BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 38, Number 3, Pages 379–381
S 0273-0979(01)00907-7
Article electronically published on March 27, 2001

Diophantine geometry: An introduction, by Marc Hindry and Joseph H. Silverman, Graduate Texts in Mathematics, vol. 201, Springer, New York, 2000, xii+ 558 pp., \$69.95, ISBN 0-387-98975-7; \$39.95, ISBN 0-387-98981-1 (paperbound)

The field of Diophantine geometry was named by Serge Lang in 1961, but the roots of the subject go back at least as far as the 1840's. In that decade, Dirichlet and Liouville respectively proved these two fundamental results:

Theorem 1. *Suppose that α is a real irrational number. Then there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ so that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Theorem 2. *Suppose that α is a real algebraic irrational number of degree d. Let $\epsilon > 0$ be a fixed constant. Then there are finitely many $\frac{p}{q} \in \mathbb{Q}$ so that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{d+\epsilon}}.$$

The key tools in proving these theorems are the pigeonhole principle and the observation that the smallest positive integer is 1. These techniques still underlie many of the proofs in this subject.

If α is an algebraic number of degree $d > 2$, then it is natural to wonder if either of these theorems can be sharpened. Theorem 1 can be improved slightly, but the real interest is in decreasing the exponent in Theorem 2. Liouville used the minimal polynomial for α (vanishing at α and not at $\frac{p}{q}$) to derive his result. In 1909, Thue used a polynomial in two variables of the form $f(X)+g(X)Y$ (vanishing at $X = Y = \alpha$ but not at nearby rational numbers) to decrease the exponent in Theorem 2 to $\frac{d}{2} + 1 + \epsilon$. In 1921, Siegel used a general polynomial in 2 variables to decrease the exponent to $2\sqrt{d} + \epsilon$. In 1947, Gelfand and Dyson independently refined Siegel's methods to change the exponent to $\sqrt{2d} + \epsilon$. In 1955, Roth used a general polynomial in an unrestricted number of variables to decrease the exponent to $2 + \epsilon$.

Roth's result is far from the last word. Even before 1955, versions of the theorem had been proved both for number fields other than $\mathbb{Q}$, and for p-adic absolute values. After Roth, Schmidt extended the theorem to systems of inequalities. In the 1980's, Vojta interpreted Roth's Theorem as analogous to a classical result from Nevanlinna Theory.

There are at least 2 common applications of Roth's Theorem, and both of them can be proved using the version known to Siegel. In the 1920's, Siegel proved

Theorem 3. *Assume that C is a smooth projective curve of genus $g \geq 1$ defined over a number field K. Then there are only finitely many points on C with coordinates in the ring of integers of K.*

2000 *Mathematics Subject Classification.* Primary 11Gxx, 14Gxx.

More generally, let S be a finite set of primes of K, including all of the infinite places, and set

$$R_S = \{k \in K : |k|_v \leq 1 \text{ if } v \notin S\}$$
$$R_S^* = \{k \in K : |k|_v = 1 \text{ if } v \notin S\}.$$

Siegel's methods can be used to show that the set of points on C with coordinates in R_S is finite.

At around the same time, Siegel and Mahler proved

Theorem 4. *There are only finitely many solutions to the equation*

$$U + V = 1$$

with $U, V \in R_S^*$.

Two other basic results of the field also have their roots in the 1920's. In 1922, Mordell conjectured that there are only finitely many rational points on a curve of genus $g \geq 2$. In 1983, Faltings proved this result, along with many other conjectures, using techniques associated with the theory of elliptic curves. This statement is now known as the Mordell-Faltings Theorem.

Some years later, Vojta gave a different proof of this theorem, since simplified by Bombieri, using ideas related to those in the proof of Roth's theorem. The theory of heights and the notion of a theta divisor allow one to define a norm $|\cdot|$ and associated inner product $\langle \cdot, \cdot \rangle$ on a curve C. The key lemma in Vojta's proof uses these to quantify how close points on such a curve can be:

Theorem 5. *Suppose that* K *is a number field, and* C *a smooth projective curve of genus* $g \geq 2$ *defined over* K. *Then there are constants* $\kappa_1 = \kappa_1(C)$ *and* $\kappa_2 = \kappa_2(g)$ *so that if* $z, w \in C(\bar{K})$, *satisfying* $|z| \geq \kappa_1$ *and* $|w| \geq \kappa_2 |z|$, *then*

$$\langle z, w \rangle \leq \frac{3}{4} |z| \, |w| \, .$$

Another fundamental result of the 1920's was proved by Mordell in 1922 (for elliptic curves and $\mathbb{Q}$) and Weil in 1928 (for abelian varieties and arbitrary number fields):

Theorem 6. *Suppose that* A *is an abelian variety defined over a number field* K. *Then the group* $A(K)$ *of points on* A *defined over* K *is finitely generated.*

This statement is proved by showing that there is an integer $m > 1$ so that the quotient group $A(K)/mA(K)$ is finite, and then applying the theory of heights (which is also used in proving the other results above) to deduce that $A(K)$ is finitely generated.

As noted, this subject depends on the theory of heights. The current text develops this material in the second chapter. (The first chapter is devoted to preliminaries from algebraic geometry, and the authors advise, correctly, that the reader should either browse the first chapter or skip over it entirely.) Succeeding chapters prove the theorems above. A concluding chapter, a bit more difficult than the first five, is devoted to some further results (mostly without proof) and many open problems. Each chapter contains many exercises of varying levels of difficulty.

One interesting problem in this field is that of stating quantitative results. Without going into too much detail, this text clarifies how one could replace the word "finite" with computable constants in some of these theorems. At the same time, the authors explain the difference between quantitative results and effective ones: for example, there is no algorithm guaranteed to find a complete set of solutions to the inequality in Roth's theorem. Hindry and Silverman clarify why this problem is intrinsic to the method of proof used.

The obvious comparison is with Lang's treatise [1], formerly the primary reference for this material. One major distinction in content is that [1] includes a proof of Hilbert's Irreducibility Theorem. However, this theorem and its proof are different in flavor from the other material, justifying their exclusion from the present text. Instead, Hindry and Silverman have included a proof of the Mordell-Faltings Theorem. The present text is more suitable than Lang's work for classroom use, because of the inclusion of exercises and the presentation of material in slightly less generality.

References

1. Lang, Serge. *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983. MR **85j:**11005

Robert Gross
Boston College
E-mail address: gross@bc.edu