ACTA ARITHMETICA
XXVII (1975)

# Zum großen Sieb von Linnik

von

EDMUND HLAWKA (Wien)

*Dem Andenken von Yu.V.Linnik gewidmet*

Das große Sieb, das von Linnik 1941 erfunden wurde, hat der analytischen Zahlentheorie bedeutende Fortschritte gebracht, wie allgemein bekannt ist. Darüber berichtet z.B. das ausgezeichnete Buch von L. Montgomery [8]. Während das eindimensionale Sieb schon viele Anwendungen fand, hat das mehrdimensionale Sieb (vgl. z.B. M. Huxley [6], E. Hlawka [4]) nicht diese Aufmerksamkeit gefunden, wohl deshalb, da hier zunächst keine schönen Resultate erzielt wurden. Das hat sich nun dadurch geändert, daß Gallagher [3] eine bedeutende Anwendung auf ein Problem von van der Waerden über Gleichungen mit Affekt gefunden hat. Dies hat mich bewogen, eine weitere Verallgemeinerung des großen Siebes aufzustellen, in dem, geometrisch gesprochen, das Würfelgitter durch ein allgemeines Gitter ersetzt wird und eine beliebige konvexe Distanzfunktion zu Grunde gelegt wird. Der Minkowskische Fundamentalsatz erscheint hier als Spezialfall. Damit ist ein Zusammenhang zur Geometrie der Zahlen hergestellt, ein Zusammenhang der auch für das letztere Gebiet fruchtbar sein könnte. Damit ist hier allerdings nur ein Beginn gemacht. Ein weiterer Fortschritt wird sick sicker ergeben, wenn man das interessante maximale Sieb von S. Uchiyama [11] ins Spiel bringt. Zu dieser vorliegenden Arbeit wurde ich angeregt durch eine Bemerkung im Buch von Montgomery [8].

1. Es sei $f$ eine Distanzfunktion im $R^n$ mit $f(x+y) \leqslant f(x)+f(y)$ und $f(tx) = |t|f(x)$; also ist $f \leqslant K$ stets ein konvexer Körper mit 0 als Mittelpunkt und Volumen $J(f)K^n$. Dabei ist $J$ das Volumen des Eichkörpers $\leqslant 1$. Es sei $H$ die polare Distanzfunktion zu $f$, definiert durch

$$\sup_y |\langle xy\rangle|/f(y).$$

($\langle xy\rangle$ Skalarprodukt von $x$ und $y$.) Es sei weiter $\Gamma$ ein Gitter mit Determinante $d(\Gamma)$, $\Gamma^*$ das reziproke Gitter zu $\Gamma$. Ferner sind gegeben $s$ Punkte

$x_1, \ldots, x_s$ im $R^n$ und es sei für ein $\delta > 0$ für alle $\gamma \in \Gamma$ und alle Paare $x_i, x_j$ mit $x_i \neq x_j$

$$f(x_i - x_j - \gamma) \geqslant \delta. \tag{1}$$

Weiter seien $M_1(\Gamma, f), \ldots, M_n(\Gamma, f)$ die $n$ Minima von $f$ in bezug auf $\Gamma$, also insbesondere $M_1(\Gamma, f) = \mathrm{Min} f(\gamma)$ (erstreckt über alle $\gamma \in \Gamma$ mit $\gamma \neq 0$). Es ist bekannt, daß $\delta \leqslant \frac{1}{2}(M_1 + \ldots + M_n)$ (vgl. z.B. [7], S. 96) sein muß. Es sei $N \geqslant 0$ eine reelle Zahl und jedem Gitterpunkt $a \in \Gamma^*$ mit $H(a) \leqslant N$ eine komplexe Zahl $L(a)$ zugeordnet und

$$S(x) = \Big| \sum_{H(a) \leqslant N} L(a) e(\langle ax \rangle) \Big|^2 \qquad (e(a) = e^{2\pi i a}).$$

Dann ist für jedes $\lambda$ mit $0 < \lambda < 1$

$$\sum_{j=1}^{s} |S(x_j)|^2 \leqslant \left(\frac{2}{\eta}\right)^n \frac{d(\Gamma)}{J(f)} \Big( |L(0)|^2 + (1-\lambda)^{-2} \sum_{0 < H(a) \leqslant N} |L(a)|^2 \Big). \tag{2}$$

Dabei ist $\eta = \mathrm{Min}\big(M_1(\Gamma, f),\ \delta,\ \lambda(\pi N)^{-1}\big)$.

Genau genommen ist (2) keine direkte Verallgemeinerung von [4], denn in diesem Fall ist

$$f(x) = \mathrm{Max}(|x_1|, \ldots, |x_n|), \qquad H(y) = \prod_{j=1}^{n} |y_j|,$$

aber es ist $H$ eine zu $f$ äquivalente Metrik.

In (2) ist der Minkowskische Fundamentalsatz enthalten und zwar für $s = 1, N = x_1 = 0, L(0) = 1$, denn dann erhalten wir $J M_1^n \leqslant 2^n d(\Gamma)$.

Wir wollen nun (2) beweisen und zwar für das Einheitsgitter $\Gamma_0$, also die Menge der Punkte $g$ mit ganzzahligen Koordinaten. Es ist $\Gamma_0^* = \Gamma_0$ und $d(\Gamma_0) = 1$. Der allgemeine Fall läßt sich darauf zurückführen. Ist $\Gamma$ ein beliebiges Gitter, dann gibt es eine Matrix $A$ mit $\mathrm{Det} A = d(\Gamma)$, so daß jedes $\gamma \in \Gamma$ die Gestalt $Ag$ hat und jeder Punkt $a$ aus $\Gamma^*$ die Gestalt $Bl$ ($l \in \Gamma_0$), wo $B = (A^{-1})^*$ ist. Statt $f$ betrachten wir $\bar{f}$: $\bar{f}(x) = f(Ax)$ mit der polaren Distanzfunktion $\bar{H}$: $\bar{H}(y) = H(By)$. Es ist $J(\bar{f}) d(\Gamma) = J(f)$. Weiter definieren wir für alle $l$ mit $\bar{H}(l) \leqslant N$: $\bar{L}(l) = L(Bl)$ und $\bar{x}_j = A^{-1} x_j$ ($j = 1, \ldots, s$). Wenden wir (2) auf $\Gamma_0, \bar{f}, \bar{x}_j$ an, so erhalten wir (2) im allgemeinen Fall. (Es ist ja $M_1(\Gamma, f) = M_1(\Gamma_0, \bar{f})$.)

Es sei also $\Gamma = \Gamma_0$. Wir bezeichnen mit $\bar{K} = K(\eta)$ den konvexen Körper $f(x) < \eta$ und es sei $\chi(.,\eta)$ (kurz $\chi$) seine Indikatorfunktion. Wir gehen nun wie beim Siegelschen Beweis [9] des Minkowskischen Fundamentalsatzes vor. Es sei $\psi(x) = \sum_g \chi(x+g)$. Es ist für alle $g \in \Gamma_0$ $\psi(x+g) = \psi(x)$. Es sei $\sum_l c_l e(\langle lx \rangle)$ die zugehörige Fouriersche Reihe.



Es ist ($E = E^n$ der Einheitswürfel)

$$c_l = \int_E \psi(x) e(-\langle lx \rangle)\, dx = \int \chi(x) e(-\langle lx \rangle)\, dx$$

($\int$ bedeutet stets Integration über dem ganzen $R^n$). Es ist $c_0 =$ Volumen von $\bar{K} = J\eta^n$. Wir schätzen nun die $c_l$ mit $0 < H(l) \leqslant N$ nach unten ab. Es ist

$$c_l = c_0 + \int_{\bar{K}} \big(e(-\langle lx \rangle) - 1\big)\, dx.$$

Nun ist

$$|e(-\langle lx \rangle) - 1| \leqslant |\sin \pi \langle lx \rangle| \leqslant \pi |\langle lx \rangle| \leqslant \pi H(l) f(x).$$

Nun ist aber für die $x \in \bar{K}$, $H(l) f(x) < N\eta \leqslant \lambda$, also ist für $0 < H(l) \leqslant N$

$$c_l > (1-\lambda) c_0. \tag{3}$$

Jetzt gehen wir wie bei Davenport und Halberstam ([1]) vor. Es ist $S(x)$ ebenfalls eine (endliche) Fourierreihe. Es sei $T(x)$ die Fourierreihe

$$\sum_{H(l) \leqslant N} B(l) e(\langle lx \rangle) \quad \text{mit} \quad B(l) = L(l)/c_l.$$

Das geht nach (3). Es ist nun

$$\begin{aligned} S(x) &= \int_E \sum_g \chi(y+g) T(x-y)\, dy \\ &= \sum_g \int_{E+g} \chi(y) T(x-y-g)\, dy = \int_R \chi(y) T(x-y)\, dy. \end{aligned}$$

Es ist also $|S(x)|^2 \leqslant \int \chi^2(y)\, dy \int \chi^2(y) |T(x-y)|^2\, dy$ also

$$\sum_{j=1}^{s} |S(x_j)|^2 \leqslant c_0 \sum_j \int \chi(y) |T(x_j - y)|^2\, dy = c_0 \sum_j \int \chi(x_j + y) |T(-y)|^2\, dy$$

also gleich

$$c_0 \sum_j \sum_g \int_{E+g} \chi(x_j + y) |T(-y)|^2\, dy = c_0 \int_E \sum_{j,g} \chi(x_j + y - g) |T(-y)|^2\, dy.$$

Setzen wir $\sup_{y \in E} \sum_{j,g} \chi(x_j + y - g) = \varrho$, so ist also

$$\sum_{j=1}^{s} |S(x_j)|^2 \leqslant c_0 \varrho \sum_{H(l) \leqslant N} |L(l)|^2 |c_l^{-1}|^2. \tag{4}$$

Es ist $\chi(x_j + y - g)$ die Indikatorfunktion des Körpers $K(x_j, g)$: $f(x_j - g + y) < \eta$. Die Körper $K(x_j, g)$ haben keinen Punkt miteinander gemeinsam; denn wäre dies der Fall, so wäre für $x_j, x_k, g, g'$

$$f(x_j - x_k - g + g') < 2\eta \leqslant \mathrm{Min}(\delta, M_1).$$

Ist $x_j \neq x_k$, so ergibt sich ein Widerspruch zu (1) und für $x_j = x_k$ ein Widerspruch zur Definition von $M_1$. Es ist also $\varrho \leqslant 1$.

Setzt man alles ein, so folgt (2).

Wir wollen noch eine Verallgemeinerung von (2) anschließen. Die Bedingung (1) kann ja so ausgesprochen werden, daß die Körper $K(x_j, g)$: $f(x_j - g + y) < \delta/2$ für verschiedenes $x_j$, $x_l$ keinen Punkt gemeinsam haben. Es sei nun $k \geqslant 1$ eine natürliche Zahl; wir setzen statt (1) voraus, daß ein Körper $K(x_j, g)$ mit höchstens $k-1$ weiteren Körpern $K(x_l, g_l)$ Punkte gemeinsam hat. Es sei weiter $M(\Gamma, f, k)$ das sogenannte $k$-te Miminum, d.h. es gibt höchstens $k-1$ Gitterpunktpaare $\gamma \in \Gamma$ mit $\gamma \neq 0$, sodaß $f(\gamma) < M(k)$ gilt. Dann ist das vorherbetrachtete $\varrho \leqslant k$, wo jetzt $\eta = \operatorname{Min}\big(M(\Gamma, f, k), \delta, \lambda(\pi N)^{-1}\big)$ und wir erhalten

$$(5) \qquad \sum_{j=1}^{s} |S(x_j)|^2 \leqslant \left(\frac{2}{\eta}\right)^n k \frac{d(\Gamma)}{J(f)} \left(|L(0)|^2 + (1-\lambda)^{-2} \sum_{0 < H(a) \leqslant N} |L(a)|^2\right).$$

Im Spezialfall $s = 1$, $N = x_1 = 0$, $L(0) = 1$ erhält man den verallgemeinerten Minkowskischen Fundamentalsatz

$$J M^n(k) \leqslant 2^n d(\Gamma) k.$$

Wir wollen noch zwei Verschärfungen von (2) anschließen.

Die erste Verschärfung besteht darin, daß wir alle $M_1, \ldots, M_n$ ins Spiel bringen. Wir behaupten: (2) bleibt richtig, wenn wir $\eta^n$ ersetzen durch $\overline{\eta} = \operatorname{Min}_{k=0,\ldots,n} (\eta_1^{n-k}, M_1, \ldots, M_k)$ (dabei ist $M_0 = 1$), wo $\eta_1 = \operatorname{Min}\big(\delta, \lambda(\pi N)^{-1}\big)$. Es ist tatsächlich $\overline{\eta} \geqslant \operatorname{Min}(\eta_1^n, M_1^n) = \eta^n$.

Beweis. Es sei $K(\eta_1)$ der Körper $f(x) < \frac{1}{2}\eta_1$ und $\chi$ seine charakteristische Funktion. Wir nehmen nun

$$\psi(x) = 1 - \prod_g \big(1 - \chi(x-g)\big).$$

Es ist stets $\psi \leqslant 1$. Wir setzen $\int_E \psi = J(\eta_1)$. Nach H. Weyl [10] gilt nun $2^n J(\eta_1) = \eta_1^n J$ für $\eta_1 < M_1$ und $2^n J(\eta_1) \geqslant M_1 \ldots M_k \eta_1^{n-k} J$ für $M_k \leqslant \eta_1 < M_{k+1}$ für $k = 1, \ldots, n$ $(M_{n+1} = \infty)$. Es gilt für die Fourierkoeffizienten $c_l$ von $\psi$ wieder (3) und daraus folgt die Behauptung.

Wir können (2) verschärfen, wenn wir mehr über $f$ voraussetzen. Es heißt $f$ $(m, \sigma)$-konvex ($m$, $\sigma$ positive Zahlen), wenn für alle $l \geqslant 2$ und alle Punkte $\xi_1, \ldots, \xi_l$ im $R^n$ gilt: Es gibt stets zwei Punkte $\overline{\xi}_1, \overline{\xi}_2$ aus der Menge dieser $l$ Punkte, so daß

$$f^\sigma(\overline{\xi}_1 - \overline{\xi}_2) \leqslant \frac{m}{l-1} \sum_{j=1}^{l} f^\sigma(\xi_j).$$



Es ist $f$ sicher $(m, \sigma)$-konvex, wenn stets gilt

$$\sum_{j,k=1}^{l} f^\sigma(\xi_j - \xi_k) \leqslant ml \sum_{j=1}^{l} f^\sigma(\xi_j).$$

Ist $f$ z.B. $\big(\sum |x_i|^\sigma\big)^{1/\sigma}$ für $\sigma \geqslant 2$, so ist diese Bedingung mit $m = 2^{\sigma-1}$ erfüllt.

Es gilt nun (2), wenn man $(2/\eta)^n$ ersetzt durch $\frac{n+\sigma}{\sigma} m^{n/\sigma} \eta^{-n}$ wo $\eta$ wieder $\operatorname{Min}\big(M_1(\Gamma, f), \delta, \lambda(\pi N)^{-1}\big)$.

Beweis. Wir nehmen $\eta_1 = m^{-1/\sigma}\eta$ und betrachten die charakteristische Funktion $\chi$ von $K(\eta_1)$ und setzen

$$\psi(x) = \sum \big(\eta_1^\sigma - f^\sigma(x+g)\big) \chi(x+g).$$

Es gilt wieder (3), wo $c_0 = \frac{\sigma}{n+\sigma} \eta_1^{n+\sigma} J$. Dann haben wir

$$|S(x)|^2 \leqslant \int \psi(y)\, dy \int \psi(y) |T(x-y)|^2\, dy,$$

also erhalten wir (4), wo jetzt

$$\varrho = \sup_{y \in E} \sum_{j,g} \psi(x_j + y - g).$$

Es ist $\varrho \leqslant \eta_1^\sigma$; denn nehmen wir an, für ein $y$ ist die Summe $\sum_{j,g} \psi(x_j + y - g) > \eta_1^\sigma$. Es gäbe $l$ Punkte $x_j + y - g$, sagen wir $\xi_1, \ldots, \xi_l$, so daß $\psi(\xi_j) \neq 0$. Es ist also

$$\sum_{k=1}^{l} \psi(\xi_k) = \sum_{k=1}^{l} \big(\eta_1^\sigma - f^\sigma(\xi_k)\big) > \eta_1^\sigma$$

so ist also

$$(l-1)\eta_1^\sigma > \sum_{k=1}^{l} f^\sigma(\xi_k).$$

Dann ist $l \geqslant 2$ und es gibt zwei Punkte $\overline{\xi}_1, \overline{\xi}_2$ so daß $m\eta_1^\sigma = \eta^\sigma > f^\sigma(\overline{\xi}_1 - \overline{\xi}_2)$, was der Definition von $\eta$ widerspricht. Daraus folgt alles.

**2.** Wir wollen uns nun überlegen, ob die Abschätzung (2) das Richtige trifft. Dazu schätzen wir $K = \sum_{H(a) \leqslant N} 1$ nach unten ab. Es ist

$$(6) \qquad d(\Gamma^*) J K \geqslant r_n N^n$$

wo $r_n = 2^n/(n!)^2$.

Beweis. Es sei $J_1$ das Volumen von $H \leqslant 1$. Es ist bekanntlich (vgl. [7], S. 106) $2^n r_n \leqslant J J_1$. (Es ist noch mehr bekannt, aber wir begnügen uns mit dieser Abschätzung.) Es sei $k = [J_1 N^n / 2^n] d(\Gamma^*)$, dann ist $J_1 N^n$

$\geqslant 2^n k d(\Gamma^*)$, also enthält $H(x) \leqslant N$ mindestens $2k$ Gitterpunkte $a \neq 0$ von $\Gamma^*$, also ist

$$K \geqslant 2k+1 > \frac{J_1 N^n}{2^n d(\Gamma^*)}.$$

Wir beschränken uns jetzt auf Gitter $\Gamma$ mit $d(\Gamma) = 1$, dann ist also auch $d(\Gamma^*) = 1$. Es sei nun

$$\varkappa(\Gamma) = \sup_L \Big( \sum_{j=1}^{s} |S(x_j)|^2 / \sum_{H(a)\leqslant N} |L(a)|^2 \Big)$$

erstreckt über alle $L(a)$ für $H(a) \leqslant N$. Es ist also

$$\sum_j \Big| \sum_a L(a) e(\langle a x_j \rangle) \Big|^2 \leqslant \varkappa \sum_a |L(a)|^2 \tag{7}$$

für alle $L(a)$. Wir folgen nun einer Methode von P.D.T.A. Elliott [2]. Es ist die linke Seite von (6) eine positiv definite Hermitesche Form

$$\sum L(a)\bar{L}(b) c_{ab}, \qquad \text{wo} \qquad c_{ab} = \sum_j \exp(\langle a-b, x_j \rangle)$$

in den Variablen $L(a)$. Es ist $C = (c_{ab})$ eine Matrix von $K$ Zeilen und Spalten. Die Eigenwerte seien $\lambda_1 \geqslant \ldots \geqslant \lambda_K \geqslant 0$. Es ist

$$\sum L(a)\bar{L}(b) c_{ab} \leqslant \lambda_1 \sum |L(a)|^2$$

und es gilt bei passendem $L(a)$ das Gleichheitszeichen. Es ist also $\lambda_1 = \varkappa$. Nun ist

$$K\lambda_1 \geqslant \lambda_1 + \ldots + \lambda_K = \text{Spur}\, C = \sum_{H(a)\leqslant N} c_{aa} = Ks,$$

also $\varkappa \geqslant s$.

Wir betrachten nun mit P.D.T.A. Elliott die duale Ungleichung

$$\sum_{H(a)\leqslant N} \Big| \sum_{j=1}^{s} \varrho_j e(\langle a x_j \rangle) \Big|^2 \leqslant \varkappa_1 \sum_{j=1}^{s} |\varrho_j|^2. \tag{8}$$

Es ist die linke Seite von (7) eine hermitesche Form $\sum \varrho_j \bar{\varrho}_k u_{jk}$ mit $u_{jk} = \sum_{H(a)\leqslant N} e(\langle a, x_j - x_k \rangle)$. Es ist nun nach Elliott $\varkappa_1 = \varkappa$.

Für die Eigenwerte $\mu_1 \geqslant \mu_2 \ldots \geqslant \mu_s$ von $U = (u_{jk})$ gilt wieder $s\mu_1 \geqslant \text{Spur}\, U = Ks$, also haben wir $\varkappa \geqslant K$, also zusammenfassend $\varkappa \geqslant \text{Max}\,(s, K)$, also ist nach (6)

$$\varkappa \geqslant N^n r_n / J. \tag{9}$$



Wir haben bisher die $x_1, \ldots, x_s$ festgehalten. Ist $E(\Gamma)$ ein Fundamentalparallelepiped von $\Gamma$, so können wir stets annehmen, daß die $x_j$ in $E(\Gamma)$ liegen. Da das Volumen von $E(\Gamma)$ gleich $d(\Gamma) = 1$ ist, so folgt aus (1), da die Körper $f(x_j - y) < \delta/2$ keinen Punkt gemeinsam haben, daß $s(\delta/2)^n J \leqslant 1$, also $s \leqslant 2^n / J\delta^n$ ist. Wir führen nun folgende Bezeichnung ein (vgl. [5]): Wir nennen eine endliche Menge $P$ in $E(\Gamma)$ eine $(f, \delta)$-Menge, wenn für alle $p_1, p_2$ aus $P$ gilt: $\operatorname{Min}_\gamma f(p_1 - p_2 - \gamma) \geqslant \delta$. Es bilden die $(x_1 \ldots x_s)$ eine $(f, \delta)$-Menge. Bedeutet $|P|$ die Anzahl der Elemente in $P$, so sei nun $\bar{s} = \text{Max}\,|P|$ erstreckt über alle $(f, \delta)$-Mengen in $E(\Gamma)$. Es gilt stets $J\delta^n \bar{s} \geqslant JM^n$, wo $M(f) = \sup M_1(\Gamma, f)$ erstreckt über alle $\Gamma$ mit $d(\Gamma) = 1$. Es gibt eine Menge $P_0$ mit $|P_0| = \bar{s}$. Es ist also $\bar{\varkappa} = \sup_P \varkappa(P)$, wo wir jetzt zum Ausdruck bringen, daß $\varkappa$ von der $(f, \delta)$-Menge abhängt, sicher $\geqslant \bar{s}$, also haben wir

$$\bar{\varkappa} \geqslant \text{Max}\,(\bar{s}, K) = \frac{1}{J} \text{Max}\left( \frac{JM^n}{\delta^n}, r_n N^n \right). \tag{10}$$

Nun hängt $\bar{\varkappa}$ noch von $\Gamma$ ab. Nun gibt es stets maximale Gitter $\bar{\Gamma}$ mit $d(\bar{\Gamma}) = 1$, so daß $M_1(\bar{\Gamma}) = \ldots = M_n(\bar{\Gamma}) = M(f)$. Es ist $JM^n(f) \geqslant 2$ (vgl. [7], S. 148). Nach W. Schmidt gilt für großes $n$ sogar $JM^n \geqslant n \log\sqrt{2} - -\beta$ mit einer Konstanten $\beta$ (vgl. [7], S. 160). Da $\delta \leqslant \frac{1}{2} n M_n = \frac{1}{2} n M_1$ für $\Gamma = \bar{\Gamma}$, so ist

$$J\bar{\varkappa}(\bar{\Gamma}) \geqslant \mu^n \tag{11}$$

wo $\mu = \text{Max}\big(\delta^{-1}, N, (nM_1)^{-1}\big)$.

Bemerkung. Analoge Abschätzungen nach unten können auch im Fall (5) gegeben werden.

**3.** Wir wollen im Anschluß an Davenport und Halberstam die Bedingung (1) ersetzen durch

$$\inf_\gamma f(x_j - x_k - \gamma) \geqslant \delta(x_j) > 0 \tag{12}$$

für $j = 1, \ldots, s$ und alle $x_k \neq x_j$. Dann gilt mit den gleichen Bezeichnungen wie bei (2), wo $\delta(x_j) = \delta(j)$ gesetzt ist

$$\sum_{j=1}^{s} \text{Min}\big(1, (N\delta(j))^n\big) |S(x_j)|^2 \leqslant (2/J\eta)^n a d(\Gamma) \Sigma \tag{13}$$

wo

$$\Sigma = |L(0)|^2 + (1-\lambda)^{-2} \sum_{0 < H(a) \leqslant N} |L(a)|^2$$

und

$$\eta = \text{Min}\big(M_1(\Gamma, f), \lambda(\pi N)^{-1}\big), \qquad a(\lambda) = 2^n(2^n - 1)\left(\frac{\lambda}{\pi}\right)^n + 1.$$

Beweis. Wir können uns wieder auf das Einheitsgitter $\Gamma_0$ beschränken und schließen uns an den Beweis von (2) an. Statt (4) gilt jetzt

$$\sum_{j=1}^{s} \mathrm{Min}\left(1, \left(N\delta(j)\right)^2\right)|S(x_j)|^2 \leqslant c_0\varrho_1 \sum_{H(l)\leqslant N} |L(l)c_l^{-1}|^2$$

wo

$$\varrho_1 = \sup_{y\in E} \sum_{i,g} \mathrm{Min}\left(1, \left(N\delta(j)\right)^n\right)\chi(x_j+y-g).$$

Wir nehmen jetzt an, daß unter den $s$ Punkten $x_1, \ldots, x_s$ für $m$ Punkte $x_1', \ldots, x_m'$ und die zugehörigen $g_j'$ gilt $\chi(x_j'+y-g_j') = 1$. Wir können o.B.d.A. $g_j' = 0$ $(j = 1, \ldots, m)$ annehmen. Für $m = 1$ ist $\sum_{i,g} = 1$. Es sei also $m > 1$. Weiters können wir annehmen, daß für die $\delta(x_j') = \delta_j$ gilt $\delta_1 \leqslant \delta_2 \leqslant \ldots \leqslant \delta_m$. Aus $f(y+x_r') < \eta$, $f(y+x_m) < \eta$ folgt $\delta_m \leqslant f(x_r'-x_m') < 2\eta$. Weiter ist für alle $z$ mit $f(z-x_k') < \frac{1}{2}\delta_k$ stets

$$f(z-y) \leqslant f(y-x_k') + f(x_k'-z) < \eta + \tfrac{1}{2}\delta_k,$$

also liegen alle Körper $K(x_k') : f(z-x_k') \leqslant \frac{1}{2}\delta_k$ in dem Körper $f(z-y) < \eta + \frac{1}{2}\delta_m$. Weiter sind die $K(x_k')$ paarweise elementfremd, denn aus $K(x_r') \cap K(x_s') \neq \emptyset$ für $r \neq s$ (o.B.d.A. $\delta_r \leqslant \delta_s$) folgt

$$\delta_s \leqslant f(x_s'-x_r') < \tfrac{1}{2}(\delta_r+\delta_s) \leqslant \delta_s.$$

Es ist also $2^{-n}J\sum_{j=1}^{m}\delta_j^n \leqslant J(\eta+\frac{1}{2}\delta_m)^n$, also $\sum_{j=1}^{m-1}\delta_j^n \leqslant (2\eta+\delta_m)^n - \delta_m^n$ also $\varrho_1 \leqslant \sum_{j=1}^{m-1} N^n\delta_j^n + 1 \leqslant 2^n(2^n-1)(N\eta)^n + 1$. Damit ist (13) bewiesen.

4. Es sei wieder ein Gitter $\Gamma$ gegeben. Es sei $\Gamma_1$ Teilgitter von $\Gamma^*$ mit $d(\Gamma_1) = gd(\Gamma^*)$. Es seien $h_1, \ldots, h_g$ die Restklassen von $\Gamma^* \bmod \Gamma_1$. Es sei $\Gamma_1^*$ das polare Gitter von $\Gamma_1$. Es ist $\Gamma_1^*$ Obergitter von $\Gamma$ mit $d(\Gamma) = gd(\Gamma_1^*)$ und die Restklassen von $\Gamma_1^*$ mod $\Gamma$ seien $\beta_1, \ldots, \beta_g$. Es ist bekanntlich $\sum_{\beta} e(\langle h\beta\rangle) = g$, wenn $h \equiv 0 \pmod{\Gamma}$ und 0 sonst, ebenso $\sum_{h} e(\langle h\beta\rangle) = g$, wenn $\beta \equiv 0 \pmod{\Gamma_1^*}$ und sonst 0.

Dann ist für beliebige komplexe Zahlen $L(a)$ für $a \in \Gamma^*$ (nur endlich viele $L(a) \neq 0$)

$$\sum_{\beta}^{*}\left|\sum_{a} L(a)e\langle\beta a\rangle\right|^2 = g\sum_{h}\left|\sum_{a\equiv h(\bmod \Gamma_1)} - \hat{L}\right|^2. \tag{14}$$

Dabei bedeute $\hat{L} = \frac{1}{g}\sum_{a} L(a)$ und $\Sigma^*$ bedeute, daß nur über die $\beta \not\equiv 0 \pmod{\Gamma_1^*}$ summiert wird.



Der Beweis verläuft wie im klassischen Fall. O.B.d.A. sei $\hat{L} = 0$. Dann kann auf der linken Seite die Summation über alle $\beta$ erstreckt werden und die Summe ist gleich

$$\sum_{\beta}\sum_{a}\sum_{b} L(a)\bar{L}(b)e(\langle\beta, a-b\rangle) = g\sum_{a\equiv b(\bmod \Gamma_1)} L(a)\bar{L}(b)$$
$$= g\sum_{h \bmod \Gamma_1}\left|\sum_{a\equiv h(\bmod \Gamma_1)} L(a)\right|^2.$$

Es sei nun statt $\Gamma_1$ eine Folge von Teilgittern $\Gamma_1, \ldots, \Gamma_K$ von $\Gamma^*$ gegeben und es sei $X$ so beschaffen, daß für die zugehörigen Indizes $g_j \leqslant X$ gilt. Die polaren Gitter seien $\Gamma_1^*, \ldots, \Gamma_K^*$ und es werde nun die Voraussetzung gemacht, daß kein $\beta_{j,r} \not\equiv 0 (\bmod \Gamma)$ für $r = 1, \ldots, K$ einem $\beta_{l,s} \not\equiv 0 \pmod{\Gamma}$ kongruent sei mod $\Gamma$ wenn $r \neq s$. Es ist dann für alle $\gamma \in \Gamma$ stets $f(\beta_{j,r}-\beta_{l,s}-\gamma) \geqslant M_1(\Gamma, f)/X^2$, wenn $\beta_{j,r} \neq \beta_{l,s}$. Ist nämlich $r = s$, dann ist $g_r(\beta_{j,r}-\beta_{l,r}-\gamma) \in \Gamma$, also $f\left(g_r(\beta_{j,r}-\beta_{l,r}-\gamma)\right) \geqslant M_1$, also

$$f(\beta_{j,r}-\beta_{l,r}-\gamma) \geqslant \frac{M_1}{g_r} \geqslant \frac{M_1}{X}.$$

Ist $r \neq s$, dann sind $g_r\beta_{j,r}$, $g_s\beta_{l,s}$ in $\Gamma$, also $g_rg_s(\beta_{j,r}-\beta_{l,s}-\gamma) \in \Gamma$ also

$$f(\beta_{j,r}-\beta_{l,s}-\gamma) \geqslant \frac{M_1}{g_rg_s} \geqslant \frac{M_1}{X^2}. \tag{15}$$

Wenden wir nun (2) an, mit $\delta = M_1/X^2$, auf die Menge der $\beta_{j,r}$ $(j = 2, \ldots, g_r, r = 1, \ldots, K)$, dann erhalten wir aus (12), wo jetzt $\sum_{a}$ sich auf alle $a$ mit $H(a) \leqslant N$ erstreckt

$$\sum_{r=1}^{K} g_r \sum_{h_{j,r} \bmod \Gamma_r}\left|\sum_{a\equiv h_{j,r}(\bmod \Gamma_r)} L(a) - \frac{1}{g_r}\sum_{a} L(a)\right|^2 \leqslant \sigma(X, N)\sum_{a}|L(a)|^2. \tag{16}$$

Dabei ist

$$\sigma(X, N) = \frac{d(\Gamma)}{J}\left(\frac{2}{\eta_1}\right)^n (1-\lambda)^{-2}, \tag{17}$$

$$\eta_1 = \mathrm{Min}\left(\frac{M_1}{X^2}, \frac{\lambda}{\pi N}\right) \tag{18}$$

da ja $X \geqslant 1$. Wir nehmen nun $X(N) = \left(\frac{M_1\pi N}{\lambda}\right)^{1/2}$. Dabei sei $N$ so groß, daß $X \geqslant 1$. Dann ist $\eta_1 = \frac{\lambda}{\pi N}$; also $\sigma = \sigma_1 N^n$, wo $\sigma_1 = \frac{d}{J}\Lambda$ $(\Lambda = \left(\frac{2\pi}{\lambda}\right)^n \times$ $\times(1-\lambda)^{-2})$, also wird die linke Seite von (16)

$$\leqslant \Lambda N^n d(\Gamma)J^{-1}\sum_{a}|L(a)|^2. \tag{19}$$

Wir können nun die üblichen Anwendungen machen. Es seien $a_1, \dots, a_z$ Punkte von $\Gamma^*$ mit $H(a_l) \leqslant N$. Weiter sei $L(a) = 1$ wenn $a = a_j$ und 0 sonst. Dann ist

$$\sum_{a \equiv h_{j,r} (\mathrm{mod}\, \Gamma)} L(a) = \sum_{a_l \equiv h_{j,r} (\mathrm{mod}\, \Gamma)} 1 = Z(\Gamma_r, h_{j,r})$$

und es ist, wenn alle $g_r \leqslant X(N)$

$$\sum_{r=1}^{K} g_r \sum_{h_{j,r} \bmod \Gamma_r} \left| Z(\Gamma_r, h_{j,r}) - \frac{Z}{g_r} \right|^2 \leqslant A \frac{d(\Gamma)}{J} N^n Z. \tag{20}$$

Es sei nun jedem $\Gamma_r$ eine Zahl $f_r$ mit $f_r < g_r$ zugeordnet, so daß $\operatorname{Min}_{r \leqslant K} f_r/g_r = \tau > 0$; dann ist $Z(\Gamma_r, h_{j,r}) > 0$ für mindestens $g_r - f_r + 1$ Restklassen für alle $\Gamma_r$ mit $g_r \leqslant X(N)$, ausgenommen höchstens $C \frac{N^n}{Z\tau}$ Gitter $\Gamma_r$, wo $C = \frac{d(\Gamma)}{J} A$.

Beweis. Angenommen es sei $Z(\Gamma_r, h_{j,r}) = 0$ für mindestens $f_r$ Restklassen. Die Menge der $\Gamma_r$ mit dieser Eigenschaft sei p und $|\mathfrak{p}|$ ihre Anzahl. Dann ist

$$N^n Z \frac{d(\Gamma)}{J} A \geqslant \sum g_r f_r \frac{Z^2}{g_r^2} \geqslant \tau Z^2 |\mathfrak{p}|$$

also

$$|\mathfrak{p}| \leqslant \frac{N^n}{Z\tau} \frac{d(\Gamma)}{J} A.$$

Daraus folgt sofort die Behauptung und damit haben wir ein Siebverfahren für Gitterpunkte. Man betrachte alle Gitterpunkte $a$ von $\Gamma^*$ mit $H(a) \leqslant N$. Man streiche alle Gitterpunkte, die zu gewissen Restklassen mod $\Gamma_r$ gehören mit $g_r \leqslant X(N)$. Es sei $\bar{f}_r$ die Anzahl der Restklassen, welche in bezug auf $\Gamma_r$ gestrichen werden und es sei $\operatorname{Min} \bar{f}_r/g_r = \tau_1 > 0$.

Dies werde für $y$ Gitter $\Gamma_r$ durchgeführt. Dann ist die Anzahl der übrig gebliebenen Gitterpunkte von $\Gamma^*$ sicher

$$\leqslant \frac{AN^n}{\tau_1 y} \frac{d(\Gamma)}{J}. \tag{21}$$

Beweis. Es seien $a_1, \dots, a_z$ die übrig gebliebenen Gitterpunkte. Dann ist $Z(\Gamma_r, h_{j,r}) = 0$ für $\bar{f}_r$ Restklassen für $y$ Gitter $\Gamma_r$. Dann ist sicher $y \leqslant d(\Gamma) A N^n (JZ\tau_1)^{-1}$ und daraus folgt (21).

Eine weitere Anwendung ist folgende: Es sei jedem $\Gamma_r$ eine Funktion $f_r$, definiert auf $\Gamma^*/\Gamma_r$, zugeordnet, dann gilt

$$\left| \sum_{H(a) \leqslant N} \left( \sum_r (f_r(a \bmod \Gamma_r) - \hat{f}_r) \right) \right|^2 \leqslant \sigma(X, N) \sum_r \frac{1}{g_r} \sum_{h_{j,r}} |f_r(h_{j,r}) - \hat{f}_r|^2. \tag{22}$$



Dabei ist $\hat{f}_r = \frac{1}{g_r} \sum_j f_r(h_{j,r})$. Es stellt (22) eine Verallgemeinerung eines Satzes von Gallagher [3] dar. Ein wichtiger Spezialfall entsteht, wenn $f_r$ die Indikatorfunktion einer Menge $S_r$ auf $\Gamma_r$ ist. Ist $|S_r|$ die Anzahl der Elemente von $S_r$ so ist $\hat{f}_r = g_r^{-1} |S_r|$.

Beweis. Es sei o.B.d.A. $\hat{f}_r = 0$ für alle $r$. Wir entwickeln $f_r$ auf $\Gamma^*/\Gamma_r$ in eine Fourierreihe $\sum c(\beta_{j,r}) e(\langle h \beta_{j,r} \rangle)$ $(h \in \Gamma^*/\Gamma_r)$. Es ist $c(0) = \hat{f}_r = 0$, allgemein

$$c(\beta_{j,r}) = g_r^{-1} \sum_{h_{j,r}} f_r(h_{j,r}) e(-\langle h_{j,r} \beta_{j,r} \rangle).$$

Es ist $\sum_{\beta_{j,r}} |c(\beta_{j,r})|^2 = \widehat{|f_r|^2}$. Es sei nun $L(a) = \sum_{r=1}^{K} f_r(a \bmod \Gamma_r)$. Es ist

$$L(a) = \sum_r \sum_j{}^* c(\beta_{j,r}) e(\langle a \beta_{j,r} \rangle).$$

(Dabei bedeute $\Sigma^*$, daß sich die Summation über alle $\beta \not\equiv 0 (\mathrm{mod}\, \Gamma)$ erstreckt.) Es ist also

$$\begin{aligned} \sum_{H(a) \leqslant N} |L(a)|^2 &= \sum_{H(a) \leqslant N} \overline{L(a)} \sum_r \sum_j{}^* c(\beta_{j,r}) e(\langle a \beta_{j,r} \rangle) \\ &= \sum_r \sum_j{}^* c(\beta_{j,r}) \sum_{H(a) \leqslant N} \bar{L}(a) e(\langle a \beta_{j,r} \rangle) \\ &\leqslant \left( \sum_r \sum_j{}^* |c(\beta_{j,r})|^2 \right)^{1/2} \left( \sum_r \sum_j{}^* \left| \sum_{H(a) \leqslant N} L(a) e(-\langle a \beta_{j,r} \rangle) \right|^2 \right)^{1/2}. \end{aligned} \tag{23}$$

Aus (2) folgt mit (15) angewendet auf die zweite Klammer in (23) sofort (22).

Wir schließen noch zwei Bemerkungen an. Es gilt doch statt (15) schärfer für alle $\beta_{l,s} \neq \beta_{j,r}$

$$f(\beta_{j,r} - \beta_{l,s} - \gamma) \geqslant M_1/g_r X.$$

Wenn wir jetzt (13) mit $\delta(j) = M_1 (g_r X)^{-1}$ anwenden, so erhalten wir statt (16)

$$\sum_{r=1}^{K} g_r \operatorname{Min}\left(1, \left(\frac{M_1 N}{g_r X}\right)^n\right) \sum_h \leqslant \sigma(X, N) \sum |L(a)|^2 \tag{16'}$$

wo $\sum_h$ wieder $\sum_{h \bmod \Gamma_r} \left| \sum_{a \equiv h (\mathrm{mod}\, \Gamma_r)} \left( L(a) - \frac{1}{g_r} \sum |L(a)| \right) \right|^2$ ist und jetzt $\sigma(X, N)$ $= \frac{d(\Gamma)}{J} \left(\frac{2}{\eta_1}\right)^n \alpha(\lambda)$ ist.

Setzen wir $X_0^2 = M_1 N$ so folgt sofort aus (16') wenn wir rechts jetzt nur die Glieder mit $X_0 < g_r \leqslant X$ nehmen, daß

$$\sum_{X_0 < g_r \leqslant X} g_1^{1-n} \sum_n \leqslant c \frac{d(\Gamma)}{J} X^n \sum |L(a)|^2 \tag{24}$$

wo $c$ nur in $\lambda$ und $M_1$ abhängt. Daraus folgt wieder ein Siebverfahren wo jetzt die Anzahl der Menge $\mathfrak{p}$ Gitter $\Gamma_r$ welche ausgenommen werden zu ersetzen ist durch $\sum_{\mathfrak{p}} \frac{d}{g_r^n}$ und diese ist also $\leqslant c_1 \frac{X^n}{\tau Z}$.

Die zweite Bemerkung die wir machen wollen, ist folgende: Wir haben stets angenommen, daß die $\Gamma_1, \ldots, \Gamma_K$ die Eigenschaft haben sollen, daß kein $\beta_{j,r} \equiv \beta_{l,s} \pmod{\Gamma}$ sein soll (wenn sie nicht kongruent 0 mod $\Gamma$ sind). Wir können jetzt allgemein annehmen, daß es ein festes $k$ gibt, so daß höchstens $k-1$ solche $\beta_{j,r} \equiv \beta_{l,s} \pmod{\Gamma}$ sind. Dann können wir (5) anwenden und es ist stets $M_1$ durch $M(\Gamma, f, k)$ zu ersetzen und z.B. in (16) ist noch ein Faktor $k$ rechts hinzuzufügen.

### Literaturverzeichnis


[1] H. Davenport and H. Halberstam, *The values of a trigonometric polynomial at well spaced points*, Mathematica 13 (1966), S. 91–96.

[2] P. D. T. A. Elliott, *An inequalities of Large Sieve type*, Acta Arith. 18 (1971), S. 405–422.

[3] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, in print.

[4] E. Hlawka, *Bemerkungen zum großen Sieb von Linnik*, Österr. Akad. Wiss. Math.-Natur. Kl. S.-B. II 178 (1970), S. 13–18.

[5] — *Ausfüllung und Überdeckung konvexer Körper durch konvexe Körper*, Monatsh. Math. 53 (1949), S. 81–131.

[6] M. Huxley, *The large sieve inequality for algebraic number fields*, Mathematica 15 (1968), S. 178–187.

[7] E.G. Lekkerkerker, *Geometry of Numbers*, Amsterdam–London 1969; Groningen 1969.

[8] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Berlin–Heidelberg–New York 1971.

[9] C. L. Siegel, *Über Gitterpunkte in konvexen Körpern und ein damit zusammenhängendes Extremalproblem*, Acta Math. 65 (1935), S. 307–323.

[10] H. Weyl, *On geometry of numbers*, Proc. London Math. Soc. (2) 47 (1942), S. 268–289.

[11] S. Uchiyama, *The maximal large sieve*, Hokkaido Mathematical Journal 1 (2) (1972), S. 118–126.


*Eingegangen 21. 4. 1973* (397)

ACTA ARITHMETICA
XXVII (1975)

# Correspondences in a finite field, I*

by

L. Carlitz (Durham, N.C.)

*To the memory of Yu. V. Linnik*

**1. Introduction.** It is well known that any function from a finite field into itself can be represented by a polynomial with coefficients in the field. More precisely, if the field is of order $q$, then the function is represented by a unique polynomial of degree less than $q$. Conversely, any field with the property that any function from the field into itself can be represented by a polynomial with coefficients in the field, is necessarily finite. It has been proved recently [1] that if a ring $R$ (with identity) has the property that any function from $R$ into itself can be represented by a generalized polynomial, then $R$ is isomorphic to the matric ring $(\mathrm{GF}(q))_n$, for some $n \geqslant 1$. By a *generalized polynomial* is meant a sum of monomials of the type

$$a_0 x^{e_1} a_1 x^{e_2} \ldots a_{k-1} x^{e_k} a_k,$$

where $a_i \in R$, $e_i > 0$ and $k \geqslant 1$ but arbitrary.

With every function from $\mathrm{GF}(q)$ into itself we may associate a set of numbers $a_1, \ldots, a_k \in F_q = \mathrm{GF}(q)$ and a partition ([3], [4], [5])

$$F_q = A_1 \cup A_2 \cup \ldots \cup A_k, \tag{1.1}$$

where

$$A_i \cap A_j = \emptyset \quad (i \neq j); \tag{1.2}$$

the sets $A_i$ are non-vacuous and

$$f(b_i) = a_i \quad (b_i \in A_i). \tag{1.3}$$

For example, for the function $f(x) = x^{q-1}$, we have $k = 2$, $a_1 = 0$, $a_2 = 1$,

$$A_1 = \{0\}, \quad A_2 = \{a \mid a \in F_q, a \neq 0\}.$$

* Supported in part by NSF grant GP-17031.