Über die Lösbarkeit diophantischer Gleichungen von additivem Typ I.

Von BÉLA KOVÁCS (Debrecen)

Einleitung

Eine der stärksten Methoden der Untersuchung der Lösbarkeit von diophantischen Gleichungen im Körper R der rationalen Zahlen ist die Methode von Hardy—Littlewood—Vinogradov, auch Methode der trigonometrischen Summen genannt. Um diese Methode verwenden zu können, muß man die lokale Lösbarkeit der untersuchten Gleichung oder Gleichungstypus nachweisen, d.h. die Lösbarkeit in jedem p-adischen Körper R_p und im reellen Körper R_∞.

In bezug auf die lokale Lösbarkeit von Gleichungen hat Artin vermutet, daß beim Erfülltsein von $n>k^2$ für die Gradzahl k und die Anzahl n der Variablen einer Gleichung, diese Gleichung in jedem p-adischen Körper R_p lösbar ist. Daß diese Vermutung nicht richtig ist haben G. TERJANIAN in [2] und J. BROWKIN in [1] voneinander unabhängig gezeigt, aber S. KOCHEN und J. AX haben nachgeweisen, daß die Anzahl derjenigen p-adischen Körper R_p, für die bei einem beliebigen, fest gewählten Exponenten k die Vermutung von Artin nicht richtig ist, endlich ist [3].

In [4] haben H. DAVENPORT und D. J. LEWIS gezeigt, daß im Falle von homogenen additiven Gleichungen die Vermutung von Artin richtig ist; sie haben sogar unter Benutzung der Methode der trigonometrischen Summen die Lösbarkeit in R_∞ nachgewiesen.

Das Ziel des Verfassers dieser Arbeit ist im wesentlichen eine Verallgemeinerung des erwähnten Ergebnisses von Davenport und Lewis auf nicht unbedingt homogen additive Gleichungen

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = 0$$

wo $a_1, \ldots, a_n$ rationale und $k_1, \ldots, k_n$ natürliche Zahlen sind. In dieser Arbeit erfolgt eine Untersuchung der Lösbarkeit in R_p nur für Primzahlen $p \geqq 3$. In einer kommenden Arbeit werden die Lösbarkeit in R_2 und mit der Methode der trigonometrischen Summen die Lösbarkeit in R untersucht.

1. §

Seien $s \geqq 1$ eine natürliche Zahl und $t_1, \ldots, t_s$ eine beliebige, aber fest gewählte Folge von verschiedenen natürlichen Zahlen. Sei $n \geqq s$ eine beliebige natürliche Zahl. Wir bilden alle n elementigen Variationen $(k_1, \ldots, k_n)$ der Zahlen $t_1, \ldots, t_s$, bezeich-

nen die Menge dieser Variationen mit $V(n; t_1, \ldots, t_s)$, und suchen eine Antwort auf das folgenden Problem:

Für welche $n_0(t_1, \ldots, t_s)$ gilt im Falle von $n > n_0$ daß für beliebige $(k_1, \ldots, k_n) \in \in V(n; t_1, \ldots, t_s)$ die Gleichung

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = 0 \tag{1}$$

für beliebige rationale Zahlen $a_1, \ldots, a_n$ $(a_i \neq 0;\ i = 1, \ldots, n)$ in jedem R_p eine nichttriviale Lösung hat. (Die Lösung $x_1 = x_2 = \cdots = x_n = 0$ nennen wir die triviale Lösung. Im folgenden verstehen wir unter Lösbarkeit die Existenz einer nichttrivialen Lösung.) Offenbar ist es ausreichend, das Problem für rationale ganze Koeffizienten $a_1, \ldots, a_n$ zu untersuchen.

Im Falle von $s = 1$ ist die Menge $V(n; t_1)$ elementig und das Problem ist identisch mit dem von Davenport und Lewis beantworteten Problem, und so muß man eine Schranke $n_0(t_1, \ldots, t_s)$ als eine solche Funktion der Zahlen $t_1, \ldots, t_s$ suchen, die im Falle $s = 1$ das von Davenport und Lewis gefundene Ergebnis $n_0 = k^2$ liefert.

Auf Grund der Natur des Problems erscheinen mehrere Funktionen der Zahlen $t_1, \ldots, t_s$ zur Abschätzung oder zur genauen Angabe des Wertes der Schranke $n_0(t_1, \ldots, t_s)$ geeignet. Eine solche eine Funktion der Zahlen $(t_1, \ldots, t_s)$ ist $L = [t_1, \ldots, t_s]$ wo [ ] das kleinste gemeinsame Vielfache der Zahlen $t_1, \ldots, t_s$ bedeutet. Bei dieser Funktion würde man eine Verallgemeinerung des Ergebnisses von Davenport und Lewis bekommen, wenn man $n_0(t_1, \ldots, t_s) \leqq L^2$ nachweisen könnte. Dies kann man zwar sehr einfach unter Verwendung des für homogen additive Gleichungen bekannten Ergebnisses gewinnen, aber es ist leicht einzusehen, daß die Abschätzung im allgemeinen schwach ist. Trivial ist auch $n_0(t_1, \ldots, t_s) \leqq \leqq t_1^2 + \cdots + t_s^2$ aber dies ist ebenfalls eine schwache Abschätzung von $n_0(t_1, \ldots, t_s)$.

Für spezielle Reihen $t_1, \ldots, t_s$ kann man leicht nachweisen, daß

$$n_0(t_1, \ldots, t_s) \leqq (t_1, \ldots, t_s)^2 = d^2$$

gilt, wo ( ) den größten gemeinsamen Teiler bedeutet. Ferner könnten wir aus der Tatsache, daß die Teilbarkeitseigenschaften der Zahlen $t_1, \ldots, t_s$ eine bedeutende Rolle spielen die Schlußfolgerung ziehen, daß man mit Hilfe von $(t_1, \ldots, t_s)$ eine gute Abschätzung für $n_0(t_1, \ldots, t_s)$ geben kann. Dies ist jedoch nicht wahr, es gilt sogar das folgende:

Sei $d \geqq 1$ eine natürliche Zahl. Zu einer beliebig großen Schranke K existieren solche natürliche Zahlen $(t_1, \ldots, t_s)$, für welche zwar $(t_1, \ldots, t_s) = d$ aber

$$n_0(t_1, \ldots, t_s) > K$$

gilt.

Dies kann man mit zwei einfachen Gegenbeispielen beweisen. Im Falle $d > 1$ ist für die Gleichung

$$x_1^d + p(x_2^{p-1} + \cdots + x_p^{p-1}) = 0$$

leicht beweisbar, daß sie in R_p nur die triviale Lösung besitzt, wobei die Primzahl p die Gestalt $p = k\,d + 1 > K$ hat. Im Falle $d = 1$ kann man für die Gleichung

$$x_1^6 + p\left(x_2^{p-1} + \cdots + x_{\frac{p-1}{2}}^{p-1} + \frac{p-1}{2}\, x_{\frac{p+1}{2}}^{\frac{3(p-1)}{2}}\right) = 0$$

leicht nachweisen, daß sie in R_p nur die triviale Lösung hat, wobei die Primzahl p die Gestalt $p = 12\,k - 1 > K$ hat.

Eine neue Möglichkeit zur Abschätzung von $n_0(t_1, \ldots, t_s)$ wird in folgenden Satz formuliert und ist das Hauptergebnis dieser Arbeit. Dabei stellt sich heraus, daß diese Abschätzung ohne weitere Einschränkungen nicht mehr verschärft werden kann.

Satz. *Sei* $(k_1, \ldots, k_n) \in V(n; t_1, \ldots, t_s)$, $p \geqq 3$ *eine beliebige Primzahl, ferner*

$$n \geqq \{\max_{1 \leqq i \leqq s} t_i\}^2 = k^2$$

Dann ist die Gleichung

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = 0$$

für beliebige ganze Zahlen $a_1, \ldots, a_n$ $(a_i \neq 0;\ i=1, \ldots, n)$ *lösbar;* $n > k^2$ *ist dann und nur dann notwendig, wenn* $k_1 = k_2 = \cdots = k_n = p-1$.

Am Ende der Arbeit wird mit einem Gegenbeispiel nachgewiesen, daß das Ergebnis auch dann nicht um mehr als ein Konstantenvielfaches verbessert werden kann, wenn wir von dem Fall $k_1 = k_2 = \cdots = k_n = p-1$ absehen.

2. §

Zum Beweis des Satzes benötigen wir einige Lemma. Ich werde die folgenden drei, aus der Literatur bekannten Lemma benutzen. Wegen des Typs des zu untersuchenden Problems und der Beweismethode ist eine Kenntnis bzw. Abschätzung der Zahl der n-ten Potenzrestklassen mod p^γ notwendig. Hierauf bezieht sich das folgende Lemma ([6]. Satz 13).

Lemma 1. *Sei* $p \geqq 3$ *eine Primzahl,* $n = p^\lambda \cdot d$ *und* $p \nmid d$ *ferner* $0 < l \leqq \lambda + 1$. *Die Zahl der verschiedenen n-ten Potenzrestklassen* mod p^l *die nicht durch p Teilbar sind, beträgt*

$$(p-1) \cdot (n \cdot p^{-\lambda}, p-1)^{-1}$$

Ist für das Polynom $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ mit ganzzahligen Koeffizienten für eine nur von dem Polynom abhängende natürliche Zahl γ die Kongruent

$$f(\mathbf{x}) \equiv 0 \mod p^\gamma$$

auf nichttriviale Weise lösbar, so ist sie im Sinne von Hensel's Lemma ([8], S. 62.) auch für alle Exponenten $k > \gamma$ lösbar. Ich werde von dieser Behauptung den folgenden Fall benutzen ([7]. Lemma 9.);

Lemma 2. *Sei* $n = p^\alpha \cdot d$ *wo* $p \nmid d$

$$\gamma = \begin{cases} \alpha + 1 & \text{wenn } p > 2 \text{ Primzahl ist,} \\ \alpha + 2 & \text{wenn } p = 2 \text{ ist.} \end{cases}$$

Wenn die Kongruenz

$$y^n \equiv a \mod p^\gamma \qquad (p, a) = 1$$

lösbar ist, dann ist für jede natürliche Zahl $k > \gamma$ *auch die Kongruenz*

$$x^n \equiv a \mod p^k$$

lösbar.

Eine wesentliche Rolle wird das folgende, leicht zu beweisende Lemma spielen [5]:

Lemma 3. *Sei $h>1$ eine feste positive ganze Zahl, H die additive Restklassengruppe modulo h und H' die Menge derjenigen Restklassen von H, die zu h relativ prim sind. Bezeichne S_0 eine nichtleere Teilmenge der verschiedenen Elemente von H, und $S_1, \ldots, S_d, \ldots$ eine nichtleere Teilmenge der verschiedenen Elemente von H'. $N(S_0, \ldots, S_d)$ bezeichne die Menge derjenigen verschiedenen Elemente von H, die als Summe von Elementen von $S_0, S_1, \ldots, S_d$ darstellbar sind derart, daß aus jeder der Mengen $S_0, \ldots, S_d$ höchstens ein Element als Summand auftritt. Wenn wir die Anzahl der Elemente einer Menge T mit $U[T]$ bezeichnen, so gilt*

$$U[N(S_0, \ldots, S_d)] \geqq \min\{h, U[S_0]+\cdots+U[S_d]\}$$

Im folgenden beweisen wir die beim Beweis des Satzes benötigten Lemma. Von diesen ist das erste sehr einfach zu beweisende Lemma gleichzeitig ein Beispiel dafür, wann

$$d^2 = (k_1, \ldots, k_n)^2 = n_0(t_1, \ldots, t_s)$$

erfüllt ist.

Lemma 4. *Ist $(k_1, \ldots, k_n) \in V(n; t_1, \ldots, t_s)$ so beschaffen, daß für irgendein natürliches Zahlenpaar $1 \leqq i \neq j \leqq n$*

$$(k_i, k_j) = 1$$

gilt, dann ist die Gleichung

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = 0$$

für beliebige von Null verschiedene ganze Zahlen $a_1, \ldots, a_n$ in R auf nichttriviale Weise lösbar.

Beweis. Ohne Beschränkung der Allgemeinheit können wir annehmen, daß $(k_1, k_2)=1$ und $k_1 = 2q+1$ gelten. Offenbar reicht es zu zeigen, daß die Gleichung

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} = 0$$

in R für alle ganzen Zahlen $a_1 \neq 0$, $a_2 \neq 0$ eine nichttriviale Lösung besitzt.

Wegen $(k_1, k_2)=1$ hat die Gleichung

$$1 + k_1 u = k_2 v$$

eine nichtnegative ganzzahlige Lösung u, v und die lineare diophantische Gleichung

$$1 + k_2 z = k_1 w$$

eine Lösung z, w derart, daß $w = 2f+1$ gilt.

Falls $\operatorname{sign} a_1 = \operatorname{sign} a_2$, so können wir voraussetzen, daß a_1 und a_2 positiv sind und dann befriedigen

$$x_1^0 = (a_1)^u \cdot (-a_2)^w$$
$$x_2^0 = (a_1)^v \cdot (a_2)^z$$

offenbar die Gleichung

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} = 0$$

wegen der Wahl von u, v, z, w und wegen $k_1 = 2q+1$.

Ist dagegen sign $a_1 \neq$ sign a_2, so können wir voraussetzen, daß $a_1 > 0$ und $a_2 < 0$, und diesem Fall ist

$$x_1^0 = (a_1)^u \cdot (-a_2)^w$$

$$x_2^0 = (a_1)^v \cdot (-a_2)^z$$

eine Lösung der Gleichung

$$a_1 x_1^{k_1} + a_2 x_2^{k_2} = 0$$

Womit der Beweis beendet ist.

Hieraus folgt schon die Lösbarkeit in jedem R_p.

Als sehr nützlich erweist sich das folgende Lemma;

Lemma 5. *Sei p eine beliebige Primzahl, $(k_1, \ldots, k_n) \in V(n; t_1, \ldots, t_s)$ sowie $a_1, \ldots, a_n$ beliebige von Null verschiedene ganze Zahlen und bezeichne*

$$k = \max_{1 \leqq i \leqq s} t_i$$

Dann ist die Lösung der Gleichung

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = 0 \tag{1}$$

in R_p äquivalent mit der Lösung einer Gleichung

$$F_0 + pF_1 + \cdots + p^{k-1} F_{k-1} = 0 \tag{2}$$

in R_p, wo F_i $(i = 0, \ldots, k-1)$ eine Form vom Typ (1) *ist, derart, daß kein koeffizient durch p teilbar ist; ferner kommt ein Variable x_m $(m = 1, \ldots, n)$ in einem und nur einem F_i mit dem gleichen Exponenten vor, wie in* (1) *und F_i hat keine in* (1) *nicht auftretende Variable.*

Beweis. Offenbar kann man

$$a_i = p^{\alpha_i + k_i \nu_i} \cdot b_i$$

so schreiben, daß $\nu_i \geqq 0$, $0 \leqq \alpha_i < k_i$, $p \nmid b_i$ für jede ganze Zahl $1 \leqq i \leqq n$. Sei nun

$$N = [k_1, \ldots, k_n] \quad \text{und} \quad x_i = p^{\frac{N - k_i \nu_i}{k_i}} \cdot x_i'.$$

Offensichtlich ist $\dfrac{N - k_i \gamma_i}{k_i}$ auf Grund der Definition von N eine ganze Zahl. Führen wir diese Substitution durch, so erhält (1) die folgende Gestalt

$$b_1 p^{\alpha_1} \cdot p^N (x_1')^{k_1} + \cdots + b_n p^{\alpha_n} \cdot p^N (x_n')^{k_n} = 0.$$

Sei

$$F_\nu = \sum_{\substack{j \\ \alpha_j = \nu}} b_j (x_j')^{k_j}, \qquad \nu = 0, 1, \ldots, k-1.$$

Teilen wir die Gleichung durch p^N und berücksichtigen, daß für alle $1 \leqq i \leqq n$ die Beziehung $0 \leqq \alpha_i < k_i \leqq k$ gilt, so erhält (1) die folgende Gestalt

$$F_0 + pF_1 + \cdots + p^{k-1} \cdot F_{k-1} = 0,$$

wobei die $F_0, F_1, \ldots, F_{k-1}$ die Bedingungen des Lemmas erfüllen.

Im weiteren bezeichnen wir in (2) die Anzahl der Variablen der F_i mit v_i.

Lemma 6. *Wenn in* (2)

$$v_0 + v_1 + \cdots + v_{k-1} \geqq k^2$$

so existiert entweder

a) *ein* $0 \leqq i \leqq k-1$ *derart, daß*

$$v_i \geqq \frac{3k}{2},$$

oder

b) $0 \leqq i \leqq k-2$ *derart,daß*

$$v_i \geqq k \quad \textit{und} \quad v_i + v_{i+1} \geqq 2k$$

BEWEIS. Nehmen wir an, daß weder a; noch b; erfüllt sind. Mit $v_{j_1}, v_{j_2}, \ldots, v_{j_m}$ bezeichnen wir diejenigen der $v_0, v_1, \ldots, v_{k-1}$, für welche $v_i \geqq k$ und $j_1, \ldots, j_m \leqq k-2$. Offenbar gilt $j_{i_1} - j_{i_2} > 1$ im Sinne der Negation der Bedingung b; für alle $1 \leqq i_1 \neq i_2 \leqq m$, sowie $v_{j_i} + v_{j_i+1} \leqq 2k-1$ ebenfalls auf Grund der Negation von b; für alle $1 \leqq i \leqq m$. Dann ist

$$v_{j_1} + v_{j_1+1} + v_{j_2} + \cdots + v_{j_m+1} \leqq m(2k-1).$$

Wir können voraussetzen, daß $j_1 < j_2 < \cdots < j_m$. Falls $j_m = k-2$, so gilt für jedes der hier nicht summierten v_i wegen der Wahl der v_{j_ν} die Bedingung $v_i \leqq k-1$. Die Zahl dieser v_i ist $(k-2 \cdot m)$ wegen $j_m = k-2$. Hieraus folgt, daß

$$\sum_{i=0}^{k-1} v_i \leqq (k-2m)(k-1), \qquad i \neq j_\nu,\ i \neq j_\nu + 1,\ \nu = 1, 2, \ldots, m,$$

was zusammen mit dem vorangehenden bedeutet, daß

$$\sum_{i=0}^{k-1} v_i \leqq (k-2m)(k-1) + m(2k-1) = k^2 - k + m.$$

Dies wiederspricht der Bedingung

$$\sum_{i=0}^{k-1} v_i \geqq k^2$$

weil offenbar $m < k$ ist.

Ist $j_m < k-2$, so haben wir wegen der Wahl der v_{j_m} die Relation $v_i \leqq k-1$ falls $i \neq j_\nu$, $i \neq j_\nu + 1$ für alle $\nu = 1, 2, \ldots, m$ und $i \neq k-1$ und so gilt

$$\sum_{i=0}^{k-2} v_i \leqq (k-1)(k-1-2m) \qquad (i \neq j_\nu,\ i \neq j_\nu + 1,\ \nu = 1, 2, \ldots, m),$$

da die Anzahl der Indizes i $(k-1-2m)$ beträgt. Auf Grund der Negation von a; ist

$$v_{k-1} \leqq \frac{3k}{2} - 1$$

und so gilt in diesem Fall

$$\sum_{i=0}^{k=1} v_i \leqq m(2k-1) + (k-2m-1)(k-1) + \frac{3k}{2} < k^2$$

da offenbar $m < \dfrac{k}{2}$, womit wir einen Wiederspruch zu der Voraussetzung des Lemmas erhalten. Damit ist die Behauptung bewiesen.

Lemma 7. *Seien $p>2$ eine belieibge Primzahl, $(k_1, \ldots, k_n) \in V(n; t_1, \ldots, t_s)$ und $b_1, \ldots, b_n$ durch p nicht teilbare von Null verschiedene ganze Zahlen. Wenn $n \geqq \frac{3k}{2}$ so ist die Gleichung*

$$b_1 x_1^{k_1} + \cdots + b_n x_n^{k_n} = 0$$

in R_p lösbar, wobei $k = \max t_i$. $1 \leqq i \leqq s$.

Beweis. Sei γ diejenige nicht negative ganze Zahl, für die $p^\gamma | t_i$ für irgenein $1 \leqq i \leqq s$ aber $p^{\gamma+1} \nmid t_i$ für alle $1 \leqq i \leqq s$.

a. 1; Ist $k \geqq p^{\gamma+1}$, so seien die Elemente der im Lemma 3 auftretenden S_i $(i=1, 2, \ldots, n)$ die durch die $b_i x_i^{k_i} \bmod p^{\gamma+1}$ angenommenen Werte über den Elementen des mod $p^{\gamma+1}$ reduzierten Restsystems. Offenbar gilt für die Zahl $U[S_i]$ der Elemente der S_i $U[S_i] \geqq 1$ und so gilt im Sinne von Lemma 3 für die Zahl N der mod $p^{\gamma+1}$ angenommenen Werte des Ausdrucks

$$b_1 x_1^{k_1} + \cdots + b_n x_n^{k_n}$$

$$N = \min \left\{ p^{\gamma+1}, \sum_{i=1}^{n} U[S_i] \right\} = p^{\gamma+1}$$

d.h. die Kongruenz

$$b_1 x_1^{k_1} + \cdots + b_n x_n^{k_n} \equiv 0 \mod p^{\gamma+1}$$

hat eine nichttriviale Lösung. Man kann voraussetzen, daß in einer Lösung $x_1^0, x_2^0, \ldots, x_n^0$ die Beziehung $x_1^0 \not\equiv 0 \bmod p$ gilt und dann ist

$$b_1 x_1^{k_1} \equiv -b_2 x_2^{k_2} \cdots - b_n x_n^{k_n} \equiv A \mod p^{\gamma+1}$$

und $A \not\equiv 0 \bmod p$ wegen $b_1 \not\equiv 0 \bmod p$ und $x_1^0 \not\equiv 0 \bmod p$. Dann ist aber im Sinne von Lemma 2 die kongruenz

$$b_1 x_1^{k_1} \equiv A \mod p^\nu$$

für jede natürliche Zahl ν lösbar, was bedeutet, daß die auch im R_p lösbar ist auf Grund der Interpretation der untersuchten Gleichung.

a. 2; Wenn $k < p^{\gamma+1}$ und $p^\gamma | k_i$ für alle $1 \leqq i \leqq n$, dann ist $k_i = d_i \cdot p^\gamma$ $1 \leqq d_i \leqq p-1$ für alle $1 \leqq i \leqq n$. Sei

$$d = \max_i d_i$$

Seien die Elemente der in Lemma 3 auftretenden S_i $(i=1, \ldots, n)$ die von den $b_i x_i^{k_i} \bmod p^{\gamma+1}$ angenommen Werte über dem reduzierten Restsystem mod $p^{\gamma+1}$. Im Sinne von Lemma 1 gilt für die Anzahl $U[S_i]$ der Elemente der S_i

$$U[S_i] = (p-1)(d_i, p-1)^{-1} \qquad 1 \leqq i \leqq n$$

Durch Anwendung vom Lemma 3 ergibt sich für die Anzahl N der durch den Ausdruck

$$b_1 x_1^{k_1} + \cdots + b_n x_n^{k_n}$$

dargestellten Restklassen mod $p^{\gamma+1}$

$$N = \min \{ p^{\gamma+1}, \sum U[S_i] \} = \min \left\{ p^{\gamma+1}, (p-1) \sum \frac{1}{(d_i, p-1)} \right\} = p^{\gamma+1}$$

wegen der Bedingung $p>2$. Dies bedeutet, daß die Kongruenz

$$b_1 x_1^{k_1} + \cdots + b_n x_n^{k_n} \equiv 0 \mod p^{\gamma+1}$$

eine nichttriviale Lösung besitzt, woraus auf ähnliche Weise wie bei a. 1; folgt, daß die untersuchte Gleichung in R_p auf nichttriviale Weise lösbar ist.

a. 3; Wenn $k<p^{\gamma+1}$ und wenn ein $1\leqq i\leqq n$ derart existiert, daß $p^{\gamma}\nmid k_i$, dann kann man voraussetzen, daß $i=1$. Seien die Elemente der S_i die durch die $b_i x_i^{k_i} \mod p^{\gamma}$ angenommenen Werte ($i=2, 3, \ldots, n$) über dem Restklassensystem mod p^{γ}. Im Sinne von Lemma 3 gilt für die Anzahl N der durch den Ausdruck

$$b_2 x_2^{k_2} + b_3 x_3^{k_3} + \cdots + b_n x_n^{k_n}$$

mod p^{γ} dargestellten Restklassen

$$N = \min\left\{p^{\gamma}, \frac{3k}{2} - 1\right\} = p^{\gamma}$$

was bedeutet, daß die Kongruenz

$$b_2 x_2^{k_2} + b_3 x_3^{k_3} + \cdots + b_n x_n^{k_n} \equiv -b_1 \mod p^{\gamma}$$

lösbar ist. Hieraus folgt, daß die Kongruenz

$$b_1 x_1^{k_1} + b_2 x_2^{k_2} + \cdots + b_n x_n^{k_n} \equiv 0 \mod p^{\gamma}$$

eine Lösung hat, derart daß $x_1 \not\equiv 0 \mod p$. Unter Beachtung daß $p^{\gamma}\nmid k_1$ und $p\nmid b_1$ kann man ähnlich wie im a. 1; einsehen, daß hieraus die Lösbarkeit der untersuchten Gleichung in R_p folgt. a. 1;, a. 2; und a. 3; zusammen zeigen die Richtigkeit der Behauptung.

Lemma 8. *Sei $p>2$ eine beliebige Primzahl, $(k_1, \ldots, k_n)\in V(n; t_1, \ldots, t_s)$ und $b_1, \ldots, b_n$ beliebige durch p nicht teilbare ganze Zahlen. Die Gleichung*

$$b_1 x_1^{k_1} + \cdots + b_m x_m^{k_m} + p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n}) = 0$$

ist in R_p lösbar, falls $m\geqq k$, $n \geqq 2k$, $p|k_i$ für irgendein $1\leqq i\leqq n$ erfüllt ist.

Beweis. A; Falls $m \geqq \frac{3}{2}k$, so ist die Behauptung im Sinne von Lemma 7 richtig und man kann voraussetzen, daß $m < \frac{3}{2}k$ gilt.

B; Wenn $k\geqq p^{\gamma+1}$, dann ergibt sich unter Anwendung von Teil a. 1; von Lemma 7 wegen der Bedingung $m\geqq k$ die Lösbarkeit der Gleichung

$$b_1 x_1^{k_1} + \cdots + b_m x_m^{k_m} = 0$$

in R_p und damit ist die Behauptung auch in diesem Fall erfüllt.

C; Wenn $k<p^{\gamma+1}$ und wenn ein $1\leqq i\leqq m$ derart existiert, daß $p^{\gamma}\nmid k_i$, dann kann man $i=1$ voraussetzen. Seien die Elemente des im Lemma 3 auftretenden S_0 die durch den Ausdruck

$$p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n})$$

dargestellten Restklassen mod p^{γ}. Die Elemente der S_i seien die über dem Restsystem

mod p^γ durch die $b_i x_i^{k_i} \bmod p^\gamma$ angenommenen Werte für alle $2 \leqq i \leqq m$. Unter Anwendung von Lemma 3 ergibt sich für die Zahl N der durch den Ausdruck

$$b_2 x_2^{k_2} + b_3 x_3^{k_3} + \cdots + b_m x_m^{k_m} + p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n})$$

dargestellten Restklassen mod p^γ

$$N = \min\{p^\gamma, m\} = p^\gamma$$

und hieraus folgt ähnlich dem Schluß von a. 3; bei Lemma 7 die Behauptung. Wir können dabei annehmen, daß $p^\gamma | k_i$ für alle $1 \leqq i \leqq m$

D. 1; Wenn $p^\gamma | k_i$ für alle $m+1 \leqq i \leqq n$ erfüllt ist, so gilt $k_i = p^\gamma \cdot d_i$, $1 \leqq d_i \leqq p-1$ für alle $1 \leqq i \leqq n$. Die Elemente des in Lemma 3 auftretenden S_0 seien die durch den Ausdruck

$$p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n})$$

Elemente des Restsystems mod $p^{\gamma+1}$ die Elemente der S_i $(i=2, \ldots, m)$ die über dem reduzierten Restsystem mod $p^{\gamma+1}$ durch die $b_i x_i^{k_i} \bmod p^{\gamma+1}$ angenommenen Werte. Ähnlich wie bei dem Teil a. 2; beim Beweis von Lemma 7 kann man einsehen, daß

$$U[S_0] \geqq \min\left\{p^\gamma, \frac{(n-m)(p-1)}{d}\right\}$$

Sei $U[S_0] = \dfrac{(n-m)(p-1)}{d}$. Aus Lemma 3 ergibt sich unter Benutzung von Lemma 1 für die Anzahl N der durch den Ausdruck

$$b_2 x_2^{k_2} + b_3 x_3^{k_3} + \cdots + b_m x_m^{k_m} + p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n})$$

dargestellten Restklassen mod $p^{\gamma+1}$

$$N \geqq \min\left\{p^{\gamma+1}, \frac{(m-1)(p-1)+(n-m)(p-1)}{d}\right\} \geqq$$

$$\geqq \min\left\{p^{\gamma+1}, \frac{(2dp^\gamma - 1)(p-1)}{d}\right\} = p^{\gamma+1}$$

sofern nur $\gamma \geqq 1$ und $p \geqq 3$, was wir vorausgesetzt hatten. Hieraus folgt, daß die Kongruenz

$$b_2 x_2^{k_2} + b_3 x_3^{k_3} + \cdots + b_m x_m^{k_m} + p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n}) \equiv -b_1 \mod p^{\gamma+1}$$

lösbar ist, woraus sich die Behauptung, ähnlich wie beim Teil a. 3; des Beweises von Lemma 7, ergibt.

Sei $U[S_0] = p^\gamma$. Die Elemente von $S_0, S_2, S_3, \ldots, S_m$ seien dieselben, wie im vorangehenden und die Elemente von S_1 seien die durch $b_1 x_1^{k_1} \bmod p^{\gamma+1}$ über dem Restsystem mod $p^{\gamma+1}$ angenommenen Werte. Unter Benutzung von Lemma 1 ergibt sich aus Lemma 3 daß für die Zahl N der durch den Ausdruck

$$b_1 x_1^{k_1} + b_2 x_2^{k_2} + \cdots + b_m x_m^{k_m} + p(b_{m+1} x_{m+1}^{k_{m+1}} + \cdots + b_n x_n^{k_n})$$