BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 33, Number 2, April 1996

Arithmetic of algebraic curves, by Serguei Stepanov, Monographs in Contemporary Math., Plenum Publishing, New York, 1994, xii + 422 pp., $115.00, ISBN 0-306-11036-9

The solution of polynomial equations in integers and in rational numbers has fascinated mathematicians since antiquity. The simplest non-trivial situation is the case of one equation in two variables. That is, let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a (non-constant) polynomial in two variables with rational coefficients. One is interested in describing the integral or rational solutions to the equation

$$(*) \qquad f(X,Y) = 0.$$

Geometrically, the equation $f = 0$ describes an algebraic curve C in the affine plane, so one also speaks of the integral or rational points on the curve C. We will denote the set of integral solutions to $(*)$ by $C(\mathbb{Z})$ and the set of rational solutions by $C(\mathbb{Q})$. More generally, if R is any ring or field, we write

$$C(R) = \big\{(x,y) \in R^2 \,:\, f(x,y) = 0\big\}.$$

Using a geometric approach turns out to be extremely fruitful. There are several simplifications which one can make. First, if the polynomial $f(X,Y)$ factors in $\mathbb{C}[X,Y]$, then C breaks up into a union of two or more curves, each of which may be studied separately, so it suffices to study curves defined by irreducible polynomials. Second, the curve C may be singular, but we can always replace C with a non-singular curve $\tilde{C}$ so that there is a map $\tilde{C} \to C$ which is bijective at all but finitely many points. It thus suffices to study integral and rational points on non-singular curves. Third, we can embed a non-singular curve C into a complete non-singular curve $\bar{C}$ so that the complement $\bar{C} \smallsetminus C$ consists of a finite set of points. It turns out that the geometry of $\bar{C}$ and $\bar{C} \smallsetminus C$ largely determines the qualitative behavior of the integral and rational points on C.

Let K be a number field (e.g. $\mathbb{Q}$), let R be a finitely generated subring of K (e.g. $\mathbb{Z}$), and let C be a non-singular curve defined by polynomial equations with coefficients in R. As above, we will let $\bar{C}$ be a non-singular completion of C. The complex points of $\bar{C}$, denoted $\bar{C}(\mathbb{C})$, form a Riemann surface, and the complement $\bar{C}(\mathbb{C}) \smallsetminus C(\mathbb{C})$ consists of a finite (possibly empty) set of points. The *Euler characteristic of* C, denoted $\chi(C)$, can be defined as the usual alternating sum of vertices, edges, and faces of a triangularization of $C(\mathbb{C})$, or by using any one of the standard (co)homology theories. Equivalently, if we write $g(\bar{C})$ for the genus of the Riemann surface $\bar{C}(\mathbb{C})$, then

$$\chi(C) = 2 - 2g(\bar{C}) - \#\big(\bar{C}(\mathbb{C}) \smallsetminus C(\mathbb{C})\big).$$

The fundamental finiteness theorems for the arithmetic of algebraic curves say that the Euler characteristic $\chi(C)$ determines the distribution of integral and rational points on C. The following table gives the precise statements, where to avoid

trivialities we have assumed that C has at least one integral point.

$\chi(C)$	C(R)
$= 2$	isomorphic to $\mathbb{P}^1(K)$
$= 1$	isomorphic to R
$= 0$	a finitely generated abelian group
< 0	a finite set

Integral Points on a Non-Singular Curve C

The first two lines of this table are classic. The third line, $\chi(C) = 0$, actually contains two theorems. One possibility is $g(\bar{C}) = 0$, in which case C looks like the curve $\mathbb{P}^1 \smallsetminus \{0, \infty\}$, and $C(R) \cong R^*$ is a finitely generated group by Dirichlet's unit theorem. The second possibility is that $C = \bar{C}$ is a curve of genus 1, and then the finite generation of $E(K)$ is the Mordell-Weil theorem. Finally, the last line of the table splits into three distinct cases. First, C may look like $\mathbb{P}^1$ with at least 3 points removed, second, C may be a curve of genus 1 with at least 1 point removed, and third, C may be a curve of genus ≥ 2 with any number of points removed. The finiteness of $C(R)$ if $C \neq \bar{C}$ was proven by Siegel in the 1920's. The finiteness of $C(K) = \bar{C}(R)$ when $C = \bar{C}$ was conjectured by Mordell, also in the 1920's, and proven by Faltings in 1983.

In addition to looking for integral and rational solutions to polynomial equations, there is a vast literature devoted to studying the solutions "modulo p", or more generally solutions in a finite field $\mathbb{F}_q$ with q elements. The set of such solutions, or equivalently the set $C(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on a curve C, is a finite set. For example, the projective line $\mathbb{P}^1(\mathbb{F}_q)$ has $q+1$ points, namely, the q points in $\mathbb{F}_q$ plus one extra point at infinity. The following estimate, which says that almost the same thing is true for any non-singular complete curve C, was conjectured by Emil Artin and proven by Hasse for curves of genus 1 and by Weil for curves of arbitrary genus:

$$\bigl|q + 1 - \#C(\mathbb{F}_q)\bigr| \leq 2g(C)\sqrt{q}.$$

One can also look at the points of C defined over extension fields $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. This information is normally encoded in a generating function called the *zeta function of* $C/\mathbb{F}_q$,

$$Z(C/\mathbb{F}_q, T) = \exp\Bigl(\sum_{n\geq 1} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n\Bigr).$$

Weil proved that

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) \in \mathbb{Z}[T]$ is a polynomial of degree $2g(C)$ satifying $P(0) = 1$ and $P(T) = q^{g(C)}T^{2g(C)}P(1/qT)$. Further, P factors as

$$P(T) = \prod_{i=1}^{2g(C)} (1 - \alpha_i T) \qquad \text{with every } |\alpha_i| \leq \sqrt{q}.$$

Notice that this gives Hasse's estimate, since one can easily check that $\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum \alpha_i^n$.

Now we come to the book under review. The author's hope was "to give a full picture of the contemporary state of the theory of Diophantine equations and the whole spectrum of methods used in it, while demonstrating their inner unity. However, space limitations [forced the omission of] the analytic aspects of the theory, in particular the ... circle method of Hardy-Littlewood and the methods of the theory of Diophantine approximation." So the author "restricts the discussion to arithmetic, algebraic-geometric, and logical aspects of the problem."

He begins in Chapter 1 by studying equations over finite fields, and, following a brief introduction to the algebraic geometry of curves in Chapter 4, proves in Chapter 5 the rationality of the zeta function $Z(C/\mathbb{F}_q, T)$ and the Hasse-Weil estimate for the number of points in $C(\mathbb{F}_q)$. The proof given, which is due to the author and Bombieri, is reasonably elementary and involves the construction of certain rational functions on C having high order zeros at the points in $C(\mathbb{F}_q)$. Also, in Chapter 2 the author discusses some analytic results concerning the distribution of quadratic residues and non-residues, including a nice description of the large sieve.

Chapters 3, 6, and 7 are devoted to the global arithmetic of curves, that is, the study of their integral and rational points over number fields. Chapter 3 discusses the arithmetic of elliptic curves E, including a description of the group law on E and a proof of Mordell's theorem that $E(\mathbb{Q})$ is a finitely generated group. Chapter 6 is devoted to an introduction to the theory of non-standard arithmetic. The author constructs the non-standard reals ${}^*\mathbb{R}$ and the non-standard natural numbers ${}^*\mathbb{N}$ and proves some of their basic properties. He then uses non-standard arithmetic in Chapter 7 to prove the Mahler-Siegel theorem asserting the finiteness of $C(R)$ for a curve C of genus at least 1 with at least one point removed.

The theory of curves over finite fields as covered in Stepanov's book is quite similar in scope and content to the monograph of Schmidt [2], although Stepanov's book has the added advantage of including numerous exercises. There are similarly other sources for the theory of curves over global (e.g. number) fields, in particular Lang's classic [1] and Serre's book [3]. However, both of these require a much greater background in algebraic geometry than does Stepanov's book, both follow the classical (as opposed to the non-standard) approach to proving the finiteness of $C(R)$, and they contain few [3] or no [1] exercises. Stepanov also feels that the non-standard proof of the Siegel-Mahler theorem has the "advantage of revealing very clearly the ideas on which Siegel's method is based" (page 258), an assertion with which the reviewer disagrees but is willing to leave to the reader's personal taste. In any case, it is certainly worthwhile to see many different proofs of major theorems, since each proof reveals new ideas and gives new insights.

Another positive aspect of this book which sets it off from any current competitor is that it contains literally hundreds of exercises, many of them quite difficult and given with extensive hints. A student looking for a challenge (as all students should) would do well to open this book to any chapter and attempt a selection of the problems. Indeed, the author is honest enough to say in the preface and repeat in the introduction that "the problems are intended for researchers active in the field."

What, then, are the drawbacks of Stepanov's book? First, although much of the book is well written, there are places where the exposition seems a trifle unclear. This was especially apparent in the proof of Mordell's theorem in Chapter 3 and the proof of Siegel's theorem in Chapter 7, although the latter difficulty may have been

due to the reviewer's lack of familiarity with non-standard methods. Second, the translation is adequate, but the book would certainly have benefitted from a final edit by a native speaker. In particular, articles are frequently missing and there are many awkward phrases. There are also a fair number of typographical errors, some of which could cause confusion for the reader. (For example, on page 79, line 7, the inequality $H > p^{1/4+s}$ should read $H > p^{1/4+\epsilon}$.) A minor related gripe concerns the references, which are extensive but not in alphabetical order! Finally, and this is a matter of no small importance in what is supposed to be a textbook for budding researchers, the list price of $115 is outrageous. Thus most graduate students who want to benefit from Stepanov's book will have to hope that their local library has ordered a copy.

References

1. S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York, 1983. MR **85j:**11005
2. W. Schmidt, *Equations over finite fields. An elementary approach*, Lect. Notes in Math., vol. 536, Springer-Verlag, Berlin, 1976. MR **55:**2744
3. J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics E15, Friedr. Vieweg, Braunschweig and Wiesbaden, 1989. MR **90c:**11086

Joseph H. Silverman
Brown University
E-mail address: JHS@GAUSS.MATH.BROWN.EDU