

ATTILA PETHÖ

HORST G. ZIMMER

Lineare rekurrente Folgen auf elliptischen Kurven

Journal de Théorie des Nombres de Bordeaux 2^e série, tome 2, n° 1 (1990),
p. 217-227

http://www.numdam.org/item?id=JTNB_1990__2_1_217_0

© Université Bordeaux 1, 1990, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Lineare rekurrente Folgen auf elliptischen Kurven

von ATTILA PETHÖ und HORST G. ZIMMER

1. Einleitung

Sei R ein kommutativer Ring und M ein Linksmodul über R . Seien $m_0, \dots, m_{k-1} \in M$, $r_1, \dots, r_k \in R$ mit $r_k \neq 0$ gegeben und

$$(1) \quad m_{n+k} = r_1 m_{n+k-1} + \dots + r_k m_n \quad \text{für } n \in \mathbf{N}_0$$

gesetzt, wobei \mathbf{N}_0 die Menge der nicht-negativen ganzen Zahlen bezeichnet. Die Folge $\{m_n\}_{n \in \mathbf{N}_0}$ wird *lineare rekurrente Folge* genannt. Die Eigenschaften solcher Folgen sind sehr intensiv untersucht worden, insbesondere für $M = R = \mathbf{C}$ oder $M = R = \mathbf{K}$, wobei \mathbf{K} ein algebraischer Zahlkörper ist (siehe Shorey und Tijdeman [7]; Evertse, Györy, Stewart und Tijdeman [1]).

Eines der Grundprobleme besteht darin, das Wachstum der Elemente $m_n \in M$ nach unten abzuschätzen. Sei also $\{m_n\}_{n \in \mathbf{N}_0}$ speziell eine lineare rekurrente Folge in $\mathbf{K} \subseteq \mathbf{C}$. Wir bezeichnen mit $\alpha_1, \dots, \alpha_t \in \mathbf{C}$ die verschiedenen Wurzeln des charakteristischen Polynoms $X^k - r_1 X^{k-1} - \dots - r_k$ von $\{m_n\}_{n \in \mathbf{N}_0}$. Zudem setzen wir noch $|\alpha_1| \geq \dots \geq |\alpha_t|$ voraus. Für $k = 2$ hat Mahler [5] und im allgemeinen haben van der Poorten und Schlickewei [6] für beliebiges $\epsilon > 0$ die Ungleichung

$$|m_n| > |\alpha_1|^{n(1-\epsilon)}$$

bewiesen - unter der Annahme, daß $\{m_n\}_{n \in \mathbf{N}_0}$ nicht ausgeartet ist.

Sei nun \mathbf{K} ein Körper, E eine elliptische Kurve über \mathbf{K} und bezeichne $E(\mathbf{K})$ die \mathbf{K} -rationale Punktgruppe von E . Nach dem Mordell-Weilschen Satz ist $E(\mathbf{K})$ eine endlich-erzeugte abelsche Gruppe. Für die Grundeigenschaften der elliptischen Kurven verweisen wir z.B. auf Lang [3] und Zimmer [10]. Die Gruppe $E(\mathbf{K})$ kann man als linken \mathbf{Z} -Modul betrachten und somit in $E(\mathbf{K})$ durch (1) lineare rekurrente Folgen definieren. In dieser Note wollen wir zunächst eine "analytische" Formel für $\{m_n\}_{n \in \mathbf{N}_0}$ beweisen.

Wenn \mathbf{K} ein algebraischer Zahlkörper ist, dann kann man auf $E(\mathbf{K})$ die absolute Néron-Tate Höhe $h : E(\mathbf{K}) \rightarrow \mathbf{R}$ definieren. Diese erweist sich als ein natürliches Maß für das Wachstum rekurrenter Folgen in $E(\mathbf{K})$. Wir beweisen eine Formel für $h(m_n)$, aus der im Falle $|\alpha_1| > |\alpha_j|$, $2 \leq j \leq t$, das genaue Wachstum von $h(m_n)$ abgelesen werden kann.

Bemerkung. Wir sind hier nur an der Betrachtung elliptischer Kurven E über einem Zahlkörper \mathbf{K} interessiert. Die Resultate dieses Artikels gelten jedoch ohne Änderung ganz allgemein für abelsche Varietäten A über \mathbf{K} , wenn zur Bildung der Néron-Tate Höhe auf $A(\mathbf{K})$ die zu einer geraden Divisorklasse $c \in \text{Pic}(A)$ gehörige Weil Höhe h_c genommen wird (s. [4], Ch. 5, §3, Th. 3.6); denn nach dem Mordell-Weilschen Satz ist auch die Gruppe $A(\mathbf{K})$ der rationalen Punkte von A über \mathbf{K} endlich-erzeugt (s. [4], Ch. 6), und genau für Torsionspunkte $T \in A(\mathbf{K})$ gilt ebenfalls $h(T) = 0$ (s. [4], Ch. 5, §3).

2. Lineare rekurrente Folgen in abelschen Gruppen

Sei G eine abelsche Gruppe. Für gegebene Elemente $m_0, \dots, m_{k-1} \in G$ und $r_1, \dots, r_k \in \mathbf{Z}$ sei $m_n \in G$ für $n \geq 0$ durch (1) definiert. Offensichtlich gilt $m_n \in \langle m_0, \dots, m_{k-1} \rangle$, wobei die Klammern die durch m_0, \dots, m_{k-1} erzeugte Untergruppe von G bezeichnen. Wir können deshalb o.B.d.A. $\langle m_0, \dots, m_{k-1} \rangle = G$ annehmen. Nach dem Struktursatz für endlich-erzeugte abelsche Gruppen haben wir

$$G = \langle G_1 \rangle \times \dots \times \langle G_s \rangle \times \langle T_1 \rangle \times \dots \times \langle T_t \rangle,$$

wobei T_j die endliche Ordnung n_j ($1 \leq j \leq t$) hat und die G_j ($1 \leq j \leq s$) von unendlicher Ordnung sind. Dabei gilt auch $k \geq s + t$. Mit diesen Bezeichnungen erhalten wir

SATZ 1. *Sei $k \geq s + t$. Dann gibt es eindeutig bestimmte Folgen $\{x_{jn}\}_{n \in \mathbf{N}_0}$, $1 \leq j \leq s$, welche jeweils unendlich viele von Null verschiedene Glieder enthalten, und mod n_j eindeutig bestimmte Folgen $\{x_{s+j,n}\}_{n \in \mathbf{N}_0}$, $1 \leq j \leq t$, aus ganzen Zahlen, die der Differenzgleichung*

$$(2) \quad X_{n+k} = r_1 X_{n+k-1} + \dots + r_k X_n$$

genügen, und dabei gilt

$$(3) \quad m_n = \sum_{j=1}^s x_{jn} G_j + \sum_{j=1}^t x_{s+j,n} T_j \quad \text{für alle } n = 0, 1, \dots$$

Beweis. Wir haben nach (3) und (1) unter Benutzung der \mathbb{Z} -Modul-Eigenschaft von G

$$\begin{aligned} \sum_{i=1}^k r_i m_{n+k-i} &= \sum_{i=1}^k r_i \left(\sum_{j=1}^s x_{j,n+k-i} G_j + \sum_{j=1}^t x_{s+j,n+k-i} T_j \right) \\ &= \sum_{j=1}^s G_j \sum_{i=1}^k r_i x_{j,n+k-i} + \sum_{j=1}^t T_j \sum_{i=1}^k r_i x_{s+j,n+k-i} \\ &= \sum_{j=1}^s G_j x_{j,n+k} + \sum_{j=1}^t T_j x_{s+j,n+k} = m_{n+k}. \end{aligned}$$

Somit genügt die durch (3) definierte Folge der Beziehung (1).

Das Gleichungssystem

$$m_u = \sum_{j=1}^s X_{ju} G_j + \sum_{j=1}^t X_{s+j,u} T_j \quad \text{für } u = 0, \dots, k-1$$

ist in ganzen Zahlen x_{ju} , $j = 0, \dots, s+t$; $u = 0, \dots, k-1$, lösbar, und zwar sind die Lösungen in den x_{ju} , $1 \leq j \leq s$, $0 \leq u \leq k-1$, eindeutig sowie in den $x_{s+j,u}$, $1 \leq j \leq t$, $0 \leq u \leq k-1$, mod n_j eindeutig. Die Anfangswerte bewirken die Eindeutigkeit bzw. Eindeutigkeit mod n_j der Lösungen von (2). Nehmen wir nun an, daß es ein j in $1 \leq j \leq s$ und ein $n_0 \in \mathbb{N}_0$ gibt, derart $da \rightarrow x_{jn_0} \neq 0$, aber $x_{jn} = 0$ für alle $n > n_0$ gilt. Sei o.B.d.A. $j = 1$ vorausgesetzt. Nach (1) gilt dann

$$G_1 \in \langle G_2 \rangle \times \dots \times \langle G_s \rangle \times \langle T_1 \rangle \times \dots \times \langle T_t \rangle,$$

im Widerspruch zur Voraussetzung. Daher enthält also in der Tat jede der Folgen

$\{x_{jn}\}_{n \in \mathbb{N}_0}$, $1 \leq j \leq s$, unendlich viele von Null verschiedene Glieder. Damit ist Satz 1 bewiesen.

Beispiel. Sei die elliptische Kurve E über \mathbb{Q} durch die Gleichung $y^2 = x^3 - 388.800$ gegeben. Ihre rationale Punktgruppe $E(\mathbb{Q})$ hat den Rang 2 mit den erzeugenden Punkten $P_0 = (76, 224)$, $P_1 = (124, 1232)$ (siehe H.M. Tschöpe und H.G. Zimmer [8]).

Wir bilden die Folge $P_n \in E(\mathbb{Q})$ durch die Rekursion

$$(4) \quad P_{n+1} = P_n + P_{n-1}.$$

Es gibt nach Satz 1 zwei Folgen f'_n und f_n ganzer Zahlen, welche die Rekurrenz (4) erfüllen mit

$$P_n = f'_n P_0 + f_n P_1.$$

Die Anfangswerte erhalten wir durch Lösung des Gleichungssystems

$$P_0 = f'_0 P_0 + f_0 P_1,$$

$$P_1 = f'_1 P_0 + f_1 P_1.$$

Setzt man $f_{-1} = 1$, so ist

$$P_n = f_{n-1} P_0 + f_n P_1$$

bewiesen, wobei f_n die *Fibonacci-Folge* bezeichnet und $f'_n = f_{n-1}$ ist.

Seien $\alpha_1, \dots, \alpha_u$ die verschiedenen Wurzeln mit Multiplizitäten k_1, \dots, k_u des Polynoms

$$X^k - r_1 X^{k-1} - \dots - r_k = \prod_{i=1}^u (X - \alpha_i)^{k_i},$$

und sei $\mathbf{L} = \mathbf{Q}(\alpha_1, \dots, \alpha_u)$ der durch diese Wurzeln erzeugte Zahlkörper. Die Kombination von Satz 1 mit einem klassischen Resultat (Theorem C.1 in Shorey und Tijdeman [7]) führt unmittelbar auf den

SATZ 2. *Es gibt Polynome $P_{ji}(X) \in \mathbf{L}[X]$ vom Grade kleiner als k_i , so daß*

$$m_n = \sum_{j=1}^s G_j \sum_{i=1}^u P_{ji}(n) \alpha_i^n + \sum_{j=1}^t T_j x_{s+j,n} \text{ für alle } n = 0, 1, \dots$$

gilt.

3. Die Höhe der Elemente rekurrenter Folgen auf elliptischen Kurven

Sei \mathbf{K} ein algebraischer Zahlkörper und E wie vorher eine elliptische Kurve über \mathbf{K} . Es bezeichne wieder $E(\mathbf{K})$ die additive abelsche Gruppe der \mathbf{K} -rationalen Punkte von E . Nach dem Mordell-Weilschen Satz (vgl. [3], [10]) ist diese Gruppe wie gesagt endlich-erzeugt.

Im weiteren wollen wir als abelsche Gruppe $G = E(\mathbf{K})$ wählen, aber die übrigen Voraussetzungen und Bezeichnungen von §2 beibehalten.

Auf $E(\mathbf{K})$ existiert eine positiv-semidefinite quadratische Form $h : E(\mathbf{K}) \rightarrow \mathbf{R}$, nämlich die *globale Néron-Tate Höhe*. Die Definition und Grundeigenschaften der Néron-Tate Höhe findet man in Lang [3] oder Zimmer [10]. Wir wollen hier nur die folgenden Eigenschaften hervorheben. Es gilt für alle $P, Q \in E(\mathbf{K})$

$$(5) \quad h(-P) = h(P),$$

$$(6) \quad h(P + Q) + h(P - Q) = 2h(P) + 2h(Q).$$

Genau für die Torsionspunkte $T \in E(\mathbf{K})$ ist

$$(7) \quad h(T) = 0.$$

Sei $E(\mathbf{K}) = \langle P_1 \rangle \times \dots \times \langle P_s \rangle \times \langle T_1 \rangle \times \dots \times \langle T_t \rangle$, wobei P_1, \dots, P_s unendliche und T_1, \dots, T_t endliche Ordnung haben und $0 \leq t \leq 2$ gilt (s.[3]). Sei weiter $k \geq s+t$; seien $m_0, \dots, m_{k-1} \in E(\mathbf{K})$, $r_1, \dots, r_k \in \mathbf{Z}$ gegeben und $m_n, n \geq k$, durch (1) definiert. Unser Ziel ist es in diesem Abschnitt, den folgenden Satz 3 zu beweisen.

SATZ 3. Seien $\alpha_1, \dots, \alpha_u$ und $P_{ji}(X), j = 1, \dots, s, i = 1, \dots, u$, die in §2 definierten Größen, und sei $\{m_n\}_{n \in \mathbf{N}_0}$ die oben definierte Folge. Dann gilt

$$(8) \quad h(m_n) = \sum_{l=1}^u \sum_{v=1}^u \alpha_l^n \alpha_v^n \left(\sum_{i=1}^s h(P_i) P_{il}(n) P_{iv}(n) + \sum_{i=1}^s \sum_{j=i+1}^s h(P_i, P_j) P_{il}(n) P_{jv}(n) \right),$$

wobei $h(P_i, P_j) = h(P_i + P_j) - h(P_i) - h(P_j)$ gesetzt wurde.

Um diesen Satz zu beweisen, benötigen wir das folgende bekannte Lemma.

LEMMA 1. Seien $Q_1, \dots, Q_v \in E(\mathbf{K})$ und $n_1, \dots, n_v \in \mathbf{Z}$. Dann gilt

$$(9) \quad h \left(\sum_{i=1}^v n_i Q_i \right) = \sum_{i=1}^v n_i^2 h(Q_i) + \sum_{i=1}^v \sum_{j=i+1}^v n_i n_j h(Q_i, Q_j),$$

wobei wieder $h(Q_i, Q_j) = h(Q_i + Q_j) - h(Q_i) - h(Q_j)$ ist.

Beweis. Eine Beweisskizze findet sich z.B. in Cassels [2]. Zur Erleichterung für den Leser geben wir jedoch einen kurzen Beweis.

Seien $P, Q, R \in E(\mathbf{K})$. Wir wollen zunächst die Identität

$$(10) \quad h(P+Q+R) = h(P+Q) + h(P+R) + h(Q+R) - h(P) - h(Q) - h(R)$$

verifizieren. Nach (6) ergeben sich die Relationen

$$(11) \quad h(P+Q+R) + h(P+Q-R) = 2h(P+Q) + 2h(R),$$

$$(12) \quad h(P+Q+R) + h(R+Q-P) = 2h(R+Q) + 2h(P),$$

$$(13) \quad h(P-R+Q) + h(P-R-Q) = 2h(P-R) + 2h(Q).$$

Aus (13) folgt mittels (5) und (6)

$$(13') \quad h(P-R+Q) + h(R+Q-P) = -2h(P+R) + 4h(P) + 4h(R) + 2h(Q).$$

Wir erhalten (10), indem wir (11)+(12)-(13') durch 2 dividieren.

Für $v = 1$ folgt (9) aus (6) durch Induktion. Nehmen wir an, daß die Relation (9) für alle $w < v$ mit beliebigen $n_1, \dots, n_w \in \mathbf{Z}$ gilt. Für $n_1 = \dots = n_v = 1$ erhalten wir (9), wenn wir diese Beziehung auf die zwei Punkte $\sum_{i=1}^{v-1} Q_i$ und Q_v anwenden. Wegen (5) können wir also $|n_1|, \dots, |n_{v-1}| \geq 1$ mit $n_v > 1$ voraussetzen. Die Identität (10), die Relation (9) für $n_1 = \dots = n_v = 1$ und die Induktionsvoraussetzung implizieren

nun

$$\begin{aligned}
 h\left(\sum_{i=1}^v n_i Q_i\right) &= \\
 h\left(\sum_{i=1}^{v-1} n_i Q_i + (n_v - 1)Q_v + Q_v\right) &= \\
 = h\left(\sum_{i=1}^{v-1} n_i Q_i + (n_v - 1)Q_v\right) + h\left(\sum_{i=1}^{v-1} n_i Q_i + Q_v\right) + h(n_v Q_v) \\
 - h\left(\sum_{i=1}^{v-1} n_i Q_i\right) - h((n_v - 1)Q_v) - h(Q_v) &= \\
 = \sum_{i=1}^{v-1} n_i^2 h(Q_i) + (n_v - 1)^2 h(Q_v) + \sum_{i=1}^{v-1} \sum_{j=i+1}^{v-1} n_i n_j h(Q_i, Q_j) \\
 + \sum_{i=1}^{v-1} n_i (n_v - 1) h(Q_i, Q_v) + \sum_{i=1}^{v-1} n_i^2 h(Q_i) + h(Q_v) + \sum_{i=1}^{v-1} \sum_{j=i+1}^{v-1} n_i n_j h(Q_i, Q_j) \\
 + \sum_{i=1}^{v-1} n_i h(Q_i, Q_v) + n_v^2 h(Q_v) - h\left(\sum_{i=1}^{v-1} n_i Q_i\right) - (n_v - 1)^2 h(Q_v) - h(Q_v) \\
 = \sum_{i=1}^v n_i^2 h(Q_i) + \sum_{i=1}^v \sum_{j=i+1}^v n_i n_j h(Q_i, Q_j),
 \end{aligned}$$

und damit ist (9) bewiesen.

LEMMA 2. Seien $T \in E(\mathbf{K})$ ein Torsionspunkt und $P \in E(\mathbf{K})$ ein beliebiger Punkt. Dann gilt

$$h(P + T) = h(P).$$

Beweis. (Vgl. [9]; S. 7 oben.) Sei n die Ordnung von T . Dann haben gemäß (7) und (9)

$$\begin{aligned}
 h(P) &= h(P + nT) = h(P) + n^2 h(T) + n(h(P + T) - h(P) - h(T)) \\
 &= h(P) + n(h(P + T) - h(P)).
 \end{aligned}$$

Nun sind wir in der Lage, Satz 3 zu beweisen.

Beweis von Satz 3. Sei $\{m_n\}_{n \in \mathbb{N}_0}$ die durch (1) definierte Folge in $E(\mathbb{K})$. Nach Satz 1 gilt

$$m_n = \sum_{j=1}^s x_{jn} P_j + \sum_{j=1}^t x_{s+j,n} T_j \text{ für alle } n = 0, 1, \dots$$

Daraus folgt nach den Lemmata 2 und 1

$$(14) \quad \begin{aligned} h(m_n) &= h\left(\sum_{j=1}^s x_{jn} P_j\right) \\ &= \sum_{i=1}^s x_{in}^2 h(P_i) + \sum_{i=1}^s \sum_{j=i+1}^s x_{in} x_{jn} h(P_i, P_j). \end{aligned}$$

Nach Theorem C.1 in Shorey und Tijdeman [7] gibt es Polynome $P_{jv}(X) \in \mathbb{L}(X)$ vom Grade kleiner als k_v mit

$$(15) \quad x_{jn} = \sum_{v=1}^u P_{jv}(n) \alpha_v^n.$$

Setzt man diese in (14) ein, so liefert das unmittelbar den Beweis von (8).

Beispiel (Fortsetzung). Wir hatten in dem Beispiel die Folge $P_n = f_{n-1} P_0 + f_n P_1$ bestimmt. In der zitierten Arbeit [8] findet man die Angaben $h(P_0) \approx 1.737652$, $h(P_1) \approx 1.889072$ und $h(P_0 + P_1) \approx 2.834031$. Durch Anwendung von Satz 3 ergibt sich nach einfacher Rechnung

$$\begin{aligned} 5h(P_n) &\approx 2.062885 \alpha^{2n} - 1.095533(-1)^n + 7.720908\beta^{2n} \\ \text{mit } \alpha &= \frac{1 + \sqrt{5}}{2}, \beta = \frac{1 - \sqrt{5}}{2}. \end{aligned}$$

Nach Satz 3 ist $h(m_n)$ eine lineare rekurrente Folge bzw. eine Potenzsumme. Wenn die Folge $h(m_n)$ einen algebraischen Zahlkörper angehört, so haben van der Poorten und Schlickewei [6] ihr Wachstum genau beschrieben. Nach einer Vermutung gehört in unserem Falle die Folge $h(m_n)$ im allgemeinen aber zu einer transzendenten Erweiterung von \mathbb{Q} , und ihr Wachstum ist sehr schwer zu beschreiben. In einem Spezialfall gelingt dies jedoch. Unser Hauptresultat lautet nämlich folgendermaßen :

SATZ 4. Seien die Bezeichnungen die gleichen wie in Satz 3. Wenn dann $s \geq 1$ ist und die Ungleichungen

$$|\alpha_1| > |\alpha_j| \quad \text{für } j = 2, \dots, u$$

erfüllt sind, so gilt

$$(16) \quad \begin{aligned} h(m_n) &= d(n)\alpha_1^{2n}(1 + o(1)) \\ \text{mit } d(n) &= \sum_{i=1}^s P_{i1}^2(n)h(P_i) + \sum_{i=1}^s \sum_{j=i+1}^s h(P_i, P_j)P_{i1}(n)P_{j1}(n) \in \mathbf{R}, \end{aligned}$$

und es gibt ein $n_0 = n_0(m_0, \dots, m_{k-1}, r_1, \dots, r_k)$, so daß $d(n) > 0$ für alle $n \geq n_0$ gilt.

Beweis. Nach (15) ist $x_{jn} = \sum_{v=1}^u P_{jv}(n)\alpha_v^n \in \mathbf{Z}$ für $j = 1, \dots, s$. Da α_1 dominant ist, muß α_1 reell sein, und somit gilt $P_{j1}(X) \in \mathbf{R}[X]$ für $j = 1, \dots, s$. Da weiter die $\frac{\alpha_1}{\alpha_j}$ für $j = 2, \dots, u$ keine Einheitswurzeln sind, sind die Folgen $\{x_{jn}\}_{n \in \mathbf{N}_0}$, $1 \leq j \leq s$, nicht-ausgeartet. Nach dem zitierten Satz von van der Poorten und Schlickewei [6] besteht dann jeweils für beliebiges $\epsilon > 0$ und alle $n \geq n_1$ die Ungleichung

$$|x_{jn}| > |\alpha_1|^{n(1-\epsilon)}, \quad 1 \leq j \leq s.$$

Daher folgt, daß

$$P_{j1}(X) \neq 0, \quad 1 \leq j \leq s,$$

gilt. Die Beziehung (16) erhalten wir unmittelbar aus (8). Zum Beweis von (16) bleibt nur noch, $d(n) > 0$ für alle $n \geq n_0$ zu zeigen.

Dazu bilden wir das Tensorprodukt $V = \mathbf{R} \otimes_{\mathbf{Z}} E(\mathbf{K})$. Dieses Produkt V ist ein Vektorraum der Dimension s über \mathbf{R} . Seien $x_1, \dots, x_s \in \mathbf{R}$, dann definiert

$$(17) \quad h(x_1(1 \otimes P_1) + \dots + x_s(1 \otimes P_s)) = \sum_{i=1}^s x_i^2 h(P_i) + \sum_{i=1}^s \sum_{j=i+1}^s x_i x_j h(P_i, P_j)$$

nach Lemma 1 die Fortsetzung der Néron-Tate Höhe auf V . Sie ist eine positiv-definite quadratische Form auf V (vgl. Lang [3], Theorem 4.3 und Zimmer [9], § 2).

Mit dieser Definition erhält man

$$d(n) = h(P_{11}(n)(1 \otimes P_1) + \dots + P_{s1}(n)(1 \otimes P_s)).$$

Die Beziehung $d(n) = 0$ ist also genau dann erfüllt, wenn $P_{11}(n) = \dots = P_{s1}(n) = 0$ gilt. Dieses Gleichungssystem hat aber nur endlich viele Lösungen, und damit ist Satz 4 bewiesen.

Bemerkung. Ein anderer, mehr begrifflicher Beweis der Lemmata 1 und 2, des Satzes 3 und der nachfolgenden Proposition ergibt sich mittels Einbettung der rationalen Punktgruppe $E(\mathbf{K})$ in den s -dimensionalen reellen Vektorraum $V = \mathbf{R} \otimes_{\mathbf{Z}} E(\mathbf{K})$ durch Ausnutzung der Grundeigenschaften der zu einer positiv-definiten quadratischen Form auf V fortgesetzten Néron-Tate Höhe h und des zugehörigen Skalarprodukts auf V . Wir haben hier jedoch den direkteren und expliziteren Zugang über die Gruppe $E(\mathbf{K})$ selbst und die positiv-semidefinite quadratische Form h auf $E(\mathbf{K})$ bevorzugt.

4. Eine Ungleichung für die Höhe

Beim Beweis von Satz 4 haben wir als Nebenprodukt folgende Ungleichung wiederentdeckt (vgl. [9], § 2, Kor. 2).

PROPOSITION. Seien P und Q unabhängige Punkte auf $E(\mathbf{K})$. Dann gilt

$$(\sqrt{h(P)} - \sqrt{h(Q)})^2 \leq h(P + Q) \leq (\sqrt{h(P)} + \sqrt{h(Q)})^2.$$

Beweis. Seien $x, y \in \mathbf{R}$. Wegen der im Beweis von Satz 4 festgestellten positiven Definitheit von h haben wir

$$xy(h(P + Q) - h(P) - h(Q)) + x^2 h(P) + y^2 h(Q) \geq 0.$$

Diese Ungleichung impliziert für $xy > 0$

$$h(P + Q) \geq \left(1 - \frac{x}{y}\right) h(P) + \left(1 - \frac{y}{x}\right) h(Q)$$

und für $xy < 0$

$$h(P + Q) \leq \left(1 - \frac{x}{y}\right) h(P) + \left(1 - \frac{y}{x}\right) h(Q).$$

Mit der Wahl $x = \sqrt{h(Q)}, y = \sqrt{h(P)}$ bzw. $x = \sqrt{h(Q)}, y = -\sqrt{h(P)}$ ergibt sich aus den letzten beiden Ungleichungen der Beweis der Proposition.

Wir danken dem Referenten für wichtige Korrekturen und ergänzende Hinweise.

LITERATUR

- [1] J.H. EVERTSE, K. GYÖRY, C.L. STEWART, R. TIJDEMAN, "*S-unit equations and their applications*". In "New Advances in Transcendence Theory, Cambridge Univ. Press (1988), 110-174
- [2] J.W.S. CASSELS, *On a theorem of Dem'janenko*. J. London Math. Soc. **43** (1968), 61-66
- [3] S. LANG, *Elliptic Curves : Diophantine Analysis*, Springer-Verlag, Berlin-Heidelberg-New York (1978).
- [4] S. LANG, *Fundamentals of Diophantine Geometry*, Springer-Verlag, Berlin-Heidelberg-New York (1983).
- [5] K. MAHLER, *Eine arithmetische Eigenschaft der rekurrierenden Reihen*, Mathematica B (Leiden) **3** (1934), 153-156.
- [6] A.J. van der POORTEN, H.P. SCHLICKEWEL, *The growth condition for recurrence sequences*. Macquarie Univ. Math. Report 82-0041, North Ryde, Australia, 1982
- [7] T.N. SHOREY, R. TIJDEMAN, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge (1986).
- [8] H.M. TSCHÖPE, H.G. ZIMMER, *Computation of the Néron-Tate height on elliptic curves*, Math. Comp. **48** (1987), 351-370.
- [9] H.G. ZIMMER, *Über eine quadratische Form auf der Gruppe der rationalen Punkte einer elliptischen Kurve über einem Funktionenkörper*, Dissertation, Tübingen (1966).
- [10] H.G. ZIMMER, *Zur Arithmetik der elliptischen Kurven*. Bericht Nr 271 (1986) der Math.-Stat. Sektion der Forschungsges. Joanneum, Graz, Österreich

Kossuth Lajos Universität
Mathematisches Institut
H-4010 Debrecen Pf.12
und
Universität des Saarlandes
Fachbereich 9.1 Mathematik
D-6600 Saarbrücken