

Sitzungsberichte

der

mathematisch-naturwissenschaftlichen

Klasse

der

Bayerischen Akademie der Wissenschaften

zu München

Jahrgang 1951

München 1952

Verlag der Bayerischen Akademie der Wissenschaften

In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung München

Zur Zahlentheorie der Polynome

Von Wilhelm Specht in Erlangen

Vorgelegt von Herrn Otto Haupt am 16. November 1951

Vor kurzem hat E. Ullrich die folgende Aufgabe gestellt: Es bezeichne $\mathfrak{P}_n(x)$ die Menge aller ganzzahligen Polynome

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \dots + a_n$$

eines festen Grades $n > 1$, deren (ganzzahligen) Koeffizienten der Höhenbedingung

$$|a_v| \leq x \quad (v = 1, 2, \dots, n)$$

genügen, und $P_n(x)$ deren Anzahl, ferner $\mathfrak{S}_n(x)$ die Teilmenge der (im Körper der rationalen Zahlen) irreduziblen Polynome $f(z)$ aus $\mathfrak{P}_n(x)$ und $I_n(x)$ deren Anzahl. Gesucht wird der asymptotische Wert der Anzahl $I_n(x)$ in Abhängigkeit von der Höhe x .

Als Lösung dieser Aufgabe sollen in der vorliegenden Arbeit die folgenden beiden Gleichungen bewiesen werden:

$$(1) \quad I_2(x) = 4x^2 - 2x \log x + O(x),$$

$$(2) \quad I_n(x) = 2^n x^n + O(x^{n-1}) \quad \text{für } n > 2.$$

Da für die Anzahl $P_n(x)$ der Polynome $f(z)$ aus $\mathfrak{P}_n(x)$ offensichtlich keine bessere Aussage als

$$(3) \quad P_n(x) = (2[x] + 1)^n = 2^n x^n + O(x^{n-1}) \quad \text{für } n \geq 2$$

erhalten werden kann, läßt sich grundsätzlich auch keine Verbesserung der Restglieder in (1) und (2) erreichen.

Bezeichnet noch $\mathfrak{R}_n(x)$ die Menge der reduziblen Polynome $f(z)$ aus $\mathfrak{P}_n(x)$ und $R_n(x)$ deren Anzahl, so ist

$$(4) \quad R_n(x) + I_n(x) = P_n(x),$$

weshalb die Aussagen

$$(1^*) \quad R_2(x) = 2x \log x + O(x)$$

$$(2^*) \quad R_n(x) = O(x^{n-1}) \quad \text{für } n > 2$$

mit den Gleichungen (1) und (2) gleichwertig sind. Der Beweis dieser Gleichungen bedarf, wenn er auch nicht schwierig ist, doch einiger Vorbereitungen; dabei werden wir zunächst den Fall $n > 2$ angreifen, um anschließend den Fall $n = 2$ gesondert zu behandeln.

Für die Höhe x werde dabei stets $x > 1$ vorausgesetzt.

Hilfssatz 1. Sind $\omega_1, \omega_2, \dots, \omega_n$ die der absoluten Größe

$$|\omega_1| \geq |\omega_2| \geq \dots \geq |\omega_n|$$

nach geordneten Nullstellen eines Polynoms $f(z)$ aus $\mathfrak{P}_n(x)$, so gilt für jedes $v = 1, 2, \dots, n$ die Ungleichung

$$|\omega_1 \omega_2 \dots \omega_v| \leq \frac{n+2}{2} x.$$

Genügen nämlich die Koeffizienten eines beliebigen komplexen Polynoms $f(z) = z^n + \alpha_1 z^{n-1} + \alpha_2 z^{n-2} + \dots + \alpha_n$ der Ungleichung

$$|\alpha_v| \leq \beta \quad (v = 1, 2, \dots, n),$$

so gelten nach einem schon früher von mir bewiesenen Satze¹ für die (der absoluten Größe nach geordneten) Nullstellen ω_v von $f(z)$ die Ungleichungen

$$|\omega_1 \omega_2 \dots \omega_v| \leq 1 + v\beta; \quad |\omega_1 \omega_2 \dots \omega_v| \leq \max(1, (n-v+1)\beta).$$

Für $\beta = x > 1$ ist daher

$$\begin{aligned} |\omega_1 \omega_2 \dots \omega_v| &\leq \min((v+1)x, (n-v+1)x) \\ &\leq \frac{v+1+n-v+1}{2} x = \frac{n+2}{2} x. \end{aligned}$$

Hilfssatz 2. Es gibt eine allein vom Grade n abhängige positive Konstante $\gamma = \gamma(n)$ mit folgender Eigenschaft: Ist $g(z) = z^h + b_1 z^{h-1} + b_2 z^{h-2} + \dots + b_h$ ein beliebiger (nor-

¹ Vgl. W. Specht, Abschätzungen der Wurzeln algebraischer Gleichungen. Math. Zeitschr. 52 (1949), 310–321, Satz 7.

mierter, komplexer) Faktor eines beliebigen Polynoms $f(z)$ aus $\mathfrak{P}_n(x)$, so gilt für jeden Koeffizienten b_x des Polynoms $g(z)$ die Ungleichung

$$(5) \quad |b_x| \leq \gamma x \quad (x = 1, 2, \dots, k).$$

Sind nämlich $\omega_1, \omega_2, \dots, \omega_n$ die Nullstellen des Polynoms $f(z)$, so gilt für jedes $v = 1, 2, \dots, n$ und jede Indexreihe

$$1 \leq \rho_1 < \rho_2 < \dots < \rho_v \leq n$$

nach Hilfssatz 1 die Ungleichung

$$|\omega_{\rho_1} \omega_{\rho_2} \dots \omega_{\rho_v}| \leq \frac{n+2}{2} x.$$

Da nun jeder Koeffizient b_x (abgesehen vom Vorzeichen) elementarsymmetrische Funktion gewisser Nullstellen des Polynoms $f(z)$ ist, erhalten wir hieraus

$$|b_x| \leq \frac{n+2}{2} \binom{k}{x} x \quad (x = 1, 2, \dots, k).$$

Setzen wir also

$$\gamma = \gamma(n) = \frac{n+2}{2} \text{Max} \binom{k}{l} \text{ für } 1 \leq l \leq k \leq n-1,$$

so ist

$$|b_x| \leq \gamma x.$$

Satz 1. Für die Anzahl $R_n(x)$ der reduziblen ganzzahligen Polynome $f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \dots + a_n$ des Grades $n > 2$ mit Koeffizienten

$$|a_v| \leq x \quad (v = 1, 2, \dots, n)$$

gilt

$$R_n(x) = O(x^{n-1}).$$

Jedes reduzible Polynom $f(z)$ aus $\mathfrak{P}_n(x)$ läßt eine Zerlegung

$$f(z) = (z^k + u_1 z^{k-1} + \dots + u_k)(z^l + v_1 z^{l-1} + \dots + v_l)$$

zu mit $k+l = n$; $2k \leq n$ und ganzen Koeffizienten $u_1, u_2, \dots, u_k, v_1, v_2, \dots, v_l$, die den Bedingungen

$$(6) \quad \left| \sum_{\rho=0}^v u_{v-\rho} v_\rho \right| \leq x \quad (v=1, 2, \dots, n)$$

unterworfen sind, wobei noch

$$u_0 = v_0 = 1; \quad u_x = 0 \text{ für } x > k; \quad v_\lambda = 0 \text{ für } \lambda > l$$

zu setzen ist.

Bezeichnet nun $Q_{n,h}(x)$ die Anzahl der Gitterpunkte $(u, v) = (u_1, u_2, \dots, u_h, v_1, v_2, \dots, v_l)$ des n -dimensionalen euklidischen Raumes, die den Bedingungen (6) genügen, so zählt $Q_{n,h}(x)$ gewiß alle reduziblen Polynome $f(z)$ aus $\mathfrak{P}_n(x)$, die einen Faktor des Grades k besitzen, einige sogar mehrfach. Folglich besteht die Ungleichung

$$R_n(x) \leq \sum_{1 \leq h \leq n/2} Q_{n,h}(x),$$

da jedes reduzible Polynom $f(z)$ aus $\mathfrak{P}_n(x)$ in mindestens einer der Anzahlen $Q_{n,h}(x)$ mitgezählt wird.

Die durch $Q_{n,h}(x)$ gezählten Gitterpunkte (u, v) genügen nach Hilfssatz 2 mit der dort eingeführten Konstanten $\gamma = \gamma(n)$ den Bedingungen

$$(6) \quad \left| \sum_{\rho=0}^v u_{v-\rho} v_\rho \right| \leq x; \quad |u_x| \leq \gamma x; \quad |v_\lambda| \leq \gamma x \quad (v=1, 2, \dots, n) \\ u_0 = v_0 = 1; \quad u_x = 0 \text{ für } x > k; \quad v_\lambda = 0 \text{ für } \lambda > l,$$

unter denen insbesondere die beiden Bedingungen

$$|u_h v_l| \leq x; \quad |u_{h-1} v_l + u_h v_{l-1}| \leq x$$

auftreten. Bezeichnet demnach $Q_{n,h}^*(x)$ die Anzahl der Gitterpunkte (u, v) mit den Eigenschaften

$$(7) \quad |u_h v_l| \leq x; \quad |u_{h-1} v_l + u_h v_{l-1}| \leq x \\ |u_x| \leq \gamma x; \quad |v_\lambda| \leq \gamma x \quad (x=1, 2, \dots, k; \lambda=1, 2, \dots, l),$$

so ist für jedes $k = 1, 2, \dots, [n/2]$

$$Q_{n,h}(x) \leq Q_{n,h}^*(x),$$

so daß wir zum Beweise des Satzes 1 nur noch für $n > 2$ und jedes $k \leq n/2$ die Beziehung

$$(8) \quad Q_{n,h}^*(x) = O(x^{n-1})$$

nachzuweisen haben.

Im Falle $n \geq 4$ und $k = 1$ liegt bei festgehaltenen Werten u_1, v_{n-2}, v_{n-1} für die restlichen Koordinaten $v_1, v_2, \dots, v_{n-3}$ in (7) nur die Beschränkung

$$|v_\lambda| \leq \gamma x \quad (\lambda = 1, 2, \dots, n-3)$$

vor, weshalb die Anzahl der Gitterpunkte (u, v) mit gleichen Werten u_1, v_{n-2}, v_{n-1} gewiß jeweils ein $O(x^{n-3})$ ist. Daher genügt es, im Falle $k = 1$ die Anzahl $Q_{3,1}^*(x)$ der Gitterpunkte (u_1, v_1, v_2) mit

$$(9.1) \quad |u_1 v_2| \leq x; \quad |v_2 + u_1 v_1| \leq x; \quad |v_1| \leq \gamma x$$

zu untersuchen und durch

$$Q_{3,1}^*(x) = O(x^2)$$

abzuschätzen.

Im Falle $n \geq 5$ und $k \geq 2$ liegt bei festgehaltenen Werten $u_h, u_{h-1}, v_l, v_{l-1}$ für die restlichen Koordinaten $u_1, u_2, \dots, u_{h-2}, v_1, v_2, \dots, v_{l-2}$ in (7) nur die Beschränkung

$$|u_x| \leq \gamma x; \quad |v_\lambda| \leq \gamma x \quad (x=1, 2, \dots, k-2; \lambda=1, 2, \dots, l-2)$$

vor, weshalb die Anzahl der Gitterpunkte (u, v) mit gleichen Werten $u_h, u_{h-1}, v_l, v_{l-1}$ gewiß jeweils ein $O(x^{n-4})$ ist. Folglich genügt es, im Falle $k \geq 2$ die Anzahl $Q_{4,2}^*(x)$ der Gitterpunkte (u_1, u_2, v_1, v_2) mit

$$(10.1) \quad |u_2 v_2| \leq x; \quad |u_1 v_2 + u_2 v_1| \leq x; \quad |u_1| \leq \gamma x; \quad |v_1| \leq \gamma x$$

zu untersuchen und durch

$$Q_{4,2}^*(x) = O(x^3)$$

abzuschätzen.

Die Anzahl $Q_{3,1}^*(x)$ kann nun auf folgendem Wege abgeschätzt werden: Zunächst ist die Anzahl der den Bedingungen (9.1) genügenden Gitterpunkte (u_1, v_1, v_2) mit $u_1 = 0$ wegen

$$|v_2| \leq x; \quad |v_1| \leq \gamma x$$

ein $O(x^2)$, so daß wir nur noch die Gitterpunkte mit $u_1 \neq 0$ ab-zuzählen haben. Da aber mit (u_1, v_1, v_2) stets auch $(-u_1, v_1, -v_2)$

die Bedingungen erfüllt, erhalten wir

$$Q_{3,1}^*(x) = 2 S_{3,1}(x) + O(x^2),$$

mit der Anzahl $S_{3,1}(x)$ der Gitterpunkte (u_1, v_1, v_2) , die den Bedingungen

$$(9.2) \quad |u_1 v_2| \leq x; \quad |v_2 + u_1 v_1| \leq x; \quad u_1 > 0; \quad |v_1| \leq \gamma x$$

genügen. Bei festgehaltenen Werten u_1, v_2 kann nun v_1 höchstens $2 \left\lceil \frac{x}{u_1} \right\rceil + 1$ verschiedene Werte annehmen. Mithin ist

$$\begin{aligned} S_{3,1}(x) &\leq \sum_{1 \leq u_1 \leq x} \sum_{|v_2| \leq \frac{x}{u_1}} \left(2 \frac{x}{u_1} + 1 \right) \leq \sum_{1 \leq u_1 \leq x} \left(2 \frac{x}{u_1} + 1 \right)^2 \\ &= 4x^2 \sum_{1 \leq u_1 \leq x} \frac{1}{u_1^3} + 4x \sum_{1 \leq u_1 \leq x} \frac{1}{u_1} + \sum_{1 \leq u_1 \leq x} 1 \\ &= 4x^2 \cdot O(1) + 4x \cdot O(\log x) + O(x) = O(x^2). \end{aligned}$$

In ähnlicher Weise wird die Anzahl $Q_{4,2}^*(x)$ abgeschätzt: Hier ist die Anzahl der den Bedingungen (10.1) genügenden Gitterpunkte (u_1, u_2, v_1, v_2) mit $u_2 = 0$ wegen

$$|u_1 v_2| \leq x; \quad |u_1| \leq \gamma x; \quad |v_1| \leq \gamma x$$

gewiß ein $O(x^3)$, so daß nur noch die Gitterpunkte mit $u_2 \neq 0$ abzuzählen sind. Da mit (u_1, u_2, v_1, v_2) auch $(u_1, -u_2, v_1, -v_2)$ die Bedingungen erfüllt, finden wir

$$Q_{4,2}^*(x) = 2 S_{4,2}(x) + O(x^3)$$

mit der Anzahl $S_{4,2}(x)$ der Gitterpunkte (u_1, u_2, v_1, v_2) , die den Bedingungen

$$(10.2) \quad \begin{aligned} &|u_2 v_2| \leq x; \quad |v_2 u_1 + v_1 u_2| \leq x; \\ &|u_1| \leq \gamma x; \quad |v_1| \leq \gamma x; \quad u_2 > 0 \end{aligned}$$

genügen. Bei festgehaltenen Werten u_1, u_2, v_2 kann v_1 wiederum höchstens $2 \left\lceil \frac{x}{u_2} \right\rceil + 1$ verschiedene Werte durchlaufen, während u_1 höchstens $2 \lceil \gamma x \rceil + 1$ verschiedener Werte fähig ist. Mithin ist

$$\begin{aligned}
 S_{4,2}(x) &\leq \sum_{1 \leq u_2 \leq x} \sum_{|v_2| \leq \frac{x}{u_2}} (2\gamma x + 1) \left(\frac{2x}{u_2} + 1 \right) \\
 &\leq \sum_{1 \leq u_2 \leq x} (2\gamma x + 1) \left(\frac{2x}{u_2} + 1 \right)^2 = (2\gamma x + 1) O(x^2) = O(x^3).
 \end{aligned}$$

Damit ist der Satz 1 vollständig bewiesen.

Satz 2. Die Anzahl $R_2(x)$ der reduziblen ganzzahligen Polynome $f(z) = z^2 + az + b$ mit Koeffizienten

$$|a| \leq x; \quad |b| \leq x$$

ist

$$R_2(x) = 2x \log x + O(x).$$

Ein reduzibles ganzzahliges Polynom $f(z) = z^2 + az + b = (z - u)(z - v)$ besitzt zwei ganzzahlige Nullstellen u, v , für die noch die Bedingung $u \leq v$ hinzugefügt werden kann. Daher zählt $R_2(x)$ die Anzahl der Gitterpunkte (u, v) im zweidimensionalen euklidischen Raume ab, die den Bedingungen

$$(11.1) \quad |u + v| \leq x; \quad |uv| \leq x; \quad u \leq v$$

genügen. Da die Anzahl dieser Gitterpunkte (u, v) mit $u = v$ wegen $u^2 \leq x$ ein $O(\sqrt{x})$, die Anzahl dieser Gitterpunkte (u, v) mit $u = 0$ (bzw. $v = 0$) wegen $|v| \leq x$ (bzw. $|u| \leq x$) ein $O(x)$ ist, ferner mit dem Punkte (u, v) auch $(-u, -v)$ den Bedingungen genügt, können wir

$$R_2(x) = S(x) + O(x)$$

setzen, wenn $S(x)$ die Anzahl der Gitterpunkte (u, v) mit

$$(11.2) \quad |u + v| \leq x; \quad |uv| \leq x; \quad u > 0; \quad v \neq 0$$

bezeichnet.

Da nun aus

$$(u - 1)(|v| - 1) \geq 0$$

die Ungleichung

$$(12) \quad |u + v| \leq u + |v| \leq |uv| + 1 \leq [x] + 1$$

folgt, ist die Bedingung $|u + v| \leq x$ unter den restlichen Bedingungen von (11.2) nur dann nicht erfüllt, wenn in (12) überall Gleichheit besteht, wenn also $v > 0$ und $u = 1$, $v = [x]$ oder $u = [x]$, $v = 1$ ist. Folglich gilt

$$S(x) = 2 T(x) + O(1),$$

wenn $T(x)$ (in der üblichen Weise) die Anzahl der Gitterpunkte (u, v) mit

$$u > 0; \quad v > 0; \quad uv \leq x$$

bezeichnet. Für unsere Zwecke genügt die (auf fast trivialem Wege erhältliche) einfache Abschätzung¹

$$\begin{aligned} T(x) &= \sum_{\substack{uv \leq x \\ u > 0 \quad v > 0}} 1 = \sum_{1 \leq u \leq x} \sum_{1 \leq v \leq \frac{x}{u}} 1 \\ &= \sum_{1 \leq u \leq x} \left(\frac{x}{u} + O(1) \right) = x \log x + O(x), \end{aligned}$$

um auch Satz 2 vollständig zu beweisen.

¹ Vgl. E. Landau, Vorlesungen über Zahlentheorie, Bd. II S. 194. S. Hirzel, Leipzig 1927.