Vojtěch Jarník

Neuer Beweis eines Khintchineschen Satzes

Časopis pro pěstování matematiky a fysiky, Vol. 67 (1938), No. 2, 109--113

Persistent URL: http://dml.cz/dmlcz/109458

Neuer Beweis eines Khintchineschen Satzes.

Vojtěch Jarník, Praha.

(Eingegangen am 28. November 1936.)

Griechische Buchstaben bedeuten reelle Zahlen; kleine lateinische Buchstaben bedeuten ganze Zahlen, eventuell auch Restklassen modulo einer natürlichen Zahl. Ein geordnetes System von n (gleichen oder ungleichen) Restklassen $a_1, \ldots, a_n$ modulo q ($n > 0$, $q > 0$) heiße ein (n, q)-System; Bezeichnung: $\{a_1, \ldots, a_n\}$. Man setze noch

$$h\{a_1, \ldots, a_n\} + k\{b_1, \ldots, b_n\} = \{ha_1 + kb_1, \ldots, ha_n + kb_n\}$$

und analog für mehrere Summanden.

Hilfssatz 1. *Zu jedem $\alpha > 0$ gibt es zwei ganze Zahlen $\beta_1 = \beta_1(\alpha) > 0$, $\beta_2 = \beta_2(\alpha) > 0$ mit folgenden Eigenschaften: Ist $q > 0$, sind $a_1, \ldots, a_l$ 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 ein System von höchstens β_1 Zahlen $\varepsilon_i a_{k_i}$ mit*

$$\varepsilon_i = \pm 1, \quad \sum_i \varepsilon_i = 0, \quad 1 \leqq k_i \leqq l, \quad \sum_i \varepsilon_i a_{k_i} \equiv br \pmod q.$$

Beweis: bekannt.[1])

Hilfssatz 2. *Zu jedem $\alpha > 0$, $n > 0$ gibt es zwei natürliche Zahlen $L_1 = L_1(\alpha, n)$, $L_2 = L_2(\alpha, n)$ mit folgenden Eigenschaften: Ist $q > 0$, $l \geqq \alpha q^n$ und ist*

$\mathfrak{A}$: $\quad A_1, A_2, \ldots, A_l \quad (A_i = \{a_{1i}, \ldots, a_{ni}\})$

eine Menge von l verschiedenen (n, q)-Systemen, so gibt es zu jedem (n, q)-System B eine Summe von höchstens L_1 (n, q)-Systemen $\varepsilon_i A_{k_i}$ mit

[1]) Hilfssatz 1. ist mit dem Hilfssatz 2. der Note von P. Erdös u. V. Jarník, Eine Bemerkung über lineare Kongruenzen (Acta arithmetica 2 (1938), S. 214—220) identisch; nur wurde dort nicht betont, daß $\Sigma\varepsilon_i = 0$ gefordert werden darf. Dies folgt aber daraus, daß der dortige Beweis nur mit den Differenzen $a_\varrho - a_\lambda$ arbeitet.

$$\varepsilon_i = \pm 1,\ \sum_i \varepsilon_i = 0,\ 1 \leqq k_i \leqq l,\ \sum_i \varepsilon_i A_{k_i} = L_2 B.$$

Beweis. Für $n = 1$ folgt Hfs. 2 aus Hfs. 1 mit $L_2 = \beta_2!$, $L_1 = \beta_1$. Es sei also $n > 1$ und Hfs. 2 sei bis $n - 1$ wahr. Für jedes a sei $\mathfrak{M}_a$ die Menge aller A_i mit $a_{ni} = a$; s_a sei die Anzahl der Elemente von $\mathfrak{M}_a$; $\mathfrak{P}$ sei die Menge aller a mit $1 \leqq a \leqq q$, $s_a > 0$. Wegen $0 \leqq s_a \leqq q^{n-1}$, $s_1 + \ldots + s_q = l \geqq \alpha q^n$ gibt es erstens ein a' mit $s_{a'} \geqq \alpha q^{n-1}$ und zweitens ist die Anzahl der Elemente von $\mathfrak{P}$ mindestens gleich αq.

Es sei $B = \{b_1, \ldots, b_n\}$ ein (n, q)-System. Nach Hfs. 2 mit $n = 1$ gibt es höchstens $L_1(\alpha, 1)$ Zahlen $\varepsilon_i c_i$ mit

$$\varepsilon_i = \pm 1,\ \sum_i \varepsilon_i = 0,\ c_i \in \mathfrak{P},^{2})\ \sum_i \varepsilon_i c_i \equiv L_2(\alpha, 1)\, b_n \pmod q.$$

Für geeignete $A_{g_i} \in \mathfrak{A}$ und geeignete $d_1, \ldots, d_{n-1}$ ist dann

$$\sum_i \varepsilon_i A_{g_i} = \{d_1, \ldots, d_{n-1}, b_n \,.\, L_2(\alpha, 1)\} = D.$$

Das n-te Element des (n, q)-Systems $E = L_2(\alpha, 1) \,.\, B - D$ ist also gleich Null. Nach Hfs. 2 mit $n - 1$ statt n gibt es also höchstens $L_1(\alpha, n - 1)$ (n, q)-Systeme $\eta_j A_{h_j}$ mit

$$\eta_j = \pm 1,\ \sum_j \eta_j = 0,\ A_{h_j} \in \mathfrak{M}_{a'},\ \sum_j \eta_j A_{h_j} = L_2(\alpha, n - 1) \,.\, E$$

(das letzte Element des (n, q)-Systems $\sum \eta_j A_{h_j}$ ist nämlich gleich $a' \sum \eta_j = 0$). Dann ist aber

$$L_2(\alpha, n - 1) \sum_i \varepsilon_i A_{g_i} + \sum_j \eta_j A_{h_j} = L_2(\alpha, n - 1)\, L_2(\alpha, 1) \,.\, B,$$

w. z. b. w.

Herr Khintchine hat folgenden schönen Satz bewiesen[3]):

Hauptsatz. *Zu jedem $n > 0$ und jedem $\gamma > 0$ gibt es ein $\Gamma = \Gamma(\gamma, n) > 0$ mit folgender Eigenschaft: Es seien $\Theta_1, \ldots, \Theta_n$, $\alpha_1, \ldots, \alpha_n$ gegeben; die Ungleichungen*

$$| q\Theta_i - p_i | < \frac{1}{t'} \quad (i = 1, \ldots, n), \quad 0 < q \leqq \gamma\, t'^n \qquad (1)$$

seien für **kein** *$t' > 1$ lösbar* (in ganzen Zahlen $q, p_1, \ldots, p_n$); *dann sind die Ungleichungen*

$$| x\Theta_i - y_i - \alpha_i | < \frac{1}{t} \quad (i = 1, \ldots, n), \ 0 < x \leqq \Gamma t^n \qquad (2)$$

für **jedes** *$t > 0$ lösbar* (in ganzen Zahlen $x, y_1, \ldots, y_n$).[4])

[2]) Lies: c_i ist ein Element der Menge $\mathfrak{P}$.

[3]) A. Khintchine, Ein Satz über lineare diophantische Approximationen, Math. Annalen **113** (1936), S. 398—415.

[4]) Die Umkehrung dieses Satzes ist auch richtig und leicht zu beweisen; vgl. l. c.[3]), S. 399—401.

Ich will für diesen Satz im Falle $n > 1$[5]) einen neuen, auf dem Hfs. 2 beruhenden Beweis geben (wobei aber mehrere Betrachtungen des Herrn Khintchine auch in meinem Beweis vorkommen).[6])

Beweis. Man setze $M_1 = L_1(2^{-n}\gamma, n-1)$, $M_2 = L_2(2^{-n}\gamma, n-1)$, $M_3 = M_2\gamma^{-\frac{n-1}{n}} + \frac{1}{2}M_1\gamma^{\frac{1}{n}}$, $\Gamma = ((M_3+1)\gamma^{-\frac{1}{n}} + 2)^n$, sodaß M_1, M_2 natürliche Zahlen sind.

Es sei $t > 0$; dann setze man $t' = \left[(M_3+1)\gamma^{-\frac{1}{n}}t\right] + 1$. Mit $q, p_1, \ldots, p_n$ bezeichne man dasjenige System mit *möglichst kleinem* $q > 0$, für welches die Ungleichungen

$$|q\Theta_i - p_i| < \frac{1}{t'} \quad (i = 1, \ldots, n)$$

gelten; also ist $(q, p_1, \ldots, p_n) = 1$, $\gamma t'^n < q \leqq t'^n$, also $\gamma < 1$, $1 \leqq t < t' < \Gamma^{\frac{1}{n}}t$. Man setze $d_i = (q, p_i)$, $q = d_iq'_i$, $p_i = d_ip'_i$ und man bestimme noch b_i so, daß $p'_ib_i \equiv 1 \pmod{q'_i}$, $(b_i, d_i) = 1$ $(i = 1, \ldots, n)$. (Das geht: denn es sei $d_i = d'_id''_i$, wo in d'_i nur die Primzahlen $p \mid q'_i$, in d''_i nur die Primzahlen $p \nmid q'_i$ aufgehen; dann kann man b_i mit $p'_ib_i \equiv 1 \pmod{q'_i}$, $b_i \equiv 1 \pmod{d''_i}$ finden, und es ist $(b_i, d'_i) = (b_i, d''_i) = 1$.)

Behauptung I. *Betrachtet man alle Zahlensysteme* $u_1, \ldots, u_n$ *mit*

$$u_i = j_iq'_i + z_i,\ 0 \leqq j_i < d_i,\ 0 \leqq z_i \leqq \tfrac{1}{2}\gamma^{\frac{1}{n}}\frac{q^{\frac{n-1}{n}}}{d_i} \quad (i = 1, \ldots, n)^7), \quad (3)$$

so sind die $(n-1, q)$*-Systeme*

$$\{u_1b_1 - u_2b_2, \ldots, u_1b_1 - u_nb_n\} \quad (4)$$

paarweise verschieden (*ihre Anzahl ist größer als* $2^{-n}\gamma q^{n-1}$).

Beweis: Sonst könnte man durch Subtraktion zweier Systeme (3) ein System $v_1, \ldots, v_n$ mit $v_1^2 + \ldots + v_n^2 > 0$ und mit

$$v_1b_1 - v_ib_i \equiv 0 \pmod{q},\ v_i = k_iq_i' + y_i,\ |k_i| < d_i,\ |y_i| \leqq \tfrac{1}{2}\gamma^{\frac{1}{n}}\frac{q^{\frac{n-1}{n}}}{d_i}$$

$$(i = 1, \ldots, n)$$

---

[5]) Der Fall $n = 1$ ist leicht und längst bekannt.

[6]) (20. XII. 1936.) Herr L. J. Mordell hat zwar einen noch kürzeren Beweis dieses Satzes gefunden, welcher den Minkowskischen Linearformensatz benutzt. Ich publiziere trotzdem meinen Beweis, da er auf einer ganz anderen Grundlage beruht.

[7]) Es ist $\frac{1}{2}\gamma^{\frac{1}{n}}q^{\frac{n-1}{n}}d_i^{-1} < qd_i^{-1} = q'_i$; also sind die betrachteten Systeme $u_1, \ldots, u_n$ paarweise verschieden.

finden. Es gäbe also ein g mit

$$|g| \leqq \tfrac{1}{2}q < q, \quad v_i b_i \equiv g \pmod q \quad (i = 1, \ldots, n),$$

also wäre (mit geeigneten m_i)

$$gp'_i \equiv b_i p'_i\,(k_i q'_i + y_i) \equiv y_i \pmod{q'_i}, \quad gp'_i - m_i q'_i = y_i,$$

$$\left| g\frac{p_i}{q} - m_i \right| = \frac{d_i}{q}\,|\,gp'_i - m_i q'_i\,| \leqq \tfrac{1}{2}\gamma^{\frac{1}{n}} q^{-\frac{1}{n}} < \frac{1}{2t'},$$

$$|\,g\Theta_i - m_i\,| \leqq |\,g\,|\left|\Theta_i - \frac{p_i}{q}\right| + \left|g\frac{p_i}{q} - m_i\right| < \frac{|\,g\,|}{qt'} + \frac{1}{2t'} \leqq \frac{1}{t'},$$

also $g = 0$ (nach der Definition von q), also $v_i b_i \equiv 0 \pmod q$, $y_i b_i \equiv 0 \pmod{q'_i}$, $y_i \equiv 0 \pmod{q'_i}$, aber $|\,y_i\,| < q'_i$ (vgl. die Fußnote[7]), also $y_i = 0$, also $b_i k_i q'_i \equiv 0 \pmod q$, $b_i k_i \equiv 0 \pmod{d_i}$, $k_i \equiv 0 \pmod{d_i}$, aber $|\,k_i\,| < d_i$, also $k_i = 0$, also $v_i = 0$ — Widerspruch.

Behauptung II. $d_i \leqq \gamma^{-\frac{n-1}{n}} q^{\frac{n-1}{n}} \quad (i = 1, \ldots, n)$.

Beweis[8]**:** Sonst wäre

$$t'^{n-1} < \gamma^{-\frac{n-1}{n}} q^{\frac{n-1}{n}} < d_i \tag{5}$$

für ein i; man wähle (Schubfachschluß) ein k und $n-1$ Zahlen m ($j \neq i$, $1 \leqq j \leqq n$) mit

$$1 \leqq k \leqq t'^{n-1}, \quad |\,kq'_i\Theta_j - m_j\,| < \frac{1}{t'} \tag{6}$$

(für $j \neq i$); nach (5) wäre aber mit $m_i = kp'_i$

$$|\,kq'_i\Theta_i - m_i\,| = k\,|\,q'_i\Theta_i - p'_i\,| < \frac{k}{d_i t'} \leqq \frac{t'^{n-2}}{d_i} < \frac{1}{t'},$$

also wäre (6) auch für $j = i$ wahr, was wegen $0 < kq'_i \leqq t'^{n-1}q'_i < d_i q'_i = q$ der Definition von q widerspricht.

Schluss des Beweises (für $n > 1$). Man bestimme nacheinander s_i, r_i, h_i $(i = 1, \ldots, n)$, sodaß

$$|\,q'_i\alpha_i - M_2 s_i\,| < M_2, \quad p'_i r_i \equiv s_i \pmod{q'_i}, \quad M_2(r_i - r_1) = h_i$$

(also $h_1 = 0$). Wendet man nun Hfs. 2 (mit $n-1$ statt n und mit $\alpha = 2^{-n}\gamma$) an, wobei man für $\mathfrak{A}$ die Menge der Systeme (4) nimmt, so ergibt sich die Existenz von $2n$ ganzen Zahlen X_i, Y_i mit

$$X_1 b_1 - X_i b_i \equiv h_i \pmod q, \quad X_i = j_i q'_i + Y_i, \quad |\,Y_i\,| \leqq \tfrac{1}{2}M_1\gamma^{\frac{1}{n}} q^{\frac{n-1}{n}} d_i^{-1}$$
$$(i = 1, \ldots, n).$$

Es gibt also ein x mit $(i = 1, \ldots, n)$

[8]) Fast wörtlich nach Khintchine, l. c.[3]), Hilfssatz 5.

$$0 < x \leqq q,\ x \equiv X_i b_i + M_2 r_i \pmod q,$$

$xp'_i \equiv p'_i (X_i b_i + M_2 r_i) \equiv X_i + M_2 s_i \equiv Y_i + M_2 s_i \pmod{q'_i}$, also $| xp'_i - y_i q'_i - M_2 s_i | = | Y_i |$ mit geeigneten y_i, also (Behauptung II)

$$| xp_i - y_i q - \alpha_i q | = d_i | xp'_i - y_i q'_i - \alpha_i q'_i | <$$

$$< d_i (\tfrac{1}{2} M_1 \gamma^{\frac{1}{n}} q^{\frac{n-1}{n}} d_i^{-1} + M_2) \leqq M_3 q^{\frac{n-1}{n}} < M_3 q \gamma^{-\frac{1}{n}} t'^{-1},$$

also wegen $0 < x \leqq q$)

$$| x\Theta_i - y_i - \alpha_i | \leqq x \left| \Theta_i - \frac{p_i}{q} \right| + \frac{1}{q} \left| xp_i - y_i q - \alpha_i q \right| <$$

$$< \frac{q}{qt'} + M_3 \frac{1}{\gamma^{\frac{1}{n}} t'} < (M_3 + 1) \gamma^{-\frac{1}{n}} \cdot \frac{1}{t'} < \frac{1}{t},$$

$$0 < x \leqq q \leqq t'^n < \Gamma t^n.\ ^9)$$

*

Nový důkaz jedné Chinčinovy věty.

(Obsah předešlého článku.)

Jde o důkaz této věty: ke každému $\gamma > 0$ a každému celému $n > 0$ existuje číslo $\Gamma = \Gamma(\gamma, n) > 0$ s touto vlastností: Buďte $\Theta_1, \ldots, \Theta_n, \alpha_1, \ldots, \alpha_n$ reálná čísla; nerovnosti

$$| q\Theta_i - p_i | < \frac{1}{t'} \quad (i = 1, \ldots, n),\ 0 < q \leqq \gamma t'^n$$

nechť nemají pro *žádné* celé $t' > 1$ řešení (v celých číslech $q, p_1, \ldots, p_n$). Potom nerovnosti

$$| x\Theta_i - y_i - \alpha_i | < \frac{1}{t} \quad (i = 1, \ldots, n),\ 0 < x \leqq \Gamma t^n$$

mají pro *každé* celé $t > 0$ řešení (v celých číslech $x, y_1, \ldots, y_n$).

---

[9]) Anmerkung bei der Korrektur: Der unter [6]) erwähnte Beweis von Mordell ist inzwischen erschienen; vgl. L. J. Mordell, A theorem of Khintchine on linear diophantine approximation, Journ. London Math. Soc. 12 (1937), 166—167.