93. On the Thue-Siegel-Roth Theorem. I

By Saburô UCHIYAMA
Department of Mathematics, Hokkaidô University, Sapporo, Japan
(Comm. by Z. SUETUNA, M.J.A., Oct. 12, 1959)

1. The main object of this note is to show that the Thue-Siegel-Roth theorem can somewhat be refined when the field of reference is an imaginary quadratic number field. The Thue-Siegel-Roth theorem [1] is

Theorem 1. *Let K be an algebraic number field of finite degree and let α be algebraic of degree at least 2 over K. Then for each $\kappa>2$, the inequality*

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

has only a finite number of solutions ξ in K.

Here $H(\xi)$ denotes the height of ξ, the maximum of the absolute values of the coefficients in the primitive irreducible equation with rational integral coefficients of which ξ is a zero, while we designate by $M(\xi)$ the absolute value of the highest coefficient in that equation for ξ.

Since an algebraic number field K of finite degree has only finitely many subfields and every element of K is a primitive number of some one of its subfields, in order to establish Theorem 1 it is enough to prove that for each $\kappa>2$, the inequality (1) is satisfied by only finitely many primitive numbers ξ in K. In this respect the following theorem will be of some interest:

Theorem 2. *Let α be any non-zero algebraic number and let K be an imaginary quadratic number field. If the inequality*

$$|\alpha-\xi|<(M(\xi))^{-\kappa} \tag{2}$$

is satisfied by infinitely many primitive numbers ξ in K, then $\kappa\leqq 1$.

It is clear that $M(\xi)\leqq H(\xi)$ for any fixed ξ and $M(\xi)=1$ for any integral ξ. From this result one can deduce at once the following

Theorem 3. *Let α and K be as in Theorem 2. Then for each $\nu>2$, the inequality*

$$0<\left|\alpha-\frac{p}{q}\right|<\frac{1}{|q|^{\nu}} \tag{3}$$

has only a finite number of integer solutions p, q $(q\neq 0)$ in K.

If, in (3), p and q $(q\neq 0)$ are restricted to be rational integers, Theorem 3 reduces to a recent result of K. F. Roth [3], and we may exclude this rational case. Then the fraction p/q with integers p, q $(q\neq 0)$ in K is a primitive number ξ in K, and, for any representation $\xi=p'/q'$ of the number ξ with integers p', q' $(q'\neq 0)$ in K, it satisfies an irreducible equation of the type*)

$$|q'|^2 x^2+2h\,x+|p'|^2=0,$$

h being a certain rational integer. Hence, by the definition of $M(\xi)$, we have $M(\xi)\leqq|q'|^2$ and, in particular,

$$M(\xi)\leqq|q|^2.$$

Thus Theorem 3 is an immediate consequence of Theorem 2.

We remark that Theorem 3 is the best result of its kind possible if ν is to be independent of $|q|$, since O. Perron's result [2] shows that for any complex irrational number α there are infinitely many pairs of integers p, q $(q\neq 0)$ in every imaginary quadratic number field K satisfying the inequality

$$\left|\alpha-\frac{p}{q}\right|<\frac{C}{|q|^2},$$

where $C>0$ is a constant depending only on K.

2. Our proof of Theorem 2 follows the lines of Roth's work [3] with some modifications. The following arguments will suggest incidentally the possibility of making a slight simplification on W. J. LeVeque's proof [1] of Theorem 1.

Let $m, q_1,\cdots, q_m, r_1,\cdots, r_m$ be positive rational integers. First we note that Lemmas 5, 6 and hence Lemma 7 in [3] hold true with any algebraic numbers $\xi_1,\cdots,\xi_p$ such that $M(\xi_1)=q_1,\cdots, M(\xi_p)=q_p$ in place of rational fractions $h_1/q_1,\cdots, h_p/q_p$, respectively, where $1\leqq p\leqq m$. Necessary changes in the proofs of them are obvious.

Suppose now that α is an algebraic integer other than zero, and let K be an imaginary quadratic number field. We take a single set of values of the numbers $m, \delta, q_1,\cdots, q_m, r_1,\cdots, r_m$ which satisfy the conditions (29), (30), (31), (32) and (33) of [3]. Also we define the numbers $\lambda, \gamma, \eta, B_1$ as in [3]. Then we can prove the following lemma which is an analogue of Lemma 9 of [3].

Lemma. Suppose that the conditions just imposed for $m, \delta, q_1,\cdots, q_m, r_1,\cdots, r_m$ are satisfied, and suppose that $\xi_1,\cdots,\xi_m$ are arbitrary numbers in K such that $M(\xi_1)=q_1,\cdots, M(\xi_m)=q_m$. 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

$$|Q_{i_1\cdots i_m}(\alpha,\cdots,\alpha)|<B_1^{1+3\delta}.$$

*) The square of the absolute value of an integer in K is equal to the norm of the integer and hence is a rational integer: it is positive when the integer is $\neq 0$.

3. We are now going to prove Theorem 2. Let α be a non-zero algebraic number and let K be an imaginary quadratic number field. Suppose that the theorem is false, so that for some $\kappa>1$, there exists a set E of infinitely many primitive numbers ξ ($\neq\alpha$) in K satisfying the inequality (2). Then $M(\xi)$ is not bounded when ξ runs through the elements of E. For, otherwise, it would follow from the relation

$$|M(\xi)\cdot\xi|^2=M(\xi)M(\xi^{-1})$$

that $M(\xi^{-1})$ is unbounded when ξ runs through the elements of E, since there are only a finite number of integers in K with a given norm. But every ξ in E is a solution of (2), so that

$$|\xi|\leqq|\alpha|+(M(\xi))^{-\kappa}\leqq|\alpha|+1,$$

$$\frac{M(\xi^{-1})}{M(\xi)}=|\xi|^2\leqq(|\alpha|+1)^2<\infty,$$

which is impossible. Hence there are primitive solutions ξ of (2) with arbitrarily large $M(\xi)$, and we may now suppose that α is an algebraic integer. For, if not, putting $a=M(\alpha)$, we have for each ξ in E

$$0<|a\alpha-a\xi|<a(M(\xi))^{-\kappa}\leqq a(M(a\xi))^{-\kappa}.$$

Hence for arbitrary $\varepsilon>0$ and for all ξ in E with $M(\xi)$ sufficiently large

$$0<|a\alpha-a\xi|<(M(a\xi))^{-\kappa+\varepsilon},$$

and ε can be chosen so small that $\kappa-\varepsilon>1$.

We first choose m so large that $m>4nm^{1/2}$, where n is the degree of α over the rationals, and that

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

which is possible since $\kappa>1$. We then take δ to be a sufficiently small positive number, so that the condition (29) of [3] holds. By the definitions of λ, γ and η, it follows from (4) that

$$\frac{(1+\delta)m+2\delta(1+4\delta)}{2(\gamma-\eta)}<\kappa \tag{5}$$

for all sufficiently small δ.

We now choose a solution ξ_1 of (2) from the infinite set E, with $M(\xi_1)=q_1$ sufficiently large to satisfy (32) of [3]. We then choose further solutions $\xi_2,\cdots,\xi_m$ of (2) from E with $M(\xi_2)=q_2,\cdots,M(\xi_m)=q_m$, where $q_2,\cdots,q_m$ are positive rational integers satisfying the condition (50) of [3]. Finally, we define the positive integers $r_1,\cdots,r_m$ by (51) and (52) of [3].

We know from the lemma noted above that there exists a polynomial $Q(x_1,\cdots,x_m)$ with the properties listed there. Then the number

$$\varphi=Q(\xi_1,\cdots,\xi_m)$$

is an element of K, and we have

$$1\leqq q_1^{r_1}\cdots q_m^{r_m}|\varphi|^2, \tag{6}$$

since the number on the right-hand side of (6) is a non-zero rational integer.

On the other hand, we have

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

and by the lemma we find that

$$|\varphi| < B_1^{1+4\delta} q_1^{-r_1(\gamma-\eta)\kappa},$$

whence follows that

$$q_1^{r_1}\cdots q_m^{r_m}|\varphi|^2 < q_1^{2\delta(1+4\delta)r_1+(1+\delta)mr_1-2r_1(\gamma-\eta)\kappa}$$

Comparing this with (6), we obtain

$$0 < 2\delta(1+4\delta)+(1+\delta)m-2(\gamma-\eta)\kappa,$$

or

$$\kappa < \frac{(1+\delta)m+2\delta(1+4\delta)}{2(\gamma-\eta)},$$

which contradicts (5). This completes the proof of Theorem 2.

We note that our argument can be extended to obtain an analogue of a theorem of D. Ridout (Rational approximations to algebraic numbers, Mathematika, 4, 125–131 (1957)) in imaginary quadratic number fields.

References

[1] W. J. LeVeque: Topics in Number Theory, Reading, Massachusetts, Addison-Wesley Publishing Co., Vol. 2, Chapter 4 (1956).

[2] O. Perron: Diophantische Approximationen in imaginären quadratischen Zahlkörpern, etc., Math. Zeitschr., **37**, 747–767 (1933); especially §2.

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