120. On the Thue-Siegel-Roth Theorem. II

By Saburô UCHIYAMA

Department of Mathematics, Hokkaidô University, Sapporo, Japan

(Comm. by Z. SUETUNA, M.J.A., Nov. 12, 1959)

1. This is a continuation of a previous note under the same title [6]. In the following we shall be concerned with some further results closely related to the Thue-Siegel-Roth theorem on the approximability of an algebraic number by other algebraic numbers.

2. The Thue-Siegel-Roth theorem [2] is an immediate consequence of the following

Theorem 1. *Let α be any algebraic number other than zero and let K be an algebraic number field of finite degree over the rationals. If the inequality*

$$|\alpha-\xi|<(H(\xi))^{-\kappa} \tag{1}$$

is satisfied by infinitely many primitive numbers ξ in K, then

$$\kappa\leqq\begin{cases}2 & \text{when } K \text{ is real,}\\ 1 & \text{when } K \text{ is complex.}^{1)}\end{cases} \tag{2}$$

Moreover, when K is the rational number field or an imaginary quadratic number field, $H(\xi)$ in (1) can be replaced by $M(\xi)$ and the bound (2) for κ is best possible.

For the definition of $H(\xi)$ and $M(\xi)$ we refer to [6, §1]. The first part of Theorem 1 is easily seen from W. J. LeVeque's proof [2] of the Thue-Siegel-Roth theorem, and the second part is a well-known theorem due to K. F. Roth [5] when K is the rational number field, and Theorem 2 in [6] when K is an imaginary quadratic field. We note that it is impossible, in general, to replace $H(\xi)$ in (1) by $M(\xi)$.

3. Let K be an algebraic number field. A non-zero integer of K is said to be *prime in K* if the principal ideal generated by the integer is a prime ideal in K. The associates of a number in K will be identified with the number itself.

Theorem 2. *Let α be any non-zero algebraic number and let K be an imaginary quadratic number field. Let $u_1,\cdots,u_s$, $v_1,\cdots,v_t$ be a finite set of distinct integers of K, each being supposed to be prime in K. Let μ, ν, c be real numbers satisfying*

$$0\leqq\mu\leqq1,\quad 0\leqq\nu\leqq1,\quad c>0.$$

Let p, q be integers in K of the form

$$p=p^*u_1^{a_1}\cdots u_s^{a_s},\quad q=q^*v_1^{b_1}\cdots v_t^{b_t},$$

where $a_1,\cdots,a_s,b_1,\cdots,b_t$ are non-negative rational integers and p^*, q^* are integers of K such that

1) A field is complex if it is not a real field.

$$0<|p^*|\leqq c|p|^{\mu},\qquad 0<|q^*|\leqq c|q|^{\nu}.$$

Then if $\kappa>\mu+\nu$, *the inequality*

$$0<|\alpha-p/q|<|q|^{-\kappa}$$

has only a finite number of solutions in integers p, q *in* K *of the form specified above.*

This result, being a refinement of Theorem 3 stated in [6], constitutes an extension of a theorem of D. Ridout [4] to an imaginary quadratic field. Proof of Theorem 2 can be carried out at once if one refers to [4], on taking account of the argument developed in [6, § 3].

4. Again, let K be an algebraic number field. Let α be an algebraic number, not necessarily in the field K. We define

$$||\alpha||_K=\min|\alpha-\xi|,$$

where the minimum is taken over all integers ξ in K. Clearly $||\alpha||_K=0$ if and only if α is an integer of K.

In virtue of Theorem 2 we can prove

Theorem 3. *Let* α *be any non-zero algebraic number, let* K *be an imaginary quadratic number field and let* u, v *be integers of* K *such that* $|u|>|v|>1$. *Suppose that the ideals* (u) *and* (v) *are relatively prime and every prime ideal containing* $(u)(v)$ *in* K *is principal. Then for any real number* $\varepsilon>0$, *arbitrarily small but fixed, the inequality*

$$\left|\left|\alpha\left(\frac{u}{v}\right)^n\right|\right|_K<e^{-\varepsilon n}$$

is satisfied by at most a finite number of positive rational integers n.

This is a generalization of a theorem due to K. Mahler [3].

5. We may naturally extend the method of Roth [5] to obtain an analogue for non-archimedean valuations of the Thue-Siegel-Roth theorem.

Let L be an algebraic number field. Given a prime ideal $\mathfrak{p}$ in L there exists a unique rational prime $p=p(\mathfrak{p})$ contained in $\mathfrak{p}$. We denote by $e=e(\mathfrak{p})$ the order of $\mathfrak{p}$. If α is a number in L, we define as usual

$$|\alpha|_{\mathfrak{p}}=\begin{cases}0 & \text{for } \alpha=0,\\ p^{a/e} & \text{for } \alpha\neq 0,\end{cases}$$

where a is a rational integer such that the fractional ideal $\mathfrak{p}^a(\alpha)$ contains the factor $\mathfrak{p}$ in neither numerator nor denominator.

Theorem 4. *Let* α *be any algebraic number other than zero and let* K *be an algebraic number field of finite degree over the rationals. Let* $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ *be a finite set of prime ideals with distinct rational primes* $p(\mathfrak{p}_1),\cdots,p(\mathfrak{p}_s)$ *in an arbitrary finite extension field* L *over* $K(\alpha)$. *Then for each* $\kappa>2$, *the inequality*

$$\prod_{k=1}^{s}|\alpha-\xi|_{\mathfrak{p}_k}<(H(\xi))^{-\kappa} \tag{3}$$

has only a finite number of solutions ξ in K.

We shall prove this theorem in some detail. First we re-formulate Theorem 4. Let $\mathfrak{a}$ be an integral ideal in L. If ζ is a number belonging to L, there is a representation $(\zeta)=\mathfrak{b}/\mathfrak{c}$ with certain integral ideals $\mathfrak{b}, \mathfrak{c}$ in L. We write

$$\zeta \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{a})$$

if, in that representation of (ζ), the ideal $\mathfrak{b}$ is contained in $\mathfrak{a}$ and the ideal $\mathfrak{c}$ is prime to $\mathfrak{a}$.

Now we put for the sake of brevity

$$p_k=p(\mathfrak{p}_k), \quad e_k=e(\mathfrak{p}_k) \qquad (k=1,\cdots,s).$$

For a positive rational integer q we set

$$a_k=e_k\left[\kappa\mu_k\frac{\log q}{\log p_k}\right] \qquad (k=1,\cdots,s),$$

where $\mu_1,\cdots,\mu_s$ are *any* non-negative real numbers[2] such that $\mu_1+\cdots+\mu_s=1$, and write

$$\mathfrak{a}(q;\kappa)=\prod_{k=1}^{s}\mathfrak{p}_k^{a_k}.$$

The following theorem can be regarded as an improvement of a result of A. O. Gel'fond [1, §3].

Theorem 5. *Let α, K, L, $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ be as in Theorem 4. Then for each $\kappa>2$, the congruence*

$$\alpha-\xi\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{a}(H(\xi);\kappa)) \qquad (4)$$

has only finitely many solutions ξ in K.

It is not difficult to see that Theorems 4 and 5 are mutually equivalent and, in Theorem 4, there is no loss in generality in supposing that α is an algebraic integer. Also, we may restrict ourselves to the solutions ξ of (3) and of (4) which are primitive numbers in K. Hence we have only to prove Theorem 5 for integral α, ξ's being restricted to be primitive numbers in K. Further, we may suppose that none of $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ contain the ideal (α).

We suppose that Theorem 5 is false, so that for some $\kappa>2$, there is an infinite set E of primitive numbers ξ in K satisfying the congruence (4). Let α be of degree n over the rationals. We choose a positive rational integer m so large that $m>4nm^{1/2}$ and

$$\frac{2m}{m-4nm^{1/2}}<\kappa,$$

which is possible since $\kappa>2$. Next we choose a sufficiently small positive number δ satisfying the conditions (29) and (30) of [5]. We define λ,γ,η as in [5, §7]. Then for all sufficiently small positive δ, we have

$$\frac{m(1+\delta)+d\delta(2+5\delta)}{\gamma-\eta}<\kappa, \qquad (5)$$

2) We note that the μ may depend on ξ, in Theorem 5 below.

where d is the degree of K over the rationals. We then take solutions $\xi_1,\cdots,\xi_m$ of (4) from E such that $H(\xi_1)=q_1,\cdots, H(\xi_m)=q_m$, where $q_1,\cdots,q_m$ are positive rational integers satisfying the conditions (32) and (50) of [5] and the inequality

$$\log q_1 > m\delta^{-1}\cdot\log(p_1\cdots p_s).$$

We take positive rational integers $r_1,\cdots,r_m$ satisfying the inequalities (51) and (52) of [5].

We need the following lemma which can be proved by Roth's method as in [5].

Lemma. Suppose that the conditions just imposed on the numbers $m, \delta, \xi_1,\cdots,\xi_m, q_1,\cdots,q_m, r_1,\cdots,r_m$ are satisfied. Then there exists a polynomial $Q(x_1,\cdots,x_m)$ with rational integral coefficients, of degree at most r_j in x_j $(j=1,\cdots,m)$, such that

(i) the index of Q at the point $(\alpha,\cdots,\alpha)$ relative to $r_1,\cdots,r_m$ is at least $\gamma-\eta$;

(ii) $Q(\xi_1,\cdots,\xi_m)\neq 0$;

(iii) for all derivatives $Q_{i_1\cdots i_m}(x_1,\cdots,x_m)$, where $i_1,\cdots,i_m$ are any non-negative integers, we have, putting $B_1=[q_1^{\delta r_1}]$,

$$|Q_{i_1\cdots i_m}(x_1,\cdots,x_m)| < B_1^{1+2\delta}\prod_{j=1}^{m}(1+|x_j|)^{r_j}.$$

Now the number $\varphi=Q(\xi_1,\cdots,\xi_m)$ is an element of K and *a fortiori* an element of L. It follows from the relation

$$Q(\xi_1,\cdots,\xi_m)=\sum_{i_1=0}^{r_1}\cdots\sum_{i_m=0}^{r_m}Q_{i_1\cdots i_m}(\alpha,\cdots,\alpha)(\xi_1-\alpha)^{i_1}\cdots(\xi_m-\alpha)^{i_m}$$

that

$$N(\varphi)\equiv 0 \qquad (\mathrm{mod}\ p_1^{b_1}\cdots p_s^{b_s}),$$

where $N(\varphi)$ denotes the norm of φ defined in K and where

$$b_k=\min\sum_{j=1}^{m}\left[\kappa\mu_k\frac{\log q_j}{\log p_k}\right]i_j \qquad (1\leqq k\leqq s),$$

the minimum being taken over all sets of integers $i_1,\cdots,i_m$ which satisfy the inequalities

$$\sum_{j=1}^{m} i_j/r_j\geqq\gamma-\eta,\quad 0\leqq i_j\leqq r_j \qquad (1\leqq j\leqq m),$$

in view of the lemma. We have for $k=1,\cdots,s$

$$b_k>\min\sum_{j=1}^{m}\kappa\mu_k\frac{\log q_j^{i_j}}{\log p_k}-mr_1,$$

$$p_k^{b_k}>p_k^{-mr_1}\cdot\min(q_1^{\mu_k i_1}\cdots q_m^{\mu_k i_m})^{\kappa},$$

whence

$$\prod_{k=1}^{s}p_k^{b_k}>q_1^{-r_1\delta}\cdot\min(q_1^{i_1}\cdots q_m^{i_m})^{\kappa}\geqq q_1^{f},$$

$$f=-r_1\delta+r_1(\gamma-\eta)\kappa.$$

Put $c_j=M(\xi_j)$ $(j=1,\cdots,m)$. Then $c_1^{r_1}\cdots c_m^{r_m}N(\varphi)$ is a non-zero rational integer and it follows that

$$|c_1^{r_1}\cdots c_m^{r_m}N(\varphi)|\geqq p_1^{b_1}\cdots p_s^{b_s}>q_1^f.$$

On the other hand, we have as in [2, p. 151]

$$|c_1^{r_1}\cdots c_m^{r_m}N(\varphi)|<B_1^{d(1+2\delta)}\prod_{j=1}^{m}(6^d q_j)^{r_j}\leqq q_1^g,$$

where

$$g=r_1 d\delta(1+5\delta)+mr_1(1+\delta).$$

Combining these results, we obtain $g>f$, or

$$\frac{m(1+\delta)+d\delta(1+5\delta)+\delta}{\gamma-\eta}>\kappa,$$

contrary to (5). This completes the proof of Theorems 4 and 5.

References

[1] A. O. Gel'fond: Transcendental and Algebraic Numbers (in Russian), Moscow (1952).

[2] W. J. LeVeque: Topics in Number Theory, Reading Massachusetts, Vol. 2, Chapter 4 (1956).

[3] K. Mahler: On the fractional parts of the powers of a rational number (II), Mathematika, **4**, 122–124 (1957).

[4] D. Ridout: Rational approximations to algebraic numbers, Mathematika, **4**, 125–131 (1957).

[5] K. F. Roth: Rational approximations to algebraic numbers, Mathematika, **2**, 1–20, 168 (1955).

[6] S. Uchiyama: On the Thue-Siegel-Roth theorem. I, Proc. Japan Acad., **35**, 413–416 (1959).