compact subgroup $G \leq J(\mathbb{Q}_p)$. Let X be an irreducible curve over $\mathbb{Q}_p$. Let $\iota\colon X \to J$ be a morphism whose image generates J. If* $\operatorname{rank}\Gamma < \dim J$, *then $\{x \in X(\mathbb{Q}_p) : \iota(x) \in \Gamma\}$ is finite.*

Sketch of proof. (The details are analogous to those in [MP12, §4].) We may assume that ι is proper. Since $J(\mathbb{Q}_p)$ has a basis of neighborhoods of 1 consisting of compact open subgroups K, we may replace G by $G + K$ for any such K to assume that G is open in $J(\mathbb{Q}_p)$. By [Bou98, III.§7.6], there is a canonical homomorphism

$$\log\colon G \to \operatorname{Lie} G = \operatorname{Lie} J.$$

The group $\log\Gamma$ is generated by at most $\operatorname{rk}\Gamma$ elements, and $\operatorname{rk}\Gamma < \dim J = \dim(\operatorname{Lie} J)$, so there is a linear functional $\lambda\colon \operatorname{Lie} J \to \mathbb{Q}_p$ that vanishes on $\log\Gamma$ and even its closure $\log\overline{\Gamma}$. Pulling λ back to the compact subset $\{x \in X(\mathbb{Q}_p) : \iota(x) \in G\}$ yields an analytic function η that is locally the integral of a nonzero 1-form on X, so the zero locus of η is discrete, and hence finite. Finally, $\{x \in X(\mathbb{Q}_p) : \iota(x) \in \Gamma\}$ is contained in the zero locus of η, by definition of λ. $\square$

Theorem 2.3 (The Skolem–Chabauty method)**.** *Let R be a ring of S-integers in a number field k. Let X be a finite-type separated R-scheme such that X_k is an irreducible curve. Let J be a finite-type separated R-group scheme such that J_k is a semiabelian variety. Let $\iota\colon X_k \to J_k$ be a morphism whose image generates J_k. If* $\operatorname{rk} J(R) < \dim J_k$, *then $X(R)$ is finite.*

Proof. Let $R_v \subset k_v$ denote the completions of $R \subset k$ at v. Let $\widehat{R} = \prod_{\ell \notin S} R_v$. Let $\mathbf{A}$ be the restricted product $\prod'_{v \notin S}(k_v, R_v)$, so the R-algebra $\widehat{R}$ is open in the k-algebra $\mathbf{A}$, and $\widehat{R} \cap k = R$. Since $X(\widehat{R})$ is compact and $J(\widehat{R})$ is open in $J(\mathbf{A})$, the map $\iota\colon X(\mathbf{A}) \to J(\mathbf{A})$ maps $X(\widehat{R})$ into a finite union of cosets of $J(\widehat{R})$. Intersecting with $J(k)$ shows that ι maps $X(R)$ into a finite union of cosets of $J(R)$ in $J(k)$.

Choose $\mathfrak{p} \notin S$ that is unramified of degree 1 over a prime p of $\mathbb{Q}$. Then $R_\mathfrak{p} \simeq \mathbb{Z}_p$ and $k_\mathfrak{p} \simeq \mathbb{Q}_p$. Proposition 2.2 applied to $\iota_{\mathbb{Q}_p}$ with $\Gamma = J(R)$ (finitely generated by Proposition 2.1) and $G = J(\mathbb{Z}_p)$ shows that $\{x \in X(R) : \iota(x) \in J(R)\}$ is finite. The same argument with ι composed with a translation shows that $\{x \in X(R) : \iota(x) \in j + J(R)\}$ is finite for each $j \in J(\mathbb{Q})$. By the first paragraph, $X(R)$ is contained in a finite union of these. $\square$

3. Proof of Siegel's theorem

Let $R = \mathbb{Z}[S^{-1}]$ and $X = \mathbb{P}^1_R - \{0, 1, \infty\}$. Let ℓ be a prime. Let A be a (finite) set of representatives for $R^\times/R^{\times\ell}$. For each $a \in A$, let $\pi_a \colon Y_a \to X$ be the finite cover obtained as the inverse image of X under the morphism

$$\begin{aligned} \mathbb{P}^1_R &\longrightarrow \mathbb{P}^1_R \\ y &\longmapsto ay^\ell. \end{aligned}$$

Any element of $X(R) \subset \mathbb{G}_m(R) = R^\times$ is ay^ℓ for some $a \in A$ and $y \in R^\times \subset \mathbb{P}^1(R)$, and then $y \in Y_a(R)$ by definition of Y_a. Thus $X(R) = \bigcup_{a \in A} \pi_a(Y_a(R))$. It remains to prove that each set $Y_a(R)$ is finite.

Let $\mathcal{O} = R[t]/(at^\ell - 1)$ and $K = \mathbb{Q}[t]/(at^\ell - 1)$. If a represents the trivial class in $R^\times/R^{\times\ell}$, then $K \simeq \mathbb{Q} \times K_0$ for a number field K_0; otherwise define $K_0 := K$, which is already a number field. Let $\mathcal{O}_0$ be the integral closure of R in K_0.

We have $Y_a = \mathbb{P}^1_R - \{0, \infty, \text{zeros of } ay^\ell - 1\}$. Over $\overline{\mathbb{Q}}$, the generalized Jacobian of Y_a (i.e., of $\mathbb{P}^1$ with modulus consisting of the $\ell + 2$ removed points) is a torus of dimension $\ell + 1$, and it has a natural model over R, namely $J := \mathbb{G}_{m,R} \times \operatorname{Res}_{\mathcal{O}/R} \mathbb{G}_{m,\mathcal{O}}$, where Res denotes restriction of scalars. The usual morphism from $(Y_a)_\mathbb{Q}$ to its generalized Jacobian $J_\mathbb{Q}$, up to translation in $J_\mathbb{Q}$, is $y \mapsto (y, y - t)$, and its image generates $J_\mathbb{Q}$. Skolem's method (Theorem 2.3) applies if we can prove that $\operatorname{rk} J(R) < \ell + 1$.

We will show that $\operatorname{rk} J(R) < \ell + 1$ holds when ℓ is large. Below, $O(1)$ denotes a quantity whose size depends only on X and S, not on ℓ or a. We have

$$\operatorname{rk} J(R) = \operatorname{rk} R^\times + \operatorname{rk} \mathcal{O}^\times \le 2 \operatorname{rk} R^\times + \operatorname{rk} \mathcal{O}_0^\times = O(1) + \operatorname{rk} \mathcal{O}_0^\times. \tag{2}$$

Since K_0 is of degree $\ell + O(1)$ and has at most one real place, the Dirichlet S-unit theorem implies that

$$\operatorname{rk} \mathcal{O}_0^\times = \ell/2 + \#\{\text{primes in } K_0 \text{ above } S\} + O(1). \tag{3}$$

Let $s = \#S$. For fixed $p \in S$, the number of primes of K_0 above p having degree $< 3s$ is at most p^{3s}, because these primes correspond to distinct irreducible factors of $ax^\ell - 1 \bmod p$ of degree $< 3s$; on the other hand, there are at most $\ell/(3s)$ primes of K_0 above p having degree $\ge 3s$, because their degrees sum to at most $[K_0 : \mathbb{Q}] \le \ell$. Thus

$$\#\{\text{primes in } K_0 \text{ above } S\} = \sum_{p \in S} \left(p^{3s} + \ell/(3s)\right) = \ell/3 + O(1). \tag{4}$$

Substituting (4) into (3) and then (3) into (2) yields

$$\operatorname{rk} J(R) \le \ell/2 + \ell/3 + O(1) < \ell + 1$$

if ℓ is sufficiently large in terms of S.

Remark 3.1. The proof does not seem to generalize readily to prove the analogue for rings of S-integers in number fields other than $\mathbb{Q}$. The limitations of this approach are investigated thoroughly in [Tri19].

Acknowledgments

I thank the referees for encouraging me to include an exposition of the Skolem–Chabauty method.

References

[Bou98] Nicolas Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998. Translated from the French; Reprint of the 1989 English translation. MR1728312 (2001g:17006)

[Cha38] Claude Chabauty, *Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini*, Ann. Mat. Pura Appl. **17** (1938), no. 1, 127–168, DOI 10.1007/BF02410698 (Italian). MR1553308

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484 (3,14d)

[Kim05] Minhyong Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656. MR2181717 (2006k:11119)

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit Methods in Number Theory: Rational Points and Diophantine Equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 99–117.

[Sie26] Carl Ludwig Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc. **1** (1926), 66–68.

[Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., Stockholm, 1934, pp. 163–188 (German).

[Tri19] Nicholas George Triantafillou, *Restriction of scalars, the Chabauty-Coleman method, and* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, June 2019. Ph.D. thesis, Massachusetts Institute of Technology.

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

Email address: poonen@math.mit.edu

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