Werk

Titel: Verschiedene Bemerkungen zur Zahlentheorie.

Autor: Polya, Georg

Jahr: 1919

PURL: https://resolver.sub.uni-goettingen.de/purl?37721857X_0028|log7

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Wir betrachten noch die Darstellung der Einheit

$$1 = \alpha_1 a' + \beta_1 b' + \gamma_1 c' + \cdots + \lambda_1 l',$$

wobei $a', b', c', \ldots, l'$ eine endliche Anzahl der Basiszahlen $a, b, c, \ldots$ bedeuten. Wir wählen die Funktion φ für alle Basiselemente beliebig, aber so, daß zwischen $\varphi(a'), \varphi(b'), \ldots, \varphi(l')$ die Relation

$$\alpha_1 \varphi(a') + \beta_1 \varphi(b') + \gamma_1 \varphi(c') + \ldots + \lambda_1 \varphi(l') = 1$$

besteht. Infolge der Definition von $\varphi(K)$ wird dann $\varphi(1) = 1$, und es ist das Postulat 3 erfüllt, da man $\varphi(\varphi(1)) = \varphi(1) = 1$ hat. Um auch das Postulat 1 in seinem ganzen Umfang zu erfüllen, betrachten wir eine beliebige positive Zahl $r = \alpha_2 a'' + \beta_2 b'' + \gamma_2 c'' + \cdots + \mu_2 m''$, deren Basiselemente $a'', b'', \ldots, m''$ nicht sämtlich unter den bei der Darstellung von 1 verwandten endlichvielen Basiselementen $a', b', c', \ldots, l'$ auftreten. Die Werte $\varphi(a''), \varphi(b''), \varphi(c''), \ldots, \varphi(m'')$ die beliebig sind, wählen wir alsdann derart, daß $\varphi(r) = \alpha_2 \varphi(a'') + \beta_2 \varphi(b'') + \cdots + \mu_2 \varphi(m'') > r$ wird. Um auszuschließen, daß $\varphi(K)$ eine stetige Lösung der Funktionalgleichung $\varphi(K_1) + \varphi(K_2) = \varphi(K_1 + K_2)$ ist, muß man $\varphi(a), \varphi(b), \varphi(c), \ldots$ noch so wählen, daß nicht etwa ihre Verhältnisse zu $a, b, c, \ldots$ allesamt derselben Zahl A gleich werden. Die Funktion $E = \varphi(K)$ erfüllt jetzt alle Postulate mit Ausnahme des vierten.

5. Man wähle $E = K(1 + i)^{\varphi(n)}$, dabei bedeute $\varphi(n)$ eine unstetige Lösung der Funktionalgleichung $\varphi(n_1) + \varphi(n_2) = \varphi(n_1 + n_2)$, über $\varphi(n)$ sei so verfügt, was möglich ist, daß wenigstens für einen positiven Wert r sich $\varphi(r) > 0$ ergibt; schließlich sei $i > 0$.

Verschiedene Bemerkungen zur Zahlentheorie.

Von GEORG PÓLYA in Zürich.

I. Über die Irreduzibilität gewisser ganzzahliger Polynome.

Ich bezeichne ein Polynom als ganzzahlig, wenn seine Koeffizienten rationale ganze Zahlen sind. Die Werte, die ein Polynom $f(x)$ für rationales ganzzahliges x annimmt, werde ich kurz „die Werte von $f(x)$“ nennen. Die Werte eines ganzzahligen Polynoms sind rationale ganze Zahlen. Dies darf nicht umgekehrt werden. Wenn sämtliche Werte eines Polynoms rationale ganze Zahlen sind, so sind zwei Fälle möglich: entweder ist das Polynom ganzzahlig oder seine Koeffizienten sind nicht rationale ganze, sondern bloß rationale Zahlen. Zur Unterscheidung dieser beiden Möglichkeiten kann bei gewissen Gelegenheiten der folgende Satz dienen:

Hat das Polynom $f(x)$ vom Grade m $m+1$ Werte, die, absolut genommen, sämtlich kleiner sind, als $\frac{m!}{2^m}$, so ist $f(x)$ nicht ganzzahlig.

Die Voraussetzung besagt, daß $f(x)$ genau vom Grade m ist

$$f(x) = ax^m + \cdots, \quad a \gtrless 0,$$

und daß es $m+1$ verschiedene ganze Zahlen $c_0, c_1, c_2, \ldots c_m$ gibt, so daß

$$|f(c_\mu)| < \frac{m!}{2^m}. \qquad (\mu = 0, 1, 2, \ldots m) \tag{1}$$

Nach der Interpolationsformel von Lagrange ist

$$f(x) = \sum_{\mu=0}^{m} f(c_\mu) \frac{(x-c_0)\ldots(x-c_{\mu-1})(x-c_{\mu+1})\ldots(x-c_m)}{(c_\mu-c_0)\ldots(c_\mu-c_{\mu-1})(c_\mu-c_{\mu+1})\ldots(c_\mu-c_m)}.$$

Daher ist der höchste Koeffizient von $f(x)$

$$a = \sum_{\mu=0}^{m} \frac{f(c_\mu)}{(c_\mu-c_0)\ldots(c_\mu-c_{\mu-1})(c_\mu-c_{\mu+1})\ldots(c_\mu-c_m)}.$$

Die Bezeichnung sei so gewählt, daß

$$c_0 < c_1 < c_2 < \cdots < c_m.$$

Dann ist offenbar

$$\begin{aligned}(c_\mu - c_0)(c_\mu - c_1)\ldots(c_\mu - c_{\mu-1})(c_{\mu+1} - c_\mu)\ldots(c_m - c_\mu)\\ \geqq \mu(\mu-1)\cdots 1 \cdot 1 \cdot 2 \cdots (m-\mu).\end{aligned}$$

So folgt aus den Ungleichungen (1)

$$a < \frac{m!}{2^m} \sum_{\mu=0}^{m} \frac{1}{\mu!\,(m-\mu)!} = \frac{1}{2^m} \sum_{\mu=0}^{m} \binom{m}{\mu} = 1. \tag{2}$$

Also kann a keine ganze Zahl sein.

Der eben bewiesene Satz soll durch folgendes Beispiel verdeutlicht werden: es gibt ganzzahlige Polynome dritten Grades, die für 4 verschiedene ganzzahlige Werte der Variablen den Wert ± 1 annehmen. So wird das Polynom

$$(x+1)x(x-2)+1 \quad \text{für} \quad x = -1, 0, 1, 2 \quad \text{bzw.} \quad 1, 1, -1, 1.$$

Wenn jedoch $m \geqq 4$ ist, so kann ein ganzzahliges Polynom m^{ten} Grades nicht $m+1$ Werte ± 1 haben, da die beständig zunehmende Zahlenfolge

$$\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{3}{4}, \tfrac{3}{2}, \tfrac{15}{4}, \tfrac{45}{4}, \tfrac{315}{8}, \ldots, \tfrac{1}{2}\cdot\tfrac{2}{2}\cdot\tfrac{3}{2}\cdots\tfrac{m}{2}, \ldots$$

mit ihrem 4^{ten} Gliede die Zahl 1 überschreitet.

Hat das ganzzahlige Polynom $P(x)$ vom n^{ten} Grade n Werte, die sämtlich von 0 verschieden und absolut genommen kleiner als $\frac{\left(n-\left[\frac{n}{2}\right]\right)!}{2^{n-\left[\frac{n}{2}\right]}}$ sind, so ist $P(x)$ irreduzibel im natürlichen Rationalitätsbereiche.

Wenn $P(x)$ in rationale Faktoren zerfallen würde, so zerfiele es auch in ganzzahlige Faktoren, nach einem Satze von Gauß. Es sei $f(x)$ ein ganzzahliger Faktor von $P(x)$ vom möglichst hohen Grade m. Dann ist

$$n - \left[\frac{n}{2}\right] \leqq m < n.$$

Nach Voraussetzung hätte $f(x)$ n, d. h. mindestens $m+1$ Werte, die absolut genommen die Schranke

$$\frac{\left(n - \left[\frac{n}{2}\right]\right)!}{2^{n-\left[\frac{n}{2}\right]}} \leqq \frac{m!}{2^m}$$

nicht übersteigen würden: also könnte $f(x)$ nicht ganzzahlig sein. Der Widerspruch löst sich nur dann, wenn man die Irreduzibilität von $P(x)$ zugibt.

Betrachten wir z. B. das Polynom[1]) vom n^{ten} Grad in x

$$x(x-1)(x-2)\ldots(x-n+1) + \lambda n.$$

Nach dem Hilbertschen Irreduzibilitätssatz existieren ganzzahlige Werte von λ, für welche dieses Polynom irreduzibel wird. Nach der vorangehenden einfachen Betrachtung kann $\lambda = \pm 1$ gewählt werden, sobald

$$\frac{\left(n - \left[\frac{n}{2}\right]\right)!}{2^{n-\left[\frac{n}{2}\right]}} > n,$$

was für $n \geqq 13$ der Fall ist. In der Tat ist für $m \geqq 7$

$$\frac{m!}{2^m} > 2m > 2m - 1, \qquad \frac{(m-1)!}{2^{m-1}} > 4.$$

Die vorangehende Betrachtung läßt sich verschiedentlich verallgemeinern. Durch eine an der Hand liegende Modifikation der Überlegung erhält man z. B.:

Gibt es n ganze Zahlen, so beschaffen, daß der Abstand von je zweien mindestens d ist, und daß sie für x eingesetzt dem Polynome n^{ten} Grades $P(x)$ Werte erteilen, die sämtlich von 0 verschieden und absolut genommen kleiner als $\left(\frac{d}{2}\right)^{n-\left[\frac{n}{2}\right]}\left(n - \left[\frac{n}{2}\right]\right)!$ sind, so ist $P(x)$ irreduzibel.

Auch hiervon sei eine Anwendung gegeben Es gibt bekanntlich ganzzahlige Polynome, deren Koeffizienten keinen von 1 verschiedenen

1) Vgl. S. 104 bei P. Stäckel, Arithmetische Eigenschaften ganzer Funktionen, Crelles Journal Bd. 148, S. 101—112. Von diesem Beispiel ist die mitgeteilte Untersuchung ausgegangen.

gemeinsamen Teiler besitzen, und deren sämtliche Werte trotzdem einen solchen Teiler zulassen. Gibt es aber derartige *irreduzible* Polynome? Diese Frage hat Herr Stäckel[1]) aufgeworfen und bejahend beantwortet. Seine Antwort sei durch das Beispiel

$$(3)\quad x(x-(n!+1))(x-2(n!+1))\dots(x-(n-1)(n!+1))+n!$$

belegt. Sämtliche Werte von (3) sind durch $n!$ teilbar, da das Polynom (3)

$$\equiv x(x-1)(x-2)\dots(x-n+1)\,(\mathrm{mod.}\ n!)$$

ist und die Binomialkoeffizienten ganze Zahlen sind. (Ich bemerke, daß $n!$ der maximale Teiler ist, den die sämtlichen Werte eines Polynoms n^{ten} Grades zulassen können, dessen Koeffizienten den größten gemeinschaftlichen Teiler 1 haben.[2]) Das Polynom (3) ist irreduzibel für $n \geqq 3$. Dies folgt aus dem letzterwähnten Kriterium. Es ist nämlich für $n \geqq 3$

$$n! < \left(\frac{n!+1}{2}\right)^{n-\left[\frac{n}{2}\right]} \left(n-\left[\frac{n}{2}\right]\right)!\,.$$

Für $n=2$ wählt man etwa das Beispiel $x(x-1)+2$.

Als Kuriosum sei noch der folgende Satz mitgeteilt:

Es sei $n \geqq 17$. Wenn unter den Werten des ganzzahligen Polynoms $P(x)$ vom Grade n dieselbe Primzahl, positiv oder negativ genommen, n-mal vorkommt, dann ist $P(x)$ entweder irreduzibel oder das Produkt zweier irreduzibler Faktoren gleichen Grades.

Wenn also n ungerade ist, ist $P(x)$ sicherlich irreduzibel. Ob die Zahl 17, die in dem Satze vorkommt, möglichst klein gewählt ist, muß ich unentschieden lassen, ebenso wie die Frage, ob der zweiterwähnte Fall (das Zerfallen in zwei Faktoren) wirklich vorkommen kann. — Die Irreduzibilität ist natürlich im Bereiche der rationalen Zahlen gemeint.

Es sei also vorausgesetzt, daß für n verschiedene ganzzahlige x der Wert von $P(x)$ zu $\pm p$ ausfällt, wo p eine Primzahl, und daß

$$P(x) = F(x)f(x),$$

wo $F(x)$ und $f(x)$ ganzzahlige Polynome sind, vom Grade M bzw. m, wobei

$$1 \leqq m \leqq M \leqq n-1, \qquad M+m=n.$$

Ich zerlege den Beweis in mehrere kleine Schritte.

1. Der größte gemeinschaftliche Teiler der Koeffizienten von $P(x)$ ist offenbar p oder 1. Ich darf mich auf den letzteren Fall beschränken.

1) A. a. O. S. 104.

2) K. Hensel, Über den größten gemeinsamen Teiler usw., Crelles Journal. Bd. 116, S. 350—356. Die analoge Frage für beliebige algebraische Körper habe ich in meiner gleichzeitig erscheinenden Arbeit, Über ganzwertige Polynome in algebraischen Zahlkörpern, Crelles Journal Bd. 149, S. 97—116 behandelt.

Denn wenn der erste Fall vorliegt, so ist $\frac{P(x)}{p}$ ein ganzzahliges Polynom, dessen n Werte ± 1 ausfallen. $P(x)$ ist dann sicher irreduzibel[1]), da

$$\frac{\left(n-\left[\frac{n}{2}\right]\right)!}{2^{n-\left[\frac{n}{2}\right]}} > 1, \qquad \text{sobald } n \geqq 7.$$

2. Es ist $4m \geqq n$. Denn wäre $4m < n$, so würde $f(x)$ einen der vier Werte $+p$, $-p$, $+1$, -1 zumindest $m+1$-mal annehmen müssen und wäre eine Konstante. Insbesondere ist $m \geqq 5$, da $n \geqq 17$.

3. Die n Werte von x, für welche $P(x)$ zu $\pm p$ wird, zerfallen in zwei Klassen: mit a_μ bezeichne ich generell solche, für welche

$$F(a_\mu) = \pm 1, \quad f(a_\mu) = \pm p, \tag{4}$$

und mit b_ν solche, für welche

$$F(b_\nu) = \pm p, \quad f(b_\nu) = \pm 1 \qquad \text{ausfällt.} \tag{5}$$

Die Anzahl der b_ν ist $\leqq m$. Denn die ganzzahlige Funktion $f(x)$, deren Grad nach 2 mindestens 5, also > 3 ist, kann, nach einer vorhergehenden Bemerkung, nicht $m+1$ Werte ± 1 haben. Die Anzahl der a_μ ist, durch dieselbe Überlegung, $\leqq M$. Da aber die Gesamtzahl der a_μ und b_ν genau $n = M + m$ ist, muß es M Stück a_μ und m Stück b_ν geben. So besteht (4) für $\mu = 1, 2, \ldots M$ und (5) für $\nu = 1, 2, \ldots m$.

4. Zwischen den Zahlen $a_1, a_2, \ldots a_M$ gibt es keine zwei mod. p kongruente. Denn wäre etwa

$$a_1 \equiv a_2 \pmod{p}, \qquad \text{so wäre} \qquad |a_2 - b_1| + |b_1 - a_1| \geqq |a_2 - a_1| \geqq p.$$

An der linken Seite können nicht beide Zahlen $< \frac{p}{2}$ sein. Es sei die Bezeichnung so gewählt, daß

$$|b_1 - a_1| \geqq \frac{p}{2}. \tag{6}$$

Die Funktion $f(x) \mp (p-1)\frac{(x-b_1)(x-b_2)\ldots(x-b_m)}{(a_1-b_1)(a_1-b_2)\ldots(a_1-b_m)}$

m^{ten} Grades nimmt an $m+1$ Stellen, nämlich für $x = a_1, b_1, b_2, \ldots b_m$ den Wert ± 1 an, und daher wird sein höchster Koeffizient, der von x^m, absolut genommen, $\leqq \frac{2^m}{m!}$ sein, nach einer obigen Rechnung (vgl. (2)). Daher ist der höchste Koeffizient von $f(x)$, (6) herangezogen,

$$\leqq \frac{p-1}{|a_1-b_1|\,|a_1-b_2|\ldots|a_1-b_m|} + \frac{2^m}{m!} < \frac{2}{|a_1-b_2|\ldots|a_1-b_m|} + \frac{2^m}{m!} \leqq \frac{2}{1\cdot 1\cdot 2\cdot 2} + \frac{2^5}{5!} < 1,$$

da doch, nach 2, $m \geqq 5$.

1) Vgl. J. Schur, Aufgabe 226 im Archiv f. Math. u. Physik (3. Reihe), Bd. 13 (1908) S. 367.

5. Die Koeffizienten von $f(x)$ haben den größten gemeinsamen Teiler 1, nach 1. Die Funktion m^{ten} Grades $f(x)$ wird $\equiv 0 \pmod{p}$ für die Werte a_μ, nach (4). Diese Werte a_μ sind in der Anzahl M, nach dem Ergebnis unter 3, und untereinander inkongruent mod. p, nach dem unter 4. Nach einem bekannten Satz über Kongruenzen resultiert daraus

$$M \leqq m, \qquad \text{also} \qquad M = m = \tfrac{n}{2},$$

womit der vorausgeschickte Satz bewiesen ist.

Es muß übrigens, wenn der höchste Koeffizient von $f(x)$ mit a bezeichnet wird,

$$f(x) = a(x - a_1)(x - a_2) \ldots \left(x - a_{\frac{n}{2}}\right) + pf^*(x)$$

sein, wo $f^*(x)$ ein ganzzahliges Polynom vom Grade $< \frac{n}{2}$ bezeichnet. $f^*(x)$ wird $= \pm 1$ für die $\frac{n}{2}$ Werte $a_1, a_2, \ldots a_{\frac{n}{2}}$, gemäß (4). Der Grad von $f^*(x)$ ist also $\leqq 3$, denn sonst könnte $f^*(x)$ nicht ganzzahlig sein. Da aber $\frac{n}{2} > 7$, nimmt $f^*(x)$ mindestens einen der zwei Werte $+1$ und -1 öfters als 3mal an und ist eine Konstante. Es ist

$$f(x) = a(x - a_1)(x - a_2) \ldots \left(x - a_{\frac{n}{2}}\right) \pm p$$

und analogerweise

$$F(x) = b(x - b_1)(x - b_2) \ldots \left(x - b_{\frac{n}{2}}\right) \pm p,$$

wo also $b_1, b_2, \ldots b_{\frac{n}{2}}$ ebenfalls untereinander inkongruent sind mod. p. Nach (4) und (5) ist sicher

$$a_\mu \not\equiv b_\nu \pmod{p}.$$

Setzt man

$$P(x) = f(x)F(x)$$
$$= ab(x - a_1)(x - a_2) \ldots \left(x - a_{\frac{n}{2}}\right)(x - b_1) \ldots \left(x - b_{\frac{n}{2}}\right) + pP^*(x),$$

so ergibt sich ähnlich, daß $P^*(x)$ ganzzahlig und daß es eine Konstante $= \pm 1$ ist.

Es sei das Beispiel

$$(x^2 - 9)(x^2 - 121)(x^2 - 49)(x^2 - 81) + 2879$$
$$= \{(x^2 - 9)(x^2 - 121) + 2879\}\{(x^2 - 49)(x^2 - 81) - 2879\}$$

angeführt. Daß bei niedrigen Graden auch andere Verhältnisse eintreten können, zeigt das Beispiel

$$(x + 1)(x - 1)(x + p) + p = x(x^2 + px - 1),$$

wo p eine beliebige Primzahl bedeutet.

II. Über eine Vermutung des Herrn Fekete.

In einem Briefe, den er vor Jahren an mich gerichtet hat[1]), hat Herr Fekete die Vermutung ausgesprochen, daß das Polynom

$$(1) \qquad f(x) = \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right)x + \left(\frac{3}{p}\right)x^2 + \cdots + \left(\frac{p-1}{p}\right)x^{p-2}$$

(p ungerade Primzahl, $\left(\frac{\nu}{p}\right)$ Legendresches Symbol) im Innern des Intervalles 0,1 nicht verschwindet.

Diese Vermutung schien mir lange Zeit sehr schwierig zu entscheiden, bis ich nach vergeblichen Versuchen in verschiedenen Richtungen darauf verfallen bin, sie durch eine äußerst einfache numerische Rechnung zu widerlegen und zu zeigen, daß es unbegrenzt viele Primzahlen p gibt, für welche das Polynom (1) zwischen 0 und 1 verschwindet.

Nach dem Reziprozitätssatz und nach dem Dirichletschen Satze über die arithmetische Progression gibt es unbegrenzt viele Primzahlen p von der Eigenschaft, daß

$$(2) \qquad \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{11}{p}\right) = \left(\frac{13}{p}\right) = -1 .$$

Unter der Bedingung (2) ist für $0 < x < 1$

$$f(x) = \sum_{\nu=1}^{10}\left(\frac{\nu}{p}\right)x^{\nu-1} - x^{10} - x^{11} - x^{12} + x^{13} + x^{14} + x^{15} \pm x^{16} \pm \cdots,$$

$$f(x) < \sum_{\nu=1}^{10}\left(\frac{\nu}{p}\right)x^{\nu-1} + \frac{x^{16}}{1-x}.$$

Die Ausrechnung der rechten Seite ergibt für $x = 0{,}7$ den Wert $-0{,}00995\ldots$, und so erhält man

$$f\left(\tfrac{7}{10}\right) < 0 .$$

Da $f(0) = 1$, verschwindet $f(x)$ zwischen 0 und 0,7.

Die Bedingungen (2) sind erfüllt für die Primzahlen $p = 67$ und $p = 163$. Durch verhältnismäßig mühelose Rechnung findet man, daß in diesen Fällen das Polynom (1) genau 2 Nullstellen zwischen 0 und 1 hat. Allgemein kann man zeigen, daß das Polynom (1) im Intervalle $0 \leqq x \leqq 0{,}5$ keine und im Intervalle $0{,}5 < x < 1$ eine gerade Anzah (eventuell 0) Nullstellen hat. Darauf will ich hier nicht näher eingehen.

1) Vgl. Fekete und Pólya, Über ein Problem von Laguerre, Rendiconti Palermo, Bd. 34 (1912) S. 89–120.

III. Empirisches über die zahlentheoretische Funktion $\lambda(n)$.

Ich will an dieser Stelle eine empirische Tatsache mitteilen. Bezeichnet man mit $\nu(n)$ die Anzahl der Primfaktoren von n, und setzt man

$$\lambda(n) = (-1)^{\nu(n)}$$

$$L(n) = \lambda(1) + \lambda(2) + \lambda(3) + \cdots + \lambda(n),$$

so findet man

$$L(n) \leqq 0 \tag{1}$$

von $n = 2$ an bis etwa $n = 1500$. D. h. bis zu dieser Grenze gibt es unter den n ersten ganzen Zahlen ebensoviel oder mehr solche, die aus einer ungeraden, als solche, die aus einer geraden Anzahl Primfaktoren zusammengesetzt sind.

Ich teile diese Beobachtung mit, um evtl. weitere numerische Untersuchung zu veranlassen. Der Beweis von (1), sogar nur für hinreichend großes n, würde den Beweis der Riemannschen Vermutung nach sich ziehen, nach geläufigen Eigenschaften der ζ-Funktion und nach einem funktionentheoretischen Satze des Herrn Landau.[1])

Mich hat eben die mitgeteilte Beobachtung auf die unter II erwähnten Bedingungen (2) geführt. Der Zusammenhang geht aus dem Beweise[2]) des folgenden Satzes hervor:

Ist p eine Primzahl, $p > 7$, und ist die Anzahl der Klassen der Gaußschen primitiven quadratischen Formen zweiter Art von der Determinante $-p$ gleich Eins, so ist

$$L\left(\frac{p-3}{4}\right) = 0.$$

Damit überhaupt primitive Formen zweiter Art existieren, muß $p \equiv 3 \pmod 4$, sein, und daß die Klassenzahl dieser Formen Eins ist, bedeutet, daß unter ihnen sich nur die einzige reduzierte Form

$$2x^2 + 2xy + \frac{p+1}{2}y^2 = 2\left(\left(x + \frac{y}{2}\right)^2 + \frac{p}{4}y^2\right) \tag{2}$$

befindet. Sollte aber $\frac{p+1}{4}$ zusammengesetzt sein, etwa

$$\frac{p+1}{4} = ab$$

und $a \leqq b$, so wäre die Form

$$2ax^2 + 2xy + 2by^2$$

1) Vgl. E. Landau, Primzahlen, Bd. II, S. 617 ff., S. 697 ff.

2) Vgl. G. Frobenius, Über quadratische Formen, die viele Primzahlen darstellen, Sitzungsber. d. Berliner Akad., 1912, S. 966—980.

reduziert, von der Determinante

$$1 - 4ab = -p$$

und primitiv zweiter Art. So ist $\frac{p+1}{4}$ eine Primzahl, und zwar eine ungerade, wenn $p > 7$. Daher ist in diesem Falle

(3) $\quad p \equiv 3 \pmod 8, \qquad$ (4) $\quad \left(\frac{2}{p}\right) = -1.$

Ferner stellt die Form (2), als einzige reduzierte, alle Zahlen der Gestalt $2q$ dar, wo q eine ungerade Primzahl und

$$\left(\frac{-p}{q}\right) = +1$$

ist. Jedoch ist die kleinste Zahl, die sie darstellt, 2, und die nächstgrößere $\frac{p+1}{2}$. Daher ist $\left(\frac{-p}{q}\right) = -1$

für alle Primzahlen $q < \frac{p+1}{4}$, oder was wegen (3) dasselbe bedeutet,

(5) $\qquad \left(\frac{q}{p}\right) = -1.$

(4) (5) zusammen besagen, daß

(6) $\qquad \left(\frac{n}{p}\right) = \lambda(n) \quad$ für $\quad n = 1, 2, 3, \cdots \frac{p-3}{4}.$

Andererseits ist aber für jede Primzahl p, wo

(7) $\qquad p = 4m + 3,$

$$\left(\frac{2}{p}\right) + \left(\frac{4}{p}\right) + \left(\frac{6}{p}\right) + \cdots + \left(\frac{2m}{p}\right) = \left(\frac{2}{p}\right)\sum_{\nu=1}^{m}\left(\frac{\nu}{p}\right)$$

$$\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right) + \left(\frac{5}{p}\right) + \cdots + \left(\frac{2m-1}{p}\right) + \left(\frac{2m+1}{p}\right) =$$

$$= \left(\frac{p-2(2m+1)}{p}\right) + \left(\frac{p-2\cdot 2m}{p}\right) + \cdots + \left(\frac{p-2(m+1)}{p}\right) = -\left(\frac{2}{p}\right)\sum_{\nu=m+1}^{2m+1}\left(\frac{\nu}{p}\right).$$

Durch Addition beider Gleichungen ergibt sich

$$\sum_{\nu=1}^{2m+1}\left(\frac{\nu}{p}\right) = \left(\frac{2}{p}\right)\left(\sum_{\nu=1}^{m}\left(\frac{\nu}{p}\right) - \sum_{\nu=m+1}^{2m+1}\left(\frac{\nu}{p}\right)\right) = \left(\frac{2}{p}\right)\left(2\sum_{\nu=1}^{m}\left(\frac{\nu}{p}\right) - \sum_{\nu=1}^{2m+1}\left(\frac{\nu}{p}\right)\right)$$

$$2\sum_{\nu=1}^{m}\left(\frac{\nu}{p}\right) = \left(1 + \left(\frac{2}{p}\right)\right)\sum_{\nu=1}^{2m+1}\left(\frac{\nu}{p}\right).$$

D. h. nach (6) (7) (4)

$$\sum_{\nu=1}^{\frac{p-3}{4}}\lambda(\nu) = 0,$$

w. z. b. w.