Journal für die reine und angewandte Mathematik

Herausgegeben von **Helmut Hasse** und **Hans Rohrbach**

Verlag Walter de Gruyter & Co., Berlin W 30

Sonderabdruck aus Band 206, Heft 1/2. 1961. Seite 61 bis 66

Über einige Probleme der additiven Zahlentheorie.

Von *P. Erdös* in Budapest.

Es seien $0 = a_0 < a_1 \cdots$; $0 = b_0 < b_1 < \cdots$ Folgen ganzer Zahlen,

$$A(m) = \sum_{1 \leqq a_i \leqq m} 1, \quad B(m) = \sum_{1 \leqq b_i \leqq m} 1.$$

Die Schnirelmannsche Dichte der Folge $\{a_i\}$ im Intervall $(1, N)$ (wo N auch unendlich sein kann) ist die größte Zahl α, für welche

$$A(m) \geqq \alpha m \tag{1}$$

für alle $m \leqq n$ gilt.

Die Folge $\{b_i\}$ nennt Khintchine eine wesentliche Komponente, wenn für jede Folge der Dichte α $(0 < \alpha < 1)$ die Dichte der Zahlen von der Form $\{a_i + b_j\}$ größer als α ist. Khintchine [1]) zeigte, daß die Quadratzahlen eine wesentliche Komponente sind. Ich [2]) bewies, daß jede Basis eine wesentliche Komponente ist (eine Folge $\{b_j\}$ wird eine Basis r-ter Ordnung genannt, wenn sich jede ganze Zahl als Summe von r oder weniger b's darstellen läßt; z. B. bilden die k-ten Potenzen der Primzahlen eine Basis für jedes k). Genauer zeigte ich, daß die Dichte der Folge $\{a_i + b_j\}$ mindestens

$$\alpha + \frac{\alpha(1 - \alpha)}{2r} \tag{2}$$

ist. Der wichtigste Schritt beim (sehr einfachen) Beweis von (2) war folgender:

Lemma. *Es sei $f(\alpha)$, $0 < \alpha < 1$ die größte Zahl mit folgender Eigenschaft: $a_1 < a_2 < \cdots$ sei eine beliebige Folge der Dichte α, und zu jedem n existiere ein $k = k(n)$, so daß die Anzahl der verschiedenen Zahlen $\leqq n$ in der Folge $\{a_i, a_i + k\}$ größer oder gleich $(\alpha + f(\alpha))\, n$ ist. Dann gilt*

$$f(\alpha) \geqq \frac{\alpha(1 - \alpha)}{2}. \tag{3}$$

Ich zeigte dann noch in meiner Arbeit, daß (2) mit $\alpha + \frac{f(\alpha)}{r}$ wahr ist. Verschiedene Autoren haben (2) und (3) verschärft [3]). Ich vermutete $f(\alpha) \geqq \alpha(1 - \alpha)$, werde aber

[1]) *A. Khintchine*, Über ein metrisches Problem der additiven Zahlentheorie, Mat. Sbornik **40** (1933), 180—189, siehe auch *A. Buchstab*, ibid. 190—195.

[2]) *P. Erdös*, On the arithmetical density of the sum of two sequences one of which forms a basis for the integers, Acta Arithmetica **1** (1936), 197—200.

[3]) Siehe z. B. *E. Landau*, Über einige Fortschritte der additiven Zahlentheorie, Cambridge 1937, 3—6 und 60—63; *A. Brauer*, Über die Dichte der Summe zweier Mengen, deren eine von positiver Dichte ist, Math. Zeitschrift **44** (1939), 212—232; *S. Selberg*, Metrical problem in the additive theory of numbers, Arch. Math. Naturvidensk. **47** (1941), 111—118; *F. Kasch*, Abschätzung der Dichte von Summenmengen, Math. Zeitschrift **66** (1956), 164—172; *H. Plünnecke*, Über ein metrisches Problem der additiven Zahlentheorie, Journal reine und angew. Math. **197** (1957), 97—103.

jetzt mit wahrscheinlichkeitstheoretischen Mitteln zeigen, daß dies für jedes α falsch ist (es ist demnach möglich, daß (2) mit $\alpha + \frac{\alpha(1-\alpha)}{r}$ wahr ist). $f(\alpha)$ kann ich aber für kein einziges α bestimmen. Ich kann zeigen, daß eine absolute Konstante c_1 existiert, so daß

$$f(\alpha) < \alpha(1-\alpha) - c_1(\min(\alpha, 1-\alpha))^{3/2} \tag{4}$$

gilt. Wenn $\alpha < \frac{1}{2}$ ist, so gilt also

$$f(\alpha) < \alpha - c_1\alpha^{3/2}.$$

Für kleine Werte von α ist dies die genaue Größenordnung für $f(\alpha)$. A. Brauer[3]) beweist nämlich, daß (2) mit $\alpha + \frac{\alpha(1-\alpha^{1/2})}{r}$ wahr ist, und vielleicht kann man durch seine Schlußweise

$$f(\alpha) > \alpha - \alpha^{3/2} \tag{5}$$

zeigen. Jedenfalls gibt seine Methode sofort

$$f(\alpha) > \alpha - 2\alpha^{3/2}. \tag{6}$$

Da weder (5) noch (6) explizit bei Brauer steht — er war nur an der Verschärfung von (2) interessiert —, werden wir (6) durch die Brauersche Schlußweise beweisen.

Ein ähnliches Problem ist das folgende: Es seien $1 \leqq a_1 < a_2 < \cdots < a_n \leqq 2n$ irgend n ganze Zahlen, $d_1, d_2, \ldots d_n$ die anderen Zahlen $\leqq 2n$. Es sei M_k die Lösungszahl der Gleichung $a_i - d_j = k$, also

$$M_k = \sum_{a_i - d_j = k} 1.$$

Es sei

$$M^{(n)} = \min \max_{-2n \leqq k \leqq 2n} M_k,$$

wo man das Minimum über alle Folgen $1 \leqq a_1 < \cdots < a_n \leqq 2n$ nehmen muß. Ich zeigte[4]) (sehr leicht) $M^{(n)} \geqq \frac{n}{4}$, Scherk verschärfte dies zu $M^{(n)} > \left(1 - \frac{1}{\sqrt{2}}\right) n$ und Swierczkowski[5]) bewies $M^{(n)} > \frac{4-\sqrt{6}}{5} n$. Schließlich zeigte Moser[6]) durch eine sehr sinnreiche Methode $M^{(n)} > \frac{\sqrt{2}}{4}(n-1)$, und er kann durch eine längere Rechnung $M^{(n)} > \sqrt{4-\sqrt{15}}\,(n-1)$ beweisen.

Ich vermutete $M^{(n)} \geqq \frac{n}{2}$, jedoch widerlegte ich dies durch wahrscheinlichkeitstheoretische Betrachtungen[6]), indem ich $M \leqq \frac{4}{9} n$ für genügend großes n bewies. Unabhängig zeigten Selfridge, Motzkin und Rolston[6]) mit Hilfe der elektronischen Maschine Swac, daß $M^{(15)} = 6$ ist, und man kann daraus leicht $M^{(n)} \leqq 0{,}4n$ für unendlich viele n folgern. Moser konnte dieses Resultat noch etwas verschärfen, aber der genaue Wert von $M^{(n)}$ ist noch nicht bekannt.

---

[4]) *P. Erdös*, Some remarks on number theory (in hebräischer Sprache), Riveon lematematika **9** (1955), 45—48.

[5]) *S. Swierczkowski*, On the intersection of a linear set with the translation of its complement, Coll. Math. **5** (1958), 185—197.

[6]) *L. Moser*, On the minimal overlap problem of Erdös, Acta Arithmetica **5** (1959), 117—119.

Man kann diese Frage noch etwas verallgemeinern. Es sei G eine Gruppe mit n Elementen. $a_1, a_2, \ldots, a_l$, $l = \left[\frac{n}{2}\right]$ seien l beliebige Elemente von G und $d_1, d_2, \ldots, d_{n-l}$ die $n - l$ anderen Elemente von G. Es ist leicht zu sehen, daß es immer ein Element x von G gibt, so daß die Lösungszahl von $a_i x = d_j$ mindestens $\left[\frac{n}{4}\right] + 1$ ist. Dies folgt sofort aus der Bemerkung, daß $l(n-l)$ die Anzahl der Elemente der Form $a_i^{-1} d_j$ ist, und da das Einselement nicht von der Form $a_i^{-1} d_j$ ist, es mindestens ein x gibt für welches die Lösungszahl von $a_i x = d_j$ größer oder gleich $\left\{\frac{l(n-l)}{n-1}\right\} = \left[\frac{n}{4}\right] + 1$ ist ($\{x\}$ sei die kleinste ganze Zahl $\geqq x$). Wenn G die additive Gruppe der Restklassen mod p ist und die a's die quadratischen Reste sind, so ist die Lösungszahl von $a_i + k = d_j$ bekanntlich höchstens $\left[\frac{p}{4}\right] + 1$, also die obige Abschätzung ist hier scharf. Ich weiß aber nicht, ob $\left[\frac{n}{4}\right] + 1$ sich nicht für gewisse Gruppen doch wesentlich verschärfen läßt. Man kann durch wahrscheinlichkeitstheoretische Betrachtungen zeigen, daß eine Konstante c so existiert, daß man in jeder Gruppe von n Elementen $l = \left[\frac{n}{2}\right]$ Elemente $a_1, a_2, \ldots, a_l$ finden kann, für die die Lösungszahl von $a_i x = d_j$ für jedes x kleiner als $\frac{n}{4} + c\,(n \log n)^{1/2}$ ausfällt.

Dies zeigt, daß $\left[\frac{n}{4}\right]$ doch eine ziemlich gute untere Abschätzung ist.

Linnik[7]) zeigte als erster, daß nicht jede wesentliche Komponente eine Basis sein muß. Kürzlich wurde dies viel einfacher von Stöhr und Wirsing[8]) bewiesen. Für Linniks wesentliche Komponente gilt aber $B(n) = O(n^\varepsilon)$ und nach seiner mündlichen Mitteilung **kann er sogar eine wesentliche Komponente mit $B(n) < \exp(n^{1-c})$ konstruieren. Ich** vermute, daß für eine wesentliche Komponente $\frac{B(n)}{\log n} \to \infty$ gelten muß. Ein spezieller Fall dieser Vermutung ist, daß eine Folge b_k mit $b_{k+1} > (1 + c)\, b_k$ keine wesentliche Komponente sein kann. Dies kann ich aber nicht beweisen.

Schließlich möchte ich noch eine Frage stellen. Gibt es eine Funktion $g(\alpha) > 0$, $0 < \alpha < 1$ und eine Folge $b_1 < b_2 < \cdots$, die keine Basis ist, so daß, wenn a_i eine Folge der Dichte α ist, zu jedem n ein $b_j = b_j(n)$ so existiert, daß die Anzahl der verschiedenen Zahlen $\leqq n$ in der Folge $\{a_i, a_i + b_j\}$ größer als $(\alpha + g(\alpha))\, n$ ist? Wenn b_i eine Basis r-ter Ordnung ist, so zeigte ich[2]), daß $g(\alpha) \geqq \frac{\alpha(1-\alpha)}{2r}$ gilt.

Nun beweisen wir

Satz 1.

$$f(\alpha) < \alpha(1 - \alpha).$$

Es sei $\varepsilon > 0$ eine von α abhängige Zahl und η sei klein im Vergleich zu ε und α. Wir definieren Folgen im Intervall $(1, n)$ durch folgende wahrscheinlichkeitstheoretische Betrachtungen. Im Intervall $\left(1, \frac{n}{2}\right)$ gehöre eine Zahl u zu unserer Folge mit der Wahrscheinlichkeit $\alpha + \varepsilon + \eta$ und im Intervall $\left(\frac{n}{2}, n\right)$ mit der Wahrscheinlichkeit $\alpha - \varepsilon$.

---

[7]) *W. V. Linnik*, On Erdös's theorem on the addition of numerical sequences, Mat. Sbornik N. S. **10** (52) (1942), 67—78.

[8]) *A. Stöhr* und *E. Wirsing*, Beispiele von wesentlichen Komponenten, die keine Basen sind, Journal reine u. angew. Math. **196** (1956), 96—98.

Die Zahlen sollen unabhängig voneinander gewählt werden. Es folgt aus bekannten Sätzen der Wahrscheinlichkeitsrechnung (Satz der großen Zahlen), daß eine Konstante $C = C(\alpha, \varepsilon, \eta)$ so existiert, daß mit einer Wahrscheinlichkeit größer als C die Dichte unserer Folge größer als α wird, daß aber $A(n) < (\alpha + 2\eta)\, n$ ausfällt. Anstatt dieser Konstruktion könnte man folgendes kombinatorische Modell betrachten. Im Intervall $\left(1, \frac{n}{2}\right)$ wählen wir auf alle möglichen Arten $l_1 = \left[\left(\frac{\alpha}{2} + \varepsilon + \eta\right) n\right]$ Zahlen, und im Intervall $\left(\frac{n}{2}, n\right)$ wählen wir auf alle möglichen Arten $\left[(\alpha - \varepsilon)\frac{n}{2}\right] = l_2$ Zahlen. Offenbar kann man diese Zahlen auf

$$\binom{\left[\frac{n}{2}\right]}{l_1}\binom{n - \left[\frac{n}{2}\right]}{l_2} = N \tag{7}$$

Arten wählen. Nun folgt durch naheliegende, aber etwas mühsame kombinatorische Betrachtungen, daß für mindestens CN dieser Folgen ihre Dichte größer als α ist.

Es sei jetzt k eine beliebige Zahl $\leqq n$, und $E(u)$ sei die Wahrscheinlichkeit des Ereignisses $e(u)$, daß $u \in A$ und $u + k \in D$ ist. (Die Folge D besteht aus den Zahlen $d_i \leqq n$, die nicht in der Folge A sind). Wir wollen nun $\sum_{u=1}^{n-k} E(u)$ von oben abschätzen (für $u > n - k$ ist $u + k > n$, also $E(u) = 0$). Offenbar gilt

$$\sum_{u=1}^{n-k} E(u) = \Sigma_1 + \Sigma_2 + \Sigma_3 \tag{8}$$

mit $1 \leqq u \leqq \frac{n}{2} - k$ in Σ_1, $\frac{n}{2} - k < u \leqq \frac{n}{2}$ in Σ_2 und $\frac{n}{2} < u \leqq n - k$ in Σ_3 (wenn $k > \frac{n}{2}$ ist, so ist natürlich $\Sigma_3 = 0$). Für $1 \leqq u \leqq \frac{n}{2} - k$ ist die Wahrscheinlichkeit für $u \in A$ gleich $\alpha + \varepsilon + \eta$ und für $u + k \in D$ gleich $1 - \alpha - \varepsilon - \eta$. Da diese beiden Ereignisse offenbar unabhängig sind, gilt

$$\Sigma_1 = \left(\frac{n}{2} - k\right)(\alpha + \varepsilon + \eta)(1 - \alpha - \varepsilon - \eta).$$

Durch denselben Gedankengang folgt

$$\Sigma_2 = k(\alpha + \varepsilon + \eta)(1 - \alpha + \varepsilon), \quad \Sigma_3 = \left(\frac{n}{2} - k\right)(\alpha - \varepsilon)(1 - \alpha + \varepsilon).$$

Also ist wegen (8)

$$\begin{aligned}\sum_{u=1}^{n-k} E(u) &= (n - 2k)\left(\alpha - \alpha^2 - \varepsilon^2 - \alpha\eta - \varepsilon\eta + \frac{\eta}{2} - \frac{\eta^2}{2}\right) \\ &\quad + k(\alpha + \varepsilon + \eta - \alpha^2 - \eta\alpha + \eta\varepsilon + \varepsilon^2) \\ &< n\left(\alpha - \alpha^2 - \frac{\varepsilon^2}{2}\right),\end{aligned} \tag{9}$$

wenn $\varepsilon = \varepsilon(\alpha)$ und $\eta = \eta(\alpha, \varepsilon)$ genügend klein sind.

Jetzt wollen wir zeigen, daß die Wahrscheinlichkeit dafür, daß

$$\sum_{e(u)\text{ wahr}} 1 > n\left(\alpha - \alpha^2 - \frac{\varepsilon^2}{4}\right) \tag{10}$$

gilt, kleiner als $(1 + c_2)^{-n}$ ist, wo $c_2 = c_2(\alpha, \varepsilon) > 0$ ist. Dies würde wegen (9) sofort aus der Bernsteinschen Ungleichung[9]) folgen, wenn die Ereignisse $e(u)$ unabhängig wären.

[9]) Siehe z. B. *I. V. Uspensky*, Introduction to mathematical probability, New York u. London, 1937, 204—205.

$e(u)$ und $e(u+k)$ schließen sich aber offenbar aus, sind also nicht unabhängig. Wir teilen jetzt die Ereignisse $e(u)$ in zwei Klassen ein. In der ersten Klasse sind die u's $(1 \leqq u \leqq n-k)$ mit

$$u = 2lk + r, \quad l = 0, 1, \ldots; \; 0 \leqq r < k$$

und in der zweiten Klasse die u's $(1 \leqq u \leqq n-k)$ mit

$$u = (2l+1)k + r, \quad l = 0, 1, \ldots; \; 0 \leqq r < k.$$

Offenbar sind die Ereignisse in derselben Klasse unabhängig, da die Differenz zweier Zahlen in derselben Klasse niemals gleich k ist. Wenn nun (10) gilt, muß wegen (9) für mindestens eine der Klassen

$$\sum_{e(u) \text{ wahr}} 1 > \sum E(u) + \frac{\varepsilon^2 n}{8} \tag{11}$$

gelten — hier läuft die Summation über die Zahlen derselben Klasse.

Da die Ereignisse derselben Klasse unabhängig sind, folgt aus der Bernsteinschen Ungleichung, daß die Wahrscheinlichkeit von (11) und also auch von (10) kleiner als $(1+c_k)^{-n}$ ist. Da für k höchstens n Werte in Betracht kommen, erhalten wir, daß die Wahrscheinlichkeit, daß es ein k, $1 \leqq k \leqq n$ gibt, für welches (10) gilt, kleiner als

$$n(1+c_2)^{-n} = o(1) \tag{12}$$

ist. Nach der Bemerkung am Anfang unseres Beweises ist aber die Wahrscheinlichkeit, daß unsere Folge die Dichte α hat und $A(n) < (\alpha + 2\eta)\, n$ befriedigt, größer als C. Daher folgt aus (12), daß für $n > n_0$ die Wahrscheinlichkeit für die Existenz einer Folge $a_1 < a_2 < \cdots$ der Dichte α, bei der für jedes k die Anzahl der Zahlen $\leqq n$ in der Folge $\{a_i, a_i + k\}$ kleiner als

$$n(\alpha + 2\eta) + n\left(\alpha - \alpha^2 - \frac{\varepsilon^2}{4}\right) < n\left(\alpha(1-\alpha) - \frac{\varepsilon^2}{8}\right) \quad (\eta < \eta(\varepsilon))$$

ausfällt, gleich $C - o(1) > \frac{C}{2}$ ist. Also folgt, daß eine solche Folge existiert, und somit ist unser Satz bewiesen.

Man könnte den Beweis auch leicht mit Hilfe unseres kombinatorischen Modells führen, nur sind die Rechnungen etwas umständlich, der Vorteil aber ist, daß man keine wahrscheinlichkeitstheoretischen Sätze und Begriffe braucht. Es sei N_k die Anzahl der nach unserer Vorschrift gebildeten Folgen $a_1 < a_2 < \cdots < a_u \leqq n$, $u = [n(\alpha + \eta)]$, für welche die Anzahl der Zahlen $\leqq n$ von der Form $a_i + k$, die nicht in der Folge a_i vorkommen, größer als $n(\alpha(1-\alpha) - 2\eta)$ ist. Man kann durch naheliegende, aber ziemlich umständliche Abschätzungen von Binomialkoeffizienten zeigen, daß für genügend kleines $\eta = \eta(\varepsilon, \alpha)$

$$N_k < N(1+c_2)^{-n} \tag{13}$$

ist. Also gilt wegen (13)

$$\sum_{k=1}^{n} N_k = o(N).$$

Wegen (7) existieren daher $(C - o(1))\, N > \frac{C}{2} N$ Folgen der Dichte α, für welche die Anzahl der verschiedenen Zahlen $\leqq n$ der Folge $\{a_i, a_i + k\}$ für jedes k kleiner als $n(\alpha(1-\alpha) - \eta)$ ist, und dies beweist wieder unseren Satz.

Nun wollen wir noch den Beweis von (4) skizzieren. Es sei zuerst $0 < \alpha \leqq \frac{1}{2}$; wir können annehmen, daß α klein ist. Hier definieren wir unsere Folgen durch folgende Wahrscheinlichkeitsverteilung: Im Intervall $(1, \alpha^{1/2} n)$ sei die Wahrscheinlichkeit, daß die

Zahl u in unserer Folge vorkommt, gleich $\frac{\alpha^{1/2}}{2} + \eta$, wo η klein im Vergleich zu α ist. Im Intervall $(\alpha^{1/2}n, n)$ sei die Wahrscheinlichkeit, daß u in A vorkommt, gleich $\frac{\alpha}{2}(1 - \alpha^{1/2})^{-1}$. Für $\frac{1}{2} < \alpha < 1$, $\delta = 1 - \alpha$ (wir können annehmen, daß δ klein ist) sei im Intervall $(n(1 - \delta^{1/2}), n)$ die Wahrscheinlichkeit, daß u nicht zu A gehört, gleich $\frac{\delta^{1/2}}{2} - \eta$ und im Intervall $(1, n(1 - \delta^{1/2})$ gleich $\frac{\delta}{2}(1 - \delta^{1/2})^{-1}$. Von diesem Punkt an ist nun der Beweis von (4) ähnlich dem Beweise von Satz 1 und kann unterdrückt werden.

Jetzt wollen wir noch den Beweis von (6) skizzieren. Es sei $a_1 < a_2 < \cdots$ eine Folge der Dichte α. Wir können annehmen, daß $A(n) < 2\alpha n$ gilt (wenn nicht, so ist (6) schon mit $k = 0$ erfüllt). Wir bezeichnen mit $L(n)$ die Lösungsanzahl von

$$a_i + x = d_j, \quad 0 < x \leqq [\alpha^{1/2}n] = T.$$

Offenbar gilt, falls $D(m) = m - A(m)$ die Anzahl der $d_i \leqq m$ bedeutet,

$$L(n) \geqq \sum_{a_i \leqq n-T} (D(a_i + T) - D(a_i)) \geqq A(n - T)\,(T - A(n)) \geqq \alpha(n - T)\,(T - A(n)) \tag{14}$$

wegen $D(a_i + T) - D(a_i) \geqq T - A(n)$. Aus (14) folgt aber: Für ein $k \leqq T$ ist die Anzahl der Zahlen $a_i + k \leqq n$, die nicht in A vorkommen, mindestens

$$\frac{\alpha(n - T)\,(T - A(n))}{T}. \tag{15}$$

Also ist für dieses k die Anzahl der Zahlen $\leqq n$ in der Folge $\{a_i, a_i + k\}$ größer oder gleich

$$A(n) + \frac{\alpha(n - T)\,(T - A(n))}{T}. \tag{16}$$

Es ist leicht zu sehen, daß (16) für $A(n) = \alpha n$ ein Minimum wird $(A(n) \geqq \alpha n)$, und eine leichte Rechnung zeigt, daß

$$A(n) + \frac{\alpha(n - T)\,(T - A(n))}{T} > (\alpha - 2\alpha^{3/2})\,n$$

ist, was zu beweisen war.

Eingegangen 3. November 1960.