14. L. A. Pars, *A treatise on analytical dynamics*, Heinemann, London, 1965.

15. H. Poincaré, *Les méthodes nouvelles de la mécanique celeste*, 3 vols., reprint, Dover, New York, 1957.

16. C. L. Siegel and J. Moser, *Lectures on celestial mechanics*, (English transl. by C. I. Kalme), Springer-Verlag, New York, 1971.

17. S. Sternberg, *Celestial mechanics*, 2 vols., Benjamin, New York, 1969.

18. J. L. Synge, *Classical dynamics*, Handbuch der Physik, III/1, Springer-Verlag, Berlin, 1960, pp. 1–225.

19. E. T. Whittaker, *A treatise on the analytical dynamics of particles and rigid bodies*, 4th ed., Cambridge Univ. Press, London, 1927.

20. A. Winter, *The analytical foundatons of celestial mechanics*, Princeton Univ. Press, Princeton, N. J., 1947.

IAN N. SNEDDON

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 2, Number 2, March 1980

0002-9904/80/0000-0112/$01.75

Elliptic curves: Diophantine analysis, by Serge Lang, Grundlehren der mathematischen Wissenschaften, vol. 231, Springer-Verlag, Berlin-Heidelberg-New York, 1978, xi + 261 pp., $37.40.

The study of the arithmetical properties of elliptic curves has been one of the most exciting areas of mathematical research for at least the past fifty years. It is customary to divide the modern theories according as one is dealing with rational points or with integer points; and both aspects of the subject can be regarded as having been initiated in 1922 by some remarkable discoveries of Mordell.

It had long been known that the rational points on an elliptic curve, defined over the rationals, form a group Γ under a chord and tangent construction; Mordell proved that Γ has a finite basis. The proof was most ingenious. It began with a demonstration that the group $\Gamma/2\Gamma$ is finite and then proceeded by a method of infinite descent (for references, see [5]). A far-reaching generalization of the finite basis theorem concerning abelian varieties was established by Weil in 1928; much important work arose therefrom, and an excellent survey of the subject as it existed in 1966 was given by Cassels [3]. Here there are discussions of the celebrated conjectures of Birch and Swinnerton-Dyer, of the theorems of Lutz and Nagell, of the Tate-Shafarevich and Selmer groups, and of a great deal besides. In another direction, Mordell showed that the Diophantine equation

$$y^2 = ax^3 + bx^2 + cx + d \qquad (*)$$

where a, b, c, d denote integers and the cubic on the right has distinct zeros, has only finitely many solutions in integers x, y. The proof involved the theory of the reduction of binary quartic forms followed by an application of a famous theorem of Thue (again, see [5]). Another proof, and indeed one that was applicable more generally to the hyperelliptic equation, was given by Siegel in 1926. Furthermore, in 1929, in a most profound work, Siegel succeeded in combining the Mordell-Weil theorem with a refinement of Thue's theorem that he had proved earlier, to show that any curve, defined over the rationals, with genus at least 1, has only finitely many integer points.

The two advances just described, though plainly of a very different nature, nevertheless have an important feature in common, namely they are both noneffective. Thus, though the Mordell-Weil theorem can be refined to yield a bound for the number of generators of Γ, it does not, in general, enable these generators to be determined explicitly. Likewise, though the works of Thue, Mordell and Siegel furnish estimates for the number of solutions of certain Diophantine equations, they do not enable the full list of solutions to be specified in any particular instance. The search for effective methods in these contexts has motivated much of the subsequent progress.

In 1966, the reviewer initiated a new method in Diophantine analysis. Gelfond had established some thirty years earlier, as a sequel to his work on Hilbert's seventh problem, an inequality giving a positive lower bound for a linear form in two logarithms, and he had raised the question of extending the result to arbitrarily many logarithms, pointing out that such an extension would have important consequences in number theory. The problem was solved by the reviewer in 1966 by means of a technique involving the construction and extrapolation of functions of several complex variables. He was thereby able to furnish, amongst other things, effective proofs of Thue's theorem on binary forms, of Mordell's theorem on the equation (*), of Siegel's theorem on the hyperelliptic equation and, in a joint work with Coates, an explicit bound for all the integer points on an arbitrary curve of genus 1 (for references, see **[1]**). In the decade that has now elapsed since the time of these discoveries the theories have been extensively developed. In particular, the basic inequalities on linear forms in logarithms have been greatly improved, and results of similar strength have been established in the p-adic domain. These have led to the effective resolution of a wide variety of Diophantine equations, many of which would seem to lie well beyond the scope of the earlier methods. An especially striking example is the demonstration by Tijdeman that all solutions x, y, m, n of the Catalan equation $x^m - y^n = 1$ can be effectively bounded. In another direction, Masser **[4]** obtained in 1975 certain analogues of the basic inequalities relating to elliptic logarithms, and these have themselves generated much further research.

We come now to the book by Lang under review. First the title might perhaps lead the reader to expect an account of the rational theory such as Cassels describes in **[3]**. If so, he will be largely disappointed. Although there is a discussion of the Mordell-Weil theorem, including preliminaries on the Weierstrass functions, and there is also a chapter on p-adic studies, including certain results of Tate, the main *raison d'être* of the book is apparently to furnish an account of the effective method of analysis introduced by the reviewer, and, in particular, its application to the integral theory of elliptic curves. In fact at least a third of the text is devoted to the theory of linear forms in logarithms. The reviewer did not find the exposition illuminating. Indeed the author's characteristically loose style of writing seemed palpably unsuited to this intricate field. It would be pointless to give a detailed criticism, but note the fallacious proofs of Theorems 5.1 to 5.4 where the box principle has been incorrectly applied. Note also the author's obvious failure to appreciate the difference between the polynomials that occur in the early papers of Feldman and the Δ-functions that were introduced by the reviewer in his 'sharpening' series; a good discussion of the distinction is given by Cijsouw in Chapter 5 of [2]. Actually the latter volume, that is, *Transcendence theory: advances and applications*, supersedes much of the text under review. In particular, all the results on linear forms in logarithms are included in a more refined theorem that is proved by the reviewer in Chapter 1 of [2], and the paper by Anderson in Chapter 7 of [2] on elliptic logarithms substantially improves upon the author's Chapter IX. The latter work involves, amongst other things, a theorem of Bashmakov yielding an elliptic analogue of Kummer theory, and the author devotes some twelve pages to its demonstration. Anderson's paper contains an Appendix by Masser giving a proof of the special case utilized there that is both shorter and avoids the language of cohomology.

In Chapter VI, which can be regarded as the kernel of the book, the author discusses the effective solution of Diophantine equations. The ground covered is similar to that of Chapter 4 of [1], but the author seems eager to record his own version of the historical importance of various earlier works in the field, and, in the reviewer's opinion, the picture he presents is very distorted. For instance, much prominence is given to an originally obscure and partly erroneous paper of Chabauty, with the suggestion that it played a significant role in the work of Coates and the reviewer on curves of genus 1. Actually it played no role whatsoever, and it was only with hindsight that the paper came to light. Though Tijdeman's work on Catalan's equation is discussed later in the book, the author makes no reference to more recent work in Diophantine analysis, such as that described in Chapter 3 of [2]. Furthermore, the extensive p-adic theory of linear forms in logarithms, as discussed by van der Poorten in Chapter 2 of [2], is mentioned by the author only in passing.

It is clear that valiant efforts to improve the text have been made by the author's young collaborator Michel Waldschmidt, and the work has certainly benefited from his attention (see, for example, pages 151 and 234). Moreover there are some novelties, such as the conjectures on pages 212 and 213, and the utilization of a height function that is conveniently semimultiplicative. But many shortcomings remain, and it seems a pity to the reviewer that such an excellent theme for the Grundlehren series did not receive better treatment.

References

1. A. Baker, *Transcendental number theory*, Cambridge Univ. Press, 1975.
2. A. Baker and D. W. Masser (editors), *Transcendence theory: advances and applications*, Academic Press, New York, 1977, Proceedings of a Conference held in Cambridge in 1976.
3. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.
4. D. W. Masser, *Elliptic functions and transcendence*, Lecture Notes in Math., vol. 437, Springer-Verlag, Berlin and New York, 1975.
5. L. J. Mordell, *Diophantine equations*, Academic Press, New York, 1969.

Alan Baker