ARKIV FÖR MATEMATIK Band 3 nr 22

Mitgeteilt am 25. Mai 1955 durch T. NAGELL

# Einige Sätze über lineare Kongruenzen

Von LARS FJELLSTEDT

**1.** Man verdankt THUE den folgenden Satz:

*Es seien $a$, $b$ und $m$ teilerfremd. Dann ist die Kongruenz*

$$ax - by \equiv 0 \pmod{m} \tag{1}$$

*immer lösbar in ganzen rationalen Zahlen $x$, $y$ mit $|x| \leqq \sqrt{m}$, $|y| \leqq \sqrt{m}$.*

Dieser Satz ist später von THUE selbst und von verschiedenen anderen Autoren neu bewiesen und verallgemeinert worden. Siehe dazu BRAUER-REYNOLDS [1]. Für die Betrachtungen dieser Arbeit werden die folgenden Sätze zugrunde gelegt:

1°. *Es sei $(a_1, a_2, \ldots, a_n) = 1$, dann ist die Kongruenz*

$$\sum_{i=1}^{r} a_i x_i \equiv 0 \pmod{m} \tag{2}$$

*immer lösbar in ganzen Zahlen $x_i$ mit $|x_i| \leqq m^{1/r}$.*

2°. *Das System von homogenen linearen Kongruenzen*

$$\sum_{i=1}^{s} a_{ik} x_i \equiv 0 \pmod{m} \qquad k = 1, 2, \ldots, r \tag{3}$$

*wo $r < s$, hat immer eine Lösung mit $|x_i| \leqq m^{r/s}$.*

Die Resultate, die wir in dieser Arbeit beweisen wollen, können als Verschärfungen des THUEschen Satzes und seine Verallgemeinerungen angesehen werden.

Wir werden der Einfachheit halber immer Ebene statt Ebene oder Hyperebene und Parallelogramm statt Parallelogramm oder Parallelepiped schreiben.

Es sei jetzt nach der Anzahl der primen Lösungen von (1) gefragt, die die Bedingung $|x| \leqq \sqrt{m}$, $|y| \leqq \sqrt{m}$ erfüllen. NAGELL [2] hat bewiesen, dass diese Anzahl gleich 1 oder 2 ist. Wenn wir statt (1) die allgemeine Kongruenz (2) betrachten, lässt sich die Frage nicht ganz so einfach beantworten. Es gilt das folgende Resultat:

**Satz 1.** *Es sei $D$ der Inhalt der Ebene*

$$\sum_{i=1}^{r} a_i x_i = 0 \tag{4}$$

*innerhalb des Würfels $|x_i| \leqq m^{1/r}$. Es sei ferner $A_r(m)$ die Anzahl der Lösungen der Kongruenz (2) mit $|x_i| \leqq m^{1/r}$. Dann gilt*

$$A_r(m) = \frac{D}{\left(\sum_{i=2}^{r} a_i^2\right)^{\frac{1}{2}}} + 0\left(m^{\frac{r-2}{r}}\right). \tag{5}$$

Es ist zu bemerken, dass die Lösungen nicht als teilerfremd vorausgesetzt sind. Weiter denken wir uns immer die Koeffizienten $a_i$ modulo $m$ reduziert.

Der Beweis von Satz 1 wird den folgenden Hilfsätzen vorausgeschickt:

**Hilfsatz 1.** *Es sei $W$ ein $n$-dimensionaler Würfel von Kantenlänge $2r$ (mit Origo als Mittelpunkt). Dann ist die Anzahl der Gitterpunkte innerhalb und auf dem Rande von $W$ gleich*

$$(2r)^n + 0(r^{n-1})$$

*oder, wenn das Gitter parallelepipedisch von der relativen Dichte $d$ ist, gleich*

$$d(2r)^n + 0(r^{n-1}).$$

Die relative Dichte wird durch $1/d =$ Inhalt eines Fundamentalparallelogramms des enthaltenen Gitters definiert.

Der Beweis verläuft vollkommen analog wie die Restabschätzung $0(r)$ im zweidimensionalen Falle. Siehe etwa LANDAU [3, S. 185, 3]. Übrigens sieht man sofort ein, dass dasselbe Resultat auch für einen beliebigen konvexen Bereich gilt, der durch eine endliche Anzahl von Ebenen begrenzt wird, und wo der Inhalt des Randes nicht zu gross ist.

Eine grobe Abschätzung ergibt

$$|0(r^{n-1})| \leqq 2^{n+1}(\sqrt{n}+1)r^{n-1}, \qquad r > n^2$$

bzw.

$$|0(r^{n-1}) \leqq d \cdot 2^{n+1}(\sqrt{n}+1)r^{n-1}, \qquad r > n^2.$$

**Hilfsatz 2.** *Die Gitterpunkte in der Ebene*

$$\sum_{i=1}^{n} a_i x_i = 0, \qquad (a_1, a_2, \ldots, a_n) = 1 \tag{6}$$

*bilden ein parallelepipedisches Gitter. Der Inhalt eines Fundamentalparallelogramms ist gleich*

$$H = \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}}.$$

**Beweis.** Wenn wir die Ebene (6) auf etwa $x_1 = 0$ abbilden, wird die Funktionaldeterminante $= a_1/H$. Da aber noch gefordert wird, dass für ganzzahlige Werte von $x_2, \ldots, x_n$ in (6) der entsprechende Wert für $x_1$ auch ganzzahlig sein soll, so folgt, dass der Inhalt eines Fundamentalparallelogramms $= H$ ist.

**Beweis von Satz 1.** Der Satz folgt unmittelbar aus den vorangehenden Hilfsätzen. Wir bemerken hier nur, dass die Abschätzungen der 0-term jetzt nicht mehr zu gelten brauchen. Es ist aber leicht einzusehen, dass

$$|0(m^{\frac{r-2}{r}})| \leqq \frac{2^{s/2} r\,(\sqrt{r}+1)}{\left(\sum_{i=1}^{r} a_i^2\right)^{\frac{1}{2}}} m^{\frac{r-2}{r}}, \qquad m > r^{2r}. \tag{6'}$$

In analoger Weise lässt sich für Systeme von Kongruenzen der folgende Satz beweisen:

**Satz 2.** *Es sei $D$ der Inhalt der Ebene*

$$\sum_{i=1}^{s} a_{ik} x_i = 0, \qquad \begin{matrix} k = 1, 2, \ldots, r, \; r < s \\ (a_{1k}, a_{2k}, \ldots, a_{sk}) = 1 \end{matrix} \tag{7}$$

*innerhalb des Würfels $|x_i| \leqq m^{r/s}$. Es sei ferner $A_r^s(m)$ die Anzahl der Lösungen des Systemes* (3) *von Kongruenzen mit $|x_i| \leqq m^{r/s}$. Dann gilt*

$$A_r^s(m) = \frac{D}{\prod_{k=1}^{r}\left(\sum_{i=1}^{s} a_{ik}^2\right)^{\frac{1}{2}}} + 0(m^{r - \frac{r(r-1)}{s}}). \tag{8}$$

Wie vorher lässt sich das Restglied leicht abschätzen, worauf wir aber hier nicht eingehen.

Unter der Annahme, dass $m$ genügend gross ist, damit wir von den Restgliedern in (5) und (8) absehen können, wollen wir jetzt die folgende Frage studieren: Wie klein kann $D$ oder, was auf dasselbe hinausläuft, wie viel können die Exponenten $1/r$ bzw. $r/s$ in den verallgemeinerten THUEschen Sätzen verkleinert werden, ohne dass $A_r^s(m) < 2$ wird? Die Antwort folgt direkt aus Satz 1 und Satz 2, die dadurch als Verallgemeinerungen der allgemeinen THUEschen Sätze angesehen werden können.

**2.** DE BACKER [4] hat die Richtigkeit des folgenden Satzes behauptet:

*Es sei $(a, m) = 1$ und $b$ eine beliebige ganze rationale Zahl. Dann hat die Kongruenz*

$$ax \equiv y + b \pmod{m}$$

*immer eine Lösung mit $|x| \leqq \sqrt{m}$, $|y| \leqq \sqrt{m}$.*

Dieser Satz ist falsch. BRAUER-REYNOLDS [1] geben ein Gegenbeispiel an. Dagegen gilt der folgende Sats.

**Satz 3.** *Es sei* $(a, m)=(a, b)=1$, $a, b$ *und* $c<\sqrt{m}$. *Dann hat die Kongruenz*

$$ax+by\equiv c \pmod{m} \tag{9}$$

*immer eine Lösung mit* $|x|\leqq\sqrt{m}$, $\left|\frac{c}{b}-y\right|\leqq\sqrt{m}$.

Speziell gibt es also immer eine Lösung mit $|x|\leqq\sqrt{m}$, $|y|\leqq\sqrt{m}+|c|$.

**Beweis:** Unter den Voraussetzungen des Satzes gibt es einen Gitterpunkt auf der Gerade

$$ax+by=0 \tag{10}$$

mit $|x|\leqq\sqrt{m}$, $|y|\leqq\sqrt{m}$. Wenn wir nun irgendeinen Punkt $(\alpha, \beta)$ auf (10) nehmen, so liegt auf dieser Gerade immer ein Gitterpunkt $(x, y)$ mit $|x-\alpha|\leqq\sqrt{m}$, $|y-\beta|\leqq\sqrt{m}$. Die Lösungen der Kongruenz (9) bilden ein Gitter $G$. Die Lösungen von (9) für $c=0$ bilden ein Gitter $G_1$. Da $G$ offenbar durch eine Translation in $G_1$ übergeführt werden kann, folgt die Richtigkeit der Satzes.

## LITERATUR

1. BRAUER, A. u. REYNOLDS, R. L., On a theorem of Aubry-Thue. Canadian J. of Math. *3*, 367–74 (1951).
2. NAGELL, T., Sur un théorème d'Axel Thue. Arkiv f. Mat. Bd. *1*, Nr. 33.
3. LANDAU, Vorlesungen über Zahlentheorie II. Leipzig 1927.
4. DE BACKER, S. M., Solutions modérées d'un système de congruences du premier degrée pour un module premier $p$. Bull. de la Cl. d. Sci. de l'Acad. R. d. Belgique (5) vol. *34*, 46–51 (1948).

Tryckt den 31 januari 1956

Uppsala 1956. Almqvist & Wiksells Boktryckeri AB