Journal of Number Theory, Vol. 36, No. 1, September, 1990, pages 127–132

A Note on Roth's Theorem

Robert Gross

Abstract

We give a quantitative version of Roth's Theorem over an arbitrary number field, similar to that given by Bombieri and van der Poorten.

Introduction. Let $K/\mathbf{Q}$ be a number field, with $[K:\mathbf{Q}]=d$. Let M_K be a complete set of inequivalent absolute values on K, normalized so that the absolute logarithmic height is given by $h:\overline{K}\to[0,\infty)$,

$$h(x)=\sum_{v\in M_L}\max\{-v(x),0\}$$

where L/K is any extension of K containing x. Let S be a finite subset of M_K, containing S_∞, the archimedean places, with each place extended to $\overline{K}$. Let s be the number of elements in S. Silverman [7] gives the following statement of Roth's Theorem:

Theorem A. *Let Υ be a finite Gal($\overline{K}/K$)-invariant subset of $\overline{K}$. Let α be a map of S to Υ. Let $\mu>2$ and $M\ge 0$ be constants. Then there are constants c_1 and c_2, depending only on d, $\#\Upsilon$, and μ, such that there are at most $4^s c_1$ elements $x\in K$ satisfying both of the following conditions:*

$$\sum_{v\in S}v(x-\alpha_v)\ge \mu h(x)-M$$

$$h(x)\ge c_2\max_{v\in S}\{h(\alpha_v),M,1\}.$$

Silverman notes, "This type of result is well-known, although this exact formulation does not appear in the literature."

In this note, we prove an explicit form of Silverman's theorem; we will use our result in a future paper concerning integral points on elliptic curves.

Theorem B. *Let $\mu=2+\zeta$, let $\zeta'=\zeta/2$, $\mu'=2+\zeta'$, $\zeta''=\min\{\zeta/4,3/\sqrt{7}\}$, and $\mu''=2+\zeta''$. Let $r=\#\Upsilon$. Let $n=[36\log r/\zeta''^2]+1$ (so that $\zeta''\ge 6\sqrt{\log r}/\sqrt{n}$). Let $\eta=(2n)!^{-1}$. Then Theorem A is true for constants c_1 and c_2 given by*

$$c_1=n-1+(n-1)\frac{\log 5rn/\eta}{\log(1+\zeta'')}$$

and

$$c_2=\frac{5\log 4}{2\eta\zeta''}.$$

Because these constants are independent of $[K:\mathbf{Q}]=d$, our result is stronger than Silverman's statement.

This type of result over $\mathbf{Q}$ at the archimedean place is nearly as old as Roth's original theorem. The first statement is in Davenport and Roth [2], with the best result using Siegel's lemma in Mignotte [6]. The best p-adic statement over $\mathbf{Q}$ may be found in Lewis and Mahler [5]. Recently, Bombieri and van der Poorten [1] have improved the previous estimates by using a strengthened form of Dyson's Lemma [3] due to Esnault and Viehweg [4].

For many applications, knowledge of the constants c_1 and c_2 for a fixed small value of ζ suffices. The following corollary is often helpful:

Corollary. *Let $\mu=2.5$, and suppose that $\#\Upsilon=r$. Let $n=[2304\log r]+1$. Then*

$$c_1=n-1+8.5(n-1)\log(5rn(2n)!)$$

and

$$c_2=28(2n)!.$$

Preliminaries. Silverman [7] gives the following lemma, an axiomatic form of what is often called "reduction to simultaneous approximation":

Lemma. *Let Γ be a set, S a finite set containing s elements, and $\phi : \Gamma \times S \to [0, \infty)$. For every $\epsilon > 0$ and each function $\xi : S \to [0, 1]$, let*

$$\Gamma(\epsilon) = \{P \in \Gamma : \sum_{v \in S} \phi(P, v) \geq \epsilon\}$$
$$\Gamma(\epsilon, \xi) = \{P \in \Gamma : \phi(P, v) \geq \epsilon \xi_v \text{ for all } v \in S\}.$$

Now fix $N \geq s$. Then there is a collection of functions Ξ, where each $\xi \in \Xi$ maps S to $[0, 1]$, such that
(1) *For each $\xi \in \Xi$, $\sum_{v \in S} \xi_v = 1$.*
(2) $\#\Xi \leq \binom{N-1}{s-1}$.
(3) $\Gamma(\epsilon) \subset \cup_{\xi \in \Xi} \Gamma\left((1 - \frac{s}{N})\epsilon, \xi\right)$.
In particular,

$$\#\Gamma(\epsilon) \leq 2^N \sup \#\Gamma\left((1 - \frac{s}{N})\epsilon, \xi\right),$$

where the supremum is taken over all functions $\xi : S \to [0, 1]$ satisfying $\sum \xi_v = 1$.

If we now apply this result with $N = 2s$, we may dispense with the summation in Roth's theorem, and deal with one absolute value at a time, at the cost of using $\mu' = 2 + \zeta'$ rather than μ. In other words, we are bounding the number of solutions to

$$|x - \alpha|_v \leq \frac{C}{H(x)^{\mu'}}$$

where $M = \log C$.

We make yet another simplification. For reasons which will shortly become apparent, we wish to deal with an inequality of the form

$$|x - \alpha|_v \leq \frac{1}{64 H(x)^{\mu''}}.$$

This follows if

$$64C \leq H(x)^{\zeta''},$$

which can be insured if

$$h(x) \geq \frac{2 \log 64}{\zeta''} \max\{1, \log C\}.$$

Since this condition is weaker than our later bound on $h(x)$, it does not appear in the statement of Theorem B.

The Proof. Bombieri and van der Poorten [1] give us the following remarkable result:

Theorem C. *Let $\alpha_1, \ldots, \alpha_n$ be elements of a number field K of degree r over the field k, with each α_i of exact degree r over k. Suppose $n \geq c_0 \log r$ (where c_0 is a sufficiently large constant), and set η such that $0 < \eta < 1/2n!$. Let $\beta_i \in k$ be approximations to α_i, $i = 1, \ldots, n$ such that we have the gap conditions*

$$\frac{1}{\eta} \log(4H(\alpha_{i+1})) + \log(4H(\beta_{i+1})) \geq \frac{4rn}{\eta}\left(\frac{1}{\eta} \log(4H(\alpha_i)) + \log(4H(\beta_i))\right).$$

Then

$$|\alpha_i - \beta_i|_v \geq \left((4H(\alpha_i))^{1/\eta} 4H(\beta_i)\right)^{-2-3\sqrt{\log r}/\sqrt{n}}$$

for at least one i, $1 \leq i \leq n$.

The authors note at the end of the proof that $c_0 = 28$ is a sufficiently large value. Note that this result does not depend on $[k : \mathbf{Q}]$.

Following the argument in [1], suppose that

$$4h(x) \geq \frac{10\log 4}{\eta\zeta''}\max\{h(\alpha), 1\}.$$

Then $4h(x) \geq \frac{5}{\eta\zeta''}(h(\alpha) + \log 4)$, or

$$4H(x) \geq (4H(\alpha))^{5/\eta\zeta''}.$$

Let $r = \#\Upsilon = [K(\alpha) : K]$. Let n be the smallest integer so that $\zeta'' \geq 6\sqrt{\log r}/\sqrt{n}$; this also implies that $n \geq 28\log r$, because $\zeta'' \leq 3/\sqrt{7}$.

Recall that we are trying to count solutions of

$$|\alpha - x|_v \leq \frac{1}{64H(x)^{2+\zeta''}}.$$

If $4H(x) \geq (4H(\alpha))^{5/\eta\zeta''}$, then we have

$$\frac{1}{64}H(x)^{-2-\zeta''} \leq (4H(x))^{-2-\zeta''} \leq \Big((4H(\alpha))^{1/\eta}4H(x)\Big)^{-2-\zeta''/2}.$$

Therefore, the solutions satisfying $h(x) \geq c_2 h(\alpha)$ must in fact satisfy

$$|\alpha - x|_v \leq \Big((4H(\alpha))^{1/\eta}4H(x)\Big)^{-2-3\sqrt{\log r}/\sqrt{n}}.$$

Solutions of this inequality can be classified into intervals I_i with

$$\log(4H(x)) \in \left[\log(4H(\beta_i)), \frac{4rn}{\eta}\left(\frac{1}{\eta}\log(4H(\alpha)) + \log(4H(\beta_i))\right)\right],$$

where the β_i are solutions of

$$|\alpha - \beta_i|_v \leq H(\beta_i)^{-2-\zeta''}$$

chosen inductively to be the minimal solutions of

$$\log(4H(\beta_1)) > \frac{5}{\eta\zeta''}\log(4H(\alpha))$$

and

$$\log(4H(\beta_{i+1})) > \frac{4rn}{\eta}\left(\frac{1}{\eta}\log(4H(\alpha)) + \log(4H(\beta_i))\right).$$

Theorem C says that there are at most $n-1$ intervals I_i. Therefore, we have only to count the number of solutions in each interval.

Let x, y be distinct elements of some interval I_i satisfying

$$|\alpha - x|_v < \frac{1}{64H(x)^{2+\zeta''}}$$
$$|\alpha - y|_v < \frac{1}{64H(y)^{2+\zeta''}}$$
$$H(x) < H(y)$$

Then

$$\frac{1}{2H(x)H(y)} \leq |x-y|_v \leq |\alpha - x|_v + |\alpha - y|_v \leq \frac{1}{32H(x)^{2+\zeta''}}$$

so that

$$4H(y) > 4(4H(x))^{1+\zeta''}.$$

Therefore, if there are n_i solutions in I_i, we have

$$\begin{aligned}(4H(\beta_i))^{(1+\zeta'')^{n_i-1}} &\leq \Big((4H(\alpha))^{1/\eta}(4H(\beta_i))\Big)^{4rn/\eta} \\ &\leq \Big((4H(\beta_1))^{\zeta''/5}\,(4H(\beta_i))\Big)^{4rn/\eta} \\ &\leq (4H(\beta_i))^{5rn/\eta}.\end{aligned}$$

This implies that

$$(1+\zeta'')^{n_i-1} \leq \frac{5rn}{\eta}$$

and then

$$n_i \leq 1 + \frac{\log 5rn - \log \eta}{\log(1+\zeta'')}.$$

Since there are $n-1$ of these sets, the result follows. □

Department of Mathematics, Boston College, Chestnut Hill, MA 02167

Bibliography

1. Bombieri, E., A. J. van der Poorten. Some quantitative results related to Roth's Theorem. *J. Australian Math. Soc. A* **45** (1988), 233—248.
2. Davenport, H., K. Roth. Rational approximations to algebraic numbers. *Mathematika* **2** (1955), 160—167.
3. Dyson, Freeman. The Approximation to Algebraic Numbers by Rationals. *Acta Math.* **79** (1947), 225—240.
4. Esnault, Hélène, Eckart Viehweg. Dyson's Lemma for polynomials in several variables (and the theorem of Roth). *Invent. Math* **78** (1984), 445—490.
5. Lewis, D.J., K. Mahler. On the representation of integers by binary forms. *Acta Arith.* **6** (1961), 333—363.
6. Mignotte, Maurice. Quelques remarques sur l'approximation rationelle de nombres algébriques. *J. reine angew. Math.* **268/269** (1974), 341—347.
7. Silverman, Joseph. A Quantitative Version of Siegel's Theorem: integral points on elliptic curves and Catalan curves. *J. reine angew. Math.* **378** (1987), 60—100.