SUB | NIEDERSÄCHSISCHE STAATS- UND UNIVERSITÄTSBIBLIOTHEK GÖTTINGEN

Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1857
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0053
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0053

LOG Id: LOG_0018
LOG Titel: Einige Sätze aus der Theorie der quadratischen Formen.
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

14.

Einige Sätze aus der Theorie der quadratischen Formen.

(Von Herrn *R. Lipschitz* zu Königsberg in Pr.)

§. 1.

Gaufs hat in seinen „Disquisitiones arithmeticae" den Zusammenhang untersucht, welcher zwischen der Anzahl der binären quadratischen Formen einer gegebenen Determinante, und der Anzahl der Formen einer andern besteht, die aus der ersten durch Multiplication mit dem Quadrat einer ganzen Zahl gebildet ist, und zwar durch Anwendung der Composition der Formen (S. art. 253 — 256). Nachdem *Gaufs* bewiesen hat, dafs die eine Anzahl zur andern in einem rationalen Verhältniss steht, bestimmt er dasselbe für den Fall *negativer* Determinanten, für den Fall *positiver* Determinanten aber nicht. Als darauf *Dirichlet* die Anzahl der quadratischen Formen für eine gegebene Determinante durch Bildung unendlicher Reihen ermittelte, ergab sich jene von *Gaufs* gegebene Relation, und die entsprechende für *positive* Determinanten sehr einfach aus der Betrachtung der Reihen (S. Applications de l'analyse infinitésimale à la théorie des nombres, Band XXI. dieses Journals). Indem ich mir nun die Aufgabe stellte, diese Sätze, sowohl für *negative* als für *positive* Determinanten, rein arithmetisch aus einer und derselben Quelle abzuleiten, wurde ich auf die Betrachtung der linearen Substitutionen geführt, deren sich *Gaufs* bedient hat, um entscheiden zu lehren, ob eine gegebene quadratische Form unter einer andern Form von verschiedener Determinante enthalten sei (S. Disq. arith. art. 213, 214), und ich gelangte so zur Lösung derselben. Da diese Anwendung der *Gaufs*ischen Untersuchung, so viel mir bekannt, noch nicht gemacht worden, so theile ich sie im Folgenden mit.

Es ist vortheilhaft, den besondern Fall zu untersuchen, in welchem der Quotient der verglichenen Determinanten das Quadrat einer *Primzahl* ist; denn während dadurch die Behandlung sehr vereinfacht wird, sind die Resultate so beschaffen, dafs die Sätze für den allgemeinen Fall sich sofort aus demselben ableiten lassen. Ich beginne daher mit der Betrachtung der speciellen Gattung linearer Substitutionen, welche diesem Falle entsprechen.

Es sei p eine Primzahl, und die ganzen Zahlen α, β, γ, δ mögen der Gleichung

$$(1.) \qquad \alpha\delta - \beta\gamma = p$$

genügen. Bedient man sich derselben, um zwei Variabeln x, y durch zwei neue Variabeln x', y' mittelst der Gleichungen

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y'$$

auszudrücken, so werden sie bekanntlich Substitutionscoefficienten genannt, ihr Complex heifst eine Substitution, und wird durch das Symbol $\binom{\alpha, \beta}{\gamma, \delta}$ bezeichnet. Aus diesem Gesichtspunkt betrachte man die Lösungen der Gleichung (1.), und nenne jede Lösung eine ***Substitution.***

Es seien α', β', γ', δ' ganze Zahlen, die der Gleichung

$$(2.) \qquad \alpha'\delta' - \beta'\gamma' = 1$$

genügen. Bildet man aus denselben, und den Coefficienten der Substitution $\binom{\alpha, \beta}{\gamma, \delta}$ die Gleichungen

$$(3.) \quad \begin{cases} \alpha\alpha' + \beta\gamma' = A, & \alpha\beta' + \beta\delta' = B, \\ \gamma\alpha' + \delta\gamma' = \Gamma, & \gamma\beta' + \delta\delta' = \Delta, \end{cases}$$

so erfüllen A, B, Γ, Δ die Gleichung (1.), und wir sagen: Die Substitution $\binom{A, B}{\Gamma, \Delta}$ ist der Substitution $\binom{\alpha, \beta}{\gamma, \delta}$ *aequivalent.*

Es ist oft wichtig, wenn zwei Substitutionen $\binom{A, B}{\Gamma, \Delta}$ und $\binom{\alpha, \beta}{\gamma, \delta}$ gegeben sind, zu beurtheilen, ob sie *aequivalent* sind, oder nicht. Um ein Criterium zu finden, bemerke man, dafs die Aequivalenz derselben die Existenz von 4 ganzen Zahlen α', β', γ', δ' voraussetzt, welche den Gleichungen (2.) und (3.) genügen. Aus den Gleichungen (3.) erhält man für dieselben die Werthe

$$(4.) \quad \begin{cases} \alpha' = \dfrac{\delta A - \beta\Gamma}{p}, & \beta' = \dfrac{\delta B - \beta\Delta}{p}, \\ \gamma' = \dfrac{-\gamma A + \alpha\Gamma}{p}, & \delta' = \dfrac{-\gamma B + \alpha\Delta}{p}, \end{cases}$$

an denen leicht zu sehen ist, dafs sie die Gleichung (2.) befriedigen. Es sind daher die gegebenen Substitutionen *aequivalent* oder nicht, je nachdem jene Werthe sämmtlich ganze Zahlen werden, oder nicht.

Wir machen jetzt die specielle Annahme, dafs in jeder der beiden gegebenen Substitutionen der erste und dritte Coefficient ohne gemeinschaft-

lichen Theiler seien. Dann läfst sich beweisen, dafs, wenn der Werth von γ' eine ganze Zahl ist, oder die Congruenz

$$(5.) \qquad \alpha A' - \gamma A \equiv 0 \pmod{p}$$

befriedigt wird, auch die Werthe von α', β', δ' ganze Zahlen sein müssen. Denn, verbindet man diese Congruenz mit der, aus der Beschaffenheit obiger Substitutionen folgenden

$$\alpha\delta - \gamma\beta \equiv 0 \pmod{p},$$

so folgt

$$\alpha(\delta A - \beta A') \equiv 0, \qquad \gamma(\delta A - \beta A') \equiv 0 \pmod{p},$$

und da α und γ nicht beide durch p aufgehn dürfen, so mufs

$$\delta A - \beta A' \equiv 0 \pmod{p},$$

das heifst, α' eine *ganze* Zahl sein. Ebenso schliefst man aus der Voraussetzung, dafs A und A' keinen gemeinschaftlichen Theiler haben, dafs die Werthe von β' und δ' *ganze* Zahlen werden. Es entscheidet daher die Congruenz (5.) über die *Aequivalenz* der gegebenen Substitutionen, und man kann hievon sogleich die Anwendung machen, dafs dieselben stets aequivalent sind, wenn $A = \alpha$, $A' = \gamma$ ist, was auch β, δ, B, A sein mögen. Doch ist nicht zu vergessen, dafs α und γ ohne gemeinschaftlichen Theiler vorausgesetzt sind.

Denkt man sich die sämmtlichen Substitutionen, die der Gleichung (1.) genügen, in Classen getheilt, so dafs zwei Substitutionen in dieselbe Classe kommen, oder in verschiedene, je nachdem sie aequivalent sind, oder nicht, und wählt man aus jeder Classe ein Individuum, so hat man ein System von Substitutionen, das die doppelte Eigenschaft besitzt, immer *eine* und *nur eine* Substitution zu enthalten, die irgend einer gegebenen aequivalent ist. Nun enthält jede Classe Substitutionen, deren erster und dritter Coefficient ohne gemeinschaftlichen Theiler sind. Denn es sei $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ eine Substitution, in welcher α und γ einen gemeinschaftlichen Theiler haben, so kann derselbe nur die Primzahl p sein, weil er vermöge der Gleichung $\alpha\delta - \beta\gamma = p$ in p aufgehn mufs. Dann aber müssen β und δ ohne gemeinschaftlichen Theiler sein, da $\frac{\alpha}{p}\delta - \beta\frac{\gamma}{p} = 1$ ist. Nun zeigen die Gleichungen (4.), dafs die Substitution $\begin{pmatrix} \beta, & -\alpha \\ \delta, & -\gamma \end{pmatrix}$ der Substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ aequivalent ist; also ist die obige Behauptung erwiesen. Aus diesem Grunde ist es gestattet, bei der Eintheilung der sämmtlichen Substitutionen in Classen, die Betrachtung auf diejenigen zu beschränken,

in welchen der erste und dritte Coefficient keinen gemeinschaftlichen Theiler haben. Da ferner unter dieser Voraussetzung alle Substitutionen, die denselben ersten und dritten Coefficienten haben, nach einer oben gemachten Bemerkung, aequivalent sind, was auch der zweite und vierte Coefficient sein mögen, so ist es ausreichend, jetzt nur den *ersten* und *dritten* Coefficienten der Substitutionen zu betrachten. Man darf endlich fordern, dafs der erste und dritte Coefficient der repräsentirenden Substitution einer Classe *nicht negativ* sei, da ganz allgemein die Substitutionen $\binom{\alpha, \beta}{\gamma, \delta}$ und $\binom{-\alpha, -\beta}{-\gamma, -\delta}$ aequivalent sind. Man erhält daher für irgend eine Classe einen ganz bestimmten Repräsentanten, wenn man, mit Ausschliefsung der Substitutionen, deren erster und dritter Coefficient einen gemeinschaftlichen Theiler haben, untersucht, für welche Individuen derselben der dritte Coefficient den kleinsten *nicht negativen* Werth hat, und aus diesen diejenige wählt, in welcher der erste Coefficient den kleinsten nicht negativen Werth hat.

Die Lösung dieser Aufgabe erfordert nur eine sehr einfache Discussion der Congruenz (5.); dieselbe zeigt, dafs $p+1$ Classen existiren, und giebt folgendes System repräsentirender Substitutionen:

$$\binom{1, 0}{0, p}, \binom{0, -p}{1, 0}, \binom{1, -p}{1, 0}, \binom{2, -p}{1, 0} \cdots \binom{p-1, -p}{1, 0}.$$

§. 2.

Die Transformation der binären quadratischen Formen durch lineare Substitution hat bekanntlich zu der Bemerkung geführt, dafs die Determinante der *enthaltenen* Form gleich dem Product der Determinante der *enthaltenden* Form in ein *Quadrat* ist. Es gehe die Form (a, b, c), deren Determinante $b^2 - ac = D$ ist, durch die Substitution $\binom{\alpha, \beta}{\gamma, \delta}$ in die Form (a', b', c') über, so hat man für die Coefficienten die Gleichungen

$$(1.) \quad \begin{cases} a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \\ b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta, \\ c' = a\beta^2 + 2b\beta\delta + c\delta^2, \end{cases}$$

und es wird die Determinante

$$D' = b'^2 - a'c' = D(\alpha\delta - \beta\gamma)^2.$$

Man nehme nun an, dafs $\alpha\delta - \beta\gamma = p$, eine Primzahl sei und setze ferner voraus, dafs die ganzen Zahlen a, b, c, wie auch $a, 2b, c$ keinen gemeinschaftlichen Theiler haben, so dafs die Form (a, b, c) nach der von

Dirichlet eingeführten Benennung eine Form der ersten Art ist*). Dann läfst sich zeigen, dafs der gröfste Theiler der Form (a', b', c') entweder die Einheit, oder p, oder p^2 sein mufs. Denn bildet man aus den Gleichungen (1.) die folgenden

$$(2.)\quad \begin{cases} p^2a &= a'\delta^2 - 2b'\delta\gamma + c'\gamma^2, \\ p^2b &= -a'\delta\beta + b'(\delta\alpha + \gamma\beta) - c'\gamma\alpha, \\ p^2c &= a'\beta^2 - 2b'\beta\alpha + c'\alpha^2, \end{cases}$$

so zeigen dieselben, dafs der gröfste gemeinschaftliche Theiler von a', b', c' in p^2a, p^2b, p^2c, mithin in p^2 aufgehen mufs. Es hat aber p^2 nur die Theiler $1, p, p^2$; also ist die obige Behauptung erwiesen.

Die Substitution $\binom{\alpha, \beta}{\gamma, \delta}$, mittelst deren die Form (a, b, c) in die Form (a', b', c') transformirt wird, gehört unter diejenigen, mit welchen wir uns oben beschäftigten, und es ist leicht zu beweisen, dafs aequivalente Substitutionen, auf die Form (a, b, c) angewandt, aequivalente Formen erzeugen.

Man denke sich nun die sämmtlichen Substitutionen $\binom{\alpha, \beta}{\gamma, \delta}$, für die $\alpha\delta - \beta\gamma = p$ ist, auf die Form (a, b, c) angewandt, und die hervorgehenden Formen in Classen geordnet. Dann ist es ausreichend, das System repräsentirender Substitutionen zu benutzen, um für jede Classe mindestens ***einen*** Repräsentanten zu erhalten. Die so entstehenden Formen sollen zunächst untersucht werden; und zwar wird gefragt, welche derselben den Theiler p haben.

Um dies zu entscheiden, stelle man die $p+1$ Formen wie folgt auf:

1) Durch $\binom{1, 0}{0, p}$, $\quad a' = a, \quad b' = bp, \quad c' = cp^2,$

2) Durch $\binom{\alpha, -p}{1, 0}$, $\quad a' = a\alpha^2 + 2b\alpha + c,$
$\qquad\qquad\qquad\qquad\quad b' = -(a\alpha + b)p,$
$\qquad\qquad\qquad\qquad\quad c' = ap^2,$

wo α der Reihe nach $= 0, 1, 2, \ldots p-1$ zu setzen ist.

Man stelle sich die Form (a, b, c) so eingerichtet vor, dafs ihr erster Coefficient durch p nicht theilbar sei, was immer möglich ist. Dann kann die erste Form (a, bp, cp^2) nicht den Theiler p haben. Um die andern p Formen zu beurtheilen, erwäge man, dafs b' und c' durch p aufgehn, mithin alles davon abhängt, ob a' durch p theilbar ist oder nicht. Statt a' zu untersuchen,

*) oder nach *Gaufs* eine forma *proprie primitiva* (S. *Dirichlet* applications etc. Bd. XXI p. 2 dieses Journals und disq. arith. art. 226).

betrachte man, da a relative Primzahl zu p ist, aa'. Es wird also eine Form (a', b', c') nur dann den Theiler p haben, wenn aa' durch p aufgeht, oder wenn

$$aa' = (a\alpha + b)^2 - D \equiv 0 \pmod{p}$$

ist. Da a relative Primzahl zu p ist, so reproducirt der Ausdruck $a\alpha + b$, wenn man α der Reihe nach $= 0, 1, \ldots p-1$ setzt, das System der Reste nach dem Modul p. Um also die quadratische Congruenz

$$(a\alpha + b)^2 - D \equiv 0 \pmod{p}$$

zu untersuchen, ist es zweckmäfsig, zu unterscheiden, ob p eine ungerade Primzahl, oder die Zahl Zwei ist.

Ist p eine ungerade Primzahl, so zeigen die Gleichungen (2.), dafs der gröfste gemeinschaftliche Theiler von a', $2b'$, c' auch in p^2 aufgehen mufs, dafs mithin die Form (a', b', c') nur von der *ersten* Art, oder aus einer Form der ersten Art abgeleitet sein kann. Es sind übrigens hier wieder drei Fälle zu sondern.

Geht die ungerade Primzahl p in D auf, so giebt die Congruenz (3.) für α einen Werth, der durch

$$a\alpha + b \equiv 0 \pmod{p}$$

bestimmt wird. Geht p^2 in D auf, so ist leicht zu sehen, dafs a', wenn es durch p aufgehen soll, auch durch p^2 theilbar sein mufs. Dann wird gleichfalls

$$b' = -(a\alpha + b)p \equiv 0 \pmod{p^2},$$
$$c' = ap^2 \equiv 0 \pmod{p^2},$$

mithin hat die Form (a', b', c') den gröfsten gemeinsamen Theiler p^2.

Ist D durch p *nicht* theilbar, und quadratischer *Rest* davon, so hat die Congruenz (3.) zwei Wurzeln, welche, wenn man

$$\zeta^2 \equiv D \pmod{p}$$

setzt, sich so definiren lassen:

$$a\alpha_1 + b - \zeta \equiv 0 \pmod{p},$$
$$a\alpha_2 + b + \zeta \equiv 0 \pmod{p}.$$

Es ist übrigens klar, dafs die beiden Formen, welche diesen Werthen von α entsprechen, den Theiler p^2 nicht haben können, da Dp^2 nicht durch p^4 aufgeht.

Ist D durch p *nicht* theilbar, und quadratischer *Nichtrest* von p, so hat die Congruenz (3.) keine Wurzel; sie ist unmöglich.

Beachtet man jetzt, dafs jede Form (a', b', c'), die nicht den Theiler p hat, ohne Theiler ist, so läfst sich folgendes für Formen der ersten Art gültige Resultat aussprechen:

Wenn die ungerade Primzahl p in D aufgeht, so giebt das System der $p+1$ Substitutionen p Formen ohne Theiler, und *eine* Form, deren gröfster gemeinschaftlicher Theiler p^2 oder p ist, je nachdem p^2 in D aufgeht, oder nicht.

Wenn D durch p nicht theilbar und quadratischer *Rest* von p ist, so giebt das System $p-1$ Formen ohne Theiler, und zwei Formen, deren gröfster gemeinschaftlicher Theiler p ist.

Wenn D durch p nicht theilbar und quadratischer *Nichtrest* von p ist, so giebt das System $p+1$ Formen ohne Theiler.

Wir kommen jetzt zu dem Fall, wo $p = 2$ ist.

Da hier der erste Coefficient der Form (a, b, c) ungerade angenommen wird, so ist die Form $(a, 2b, 4c)$, welche der Substitution $\binom{1, 0}{0, 2}$ entspricht, von der *ersten* Art. Diese Bezeichnung soll nämlich schon ausdrücken, dafs die betreffende Form ohne Theiler ist. Um ferner zu untersuchen, wann a' *gerade* ist, bedient man sich wie oben der Congruenz

$$(4.) \qquad aa' = (a\alpha + b)^2 - D \equiv 0 \pmod 2.$$

Denn ist a' *ungerade*, so ist die Form (a', b', c') nothwendig von der *ersten* Art.

Es sind hier wieder zwei Fälle zu unterscheiden. Ist D *gerade*, so giebt die Congruenz (4.) für ihre Wurzel die Bestimmung

$$a\alpha + b \equiv 0 \pmod 2,$$

und es ist leicht zu sehen, dafs die entsprechende Form (a', b', c') aus einer Form der ersten Art durch Multiplication mit dem Factor 2 oder 4 abgeleitet ist, je nachdem $D \equiv 2$, oder $D \equiv 0 \pmod 4$ ist. Ist D *ungerade*, so hat die Congruenz (4.) auch nur *eine* Wurzel, die durch

$$a\alpha + b \equiv 1 \pmod 2$$

bestimmt wird. Erwägt man jetzt, dafs das Quadrat einer ungeraden Zahl, durch 4 getheilt, den Rest 1 läfst, so folgt für $D \equiv 3 \pmod 4$: $a' \equiv 2$, $b' \equiv 2$, $c' \equiv 0 \pmod 4$, also (a', b', c') aus einer Form von der ersten Art durch

Multiplication mit dem Factor 2 abgeleitet; dagegen für $D \equiv 1 \pmod 4$: $a' \equiv 0$, $b' \equiv 2$, $c' \equiv 0 \pmod 4$, also (a', b', c') aus einer Form von der zweiten Art durch Multiplication mit dem Factor 2 abgeleitet. Es ergiebt sich also folgendes für Formen der ersten Art und $p = 2$ gültige Resultat:

Ist $D \equiv 2$, oder $\equiv 0 \pmod 4$, so giebt das hier aus dreien bestehende System der Substitutionen zwei Formen der ersten Art von der Determinante $4D$, und *eine* Form, die respective aus einer Form der ersten Art von der Determinante D durch Multiplication mit 2, oder aus einer Form der ersten Art von der Determinante $\frac{1}{4}D$ durch Multiplication mit 4 abgeleitet ist.

Ist $D \equiv 3$, oder $\equiv 1 \pmod 4$, so giebt das System zwei Formen der ersten Art von der Determinante $4D$, und *eine* Form, die respective aus einer Form der ersten oder zweiten Art von der Determinante D durch Multiplication mit dem Factor 2 abgeleitet ist.

Die für eine Form der ersten Art durchgeführte Untersuchung könnte man auch auf Formen der zweiten Art*) ausdehnen. Es ist aber hier nur von Interesse, den Fall zu betrachten, wo (a, b, c) eine Form der zweiten Art, und $\alpha\delta - \beta\gamma = 2$ ist.

Es sei diese Form, deren Determinante $D \equiv 1 \pmod 4$ sein mufs**), so eingerichtet, dafs a das Doppelte einer ungeraden Zahl wird. Eine Form, die durch Anwendung der Substitution $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ aus der gegebenen abgeleitet wird, gehört zur Determinante $4D$. Der gröfste gemeinschaftliche Theiler, den a', b', c' haben können, ist 2; der gröfste gemeinschaftliche Theiler, den a', $2b'$, c' haben können, ist 4. Das System, welches hier aus drei Substitutionen besteht, giebt

1) für $\begin{pmatrix} 1, 0 \\ 0, 2 \end{pmatrix}$, $\quad a' = a, \quad b' = 2b, \quad c' = 4c,$

2) für $\begin{pmatrix} \alpha, -2 \\ 1, 0 \end{pmatrix}$, $\quad a' = a\alpha^2 + 2b\alpha + c, \quad b' = -2(a\alpha + b), \quad c' = 4a,$

wo $\alpha = 0, 1$ zu setzen ist.

Man sieht, dafs die erste Form das Doppelte einer Form der ersten Art wird, da $\frac{1}{2}a'$ ungerade ist. Um zu beurtheilen, ob in den andern beiden Formen

---

*) d. h. Formen, in welchen die Zahl 2 der gröfste gemeinschaftliche Theiler von a, $2b$, c ist; nach *Gaufs* formae *improprie primitivae* (disq. arith. art. 226).

**) Siehe ebendaselbst.

a', welches immer *gerade* ist, durch 4 aufgeht oder nicht, untersuche man, ob aa' nach dem Modul 8 den Rest 0 oder 4 läfst.

Da b *ungerade*, a *gerade* ist, so ist auch $a\alpha + b$ *ungerade*, folglich $(a\alpha + b)^2 \equiv 1 \pmod 8$; mithin ist,

für $D \equiv 5 \pmod 8$, $aa' = (a\alpha + b)^2 - D \equiv 4 \pmod 8$,

für $D \equiv 1 \pmod 8$, $aa' = (a\alpha + b)^2 - D \equiv 0 \pmod 8$.

Hieraus sieht man, dafs die beiden Formen, welche den Werthen $\alpha = 0$, $\alpha = 1$ entsprechen, sich gleich verhalten.

Ist $D \equiv 5 \pmod 8$, so wird

$$a' \equiv 2 \pmod 4$$

also jede das Doppelte einer Form der ersten Art; ist $D \equiv 1 \pmod 8$, so wird

$$a' \equiv 0 \pmod 4, \quad b' \equiv 2 \pmod 4, \quad c' \equiv 0 \pmod 4,$$

also jede das Doppelte einer Form der zweiten Art. — Man hat demnach folgendes für Formen der zweiten Art und $p = 2$ gültige Resultat:

Ist $D \equiv 5 \pmod 8$, so giebt das aus dreien bestehende System der Substitutionen drei Formen, die aus Formen der ersten Art von der Determinante D durch Multiplication mit dem Factor 2 abgeleitet sind.

Ist $D \equiv 1 \pmod 8$, so giebt das System *eine* Form, die aus einer Form der ersten Art von der Determinante D, und zwei Formen, die aus Formen der zweiten Art von der Determinante D, durch Multiplication mit dem Factor 2 abgeleitet sind.

§. 3.

Nach diesen Vorbereitungen kann man den folgenden Satz beweisen:

Es sei (a', b', c') eine Form der ersten Art von der Determinante $D' = Dp^2$, wo D eine ganze Zahl, p irgend eine Primzahl bedeutet. Dann läfst sich immer eine Form der ersten Art von der Determinante D angeben, unter welcher die Form (a', b', c') eigentlich enthalten ist. Es sei (a, b, c) eine solche Form, so genügt jede Form derselben Classe der gestellten Forderung, jedoch keine Form einer anderen Classe.

Denn es sei die Substitution, vermöge deren die Form (a', b', c') unter der Form (a, b, c) enthalten ist, $\binom{\alpha, \beta}{\gamma, \delta}$, so hat man

$$(1.) \quad \begin{cases} a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \\ b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta, \\ c' = a\beta^2 + 2b\beta\delta + c\delta^2, \end{cases}$$

und hieraus leitet man ab

$$(2.)\quad \begin{cases} ap^2 = a'\delta^2 - 2b'\delta\gamma + c'\gamma^2, \\ bp^2 = a'\delta\beta + b'(\alpha\delta + \beta\gamma) - c'\gamma\alpha, \\ cp^2 = a'\beta^2 - 2b'\beta\alpha + c'\alpha^2. \end{cases}$$

Wenn also eine Form (a, b, c) existirt, aus welcher mittelst einer Substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, wo $\alpha\delta - \beta\gamma = p$, die gegebene Form (a', b', c') hergeleitet werden kann, so mufs aus der Form (a', b', c') mittelst der Substitution $\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$ die Form (ap^2, bp^2, cp^2) hergeleitet werden können.

Nun ist oben gezeigt worden, dafs das System der $p+1$ Substitutionen, auf eine Form der ersten Art von der Determinante $D' = Dp^2$ angewandt, p Formen ohne Theiler, und *eine* Form vom gröfsten Theiler p^2 giebt. Da aber eine Form ohne Theiler einer Form vom Theiler p^2 nie aequivalent werden kann, so ist klar, dafs die sämmtlichen Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, auf die genannte Form angewandt, immer eine und nur *eine* Classe von Formen erzeugen, die den Theiler p^2 haben. Es sei also (A, B, C) eine Form, die den Theiler p^2 hat, und sie sei aus der Form (a', b', c') durch die Substitution $\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$ erzeugt worden. Dann setze man

$$a = \frac{A}{p^2}, \quad b = \frac{B}{p^2}, \quad c = \frac{C}{p^2},$$

so ist (a, b, c) eine Form, unter welcher (a', b', c') enthalten ist. Denn nach der Herleitung gelten die Gleichungen (2.), von welchen die Gleichungen (1.) eine Folge sind.

Man sieht leicht, dafs jede der Form (a, b, c) aequivalente Form derselben Forderung genügt. Und umgekehrt, soll eine Form (h, i, k) jener Forderung genügen, so mufs sie mit (a, b, c) in dieselbe Classe gehören. Denn es folgt aus den Gleichungen (2.), dafs die Form (hp^2, ip^2, kp^2) zu der einfach bestimmten Classe von Formen gehört, welche aus der Form (a', b', c') erzeugt werden, und den Theiler p^2 haben, mithin der Form (ap^2, bp^2, cp^2) aequivalent ist. Es ist daher auch (h, i, k) aequivalent (a, b, c). Ganz auf dieselbe Weise beweist man den folgenden Satz:

Es sei (a', b', c') eine Form der ersten Art von der Determinante D, die $\equiv 1 \pmod 4$ ist; so läfst sich immer eine Form der zweiten Art von der Determinante D angeben, unter welcher die Form $(2a', 2b', 2c')$ eigentlich enthalten ist. Es sei (a, b, c) eine solche Form, so genügt der

gestellten Forderung jede Form derselben Classe, jedoch keine Form einer anderen.

Denn es sei die Substitution, vermöge deren die Form $(2a', 2b', 2c')$ unter der Form (a, b, c) enthalten ist, $\binom{\alpha, \beta}{\gamma, \delta}$, wo $\alpha\delta - \beta\gamma = 2$ ist, so hat man

$$(3.) \quad \begin{cases} 2a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \\ 2b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta, \\ 2c' = a\beta^2 + 2b\beta\delta + c\delta^2, \end{cases}$$

woraus die Gleichungen

$$(4.) \quad \begin{cases} 2a = a'\delta^2 - 2b'\delta\gamma + c'\gamma^2, \\ 2b = -a'\delta\beta + b'(\alpha\delta + \beta\gamma) - c'\gamma\alpha, \\ 2c = a'\beta^2 - 2b'\beta\alpha + c'\alpha^2 \end{cases}$$

folgen. Es ist jetzt nur von dem Satze Gebrauch zu machen *), dafs sämmtliche Substitutionen $\binom{\alpha, \beta}{\gamma, \delta}$, wo $\alpha\delta - \beta\gamma = 2$ ist, auf eine Form der ersten Art, deren Determinante $D \equiv 1 \pmod 4$ ist, angewendet, immer eine und *nur eine* Classe von Formen geben, die aus einer Form der zweiten Art von der Determinante D, durch Multiplication mit dem Factor 2 abgeleitet sind. Dann folgt Alles, wie vorhin.

§. 4.

Es sei $\varphi_1, \varphi_2, \ldots \varphi_h$ das vollständige System der Formen erster Art von der Determinante D; es sei p irgend eine Primzahl; man wende auf die Form φ_1 die sämmtlichen Substitutionen $\binom{\alpha, \beta}{\gamma, \delta}$ an, wo $\alpha\delta - \beta\gamma = p$ ist, und unterwerfe die daraus hervorgehenden Formen der Bedingung, ohne Theiler zu sein. Diese Formen, zur Determinante $D' = Dp^2$ gehörig, und von der ersten Art, ordne man in Classen, und wähle für jede Classe einen Repräsentanten; ebenso verfahre man der Reihe nach mit den Formen $\varphi_2, \varphi_3, \ldots \varphi_h$: so behaupte ich, dafs die respräsentirenden Formen ein vollständiges System der Formen erster Art, von der Determinante D', bilden.

Denn wollte man annehmen, dafs dieselbe Form zwei Mal erscheint, so müfste sie unter zwei verschiedenen Formen des Systems $\varphi_1, \varphi_2, \ldots \varphi_h$ enthalten sein, was nach dem ersten in §. 3 aufgestellten Satz unmöglich ist.

---

*) Derselbe bildet einen Theil des zweiten in §. 2 ausgesprochenen Resultats.

Oder wollte man annehmen, dafs eine Form fehlt, so müfste diese Form nach demselben Satz dennoch unter einer ganz bestimmten Form des Systems φ_1, φ_2, ... φ_h enthalten sein; was einen Widerspruch giebt.

Auf ganz analogen Gründen beruht der folgende Satz:

Es sei φ_1, φ_2, ... $\varphi_{h'}$ das vollständige System der Formen zweiter Art von der Determinante D. Man wende auf die Form φ_1 die sämmtlichen Substitutionen $\binom{\alpha, \beta}{\gamma, \delta}$ an, wo $\alpha\delta - \beta\gamma = 2$ ist, und unterwerfe die daraus hervorgehenden Formen der Bedingung, aus Formen der ersten Art durch Multiplication mit dem Factor 2 abgeleitet zu sein. Diese Formen, zur Determinante $4D$ gehörig, ordne man in Classen, und wähle für jede Classe einen Repräsentanten; ebenso verfahre man der Reihe nach mit den Formen φ_2, φ_3, ... $\varphi_{h'}$: so behaupte ich, dafs die repräsentirenden Formen ein vollständiges System der Formen erster Art von der Determinante D bilden, jede Form mit dem Factor 2 multiplicirt.

§. 5.

Um aus den Sätzen des vorigen Paragraphen weitere Schlüsse zu ziehen, ist es nöthig, folgende Aufgabe zu lösen:

Es sei $\varphi = (a, b, c)$ eine Form der ersten Art von der Determinante D: man soll die sämmtlichen Formen (a', b', c'), die aus derselben durch alle Substitutionen $\binom{\alpha, \beta}{\gamma, \delta}$, wo $\alpha\delta - \beta\gamma = p$, abgeleitet werden können und die ohne Theiler sind, in Classen ordnen, und die Anzahl der Classen angeben.

Wie oben bemerkt, ist es nur nöthig das System der $p+1$ Substitutionen*) anzuwenden, um sicher zu sein, dafs keine Classe unvertreten bleibe; auch hat sich gezeigt, dafs unter diesen $p+1$ Formen diejenigen, welche ohne Theiler sind, Formen der ersten Art werden, d. h. dafs sobald a', b', c' ohne gemeinschaftlichen Theiler sind, dasselbe auch für a', $2b'$, c' der Fall ist. Die Substitutionen, welche solche Formen geben, sind in §. 2 bestimmt worden und das für ihre Anzahl k daselbst gefundene Ergebnifs kann wie folgt in Zeichen zusammengefafst werden:

Wenn p eine ***ungerade*** Primzahl ist, die in D nicht aufgeht, und das Zeichen $\left(\frac{D}{p}\right)$ die positive oder negative Einheit bedeutet, je nachdem D

*) Siehe §. 1 zu Ende.

quadraticher Rest oder Nichtrest von p ist, so erhält man

$$k = p - \left(\frac{D}{p}\right).$$

Ist dagegen p eine *ungerade* Primzahl, die in D aufgeht, oder die Zahl 2, so ist

$$k = p.$$

Es sei nun aus der gegebenen Form $\varphi = (a, b, c)$ die Reihe der k Formen ohne Theiler, von der Determinante $D' = Dp^2$ abgeleitet:

$$(1.) \quad f_1, \; f_2, \; \ldots \; f_k,$$

so bedarf es eines Mittels zu beurtheilen, welche von diesen Formen einer bestimmten Form f unter denselben aequivalent sind.

Gesetzt es sei die Form f_1 der Form f aequivalent, so dafs f_1 durch die Substitution $\left(\begin{smallmatrix}\alpha', \beta' \\ \gamma', \delta'\end{smallmatrix}\right)$, wo $\alpha'\delta' - \beta'\gamma' = 1$, in f übergeht; es sei ferner f aus φ durch die zu dem oben aufgestellten System gehörige Substitution $\left(\begin{smallmatrix}\alpha, \beta \\ \gamma, \delta\end{smallmatrix}\right)$, f_1 aus φ durch die ebenfalls zum oben aufgestellten System gehörige Substitution $\left(\begin{smallmatrix}\alpha_1, \beta_1 \\ \gamma_1, \delta_1\end{smallmatrix}\right)$ entstanden. Da durch die Substitution $\left(\begin{smallmatrix}\alpha_1, \beta_1 \\ \gamma_1, \delta_1\end{smallmatrix}\right)$ die Form φ in die Form f_1, durch die Substitution $\left(\begin{smallmatrix}\alpha', \beta' \\ \gamma', \delta'\end{smallmatrix}\right)$ die Form f_1 in f transformirt wird, so bilde man die Ausdrücke:

$$\begin{aligned} \alpha_1\alpha' + \beta_1\gamma' &= A, & \alpha_1\beta' + \beta_1\delta' &= B, \\ \gamma_1\alpha' + \delta_1\gamma' &= \Gamma, & \gamma_1\beta' + \delta_1\delta' &= \Delta, \end{aligned}$$

und die Substitution $\left(\begin{smallmatrix}A, B \\ \Gamma, \Delta\end{smallmatrix}\right)$ transformirt die Form φ in die Form f. Diese Substitution ist aequivalent der Substitution $\left(\begin{smallmatrix}\alpha_1, \beta_1 \\ \gamma_1, \delta_1\end{smallmatrix}\right)$, durch welche die Form φ in f_1 übergeht. Denkt man sich also die sämmtlichen Substitutionen aufgestellt, durch welche die Form φ in f übergeht, so mufs sich die Substitution $\left(\begin{smallmatrix}A, B \\ \Gamma, \Delta\end{smallmatrix}\right)$, welche der Substitution $\left(\begin{smallmatrix}\alpha_1, \beta_1 \\ \gamma_1, \delta_1\end{smallmatrix}\right)$ aequivalent ist, unter denselben befinden.

Diese Betrachtung führt zu folgendem Verfahren:

Es ist gezeigt worden, dafs aus *einer* gegebenen Substitution $\left(\begin{smallmatrix}\alpha, \beta \\ \gamma, \delta\end{smallmatrix}\right)$, die von der Form φ zur Form f führt, die sämmtlichen ähnlichen Substitutionen abgeleitet werden können (*Gaufs* disq. arith. art. 162). Nachdem dieselben aufgestellt worden, ordne man sie in Classen, und wähle die Repräs-

sentanten aus dem System der $p+1$ Substitutionen. Es sei z. B. der Repräsentant einer dieser Classen $\binom{\alpha_\lambda, \beta_\lambda}{\gamma_\lambda, \delta_\lambda}$, so ist leicht zu sehen, dafs die Form f_λ der Form f aequivalent ist; und so ergiebt jede Substitutions-Classe eine Form aus der Reihe

$$f_1, \quad f_2, \quad \ldots \quad f_k$$

mit der die betrachtete Form f aequivalent ist. Nähme man an, dafs aufser den so gefundenen Formen noch eine Form der Form f aequivalent werde, so würde ein Widerspruch entstehen. Denn es sei diese Form f_1, so ist oben gezeigt worden, dafs unter den sämmtlichen Substitutionen, die φ in f transformiren, *eine* Substitution $\binom{A, B}{\Gamma, \Delta}$ sich finden mufs, deren aus dem System der $p+1$ Substitutionen genommener Repräsentant $\binom{\alpha_1, \beta_1}{\gamma_1, \delta_1}$ ist.

Es ist jetzt zunächst folgende Untersuchung anzustellen:

Die Form $\varphi = (a, b, c)$ gehe durch die Substitution unseres Systems $\binom{\alpha, \beta}{\gamma, \delta}$ in die Form $f = (a', b', c')$ über, welche zur Determinante $D' = Dp^2$ gehört, ohne Theiler und von der ersten Art ist. Dann erhält man die sämmtlichen ähnlichen Substitutionen durch die Ausdrücke *)

$$(2.) \quad \begin{cases} A = \alpha t - (\alpha b + \gamma c) u, \\ B = \beta t - (\beta b + \delta c) u, \\ \Gamma = \gamma t + (\alpha a + \gamma b) u, \\ \Delta = \delta t + (\beta a + \delta b) u, \end{cases}$$

wo t, u alle ganzen Zahlen sind, die der unbestimmten Gleichung

$$(3.) \quad t^2 - Du^2 = 1$$

genügen. Diese Substitutionen $\binom{A, B}{\Gamma, \Delta}$ sollen in Classen geordnet, und die Anzahl der Classen soll angegeben werden.

Um jetzt für die Aequivalenz zweier Substitutionen das Criterium (5.) des §. 1 anwenden zu können, ist es nöthig zu zeigen, dafs im gegenwärtigen Falle der erste und dritte Substitutionscoefficient nicht gleichzeitig durch p aufgehen. Es ist aber in unserm System von Substitutionen $\beta \equiv 0$, $\delta \equiv 0 \pmod{p}$, folglich vermöge der Gleichungen (2.), auch $B \equiv 0$,

*) Sie sind in den von *Gaufs* (disq. arith. art. 162 pag. 181) gegebenen als specieller Fall enthalten, da hier der gröfste gemeinschaftliche Theiler von a', $2b'$, c', also nach *Gaufs* die mit m bezeichnete Zahl, $= 1$ ist.

$\Delta \equiv 0 \pmod{p}$. Daher hat man die Gleichung

$$A\frac{\Delta}{p} - \frac{B}{p}I' = 1,$$

so dafs A und I' ohne gemeinschaftlichen Theiler sein müssen.

Es seien nun $\begin{pmatrix} A, B \\ \Gamma, \Delta \end{pmatrix}$ und $\begin{pmatrix} A', B' \\ \Gamma', \Delta' \end{pmatrix}$ Substitutionen, die respective den Lösungen t, u und t', u' der unbestimmten Gleichung (3.) entsprechen. Dieselben werden (nach §. 1 Gl. (5.)) aequivalent sein, oder nicht, je nachdem die Congruenz

$$AI'' - A'I' \equiv 0 \pmod{p}$$

befriedigt wird, oder nicht. Setzt man für A, I', A', I'' ihre Werthe aus den Gleichungen (2.), so geht dieselbe in

$$a'(tu' - t'u) \equiv 0 \pmod{p}$$

über, und, da die Form (a', b', c') so beschaffen ist, dafs a' durch p nicht aufgeht *), so läfst sich die Congruenz ersetzen durch

$$(4.) \qquad tu' - t'u \equiv 0 \pmod{p}.$$

Man sieht sogleich, dafs entgegengesetzte Lösungen, wie t, u und $-t$, $-u$ aequivalente Substitutionen geben. Für das Weitere ist es aber nöthig zu unterscheiden, ob die Determinante *negativ* oder *positiv* ist.

I. Die Determinante D sei *negativ*, und ihr absoluter Werth gröfser als die Einheit; dann hat die Gleichung (3.) nur die beiden Lösungen $t = \pm 1$, $u = 0$, welche *eine* Classe von Substitutionen geben.

Ist die Determinante $D = -1$, so hat die unbestimmte Gleichung

$$t^2 + u^2 = 1,$$

aufser den Lösungen $t = \pm 1$, $u = 0$, welche eine Classe von Substitutionen geben, die beiden $t = 0$, $u = \pm 1$, welche auch *nur eine* Classe geben. Die entscheidende Congruenz (4.) zeigt aber, dafs diese beiden Classen von einander verschieden sind.

II. Die Determinante D sei *positiv*, so sind die sämmtlichen Lösungen der Gleichung (3.) in der Formel

$$t_n + u_n\sqrt{D} = \pm(T + U\sqrt{D})^n$$

*) Es hat sich nämlich (§. 2, zu Anfang) gezeigt, dafs sämmtliche aus der Anwendung des Systems der $p+1$ Substitutionen hergeleiteten Werthe von b', c' durch p theilbar sind, sodafs, in den hier betrachteten k Formen ohne Theiler, a' zu p relative Primzahl sein mufs.

enthalten, wo T, U die kleinsten positiven Werthe sind, welche derselben genügen, n aber alle ganzen Zahlen von $-\infty$ bis $+\infty$ bedeutet. Zu Folge einer oben gemachten Bemerkung genügt es für den gegenwärtigen Zweck diejenigen Lösungen zu betrachten, für welche in dieser Gleichung das Pluszeichen zu nehmen ist.

Die Determinante der Form $f=(a', b', c')$ ist $D'=Dp^2$. Bezeichnet man die kleinsten positiven Werthe, die der unbestimmten Gleichung

$$t'^2 - D'u'^2 = 1$$

genügen, durch T', U', so sind T', pU' Lösungen der unbestimmten Gleichung (3.); und da pU' *positiv* ist, so mufs ein positiver Index ϱ existiren, für welchen

$$(T+U\sqrt{D})^{\varrho} = T'+U'\sqrt{D'}$$

ist. Man sieht leicht, dafs ϱ der kleinste positive Exponent ist, für welchen der Werth u durch p theilbar wird, und dafs, wenn $m\varrho$ irgend ein Vielfaches von ϱ bedeutet,

$$t_{m\varrho}+u_{m\varrho}\sqrt{D} = (T+U\sqrt{D})^{m\varrho} = (T'+U'\sqrt{D'})^{m},$$

mithin $u_{m\varrho}$ auch durch p theilbar ist.

Ich behaupte jetzt, dafs wenn man in der Formel

$$t_{\mu}+u_{\mu}\sqrt{D} = (T+U\sqrt{D})^{\mu}$$

der Reihe nach $\mu=0, 1, 2, \ldots \varrho-1$ setzt, die daraus entstehenden ϱ Lösungen der unbestimmten Gleichung (3.) die doppelte Eigenschaft haben, dafs nicht zwei verschiedene unter ihnen vorkommen, für welche

$$tu'-t'u \equiv 0 \pmod{p}$$

würde, und dafs für jede beliebige Lösung $t_{\mu'}$, $u_{\mu'}$ eine Lösung t_{μ}, u_{μ} aus jener Reihe der ϱ Lösungen angegeben werden kann, so dafs

$$t_{\mu}u_{\mu'}-t_{\mu'}u_{\mu} \equiv 0 \pmod{p}$$

ist.

Um den zweiten Punct zuerst zu erledigen, nehme man für das gegebene μ' den Werth μ als seinen Rest nach dem Modul ϱ, aus dem System $0, 1, 2, \ldots \varrho-1$. Dann ist also $\mu'-\mu$ ein Vielfaches von ϱ, und $u_{\mu'-\mu}\equiv 0 \pmod{p}$. Bildet man nun die Ausdrücke:

$$\begin{aligned} t_{\mu'-\mu}+u_{\mu'-\mu}\sqrt{D} &= (T+U\sqrt{D})^{\mu'}(T+U\sqrt{D})^{-\mu} \\ &= (t_{\mu'}+u_{\mu'}\sqrt{D})(t_{\mu}-u_{\mu}\sqrt{D}) \\ &= t_{\mu'}t_{\mu}-Du_{\mu'}u_{\mu}+(t_{\mu}u_{\mu'}-t_{\mu'}u_{\mu})\sqrt{D}, \end{aligned}$$

so erhält man

$$u_{\mu'-\mu} = t_\mu u_{\mu'} - t_{\mu'} u_\mu \equiv 0 \pmod{p};$$

was gezeigt werden sollte.

Wollte man aber annehmen, dafs es unter den aufgestellten ϱ Lösungen zwei gäbe, die der Congruenz (4.) genügen, und es seien die beiden Indices derselben μ' und μ, wo $\mu' \geqq \mu$, so würde man zu dem Schlufs gelangen, dafs

$$u_{\mu'-\mu} \equiv 0 \pmod{p}$$

sein mufs. Da aber der Annahme gemäfs ϱ der kleinste positive Index ist, für welchen $u \equiv 0 \pmod{p}$ wird, und sowohl μ' als μ positiv und $< \varrho$ sein sollen, so mufs $\mu' - \mu = 0$ sein, d. h. die beiden Lösungen sind identisch.

Man hat demnach das Resultat, dafs die aufgestellten ϱ Lösungen ϱ von einander verschiedene Substitutionen der Form φ in die Form f geben, welche die sämmtlichen Substitutionen dieser Art repräsentiren; oder, die Anzahl der Classen von Substitutionen, welche man erhält, ist

$$\varrho = \frac{\log(T' + U'\sqrt{D'})}{\log(T + U\sqrt{D})}.$$

Man sieht, dafs die Anzahl der Classen, in welche die sämmtlichen Substitutionen $\binom{A, B}{I, \Delta}$, vermöge deren eine Form φ in eine Form f übergeht, zerfallen, nur von der Determinante D und der Primzahl p abhängt. Diese Anzahl bestimmt aber, wieviel Formen aus der Reihe

$$f_1, \quad f_2, \quad f_3, \quad \ldots \quad f_k$$

einer derselben f aequivalent sind. Es müssen also, da D und p in allen dieselben Werthe haben, jeder Form gleichviel Formen aequivalent sein, oder: die oben bestimmte Anzahl der aequivalenten Formen mufs in k aufgehn. Es läfst sich daher die Anzahl der wesentlich verschiedenen Formen aus jener Reihe, die mit l bezeichnet werden möge, angeben.

I. Wenn die Determinante D ***negativ*** ist, so wird, wenn sie numerisch gröfser als 1 ist,

$$l = k;$$

für den besondern Fall $D = -1$,

$$l = \frac{k}{2}.$$

II. Wenn die Determinante D ***positiv*** ist, so wird

$$l = \frac{\log(T + U\sqrt{D})}{\log(T' + U'\sqrt{D'})} k.$$

Um diese Sätze mit dem ersten Satze in diesem §. verbinden zu können, bemerke man, dafs der Werth k auch nur von der Determinante D und der Primzahl p abhängt, und nicht individuell von der Form $\varphi = (a, b, c)$. Es wird also aus jeder der Formen $\varphi_1, \varphi_2, \ldots \varphi_h$ dieselbe Anzahl von Formen ohne Theiler von der Determinante $D' = Dp^2$ erzeugt. Ist daher h die Anzahl der Formen erster Art von der Determinante D, h' die Anzahl der Formen erster Art von der Determinante $D' = Dp^2$, so ergiebt sich die Beziehung, dafs h' und h in einem angebbaren Verhältnifs stehen, und zwar dafs

$$h' = hl$$

ist. Durch successive Anwendung dieses Satzes ist man im Stande, folgendes allgemeine Resultat herzuleiten:

Es sei h die Anzahl der Formen erster Art von der Determinante D, ferner h' die Anzahl der Formen erster Art von der Determinante $D' = DS^2$, wo S irgend eine Zahl bedeutet, es seien $r, r', r'' \ldots$ die ungeraden Primzahlen, die in D' aufgehen, ohne D zu theilen, und es bezeichne das Symbol $\Pi F(r)$ die Bildung eines auf die Primzahlen $r, r', r'' \ldots$ auszudehnenden Products, so ist für eine *negative* Determinante:

$$h' = hS\Pi\left(1-\left(\frac{D}{r}\right)\frac{1}{r}\right).$$

In dem Fall, wo $D = -1$, ist indefs die linke Seite zu verdoppeln.

Für eine *positive* Determinante dagegen hat man, wenn T, U und T', U' die kleinsten positiven Werthe sind, die resp. den Gleichungen $t^2 - Du^2 = 1$, $t'^2 - D'u'^2 = 1$ genügen:

$$h' = hS\frac{\log(T+U\sqrt{D})}{\log(T'+U'\sqrt{D'})}\Pi\left(1-\left(\frac{D}{r}\right)\frac{1}{r}\right).$$

(Man vergleiche die in §. 1 angeführte *Dirichlet*sche Abhandlung, Bd. XXI pag. 12 dieses Journals.)

§. 6

Um aus dem zweiten Satze des §. 4 ähnliche Resultate zu erhalten, ist folgende Aufgabe zu lösen:

Es sei $\varphi = (a, b, c)$ eine Form der zweiten Art, von der Determinante D: man soll die Formen, welche durch Anwendung der sämmtlichen Substitutionen $\left(\begin{smallmatrix}\alpha, \beta\\ \gamma, \delta\end{smallmatrix}\right)$, wo $\alpha\delta - \beta\gamma = 2$ ist, erzeugt werden, und der Bedingung genügen, aus Formen der ersten Art von der Determinante D durch Multiplication mit

dem Factor 2 abgeleitet zu sein, in Classen ordnen, und die Anzahl der Classen angeben.

Der Untersuchung des §. 2 und dem daselbst ausgesprochenen dritten Resultat gemäfs ist hier, wo unter allen Umständen $D \equiv 1 \pmod 4$ sein mufs, zu unterscheiden, ob $D \equiv 1$, oder $\equiv 5 \pmod 8$. Im ersten Fall, wenn $D \equiv 1 \pmod 8$, giebt das oben aufgestellte System von Substitutionen nur *eine* Form von der vorgeschriebenen Beschaffenheit, also existirt immer nur *eine* solche Classe von Formen. Ist dagegen $D \equiv 5 \pmod 8$, so giebt das System von Substitutionen drei Formen von der verlangten Beschaffenheit, deren Aequivalenz beurtheilt werden mufs. Um aber die Betrachtungen des vorigen Paragraphen nicht zu wiederholen, kann man sogleich folgende Frage stellen:

Die Form $\varphi = (a, b, c)$ gehe durch die zum aufgestellten System gehörige Substitution $\left(\begin{smallmatrix}\alpha, \beta\\ \gamma, \delta\end{smallmatrix}\right)$ in die Form f über, welche aus einer Form der ersten Art von der Determinante D durch Multiplication mit dem Factor 2 abgeleitet ist; dann erhält man die sämmtlichen ähnlichen Substitutionen durch die Ausdrücke

$$(1.)\quad \begin{cases} A = \dfrac{\alpha t - (\alpha b + \gamma c)u}{2}, \\ B = \dfrac{\beta t - (\beta b + \delta c)u}{2}, \\ \Gamma = \dfrac{\gamma t + (\alpha a + \gamma b)u}{2}, \\ \Delta = \dfrac{\delta t + (\beta a + \delta b)u}{2}, \end{cases}$$

wo t, u sämmtliche Zahlen sind, die der unbestimmten Gleichung

$$(2.)\quad t^2 - Du^2 = 4$$

genügen; wieviel verschiedene Classen geben diese Substitutionen $\left(\begin{smallmatrix}A, B\\ \Gamma, \Delta\end{smallmatrix}\right)$?

Ehe diese Frage beantwortet wird, ist zu bemerken, dafs der Nachweis, dafs A, B, Γ, Δ *ganze* Zahlen werden, für diesen Fall von *Gaufs* (Disq. arith. art. 162) nicht gegeben ist. Doch läfst sich, ebenso wie dort, zeigen, dafs, da $\varphi = (a, b, c)$ eine Form der zweiten Art ist, die Ausdrücke $\frac{t - bu}{2}$, $\frac{t + bu}{2}$ *ganze* Zahlen sind. Daraus folgt dann auch, da in dem aufgestellten Substitutions-System $\beta \equiv 0$, $\delta \equiv 0 \pmod 2$, dafs $B \equiv 0$, $\Delta \equiv 0 \pmod 2$, folglich A und Γ ohne Theiler sind. Es seien $\left(\begin{smallmatrix}A, B\\ \Gamma, \Delta\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}A', B'\\ \Gamma', \Delta'\end{smallmatrix}\right)$

Substitutionen, die resp. den Lösungen t, u und t', u' der Gleichung (2.) entsprechen, so werden dieselben aequivalent sein, oder nicht, je nachdem der Congruenz

$$AT' - A'T \equiv 0 \pmod 2$$

genügt wird oder nicht. Setzt man hier die Werthe aus den Gleichungen (1.) ein, so ergiebt sich:

$$a' \frac{tu' - t'u}{4} \equiv 0 \pmod 2,$$

oder, da a' das Doppelte einer ungeraden Zahl ist: *)

$$(3.) \quad tu' - t'u \equiv 0 \pmod 4.$$

Ganz wie im Fall des vorigen §. sieht man, dafs Lösungen wie t, u und $-t$, $-u$ aequivalente Substitutionen geben; und auch hier ist der Fall einer *positiven* Determinante und der einer *negativen* zu sondern.

I. Ist die Determinante *negativ*, und $-D > 3$, so hat die unbestimmte Gleichung (2.) nur die beiden Lösungen $t = \pm 2$, $u = 0$, welche *einer* Classe von Substitutionen angehören.

Ist $D = -3$, so hat die unbestimmte Gleichung

$$t^2 + 3u^2 = 4$$

die 6 Lösungen $t = \pm 2$, $u = 0$; $t = \pm 1$, $u = 1$; $t = \pm 1$, $u = -1$. Je zwei derselben geben zufolge einer oben gemachten Bemerkung dieselbe Classe von Substitutionen. Die Lösungen $t = 2$, $u = 0$; $t = 1$, $u = 1$; $t = 1$, $u = -1$ bezeichnen aber drei verschiedene Classen.

II. Ist die Determinante D *positiv*, so werden die sämmtlichen Lösungen der unbestimmten Gleichung (2.) wie folgt ausgedrückt:

$$\frac{t_n + u_n \sqrt{D}}{2} = \pm \left(\frac{T' + U' \sqrt{D}}{2} \right)^n,$$

wo T' und U' die kleinsten positiven Werthe sind, welche derselben genügen, und n alle ganzen Zahlen von $-\infty$ bis $+\infty$ bedeutet. Zufolge der oben gemachten Bemerkung ist es ausreichend, das obere *positive* Zeichen zu nehmen.

Es sind nun zwei Fälle zu unterscheiden.

---

*) Die Gründe hierfür sind denen analog, nach welchen a' im Fall des vorigen §. ungerade war. In allen drei Substitutionen, aus welchen hier das System derselben besteht, da $p = 2$, haben nämlich $2b'$ und c' den gemeinschaftlichen Theiler 4; also kann (a', b', c') nicht das Doppelte einer Form der ersten Art sein, ohne dafs a' das Doppelte einer ungeraden Zahl ist.

Wenn U' *gerade* ist, so mufs vermöge der Gleichung

$$T'^2 - DU'^2 = 4,$$

auch T' *gerade* sein. Dann sind $\frac{T'}{2}$, $\frac{U'}{2}$ die kleinsten positiven Werthe der unbestimmten Gleichung

$$T^2 - DU^2 = 1,$$

und man hat

$$\frac{t_n + u_n\sqrt{D}}{2} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^n = (T + U\sqrt{D})^n;$$

folglich wird jedes u *gerade,* und deshalb auch jedes t *gerade,* also die Congruenz (3.) immer befriedigt, und es existirt nur *eine* Classe von Substitutionen.

Ist dagegen U' *ungerade,* so ist bemerkt worden (S. die angeführte Abhandlung von *Dirichlet* Bd. XXI pag. 11 dieses Journals), dafs der Exponent 3 den Werth u_3 immer *gerade* macht, und dafs es der kleinste ist, der dies bewirkt. Setzt man

$$\frac{t_3 + u_3\sqrt{D}}{2} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^3 = T + U\sqrt{D},$$

so sind daher T, U die kleinsten positiven Werthe der unbestimmten Gleichung $t^2 - Du^2 = 1$.

Man kann nun, ganz wie im vorigen Paragraph, beweisen, dafs, wenn man in der Formel

$$\frac{t_\mu + u_\mu\sqrt{D}}{2} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^\mu$$

μ der Reihe nach $= 0, 1, 2$ setzt, die drei entstehenden Lösungen so beschaffen sind, dafs nicht

$$tu' - t'u \equiv 0 \pmod 4$$

werden kann, aufser wenn $t = t'$, $u = u'$ ist. Diese drei Lösungen geben also drei von einander verschiedene Classen von Substitutionen, und mehr Classen existiren nicht; also müssen sich die sämmtlichen Substitutionen unter diese drei repräsentirende vertheilen, was auch direct gezeigt werden kann.

Die Anzahl der Classen, in welche die sämmtlichen ähnlichen Substitutionen zerfallen, welche, je nachdem U' gerade oder ungerade, $= 1$ oder $= 3$ ist, läfst sich durch eine und dieselbe Formel darstellen. Diese Formel kann sogar den Fall $D \equiv 1 \pmod 8$ umfassen, wo immer nur *eine* Classe existirt, und die unbestimmte Gleichung

$$t^2 - Du^2 = 4,$$

nur durch ein *gerades* u befriedigt werden kann.

Nennt man nämlich T', U' die kleinsten positiven Werthe, welche dieser Gleichung, T, U die kleinsten positiven Werthe, die der Gleichung $t^2 - Du^2 = 1$ genügen, so ist jene Anzahl

$$= \frac{\log(T + U\sqrt{D})}{\log\frac{1}{2}(T' + U'\sqrt{D})}.$$

Man sieht, dafs die Anzahl von Classen, in welche die sämmtlichen Substitutionen $\left(\begin{smallmatrix} A, & B \\ \Gamma, & \Delta \end{smallmatrix}\right)$ zerfallen, immer nur von der Determinante D abhängt. Man findet daher für die Anzahl l der Classen, welche die aus der Form der zweiten Art $\varphi = (a, b, c)$ auf die vorgeschriebene Art erzeugten Formen bilden, vermöge ganz derselben Betrachtung wie oben, folgendes Resultat:

I. Ist die Determinante D *negativ*, und numerisch gröfser als 3, so wird

$$l = 1, \quad D \equiv 1 \pmod 8; \quad l = 3, \quad D \equiv 5 \pmod 8.$$

Für die Determinante $D = -3$ aber ist

$$l = 1.$$

II. Ist die Determinante D *positiv*, so hat man

$$l = \frac{\log\frac{1}{2}(T' + U'\sqrt{D})}{\log(T + U\sqrt{D})}, \qquad D \equiv 1 \pmod 8;$$

$$l = 3\frac{\log\frac{1}{2}(T' + U'\sqrt{D})}{\log(T + U\sqrt{D})}, \qquad D \equiv 5 \pmod 8.$$

Erwägt man nun, dafs der Werth von l gar nicht individuell von der Form $\varphi = (a, b, c)$ abhängt, sondern nur von der Determinante D, so giebt die Verbindung dieser Resultate mit dem zweiten Satze des §. 4 den Schlufs, dafs jede Form des Systems $\varphi_1, \varphi_2, \ldots \varphi_{h'}$ dieselbe Anzahl von Formen erzeugt, welche aus Formen der ersten Art von der Determinante D durch Multiplication mit dem Factor 2 entstanden sind, und so gelangt man zu folgendem Satz:

Es sei h die Anzahl der Formen erster Art von der Determinante D, h' die Anzahl der Formen zweiter Art von derselben Determinante, die immer $\equiv 1 \pmod 4$ sein mufs, so existirt zwischen h und h' die Relation

$$h = h'l.$$

(Man vergleiche die angeführte *Dirichlet*sche Abhandlung Bd. XXI pag. 10 dieses Journals.)

Königsberg in Pr. im November 1854.