Eine Bemerkung über lineare Kongruenzen.

Von

P. Erdös (Budapest) und V. Jarník (Praha).

Kleine lateinische Buchstaben bedeuten in dieser Note ganze Zahlen, kleine griechische Buchstaben — reelle Zahlen.

Herr A. Khintchine hat in zwei Arbeiten mit dem gemeinsamen Titel „Über die angenäherte Auflösung linearer Gleichungen in ganzen Zahlen“ [1]) zwei wichtige Sätze über die angenäherte Lösung der Gleichung

$$\vartheta_1 x_1 + \vartheta_2 x_2 + \ldots + \vartheta_n x_n + x_{n+1} = \alpha$$

bewiesen. Die Hauptschwierigkeit lag dabei im Beweis des folgenden Hilfssatzes, der auch ein selbständiges Interesse beanspruchen darf:

Satz [2]). *Zu jedem Paar von positiven Zahlen γ, n gibt es ein $\delta = \delta(\gamma, n) > 0$ mit folgender Eigenschaft:*

Sind $r_1, r_2, \ldots, r_n, q$ ganze Zahlen mit

$$q > 0, \quad (r_1, \ldots, r_n, q) = 1 \tag{1}$$

und besitzt die Kongruenz

$$\sum_{i=1}^{n} r_i x_i \equiv 0 \pmod q \tag{2}$$

keine Lösung mit

$$0 < \max_{1 \le i \le n} |x_i| \le \gamma q^{\frac{1}{n}}, \tag{3}$$

so besitzt die Kongruenz

$$\sum_{i=1}^{n} r_i x_i \equiv m \pmod q$$

für jedes m eine Lösung mit

$$\max_{1 \le i \le n} |x_i| \le \delta q^{\frac{1}{n}}.$$

Für diesen Satz wollen wir einen neuen und einfacheren Beweis mitteilen. Dazu brauchen wir zwei Hilfssätze.

Hilfssatz 1 [3]). *Zu jedem $\mu > 0$ gibt es ein ganzes $\lambda = \lambda(\mu) > 0$ mit folgender Eigenschaft: Es sei $q > 0$, $l > 0$ und es sei $0 < a_1 < a_2 < \ldots < a_l \le q$; für jedes x mit $0 < x \le q$ sei die Anzahl der $a_i \le x$ mindestens gleich μx (also $a_1 = 1$); dann ist jede natürliche Zahl $\le q$ als Summe von höchstens λ (gleichen oder ungleichen) Summanden a_i darstellbar.*

Beweis [4]). Ohne Beschränkung der Allgemeinheit sei $\mu \le 1$. Für $h \ge 1$ seien

$$a_{1,h} < a_{2,h} < \ldots$$

diejenigen natürlichen Zahlen $\le q$, die sich als Summe von höchstens h Summanden a_i darstellen lassen (also $a_{i,1} = a_i$). Für $0 \le x \le q$ sei $N_h(x)$ die Anzahl der $a_{i,h} \le x$ (also $N_h(0) = 0$; zur Abkürzung werde $N_1(x) = N(x)$ gesetzt); μ_h sei die untere Grenze von $N_h(x) : x$ für $x = 1, 2, \ldots, q$ (also $\mu_1 \ge \mu$). Wir wollen zuerst zeigen, dass

$$1 - \mu_h \le (1 - \mu)^h. \tag{4}$$

---

[1]) Rec. math. de la Soc. math. de Moscou 32 (1924), S. 203 — 218 und Acta Arithmetica 2.

[2]) Dieser Satz tritt in den beiden zitierten Arbeiten als Hilfssatz 3 auf. Herr Khintchine schreibt in (3)

$$\left(\sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}} \quad \text{statt} \quad \max_{1 \le i \le n} |x_i|,$$

was freilich für unsere Zwecke auf dasselbe hinausläuft.

[3]) Wohlbekannt; man kann diesen Hilfssatz z. B. sofort aus den Betrachtungen vom Herrn E. Landau in seiner Arbeit Die Goldbachsche Vermutung und der Schnirelmannsche Satz, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Math.-Phys. Klasse 1930, S. 255 — 276 ablesen (vgl. insb. Satz 14 und den Beweis des Satzes 15).

[4]) Fast wörtlich nach E. Landau, l. c.[3]).

Für $h=1$ ist (4) wahr. Ist aber (4) für ein $h \geqq 1$ wahr, so ergibt sich die Richtigkeit für $h+1$ folgendermassen: für $1 \leqq x \leqq q$ ist (man beachte, dass im Intervall $a_i < z \leqq b$ für $a_i \leqq b \leqq q$ genau $N_h(b-a_i)$ Zahlen $a_i + a_{j,h}$ liegen)

$$N_{h+1}(x) \geqq N(x) + \sum_{i=1}^{N(x)-1} N_h(a_{i+1}-a_i-1) + N_h(x-a_{N(x)})$$

$$\geqq N(x) + \mu_h \left\{ \sum_{i=1}^{N(x)-1} (a_{i+1}-a_i-1) + x - a_{N(x)} \right\}$$

$$= N(x) + \mu_h (x - N(x)) \geqq (1-\mu_h)\mu x + \mu_h x;$$

$$\mu_{h+1} \geqq \mu - \mu_h \mu + \mu_h;$$

$$1 - \mu_{h+1} \leqq (1-\mu)(1-\mu_h) \leqq (1-\mu)^{h+1}.$$

Also gilt (4) stets. Man wähle nun ein $h = h(\mu)$ so, dass $(1-\mu)^h \leqq \frac{1}{2}$, also $\mu_h \geqq \frac{1}{2}$ und man setze $\lambda(\mu) = 2h(\mu)$.

Es sei $1 \leqq x \leqq q$; es seien

(5) $$b_1 < b_2 < \ldots < b_k$$

diejenigen $a_{i,h(\mu)}$, die $\leqq x$ sind. Die Anzahl dieser Zahlen und ebenso die Anzahl der Zahlen

(6) $$x - b_1,\ x - b_2,\ \ldots,\ x - b_k$$

ist $\geqq \frac{1}{2}x$. Ist $b_k = x$, so ist x als Summe von höchstens $h(\mu) < \lambda(\mu)$ Summanden a_i darstellbar. Ist aber $b_k < x$, so sind alle Zahlen (5) und (6) $\geqq 1$ und $< x$; also gibt es unter ihnen höchstens $x-1$ verschiedene Zahlen, also ist für geeignete i, j

$$b_i = x - b_j, \qquad x = b_i + b_j,$$

also ist x als Summe von höchstens $2h(\mu) = \lambda(\mu)$ Summanden a_i darstellbar, w. z. b. w.[5]).

[5]) Unser Wert von λ ist im Allgemeinen nicht scharf; schärfere Sätze in dieser Richtung findet man bei A. Khintchine, Zur additiven Zahlentheorie, Rec. math. de la Soc. math. de Moscou 39 (1932), S. 27 — 34 und A. S. Besicovitch, On the density of the sum of two sequences of integers, Journal of the London Math. Soc. 10 (1935), S. 246 — 248.

Hilfssatz 2. *Zu jedem $\alpha > 0$ gibt es zwei Zahlen $\beta_1 = \beta_1(\alpha) > 0$, $\beta_2 = \beta_2(\alpha) > 0$ mit folgender Eigenschaft: Ist $q > 0$, sind $a_1, a_2, \ldots, a_l$ paarweise inkongruent mod q und ist $l \geqq \alpha q$, so gibt es ein b mit folgenden Eigenschaften:*

1) $$0 < b \leqq \beta_2;$$

2) *zu jedem r gibt es eine Summe von höchstens β_1 Summanden $\pm a_i$, welche modulo q kongruent der Zahl br ist.*

Beweis. Ohne Beschränkung der Allgemeinheit sei $\alpha \leqq 1$,

$$0 \leqq a_1 < a_2 < \ldots < a_l < q \qquad (l \geqq \alpha q).$$

Man setze $\beta_1 = 4\lambda\left(\frac{\alpha^2}{8}\right) \geqq 4$, $\beta_2 = \frac{4}{\alpha^2} > \frac{2}{\alpha}$.

Ist $q \leqq \frac{4}{\alpha^2}$, so setze man $b = q \leqq \beta_2$; es ist dann stets $a_1 - a_1 \equiv br \pmod q$, also die Behauptung wahr (da $\beta_1 \geqq 2$).

Es sei nun $q > \frac{4}{\alpha^2} > \frac{2}{\alpha}$. Man bezeichne mit

(7) $$b_0 < b_1 < \ldots < b_m$$

die Menge aller Zahlen $a_k - a_i$ mit $1 \leqq i \leqq k \leqq l$. Also ist $b_0 = 0$, $b_m < q$, $m \geqq l - 1 \geqq \alpha q - 1 > \frac{1}{2}\alpha q$; daher ist $0 < b_1 < \frac{2}{\alpha} < \beta_2$ (denn sonst wäre $a_l \geqq \frac{2}{\alpha}(l-1) > q$). Unter den Zahlen (7) gibt es also eine Menge von mindestens

$$\frac{m+1}{b_1} \geqq \frac{l}{b_1} \geqq \frac{\alpha q}{b_1} > \frac{\alpha^2 q}{2}$$

Zahlen, welche einer und derselben Restklasse modulo b_1 angehören; man bezeichne die Zahlen dieser Menge mit $c_1, c_2, \ldots, c_s \left(s > \frac{1}{2}\alpha^2 q\right)$; weiter sei

(8) $$d_1 < d_2 < \ldots < d_t$$

die Menge aller Differenzen $c_i - c_j$ mit $c_j < c_i$; endlich sei

$$b_1 f_1 < b_1 f_2 < \ldots < b_1 f_v$$

die Menge, welche aus (8) durch Hinzufügen der Zahl b_1 entsteht (also $v = t$ oder $v = t+1$; man beachte, dass alle d_j durch b_1 teilbar sind). Also ist

$$1 = f_1 < f_2 < \ldots < f_v,\ f_v \leqq b_1 f_v < q.$$

Ist $0<k\leqq\frac{\alpha^2}{4}q$, so gibt es mindestens ein Intervall

$$\left\langle \frac{i}{k}q,\quad \frac{i+1}{k}q \right\rangle$$

mit $0\leqq i<k$, in welchem mindestens

$$\frac{s}{k}>\frac{\alpha^2 q}{2k}\geqq 2$$

Zahlen c_j liegen; unter den Zahlen d_{j-} also umsomehr unter den Zahlen f_j, gibt es also mindestens $\frac{s}{k}-1>\frac{\alpha^2 q}{4k}$ Zahlen, die $\leqq\frac{q}{k}$ sind.

Es sei nun $1\leqq x\leqq q$; $z(x)$ sei die Anzahl der $f_j\leqq x$. Für $1\leqq x\leqq\frac{8}{\alpha^2}$ ist $z(x)\geqq 1\geqq\frac{\alpha^2 x}{8}$. Ist aber $\frac{8}{\alpha^2}<x\leqq q$, so setze man $k=\left[\frac{2q}{x}\right]$, also $k\leqq\frac{2q}{x}<\frac{\alpha^2 q}{4}$, andererseits $k>\frac{q}{x}$, $x>\frac{q}{k}$; also ist $z(x)>\frac{\alpha^2 q}{4k}\geqq\frac{\alpha^2 x}{8}$. Also ist stets $z(x)\geqq\frac{\alpha^2 x}{8}$. Nach dem Hilfssatz 1 ist also jede natürliche Zahl $r\leqq q$ als Summe von höchstens $\lambda\left(\frac{\alpha^2}{8}\right)=\frac{1}{4}\beta_1$ Summanden f_j darstellbar; jede Zahl rb_1 mit $0<r\leqq q$ ist also als Summe von höchstens $\frac{1}{4}\beta_1$ Summanden $b_1 f_j$ darstellbar; jede Zahl rb_1 $(-\infty<r<\infty)$ ist also modulo q kongruent einer Summe von höchstens $\frac{1}{4}\beta_1$ Summanden $b_1 f_j$. Man beachte nun, dass $b_1 f_1=b_1$ gleich der Differenz zweier a_i ist und dass jedes andere $b_1 f_j$ die Gestalt $a_k-a_i+a_h-a_g$ hat. Daraus und aus $0<b_1<\beta_2$ folgt die Behauptung.

Beweis des Khintchineschen Satzes. Es seien $\gamma>0$, $n>0$, $r_1,\ldots,r_n$, q mit (1) gegeben; (2) besitze keine Lösung mit (3). Daraus folgt: lässt man die Zahlen $x_1,\ldots,x_n$ unabhängig voneinander die Werte $0, 1, 2, \ldots, \left[\gamma q^{\frac{1}{n}}\right]$ durchlaufen, so sind die zugehörigen Zahlen

$$\sum_{i=1}^{n} r_i x_i \qquad \left(0\leqq x_i\leqq\gamma q^{\frac{1}{n}}\right) \tag{9}$$

paarweise inkongruent mod q; ihre Anzahl ist $>\gamma^n q$. Wendet man nun auf die Menge der Zahlen (9) den Hilfssatz 2 mit $\alpha=\gamma^n$ an, so folgt die Existenz einer Zahl b mit $0<b\leqq\beta_2(\gamma^n)$, welche folgende Eigenschaft besitzt: für jedes r sind die Beziehungen

$$\sum_{i=1}^{n} r_i x_i\equiv r\,b\ (\mathrm{mod}\ q),\quad |x_i|\leqq\gamma\,\beta_1(\gamma^n)\,q^{\frac{1}{n}} \qquad (l=1,2,\ldots,n) \tag{10}$$

lösbar.[6])

Es sei nun m beliebig gegeben; wegen (1) gibt es Zahlen $y_1,\ldots,y_n$, r, z mit

$$\sum_{i=1}^{n} r_i y_i + r\,b + z\,q = m\,. \tag{11}$$

Da diese Gleichung bestehen bleibt, wenn man y_i um $\pm b$ und gleichzeitig r um $\mp r_i$ ändert, darf man voraussetzen, dass $|y_i|<b\leqq\beta_2(\gamma^n)$ für $i=1,2,\ldots,n$ ist. Dann folgt aber aus (10), (11)

$$\sum_{i=1}^{n} r_i(x_i+y_i)\equiv m\ (\mathrm{mod}\ q)\,,$$

$$\max_{1\leqq i\leqq n}|x_i+y_i|\leqq\gamma\,\beta_1(\gamma^n)\,q^{\frac{1}{n}}+\beta_2(\gamma^n)\leqq(\gamma\,\beta_1(\gamma^n)+\beta_2(\gamma^n))\,q^{\frac{1}{n}}=\delta(\gamma,n)\,q^{\frac{1}{n}}\,.$$

Bemerkung zum Hilfssatz 2. Wir wollen noch zeigen, dass man die Zahl b des Hilfssatzes 2 durch die Zahl

$$d=(a_1,\ldots,a_l,q)$$

ersetzen darf. Da b mod q einer Summe von Zahlen $\pm a_i$ kongruent ist, ist $d|b$. Es sei $a_i=a_i' d$, $b=b' d$, $q=q' d$. Es seien $p_1,\ldots,p_y$ die verschiedenen Primfaktoren von (b',q'); also $0\leqq y\leqq b'\leqq b\leqq\beta_2$ und wegen $(a_1',\ldots,a_l',q')=1$ gibt es zu jedem j $(1\leqq j\leqq y)$ ein $a'_{i(j)}$ mit $p_j\nmid a'_{i(j)}$. Also ist $(a'_{i(1)},\ldots,a'_{i(y)},b',q')=1$. Für jedes r gibt es also Zahlen w_j, r', z mit

$$\sum_{j=1}^{y} a'_{i(j)}\,w_j + b'\,r' + q'\,z = r\,, \tag{12}$$

wobei man offenbar noch erreichen kann, dass $|w_j|<b'\leqq\beta_2$ ist. Aus (12) folgt aber

[6]) Die Beziehung $(r_1,\ldots r_n,q)=1$ haben wir bisher noch garnicht benutzt; das wollen wir erst jetzt tun.

$$\sum_{j=1}^{v} a_{i(j)} w + b r' + q z = r d ;$$

nach der im Hilfssatz 2 hervorgehobenen Eigenschaft von b ist also $r d$ modulo q einer Summe von höchstens $\beta_2 \cdot \beta_2 + \beta_1$ Summanden $\pm a_i$ kongruent.

Bemerkung. Beschränkt man sich im Khintchineschen Satz auf den Fall, dass q eine *Primzahl* ist, so ist dieser Satz — und zwar mit $\delta = \frac{2}{\gamma^{n-1}}$ — eine unmittelbare Folge des folgenden Satzes vom Herrn Davenport[7]): „Ist q eine Primzahl, sind die Zahlen $a_1, \ldots, a_k$ — und ebenso die Zahlen $b_1, \ldots b_l$ — paarweise inkongruent modulo q, so stellen die Zahlen $a_i + b_j (1 \leqq i \leqq k,\ 1 \leqq j \leqq l)$ mindestens $\mathrm{Min}(k+l-1, q)$ verschiedene Restklassen modulo q dar". In der Tat: ist $\gamma^n q \leqq 2$, so hat jede Kongruenz

$$(13) \qquad \sum_{i=1}^{n} r_i x_i \equiv m \pmod q$$

eine Lösung mit

$$|x_i| < q = q^{\frac{n-1}{n}} q^{\frac{1}{n}} \leqq \frac{2^{\frac{n-1}{n}}}{\gamma^{n-1}} q^{\frac{1}{n}} < \delta q^{\frac{1}{n}} .$$

Ist aber $\gamma^n q > 2$, so beachte man, dass die Zahlen (9) mehr als $\gamma^n q > 2$ verschiedene Restklassen modulo q darstellen (also $\gamma \leqq 1$). Man wähle $c = \left[\frac{2}{\gamma^n}\right]$; dann ist

$$\gamma^n q + (c-1)(\gamma^n q - 1) > (c+1)\frac{\gamma^n}{2} q > q ;$$

durch wiederholte Anwendung des Davenportschen Satzes bekommt man also folgendes Resultat: jedes m ist modulo q einer Summe von höchstens c Zahlen (9) kongruent; also hat (13) eine Lösung mit

$$|x_i| \leqq c \cdot \gamma q^{\frac{1}{n}} \leqq \delta q^{\frac{1}{n}} .$$

(Eingegangen am 1. Oktober 1936.)

[7]) H. Davenport: On the addition of residue classes, Journal of the London Mathematical Society **10** (1935), S. 30 — 32.

Eine Aufgabe aus der algebraischen Zahlentheorie.

Von

N. Tschebotarŏw (Kasan).

(Meinem verehrten Lehrer Prof. Dr. A. Grawe zum 50. Jahr seiner wissenschaftlichen Tätigkeit gewidmet).

In einer meiner früheren Arbeiten[1]) habe ich die Existenzfrage von gewissen relativ Abelschen Zahlkörper auf das Existenzproblem der l-primären Primideale $\mathfrak{p}$ innerhalb eines gegebenen normalen algebraischen Zahlkörpers k zurückgeführt derart, dass das Potenzrestsymbol

$$(1) \qquad \left\{ \frac{\Pi_2 \cdot \Pi_3 \ldots \Pi_x}{\mathfrak{p}} \right\}$$

einen vorgeschriebenen Wert hat, wobei $\mathfrak{p}_1 = \mathfrak{p}, \mathfrak{p}_2, \ldots, \mathfrak{p}_x$ die mit $\mathfrak{p}$ konjugierten Primideale und $\Pi_i = \mathfrak{p}_i \mathfrak{q}_i^l$ $(i = 1, 2, \ldots, k)$ die miteinander konjugierten ganzen Zahlen von k $[(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_x, \mathfrak{q}_i) = 1]$ bedeuten. Der Wert des Symbols (1) hängt wegen der Primärität von $\mathfrak{p}$ nicht von der Wahl der $\mathfrak{q}_i$ ab.

Diese Aufgabe schien mir mit Hilfe der heutigen Methoden der analytischen Zahlentheorie unauflösbar, da ich sie nicht auf die Frobeniussche Aufgabe über die Existenz von zu verschiedenen Substitutionen der Gruppe eines Zahlkörpers gehörenden Primidealen zurückführen

[1]) N. Tschebotarŏw, Untersuchungen über relativ Abelsche Zahlkörper, Journ. für Math. **167** (1932), S. 98 — 121.