## Werk

**Titel:** Vorlesungen über Zahlentheorie
**Autor:** Dirichlet, Peter
**Verlag:** Vieweg
**Ort:** Braunschweig
**Jahr:** 1871
**Kollektion:** Mathematica
**Digitalisiert:** Niedersächsische Staats- und Universitätsbibliothek Göttingen
**Werk Id:** PPN30976923X
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
**OPAC:** http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

**LOG Id:** LOG_0170
**LOG Titel:** §. 151. Resultat dieser Vergleichung
**LOG Typ:** chapter



## Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

lich $\delta$ in $\sigma = \delta\varrho$ auf; mithin ist (nach §. 60) $\varrho^2$ eigentlich darstellbar durch die Formen der Classe $R$, und folglich kann man (nach §. 60) als Repräsentanten von $R$ eine Form wählen, deren erster Coefficient $= \varrho^2$ ist. Da umgekehrt durch jede solche Form auch $\sigma^2$ dargestellt wird, wenn den Variabelen die Werthe $x = \delta$, $y = 0$ ertheilt werden, so gehört sie, wenn sie zugleich ursprünglich von der ersten Art ist, einer Classe $R$ aus der Gruppe $\mathfrak{R}$ an. Wir haben mithin folgenden Satz erhalten:

*Der Grad r der Gruppe $\mathfrak{R}$ ist gleich der Anzahl aller nicht äquivalenten ursprünglichen Formen der ersten Art, deren erster Coefficient ein quadratischer Divisor $\varrho^2$ vom Quadrate des Theilers $\sigma$ ist.*

Wir bemerken schliesslich, dass für jeden solchen quadratischen Divisor $\varrho^2$ (zufolge §. 56) nur alle diejenigen Formen zu untersuchen sind, deren mittlere Coefficienten ein vollständiges Restsystem nach dem Modulus $\varrho^2$ bilden.

## §. 151.

Nachdem im Vorhergehenden der Weg allgemein vorgezeichnet ist, auf welchem man zur Bestimmung des Verhältnisses der Classenanzahlen $h$ und $h'$ gelangt, schreiten wir zur Betrachtung der speciellen Fälle, in welchen $\sigma$ eine *Primzahl* ist, weil aus ihnen das allgemeine Resultat abgeleitet werden kann.

I. Ist die Determinante $D = 1 - 4n \equiv 1 \pmod 4$, und $\sigma = 2$, so handelt es sich um die Vergleichung der Classenanzahlen der ursprünglichen Formen der ersten und zweiten Art. Bezeichnet man dieselben wieder mit $h$ und $h'$, so ist $h = rh'$, wo $r$ die Anzahl der nicht äquivalenten ursprünglichen Formen erster Art bedeutet, deren erster Coefficient $= 1$ oder $= 4$ ist. Da im zweiten Fall der mittlere Coefficient ungerade sein muss, so sind nur die drei Formen

$$(1, 0, -D), \quad (4, \pm 1, n)$$

in Betracht zu ziehen.

Ist $D \equiv 1 \pmod 8$, also $n$ gerade, so ist nur die erste dieser Formen ursprünglich von der ersten Art, folglich $r = 1$, und $h = h'$.

Ist aber $D \equiv 5 \pmod 8$, also $n$ ungerade, so sind alle drei Formen ursprünglich von der ersten Art, und es braucht nur noch untersucht zu werden, ob sie verschiedenen Classen angehören oder nicht. Zunächst lässt sich beweisen, dass sie entweder zu einer und derselben, oder zu drei verschiedenen Classen gehören. *Gauss* zeigt dies durch die Composition der ihnen entsprechenden Classen $1, P, Q$; da die Classen $P$, $Q$ entgegengesetzt sind, so ist $PQ = 1$, und ferner lässt sich leicht zeigen, dass $PP = Q$ und $QQ = P$ ist (denn aus den beiden einigen, in $P$ enthaltenen Formen $(4, 1, n)$, $(n, -1, 4)$ ist die Form $(4n, 2n-1, n)$ zusammengesetzt, und da diese mit $(n, 1-2n, 4n)$, $(n, 1, 4)$, $(4, -1, n)$ äquivalent ist, so folgt $PP = Q$); nimmt man nun an, dass zwei der drei Classen $1$, $P$, $Q$ identisch sind, so ergiebt sich hieraus sofort, dass auch die dritte mit ihnen übereinstimmt. Dasselbe lässt sich auch durch die folgenden Sätze erweisen.

*Sind irgend zwei der drei Formen* $(1, 0, -D)$, $(4, \pm 1, n)$ *äquivalent, so ist die Gleichung* $t^2 - Du^2 = 4$ *durch ungerade Zahlen* $t$, $u$ *lösbar.*

Ist nämlich die erste Form mit einer der beiden anderen äquivalent, so ist (nach §. 60) der erste Coefficient 4 dieser letztern eigentlich darstellbar durch die Form $(1, 0, -D)$, also giebt es zwei relative Primzahlen $t$, $u$, welche der Gleichung $t^2 - Du^2 = 4$ genügen, woraus folgt, dass $t$, $u$, da sie nicht beide gerade sein können, nothwendig beide ungerade sein müssen. Sind ferner die beiden letzten Formen äquivalent, so giebt es (nach §. 60. Anm.) zwei ganze Zahlen $x$, $y$, welche den Bedingungen

$$4x^2 + 2xy + ny^2 = 4, \quad -2x + ny \equiv 0 \pmod 4$$

genügen; da $n$ ungerade ist, so muss $y$ gerade sein $= 2u$; setzt man dann $2x + u = t$, so gehen diese Bedingungen in die folgenden über

$$t^2 - Du^2 = 4, \; t \equiv -u \pmod 4;$$

da aus der letztern $t^2 \equiv u^2 \pmod 8$ folgt, und ausserdem $-D \equiv 3 \pmod 8$ ist, so folgt aus der erstern $4u^2 \equiv 4 \pmod 8$, mithin ist $u$, also auch $t$ ungerade, was zu beweisen war.

*Ist die Gleichung* $t^2 - Du^2 = 4$ *durch ungerade Zahlen* $t$, $u$ *lösbar, so sind alle drei Formen* $(1, 0, -D)$, $(4, \pm 1, n)$ *äquivalent.*

Denn wenn man $t$ mit beliebigem Vorzeichen, dann aber $u \equiv -t \pmod 4$ wählt, so geht die Form $(1, 0, -D)$ durch die Substitutionen

$$\begin{pmatrix} t, & \pm\dfrac{t+Du}{4} \\ \pm u, & \dfrac{t+u}{4} \end{pmatrix}$$

in die beiden Formen $(4, \pm 1, n)$ über. — Durch Verbindung der beiden vorstehenden Sätze ergiebt sich:

*Die drei obigen Formen sind äquivalent oder gehören drei verschiedenen Classen an, je nachdem die Gleichung* $t^2 - Du^2 = 4$ *durch ungerade Zahlen* $t, u$ *lösbar ist oder nicht; im ersten Falle ist* $h = h'$, *im zweiten* $h = 3h'$.

Ist nun $D$ positiv, so tritt der erste Fall ein oder der zweite, je nachdem die *kleinste* Lösung $t = T'$, $u = U'$ aus ungeraden oder geraden Zahlen besteht. Ist $D$ negativ, so besitzt die Gleichung im Allgemeinen nur die beiden Auflösungen $t = \pm 2$, $u = 0$, und mithin ist $h = 3h'$; die einzige Ausnahme hiervon bildet die Determinante $D = -3$, weil die Gleichung ausser den beiden Lösungen $t^2 = 4$, $u = 0$ noch die vier Lösungen $t^2 = u^2 = 1$ besitzt, und folglich ist in diesem Falle wieder $h = h'$.

Diese Resultate stimmen vollkommen mit denjenigen überein, welche wir früher (§§. 97, 99) mit Hülfe ganz anderer Principien abgeleitet haben.

II. Ist $D = D'\sigma^2$, so leuchtet ein, dass $h'$ zugleich die Anzahl der ursprünglichen Classen erster Art von der Determinante $D'$ ist. Unter der Voraussetzung, dass $\sigma$ eine Primzahl ist, haben wir, um das Verhältniss $r = h : h'$ zu bestimmen, nur die $l$ Formen

$$(1, 0, -D) \quad \text{und} \quad (\sigma^2, B\sigma, BB - D') \tag{1}$$

zu betrachten, wo $B$ ein vollständiges Restsystem (mod. $\sigma$) durchlaufen muss, mit Ausnahme derjenigen Werthe, für welche $BB \equiv D'$ (mod. $\sigma$) wird, weil diesen keine ursprünglichen Formen entsprechen; die Anzahl der zu betrachtenden ursprünglichen Formen ist daher

$$l = 2 \quad \text{oder} \quad \sigma - \left(\frac{D'}{\sigma}\right) \tag{2}$$

je nachdem $\sigma = 2$ oder eine ungerade Primzahl ist. Zur Bestimmung der Anzahl $r$ der verschiedenen Classen, welchen diese $l$ Formen angehören, gelangen wir durch die folgenden Sätze.

*Die beiden Formen* $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ *sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen* $t', u'$ *giebt, welche den Bedingungen*

$$t't' - D'u'u' = 1, \quad t' + \beta u' \equiv 0 \ (mod.\ \sigma) \tag{3}$$

*genügen; zwei Formen* $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ *sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen* $t', u'$ *giebt, welche den Bedingungen*

$$t't' - D'u'u' = 1, \ (b - b')t' + (bb' - D')u' \equiv 0 \ (mod.\ \sigma) \tag{4}$$

*genügen.*

Die Aequivalenz der Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ ist (nach §. 60 Anmerkung) gleichbedeutend mit der Annahme der Existenz zweier ganzen Zahlen $x, y$, welche die Bedingungen

$$x^2 - D'\sigma^2 y^2 = \sigma^2,$$

$$x + \beta\sigma y \equiv 0, \ -\beta\sigma x - D'\sigma^2 y \equiv 0 \ (\text{mod. } \sigma^2)$$

erfüllen; da nun aus der ersten folgt, dass $x$ durch $\sigma$ theilbar ist, und da sie durch die Substitutionen $x = \sigma t', y = u'$ in die Bedingungen (3) übergehen, aus welchen sie umgekehrt folgen, so ist der erste Theil des Satzes erwiesen. Ebenso fällt die Annahme der Aequivalenz der Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ zusammen mit der Annahme der Existenz zweier ganzen Zahlen $x, y$, welche die Bedingungen

$$\sigma^2 x^2 + 2b\sigma xy + (bb - D')y^2 = \sigma^2,$$

$$\sigma^2 x + (b + b')\sigma y \equiv 0, \ (b - b')\sigma x + (bb - D')y \equiv 0 \ (\text{mod. } \sigma^2)$$

befriedigen; da nun der Voraussetzung nach $bb - D'$ nicht durch $\sigma$ theilbar ist, so muss $y^2$ und folglich auch $y$ durch die Primzahl $\sigma$ theilbar sein; da ferner die vorstehenden Bedingungen durch die Substitution $y = \sigma u', x = t' - bu'$ in die Bedingungen (4) übergehen, aus denen sie auch rückwärts folgen, so ist auch der zweite Theil des obigen Satzes bewiesen.

*Bedeutet* $\lambda$ *die Anzahl derjenigen Formen* (1), *welche der Hauptclasse angehören, so ist* $l = r\lambda$.

Gehört die Form $(\sigma^2, \beta\sigma, \beta^2 - D')$ der Hauptclasse an, so existirt eine Lösung $(t', u')$ der Gleichung

$$t't' - D'u'u' = 1 \tag{5}$$

welche der Congruenz $t' + \beta u' \equiv 0$ (mod. $\sigma$) genügt, und folglich kann $u'$ nicht durch $\sigma$ theilbar sein. Ist umgekehrt $(t', u')$ eine Lösung der Gleichung (5), und $u'$ nicht theilbar durch $\sigma$, so existirt

stets eine und nur eine Zahlclasse $\beta$ (mod. $\sigma$), welche der Congruenz $t' + \beta u' \equiv 0$ (mod. $\sigma$) genügt, und ihr entspricht eine zur Hauptclasse gehörige Form $(\sigma^2, \beta\sigma, \beta^2 - D')$. Um also alle diese Formen zu erhalten, muss man alle Lösungen $(t', u')$ der Gleichung (5) aufstellen, in welchen $u'$ nicht durch $\sigma$ theilbar ist, und jedesmal die entsprechende Zahlclasse $\beta$ (mod. $\sigma$) durch die Congruenz $t' + \beta u' \equiv 0$ (mod. $\sigma$) bestimmen. Da ausserdem die Form $(1, 0, -D)$ zur Hauptclasse gehört, und $\lambda$ die Anzahl aller zur Hauptclasse gehörenden Formen (1) bedeutet, so ist also $\lambda - 1$ die Anzahl der sämmtlichen incongruenten Zahlclassen $\beta$ (mod. $\sigma$), welche aus Lösungen $(t', u')$ der Gleichung (5) vermöge der Congruenz $t' + \beta u' \equiv 0$ (mod. $\sigma$) erzeugt werden können.

Sind hierdurch schon alle Formen (1) erschöpft, so ist $l = \lambda$ und $r = 1$, also der Satz richtig. Giebt es aber eine nicht zur Hauptclasse gehörende ursprüngliche Form $(\sigma^2, b'\sigma, b'b' - D')$, d.h. giebt es eine von den $\lambda - 1$ Zahlclassen $\beta$ (mod. $\sigma$) verschiedene Zahlclasse $b'$ von der Beschaffenheit, dass $b'b' - D'$ nicht durch $\sigma$ theilbar ist, so wollen wir zeigen, dass unter den $l$ Formen (1) sich genau $(\lambda - 1)$ Formen $(\sigma^2, b\sigma, bb - D')$ finden, welche alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und von ihr verschieden sind. Ist nämlich $(\sigma^2, b\sigma, bb - D')$ eine solche Form, also $b - b'$ nicht durch $\sigma$ theilbar, so giebt es, wie oben gezeigt ist, eine Lösung $(t', u')$ der Gleichung (5), welche der Congruenz

$$(b - b')t' + (bb' - D')u' \equiv 0 \text{ (mod. } \sigma) \tag{4}$$

genügt, aus welcher zugleich folgt, dass $u'$ nicht durch $\sigma$ theilbar ist. Umgekehrt, ist $(t', u')$ eine Lösung der Gleichung (5), in welcher $u'$ nicht durch $\sigma$ theilbar ist, und $t' + \beta u' \equiv 0$ (mod. $\sigma$), so existirt, weil $b' - \beta$ nicht durch $\sigma$ theilbar ist, immer eine und nur eine Zahlclasse $b$ (mod. $\sigma$), welche die Congruenz

$$(b' - \beta)\, b \equiv D' - b'\beta \text{ (mod. } \sigma) \tag{6}$$

befriedigt, und zwar kann $b$ nicht $\equiv b'$ (mod. $\sigma$) sein, weil hieraus $b'b' \equiv D'$ (mod. $\sigma$) folgen würde; multiplicirt man nun (6) mit $u'$, so ergiebt sich (4), und folglich ist wirklich $(\sigma^2, b\sigma, bb - D')$ äquivalent mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ und zugleich verschieden von ihr, weil $b - b'$ nicht durch $\sigma$ theilbar ist. Um also alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalenten und von ihr verschiedenen Formen $(\sigma^2, b\sigma, bb - D')$ zu erhalten, braucht man nur die sämmtlichen $(\lambda - 1)$ Congruenzen (6) aufzustellen, welche den $(\lambda - 1)$ incongruenten Zahlclassen $\beta$ (mod. $\sigma$) entsprechen, und für

jede die entsprechende Zahlclasse $b$ zu bestimmen. Auf diese Weise entstehen aber wirklich auch $(\lambda - 1)$ verschiedene Zahlclassen $b \pmod{\sigma}$; denn wollte man annehmen, es könnte zwei verschiedenen Zahlclassen $\beta$, $\beta'$ (mod. $\sigma$) eine und dieselbe Zahlclasse $b$ (mod. $\sigma$) entsprechen, so wäre

$$(b' - \beta)b \equiv D' - b'\beta, \quad (b' - \beta')b \equiv D' - b'\beta' \pmod{\sigma};$$

hieraus würde aber durch Subtraction $(\beta' - \beta)(b - b') \equiv 0 \pmod{\sigma}$ folgen, was unmöglich ist, da weder $\beta' - \beta$ noch $b - b'$ durch $\sigma$ theilbar ist. Mithin giebt es wirklich genau $\lambda - 1$ verschiedene Formen $(\sigma^2, b\sigma, bb - D')$, welche mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und zugleich von ihr verschieden sind. Von den $l$ Formen (1) gehören daher immer je $\lambda$, und nicht mehr, zu einer und derselben Classe, folglich ist $l = r\lambda$, was zu beweisen war.

*Ist die Determinante $D = D'\sigma^2$ negativ, so ist $h$ im Allgemeinen $= lh'$, und nur dann $= \frac{1}{2}lh'$, wenn $D' = -1$.*

Denn die Gleichung (5) besitzt nur im letztern Falle Lösungen $(t' = 0, u' = \pm 1)$, in welchen $u'$ nicht durch $\sigma$ theilbar ist; da denselben nur die eine Zahlclasse $\beta \equiv 0 \pmod{\sigma}$ entspricht, so ist $\lambda = 2$, also $r = \frac{1}{2}l$; in allen anderen Fällen ist $\lambda = 1$, also $r = l$.

*Ist die Determinante $D = D'\sigma^2$ positiv, so ist $h \log(T + U\sqrt{D}) = l.h' \log(T' + U'\sqrt{D'})$, wo $(T, U)$, $(T', U')$ resp. die kleinsten positiven Auflösungen der Gleichungen $T^2 - DU^2 = 1$, $T'^2 - D'U'^2 = 1$ bedeuten.*

Um dies zu beweisen, schicken wir eine Bemerkung über die Lösungen der Gleichung (5) voraus. Wenn zwei solche Lösungen $(t', u')$, $(t'', u'')$ der Bedingung

$$t'u'' - u't'' \equiv 0 \pmod{\sigma} \tag{7}$$

genügen, so kann man, wenn $\sqrt{D'}$ und $\sqrt{D} = \sigma\sqrt{D'}$ immer positiv genommen werden,

$$t' + u'\sqrt{D'} = (t'' + u''\sqrt{D'})(t + u\sqrt{D}), \tag{8}$$

setzen, wo die ganzen Zahlen $t, u$ eine Lösung der Gleichung

$$t^2 - Du^2 = 1 \tag{9}$$

bilden. Umgekehrt, sind $(t'', u'')$, $(t, u)$ resp. Lösungen der Gleichungen (5), (9), so liefert die Gleichung (8) stets eine Lösung $(t', u')$ der Gleichung (5), welche zugleich der Bedingung (7) genügt. Je zwei solche Lösungen $(t', u')$, $(t'', u'')$ der Gleichung (5) wollen wir äquivalent nennen; dann leuchtet sofort ein, dass zwei Lö-

sungen, welche einer dritten äquivalent sind, auch einander äquivalent sein müssen. Man kann daher die sämmtlichen Lösungen der Gleichung (5) in Classen eintheilen, deren jede alle und nur solche Lösungen enthält, die unter einander äquivalent sind. Da nun die Gleichung (8) lehrt, aus einer gegebenen Lösung $(t'', u'')$ alle ihr äquivalenten Lösungen $(t', u')$ zu finden, und da $t + uV D = \pm (T + UV D)^n$ ist, wo das Vorzeichen nach Belieben, und für $n$ jede ganze Zahl gewählt werden darf (§. 85), so leuchtet ein (vergl. §. 87), dass aus jeder Classe von Lösungen ein und nur ein Repräsentant $(t', u')$ so gewählt werden kann, dass

$$1 \leqq t' + u' V D' < T + UV D$$

wird; da ferner $(T, U\sigma)$ ebenfalls eine Lösung der Gleichung (5), und folglich (§. 85)

$$T + UV D = (T' + U' V D')^{\lambda'}$$

ist, wo $\lambda'$ eine bestimmte positive ganze Zahl bedeutet, so leuchtet ein, dass die ersten Factoren $t' + u' V D'$ der obigen Repräsentanten $(t', u')$ von der Form $(T' + U' V D')^{n'}$ sind, wo $n'$ die $\lambda'$ Werthe 0, 1, 2 ... $(\lambda' - 1)$ durchlaufen muss, dass also die Anzahl der Classen $= \lambda'$ ist.

Die erste von diesen Classen enthält also die Lösungen $(t', u')$ und nur solche, deren zweite Elemente $u'$ durch $\sigma$ theilbar sind. Jede Lösung $(t', u')$ aus einer der übrigen $\lambda' - 1$ Classen liefert aber durch die Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ eine zugehörige Zahlclasse $\beta \pmod{\sigma}$, und da unmittelbar einleuchtet, dass zwei solche Lösungen stets und nur dann zu derselben Zahlclasse $\beta \pmod{\sigma}$ führen, wenn sie derselben Classe von Lösungen angehören, so muss die Anzahl $\lambda - 1$ der Zahlclassen $\beta$ mit der Anzahl $\lambda' - 1$ dieser Classen von Lösungen übereinstimmen; also ist $\lambda = \lambda'$, was zu beweisen war.

Offenbar lässt sich aus dem hier behandelten speciellen Fall ohne Schwierigkeit das in §. 100 erhaltene Resultat für den allgemeinen Fall ableiten, in welchem $\sigma$ eine beliebige zusammengesetzte Zahl ist.