APPEARED IN BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 30, Number 2, April 1994, Pages 248-252

BOOK REVIEW

Rational points on elliptic curves, by Joseph H. Silverman and John T. Tate. Undergraduate Texts in Mathematics, Springer-Verlag, New York and Berlin, 1992 (first ed. 1989), x+281 pp., $29.95. ISBN 0-387-97825-9

Fermat's Last Theorem provides the latest answer to the question: Why study elliptic curves? Suppose that p is an odd prime and that a, b, and c are relatively prime nonzero integers for which $a^p + b^p + c^p = 0$. In [7], Frey predicted that the elliptic curve with equation $y^2 = x(x - a^p)(x + b^p)$ would be incompatible with the Taniyama-Shimura conjecture, a central conjecture about elliptic curves which states that elliptic curves over $\mathbf{Q}$ are *modular* in the sense that they arise from modular forms. After Serre analyzed Frey's construction, the second reviewer was able to confirm Frey's prediction. (See [23, 24] and [21, 22].) As we write this review, A. Wiles has just announced a proof of the Taniyama-Shimura conjecture for a large class of elliptic curves over $\mathbf{Q}$, including the semistable ones, those with the simplest type of "bad reduction" [30]. Since Frey's elliptic curves are semistable, Fermat's Last Theorem follows as a corollary.

Those indifferent to Fermat's Last Theorem might nonetheless be attracted by other applications of elliptic curves. For example, elliptic curves are used in factoring integers, cf. [18]. Elliptic curves play a central role in the solution, by Goldfeld, Gross, and Zagier, of Gauss's class number problem [11, pp. 231–232]. Elliptic curves underly the theory of elliptic functions and modular forms. They figure prominently in many articles in *Communications in mathematical physics* and in the recent book *From number theory to physics* [28]. This list of examples could be expanded easily.

The theory of elliptic curves belongs to an important branch of mathematics called arithmetical algebraic geometry (or "arithmetic" for short). Arithmetic is a synthesis of algebraic number theory and algebraic geometry: it is the study of number theory in a geometric situation. For instance, consider again Fermat's equation $a^p+b^p+c^p = 0$, where a, b, and c are nonzero integers. Solving it amounts to finding all pairs of rational numbers x and y which satisfy $x^p + y^p = 1$. One can make considerable progress toward solving this equation by algebraic number theory (see, e.g., [9, 8, 26]). As soon as we start thinking about rational points on the *curve* $x^p + y^p = 1$, however, we have probably stepped into the world of arithmetical algebraic geometry.

The simplest objects of algebraic geometry are points, lines, and conics. Next in complexity come the elliptic curves: curves of genus one, furnished with a distinguished rational point. Already for these we are faced with a plethora of deep open questions.

Let E be an elliptic curve, and let $E(\mathbf{Q})$ be the set of points on the curve with rational coordinates. We can realize E as the projective plane curve associated with a cubic equation $y^2 = x^3 + ax + b$. Then $E(\mathbf{Q})$ becomes the set of pairs of rational numbers which satisfy this equation, augmented by a single "point at infinity" O on E. The well-known "chord and tangent" process endows $E(\mathbf{Q})$ with the structure of an abelian group, in which O is the zero-element. This group, now known as the Mordell-Weil group, was studied by Poincaré and by Mordell, who proved in 1922 that $E(\mathbf{Q})$ is *finitely generated* and, therefore, isomorphic to the direct sum of a finite abelian group $E(\mathbf{Q})_{\mathrm{tors}}$ and a free abelian group $\mathbf{Z}^{r(E)}$ of finite rank. The integer $r(E)$ is known as the *rank* of E over $\mathbf{Q}$.

A number of unsolved problems concern $r(E)$. First of all, there is at present no known effective algorithm which calculates $r(E)$. Secondly, one suspects that $r(E)$ is unbounded as E varies among all elliptic curves over $\mathbf{Q}$. Although recent examples [6] show that the rank can be 19 or even higher, it is not known whether $r(E)$ can be arbitrarily large. (The group $E(\mathbf{Q})_{\mathrm{tors}}$ has bounded order; more precisely, a theorem of Mazur [19] states that $E(\mathbf{Q})_{\mathrm{tors}}$ is limited to fifteen possibilities. Also, $E(\mathbf{Q})_{\mathrm{tors}}$ is easy to compute in any specific example.)

Other problems about elliptic curves concern the L-function $L(E, s)$, which bears the same relation to E as does the Riemann zeta function to $\mathbf{Z}$. The function $L(E, s)$ is defined by a Euler product which converges to an analytic function on the half-plane $\Re(s) > 3/2$. One conjectures that $L(E, s)$ extends to an analytic function on the entire complex plane. This statement is a direct consequence of the Taniyama-Shimura conjecture; conversely, Weil [29] showed that the conjecture follows from an appropriate statement about the analytic behavior of $L(E, s)$ and its variants. Until recently, it was generally thought that all results of this nature were too hard to prove. Now that we know that semistable elliptic curves over $\mathbf{Q}$ are modular, we imagine that the full Taniyama-Shimura conjecture is within reach.

Assuming that $L(E, s)$ has been analytically continued, we can discuss the behavior of $L(E, s)$ at $s = 1$. The conjecture of Birch and Swinnerton-Dyer states (in particular) that $L(E, s)$ has a zero of order $r(E)$ at $s = 1$. Theorems of Kolyvagin [16] and Gross-Zagier [11] combine to prove most of this conjecture for modular elliptic curves of low rank; see [10] for a survey of results of this type. Again, because of [30], the word "modular" becomes nearly irrelevant. At the present time, the conjecture of Birch and Swinnerton-Dyer seems wide open for elliptic curves with $r(E) > 1$.

Elliptic curves are extremely palpable objects, despite the variety and depth of the problems that they pose. They are one-dimensional plane curves whose real and complex loci can be visualized easily. They can also be tabulated: Cremona [5] has made an extensive list of modular elliptic curves over $\mathbf{Q}$ and has amassed a large amount of data for each curve on his list. (Cremona's tables list the modular elliptic curves of conductor < 1000; the conductor of an elliptic curve measures its "bad reduction" modulo various primes.) Even the Taniyama-Shimura conjecture can be stated in elementary terms [20].

The accessibility and importance of elliptic curves have made them favorites with authors and readers. Two classic survey articles about elliptic curves are [1] and [27]. Among the recent books which have focused primarily, or exclusively, on the theory of elliptic curves are [2–4, 12–15, 17, 25].

Rational points on elliptic curves, by Silverman and Tate is a new *undergraduate* book on elliptic curves; it will appeal to graduate students and to professional mathematicians, both specialists in the theory and outsiders who want to learn more. The book grew out of a series of lectures given by the second author to an audience of undergraduate mathematics majors in 1961. Those lectures centered around a proof of the theorem of Mordell which was alluded to above: the finite generation of $E(\mathbf{Q})$. The first half of the book follows closely the 1961 lectures. (As the authors explain in their preface, lecture notes were mimeographed in 1961 and have continued to circulate since.) New topics include the behavior of points of finite order under reduction mod p, factorization of integers using elliptic curves, points with integer coordinates on elliptic curves, and complex multiplication. The authors conclude with an appendix on projective geometry.

The exposition of this book is extremely nonthreatening: the reader is addressed directly as "you" and is invited to participate in a dialogue with the authors and their theorems. There are a large number of exercises, of varying levels of difficulty. These are important off-shoots of the text; quite a few are challenging. For example, the Taniyama-Shimura conjecture is first mentioned in a beautiful section of Chapter IV entitled "A Theorem of Gauss". In that section the authors derive Gauss's formula for the number of solutions to $x^3 + y^3 = 1$ over the finite field $\mathbf{F}_p$ and allude to the possibility of relating the analogous numbers for other elliptic curves to certain holomorphic functions. Later, in Exercise 4.6, the reader is called upon to formulate a conjecture linking the number of $\mathbf{F}_p$-valued points of $y^2 = x^3 - 4x^2 + 16$ to the pth coefficient of the series obtained by expanding $q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$ in powers of q. (The authors include a doubly asterisked invitation to *prove* the conjecture.)

The book's exposition is rooted in the concrete: computations are carried out explicitly, and the reader is encouraged to reproduce them and to experiment with other examples. General results are often stated to orient the reader, but they are not necessarily proved. For example, the chapter on complex multiplication begins with a statement of the Kronecker-Weber theorem, which is illustrated by the fact that the quadratic field $\mathbf{Q}(\sqrt{p})$ lies in a cyclotomic extension of $\mathbf{Q}$. The chapter then explains how division points on rational elliptic curves lead to two-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The authors show that division points on the elliptic curve $y^2 = x^3 + x$ generate abelian extensions of $\mathbf{Q}(i)$ and conclude with a statement of Kronecker's Jugendtraum as it applies to $\mathbf{Q}(i)$: each abelian extension of $\mathbf{Q}(i)$ is contained in a field generated by division points of $y^2 = x^3 + x$.

Although not required, a personal computer or programmable calculator will be extremely useful for the numerical examples included in the book. In this connection, Silverman is distributing two computer packages which will interest readers. The first is a stand-alone Macintosh application that serves as a calculator for elliptic curves. The second is a more recent Mathematica notebook, written by Paul van Mulbregt and Silverman; it is distributed along with TEX documentation. Instructions for obtaining these packages by mail are given in the book's preface. Alternatively, readers with Internet access can download the packages by `ftp` from `gauss.math.brown.edu`—look in the directory `~ftp/dist/EllipticCurve`. Also available in this directory is a list of errata for the book. The list catalogs errors which have come to the authors' attention and in most cases supplies corrections.

References

1. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, Survey article, J. London Math. Soc. **41** (1966), 193–291.

2. ———, *Lectures on elliptic curves*, Cambridge Univ. Press, Cambridge and New York, 1991.
3. J. Chahal, *Topics in number theory*, Plenum Press, New York and London, 1988.
4. D. A. Cox, *Primes of the form* x^2+ny^2: *Fermat, class field theory, and complex multiplication*, Wiley, New York, 1989.
5. J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge and New York, 1992.
6. S. Fermigier, *Un exemple de courbe elliptique définie sur* $\mathbf{Q}$ *de rang* ≥ 19, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), 719–722.
7. G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), 1–40.
8. A. Granville, *On the Kummer-Wieferich-Skula approach to the first case of Fermat's Last Theorem*, Advances in Number Theory (F. Q. Gouvêa and N. Yui, eds.), Clarendon Press, Oxford, 1993, pp. 479–498.
9. A. Granville and M. B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714,591,416,091,389, Trans. Amer. Math. Soc. **306** (1988), 329–359.
10. B. H. Gross, *Kolyvagin's work on modular elliptic curves*, London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.
11. B. H. Gross and D. B. Zagier, *Heegner points and the derivatives of L-series*, Invent. Math. **84** (1986), 225–320.
12. D. Husemöller, *Elliptic curves*, Graduate Texts in Math., vol. 111, Springer-Verlag, Berlin and New York, 1987.
13. K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Math., vol. 84, second ed., Springer-Verlag, Berlin and New York, 1990.
14. A. W. Knapp, *Elliptic curves*, Math. Notes, vol. 40, Princeton Univ. Press, Princeton, NJ, 1992.
15. N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Math., vol. 97, Springer-Verlag, Berlin and New York, 1984.
16. V. Kolyvagin, *Euler systems*, Prog. in Math., vol. 87, Birkhäuser, Boston, 1990, pp. 435–483.
17. S. Lang, *Elliptic curves diophantine analysis*, Grundlehren der Math. Wiss., vol. 231, Springer-Verlag, Berlin and New York, 1978.
18. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.
19. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.
20. ———, *Number theory as gadfly*, Amer. Math. Monthly **98** (1991), 593–610.
21. K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
22. ———, *From the Taniyama-Shimura Conjecture to Fermat's Last Theorem*, Ann. Fac. Sci. Toulouse Math. (5) **11** (1990), 116–139.
23. J. P. Serre, *Lettre à J. F. Mestre*, 13 août 1985, Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 263–268.
24. ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.
25. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.
26. J. W. Tanner and S. S. Wagstaff, Jr., *New bounds for the first case of Fermat's Last Theorem*, Math. Comp. **53** (1989), 743–750.
27. J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.
28. M. Waldschmidt et al., eds., *From number theory to physics* (Lectures given at the meeting "Number Theory and Physics" held at the Centre de Physique, Les Houches, 1989), Springer-Verlag, Berlin and New York, 1992.
29. A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156.
30. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem* (to appear).

William R. Hearst III
The San Francisco Examiner
E-mail address: `whearst@MCIMail.com`

Kenneth A. Ribet
University of California, Berkeley
E-mail address: ribet@math.berkeley.edu