BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 55, Number 3, July 2018, Pages 353–358
http://dx.doi.org/10.1090/bull/1630
Article electronically published on April 19, 2018

AFTERWORD TO THE ARTICLE "ARITHMETIC ON CURVES"

B. MAZUR

Abstract. In this afterword the author discusses his previously published article "Arithmetic on curves", which appeared in the *Bulletin of the American Mathematical Society (N.S.)* **14** (1986), no. 2, 207–259.

I am delighted to have been asked by Susan Friedlander, the editor of *Bulletin of the American Mathematical Society*, to revisit my survey article "Arithmetic on Curves" and write a brief afterword, mentioning some major advances in the subject in the intervening three decades. But since our subject—algebraic curves and their arithmetic properties—is so closely interconnected with so many branches of mathematics, to give useful comments about major advances, it makes sense to impose strong limits on the range of the discussion. Especially so, since much has been achieved.

I'll keep to two themes, rational points and modularity, as foci of attention regarding the arithmetic of curves. These, of course, represented goals that were of great interest when my article was written. But an up-to-date survey of our subject would have a good deal more to say about them! *Arithmetic statistics* regarding curves, for example, has inspiring new results: striking *theoretical* work—i.e., *theorems*—in arithmetic statistics being due to Manjul Bhargava and his co-authors, and important *experimental* work regarding Mordell–Weil groups of elliptic curves.

- As for *rational points*, we still don't know whether there is an algorithm that (for any curve C defined over a number field K) is guaranteed to terminate in finite time, finding all of the K-rational points of C. Nevertheless, this general question (which—perhaps in less specific terms and different language—has been around since Diophantus) remains a primary goal, and it fits into more structural questions and broader frameworks (e.g., in its connection with higher-dimensional varieties that are *potentially dense* in the terminology of Bogomolov and Tschinkel: varieties whose K-rational points are Zariski-dense), and for which there are some new tools for finding explicit solutions.
- The arithmetic of elliptic curves has had major breakthroughs, what with their *modularity*, advances toward "their" Iwasawa Theory, Main Conjecture [26], and Birch–Swinnerton-Dyer Conjecture; "modularity" taken broadly and in its relation to the grand Langlands Program, has made great strides, with modular curves being more closely understood, and viewed—more and more—within the general framework of Shimura varieties.

I'll expand on these issues in the brief remarks below.

Received by the editors April 4, 2018.
2010 *Mathematics Subject Classification.* Primary 11-XX.

1. Rational points; arithmetic statistics

Since the arithmetic of a curve is often tightly controlled by the arithmetic properties of its jacobian, any advance in the number theory of abelian varieties will help with our understanding of curves; and also conversely, since any abelian variety is a quotient of a jacobian. The Mordell–Lang Conjecture, proven by Gerd Faltings [13] is entirely a statement about abelian varieties and their subvarieties—no explicit mention of curves in it. Nevertheless, it is a powerful extension of Mordell's (classical) Conjecture that a projective curve of genus > 1 over a number field K has only finitely many K-rational points:

Theorem 1. *Let A be an abelian variety over a number field K, and let $V \subset A$ be a subvariety defined over K that is the Zariski-closure of its K-rational points. Then V is a finite union of abelian subvarieties of A.*

This theorem,[1] originally conjectured by Lang, captures the spirit of Lang's more general view regarding rational points on algebraic varieties: roughly speaking, rational points tend to be sparse, except when there is a compelling geometric reason for them to be plentiful.[2] More explicitly and more boldly, he conjectured that if V is an algebraic variety over a number field K with infinitely many K-rational points, then V contains a positive dimensional subvariety that is the birational image of an abelian variety or a rational curve. There are various strengths of "Lang's Conjecture". A form of it (known as the *Strong Lang Conjecture*)—and I'm still not sure whether there is consensus about its likelihood of being correct—was shown to imply a striking uniformity in the upper bounds of the number of rational points a curve of genus > 1 defined over a number field:[3]

Conjecture 2. *For any $g > 1$, there is a finite bound $N(g)$ such that for any number field K there are only finitely many isomorphism classes of projective smooth curves of genus g defined over K having more than $N(g)$ K-rational points.*

Of course to exhibit a lower bound $N(g) > B$ for this conjecturally finite number $N(g)$, one must exhibit infinitely many curves of genus g over some number field K with more than B K-rational points. Families of hyperelliptic curves with all their Weierstrass points $\mathbf{Q}$-rational show that $N(g) \geq 2g + 2$. Can one improve this lower bound? I.e., is there some $\kappa > 2$ such that $N(g) \geq \kappa \cdot g$ for $g \gg 0$?

One might ask—especially in light of current advances in arithmetic statistics—whether or not there is an upper bound B—even independent of the number field of definition, K, or of the genus—for which a positive proportion of curves over K a given genus $g > 1$ (when organized in a natural way) have fewer than B K-rational points?

Even if that's too stark a question, it may be an appropriate moment—thanks to the many results of Manjul Bhargava and his co-authors—to ask more generally, "How many rational points does a random curve have?" This is the title of an excellent survey article by Wei Ho [16]. Among other results cited there, there's the theorem that for fixed $g > 1$ a positive proportion of genus g hyperelliptic

[1] For an introductory exposition to background of some of the ideas behind, and related to, this result, see [21].

[2] Here is an example: $\mathbf{P}^1$ is the *only* irreducible curve V defined over a number field to have the property that for every nontrivial number field extension L/K (where K contains the field of definition of V) V has *more* L-rational points than K-rational points. This is [22, Theorem 1.10].

[3] See [8] and a corrected version of it(!) that will appear soon.

curves over $\mathbf{Q}$ (organized by size of discriminant) possessing a rational Weierstrass point have *no other rational points.* Moreover, a majority of such curves have at most seven rational points. These are results of Poonen and Stoll [25] building on the work of Bhargava and Gross [2] and depending on Chabauty's method. They also show that as the genus g tends to infinity, the lower density of these curves for which the given Weierstrass point is the only $\mathbf{Q}$-rational point tends to 1.

There are also striking results when you ask, more generally, for rational points over number fields other than $\mathbf{Q}$ (cf. [7], [24], [14]).

And, regarding elliptic curves, Manjul Bhargava, Christopher Skinner, and Wei Zhang have shown that "a majority of elliptic curves over $\mathbf{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture", this being the title of their preprint.[4]

The known proofs of Mordell's Conjecture and of Theorem 1 quoted above are nonconstructive. Thanks to Robert Coleman ([11]), Chabauty's method ([9]), which is an earlier strategy, leads—but only when applicable—to a constructive way of achieving upper bounds for the numbers of rational points. For an overview of these results, see [23].

Here is the gist of the Chabauty's method for a curve C of genus $g > 1$ over $\mathbf{Q}$ as amplified by Coleman (see, in particular, [23, 5.4, 5.5]). If the jacobian J of the curve C has Mordell–Weil rank strictly less than g, then for a prime p the p-adic subgroup of $J(\mathbf{Q}_p)$ generated by the $\mathbf{Q}$-rational points of J is necessarily of dimension strictly less than the dimension of $J(\mathbf{Q}_p)$; even more to the point, for a suitable prime p one *constructs* a nontrivial homomorphism $\phi : J(\mathbf{Q}_p) \to \mathbf{Q}_p$ having the property that the full subgroup of $\mathbf{Q}$ rational points of J lies in H, its kernel. The $\mathbf{Q}$-rational points of C, then, lie in the *finite* set $H \cap C(\mathbf{Q}_p) \subset J(\mathbf{Q}_p)$, and Coleman's approach to this, in good situations, can yield a computable upper bound for the number of $\mathbf{Q}$-rational points of C.

Of course, this only works if the Mordell–Weil rank of J is strictly less than g. To get to a broader range of cases, an exciting new development due to Minhyong Kim [19], inspired by the anabelian approach of Grothendieck, offers yet another powerful tool to deal with this fundamental question. The idea ([20]) is—effectively—to expand Chabauty–Coleman's method by replacing the jacobian J by a suitable more discriminating object that is functorially dependent on the curve and then proceed analogously. Illustrative applications can be found in [12] and [1].

2. Elliptic curves; modularity

The most striking direction of progress since the late 1980s is the establishment of what is now referred to as the *modularity conjecture*[5] that says that any elliptic curve of conductor N over the field of rational numbers $\mathbf{Q}$ is isomorphic to a quotient of the modular curve $X_0(N)$. The magnificent method of Andrew Wiles—and Taylor & Wiles (1995)—proved the modularity conjecture for semistable elliptic

[4] This is published in arxiv.org/abs/1407.1826: their result follows from a combination of

- the theorem of Bhargava & Shankar (2015) that the average rank of the Mordell–Weil group of an elliptic curve over $\mathbf{Q}$ is bounded above by 7/6;
- results of Nekovàr and Dokchitser & Dokchitser regarding parity; and
- the proof of the main conjecture of Iwasawa theory for $GL(2)$ by Skinner & Urban [26].

They use these results and the classical powerful method of Kolyvagin to prove their theorem.

[5] The modularity conjecture was referred to in my article as the "Weil–Taniyama Conjecture". This conjecture has undergone a number of curious name changes in its history—the reasons behind this might deserve to be explored as a project in the sociology of mathematics.

curves (and this result implied Fermat's Last Theorem). The full modularity conjecture was proved by an extension of the method of Wiles in 2001 by Breuil, Conrad, Diamond & Taylor.

Here's a three-sentence telegraphic hint of the method that proves that an elliptic curve E over $\mathbf{Q}$ is modular. To get started, one shows (using results of Langlands and others—and a very clever and incisive step known as the $3-5$ trick) that for an appropriate prime p, the Galois representation obtained by Galois action on $E[p]$, the group of p-torsion points of E is "modular" in the sense that it is the *residual characteristic p Galois representation attached to a modular form—more specifically, a modular form that is an eigenform for the Hecke operators.* Then by a close understanding of the deformation theory of such modular residual characteristic p representations, one shows that *appropriate* corresponding p-adic representations lifting them are modular; in particular, so is the p-adic Galois representation associated to E. Then one uses Faltings' Isogeny Theorem and eventually concludes that E is itself a quotient of the modular curve $X_0(N)$, where N is the conductor of E. This approach has expanded enormously and in striking ways. To give a responsible account—even just hints and appropriate attributions—would lead us too far afield, and it would do so even if we restrict our discussion to results that produce, in various contexts, modularity or automorphy.[6] At the very least, though, we might note the resolution of the classical Sato–Tate Conjecture that gives—among many other things!—the precise statistical distribution of the numbers of points over $\mathbf{F}_p$ (for p varying) of a given elliptic curve over $\mathbf{Q}$.[7] See also the extension of this result by Michael Harris [15] where the (un-)correlation of such statistical distributions for different elliptic curves is treated. In short, the arithmetic of curves is as alive as ever!

References

[1] S. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, arxiv.org/abs/1711.05846 (2017).

[2] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and L-functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91. MR3156850

[3] Kevin Buzzard, *Potential modularity—a survey*, Non-abelian fundamental groups and Iwasawa theory, London Math. Soc. Lecture Note Ser., vol. 393, Cambridge Univ. Press, Cambridge, 2012, pp. 188–211. MR2905534

[6] E.g., Serre's modularity conjecture *that an odd, irreducible, two-dimensional Galois representation over a finite field arises from a modular form* thanks to [17], [18]; potential modularity for elliptic curves over totally real fields, and modularity for a host of higher rank automorphic forms.

For an excellent brief survey of results along these lines, see [3], and for a proof that any irreducible, totally odd, essentially self-dual, regular, weakly compatible system of ℓ-adic representations of the absolute Galois group of a totally real field is potentially automorphic, see [4]. For a marvelous exposition regarding issues of reciprocity spanning the classical origins to recent developments, including some of the current extraordinary work of Peter Scholze, see [27].

[7] This is a corollary of the result of Laurent Clozel, Michael Harris, Nicholas Shepherd-Barron, and Richard Taylor ([10], [5]) that the odd symmetric powers of the ℓ-adic representation associated to E is potentially automorphic (if the j-invariant of E is not an algebraic integer) in that it is associated to a cuspidal automorphic representation of $GL(n)$ over some totally real Galois extension of $\mathbf{Q}$. (Here, n is even.)

[4] Thomas Barnet-Lamb, Toby Gee, David Geraghty, and Richard Taylor, *Potential automorphy and change of weight*, Ann. of Math. (2) **179** (2014), no. 2, 501–609, DOI 10.4007/annals.2014.179.2.3. MR3152941

[5] Michael Harris, Nick Shepherd-Barron, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), no. 2, 779–813, DOI 10.4007/annals.2010.171.779. MR2630056

[6] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, Publ. Res. Inst. Math. Sci. **47** (2011), no. 1, 29–98, DOI 10.2977/PRIMS/31. MR2827723

[7] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over* $\mathbb{Q}$ *have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493, DOI 10.1090/jams/863. With an appendix by Tim Dokchitser and Vladimir Dokchitser. MR3600041

[8] Lucia Caporaso, Joe Harris, and Barry Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35, DOI 10.1090/S0894-0347-97-00195-1. MR1325796

[9] 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. MR0004484

[10] Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some* l*-adic lifts of automorphic mod* l *Galois representations*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181, DOI 10.1007/s10240-008-0016-1. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras. MR2470687

[11] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103

[12] J. Ellenberg and D. Hast, *Rational points on solvable curves over* **Q** *via non-abelian Chabauty*, arxiv.org/abs/1706.00525 (2017)

[13] Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR1307396

[14] M. Gunther and M. Morrow, *A positive proportion of odd degree hyperelliptic curves over* **Q** *have at most* 12 *pairs of unexpected quadratic points*, arxiv.org/abs/1709.02041v1

[15] M. Harris, "Potential automorphy of odd-dimensional symmetric powers of elliptic curves, and applications", Vol. 270 in *Algebra, Arithmetic, and Geometry, Volume II: In Honor of Yu. I. Manin*, (Yuri Tschinkel and Yuri Zarhin, eds.) Progress in Mathematics, (2009) pp. 1–21, Birkhäuser, Boston. MR2646496

[16] Wei Ho, *How many rational points does a random curve have?*, Bull. Amer. Math. Soc. (N.S.) **51** (2014), no. 1, 27–52, DOI 10.1090/S0273-0979-2013-01433-2. MR3119821

[17] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504, DOI 10.1007/s00222-009-0205-7. MR2551763

[18] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586, DOI 10.1007/s00222-009-0206-6. MR2551764

[19] 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

[20] Minhyong Kim, *Galois theory and Diophantine geometry*, Non-abelian fundamental groups and Iwasawa theory, London Math. Soc. Lecture Note Ser., vol. 393, Cambridge Univ. Press, Cambridge, 2012, pp. 162–187. MR2905533

[21] Barry Mazur, *Abelian varieties and the Mordell-Lang conjecture*, Model theory, algebra, and geometry, Math. Sci. Res. Inst. Publ., vol. 39, Cambridge Univ. Press, Cambridge, 2000, pp. 199–227. MR1773708

[22] B. Mazur and K. Rubin (with and appendix by M. Larsen), *Diophantine stability*, arxiv.org/abs/1503.04642 (to appear: Amer. J. of Math.)

[23] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman* (English, with English and French summaries), Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117. MR3098132

[24] Jennifer Mun Young Park, *Effective Chabauty for symmetric powers of curves*, ProQuest LLC, Ann Arbor, MI, 2014. Thesis (Ph.D.)–Massachusetts Institute of Technology. MR3279033

[25] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7. MR3245014

[26] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277, DOI 10.1007/s00222-013-0448-1. MR3148103

[27] Jared Weinstein, *Reciprocity laws and Galois representations: recent breakthroughs*, Bull. Amer. Math. Soc. (N.S.) **53** (2016), no. 1, 1–39, DOI 10.1090/bull/1515. MR3403079

Department of Mathematics, Harvard University, Cambridge, Massachusetts