Über die lokale Lösbarkeit diophantischer Gleichungen

Von GY. REMÉNYI (Debrecen)

Herrn Professor A. Rapcsák zum 60-sten Geburtstag mit Ehre gewidmet

Einführung

Bezeichne Q den rationalen Zahlkörper und sei $F(x_1, \ldots, x_m) \in Q(x_1, \ldots, x_m)$ ein homogenes Polynom. Die Gleichung

$$(1) \qquad F(x_1, \ldots, x_m) = 0$$

besitzt nur dann eine nichttriviale Lösung $\mathbf{x} = (x_1, \ldots, x_m)$ in Q, wenn sie eine nichttriviale Lösung im Körper Q_∞ der reellen Zahlen und in jedem p-adischen Zahlkörper Q_p besitzt.

Im weiteren p bezeichnet eine Primzahl und wir untersuchen die Lösbarkeit von (1) in Q_p.

Sei

$$K(Q_p) = \sup_{(n,m)} \overset{n}{\breve{\log}}\, m,$$

wobei wir alle diejenigen natürlichen Zahlenpaare (n, m) betrachten, zu denen man ein homogen Polynom n-ten Grades in m Unbekannten mit rationalen Koeffizienten finden kann, derart, daß dieses Polynom in Q_p nur triviale Lösungen hat.

Es ist bekannt (vgl. z. B. [1]) daß $K(Q_p) \geqq 2$. E. ARTIN [2] vermutete, daß $K(Q_p) = 2$. G. TERJANIAN [3] bewies, daß $K(Q_2) \geqq \overset{4}{\breve{\log}}\, 18 > 2$, d.h. die Artinsche Vermutung ist nicht richtig. Gleichzeitig bewies J. BROWKIN [4] daß $K(Q_p) \geqq 3$ für alle p. Die im Beweis von Browkin auftretende Konstruktion ist jedoch ziemlich kompliziert.

In unserer Arbeit geben wir eine einfache Kontsruktion der Formen von Terjanian-Typ. Als Anwendung geben wir einen einfacheren Beweis für den Satz von Browkin.

Ergebnisse

Im weiteren bezeichnen wir mit $\mathscr{Z}$ den Ring der ganzen rationalen Zahlen.

Ist $\mathbf{x} = (x_1, \ldots, x_k) \in \mathscr{Z}^k$ ein ganzer Vektor, p eine Primzahl und $x_i \equiv 0 \pmod p$ für alle i, so bezeichnen wir die einfach mit $\mathbf{x} \equiv 0 \pmod p$.

Satz 1. *Zu jeder Primzahl p und zu jeder ganzen Zahl $m \geqq 0$ existiert eine Form $f_m(\mathbf{x})$ $(p-1)p^{2^m-1}$-ten Grades in p^{2^m-m-1} Unbekannten mit Koeffizienten in $\mathscr{Z}$, sodaß für jeden ganzen Vektor* $\mathbf{x}$

$$f_m(\mathbf{x}) \equiv 1 \pmod{p^{2^m}},$$

falls $\mathbf{x} \not\equiv 0 \pmod{p}$.

Zum Beweis der Behauptung brauchen wir zuerst zwei einfache Hilfssätze:

Hilfssatz 1. *Sei $r \geqq 2$ eine natürliche Zahl. Zu jeder ganzen Zahl k mit $1 \leqq k \leqq r-1$ existiert ein homogenes Polynom G_k r-ten Grades in k Veränderlichen mit Koeffizienten aus $\mathscr{Z}$, derart daß für die Substitutionswerte $\mathbf{x} = (x_1, \dots, x_k)$, $\mathbf{x} \in \mathscr{Z}^k$*

$$G_k(\mathbf{x}) \equiv \begin{cases} 1 \pmod{r^2}, & \text{wenn alle} \quad x_i \equiv 1 \pmod{r}, \\ 0 \pmod{r^2}, & \text{wenn ein} \quad x_i \equiv 0 \pmod{r^2} \end{cases}$$

gilt.

Beweis. Wir definieren G^* folgendermaßen

$$G^* = \prod_{i=1}^{r} x_i - \prod_{j=1}^{r-1} x_j \left(\sum_{i=0}^{r} x_i \right) + r \prod_{i=1}^{r} x_i .$$

Wenn $\mathbf{x} = (x_1, \dots, x_r) \in \mathscr{Z}^r$ und für irgendeinen $i \leqq r-1$ $x_i \equiv 0 \pmod{r^2}$, so gilt

$$G^*(\mathbf{x}) \equiv 0 \pmod{r^2}.$$

Wenn aber $x_i \equiv 1 \pmod{r}$ für alle $1 \leqq i \leqq r$, so gilt für $x_i = k_i r + 1$

$$G^*(\mathbf{x}) \equiv r \sum_{i=1}^{r} k_i + 1 - \left(r \sum_{i=1}^{r-1} k_i + 1 \right) \left(r \sum_{i=1}^{r} k_i + r \right) + r \equiv 1 \pmod{r^2}.$$

Sei nun in G^* $x_{k+1} = \dots = x_r = x_1$ und das so erhaltene Polynom bezeichnen wir mit G_k. Auf Grund des Vorangehenden erfüllt G_k die Bedingungen des Hilfssatzes.

Hilfssatz 2. *Zu einer beliebigen ganzen Zahl $r \geqq 2$ existiert ein Polynom r-ten Grades in $r-1$ Unbekannten mit Koeffizienten aus Z derart, daß für die Substitutionswerte $\mathbf{x} = (x_1, x_2, \dots, x_{r-1}) \in \mathscr{Z}^{r-1}$ die Beziehung*

$$F(\mathbf{x}) \equiv \begin{cases} 1 \pmod{r^2}, & \text{wenn wenigstens ein} \quad x_i \equiv 1 \pmod{r} \\ & \text{und die anderen} \quad x_i \equiv 0 \pmod{r^2}, \\ 0 \pmod{r^2}, & \text{wenn alle} \quad x_i \equiv 0 \pmod{r^2} \end{cases} \tag{2}$$

gilt.

Beweis. Wir führen den Beweis für eine feste Gradzahl $r \geqq 2$ mit Induktion nach der Zahl der Veränderlichen. Im weiteren bezeichne bei F der Index gleichzeitig die Zahl der Veränderlichen. Wir konstruieren fortlaufend homogene Polynome $F_1(\mathbf{x}), \dots, F_{r-1}(\mathbf{x})$ mit Koeffizienten aus $\mathscr{Z}$ derart, daß diese Polynome die Beziehung (2) befriedigen.

Sei

$$F_1(\mathbf{x}) = x_1^r.$$

Für dieses Polynom ist (2) erfüllt. Wir setzen voraus, daß wir die Polynome $F_1(\mathbf{x}), \ldots, F_k(\mathbf{x})$ mit der gewünschten Eigenschaft schon konstruiert haben. Sei nun

$$F_{k+1} = (-1)^k[G_{k+1}+(-1)^1 \sum F_1+(-1)^2 \sum F_2+\ldots+(-1)^k \sum F_k]$$

wo wir die i-te Summierung so vornehmen, daß in den F_i jede Kombination der i-ten Klasse ohne Wiederholungen der Veränderlichen $x_1, \ldots, x_{k+1}$ auftritt. Wenn jedes $x_i \equiv 0 \pmod{r^2}$ so ist $F_{k+1}(x) \equiv 0 \pmod{r^2}$. Wenn jedes $x_i \equiv 1 \pmod r$, so ist nach der Induktionsvoraussetzung

$$F_{k+1} \equiv (-1)^k\left[1+(-1)\binom{k+1}{1}+\ldots+(-1)^k\binom{k+1}{k}\right] \equiv$$
$$\equiv (-1)^k[(1-1)^{k+1}-(-1)^{k+1}] \equiv 1 \pmod{r^2},$$

Gilt aber für $j < k+1$ der x_i die Beziehung $x_i \equiv 0 \pmod{r^2}$ und für die übrigen $x_i \equiv 1 \pmod r$, so muß von der obigen Summe die Summe

$$1+(-1)^1\binom{j}{1}+\ldots+(-1)^j\binom{j}{j} = 0$$

abgezogen werden. D.h. für $j < k+1$ nichts abgezogen zu werden. Damit ist der Hilfssatz 2. bewiesen.

Beweis von Satz 1. Wir beweisen mehr indem wir die Existenz solcher, die Bedingungen des Satzes erfüllender Polynome zeigen, für die im Fall $\mathbf{x} \equiv 0 \pmod p$ sogar $f_m(\mathbf{x}) \equiv 0 \pmod{p^{2^{m+1}}}$ erfüllt ist. Ausgenommen ist der Fall $p=2$ und $m=0, 1$, für den $f_m(\mathbf{x}) \equiv 0 \pmod{p^{2^m}}$: Sei zuerst $p=2$. Man sieht dann leicht, daß $f_0(\mathbf{x})=x$, $f_1(\mathbf{x})=x^2$ und $f_2(\mathbf{x}) = x_1^8+x_2^8$ geeignete Polynome sind, Ferner ist $f_2(\mathbf{x}) \equiv 0 \pmod{2^{2^3}}$ falls $\mathbf{x} \equiv 0 \pmod p$. Ist $p \geqq 3$ und $m=0$, so sei $f_0(\mathbf{x})=x^{p-1}$ und man sieht daß dieses Polynom die Behauptung des Satzes erfüllt und daß $f_0(\mathbf{x}) \equiv 0 \pmod{p^2}$ falls $\mathbf{x} \equiv 0 \pmod p$. Wir setzen jetzt voraus, daß die obige Behauptung für m richtig sei, wobei $m \geqq 2$ für $p=2$ und $m \geqq 0$ für $p \geqq 3$. Dann existiert ein Polynom $f_m(\mathbf{x})$ $(p-1)\cdot p^{2^m-1}$-ten Grades in p^{2^m-m-1} Unbekannten mit Koeffizienten in $\mathscr{Z}$ derart daß $f_m(\mathbf{x}) \equiv 1 \pmod{p^{2^m}}$ falls $\mathbf{x} \not\equiv 0 \pmod p$ und $f_m(\mathbf{x}) \equiv 0 \pmod{p^{2^{m+1}}}$ falls $\mathbf{x} \equiv 0 \pmod p$. Wir zeigen, daß dann für $m+1$ ebenfalls ein Polynom mit dieser Eigenschaft existiert.

Wir benutzen das im Hilfssatz 2. für $r=p^{2^m}$ auftretende Polynom F. Wir betrachten nun das obige Polynom f_m mit $(p^{2^m}-1)$-fach paarweise disjunkten Veränderlichen. Mit diesen bilden wir das Polynom

$$f_{m+1}^* = F(f_m, \ldots, f_m),$$

dessen ganze rationale Substitutionen die Beziehung

$$f_{m+1}^* = F(\underbrace{f_m, \ldots, f_m}_{p^{2^m}-1}) \equiv \begin{cases} 1 \pmod{p^{2^{m+1}}}, & \text{wenn irgendein } f_m \equiv 1 \pmod{p^{2^m}}, \\ 0 \pmod{p^{2^{m+2}}}, & \text{wenn jedes } f_m \equiv 0 \pmod{p^{2^{m+1}}}. \end{cases}$$

Die Gradzahl des Polynoms f_{m+1}^* ist

$$(p-1)\cdot p^{2^m-1}\cdot p^{2^m} = (p-1)\cdot p^{(2^{m+1}-1)},$$

die Zahl der Unbekannten dieses Polynoms ist

$$(p^{2^m-1})\cdot p^{2^m-m-1} \geqq p^{2^m-1}\cdot p^{2^m-m-1} = p^{2^{m+1}-(m+1)-1}.$$

Wenn wir nun in f_{m+1} diejenigen Unbekannten, die die Indizes $p^{2^{m+1}-(m+1)-1}+1, \dots$ usw. besitzen mit x_1 identifizieren, dann erfüllt das sich so ergebende Polynom f_{m+1} schon den Satz 1. zusammen mit der am Anfang des Satzes gemachten Bemerkung.

Satz 2. *Für eine beliebige Primzahl p gilt*

$$K(Q_p) \geqq 3.$$

Beweis. Sei $m\geqq 2$ eine natürliche Zahl und f_m ein den Satz 1. erfüllendes Polynom. Wir betrachten nun die Polynome $f_m(\mathbf{x}_1), f_m(\mathbf{x}_2)$ usw. mit paarweise disjunkten Unbekannten und bilden das Polynom

$$G = \sum_{i=1}^{p^{2^m}-1} f_m(\mathbf{x}_i).$$

Mit $\mathbf{Y}_0, \dots, \mathbf{Y}_r$ bezeichnen wir jetzt die paarweise disjunkten Mengen der Unbekannten und betrachten das homogene Polynom

$$H = G(\mathbf{Y}_0) + rG(\mathbf{Y}_1) + \dots + r^q G(\mathbf{Y}_q)$$

wo $r=p^{2^m}$ und

$$q = \left[\frac{(p-1)p^{2^m-1}}{2^m} - 1\right].$$

Wir zeigen, daß die Gleichung $H=0$ in Q_p nur die triviale Lösung $O=(0, 0, \dots)$ besitzt.

Im gegenteiligen Fall hätte nämlich die Gleichung

(3) $$H(\mathbf{Y}_0, \dots, \mathbf{Y}_q) = 0$$

in Q_p eine ganze Lösung derart, daß $Y_i \not\equiv 0 \pmod p$ für irgendein i. Dann ergibt sich aber aus (3) für die obige ganze Zahl $m\geqq 2$

$$G(\mathbf{Y}_0) \equiv 0 \pmod{p^{2^m}}$$

während aber aus der Konstruktion von G und aus Satz 1. $\mathbf{Y}_0\equiv 0 \pmod p$ folgt. In diesem Fall ist

$$G(\mathbf{Y}_0) \equiv 0 \pmod{p^{\operatorname{grad} G}}$$

sowie nach dividieren von (3) durch p^{2^m}

$$G(\mathbf{Y}_1) \equiv 0 \pmod{p^{2^m}}.$$

Hieraus erhalten wir analog $\mathbf{Y}_1\equiv 0 \pmod p$ und es ergibt sich

$$G(\mathbf{Y}_1) \equiv 0 \pmod{p^{\operatorname{grad} G}}.$$

Indem wir das Verfahren für alle $i\leqq q$ fortsetzen, bekommen wir

$$G(\mathbf{Y}_i) = 0 \pmod{p^{2^m}}$$

und $\mathbf{Y}_i \equiv 0 \pmod p$, da q so gewählt war, daß $r^{q+1} \leqq p^{\operatorname{grad} G}$. Dies aber ist ein Widerspruch. Also hat (3) in Q_p nur die triviale Lösung. Man kann einsehen, daß die Gradzahl von $H(p-1)\cdot p^{2^m-1}$ ist, während die Zahl der Unbekannten

$$p^{2^m-m-1}(p^{2^m}-1)\cdot(q+1) \geqq p^{2^m-m-1}\cdot p^{2^m-1}\cdot p^{2^m-m-2} = p^{3\cdot 2^m-2m-4}$$

beträgt.

Hieraus ergibt sich

$$K(Q_p) \geqq \overset{u}{\breve{\log}}\,[p^{2^m-m-1}\cdot(p^{2^m}-1)\cdot(q+1)] \geqq \overset{v}{\breve{\log}}\,p^{3\cdot 2^m-2m-4} \geqq 3-\overset{v}{\breve{\log}}\,p^{2m+4}$$

wo

$$u = (p-1)\cdot p^{2^m-1}$$

und

$$v = p^{2^m}$$

das heißt für $m\to\infty$ ist $K(Q_p) \geqq 3$, was zu beweisen war.

Literatur

[1] Z. I. Borewicz—I. R. Šafarevič, Zahlentheorie. *Basel,* 1966.

[2] S. Lang, Some theorems and conjectures in Diophantine equations. *Bull. Amer. Math. Soc.* **66** (1960), 240—249.

[3] G. Terjanian, Un contre-exemple a une conjecture d'Artin, *C. R. Acad. Sci. Paris,* **262** (1966), 612.

[4] J. Browkin, On Forms over p-adic Fields, *Bull. de l'Academie Polonaise des Sci.,* **14** (1966), 489—492.

(Eingegangen am 17. Januar 1973.)