Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante.

Von

EDMUND LANDAU in Berlin.

Im Artikel 303 der *disquisitiones arithmeticae* spricht Gauß die Vermutung aus, daß die Menge der negativen Discriminanten, für welche die Anzahl der Klassen eigentlich primitiver positiver binärer quadratischer Formen einen bestimmten Wert h hat, eine endliche ist; er hält einen strengen Beweis hiervon für sehr schwierig und begnügt sich damit, durch Abzählung in den ersten Tausenden zu konstatieren, daß die den kleinsten Werten $h = 1, 2, 3, \dots$ entsprechenden negativen Discriminanten zuerst in geringer Zahl vorhanden sind, aber in dem weiteren Verlaufe des betrachteten Intervalles nicht mehr auftreten; dies berechtigt zu der Vermutung*), daß $h(D) = h(-\Delta)$ mit Δ ins Unendliche wächst.

Das Problem, diese Vermutung zu bestätigen oder zu widerlegen, scheint auch bei dem heutigen Stande der Arithmetik und Analysis in seiner Allgemeinheit noch nicht angreifbar zu sein; dagegen ist es, wie im folgenden ausgeführt werden soll, wohl möglich, für den Fall $h=1$ **) eine Entscheidung herbeizuführen. Gauß hat empirisch konstatiert, daß bis $-D = \Delta = 3000$ die fünf Werte $\Delta = 1, 2, 3, 4, 7$ die einzigen sind, denen die Klassenzahl 1 entspricht, und es läßt sich in der Tat nachweisen, daß (in Übereinstimmung mit der a. a. O. ausgesprochenen Ver-

*) In der erwähnten Tabelle zerlegt übrigens Gauß die einem bestimmten Werte von h entsprechenden Discriminanten in Unterabteilungen nach der Anzahl g der Geschlechter, welche ja ein Teiler von h ist:

$$h = gk,$$

und er spricht die Vermutung in der Form aus, daß die jedem Typus (g, k) entsprechenden Discriminanten nur in endlicher Anzahl vorhanden sind; dies ist aber mit der Formulierung des Textes sachlich identisch.

**) In Gaußscher Terminologie ist dies der Typus I. 1, d. h. $g = 1, k = 1$, also die erste Zeile der Gaußschen Tabelle.

mutung) überhaupt nur für jene fünf negativen Discriminanten $h = 1$ ist; dieser Nachweis läßt sich sogar mit elementaren Mitteln erbringen, während die Gauß-Dirichletschen Klassenzahlformeln hierfür ungeeignet scheinen.

Es handelt sich also darum, nachzuweisen, daß für jede Discriminante $D < -7$ mindestens zwei nicht äquivalente Formen*) existieren, oder, was dasselbe besagt, daß mindestens eine der Hauptform $(1, 0, \Delta)$ nicht äquivalente Form vorhanden ist. Dazu genügt es, die Existenz einer zweiten reduzierten Form (a, b, c) nachzuweisen, d. h. dreier ganzer Zahlen a, b, c , für welche zugleich

$$(1) \quad \Delta = ac - b^2,$$

$$(2) \quad 2|b| \leq a \leq c$$

und

$$(3) \quad \{a, 2b, c\} = 1^{**})$$

ist, aber nicht zugleich $a = 1, b = 0, c = \Delta$. Denn es können zwar in gewissen Fällen zwei reduzierte Formen äquivalent sein; dies tritt jedoch nur dann ein, wenn in (2) ein Gleichheitszeichen gilt; dann sind die beiden Formen $(a, \frac{1}{2}a, c)$ und $(a, -\frac{1}{2}a, c)$ bzw. (a, b, a) und $(a, -b, a)$ äquivalent; die Hauptform $(1, 0, \Delta)$ ist also keinesfalls einer anderen reduzierten Form äquivalent.

Zunächst darf für $h = 1$ außer $(1, 0, \Delta)$ keine reduzierte Form mit mittlerem Koeffizienten 0 existieren; es darf also kein Zahlenpaar a, c geben, für welches

$$(4) \quad \Delta = ac,$$

$$(5) \quad 1 < a \leq c$$

und

$$(6) \quad \{a, c\} = 1$$

ist. Δ darf also nicht in zwei von 1, Δ verschiedene teilerfremde Faktoren zerlegbar sein, da sonst der kleinere Faktor mit a , der größere mit c bezeichnet werden kann, was den Relationen (4), (5), (6) genügen würde. Δ darf also nicht durch zwei verschiedene Primzahlen teilbar sein, ist also eine Primzahlpotenz:

$$(7) \quad \Delta = p^\lambda.***)$$

*) Es handelt sich durchweg um eigentlich primitive positive Formen.

**) $\{\alpha, \beta, \dots\}$ soll den größten gemeinsamen Teiler der ganzen Zahlen $\alpha, \beta, \dots$ bezeichnen.

***) Man könnte versucht sein, für die vorliegende Aufgabe die Theorie der Geschlechter heranzuziehen, da die Existenz mindestens zweier Geschlechter a fortiori

I. Es sei $p = 2$, also

$$\Delta = 2^\lambda.$$

Für $\lambda = 1$ und $\lambda = 2$, d. h. $\Delta = 2$ und $\Delta = 4$ ist in der Tat $h = 1$; für $\lambda = 3$, d. h. $\Delta = 8$ ist $h = 2$. Für $\lambda \geq 4$ werde mit Rücksicht auf

$$\Delta + 2^2 = \Delta + 4 = 4(2^{\lambda-2} + 1)$$

$$a = 4, b = 2, c = 2^{\lambda-2} + 1$$

gesetzt; dann erfüllen a, b, c die Relationen (1), (2), (3), und es würde gegen die Annahme $h = 1$ eine zweite reduzierte Form existieren.

II. Es sei p , also Δ ungerade. Ich setze $b = 1$; dann darf es (unter der Annahme $h = 1$) kein Zahlenpaar a, c geben, für welches zugleich

$$(8) \quad \Delta + 1 = ac,$$

$$(9) \quad 2 \leq a \leq c$$

und

$$(10) \quad \{a, 2, c\} = 1$$

ist. Die gerade Zahl $\Delta + 1$ muß also eine Potenz von 2 sein; denn hätte $\Delta + 1$ einen ungeraden Faktor > 1 , so wäre es in zwei teilerfremde Faktoren a und $c \geq a$ zerlegbar, welche beide ≥ 2 sind, was (8), (9) und (10) erfüllen würde. Daher ist

$$\Delta + 1 = 2^\nu.$$

Für $\nu = 1, 2, 3$ ergibt sich $\Delta = 1, 3, 7$, wofür in der Tat $h = 1$ ist; für $\nu = 4$ ($\Delta = 15$) ist $h = 2$, für $\nu = 5$ ($\Delta = 31$) ist $h = 3$. Für $\nu \geq 6$ genügen wegen

$$\Delta + 3^2 = \Delta + 9 = \Delta + 1 + 8 = 2^\nu + 8 = 8(2^{\nu-3} + 1)$$

die drei Zahlen

$$a = 8, b = 3, c = 2^{\nu-3} + 1$$

den Relationen (1), (2), (3), so daß auch hier $h > 1$ wäre.

Damit ist bewiesen:

Es gibt nur endlich viele negative Discriminanten, nämlich $\Delta = -1, -2, -3, -4, -7$, für welche die Anzahl der eigentlich primitiven positiven Klassen gleich 1 ist.

die Existenz mindestens zweier Klassen bedingt. Jedoch kommt man so nicht viel weiter als bis zur Gleichung (7); aus $h = 1$ folgt

$$1 = g = 2^{\varpi + \sigma - 1},$$

wo ϖ die Anzahl der ungeraden Primfaktoren von D ist, $\sigma = 0$ für $D \equiv 1 \pmod{4}$, $\sigma = 2$ für $D \equiv 0 \pmod{8}$ und sonst $\sigma = 1$. g ist also dann und nur dann $= 1$, wenn Δ eine ungerade Primzahlpotenz von der Form $4\nu + 3$ ist oder wenn $\Delta = 1, 2, 4$ ist. Der Hauptfall der ungeraden Primzahlpotenz bleibt also hiernach offen und ist wie im Texte zu erledigen.

Ich benutze diese Gelegenheit, um einen analogen Endlichkeitsbeweis bei einer dem Namen, nicht dem Inhalte nach verwandten Frage zu führen. Herr Frobenius*) hat in die Gruppentheorie den Begriff der Klassen konjugierter Elemente einer Gruppe eingeführt, durch folgende Definitionen und Sätze: Es mögen zwei Elemente A und B einer (abstrakten) Gruppe $\mathfrak{G}$ konjugiert oder ähnlich heißen, wenn mindestens ein Element C in der Gruppe gefunden werden kann, für welches

$$(11) \quad C^{-1}AC = B$$

ist. Diese Definition ist in A und B symmetrisch, da aus (11)

$$(C^{-1})^{-1}BC^{-1} = A$$

folgt, wo C^{-1} der Gruppe $\mathfrak{G}$ angehört; man erkennt ferner leicht, daß jedes Element sich selbst konjugiert ist und daß zwei einem dritten konjugierte Elemente einander konjugiert sind; man gelangt so zur Einteilung aller n Elemente der Gruppe $\mathfrak{G}$ in h Klassen; die Anzahlen der Elemente dieser Klassen seien beziehlich $\nu_1, \nu_2, \dots, \nu_h$, und die Klassen seien so geordnet, daß

$$\nu_1 \leq \nu_2 \leq \dots \leq \nu_h$$

ist. In

$$(12) \quad n = \nu_1 + \nu_2 + \dots + \nu_h$$

sind, wie Herr Frobenius gezeigt hat, die Zahlen $\nu_1, \nu_2, \dots, \nu_h$ sämtlich Divisoren von n , und ν_1 ist gleich 1, weil in jeder Gruppe für beliebiges C

$$C^{-1}EC = E$$

ist, falls E das Einheitselement bedeutet, so daß dieses nur sich selbst konjugiert ist und eine Klasse für sich bildet.

Die letztere Bemerkung ergibt ohne weiteres, daß der Klassenzahl $h = 1$ nur die identische Gruppe entspricht, indem jede andere außer dem Einheitselement noch mindestens ein Element, also noch mindestens eine Klasse enthält. Im Falle $h = 2$ würde $\nu_1 = 1$ und $\nu_2 = n - 1$ sein; da $n - 1$ nur für $n = 2$ die Zahl n teilt, gehört hierher nur die Gruppe zweiter Ordnung.

Ich behaupte nun, daß allgemein jeder Klassenzahl h nur endlich viele Gruppen entsprechen; da zu jeder Ordnung n nur endlich viele Gruppen gehören, läßt sich die Behauptung auch so aussprechen: nach Annahme einer Zahl h läßt sich eine Zahl $N(h)$ so bestimmen, daß für alle $n \geq N$ die Klassenzahl aller Gruppen der Ordnung n größer als h ist.

Da $\nu_1, \nu_2, \dots, \nu_h$ Divisoren von n sind, kann man in (12)

$$1 = \nu_1 = \frac{n}{g_1}, \quad \nu_2 = \frac{n}{g_2}, \quad \dots, \quad \nu_h = \frac{n}{g_h}$$

*) „Neuer Beweis des Sylowschen Satzes“, Journal für die reine und angewandte Mathematik, Bd. 100, 1887, S. 181.

setzen, wo $g_1, g_2, \dots, g_h$ ganze Zahlen sind, und zwar ist $g_1 = n$ und

$$(13) \quad g_1 \geq g_2 \geq \dots \geq g_h;$$

aus (12) folgt

$$(14) \quad n = \frac{n}{g_1} + \frac{n}{g_2} + \dots + \frac{n}{g_h},$$

$$\frac{1}{g_1} + \frac{1}{g_2} + \dots + \frac{1}{g_h} = 1.$$

Von der diophantischen Gleichung (14) läßt sich nun nachweisen, daß sie bei gegebenem h nur endlich viele Lösungen in positiven ganzen Zahlen $g_1, g_2, \dots, g_h$ besitzt, oder, was nicht spezieller ist, daß sie bei gegebenem h nur endliche viele Lösungen in positiven ganzen Zahlen $g_1, g_2, \dots, g_h$ mit der Nebenbedingung (13) besitzt. Aus (13) und (14) folgt nämlich zunächst

$$1 \leq \frac{1}{g_h} + \frac{1}{g_h} + \dots + \frac{1}{g_h} = \frac{h}{g_h},$$

$$g_h \leq h.$$

g_h ist also nur endlich vieler Werte fähig; für $h \geq 2$ ist der Wert $g_h = 1$ jedenfalls unbrauchbar, und für jeden der übrigen eventuell brauchbaren $h - 1$ Werte $g_h = 2, 3, \dots, h$ ergibt sich weiter

$$1 - \frac{1}{g_h} = \frac{1}{g_1} + \frac{1}{g_2} + \dots + \frac{1}{g_{h-1}} \leq \frac{1}{g_{h-1}} + \frac{1}{g_{h-1}} + \dots + \frac{1}{g_{h-1}} = \frac{h-1}{g_{h-1}},$$

$$g_{h-1} \leq \frac{h-1}{1 - \frac{1}{g_h}} \leq \frac{h-1}{1 - \frac{1}{2}} = 2(h-1),$$

und so fort. Es sei schon bewiesen, daß in (14) $g_h, g_{h-1}, \dots, g_\lambda$ ($\lambda \geq 2$) beziehlich gewisse Schranken $G_h, G_{h-1}, \dots, G_\lambda$ nicht übersteigen können. Unter den endlich vielen Möglichkeiten, $g_h, g_{h-1}, \dots, g_\lambda$ beziehlich $\leq G_h, G_{h-1}, \dots, G_\lambda$ zu wählen, gibt es a fortiori nur endlich viele, für welche außerdem*)

$$(15) \quad \frac{1}{g_\lambda} + \dots + \frac{1}{g_{h-1}} + \frac{1}{g_h} < 1$$

ist, und nur diese kommen zur Bildung von Lösungen von (14) in Frage. Für jedes solche System $g_h, g_{h-1}, \dots, g_\lambda$ ergibt sich

$$1 - \frac{1}{g_\lambda} - \dots - \frac{1}{g_{h-1}} - \frac{1}{g_h} = \frac{1}{g_1} + \dots + \frac{1}{g_{\lambda-1}} \leq \frac{1}{g_{\lambda-1}} + \dots + \frac{1}{g_{\lambda-1}} = \frac{\lambda-1}{g_{\lambda-1}},$$

$$g_{\lambda-1} \leq \frac{\lambda-1}{1 - \frac{1}{g_\lambda} - \dots - \frac{1}{g_{h-1}} - \frac{1}{g_h}};$$

*) Daß (15), ohne Nebenbedingungen als diophantische Ungleichung aufgefaßt, bei gegebenem h unendlich viele Lösungen hat, ist unerheblich.

also existiert auch für $g_{\lambda-1}$ eine obere Schranke $G_{\lambda-1}$, und man erkennt durch vollständige Induktion, daß (14) nur endlich viele Lösungen besitzt*).

Da nun die größte der Zahlen g gleich n ist, so ergibt sich, daß in (12) bei gegebenem h die Zahl n eine endliche Schranke nicht übersteigen kann; anders ausgedrückt: es gibt nur endlich viele Zahlen, welche als Summe von h ihrer Divisoren, unter denen der Divisor 1 als Summand vorkommt, darstellbar sind. Da zu jedem n nur endlich viele Gruppen gehören, ist damit bewiesen:

Es gibt nur endlich viele Gruppen mit gegebener Klassenzahl.

Berlin, den 4. Oktober 1902.

*) Natürlich erkennt man ebenso, daß $\frac{1}{g_1} + \frac{1}{g_2} + \dots + \frac{1}{g_h}$ bei gegebenem h keinen Wert unendlich oft annehmen kann.