PAPERS COMMUNICATED

174. *Verschärfung des Thue-Siegelschen Satzes über die Approximation algebraischer Zahlen.*

Von Sigekatu KURODA.

Tokyo Higher Normal School for Girls.

(Comm. by T. TAKAGI, M.I.A., Dec. 12, 1934.)

Wohlbekannt ist, dass für eine algebraische Zahl ϑ vom Grade $n \geqq 2$ die diophantische Ungleichung

$$(1) \qquad \left|\vartheta - \frac{x}{y}\right| < \frac{1}{y^{\mu}}, \qquad y > 0$$

nur endlich viele ganze rationale Lösungen x, y hat, wenn

1. $\mu = \frac{n}{2} + 1 + \theta, \quad \theta > 0$ (Thue[1]),

2. $\mu = \underset{1 \leq s \leq n-1}{\text{Min}} \left(\frac{n}{s+1} + s\right) + \theta, \quad \theta > 0$ (Siegel[2]).

Diese Ergebnisse lassen sich nun verschärfen. In der Tat, wir können beweisen, dass mit $\mu = 2 + \theta$, $\theta > 0$ dieselbe Behauptung schon gültig ist. Dabei dürfen wir annehmen, dass ϑ ganz sei.

Es sei k eine natürliche Zahl, die $\mu = 2 + \theta > \left(\frac{n}{2}\right)^{\frac{1}{k}} + 1$ erfüllt, und

$$(2) \qquad \varepsilon = \mu - \left(\frac{n}{2}\right)^{\frac{1}{k}} - 1 > 0.$$

Es sei r eine natürliche, δ eine reelle Zahl, und

$$(3) \qquad 2n < r,$$

$$(4) \qquad 0 < \delta < \frac{1}{2},$$

$$(5) \qquad \frac{\delta}{kn}\left(\frac{n}{2}\right)^{\frac{1}{k}} + \delta\mu < \frac{\varepsilon}{4}.$$

Ist ferner $m = \left[\left(\left(\frac{n+\delta}{2}\right)^{\frac{1}{k}} - 1\right) r\right]$, so ist

$$(6) \qquad m + r \leqq \left(\frac{n+\delta}{2}\right)^{\frac{1}{k}} r \leqq \left(1 + \frac{\delta}{kn}\right)\left(\frac{n}{2}\right)^{\frac{1}{k}} r < nr,$$

1) A. Thue: Om en generel i store hele tal ulφsbar ligning. Skrifter udgivne af Videnskabs-Selskabet i Christiania (1908).

2) C. Siegel: Approximation algebraischer Zahlen. Math. Zeitschr. **10** (1921), 173–213. Vgl. hierzu auch E. Landau, Vorlesungen über Zahlentheorie, III (1927), Kap. 2, § 4, 37–65.

$$(7) \qquad 2(m+r+1)^k - nr^k > 2\left(\frac{n+\delta}{2}\right)r^k - nr^k = \delta r^k .$$

Wir betrachten nun alle ganzzahligen Polynome von $k+1$ Variablen

$$P(z\,;\,x_1,\,\cdots,\,x_k) = P(z\,;\,x_\varkappa) = \sum_{\alpha_1=0}^{m+r}\cdots\sum_{\alpha_k=0}^{m+r}\sum_{\beta=0}^{1} B_{\alpha_1\ldots\alpha_k\beta}x_1^{\alpha_1}\cdots x_k^{\alpha_k}z^\beta ,$$

wovon jeder Koeffizient absolut eine feste natürliche Zahl a nicht übersteigt. Im ganzen gibt es $N=(2a+1)^{2(m+r+1)^k}$ verschiedene Polynome dieser Art. Wenn bei jedem dieser Polynome $P(z\,;\,x_\varkappa)$

$$P_{\lambda_1\ldots\lambda_k}(z\,;\,x_\varkappa) = \frac{1}{\lambda_1!}\cdots\frac{1}{\lambda_k!}\frac{\partial^{\lambda_1+\cdots+\lambda_k}}{\partial x_1^{\lambda_1}\cdots\partial x_k^{\lambda_k}}P(z\,;\,x_\varkappa)$$

$$\lambda_\varkappa = 0,\,1,\,\cdots,\,r-1 \qquad (\varkappa=1,\,\cdots,\,k),$$

gesetzt wird, so gilt für jede Konjugierte ϑ_ν $(\nu=1,\,\cdots,\,n)$ von ϑ

$$(8) \qquad |P_{\lambda_1\ldots\lambda_k}(\vartheta_\nu\,;\,\vartheta_\nu,\,\cdots,\,\vartheta_\nu)| < ac_1^{m+r} = t ,$$

wobei c_1, wie nachher c_2, c_3, $\cdots$, eine nur von k, δ und ϑ aber nicht von r abhängige natürliche Zahl ist.

Es seien ϑ_ν für $\nu=1,\,\cdots,\,r_1$ reell und das Paar ϑ_ν und $\vartheta_{\nu+r_2}$ für $\nu=r_1+1,\,\cdots,\,r_1+r_2$ konjugiert komplex. Werden für $\lambda_\varkappa=0,\,1,\,\cdots,\,r-1$

$$(9) \qquad \gamma_\nu^{(\lambda_1,\,\cdots,\,\lambda_k)} = \begin{cases} P_{\lambda_1\ldots\lambda_k}(\vartheta_\nu\,;\,\vartheta_\nu) & \text{für } \nu=1,\,\cdots,\,r_1, \\ \Re P_{\lambda_1\ldots\lambda_k}(\vartheta_\nu\,;\,\vartheta_\nu) & \text{für } \nu=r_1+1,\,\cdots,\,r_1+r_2, \\ \Im P_{\lambda_1\ldots\lambda_k}(\vartheta_\nu\,;\,\vartheta_\nu) & \text{für } \nu=r_1+r_2+1,\,\cdots,\,r_1+2r_2 \end{cases}$$

gesetzt, so entspricht jedem der N Polynome P das System von nr^k Zahlen $\gamma_\nu^{(\lambda_1,\,\cdots,\,\lambda_k)}$, die wir als Koordinaten eines nr^k-dimensionalen Raumes betrachten. Wegen $|\gamma_\nu^{(\lambda_1,\,\cdots,\,\lambda_k)}|<t$ (nach (8) und (9)) liegen unsere N Polynome innerhalb eines Würfels mit der Kante $2t$. Wir zerfällen ihn in $(3t)^{nr^k}$ kongruente Teilwürfel mit der Kante $\frac{2t}{3t}=\frac{2}{3}$. Alsdann ergibt sich aus (6) und (8)

$$(10) \qquad (3t)^{nr^k} < a^{nr^k}(3c_1)^{nr^k(m+r)} < a^{nr^k}c_2^{nr^k\cdot nr} = a^{nr^k}c_3^{r^{k+1}} .$$

Weil wir mehr als $a^{2(m+r+1)^k}$ Polynome haben, so gibt es sicherlich mehr Polynome als Teilwürfel, wenn nur

$$a^{2(m+r+1)^k} > a^{nr^k}c_3^{r^{k+1}}, \qquad a^{2(m+r+1)^k - nr^k} > c_3^{r^{k+1}} .$$

Nach (7) ist dies natürlich erfüllt, wenn $a=([c_3^{\frac{1}{\delta}}]+1)^r > c_3^{\frac{r}{\delta}}$. Alsdann gehören mindestens einem Teilwürfel zwei unserer Polynome $P^*(z\,;\,x_\varkappa)$ und $P^{**}(z\,;\,x_\varkappa)$. Wir setzen nun

$$(11) \qquad R(z\,;\,x_\varkappa) = P^* - P^{**} = \sum_{\alpha_1=0}^{m+r}\cdots\sum_{\alpha_k=0}^{m+r}\sum_{\beta=0}^{1} b_{\alpha_1\ldots\alpha_k\beta}x_1^{\alpha_1}\cdots x_k^{\alpha_k}z^\beta .$$

Das Polynom R hat die folgenden Eigenschaften:

1. Es gibt für alle Koeffizienten b von $R(z; x_\varkappa)$ ein c_4 derart, dass $|b_{\alpha_1 \ldots \alpha_k \beta}| < c_4^r$ sind.

In der Tat ist $|b| \leqq 2a = 2([c_3^{\frac{1}{\delta}}]+1)^r < c_4^r$.

2. $R(z; x_\varkappa)$ ist durch $\prod_{\varkappa=1}^{k}(x_\varkappa - \vartheta)^r$ teilbar.

Da wegen (11) und (9) $|R_{\lambda_1 \ldots \lambda_k}(\vartheta_\nu; \vartheta_\nu)| < 1$ für $\lambda_\varkappa = 0, 1, \ldots, r-1$ $(\varkappa = 1, \ldots, k)$ sind und ϑ ganz algebraisch ist, so ergibt sich $R_{\lambda_1 \ldots \lambda_k}(\vartheta; \vartheta) = 0$, was 2. bestätigt.

3. $R(z; x_\varkappa)$ hängt wirklich von $z, x_1, \ldots, x_k$ ab.

Denn $R(z; x_\varkappa)$ verschwindet natürlich nicht identisch. Käme erstens z in R nicht vor, so wäre $R(z; x_\varkappa) = R(\vartheta; x_\varkappa)$ durch $(x_1 - \vartheta)^r$, also durch $f(x_1)^r$ ($f(x)$ bezeichnet das zu ϑ zugehörigen irreduziblen Polynom) teilbar, also wäre $m + r \geqq nr$, was widerspricht gegen (6). Käme zweitens in R irgendein $x_\varkappa$ nicht vor, dann müsste $R(\vartheta; x_\varkappa)$ wegen 2. identisch verschwinden; daraus folgte, dass ϑ rational ist.

4. Sind $|\vartheta - x_\varkappa| \leqq 1$ $(\varkappa = 1, \ldots, k)$, $|\vartheta - z| \leqq 1$, so gibt es ein c_5 derart, dass für alle nicht negativen $\lambda_\varkappa < r$ gilt

$$|R_{\lambda_1 \ldots \lambda_k}(z; x_\varkappa)| < c_5^r \operatorname{Max}\left(\prod_{\varkappa=1}^{k} |\vartheta - x_\varkappa|^{r-\lambda_\varkappa},\ |\vartheta - z|\right).$$

Dies ergibt sich aus 2. durch leichte Abschätzung.

5. Wenn für ganze rationale $h_\varkappa$, $q_\varkappa$ (> 0) $(\varkappa = 0, 1, \ldots, k)$

$$R_{\lambda_1 \ldots \lambda_k}\left(\frac{h_0}{q_0}; \frac{h_\varkappa}{q_\varkappa}\right) \neq 0, \qquad \left|\vartheta - \frac{h_\varkappa}{q_\varkappa}\right| \leqq 1$$

ist, so ist

$$1 < c_5^r q_0 q_1^{m+r} \ldots q_k^{m+r} \operatorname{Max}\left(\prod_{\varkappa=1}^{k} \left|\vartheta - \frac{h_\varkappa}{q_\varkappa}\right|^{r-\lambda_\varkappa},\ \left|\vartheta - \frac{h_0}{q_0}\right|\right).$$

Dies folgt unmittelbar aus 4.

6. Es seien $s_0, s_1, \ldots, s_k$ beliebige rationale Zahlen. Dann gibt es k Zahlen $\lambda_\varkappa = \lambda_\varkappa(\vartheta, \delta, r, s_0, s_1, \ldots, s_k)$ derart, dass

$$R_{\lambda_1 \ldots \lambda_k}(s_0; s_\varkappa) \neq 0 \qquad \text{und} \qquad 0 \leqq \lambda_\varkappa \leqq \delta r + n$$

ist. (Wegen (3) und (4) sind $\lambda_\varkappa \leqq \delta r + n < r$).

Denn $R(z; x_\varkappa)$ kann wegen 3. so geschrieben werden, dass

$$R(z; x_\varkappa) = (g_1(x_1)z + g_0(x_1))x_2^{\alpha_2^0} \ldots x_k^{\alpha_k^0} + S(z; x_\varkappa)$$

ist, wobei $S(z; x_\varkappa)$ kein Glied der Gestalt $x_2^{\alpha_2^0} \ldots x_k^{\alpha_k^0}$ enthält und $g_1(x_1)$ und $g_0(x_1)$ bezüglich des Körpers der rationalen Zahlen linear unabhängig sind:

$$\Delta(x_1)=\begin{vmatrix} g_0(x_1) & g_1(x_1) \\ g_0'(x_1) & g_1'(x_1) \end{vmatrix} \neq 0 .$$

Indem man das Polynom

$$T(z\,;\,x_\varkappa)=g_1'(x_1)R(z\,;\,x_\varkappa)-g_1(x_1)\frac{\partial}{\partial x_1}R(z\,;\,x_\varkappa)$$

$$=\Delta(x_1)x_2^{\alpha_2^0}\cdot\ldots\cdot x_k^{\alpha_k^0}+U(z\,;\,x_\varkappa)$$

betrachtet, ersieht man, dass $\Delta(x_1)$ durch $(x_1-\vartheta)^{r-1}$, also durch $f(x_1)^{r-1}$ teilbar und dass es ein von s_1 abhängiges γ_1 gibt derart, dass $\Delta^{(\gamma_1)}(s_1)\neq 0$, $0\leqq\gamma_1\leqq\delta r+n-1$ ist. Wenn man ferner T γ_1-mal nach x_1 differenziert, so sieht man ein, dass es ein von s_0 und s_1 abhängiges λ_1 gibt derart, dass $0\leqq\lambda_1\leqq\delta r+n$, $R_{\lambda_1,0,\ldots,0}(s_0\,;\,s_1,\,x_2,\,\cdots,\,x_k)\neq 0$ ist. Indem wir dies Verfahlen k-mal wiederholen, lässt sich 6. vollständig beweisen.

Nun sei vorausgesetzt: (1) habe unendlich viele Lösungen mit $(x,\,y)=1$. Wir wählen k Lösungen $x=h_\varkappa$, $y=q_\varkappa$ (>0) $(\varkappa=1,\,\ldots,\,k)$, wovon die k-te: $x=h_k$, $y=q_k$ mit der Eigenschaft

$$(12)\qquad c_5 q_1^n\cdot\ldots\cdot q_{k-1}^n<q_k^{\frac{\varepsilon}{4}}.$$

Wir nehmen noch eine andere Lösung $x=h_0$, $y=q_0$ und dazu r so dass

$$(13)\qquad \frac{\mu n+1}{r}<\frac{\varepsilon}{4},\qquad (14)\quad q_k^r\leqq q_0<q_k^{r+1}.$$

Für dies r und $h_\varkappa/q_\varkappa=s_\varkappa$ $(\varkappa=0,\,1,\,\ldots,\,k)$ sind das Polynom $R(z\,;\,x_\varkappa)$ und $\lambda_\varkappa$ wie in 6. beschaffen. Deshalb folgte aus (1) und 5.

$$1<c_5^r q_0 q_1^{m+r}\cdot\ldots\cdot q_k^{m+r}\,\mathrm{Max}\left(\prod_{\varkappa=1}^{k} q_\varkappa^{-\mu(r-\lambda_\varkappa)},\ q_0^{-\mu}\right).$$

Da ferner nach 6. und (6)

$$m+r-\mu r+\mu\lambda_\varkappa<nr-\mu r+\mu(\delta r+n)<nr$$

ist, so würde nach (12), (14), (6), (2), (13) und (5)

$$\begin{aligned}
1&<\mathrm{Max}\left(q_0 q_k^{\frac{\varepsilon}{4}r+m+r-\mu r+\mu\lambda_k},\ q_0^{1-\mu}q_k^{\frac{\varepsilon}{4}r+m+r}\right)\\
&<\mathrm{Max}\left(q_k^{r+1+\frac{\varepsilon}{4}r+m+r-\mu r+\mu\lambda_k},\ q_k^{(1-\mu)r+\frac{\varepsilon}{4}r+m+r}\right)\\
&=q_k^{r+1+\frac{\varepsilon}{4}r+m+r-\mu r+\mu\lambda_k}\\
&\leqq q_k^{r+1+\frac{\varepsilon}{4}r+\left(1+\frac{\delta}{kn}\right)\left(\frac{n}{2}\right)^{\frac{1}{k}}r-\mu r+\mu(\delta r+n)}\\
&=q_k^{-\frac{\varepsilon}{4}r+\left(\left(\frac{n}{2}\right)^{\frac{1}{k}}+1-\mu\right)r+\frac{\mu n+1}{r}r+\left(\frac{\delta}{kn}\left(\frac{n}{2}\right)^{\frac{1}{k}}+\delta\mu\right)r}\\
&<q_k^{-\frac{\varepsilon}{4}r-\varepsilon r+\frac{\varepsilon}{4}r+\frac{\varepsilon}{4}r}=q_k^{-\frac{\varepsilon}{4}r}<1,
\end{aligned}$$

was sicherlich unmöglich ist.