J. Austral. Math. Soc. (*Series A*) **59** (1995), 375–383

THE NUMBER OF EXCEPTIONAL APPROXIMATIONS IN ROTH'S THEOREM

WOLFGANG M. SCHMIDT

(Received 24 November 1993)

Communicated by J. H. Loxton

Abstract

Roth's Theorem says that given $\rho > 2$ and an algebraic number α, all but finitely many rational numbers x/y satisfy $|\alpha - (x/y)| > |y|^{-\rho}$. We give upper bounds for the number of these exceptional rationals when $3 \le \rho \le d$, where d is the degree of α. Our result supplements bounds given by Bombieri and Van der Poorten when $2 < \rho \le 3$; naturally the bounds become smaller as ρ increases.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 11J68.

1. Introduction

THEOREM 1. *Suppose that $\rho \ge 3$ and that α is algebraic of degree $d \ge \rho$. Let $h(\alpha)$ be the (multiplicative) height of α as discussed below. Then the number of reduced rationals x/y (with $y > 0$) having*

$$\left|\alpha - \frac{x}{y}\right| < y^{-\rho} \tag{1.1}$$

is at most

$$\frac{\log^+ \log h(\alpha)}{\log(\rho - 1)} + O\left(\left(\frac{\log d}{\log \rho}\right)^2 \left(1 + \frac{\log\log d}{\log \rho}\right)\right). \tag{1.2}$$

The number of such rationals with

$$y \ge h(\alpha) \tag{1.3}$$

is bounded by the second summand in (1.2), *that is, it is*

$$\ll ((\log d/\log \rho)^2(1 + (\log\log d)/\log \rho). \tag{1.4}$$

Supported in part by NSF grant DMS-9108581

Here $\log^+ x = \log x$ when $x \geq e$, and $\log^+ x = 1$ otherwise. Throughout, the constants implicit in big "O" and $\ll$ are absolute. As was shown in [2, Ch. II, Theorem 9C], the first summand in (1.2) is best possible, in the sense that it would become false if $\log(\rho - 1)$ were replaced by a larger quantity. Our theorem supplements Theorem 9B of [2, Ch. II] (which was essentially given in [1]) where the case $2 < \rho < 3$ had been considered. In that case, with $\delta = \rho - 2$ satisfying $0 < \delta < 1$, we had at most

$$\frac{\log^+ \log h(\alpha)}{\log(\rho - 1)} + O(\delta^{-5}(\log d)^2(\log \delta^{-1} + \log\log d)) \tag{1.5}$$

solutions.

The theorem remains correct for a wide choice of heights $h(\alpha)$. For instance we may take $h(\alpha)$ to be any of $H_1(\alpha)$, $H_2(\alpha)$, $H_3(\alpha)$, $h_1(\alpha)$, $h_2(\alpha)$, $h_3(\alpha)$, which are defined as follows. $H_1(\alpha)$ is the most naive height, that is, the maximum modulus of the coefficients of the defining polynomial of α over $\mathbb{Z}$, with these coefficients coprime. $H_2(\alpha)$ is the Mahler measure, that is,

$$H_2(\alpha) = \prod_{v \in M(K)} \max(1, |\alpha|_v)^{n_v} \tag{1.6}$$

where $K = \mathbb{Q}(\alpha)$, $M(K)$ indexes the absolute values of K which extend the ordinary or a p-adic absolute value of $\mathbb{Q}$, and the n_v are the local degrees. $H_3(\alpha)$ is a variation on $H_2(\alpha)$, where for v archimedean the factor $\max(1, |\alpha|_v)$ in (1.6) is replaced by $(1 + |\alpha|_v^2)^{1/2}$. Finally $h_i(\alpha) = H_i(\alpha)^{1/d}$ $(i = 1, 2, 3)$.

Our proofs will be close to those in [2], and we will often refer to that work. A new ingredient will be an estimate of volumes inspired by ideas of Wirsing.

2. Location of the exceptions to Roth's Theorem

Following the definition in [2, §II.6], an interval of real numbers of the type $X \leq \xi < X^C$ with $X > 1$ will be called a *window of exponential width* C. Given $C > 1$, such a window can be arbitrarily long if we don't have information on X. *In what follows, $h(\alpha)$ will be $h_3(\alpha)$*, unless stated otherwise. Accordingly, the height of a rational number $\beta = x/y$ in reduced form is $h(\beta) = (x^2 + y^2)^{1/2}$.

THEOREM 2. *Suppose α is algebraic of degree $d \geq 3$. Suppose natural $m \geq 2$ and real λ, T have $T \geq 1$ and*

(i) $m \log(mT/8) \geq \log d$,

(ii) $\lambda \geq 2m!T^m$.

Then the rational solutions β of the inequality

$$|\alpha - \beta| < h(\beta)^{-10d^{1/m}} \tag{2.1}$$

https://doi.org/10.1017/S1446788700037277 Published online by Cambridge University Press

have their heights in the union of the interval

$$h(\beta) < 260(4h(\alpha))^{4\lambda} = B, \tag{2.2}$$

say, and at most $m - 1$ *windows of exponential width*

$$C = 6dm\lambda. \tag{2.3}$$

This theorem is analogous to Theorem 6A of [2, Ch. II]. The proof is postponed. Here we will deduce Theorem 1 from Theorem 2.

Clearly $H_2(\alpha) \leq H_3(\alpha) \leq 2^{d/2}H_2(\alpha)$, and $2^{-d}H_2(\alpha) \leq H_1(\alpha) < 2^dH_2(\alpha)$ as demonstrated, for instance, in [3, Ch. VIII, Theorem 5.9]. Therefore the six quantities $\log\log H_i(\alpha)$ and $\log\log h_i(\alpha)$ $(i = 1, 2, 3)$ differ from each other by $\ll \log d$, so that the bound (1.2) with $h(\alpha)$ any of these implies it for the others. Thus in the proof of (1.2) we may take $h(\alpha) = h_3(\alpha)$. On the other hand, since $h_0(\alpha) =: \min(h_1(\alpha), h_2(\alpha))$ is the smallest of the six quantities, we will prove the second assertion of Theorem 1 with $h = h_0$ in (1.3).

In what follows, observe that $d \geq \rho \geq 3$, so that $\log\log d \geq \log\log 3 > 0$. We set

$$m = \{c \log d / \log \rho\} \tag{2.4}$$

where $\{\ \ \}$ denotes the next largest integer and c is a large constant yet to be chosen. We further set

$$T = \begin{cases} 1 & \text{if} \quad \rho < \log d, \\ (\rho \log \rho)/\log d & \text{if} \quad \rho \geq \log d, \end{cases} \tag{2.5}$$

as well as

$$\lambda = 2(mT)^m. \tag{2.6}$$

We have $T \geq 1$, and the two cases in (2.5) yield respectively

$$mT = m \geq (c \log d)/\log\log d > 8(\log d)^{3/4} > 8\rho^{3/4},$$
$$mT \geq c\rho > 8\rho^{3/4}$$

provided c is large enough, and therefore

$$m \log(mT/8) > c\frac{\log d}{\log \rho} \log \rho^{3/4} > \log d.$$

Both (i), (ii) of Theorem 2 hold. Also $\log \lambda > m \log(mT) > \log d$, so that

$$\lambda > d; \tag{2.7}$$

and

$$\rho > d^{c/m} > 20d^{1/m} \tag{2.8}$$

https://doi.org/10.1017/S1446788700037277 Published online by Cambridge University Press

directly from (2.4). Depending on the cases in (2.5) we have $mT = m \ll \log d$ or $mT \ll \rho$, so that in general

$$\log \lambda \ll m(\log \rho + \log\log d). \tag{2.9}$$

We now define B, C, by (2.2), (2.3), and then $\log B = 4\lambda \log(4h(\alpha)) + O(1)$, therefore

$$\log\log B \le \log^+\log h(\alpha) + O(\log\lambda) = \log^+\log h(\alpha) + O(m(\log\rho + \log\log d), \tag{2.10}$$

and similarly

$$\log 2C \le \log\lambda + \log d + \log m + O(1) \ll m(\log\rho + \log\log d). \tag{2.11}$$

We first will estimate the number of "small" solutions of (1.1), that is, solutions with $1 \le y < B$. The approximations x/y with (1.1) are, in the language of [2], δ-approximations with $\delta = \rho - 2$. The approximations with $4 \le y \le B$ lie in a window $W \le y \le W^\gamma$ with $\gamma = \log B/\log 4 < \log B$. By Lemma 8C in [2, Ch. II], the number of such approximations is

$$\le 1 + (\log 2\gamma)/L$$

where $L = \log(1+\delta) = \log(\rho - 1)$. The number of possible solutions with $y = 1, 2$ or 3 is bounded, so that the number of small solutions is

$$\le L^{-1}\log\gamma + O(1) = L^{-1}\log\log B + O(1)$$
$$\le L^{-1}\log^+\log h(\alpha) + O(m(1 + (\log\log d/\log\rho))) \tag{2.12}$$

by (2.10) and since $L \gg \log\rho$.

We now turn to the "large" solutions, that is, those with $y > B$. With $\beta = x/y$ we have $|x/y| < |\alpha| + 1$, therefore

$$h(\beta) \le |x| + |y| < (|\alpha| + 2)y < 3h(\alpha)^d y$$

(where the exponent d is needed since $h(\alpha) = h_3(\alpha) = H_3(\alpha)^{1/d}$). On the other hand $y \ge B > (4h(\alpha))^{4\lambda} > (3h(\alpha))^{4d}$ by (2.7), so that $h(\beta) < y^{5/4}$, and (1.1) yields

$$|\alpha - \beta| < h(\beta)^{-4\rho/5} < h(\beta)^{-10d^{1/m}} \tag{2.13}$$

in view of (2.8). By Theorem 2, the solutions with $h(\beta) \ge y \ge B$ lie in at most $m - 1$ windows of exponential width C. By Lemma 8C in [2], the number of approximations β with (2.13) and with y in such a window is $\le 1 + (\log 2C)/L'$ with $L' = \log((4\rho/5) - 1) \gg \log\rho$. In view of (2.11) we obtain

$$\ll 1 + (\log 2C)/\log\rho \ll m(1 + \log\log d/\log\rho).$$

https://doi.org/10.1017/S1446788700037277 Published online by Cambridge University Press

We have to multiply by the number $m-1$ of possible windows. Adding the estimate (2.12), we obtain the bound

$$\leq L^{-1}\log^+\log h(\alpha) + O(m^2(1+\log\log d/\log\rho))$$

for the total number of solutions to (1.1). By our definition (2.4) of m, the first assertion of Theorem 1 follows.

In the course of our arguments we have shown that the number of solutions with $y \geq B$ is bounded by (1.4). In order to verify the second assertion of Theorem 1 it remains for us to estimate the number of solutions with $h_0(\alpha) \leq y \leq B$. Since there are at most 2 solutions with $y = 1$, we may restrict to

$$\hbar(\alpha) \leq y \leq B \tag{2.14}$$

where $\hbar(\alpha) =: \max(2, h_0(\alpha))$. By the comparison of heights $H_i(\alpha)$ given above,

$$h_0(\alpha) = \min(h_1(\alpha), h_2(\alpha)) \geq 2^{-1}h_2(\alpha) \geq 2^{-3/2}h_3(\alpha) = 2^{-3/2}h(\alpha).$$

Therefore $\log\hbar((\alpha) \gg \log(4h(\alpha))$, so that (2.14) is a window of exponential width

$$w = \log B/\log\hbar(\alpha) \ll \log B/\log(4h(\alpha)) \ll \lambda$$

by (2.2). By Lemma 8C of [2] again, the number of our approximations is

$$\leq 1 + (\log 2w)/\log(\rho-1) \ll 1 + (\log\lambda)/\log\rho \ll m(1+\log\log d/\log\rho)$$

by (2.9). Since m is given by (2.4), this is amply bounded by (1.4).

When $2 < \rho < 3$, the argument in [2] can be modified in an analogous way to show that the number of solutions of (1.1) with (1.3) is bounded by the second summand in (1.5).

3. A more general theorem

Given $\lambda > 0$ we define the *mixed height* of numbers α, β by

$$H_\lambda(\alpha,\beta) = (4h(\alpha))^\lambda \cdot 4h(\beta).$$

THEOREM 3. *Let K be a number field of degree d. Suppose natural $m \geq 2$ and real λ, T have $T \geq 1$ and* (i), (ii) *of Theorem* 2. *Let $(\alpha_1,\beta_1),\ldots,(\alpha_m,\beta_m)$ be such that $\mathbb{Q}(\alpha_i) = K$ and $\beta_i \in \mathbb{Q}$ $(i = 1,\ldots,m)$. Suppose further that*

(iii) $|\alpha_i - \beta_i| < h_\lambda(\alpha_i,\beta_i)^{-8d^{1/m}}$ $(i = 1,\ldots,m)$,

(iv) $h_\lambda(\alpha_{i+1},\beta_{i+1}) > h_\lambda(\alpha_i,\beta_i)^{3dm\lambda}$ $(i = 1,\ldots,m-1)$.

This is impossible.

https://doi.org/10.1017/S1446788700037277 Published online by Cambridge University Press

This is analogous to Theorem 6A of [2, Ch. II]. Let us first derive Theorem 2 from it. (2.1), (2.2) yield

$$|\alpha - \beta| < h(\beta)^{-8d^{1/m}} B^{-2d^{1/m}} < h(\beta)^{-8d^{1/m}} (4(4h(\alpha))^{\lambda})^{-8d^{1/m}} = h_\lambda(\alpha, \beta)^{-8d^{1/m}}.$$

If there is no approximation with $h(\beta) \geq B$, we are finished. Otherwise, let β_1 have minimal height with $h(\beta_1) \geq B$. If every β with (2.1) and $h(\beta) \geq B$ has $h(\beta) < h(\beta_1)^{6dm\lambda}$, then all these β lie in a single window of exponential width $C = 6dm\lambda$, and we are done. Otherwise, let β_2 have minimal height with $h(\beta_2) \geq h(\beta_1)^{6dm\lambda}$. Then

$$h_\lambda(\alpha, \beta_2) > h(\beta_2) \geq h(\beta_1)^{3dm\lambda} B^{3dm\lambda} \geq (h(\beta_1)(8h(\alpha))^{\lambda})^{3dm\lambda} \geq h_\lambda(\alpha, \beta_1)^{3dm\lambda}.$$

Continue in this fashion. If the solutions with $h(\beta) \geq B$ do not lie in $m - 1$ windows of exponential width C, then $\beta_1, \dots, \beta_m$ can be found such that the pairs $(\alpha, \beta_1), \dots, (\alpha, \beta_m)$ satisfy the conditions of Theorem 3, and we reach a contradiction.

THEOREM 4. *Let $V_m(t)$ be the volume of the intersection of the cube $0 \leq x_i \leq 1$ $(i = 1, \dots, m)$ in $\mathbb{R}^m$ with the half-space $x_1 + \cdots + x_m \leq t$. Then we have*

$$V_m(t) < (e(1 + e^{-m/t})t/m)^m.$$

We postpone the proof of this to the last section. Instead, we will now derive Theorem 3.

The beginning of the argument is as in [2, §II.7]. Suppose we have pairs (α_i, β_i) $(i = 1, \dots, m)$ with $\mathbb{Q}(\alpha_i) = K$, $\beta_i \in \mathbb{Q}$, $|\alpha_i - \beta_i| < h_\lambda(\alpha_i, \beta_i)^{-\psi}$, and with (iv). Then (7.4) of [2, Ch. II] holds, that is,

$$\psi \leq \frac{m}{t - \tau}. \tag{3.1}$$

Here t, τ were given in [2] by $dV_m(t) = 1 - \lambda^{-1}$, $V_m(\tau) = 2/\lambda \leq 1/(m!T^m)$ by (ii). In particular, $V_m(\tau) \leq 1/m!$, and in this case $V_m(\tau)$ is the volume of a certain simplex, and $V_m(\tau) = \tau^m/m!$. Therefore $\tau \leq 1/T$. We will show that

$$t > m/(4d^{1/m}). \tag{3.2}$$

If (3.2) were false, then $m/t > 4$ and $e(1 + e^{-m/t}) < 3$. Now Theorem 4 gives $(3t/m)^m > V_m(t) = d^{-1}(1 - \lambda^{-1}) \geq (3/4)d^{-1}$ since $\lambda \geq 2m \geq 4$, so that

$$t \geq (m/3)(3/4)^{1/m} d^{-1/m} > (m/4)d^{-1/m},$$

and (3.2) holds after all. This and our estimate of τ yield

$$t - \tau > (m/4)d^{-1/m} - T^{-1} \geq (m/8)d^{-1/m}$$

by (i), so that $\psi < 8d^{1/m}$ by (3.1). This finishes the proof of Theorem 3.

4. Estimation of volumes

Although our estimate is perhaps known, our short argument should be convenient for the reader. As was pointed out in the Introduction, the basic ideas are due to Wirsing. Note that

$$V_1(t) = \begin{cases} 0 & \text{if } t \le 0, \\ t & \text{if } 0 \le t \le 1, \\ 1 & \text{if } t \ge 1, \end{cases} \tag{3.2}$$

so that the derivative $V_1'(t)$ exists for $t \neq 0, 1$, with $V_1'(t) = 1$ for $0 < t < 1$ and $V_1'(t) = 0$ otherwise. Now

$$\begin{aligned} V_{n+1}(t) &= \int\cdots\int_{\substack{0\le x_1,\dots,x_{n+1}\le 1 \\ x_1+\cdots+x_{n+1}\le t}} dx_1\cdots dx_{n+1} \\ &= \int_0^1 \Bigg(\int\cdots\int_{\substack{0\le x_1,\dots,x_n\le 1 \\ x_1+\cdots+x_n\le t-x_{n+1}}} dx_1\cdots dx_n \Bigg) dx_{n+1} \\ &= \int_0^1 V_n(t-x_{n+1})dx_{n+1} = \int_{\mathbb{R}} V_n(t-s)V_1'(s)ds. \end{aligned}$$

Taking the derivative we obtain

$$V_{n+1}'(t) = \int_{\mathbb{R}} V_n'(t-s)V_1'(s)ds = (V_n' * V_1')(t),$$

where $*$ denotes the convolution product. Repeated application of the last formula yields

$$V_m'(t) = (\underset{\leftarrow}{V_1'} * \cdots * \underset{\rightarrow}{V_1'})(t). \tag{4.1}$$

The Fourier transform of a function $f(t)$ is $\widehat{f}(x) = (2\pi)^{-1/2}\int_{\mathbb{R}} e^{-itx} f(t)dt$, and f is retrieved from its transform by $f(t) = (2\pi)^{-1/2}\int_{\mathbb{R}} e^{itx}\widehat{f}(x)dx$. The Fourier transform of a convolution product is

$$\widehat{f * g} = (2\pi)^{1/2}\widehat{f}\cdot\widehat{g}. \tag{4.2}$$

Now

$$\widehat{V_1'}(x) = (2\pi)^{-1/2}\int_0^1 e^{-itx}dt = (2\pi)^{-1/2}e^{-ix/2}(2/x)\sin(x/2),$$

https://doi.org/10.1017/S1446788700037277 Published online by Cambridge University Press

so that (4.1) and $m-1$ applications of (4.2) give

$$\widehat{V_m'}(x) = (2\pi)^{(m-1)/2}((2\pi)^{-1/2}e^{-ix/2}(2/x)\sin(x/2))^m.$$

From this we find that $V_m'(t)$ itself is given by

$$V_m'(t) = (2\pi)^{-1}\int_{\mathbb{R}} e^{ixt}(e^{-ix/2}(2/x)\sin(x/2))^m dx,$$

and this becomes

$$\pi^{-1}\int_{\mathbb{R}} e^{2ixt}(e^{-ix}x^{-1}\sin x)^m dx$$

after an obvious substitution. Therefore

$$V_m(t) = \int_0^t V_m'(s)ds = \pi^{-1}\int_0^t \left(\int_{\mathbb{R}} e^{2ixs}(e^{-ix}x^{-1}\sin x)^m dx\right) ds.$$

We change the order of integration (certainly allowed when $m > 1$, which we may suppose) and integrate over s, to find

$$V_m(t) = \pi^{-1}\int_{\mathbb{R}} (2ix)^{-1}(e^{2ixt}-1)(e^{-ix}x^{-1}\sin x)^m dx = \pi^{-1}\int_{\mathbb{R}} f(x)dx, \tag{4.3}$$

say.

Here $f(z)$ is an entire function which tends to zero when the real part of z tends to $\pm\infty$ while the imaginary part remains bounded. We therefore may shift the path of integration to a line L parallel to the real axis and through a point $-iy_0$ with real $y_0 > 0$. We write $f(z) = f_1(z) + f_2(z)$, with f_1, f_2 coming respectively from the summands e^{2ixt}, -1 of $e^{2ixt}-1$ in (4.3). Both f_1, f_2 are analytic in the lower half plane. In fact $e^{-iz}\sin z$ stays bounded in the lower half plane, so that $|f_2(z)|$ will tend to zero like $|z|^{-m-1}$ as z tends to infinity in this half plane. Shifting the path of integration further and further south we find that $\int_L f_2(z)dz = 0$. Therefore

$$\begin{aligned} V_m(t) &= \pi^{-1}\int_L f_1(z)dz = (2\pi i)^{-1}\int_L z^{-1}(e^{(2izt/m)-iz}z^{-1}\sin z)^m dz \\ &= \pi^{-1}\int_L z^{-1}K(z)^m dz \end{aligned} \tag{4.4}$$

where, with the notation $t/m = s$, we have

$$K(z) = e^{(2s-1)iz}z^{-1}\sin z = (2iz)^{-1}e^{2siz}(1-e^{-2iz}).$$

The best choice of y_0 is made by the saddle point method. However, we need not be that precise, and we set $y_0 = 1/(2s)$. Then for $z \in L$, $z = (-i/2s) + x$ with $x \in \mathbb{R}$, so that

$$K(z) = (2iz)^{-1}e^{1+2sxi}(1-e^{(-1/s)-2ix})$$

https://doi.org/10.1017/S1446788700037277 Published online by Cambridge University Press

and

$$|K(z)| \leq |2z|^{-1}e(1 + e^{-1/s}) = D|z|^{-1}$$

with $D = (e/2)(1 + e^{-1/s})$. Substitution into (4.4) gives

$$V_m(t) \leq \pi^{-1}D^m \int_L |z|^{-m-1}dz = \pi^{-1}D^m \int_{\mathbb{R}} (x^2 + y_0^2)^{-(m+1)/2}dx$$
$$= \pi^{-1}(2sD)^m \int_{\mathbb{R}} (x^2 + 1)^{-(m+1)/2}dx,$$

since $y_0 = 1/(2s)$. Denote the last integral by I_m. Then $I_m \leq I_1 = \pi$, so that $V_m \leq (2sD)^m$, and Theorem 4 is established.

A more careful analysis is as follows: $I_m = \pi \cdot 2^{1-m}\binom{m-1}{(m-1)/2}$ when m is odd. By Stirling's formula, $(m-1)^{1/2}I_m \to \sqrt{2\pi}$ as odd $m \to \infty$. It is easily seen that $(m-1)^{1/2}I_m$ increases as m runs through odd integers, and hence it is $< \sqrt{2\pi}$, so that $I_m < (2\pi/(m-1))^{1/2}$ when $m > 1$ is odd. Since I_m decreases with m, we have $I_m < (2\pi/(m-2))^{1/2}$ when $m \geq 4$, and then $V_m(t) < (2/(\pi(m-2)))^{1/2}(2sD)^m$.

References

[1] E. Bombieri and A. J. Van der Poorten, 'Some quantitative results related to Roth's theorem', *J. Austral. Math. Soc. (Series A)* **45** (1988), 233–248.

[2] W. M. Schmidt. *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics 1467 (Springer, Berlin, 1991).

[3] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics (Springer, Berlin, 1986).

Department of Mathematics
University of Colorado at Boulder
Boulder, Colorado
USA