Conspectus materiae tomi XXXV, fasciculi 2

La revue est consacrée à la Theorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

ISBN 83-01-01225-0 ISSN 0065-1036

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XXXV (1979)

Die arithmetische Struktur der rationalen Punkte auf Kurven vom Geschlecht Eins

von

S. V. Kotov (Minsk)

1. Einleitung. Der berühmte Siegelsche Satz [13] behauptet die Endlichkeit der Anzahl der ganzen Punkte auf Kurven vom Geschlecht $\geqslant 1$. Für den Beweis dieser Behauptung benutzte er den Satz von A. Weil über die endliche Basis und klassische Ergebnisse der Approximation algebraischer Zahlen. K. Mahler ergänzte die Überlegungen von Siegel durch Ergebnisse über die Approximation der algebraischen Zahlen in der p-adischen Metrik aus [11] und untersuchte in [12] die spezielle Menge der rationalen Punkte auf Kurven vom Geschlecht Eins. Insbesondere stellte er fast, daß auf einer Kurve vom Geschlecht Eins nur eine endliche Anzahl von rationalen Punkten liegt, deren Nenner Produkte von Potenzen der Primzahlen aus einem fixierten endlichen Tupel sind. Die genannten Ergebnisse von C. Siegel und K. Mahler waren jedoch nicht effektiv, d.h. sie ließen keine algorithmische Behandlung zu.

Von kurzem stellten A. Baker und J. Coates [7] einen Algorithmus zur Bestimmung aller ganzen Punkte auf einer Kurve vom Geschlecht Eins fest. Die Begründung dieses Algorithmus fußte auf Ergebnissen von J. Coates [8] über die explizite Konstruktion von rationalen Funktionen auf einer Kurve und auf der effektiven Bestimmung der ganzzahligen Lösungen der Gleichung $Y^2 = f(X)$, wobei $f(X)$ ein kubisches Polynom mit Koeffizienten aus dem Ring der ganzen Zahlen eines algebraisches Körpers ist. Letztere befindet sich schon in der Arbeit von A. Baker [6].

In der vorliegenden Arbeit wird eine effektive Variante des Mahlerschen Satzes [12] dargelegt. Sei $F(x, y)$ ein absolutirreduzibles Polynom des Grads $n \geqslant 3$ mit ganzen rationalen Koeffizienten und die Kurve $F(x, y) = 0$ vom Geschlecht Eins. Wir betrachten auf der Kurve $F(x, y) = 0$ rationale Punkte der Form

$$x = \frac{\tilde{x}}{p_1^{z_1} \ldots p_s^{z_s}}, \qquad y = \frac{\tilde{y}}{p_1^{z_1'} \ldots p_s^{z_s'}}, \tag{1}$$

wobei $\tilde{x}, \tilde{y}$ ganze rationale Zahlen und $p_1, \ldots, p_s$ Primzahlen sind mit $(\tilde{x}, \tilde{y}, p_1 \ldots p_s) = 1$.

Es gilt:

Satz 1. *Wenn $F(x, y)$ ein Polynom der obigen Form ist, Punkte x, y auf der Kurve $F(x, y) = 0$ die Form* (1) *haben und* $P = \max_{(l)}(p_l)$ $(1 \leqslant l \leqslant s)$ *ist, dann gilt die Abschätzung*

$$P > c_1(\ln\ln \tilde{\mathscr{X}} \cdot \ln\ln\ln \tilde{\mathscr{X}})^{1/2}, \tag{2}$$

wobei $\tilde{\mathscr{X}} = \max(|\tilde{x}|, |\tilde{y}|)$, $c_1 > 0$ *nur von* $F(x, y)$ *abhängt und effektiv bestimmt ist.*

Der Beweis dieses Satzes besteht aus zwei Teilen. Im ersten Teil führen wir die Ausgangsaufgabe auf die effektive Bestimmung der Lösungen der Gleichung $Y^2 = f(X)$ zurück, wobei $f(X)$ ein kubisches Polynom mit Koeffizienten aus einem algebraischen Körper ist, und X, Y (zum Unterschied von [7]) algebraische Zahlen (nicht unbedingt ganze) spezieller Form sind. Im zweiten Teil führen wir die effektive Analyse dieser Gleichung durch.

2. Der erste Teil. Wir folgen hier der Arbeit [7]. Seien Ω der Körper aller algebraischen Zahlen, $\Omega(x)$ der Körper der rationalen Funktionen von x mit Koeffizienten aus Ω, $\mathfrak{R}$ die durch Adjunktion der Wurzeln von $F(x, y) = 0$ erzeugte algebraische Erweiterung von $\Omega(x)$. Wir bezeichnen mit $Q_1, \ldots, Q_r$ die Bewertungen von $\mathfrak{R}$, die eine Fortsetzung der durch $1/x$ bestimmten Bewertungen von $\Omega(x)$ sind; mit $e_1, \ldots, e_r$ die entsprechenden Verzweigungsindizes; mit $v_{Q_i}(g)$ die Ordnung des Elements $g \in \mathfrak{R}$ relativ zu Q_i $(1 \leqslant i \leqslant r)$.

Man kann zwei Funktionen X_1 und X_2 mit der Entwicklung relativ Q_i $(i = 1, \ldots, r)$ [7] bilden:

$$X_j = (x-b)^{\nu_i/e_i} \sum_{k=0}^{\infty} u_{ijk}(x-b)^{-k/e_i} \quad (j = 1, 2),$$

wobei b eine der Bedingung $0 \leqslant b \leqslant n^3$ genügende Zahl ist, $\nu_1 = 3$ und $\nu_i = 0$ $(2 \leqslant i \leqslant r)$ ist, die u_{ijk} zu einem algebraischen Zahlkörper K gehören ($K = Q(\theta)$, Q der Körper der rationalen Zahlen, θ eine über Q algebraische Zahl vom Grade $d \leqslant 8^{n^6}$ ist und $\overline{|\theta|} \leqslant (2H_F)^D$ $(D = 8^{n^8})$ gilt, wobei H_F das Maximum der Beträge der Koeffizienten des Polynoms $F(x, y)$ ist(¹)), und

$$\max_{(i,j)}\left(\Delta^{k+1}, \Delta^{k+1}\overline{|u_{ijk}|}\right) \leqslant c_2^{k+1} \quad (1 \leqslant i \leqslant r;\quad j = 1, 2;\quad k = 0, 1, \ldots), \tag{3}$$

wobei Δ eine ganze rationale Zahl ist, für die $\Delta^{k+1}u_{ijk}$ ganzalgebraisch ist und $c_2 > 0$ effektiv durch die Parametern von $F(x, y)$ bestimmt ist. X_1 und X_2 sind nach [7] rationale Funktionen von x, y in K und haben folgende Eigenschaften:

$$v_{Q_1}(X_1) = -2, \quad v_{Q_1}(X_2) = -3, \tag{4}$$

d.h. $u_{110} = 0$, $u_{111} \neq 0$, $u_{120} \neq 0$ und

$$v_Q(X_1) \geqslant 0, \quad v_Q(X_2) \geqslant 0 \tag{5}$$

für alle weiteren Bewertungen Q in $\mathfrak{R}$.

Weiter können wir folgendes ersehen [7]: wenn y in $F(x, y)$ den Grad m $(m \leqslant n)$ hat, dann gilt:

$$X_1^m + P_1(x)X_1^{m-1} + \ldots + P_m(x) = 0, \tag{6}$$

wobei

$$P_j(x) = q_{j0}x^2 + q_{j1}x + q_{j2} \quad (1 \leqslant j \leqslant m) \tag{7}$$

und die q_{jk} $(1 \leqslant j \leqslant m;\ k = 0, 1, 2)$ zum Körper K gehören. Aus (3) folgt die Abschätzung:

$$\max_{(j,k)}\left(\Delta^{n^5}, \Delta^{n^5}\overline{|q_{jk}|}\right) \leqslant c_3 \quad (1 \leqslant j \leqslant m;\ k = 0, 1, 2), \tag{8}$$

wobei die $\Delta^{n^5}q_{jk}$ ganzalgebraisch sind und $c_3 > 0$ durch die Parametern von $F(x, y)$ bestimmt ist.

Wir betrachten die Struktur der in den Nenner des Ideals (X_1) eingehenden Primideale. Der Vergleich von (6) und (7) läßt uns schreiben:

$$X_1^m + \frac{P_1'(\tilde{x})}{\Delta_1^2}X_1^{m-1} + \ldots + \frac{P_m'(\tilde{x})}{\Delta_1^2} = 0, \tag{9}$$

wobei $\Delta_1 = p_1^{z_1} \ldots p_s^{z_s}$ und

$$P_j'(\tilde{x}) = q_{j0}\tilde{x}^2 + \Delta_1 q_{j1}\tilde{x} + \Delta_1^2 q_{j2} \quad (1 \leqslant j \leqslant m). \tag{10}$$

Aus (9) und (11) folgt, daß $\Delta_1^2\Delta^{n^5}X_1$ eine ganze algebraische Zahl ist. Folglich besteht der Nenner des Ideals (X_1) aus einem Produkt von Potenzen von $p_1, \ldots, p_s$ und in Δ eingehenden Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ $(t \leqslant \tilde{c}_3 s)$.

Wenn wir die Funktionen $X_1, X_2, X_1X_2, X_1^2, X_2^2, X_1^3$ analysieren, so stellen wir in Analogie zu [7] fest, daß sie der Gleichung

$$x_1 + x_2X_1 + x_3X_2 + x_4X_1X_2 + x_5X_1^2 + x_6X_2^2 + x_7X_1^3 = 0 \tag{11}$$

genügen, wobei $x_1, \ldots, x_7$ ganze algebraische Zahlen aus K sind,

$$\max_{(i)}\left(\overline{|x_i|}\right) \leqslant c_4 \quad (i = 1, \ldots, 7) \tag{12}$$

gilt und $c_4 > 0$ durch die Parametern von $F(x, y)$ effektiv bestimmt ist. Unter der Annahme, daß in (11)

$$\begin{gathered} X = X_1, \quad Y = x_3 + x_4X_1 + 2x_6X_2, \\ \alpha = -4x_6x_7, \quad \beta = x_4^2 - 4x_5x_6, \\ \gamma = 2x_3x_4 - 4x_2x_6, \quad \delta = x_3^2 - 4x_1x_6, \end{gathered} \tag{13}$$

(¹) $\overline{|\xi|}$ bezeichnet hier und weiter unter das Maximum der Beträge der zur algebraischen Zahl ξ konjungierten Zahlen.

bekommen wir die Gleichung

$$Y^2 = \alpha X^3 + \beta X^2 + \gamma X + \delta, \tag{14}$$

wobei

$$\max\left(\overline{|\alpha|}, \overline{|\beta|}, \overline{|\gamma|}, \overline{|\delta|}\right) \leqslant c_5$$

und $c_5 > 0$ durch die Parametern von $F(x, y)$ effektiv bestimmt ist, was aus (12) und (13) folgt. Das kubische Polynom im rechten Teil von (14) kann keine mehrfachen Wurzeln haben, weil (4) und (5) erfüllt sind und $\mathfrak{R}$ das Geschlecht Eins hat (siehe [7]).

Aus (14) folgt, daß der Nenner des Ideals (Y) auch aus einem Produkt von Potenzen der Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ besteht.

Schließlich bemerken wir, daß nach Konstruktion X_1, X_2 ganze rationale Funktionen von x, y mit Koeffizienten aus dem Körper $\boldsymbol{K}$ sind, d.h. X, Y algebraische Zahlen aus $\boldsymbol{K}$ sind, wenn x, y rationale Zahlen sind.

3. Der zweite Teil. Wir betrachten folgende Aufgabenstellung: Es sei eine Gleichung der Form (14) mit ganzen algebraischen Koeffizienten aus dem Körper $\boldsymbol{K} = \boldsymbol{Q}(\theta)$ vorgegeben, $[\boldsymbol{K}:\boldsymbol{Q}] = d$,

$$(X) = \frac{\mathfrak{X}}{\mathfrak{p}_1^{w_1} \ldots \mathfrak{p}_t^{w_t}}, \quad (Y) = \frac{\mathfrak{Y}}{\mathfrak{p}_1^{w_1'} \ldots \mathfrak{p}_t^{w_t'}} \tag{15}$$

wobei $\mathfrak{X}, \mathfrak{Y}$ ganze Ideale in $\boldsymbol{K}$ und $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ Primideale in $\boldsymbol{K}$ sind mit

$$(\mathfrak{X}, \mathfrak{Y}, \mathfrak{p}_1 \ldots \mathfrak{p}_t) = 1, \tag{16}$$

$$N(\mathfrak{p}_l) = p_l^{f_l}, \quad 1 \leqslant f_l \leqslant d, \quad P = \max_{(l)}(p_l) \quad (1 \leqslant l \leqslant t).$$

Wir beweisen folgendes Ergebnis:

SATZ 2. *Wenn eine Gleichung der Form* (14) *vorgegeben ist und ihre Lösungen X, Y die Form* (15) *mit der Bedingung* (16) *haben, dann gilt die Abschätzung*

$$N(\mathfrak{p}) > c_6 (\ln\ln N \cdot \ln\ln\ln N)^{f/2} \tag{17}$$

für die maximale Norm $N(\mathfrak{p}) = P^f$ $(1 \leqslant f \leqslant d)$ der Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, wobei $N = \max(N(\mathfrak{X}), N(\mathfrak{Y}))$, $c_6 > 0$ durch Koeffizienten der Gleichung (14) *und Parametern des Körpers $\boldsymbol{K}$ effektiv bestimmt ist.*

Der Beweis Satzes 2 benutzt einige Überlegungen aus den Arbeiten [4] und [7]. Im Laufe vom Beweis bekommen wir die für die Begründung von (2) notwendigen Abschätzungen.

Wir führen einige Bezeichnungen ein. Es seien $\boldsymbol{Z}_{\boldsymbol{K}_i}, h_{\boldsymbol{K}_i}, R_{\boldsymbol{K}_i}, D_{\boldsymbol{K}_i}$ der Ring der ganzen Zahlen, die Klassenzahl der Ideale, der Regulator,

die Diskriminante bzw. der endlichen Erweiterung $\boldsymbol{K}_i$ $(i = 1, 2, \ldots)$ des Körpers $\boldsymbol{K}$. $c_7, c_8, \ldots$ haben dieselbe Bedeutung wie c_5.

Wir setzen $\mathscr{X} = \alpha X$, $\mathscr{Y} = \alpha Y$, $g(\mathscr{X}) = \mathscr{X}^3 + \beta \mathscr{X}^2 + \alpha\gamma \mathscr{X} + \alpha^2 \delta$. ω_1, ω_2, ω_3 seien die Wurzeln des Polynoms $g(\mathscr{X})$. Wenn wir, wie in der Arbeit [2] verfahren und der Bedingung (16) folgen, so bekommen wir im Körper $\boldsymbol{K}(\omega_i)$ die Gleichung

$$\mathscr{X} - \omega_i = (\mu_i/\lambda_i)\eta_i^2, \tag{18}$$

wo der Zähler und der Nenner des Ideals (η_i) entsprechend die Idealen $\mathfrak{a}_i\mathfrak{Y}$ und $\mathfrak{p}_1^{w_1'} \ldots \mathfrak{p}_t^{w_t'}$ dividieren, und $\mathfrak{a}_i$ ganzes Ideal ist $(\mu_i, \lambda_i, \eta_i \in Z_{\boldsymbol{K}(\omega_i)})$. Außerdem gelten

$$N(\mathfrak{a}_i) \leqslant c_7 \quad \text{und} \quad \max\left(\overline{|\mu_i|}, \overline{|\lambda_i|}\right) \leqslant c_8 \tag{19}$$

für alle $i = 1, 2, 3$.

Insofern

$$(\eta_i) = \frac{\mathfrak{a}_i \mathfrak{Y}_i}{(\mathfrak{p}_1')^{w_{1i}} \ldots (\mathfrak{p}_q')^{w_{qi}}},$$

wobei $\mathfrak{Y}_i | \mathfrak{Y}$, die in $\boldsymbol{K}_1 = \boldsymbol{K}(\omega_1, \omega_2, \omega_3)$ primen Ideale $\mathfrak{p}_1', \ldots, \mathfrak{p}_q'$ $(q \leqslant 6t)$ Teiler der in $\boldsymbol{K}$ primen Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ sind, können wir folgendes schreiben:

$$(\eta_i) = (\eta_i')(\nu_i)^{-1} \quad (i = 1, 2, 3), \tag{20}$$

$$(\eta_i') = \mathfrak{a}_i \mathfrak{Y}_i (\mathfrak{p}_1')^{h_{\boldsymbol{K}_1} - r_{1i}} \ldots (\mathfrak{p}_q')^{h_{\boldsymbol{K}_1} - r_{qi}},$$

$$(\nu_i) = (\varrho^{v_{1i}+1} \ldots \varrho_q^{v_{qi}+1}), \quad (\varrho_l) = (\mathfrak{p}_l')^{h_{\boldsymbol{K}_1}},$$

$(1 \leqslant l \leqslant q)$, $w_{li} = h_{\boldsymbol{K}_1} v_{li} + r_{li}$, $0 \leqslant r_{li} < h_{\boldsymbol{K}_1}$ $(1 \leqslant l \leqslant q;\ i = 1, 2, 3)$. Unter Ausnutzung von Lemma 2 aus [2] führen wir „eine Normierung" der Grössen $\overline{|\varrho_l|}$ durch:

$$\overline{|\tau_l \varrho_l|} = \overline{|\varrho_l'|} \leqslant c_9 P^{c_{10}} \quad (1 \leqslant l \leqslant q), \tag{21}$$

wobei τ_l Einheiten in $\boldsymbol{K}_1$ sind. Aus (20) bekommen wir

$$\eta_i = \varkappa_i \eta_i' (\nu_i')^{-1} \quad (i = 1, 2, 3), \tag{22}$$

wobei $\nu_i' = (\varrho_1')^{v_{1i}+1} \ldots (\varrho_q')^{v_{qi}+1}$ und $\varkappa_i$ Einheiten in $\boldsymbol{K}_1$ sind. Sei $v_l = \max\limits_i (v_{li})$ $(1 \leqslant l \leqslant q;\ i = 1, 2, 3)$; $\nu = (\varrho_1')^{v_1+1} \ldots (\varrho_q')^{v_q+1}$ und $\eta_i'' = \nu \eta_i$ $(i = 1, 2, 3)$. Offenbar ist $\eta_i'' \in \boldsymbol{Z}_{\boldsymbol{K}_1}$. Da $g(\mathscr{X})$ keine vielfachen Wurzeln hat, gelten infolge der Gleichungen (18) und (22) im Körper $\boldsymbol{K}_1$ folgende Beziehungen:

$$(23)\qquad \begin{cases} Z_1^2-A_1W_1^2 = B_1\nu^2, \\ Z_1 = \mu_1\lambda_2\eta_1'', \quad W_1 = \eta_2'', \\ A_1 = \mu_1\mu_2\lambda_1\lambda_2, \quad B_1 = (\omega_2-\omega_1)\mu_1\lambda_1\lambda_2^2, \end{cases}$$

$$(24)\qquad \begin{cases} Z_2^2-A_2W_2^2 = B_2\nu^2, \\ Z_2 = \mu_1\lambda_3\eta_1'', \quad W_2 = \eta_3'', \\ A_2 = \mu_1\mu_3\lambda_1\lambda_2, \quad B_2 = (\omega_3-\omega_1)\mu_1\lambda_1\lambda_3^2, \end{cases}$$

$$(25)\qquad \begin{cases} Z_3^2-A_3W_3^2 = B_3\nu^2, \\ Z_3 = \mu_2\lambda_3\eta_2'', \quad W_3 = \eta_3'', \\ A_3 = \mu_2\mu_3\lambda_2\lambda_3, \quad B_3 = (\omega_3-\omega_2)\mu_2\lambda_2\lambda_3^2. \end{cases}$$

Aus (19) folgt, daß

$$(26)\qquad \max_i\left(\overline{|A_i|}, \overline{|B_i|}\right) \leqslant c_{11} \qquad (i = 1, 2, 3).$$

Betrachten wir den Körper $\boldsymbol{K}_2 = \boldsymbol{K}_1(\sqrt{\mu_1}, \sqrt{\mu_2}, \sqrt{\mu_3}, \sqrt{\lambda_1}, \sqrt{\lambda_2}, \sqrt{\lambda_3})$. Wenn wir die bekannten Überlegungen (z.B. aus [3] benutzen, bekommen wir aus (23), (24) und (25), daß

$$(27)\qquad Z_i-\theta_{ij}W_i = \pi_{ij}(\varrho_1'')^{U_{1ij}}\ldots(\varrho_r'')^{U_{rij}}(\varepsilon_1)^{V_{1ij}}\ldots(\varepsilon_k)^{V_{kij}} = \Delta_{ij}$$
$$(i = 1, 2, 3;\ j = 1, 2;\ r = 64q;\ k < 384d),$$

wobei θ_{i1}, θ_{i2} die Werte $\sqrt{A_i}$ $(i = 1, 2, 3)$ sind, $(\varrho_l'') = (\mathfrak{p}_l'')^{h\boldsymbol{K}_2}$ $(1 \leqslant l \leqslant r)$, die in $\boldsymbol{Z}_{\boldsymbol{K}_2}$ primen Ideale $\mathfrak{p}_1'', \ldots, \mathfrak{p}_r''$ Teiler der in $\boldsymbol{Z}_{\boldsymbol{K}_1}$ primen Ideale $\mathfrak{p}_1', \ldots, \mathfrak{p}_q'$ sind, $\varepsilon_1, \ldots, \varepsilon_k$ ein System von unabhängigen Einheiten ist und

$$(28)\qquad \max\left(\overline{|\pi_{ij}|}, \overline{|\varrho_l''|}, \overline{|\varepsilon_h|}\right) \leqslant c_{12}P^{c_{13}t}$$

für alle Indexe i, j, l, h $(i = 1, 2, 3;\ j = 1, 2;\ 1 \leqslant l \leqslant r;\ 1 \leqslant h \leqslant k)$ gilt. Die Abschätzung (28) folgt aus der Ungleichung (26) und Lemma 2 aus [2].

Wir betrachten eine Besonderheit der Zahlen Δ_{ij}, die weiter benützt wird. Es sei

$$(\mathfrak{p}_l'')^{U_{li}} \| (\Delta_{i1}, \Delta_{i2}).$$

Dann gilt:

$$(\mathfrak{p}_l'')^{U_{li}} | (2Z_i),$$

weil $\theta_{i1} = -\theta_{i2}$. Folglich, haben wir;

$$(\mathfrak{p}_l'')^{U_{li}} | (\theta_{ij}W_i) \qquad (i = 1, 2, 3;\ j = 1, 2;\ 1 \leqslant l \leqslant r).$$

Da unserer Konstruktion zufolge $|\mathrm{Nm}(Z_i, W_i)| \leqslant c_{14}P^{c_{15}t}$ ist, gilt U_{li}

$\leqslant c_{16}P$ (2) $(i = 1, 2, 3;\ 1 \leqslant l \leqslant r)$. Wir nehmen an, daß für irgendeinen Index $l = 1, \ldots, r$

$$(\mathfrak{p}_l'')^{U_l} \| (\Delta_{11}, \Delta_{21})$$

und

$$(29)\qquad U_l > c_{16}P$$

gelten.

Wenn wir annehmen, daß

$$(\mathfrak{p}_l'')^{U_l'} \| (\Delta_{12}, \Delta_{21}),$$

dann haben wir entweder $U_l' \leqslant U_{l1}$ oder die Annahme (29) stimmt nicht.

Es gelten die Identitäten:

$$(30)\qquad (\lambda_1\mu_2\mu_3)^{1/2}\lambda_3\Delta_{11}+(\lambda_3\mu_1\mu_2)^{1/2}\lambda_2\Delta_{21}+(\lambda_2\mu_1\mu_3)^{1/2}\lambda_1\Delta_{31} = 0$$

und

$$(31)\qquad (\lambda_1\mu_2\mu_3)^{1/2}\lambda_2\Delta_{12}-(\lambda_3\mu_1\mu_2)^{1/2}\lambda_2\Delta_{21}-(\lambda_2\mu_1\mu_3)^{1/2}\lambda_1\Delta_{32} = 0.$$

Wenn für einen Index $l = 1, \ldots, r$ die Ungleichung (29) gilt, dann analysieren wir (31), wenn das nicht der Fall ist, nehmen wir (30). Da die beiden Identitäten analog sind, betrachten wir ohne Beschränkung der Allgemeinheit nur (30).

Wenn wir annehmen, daß $U_{li1} = 4U_{li1}'+U_{li1}''$, $0 \leqslant U_{li1}'' < 4$; $V_{ji1} = 4V_{ji1}'+V_{ji1}''$, $0 \leqslant V_{ji1}'' < 4$ $(i = 1, 2, 3;\ 1 \leqslant j \leqslant k;\ 1 \leqslant l \leqslant r)$; $\varepsilon = \varepsilon_1^{V_{131}}\ldots\varepsilon_k^{V_{k31}}$;

$$(32)\qquad \begin{aligned} A &= (\lambda_1\mu_2\mu_3)^{1/2}\lambda_3\pi_{11}(\varrho_1'')^{U_{111}''}\ldots(\varrho_r'')^{U_{r11}''}\varepsilon_1^{V_{111}''}\ldots\varepsilon_k^{V_{k11}''}, \\ B &= (\lambda_3\mu_1\mu_2)^{1/2}\lambda_3\pi_{21}(\varrho_1'')^{U_{121}''}\ldots(\varrho_r'')^{U_{r21}''}\varepsilon_1^{V_{121}''}\ldots\varepsilon_k^{V_{k21}''}, \\ C &= -(\lambda_2\mu_1\mu_3)^{1/2}\lambda_1\pi_{31}, \end{aligned}$$

und

$$(33)\qquad \begin{aligned} U &= (\varrho_1'')^{U_{111}'}\ldots(\varrho_r'')^{U_{r11}'}\,\varepsilon_1^{V_{111}'}\ldots\varepsilon_k^{V_{k11}'}, \\ V &= (\varrho_1'')^{U_{121}'}\ldots(\varrho_r'')^{U_{r21}'}\,\varepsilon_1^{V_{121}'}\ldots\varepsilon_k^{V_{k21}'} \end{aligned}$$

dann bekommen wir aus (30) im Körper K_2 die Gleichung

$$F_1(U_1, V_1) = U_1^4+A^3BV_1^4 = \varepsilon A^3(\varrho_1'')^{U_{131}}\ldots(\varrho_r'')^{U_{r31}}$$

---

(2) Wir benutzen die Tschebyschevsche Ungleichung: $t \leqslant \pi(P) < cP/\ln P$, wobei c die Tschebyschevsche Konstante ist (siehe [5], Seite 850).

mit den Unbekannten $U_1 = AU$, $V_1 = V$, wobei $U_{311} \geqslant 0, \ldots, U_{r31} \geqslant 0$. Für die Abschätzung ihrer ganzzahligen Lösungen benutzen wir den Satz aus der Arbeit [2]. Wir wollen jetzt mittels P und t alle hierin eingehenden Parameter abschätzen.

Es folgt aus unseren Überlegungen, daß

$$R_{K_2} \leqslant c_{17}. \tag{34}$$

Es seien $K_3 = K_2(\theta_1, \theta_2, \theta_3, \theta_4)$ ein Zerfällungskörper der binären Form $F_1(U_1, V_1)$, und $\theta_1, \theta_2, \theta_3, \theta_4$ ihre Wurzeln. Da die Diskriminante D_{K_3} des Körpers K_3 die Norm der Zahl

$$\delta(\theta)\prod_{i=1}^{3}(3\omega_i^2+2\beta\omega_i+\alpha\gamma)64\prod_{i=1}^{3}(\mu_i\lambda_i)^{1/2}256(\theta_1\theta_2\theta_3\theta_4)^3$$

dividiert, wobei $\delta(\theta)$ die Differente der Zahl θ (siehe [1] auf den Seiten 131–147) ist, bekommen wir

$$|D_{K_3}| < c_{18}P^{c_{19}t}$$

aus (26), (27) und (32). Aus der Landauschen Ungleichung folgt

$$R_{K_3} < c_{20}P^{c_{21}t}. \tag{35}$$

Aus der Abschätzung für $|D_{K_3}|$, erhalten wir auf Grund der Ergebnisse von [10], daß

$$h_{K_3} < c_{22}\,P^{c_{23}t}. \tag{36}$$

Wegen (26), (27) und (32) gelten

$$H_{F_1} < c_{24}P^{c_{25}t} \tag{37}$$

mit $H_{F_1} = A^3B$ und

$$|\mathrm{Nm}(A^3C)| < c_{26}P^{c_{27}t}. \tag{38}$$

Unserer Annahme anfolge, daß (29) für jeden Index $l = 1, \ldots, r$ erfüllt ist, können wir vermuten, daß

$$|\mathrm{Nm}(U_1, V_1)| < c_{28}P^{c_{29}tP}. \tag{39}$$

Ist $\varepsilon = 1/4$ entsprechend der Annahme aus [2], dann läßt sich aus den Ungleichungen (34), (36), (37), (38) und (39) folgern, daß

$$\ln\{\max(\overline{|\zeta U_1|}, \overline{|\zeta V_1|})\} < c_{30}P^{c_{31}t^2} \tag{40}$$

wobei ζ irgendeine Einheit in K_2 ist. Dann folgt aus (30), (32), (33) und (40), daß

$$\max(\overline{|\zeta\Delta_{11}|}, \overline{|\zeta\Delta_{21}|}, \overline{|\zeta\Delta_{31}|}) < \exp\{c_{32}P^{c_{33}t^2}\}. \tag{41}$$

Wenn $\Delta'_{i1} = \zeta\Delta'_{i1}$ $(i = 1, 2)$, gesetzt wird, bekommen wir aus den

Beziehungen

$$\begin{aligned} \mu_1\lambda_2\eta_1'' - (\mu_1\mu_2\lambda_1\lambda_2)^{1/2}\eta_2'' &= \Delta'_{11}\zeta^{-1}, \\ \mu_1\lambda_3\eta_2'' - (\mu_1\mu_3\lambda_1\lambda_3)^{1/2}\eta_3'' &= \Delta'_{21}\zeta^{-1} \end{aligned} \tag{42}$$

die Gleichung

$$\eta_3'' = \delta_1\eta_1'' + \delta_2\eta_2'', \tag{43}$$

wobei

$$\delta_1 = \frac{\mu_1^{1/2}(\lambda_3\Delta'_{11} - \lambda_2\Delta'_{21})}{(\mu_3\lambda_1\lambda_3)^{1/2}\Delta'_{11}}, \qquad \delta_2 = \frac{(\mu_2\lambda_2)^{1/2}\Delta'_{21}}{(\mu_3\lambda_3)^{1/2}\Delta'_{11}}$$

und

$$\max(h(\delta_1), h(\delta_2)) < \exp\{c_{34}P^{c_{35}t^2}\} \tag{44}$$

der Gleichungen (19) und (41) zufolge gilt. Aus den Beziehungen (42) und der Gleichung (43) erhalten wir

$$\begin{aligned} (\eta_1'')^2 - \frac{\mu_2\lambda_1}{\mu_1\lambda_2}(\eta_2'')^2 &= \frac{B_1}{(\mu_1\lambda_2)^2}\,\nu^2, \\ (\eta_1'')^2 - \frac{\mu_3\lambda_1}{\mu_1\lambda_3}(\delta_1\eta_1'' + \delta_2\eta_2'') &= \frac{B_2}{(\mu_1\lambda_3)^2}\,\nu^2. \end{aligned} \tag{45}$$

Die Elimination von η_2'' aus dem System (45) ergibt eine Gleichung der Form

$$\xi_1(\eta_1'')^4 + \xi_2(\eta_1'')^2 + \xi_3 = 0 \tag{46}$$

mit

$$\xi_2 = \nu^2\xi_2', \qquad \xi_3 = \nu^4\xi_3' \tag{47}$$

und

$$\max(h(\xi_1), h(\xi_2'), h(\xi_3')) < \exp\{c_{36}P^{c_{37}t^2}\}, \tag{48}$$

was aus (19) und (44), (46) folgt.

Wenn man die Koeffizienten ξ_1, ξ_2, ξ_3 explizit hinschreibt, kann man sich überzeugen, daß die Gleichung (46) nicht trivial ist. Aus (46) und (47) folgt, daß $\nu^2 | a\,\xi_1(\eta_1'')^4$, wo a maximaler aus den höchsten Koeffizienten der Minimalpolynomen für ξ_1, ξ_2', ξ_3' ist. Da nach der Konstruktion $|\mathrm{Nm}(\nu, \eta_1'')| < c_{38}P^{c_{39}t}$, so aus letzter Bemerkung und (48) wir schlissen

$$|\mathrm{Nm}(\nu)| < \exp\{c_{40}P^{c_{41}t^2}\}$$

woraus wir nach Lemma 2 der Arbeit [2] bekommen:

$$\overline{|\tau\nu|} < \exp\{c_{42}P^{c_{43}t}\}. \tag{49}$$

τ ist dabei irgendeine Einheit im Körper $\boldsymbol{K}_1$. Dann haben (46), (47), (48) und (49)

$$(50)\qquad \overline{|\tau\eta_1''|} < \exp\{c_{44}P^{c_{45}t^2}\}$$

zu Folge. (23), (24), (19), (49) und (50) ergeben, daß

$$(51)\qquad \max\left(\overline{|\tau\eta_2''|}, \overline{|\tau\eta_3''|}\right) < \exp\{c_{46}P^{c_{47}t^2}\}.$$

Weiter sehen wir, daß (50) und (51)

$$(52)\qquad N(\mathfrak{Y}) < N(\mathfrak{Y}_1\mathfrak{Y}_2\mathfrak{Y}_3) < |\mathrm{Nm}(\eta_1''\eta_2''\eta_3'')| < \exp\{c_{48}P^{c_{49}t^2}\}$$

nach sich zieht. Da (18) gilt und sich aus (21), (22), (49) und (50)

$$\max_{(i)}\left(\overline{|\tau\nu_i|}\right) < \exp\{c_{50}P^{c_{51}t^2}\} \qquad (i = 1, 2, 3)$$

folgern läßt, erhält man

$$(53)\qquad N(\mathfrak{X}) < \exp\{c_{52}P^{c_{53}t^2}\}.$$

Schätzt man t durch P mit Hilfe der Tschebyschevschen Ungleichung [5] ab, so bekommt man die Abschätzung (17) aus (52) und (53). Damit ist Satz 2 bewiesen.

4. Der Beweis des Satzes 1. Da die Ideale (X), (Y) nach unserer Konstruktion in § 2 die Form (15) haben und alle Bedingungen des Satzes 2 erfüllt sind, können die Abschätzungen aus dem obigen Paragraphen für die Gleichung (14) verwendet werden.

Zunächst stellen wir fest, daß auf Grund von (18) und (22)

$$\mathscr{X} - \omega_1 = (\mu_1/\lambda_1)\left(\frac{\tau\eta_1''}{\tau\nu}\right)^2$$

und damit

$$(54)\qquad X = \frac{\mu_1(\tau_1\eta_1'')^2 + \lambda_1(\tau\nu)^2\omega_1}{a\lambda_1(\tau\nu)^2}$$

gelten.

Setzen wir $\tilde{X} = \mu_1(\tau\eta_1'')^2 + \lambda_1(\tau\nu)^2\omega_1$, so ist aus den Abschätzungen (19), (49) und (50) zu ersehen, daß

$$(55)\qquad \overline{|\tilde{X}|} < \exp\{c_{54}P^{c_{55}s^2}\}.$$

Die Gleichungen (6) und (7) ergeben

$$(56)\qquad R_0(X)\left(\frac{\tilde{x}}{\varDelta_1}\right)^2 + R_1(X)\frac{\tilde{x}}{\varDelta_1} + R_2(X) = 0$$

wobei

$$(57)\qquad R_k(X) = \sum_{j=1}^{m} q_{jk}X^{m-j} \quad (k = 0, 1), \quad R_2(X) = X^m + \sum_{j=1}^{m} q_{j2}X^{m-j}.$$

Aus (8), (49), (54), (55) und (57) ersieht man, daß

$$(58)\qquad \max_{(k)}\left(\overline{|(a\lambda_1(\tau\nu)^2)^m\varDelta^{n^5}R_k(X)|}\right) < \exp\{c_{56}P^{c_{57}s^2}\} \qquad (k = 0, 1, 2).$$

Aus (56) folgt, daß $(a\lambda_1(\tau\nu)^2)^{m-1}\varDelta^{n^5}R_0(X)\dfrac{\tilde{x}}{\varDelta_1}$ eine ganze algebraische Zahl ist. Weiter ist zu bemerken, daß $\varDelta_1 \mid \mathrm{Nm}\left((a\lambda_1(\tau\nu)^2)^{m-1}\varDelta^{n^5}R_0(X)\right)$. Damit haben wir unter Beachtung von (58) und ([3]) die Abschätzungen

$$(59)\qquad |\tilde{x}| < \exp\{c_{58}P^{c_{59}s^2}\}$$

und

$$(60)\qquad \varDelta_1 < \exp\{c_{60}P^{c_{61}s^2}\}.$$

Es sei $\varDelta_2 = p_1^{z_1'} \ldots p_s^{z_s'}$. Es ist ohne Beschränkung der Allgemeinheit anzunehmen, daß $\max(z_1, \ldots, z_s, z_1', \ldots, z_s')$ unter $z_1, \ldots, z_s$ zu finden ist, weil wir sonst die volle Konstruktion in § 2 bezüglich y geführt hätten. Auf Grund dieser Bemerkung und der Abschätzung (60) läßt sich follgern daß

$$(61)\qquad \varDelta_2 < \exp\{c_{62}P^{c_{63}s^2}\}.$$

Da x, y die Gleichung $F(x, y) = 0$ erfüllen und die Grade, mit denen sie in $F(x, y)$ auftreten, n nicht übertreffen, ist $(\varDelta_1\varDelta_2)^n F(x, y)$ ein Polynom in $\tilde{x}, \tilde{y}$ mit ganzen rationalen Koeffizienten. Nach den Abschätzungen (59), (60) und (61) und der Bemerkung ([3]) erhalten wir, daß

$$(62)\qquad |\tilde{y}| < \exp\{c_{64}P^{c_{65}s^2}\}.$$

Aus den Abschätzungen (59), (62) und aus der Tschebyschevschen Ungleichung [5] ergibt sich (2). Damit ist der Beweis des Satzes 1 beendet.

5. Schlußfolgerung. Ein Sonderfall des Mahlerschen Satzes [12] wurde von J. Coates [9] studiert. Er stellt fest, daß der maximale Primteiler der Differenz $x^3 - y^2$ (x, y ganzrational, $(x, y) = 1$)

$$(63)\qquad 10^{-3}(\ln\ln X)^{1/4}$$

übertrifft, wobei $X = \max(|x|, |y|)$. Hierzu bemerkte J. Coates, daß der Satz von Mahler sich für beliebige Kurven vom Geschlecht Eins effektivisieren lasse. Das Ergebnis ist aber viel schwächer als (63). Wir haben die Abschätzung (2) unter Ausnutzung des Satzes aus der Arbeit [2] bekommen. Unsere Überlegungen beruhen auf eine feine Verbindung zwischen den Abschätzungen der Linearformen von Logarithmen der

([3]) Wenn ξ eine Wurzel des Polynoms $G(Z)$ vom Grade n ist und H_G das Maximum der Beträge der Koeffizienten von $G(Z)$, dann gilt $\overline{|\xi|} < nH_G$ (siehe z.B. [3]).

algebraischen Zahlen in archimedischen und in p-adischen Bewertungen (siehe die Vorschläge 1 und 2 aus [3]).

Wir wollen noch eine Variante von Satz 1 anführen. Es sei $z = v/w$ ein rationaler Punkt. Wir definieren „die Höhe" $h(z)$ des Punktes z, als $\max(|v|, |w|)$. Dann ist es leicht sich zu überzeugen, daß aus unseren Überlegungen

$$P > c_{66}(\ln\ln h\cdot\ln\ln\ln h)^{1/2} \tag{64}$$

folgt, wobei $h = \max(h(x), h(y))$.

Es ist zu sehen, daß sich aus dem Beweis von Satz 1 eine effektive Abschätzung für

$$\max(|\tilde{x}|, |\tilde{y}|, z_1, \ldots, z_s, z_1', \ldots, z_s')$$

mit Hilfe der Parameter von $F(x, y)$, P und s ergibt. Insbesondere bemerken wir, daß für $x = \tilde{x}$ und $y = \tilde{y}$ (d.h. wir betrachten auf der Kurve $F(x, y) = 0$ ganze Punkte)

$$\max(|\tilde{x}|, |\tilde{y}|) < \exp\exp\{H_F^{c_{67}}\}, \tag{65}$$

wobei $c_{67} > 0$, durch n effektiv bestimmt ist. Damit verbessern wir das Ergebnis von A. Baker und J. Coates [7] um einen Exponenten. Es wäre möglich, nur „einmal exp" in (65) zu bekommen, wenn wir die Überlegungen aus [4] benutzt hätten. Obgleich das nicht unserer Gegenstand ist, könnten sie nützlich sein, um die Abschätzung (2) zu verbessern.

Bemerkungen bei der Korrektur

1. Vor kurzem hatte der Autor eine Möglichkeit, die Arbeit von A. van der Poorten „Linear forms in logarithms in the p-adic case" (siehe: Transcendence theory: Advances and applications, Academic Press, London und New York 1977) kennenzulernen. Ändern wir unbedeutend die Überlegungen unseres Artikles unter dem Gesichtspunkt der Methode von Sprindžuk über die effektive Analyse der hyperelliptischen Diophantischen Gleichung [4] und benützen wir den Satz 2 von A. van der Poorten aus der genannten Arbeit, so kann man (2) und (64) bis zu Abschätzungen der Form

$$s\ln P > c_{68}\ln\ln\tilde{X}$$

und

$$s\ln P > c_{69}\ln\ln h \tag{66}$$

entsprechend versträrken. Über die letzten Abschätzungen hatte der Autor an der Tagung „Algebrische Zahlentheorie" (August 1977, Oberwolfach, BRD) berichtet.

2. Dem Autor wurde bekannt, dass D. Bertrand vor kurzem eine schärfere uneffektive Abschätzung für elliptische Kurven mit komplexer Multiplikation erhielt, als (66) (siehe D. Bertrand, *Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe*, Preprint M 291.1176, November 1976, Centre de Mathématiques de l'École Polytechnique Plateau 91128 Palaiseau Cedex „Laboratoire de Recherche associéau C.N.R.S. no 169", der Satz 3).

Literaturverzeichnis

[1] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1954.

[2] S. V. Kotov, *Über die maximale Norm des Polynoms $\alpha x^m+\beta y^n$ mit den algebraischen Koeffizienten*, Acta Arith. 31 (1977), S. 219–230.

[3] С. В. Котов, *Уравнение Туэ-Малера в относительных полях*, ibid. 27 (1975), S. 293–315.

[4] В. Г. Спринджук, *Свободные от квадратов делители многочленов и числа классов идеалов алгебраических числовых полей*, ibid. 24 (1973), S. 143–149.

[5] П. Л. Чебышев, *Избранные труды*, Москва 1955.

[6] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Phil. Soc. 65 (1969), S. 439–444.

[7] A. Baker and J. Coates, *Integer points on curves of genus* 1, ibid. 67 (1970), S. 595–602.

[8] J. Coates, *Construction of rational functions on a curve*, ibid. 68 (1970), S. 105–123.

[9] — *An effective p-adic analogue of a theorem of Thue (III), The diophantine equation $y^2 = x^3+k$*, Acta Arith. 16 (1970), S. 425–435.

[10] E. Landau, *Abschätzungen von Charactersummen, Einheiten und Klassenzahlen*, Nachr. Königl. Gesellschaft Wiss. Göttingen, 1918, S. 79–97.

[11] K. Mahler, *Zur Approximation algebraischer Zahlen*, Math. Ann. I, 107 (1933), S. 691–730.

[12] K. Mahler, *Über die rationalen Punkte auf Kurven vom Geschlecht Eins*, J. Reine Angew. Math. 170 (1934), S.168–178.

[13] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss, Akad. Wiss., 1929, N1.

INSTITUT FÜR MATHEMATIK
AKADEMIE DER WISSENSCHAFTEN DER BSSR

Eingegangen am 1. 5. 1976
und in revidierter Form 10. 7. 1976 (850)