BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 54, Number 4, October 2017, Pages 591–594
http://dx.doi.org/10.1090/bull/1542
Article electronically published on January 5, 2017

RATIONAL POINTS ON, AND THE ARITHMETIC OF, ELLIPTIC CURVES: A TALE OF TWO BOOKS (AND AN ARTICLE)

JOSEPH H. SILVERMAN

It was the best of talks,
~~it was the worst of talks~~,

Our tale begins in 1961, when Professor John Tate was invited by John Solomon to deliver a series of lectures[1] at Haverford College on the subject of "Rational Points on Cubic Curves" [8]. Quoting from the preface to [6], "these lectures, intended for junior and senior mathematics majors, were recorded, transcribed, and printed in mimeograph[2] form. Since that time they have been widely distributed as photocopies of ever decreasing legibility, and portions have appeared in various textbooks . . . In view of the recent interest in the theory of elliptic curves . . . it seems a propitious time to publish an expanded version of those original notes suitable for presentation to an advanced undergraduate audience."

Several generations of students, myself included, received their first introduction to the arithmetic of elliptic curves from Tate's Haverford lecture notes, supplemented by his later advanced survey article [9]. After receiving my PhD in 1982 under Tate's supervision, one of my first teaching assignments was an undergraduate course in abstract algebra at Brown University during the 1989–1990 academic year. The first semester always covered groups, rings, and the start of field theory, while the second semester generally included Galois theory and one or more additional topics. I decided that my added topic would be elliptic curves taught from the Haverford notes, and rather than simply photocopying my own barely legible photocopy, I decided to retype the lectures using (plain) TEX, with some minor editing and the addition of exercises. After teaching the course, it seemed worthwhile to expand the notes and publish them in a more permanent format. So I proposed to Tate that I add material on Lenstra's elliptic curve factorization

Received by the editors May 24, 2016.
2010 *Mathematics Subject Classification.* Primary 11G05.
Key words and phrases. Elliptic curve.

[1]There were six lectures in all, delivered over a three-week period April 20–May 5, 1961. Lecture 1 introduced the group law on a cubic curve, Lecture 2 gave a proof of the Nagell–Lutz theorem describing the torsion subgroup, Lectures 3–5 proved the Mordell–Weil theorem on the finite generation of the group of rational points, and Lecture 6 considered points on cubic curves defined over finite fields.

[2]Mimeograph machines were an "ancient" means of inexpensively creating multiple copies of documents. The material had to be typed onto sheets of special wax-covered paper, which were wrapped around an ink-filled drum. The typing removed the wax from the template, so when ink was applied, it produced a copy of the document on a piece of paper. A hand-crank allowed production of reasonably large numbers of copies before the wax template disintegrated.

algorithm, Diophantine approximation, and complex multiplication, all at the expository level of his lectures, and that we ask Springer–Verlag if they might be interested in publishing the resulting volume. Tate's response to me was very positive, as was the reception to our proposal by Ina Lindemann at Springer. And thus was born the book that appeared in 1992 as *Rational points on elliptic curves* [6].

In addition to the new chapters and exercises that I provided, Tate suggested adding an appendix on projective geometry. In this appendix he proposed to develop intersection theory in the projective plane and to prove Bézout's theorem and other material required for a synthetic proof of the associative law for the group operation on a cubic curve. This was a wonderful idea, and he periodically sent me handwritten pages which I typed and added to the TEX source file. With the publisher's deadline fast approaching, Tate (then in Texas) started to fax me each few pages as he finished them. But since I had no fax machine at home, this required driving to a local store and paying some absurd amount per page to use their fax machine. With the modern proliferation of high-speed home internet connections, it's sometimes hard to remember the extent to which the data and commmunication revolution is such a recent phenomenon.

Both Tate and I were delighted with the reception that the book received upon publication.[3] And presumably the folks at Springer were also pleased, since just two years later we received an urgent email:

```
Date: Tue, 07 Jun 1994 12:55 EST
Subject: corrections for RPEC
Dear Joe:
We have to reprint your RPEC quite urgently (sales just didn't
slow down).  Do you have a list of corrections? Shall I also
contact Tate or will you do that? We need the corrections as
soon as possible.
All the best, Ina
```

The corrected printing appeared shortly thereafter, and there matters stood for many years. Then in 2015 we decided to put together an expanded second edition [7] with two new sections, one on the use of elliptic curves in cryptography and the other a brief discussion of the use of elliptic curves in Wiles's proof of Fermat's last theorem. This also gave us an opportunity to correct a number of minor mathematical glitches, generate new figures, add some new exercises, and write a short second appendix illustrating how to transform a general plane cubic into Weierstrass form.

I turn now to the second book alluded to in the title, *The arithmetic of elliptic curves* [3], which appeared in 1986. Although not formally a joint project with Tate, in my mind this book has always represented an expanded version of (part of) Tate's beautiful and highly influential survey article [9] of the same title that appeared in *Inventiones Mathematicae* in 1974.[4]

[3]There were, of course, also some criticisms. After an approving "Très bien!", Serre offered "Trois critiques" [2, 11 septembre 1992], followed three months later [2, 5 décembre 1993] by his not unjustified "horror" at the informality of the "proof" of associativity in Chapter 1.

[4]It turns out that the mathematical community is lucky that Tate's article ever appeared, since shortly thereafter he wrote to Serre [2, April 13, 1974] that in view of the fact that "*Inventiones* has declared a moratorium on papers ... I feel guilty for taking up space with that survey of mine." But barely one week later [2, April 21, 1974], he wrote again to say that the "reprints of my survey article on elliptic curves just arrived. I'm sending them out now, and am astonished at the number of requests I've already gotten."

As noted in the preface to [3], "considering the vast amount of research currently [in the 1980s] being done in this area [the arithemtic theory of elliptic curves], the paucity of introductory texts is somewhat surprising." My own knowledge of elliptic curves was shaped during graduate school by a handful of books by Serge Lang, Neal Koblitz, and Alain Robert, plus a long article of J.W.S Cassels [1] and the aforementioned survey of Tate.[5] After completing my degree and obtaining a post-doc at MIT, I was told that during my first year, I could teach a graduate topics course in a subject of my choosing. My choice was, naturally, elliptic curves, and my goal was to create the course that I wished that I'd been able to take as a second or third year PhD student. Tate's survey article served as my syllabus.

At the end of the course, I had about 100 pages of handwritten course notes, which I showed to Gary Cornell and casually mentioned that maybe, someday, I'd try turning them into a book. Shortly thereafter I received a letter (snail-mail, no email back then) from Walter Kaufmann-Bühler at Springer New York asking if I'd like to submit my book proposal. I responded with a short note giving a rough table of contents, and Kaufmann-Bühler sent me a contract!

The original plan was for the book to include all of the topics in Tate's survey article, and with my detailed course notes in hand, I naively estimated that it would take about one year to complete the task. Three years later, there was a 400 page book consisting of 10 chapters which managed to cover about half of the planned material.[6]

The original manuscript for [3] was written by hand, typed by Ann Clee at MIT on an IBM typewriter (n.b. that's typewriter, not word processor), and shipped to Hong Kong to be typeset. During this lengthy process, I proofread the entire book at least eight times in four different formats. Such meticulous perusal ensured that when the book finally appeared, no mathematical or typographical errors remained.[7] In fact, within one year of publication, kindly readers had discovered 400+ errata, some of which I found, on checking, had propagated from the original handwritten copy. Based on this experience, and supplemented by further authorship adventures, I herewith share my personal rules-of-thumb for budding authors: (1) Estimate the maximum amount of time that you expect it will take you to write your book and triple it. (2) No matter how many times you proofread your book, after publication there will be roughly one typo per page.

Acknowledgments

The author would like to thank Greg Call, Ted Chinburg, Dale Husemoller, Jonathan Lubin, and John Tate for their helpful comments on the initial draft of this note.

[5]I must also give a "shout out" to the graduate student organizers and speakers at the Harvard Elliptic Curve Seminar, which ran for many years and from which I learned so much.

[6]Eventually, there was a second volume, *Advanced topics in the arithmetic of elliptic curves* [4, 1994], which weighed in at 500+ pages and still only managed to deal with about half of the remaining half of the material in Tate's article. A second edition of the first volume [5, 2009] added some new topics, but since the original edition had been typeset using classical, i.e., non-TEX, publishing methods, it was necessary to retype the entire book. This naturally introduced many new typos, possibly the most egregious of which was the statement that a Weierstrass equation is non-singular if and only if $\Delta = 0$.

[7]Readers who accept this sentence at face value should contact me to arrange their purchase of a bridge.

References

[1] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291. MR0199150
[2] *Correspondance Serre–Tate. Vol. II* (French), Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 14, Société Mathématique de France, Paris, 2015. Edited, and with notes and commentaries by Pierre Colmez and Jean-Pierre Serre. MR3379330
[3] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210
[4] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368
[5] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094
[6] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR1171452
[7] Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR3363545
[8] John T. Tate. *Rational points on cubic curves*, unpublished notes of lectures delivered at Haverford College, 1961.
[9] John T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206. MR0419359

Mathematics Department, Box 1917 Brown University, Providence, Rhode Island 02912

E-mail address: jhs@math.brown.edu