

Carter's book contains a very good introduction to the present state of affairs and can be warmly recommended to anyone who is interested in penetrating into the highly interesting domain of finite groups of Lie type. The book has an extensive bibliography.

T. A. SPRINGER

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 17, Number 1, July 1987
©1987 American Mathematical Society
0273-0979/87 \$1.00 + \$.25 per page

The arithmetic of elliptic curves, by Joseph H. Silverman, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, Berlin, Heidelberg and Tokyo, 1986, xii + 400 pp., \$48.00. ISBN 0-387-96203-4

The arithmetic (= diophantine theory) of curves of genus 0 is now very well understood. That of curves of genus > 1 is still in a rudimentary and unsatisfactory state. For curves of genus 1 there is a large body of established theory and an even larger body of interrelated conjecture: the whole being currently in a state of exciting development.

We work over a ground field k , which may be the rationals \mathbf{Q} , or e.g., a global or local field. An elliptic curve defined over k consists of a curve of genus 1 together with a point 0 (say) on it, both defined over k (we shall often say "rational" instead of "defined over k "). Here we encounter our first puzzle. There is no known algorithm for deciding (e.g., when $k = \mathbf{Q}$) whether there is a rational point on a given curve of genus 1 or not: in particular there is no Hasse principle (local-global principle). However, to every curve of genus 1 there is associated in a canonical way an elliptic curve over the same ground field (its jacobian, a generalization of the notion from algebraic geometry). The theory of curves of genus 1 thus largely reduces to that of elliptic curves.

The points of an elliptic curve have a natural structure as an abelian group, the given point 0 being the neutral element ("zero") of the group. In fact the elliptic curves over a field k are precisely the abelian varieties of dimension 1 over k . In particular the set of rational points has a natural abelian group structure. When $k = \mathbf{Q}$ a famous theorem of Mordell states that this group is finitely generated. This result was generalized by Weil and others and the group is usually called the Mordell-Weil group (for the given elliptic curve and ground field). There is, however, as yet no algorithm for determining the Mordell-Weil group, though this can usually be done in specified cases. The absence of an algorithm here is closely associated with the failure of the Hasse principle mentioned above. The "obstruction" to the Hasse principle is encapsulated in a group discovered independently by Tate and Shafarevich and called the Tate-Shafarevich group. It has many interesting properties, both proved and conjectural. Without doubt the reviewer's most lasting contribution to the theory is the introduction of the cyrillic letter \mathbb{III} ("sha") to denote this group, a usage which has become universal.

