

UNTERSUCHUNGEN ÜBER QUADRATISCHE FORMEN.

I. BESTIMMUNG DER ANZAHL VERSCHIEDENER FORMEN,  
WELCHE EIN GEGEBENES GENUS ENTHÄLT.

VON

HERMANN MINKOWSKI

in KOENIGSBERG <sup>1</sup>/Pr.

In meiner Arbeit »*Sur la théorie des formes quadratiques à coefficients entiers*»<sup>1</sup> habe ich den Begriff des Genus lediglich aus dem Begriffe der Formencongruenz hergeleitet. Ein solches Verfahren erwies sich bereits dort als äusserst vortheilhaft. Seine Berechtigung wird vielleicht noch schärfer durch die folgenden Entwicklungen hervortreten. Ich werde mich hier mit jenen Zahlen beschäftigen, welche im Falle allgemeiner Genera dieselbe Rolle spielen, wie im Falle binärer Genera die Classenzahlen. Gewisse Sätze über Formencongruenzen werden zunächst errathen lassen, in welcher Gestalt sich die Ausdrücke jener Zahlen darbieten müssen. Unter Anwendung DIRICHLET'scher Principien soll alsdann gezeigt werden, dass die errathenen Formeln in Wirklichkeit richtig sind.

---

<sup>1</sup> Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut de France. Tome XXIX, N° 2 (1884). — Ich citire diese Arbeit im Folgenden kurz mit *P. Q.*

## Einleitung.

### 1. *Ein Genus und seine Formenanzahl.*

Unter den *Resten* einer quadratischen Form  $f = \sum_1^n a_{ik} x_i x_k$  in Bezug auf einen Modul  $N$  verstehen wir alle diejenigen Formen, welche aus  $f$  hervorgehen, indem die Coefficienten  $a_{ik}$  in beliebiger Weise um Vielfache des Moduls  $N$  geändert werden.

Wir nennen zwei Formen  $f$  und  $g$  (von derselben Variabelnzahl  $n$ ) *congruent* in Bezug auf einen Modul  $N$ ,  $f \cong g \pmod{N}$ , wenn es lineare Substitutionen von einer Determinante  $\equiv 1 \pmod{N}$  giebt, durch welche die Reste der einen Form für den Modul  $N$  in Reste der anderen Form für den Modul  $N$  übergehen.

Wir betrachten ausschliesslich Formen von nichtverschwindender Determinante.

Es kann der Fall eintreten, dass zwei Formen  $f$  und  $g$  für *einen jeden beliebigen Modul* congruent sind. Solches findet offenbar immer statt, wenn  $f$  und  $g$  derselben Classe äquivalenter Formen angehören, d. i. durch ganzzahlige Substitutionen von der Determinante 1 in einander übergehen. Es ereignet sich überhaupt dann und nur dann, wenn  $f$  und  $g$  dieselbe Determinante  $\Delta$  besitzen, und in Bezug auf den Modul  $2\Delta$  congruent sind.

Immer und nur dann, wenn die Formen  $f$  und  $g$  diesen Bedingungen genügen, und dazu einen gleichen Trägheitsindex liefern, wird es möglich sein, die eine dieser Formen in die andere durch solche linearen Substitutionen von der Determinante 1 überzuführen, in welchen die Coefficienten rationale Zahlen mit einem zu  $2\Delta$  relativ primen Generalnenner sind.<sup>1</sup>

---

<sup>1</sup> HENRY I. STEPHEN SMITH, Phil. Trans., CLVII, 1867 (*On the Orders and Genera of Ternary Quadratic Forms*, art. 12) und: Roy. Soc. Proc., XVI, 1868 (*On the Orders and Genera of Quadratic Forms containing more than three Indeterminates*, p. 202).

Alle Formen, welche denselben Trägheitsindex  $I$  haben wie eine gegebene Form, und welche mit dieser Form für einen jeden beliebigen Modul congruent sind, fassen wir in ein *Genus* zusammen. Da die Formen eines Genus eine feste Determinante besitzen, so können sie, nach bekannten Sätzen, nur in eine endliche Anzahl verschiedener Formenclassen zerfallen.

Es ist aber im Allgemeinen nicht sowohl die Anzahl dieser *Classen*, welche sich durch einfache Formeln ausdrücken lässt, als vielmehr die Anzahl der in einem Genus enthaltenen *Formen*. Zwar ist die letztere Anzahl stets eine unendliche, denn schon jede einzelne Formenclasse besitzt unendlich viel Formen. Doch zeigt es sich bald, dass für ein jedes Genus eine gewisse, positiv unendliche Grösse  $\Omega$  existirt, welche nur von den einfachsten Invarianten des Genus abhängt, und zu welcher alle die Formenanzahlen der einzelnen Classen des Genus in endlichen Verhältnissen stehen. Dieses  $\Omega$  bestimmt dann auch den Grad, in welchem die Formenanzahl des gesammten Genus unendlich wird. Fällt die Formenanzahl in einer oder in mehreren Classen des Genus gleich  $M \cdot \Omega$  aus, so bezeichnen wir die positive endliche Grösse  $M$  als das *Maass* der betreffenden Classen.

Am einfachsten gestaltet sich der Begriff des Maasses für definite Formen, also in den Fällen  $I = 0$  und  $I = n$ , mit welchen wir uns später hauptsächlich beschäftigen werden. Man weiss, dass eine definite quadratische Form  $f$  immer nur eine endliche Anzahl von Transformationen von der Determinante 1 in sich zulässt. Sei  $t(f)$  diese Anzahl. Nennen wir ferner  $\Omega_0$  die Anzahl aller möglichen linearen ganzzahligen Substitutionen  $S$  von  $n$  Reihen und von der Determinante 1. Würden wir alle diese  $S$  auf die Form  $f$  anwenden, so müssten wir zu einer jeden Form der Classe  $f$  gelangen, und zwar zu einer jeden genau  $t(f)$  Mal. Die Anzahl der verschiedenen Formen der Classe  $f$  wird daher  $\frac{1}{t(f)} \cdot \Omega_0$  betragen. Wählen wir demnach, was in der That geschehen soll, im Falle definiten Formen die erwähnte Grösse  $\Omega = \Omega_0$ , so können wir als das Maass einer definiten Classe  $f$  die Grösse  $\frac{1}{t(f)}$  erklären. Das Maass für die Formenanzahl eines definiten Genus wird dann  $\sum \frac{1}{t(f)}$  sein, wo die Summe über alle verschiedenen Classen  $f$  des Genus zu erstrecken ist.

In solchen speciellen Fällen, wo die Grösse  $t(f)$  constant ausfällt für alle Formen eines Genus, ergibt die vorstehende Summe einfach den  $t(f)^{\text{ten}}$  Theil der Classenzahl des Genus. Derartige Fälle sind Regel bei binären Formen. Man hat da gewöhnlich  $t(f) = 2$ . Nur für die Classen  $f = d(x^2 + y^2)$  wird  $t(f) = 4$ , und für die Classen  $f = 2d(x^2 + xy + y^2)$  wird  $t(f) = 6$ .

Ich bemerke noch beiläufig, dass die Grösse  $\Omega_0$  sich mit der  $(n^2 - 1)^{\text{ten}}$  Potenz der Anzahl  $\omega$  aller möglichen ganzen Zahlen von  $-\infty$  bis  $+\infty$  vergleichen lässt. Es gilt nämlich in gewissem Sinne die Beziehung:

$$\Omega_0 = \frac{\omega^{n^2-1}}{S_2 S_3 \dots S_n},$$

wo

$$S_k = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \dots \quad (k = 2, 3, \dots, n)$$

Eine Deutung des Maassbegriffes für indefinite Formen soll den Gegenstand einer späteren Arbeit bilden. Ich erwähne nur, dass als Maass einer primitiven binären Form  $ax^2 + 2bxy + cy^2$  von einer negativen, nicht quadratischen Determinante  $ac - b^2 = -D < 0$  am passendsten der Ausdruck

$\frac{\pi}{\log\left(\frac{T + U\sqrt{D}}{\sigma}\right)}$  festgesetzt wird, wo  $\sigma (= 1, 2)$  den grössten Theiler der

Coefficienten  $a, 2b, c$  bedeutet, und wo  $T$  und  $U$  die zwei kleinsten positiven Zahlen sind, welche der Gleichung  $T^2 - DU^2 = \sigma^2$  Genüge leisten.

## 2. Das vollständige System von Invarianten eines Genus.

Um ein Genus eindeutig zu characterisiren, bedarf es nicht durchaus der Kenntniss einer seiner Formen. Es genügt bereits, wenn man im Stande ist, sein *vollständiges System von Invarianten* anzugeben. Wir verstehen unter dieser Bezeichnung eine Reihe von Grössen, welche sich als arithmetische Functionen einer repräsentirenden Form  $f$  des Genus darstellen lassen, und welche die doppelte Eigenschaft haben, einmal: ungeändert zu bleiben, so oft die Form  $f$  durch eine andere Form *desselben*

Genus ersetzt wird, dann aber: in ihrer Gesamtheit sich stets zu ändern, sobald für  $f$  irgend eine Form eines *anderen* Genus genommen wird.

Ein vollständiges System von Invarianten eines Genus  $f$  umfasst die folgenden Grössen:

1° den Trägheitsindex  $I$  der Form  $f$ . Derselbe sagt aus, wie viele Quadrate mit dem Vorzeichen Minus auftreten, sobald  $f$  durch irgend eine reelle Substitution in eine Summe von  $n$ , zum Theil positiven, zum Theil negativen Quadraten transformirt wird.

2° die  $n$  Invarianten  $d_0; o_1, o_2, \dots, o_{n-1}$ , und die  $n - 1$  Invarianten  $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$  der Form  $f$ .

Die Invariante  $d_0$  stellt den positiven grössten gemeinsamen Theiler der Coefficienten  $a_{ik}$  von  $f$  vor.

Zu den Invarianten  $o_h$  gelangt man in folgender Weise. Man bezeichne mit  $d_1, d_2, \dots, d_{n-1}$  die positiven grössten gemeinsamen Theiler aller 2-, 3-, ...,  $n$ -reihigen Unterdeterminanten von  $|a_{ik}|$ , sodass insbesondere  $\Delta = (-1)^l \cdot d_{n-1}$  kommt. Aus den Zahlen  $d_h$  entstehen die Invarianten  $o_h$  mittelst der Gleichungen:

$$\frac{d_1}{d_0^2} = o_1, \quad \frac{d_2}{d_0^3} = o_1^2 o_2, \quad \dots, \quad \frac{d_{n-1}}{d_0^n} = o_1^{n-1} o_2^{n-2} \dots o_{n-1},$$

oder

$$o_h = \frac{d_h d_{h-2}}{d_{h-1}^2}.$$

Die Invarianten  $\sigma$  sind Grössen von den Werthen 1 oder 2. Man hat  $\sigma_h = 1$ , wenn unter den symmetrischen  $h$ -reihigen Minoren von  $f$  sich solche vorfinden, die, von dem Factor  $d_{h-1}$  befreit, ungerade ausfallen; dagegen  $\sigma_h = 2$ ; wenn diese Minoren alle durch  $2d_{h-1}$  aufgehen.

Die Grössen  $o_h$  sind stets ganze Zahlen, und die Grössen  $\sigma_h$  müssen den folgenden Bedingungen genügen:

(1). Die Zahlen  $\sigma_{h-1} o_h \sigma_{h+1}$  und  $\sigma_h$  dürfen nicht zugleich durch 2 theilbar sein.

(2). Die Quotienten  $\frac{\sigma_{h-1} o_h}{\sigma_{h+1}}$  und  $\frac{o_h \sigma_{h+1}}{\sigma_{h-1}}$  müssen ganz sein.

Wir führen noch die Invarianten ein:  $\sigma_0 = 1$ ,  $\sigma_n = 1$  und  $o_0 = 0$ ,  $o_n = 0$ .

3° die *Characteres* der Form  $f$ . Dieses sind eine Reihe von Einheiten

$\pm 1$ , welche in Gestalt LEGENDRE'scher Symbole auftreten. Um sie möglichst einfach darzustellen, trifft man am besten folgende Voraussetzung über die repräsentirende Form  $f$ : Die aus den ersten  $h(= 1, 2, \dots, n-1)$  Reihen von  $f$  gebildeten symmetrischen Minoren sollen Werthe  $\sigma_h d_{h-1} \varphi_h$  ergeben von solcher Art, dass ein jedes  $\varphi_h$  relativ prim zu  $2o_1 o_2 \dots o_{n-1}$  und zu  $\varphi_{h-1}$  und  $\varphi_{h+1}$  ausfällt. Dabei hat man sich noch  $c_0 = 1$  und  $\varphi_n = (-1)^l$  zu denken. Nach *F. Q.*, p. 83, lassen sich in jeder Classe des Genus Formen  $f$  von dieser Eigenthümlichkeit finden; man nennt sie *characteristische Formen*.

Es sei allgemein  $c_h$  das Vorzeichen von  $\varphi_h$ ; ferner mag  $I_h$  angeben, wie viele von den Einheiten  $\frac{c_1}{c_0}, \frac{c_2}{c_1}, \dots, \frac{c_h}{c_{h-1}}$  negativ ausfallen, sodass insbesondere  $I_0 = 0$  und  $I_n = I$  zu nehmen ist. Für eine characteristische Form  $f$  erweisen sich folgende Einheiten  $C$  als Charactere:

1) wenn  $\sigma_{h-1} o_h \sigma_{h+1}$  durch eine ungerade Primzahl  $p$  theilbar ist, die Einheit

$$\left(\frac{\varphi_h}{p}\right);$$

2) wenn  $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod{4}$  ist, die Einheiten

$$(-1)^{\frac{\varphi_h - 1}{2}}, \quad \left(\frac{\varphi_{h-1}}{c_h \varphi_h}\right) (-1)^{\frac{I_h(I_h-1)}{2}}, \quad \left(\frac{\varphi_{h+1}}{c_h \varphi_h}\right) (-1)^{\frac{I_h(I_h+1)}{2}};$$

3) wenn  $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod{8}$  ist, die Einheit

$$\left(\frac{2}{\varphi_h}\right).$$

Diese Einheiten  $C$  bilden zusammen mit den Grössen  $I, d_0, o_h, \sigma_h$  wirklich ein vollständiges System von Invarianten für das betrachtete Genus, sodass kein zweites Genus da sein kann, welches zu eben diesen Invarianten führt.

Die Einheiten  $C$  müssen alle Bedingungen erfüllen, welche sich für sie aus den quadratischen Congruenzen

$$(h) \quad -\sigma_{h-1} o_h \sigma_{h+1} \varphi_{h-1} \varphi_{h+1} \equiv X_h^2 \pmod{\sigma_h^2 \varphi_h}$$

erschliessen lassen. Man findet diese Bedingungen in *F. Q.*, pp. 87—88, zusammengestellt.

Es gilt der Satz:

(G) Wenn die Invarianten  $I, d_0, o, \sigma$  und die Charactere  $U$  in beliebiger Weise festgesetzt werden, doch so, dass sie den Bedingungen (1), (2) genügen, ferner allen Bedingungen, welche aus den Congruenzen (h) folgen, so existirt wirklich ein Genus, welches zu diesen Invarianten und Characteren Veranlassung giebt.

Ein Beweis dieses Satzes ist *F. Q.*, pp. 89—90, mit Hilfe des bekannten Theoremes über die arithmetischen Progressionen geführt. Ich habe dort diesen Hilfssatz  $n - 1$  Mal hintereinander angewandt zur successiven Auffindung von  $n - 1$  Zahlen  $\varphi_1, \varphi_2, \dots, \varphi_{n-1}$  für eine charakteristische Form des gewünschten Genus. Man überzeugt sich aber leicht, dass es immer genügt, ein einziges Mal von diesem Satze Gebrauch zu machen, nämlich um allein  $\varphi_{n-1}$  als Primzahl zu bestimmen; und man sieht dann ferner, dass in den Fällen  $n \geq 3$  dieser Hilfssatz sich ganz entbehren lässt, wenn nur der Satz (G) bereits für  $n = 2$  bewiesen ist.

Alle Formengenera, welche dieselben Werthe der Grössen  $I, d_0, o_n, \sigma_n$  besitzen, werden in eine *Ordnung*

$$d_0, \quad \begin{pmatrix} \sigma_1, \sigma_2, \dots, \sigma_{n-1} \\ o_1, o_2, \dots, o_{n-1} \end{pmatrix}, \quad I$$

zusammengefasst.

Wir beschäftigen uns meist mit Formen  $f$ , deren  $d_0$  gleich 1 ist, und die man *primitive* Formen nennt. Im Falle die Grösse  $d_0$  einer Form  $f$  relativ prim zu einer Zahl  $N$  ist, heisst diese Form primitiv in Bezug auf  $N$ .

---

### Erster Theil.

#### 3. Die Anzahl der Reste eines Genus in Bezug auf einen Modul $N$ .

Wir wollen zunächst untersuchen, wieviel verschiedene Formenreste ein gegebenes Genus in Bezug auf einen gegebenen Modul  $N$  liefert. In der Anzahl dieser Formenreste finden wir einen Divisor der Formenanzahl des Genus, und wir werden so alle wesentlichen Factoren kennen lernen, aus welchen sich die Ausdrücke für die Formenanzahl zusammensetzen.

Das Genus möge durch eine beliebige seiner Formen,  $f$ , repräsentirt werden. Es ist dann klar, dass wir die Reste des Genus nach dem Modul  $N$  nur unter denjenigen Formen suchen dürfen, welche  $\cong f \pmod{N}$  sind. Man gelangt zu diesen Formen, indem man auf  $f$  ein vollständiges System von lauter incongruenten Substitutionen  $T$  von einer Determinante  $\equiv 1 \pmod{N}$  anwendet. Ein solches System wird leicht bestimmt. Man braucht beispielsweise nur von den  $N^{n^2}$  incongruenten Substitutionen

$$x_i \equiv \sum_k t_i^k y_k \pmod{N}, \quad t_i^k = 1, 2, \dots, N \quad (i, k=1, 2, \dots, n)$$

alle diejenigen fortzulassen, in welchen die Determinante nicht  $\equiv 1 \pmod{N}$  ausfällt.

In dem Systeme der  $T$  mögen sich im Ganzen  $\mathfrak{N}$  Substitutionen finden lassen, — etwa die folgenden:  $T_1, T_2, \dots, T_{\mathfrak{N}}$ , durch welche  $f$  in  $\mathfrak{N}$  verschiedene Reste:  $g_1, g_2, \dots, g_{\mathfrak{N}} \pmod{N}$  übergehe. Das gegebene Genus enthält dann sicher nicht mehr als diese  $\mathfrak{N}$  Reste. Wir behaupten aber, dass diese Reste wirklich alle dem gegebenen Genus, ja schon der (ganz beliebigen) Classe  $f$  eigen sind.

In der That, zu jeder Substitution

$$T \equiv \begin{vmatrix} x_1, & \dots & \dots & \dots \\ x_2, & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ x_n, & \dots & \dots & \dots \end{vmatrix} \equiv 1 \pmod{N}$$

lässt sich immer eine nach dem Modul  $N$  congruente Substitution  $S$  von einer Determinante  $1$  bestimmen. Im Falle  $n = 1$  leuchtet dieses unmittelbar ein. Wenn  $n > 1$  ist, so bedienen wir uns zum Beweise eines Schlusses von  $n - 1$  auf  $n$ . Offenbar muss der grösste Theiler der  $n$  Zahlen  $x_i$  zu  $N$  relativ prim sein. Man kann daher  $n$  Zahlen  $\xi_i \equiv x_i \pmod{N}$  finden, deren grösster Theiler gleich  $1$  ist. Alsdann lässt sich bekanntlich eine Substitution

$$S_0 = \begin{vmatrix} \xi_1, & \dots & \dots & \dots \\ \xi_2, & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \xi_n, & \dots & \dots & \dots \end{vmatrix}$$



von der Determinante 1 bilden (*F. Q.*, p. 98). Das Product  $S_0^{-1} \cdot T$  gewinnt jetzt die Form

$$U \equiv \begin{vmatrix} 1, & U_1, & \dots, & U_{n-1} \\ 0, & u_1^1, & \dots, & u_1^{n-1} \\ \dots & \dots & \dots & \dots \\ 0, & u_{n-1}^1, & \dots, & u_{n-1}^{n-1} \end{vmatrix} \equiv 1 \pmod{N}.$$

Ist unser Lemma bereits für den Fall  $n - 1$  erwiesen, so können wir an Stelle der  $u_i^k$  solche congruente Zahlen einführen, dass  $|u_i^k|$  in 1 übergeht. Ferner setzen wir an Stelle der ersten Verticalreihe von  $U$  einfach die Zahlen 1, 0, ..., 0. Auf diese Weise wird  $U$  in eine congruente Substitution  $V$  von der Determinante 1 übergehen, und das Product  $S_0 \cdot V = S$  erscheint als eine mit  $T$  congruente Substitution von der Determinante 1.

Wir können so zu allen Substitutionen  $T_1, T_2, \dots, T_{\mathfrak{N}}$  congruente Substitutionen  $S_1, S_2, \dots, S_{\mathfrak{N}}$  von der Determinante 1 bilden. Durch diese muss sich  $f$  in äquivalente Formen mit den Resten  $g_1, g_2, \dots, g_{\mathfrak{N}}$  verwandeln, was zu beweisen war.

Es ist nun leicht plausibel zu machen, dass die Formenanzahl der Classe  $f$  ein Vielfaches der Zahl  $\mathfrak{N}$  wird. Man denke sich zu dem Behufe in der Classe  $f$  alle verschiedenen Formen gekennzeichnet, welche nach dem Modul  $N$  den Rest  $f$  lassen, und für jede dieser Formen je eine Substitution  $S$  notirt, durch welche dieselbe aus  $f$  entsteht. Durch Anwendung aller  $S \cdot S_1, S \cdot S_2, \dots, S \cdot S_{\mathfrak{N}}$  müssen dann aus  $f$  die sämtlichen Formen der Classe  $f$  hervorgehen, und zwar eine jede ein einziges Mal. Die Zahl  $\mathfrak{N}$  theilt somit wirklich in gewissem Sinne die (unendliche) Formenanzahl der Classe  $f$ , und da diese Classe eine beliebige ist, auch die Formenanzahl des gesammten Genus, wie am Anfange ausgesprochen war.

Um einen Ausdruck für die Zahl  $\mathfrak{N}$  zu gewinnen, verfährt man folgendermaassen. Es sei  $\phi_n(N)$  die Anzahl der Individuen eines vollständigen Systemes von incongruenten Substitutionen  $T$  von einer Determinante  $\equiv 1 \pmod{N}$ . Alle diejenigen  $T$ , welche auf den Rest  $f \pmod{N}$  ohne Wirkung bleiben, nenne man  $\mathfrak{T}$ , und es sei  $f(N)$  die Anzahl der ver-

schiedenen  $\mathbb{T}$ . Die Substitutionen  $\mathbb{T}.T_1, \mathbb{T}.T_2, \dots, \mathbb{T}.T_{\mathfrak{N}}$  müssen das gesammte System der  $T$  erschöpfen, und man erhält so:

$$\mathfrak{N} = \frac{\phi_n(N)}{f(N)}.$$

In welcher Weise die Grösse  $\phi_n(N)$  gefunden wird, ist bekannt.<sup>1</sup> Damit ein  $T \equiv 1 \pmod{N}$  ausfalle, ist zunächst erforderlich, dass die  $n$  Zahlen  $x_1, x_2, \dots, x_n$  der ersten Verticalreihe ohne gemeinsamen Theiler mit  $N$  gewählt seien. Eine solche Wahl kann auf  $N^n \cdot (N)_n$  Arten geschehen, wenn  $(N)_n$  das über alle verschiedenen Primzahlen  $q$  von  $N$  ausgedehnte Product  $\prod \left(1 - \frac{1}{q^n}\right)$  bedeutet. Man sieht leicht, dass zu jedem, ohne Theiler mit  $N$  gewählten Systeme  $x_i$  mindestens ein  $T$  gehört. Alle möglichen  $T$  mit der ersten Verticalreihe  $x_i$  folgen dann durch Zusammensetzung dieses einen mit den verschiedenen Substitutionen  $U \equiv 1 \pmod{N}$ . In  $U$  unterliegen die  $n - 1$  Zahlen  $U_i$  gar keiner Beschränkung. Es lassen sich also im Ganzen  $N^{n-1} \cdot \phi_{n-1}(N)$  incongruente  $U$  bilden, und man erlangt die Beziehung:

$$\phi_n(N) = N^{2n-1} \cdot (N)_n \cdot \phi_{n-1}(N).$$

Da nun  $\phi_1(N) = 1$  ist, so entsteht

$$\phi_n(N) = N^{n^2-1} \cdot (N)_2 \cdot (N)_3 \cdot \dots \cdot (N)_n.$$

Es handelt sich also wesentlich um die Bestimmung der Grössen  $f(N)$ . Dabei genügt es, den Fall zu untersuchen, wo  $N$  eine Primzahlpotenz  $q^t$  ist.

Denn setzt  $N$  sich aus mehreren Primzahlpotenzen  $q^t$  zusammen,  $N = \prod q^t$ , so hat man  $f(N) = \prod f(q^t)$ .

So oft nämlich eine Substitution  $\mathbb{T} \equiv 1 \pmod{N}$  ist, ergiebt sich dieselbe auch  $\equiv 1$  nach jedem der Moduln  $q^t$ , und ändert sie den Rest  $f \pmod{N}$  nicht, so ändert sie auch keinen der Reste  $f \pmod{q^t}$ . Liegt andererseits für einen jeden Modul  $q^t$  ein  $\mathbb{T}_q$  vor, von einer Determinante  $\equiv 1 \pmod{q^t}$ , welches auf  $f \pmod{q^t}$  ohne Wirkung bleibt, so wird die Substitution  $\mathbb{T} \pmod{N}$ , welche allen Congruenzen

$$\mathbb{T} \equiv \mathbb{T}_q \pmod{q^t}$$

<sup>1</sup> JORDAN, *Traité des substitutions*, 120—124.

genügt,  $\equiv 1 \pmod{N}$  ausfallen, und den Rest  $f \pmod{N}$  nicht ändern. So geht die behauptete Relation hervor.

**4. Hilfssätze zur Bestimmung der Zahlen  $f(q')$ .**

Wir brauchen in Betreff der Grössen  $f(q')$  nur den Fall zu betrachten, wo  $f$  primitiv in Bezug auf  $q$  ist, also die Coefficienten  $a_{ik}$  von  $f$  nicht sämmtlich den Theiler  $q$  haben. Denu sei etwa  $f = q^d \cdot g$  und  $d > 0$ . So lange man  $d \geq t > 0$  hat, bleibt der Rest  $f \pmod{q'}$  bei jeder Substitution ungeändert, und man erhält  $f(q') = \phi_n(q')$ . Wenn aber  $d < t$  ist, so gilt die Relation

$$(1) \quad f(q') = q^{(n^2-1)d} \cdot g(q'^{-d}).$$

In der That, eine jede Substitution  $T \equiv 1 \pmod{q'}$ , welche auf  $f \pmod{q'}$  ohne Wirkung ist, ändert auch  $g \pmod{q'^{-d}}$  nicht; und ebenso wird ein jedes  $\mathfrak{Z} \equiv 1 \pmod{q'^{-d}}$ , welches auf  $g \pmod{q'^{-d}}$  ohne Wirkung bleibt, auch  $f \pmod{q'}$  nicht ändern. Aus einem jeden  $\mathfrak{Z}$  lassen sich aber  $q^{(n^2-1)d}$ , nach dem Modul  $q'$  verschiedene Substitutionen  $T$  herleiten. Denn in einem  $\mathfrak{Z}$  ist immer mindestens ein Coefficient  $c$  da, für welchen  $\frac{\partial \mathfrak{Z}}{\partial c}$  zu  $q$  relativ prim ausfällt. Wir können nun, um eine Substitution  $T$  zu gewinnen, erst jeden der  $n^2 - 1$  übrigen Coefficientenreste  $\pmod{q'^{-d}}$  von  $\mathfrak{Z}$  durch  $q^d$  verschiedene Reste  $\pmod{q'}$  ersetzen. Der Rest von  $c$  für den Modul  $q'$  folgt hernach eindeutig aus der Bedingung, dass die veränderte Substitution eine Determinante  $\equiv 1 \pmod{q'}$  ergebe.

Insofern es uns um Factoren für die Formenanzahl eines Genus zu thun ist, reicht die Betrachtung solcher Moduln  $q'$  aus, welche gewisse Grenzen  $q^{G(q)}$  überschreiten. Denn ist  $t \geq t - d > 0$ , so beweist man leicht, dass die Zahl  $\phi_n(q'^{-d}) : f(q'^{-d})$  einen Divisor der Zahl  $\mathfrak{R} = \frac{\phi_n(q')}{f(q')}$  vorstellt. Beachtet man die oben gegebenen Werthe von  $\phi_n(q')$ , so läuft dieses darauf hinaus, dass die Zahl  $f(q')$  in der Zahl  $q^{(n^2-1)d} \cdot f(q'^{-d}) [t - d > 0]$  aufgeht.

Für eine mit  $q$  primitive Form  $f$  machen wir von folgenden Bezeich-

nungen Gebrauch. Die höchsten in den Invarianten  $o_1, o_2, \dots, o_{n-1}$  enthaltenen Potenzen von  $q$  sollen die Exponenten besitzen:  $\omega_1, \omega_2, \dots, \omega_{n-1}$ , und es sei allgemein

$$v_h = \omega_1 + \omega_2 + \dots + \omega_h, \quad \partial_h = h\omega_1 + (h-1)\omega_2 + \dots + \omega_h.$$

Ferner nehmen wir an, von den  $n-1$  nicht negativen Zahlen  $\omega_h$  seien im Ganzen  $\lambda-1$  grösser als Null, nämlich die folgenden:

$$(\partial_0 = 0) \quad \omega_{\partial_1}, \omega_{\partial_2}, \dots, \omega_{\partial_{\lambda-1}} \quad (\partial_\lambda = n)$$

und wir bilden die Gleichungen

$$\partial_1 = x_1, \quad \partial_2 = x_1 + x_2, \quad \dots, \quad \partial_\lambda = x_1 + x_2 + \dots + x_\lambda,$$

d. i.

$$x_k = \partial_k - \partial_{k-1}.$$

Der Quotient aus der Determinante  $\Delta$  von  $f$  und der Potenz  $q^{\partial_n}$  mag für einen Moment  $\Delta_0$  heissen. Wir werden weiterhin voraussetzen, dass unsere Moduln  $q^t$ , wenn  $q$  einer ungeraden Primzahl  $p$  gleich ist, die Potenz  $p^G = p^{r_{n-1}}$ , und wenn  $q = 2$  ist, die Potenz  $2^G = 2^{1+r_{n-1}}$  überschreiten. Die Folge davon wird sein, dass ein jeder Rest  $f \pmod{q^t}$  uns, wenn  $q = p$  ist, den Werth der Einheit  $\left(\frac{\Delta_0}{p}\right)$ , und wenn  $q = 2$  ist, den Werth der Einheit  $(-1)^{\frac{\partial_0-1}{2}}$ , sowie im Falle  $\sigma_{n-1} = 2$ , auch den Werth der Einheit  $\left(\frac{2}{\Delta_0}\right)$  liefert. Denn es gilt der Satz:

Genügt eine Form  $g$  schon der Congruenz

$$g \cong f \pmod{q^{G+1}},$$

und soll noch  $g \cong f \pmod{q^t}$  sein, so ist nothwendig und hinreichend, dass, wenn  $q = p$ , die Beziehung

$$\Delta(g) \equiv \Delta(f) \pmod{p^{t+\partial_{n-2}}}$$

und wenn  $q = 2$ , die Beziehung

$$\Delta(g) \equiv \Delta(f) \pmod{\sigma_{n-1} \cdot 2^{t+\partial_{n-2}}}$$

bestehe.

Ich erwähne noch einige, zum Theil bekannte Sätze über Congruenzen, welche bald ihre Anwendung finden werden.

(2). Ist eine Form  $f$  und eine Zahl  $\alpha$  prim in Bezug auf eine ungerade Primzahl  $p$ , und hat die Congruenz

$$f(\xi_i) \equiv \alpha \pmod{p}$$

$A \cdot p^{n-1}$  Lösungen, so besitzt die Congruenz

$$(t) \quad f(\xi_i) \equiv \alpha \pmod{p^t} \quad (t > 1)$$

$A \cdot p^{(n-1)t}$  Lösungen.

Denn genügt ein System  $\xi_i$  der Congruenz

$$(t-1) \quad f(\xi_i) \equiv \alpha \pmod{p^{t-1}},$$

und setzt man  $x_i \equiv \xi_i + p^{t-1} u_i \pmod{p^t}$ , so kommt, da  $t > 1$  sein soll,

$$f(x_i) \equiv f(\xi_i) + p^{t-1} \cdot \sum u_i \frac{\partial f}{\partial \xi_i} \pmod{p^t}.$$

Nun können die Zahlen  $\frac{\partial f}{\partial \xi_i}$  nicht sämtlich durch  $p$  theilbar sein, da

man  $\frac{1}{2} \sum \xi_i \frac{\partial f}{\partial \xi_i} \equiv \alpha \pmod{p}$  hat. Also ergibt die Congruenz

$$\frac{\alpha - f(\xi_i)}{p^{t-1}} \equiv \sum u_i \frac{\partial f}{\partial \xi_i} \pmod{p}$$

$p^{n-1}$  Lösungen  $u_i \pmod{p}$ , und eine jede Lösung von  $(t-1)$  liefert  $p^{n-1}$  Lösungen von  $(t)$ , woraus unmittelbar unser Satz folgt.

Jetzt sei  $f = \sum a_{ik} x_i x_k$  eine in Bezug auf 2 primitive Form, und  $\alpha$  eine ungerade Zahl. Wir unterscheiden zwei Fälle, je nachdem die Invariante  $\sigma_1$  von  $f$  den Werth 1 oder 2 hat, die Zahlen  $a_{ii}$  also zum Theil ungerade oder sämtlich gerade ausfallen.

(3). Ist  $\sigma_1 = 1$ , und besitzt die Congruenz

$$f(\xi_i) \equiv \alpha \pmod{8}$$

$A \cdot 2^{3(n-1)}$  Lösungen, so liefert die Congruenz

$$(t) \quad f(\xi_i) \equiv \alpha \pmod{2^t} \quad (t > 3)$$

$A \cdot 2^{3(n-1)t}$  Lösungen.

In der That, es genügen der Congruenz

$$(t-1) \quad f(\xi_i) \equiv \alpha \pmod{2^{t-1}}$$

zusammen mit einem Systeme  $\xi_i \pmod{2^{t-1}}$  immer alle die  $2^n$  Systeme  $x_i \pmod{2^{t-1}}$ , für welche  $x_i \equiv \xi_i \pmod{2^{t-2}}$  ist. Denn jedes dieser Systeme lässt sich in die Form  $x_i \equiv \xi_i + 2^{t-2} \delta_i \pmod{2^{t-1}}$  setzen, wo die  $n$  Grössen  $\delta_i$  entweder 0 oder 1 bedeuten; man hat also wirklich:

$$f(x_i) \equiv f(\xi_i) + 2^{t-1} \cdot \sum \delta_i \frac{1}{2} \frac{\partial f}{\partial \xi_i} \equiv \alpha \pmod{2^{t-1}}.$$

Bildet man nun mit Hilfe einer Lösung  $\xi_i \pmod{2^{t-2}}$  von  $(t-1)$  ein System  $x_i \equiv \xi_i + 2^{t-2} u_i \pmod{2^{t-1}}$ , so kommt

$$f(x_i) \equiv f(\xi_i) + 2^{t-1} \cdot \sum u_i \frac{1}{2} \frac{\partial f}{\partial \xi_i} \pmod{2^t},$$

und die Congruenz

$$\frac{\alpha - f(\xi_i)}{2^{t-1}} \equiv \sum u_i \frac{1}{2} \frac{\partial f}{\partial \xi_i} \pmod{2}$$

ergibt  $2^{n-1}$  Lösungen  $u_i \pmod{2}$ . So führt eine jede Lösung  $\xi_i \pmod{2^{t-2}}$  von  $(t-1)$  zu  $2^{n-1}$  Lösungen  $\xi_i \pmod{2^{t-1}}$  von  $(t)$ , woraus die Richtigkeit unserer Behauptung erhellt.

Es ist auch klar, dass unser Satz gültig bleibt, wenn wir alle solchen Lösungen  $\xi_i$  ausschliessen, die zugleich gewissen gegebenen linearen Congruenzen nach dem Modul 2 genügen.

(4). Ist zweitens  $\sigma_1 = 2$ , und hat die Congruenz

$$f(\xi_i) \equiv 2\alpha \pmod{4}$$

$2A \cdot 2^{2(n-1)}$  Lösungen, in welchen die  $n$  Zahlen  $\frac{1}{2} \frac{\partial f}{\partial \xi_i}$  nicht sämtlich gerade sind, so liefert die Congruenz

$$(t) \quad f(\xi_i) \equiv 2\alpha \pmod{2^t} \quad (t > 2)$$

$2A \cdot 2^{(n-1)t}$  Lösungen, bei welchen die  $n$  Zahlen  $\frac{1}{2} \frac{\partial f}{\partial \xi_i}$  nicht sämtlich gerade sind.

Denn setzt man  $\frac{1}{2} f = \varphi$ , so gruppieren sich je  $2^n$  Lösungen  $\xi_i \pmod{2^t}$

von (t) zu je einer Lösung  $\xi_i \pmod{2^{t-1}}$  von  $\varphi(\xi_i) \equiv \alpha \pmod{2^{t-1}}$ . Unser Satz geht so in einen analogen Satz in Betreff des Ausdruckes  $\varphi$  über, welcher dann ähnlich bewiesen wird wie der Satz (2).

Wir schreiten nun zur Bestimmung der Grössen  $f(q')$ .<sup>1</sup> Dabei werden wir uns hauptsächlich auf diejenigen Resultate stützen, welche in der Note zu meiner am Anfange citirten Arbeit enthalten sind (*F. Q.*, pp. 169—178).

### 5. Der Fall einer ungeraden Primzahl.

Wir betrachten zunächst den einfacheren Fall, wo  $q$  gleich einer ungeraden Primzahl  $p$  ist. Die Form  $f$  sei primitiv in Bezug auf  $p$ . Der Modul  $p'$  möge die Potenz  $p^{n-1}$  überschreiten.

Da wir  $f$  durch jeden nach dem Modul  $p'$  congruenten Rest ersetzen dürfen, so können wir annehmen (*F. Q.*, p. 7),  $\hat{f}$  habe den Typus

$$f \equiv \alpha \xi^2 + F \pmod{p'},$$

wo  $\alpha$  zu  $p$  prim ist, und  $F$  einen Rest von  $n - 1$  Variablen vorstellt. Die Coefficienten von  $F$  müssen den Factor  $p^{\omega_1}$  enthalten, und setzen wir

$$F \equiv p^{\omega_1} f^{(1)} \pmod{p'},$$

so fällt der Rest  $f^{(1)}$  primitiv in Bezug auf  $p$  aus, und die  $n - 2$  Invarianten  $p^{\omega_k^{(1)}}$ , welche diesem Reste angehören, erfüllen die Gleichungen:

$$\omega_{h-1}^{(1)} = \omega_h. \qquad (h=2, 3, \dots, n-1)$$

Wir denken uns die  $f(p')$  verschiedenen Substitutionen  $\mathbf{T}$  von einer Determinante  $\equiv 1 \pmod{p'}$  aufgestellt, welche den Rest  $f \pmod{p'}$  in sich selbst überführen. In jeder dieser Substitutionen muss die erste Verticalreihe aus  $n$  Zahlen  $\xi_i \pmod{p'}$  bestehen, welche

$$f(\xi_i) \equiv \alpha \pmod{p'}$$

ergeben. Der vorstehenden Congruenz mögen  $A \cdot p^{(n-1)'$  verschiedene Systeme  $\xi_i \pmod{p'}$  Genüge leisten. Die Betrachtungen aus *F. Q.*, p. 170,

<sup>1</sup> In einem ausgezeichneten Falle, nämlich für die Form  $f = x_1^2 + x_2^2 + \dots + x_n^2$ , sind die Zahlen  $f(q)$  von Herrn JORDAN gegeben (*Traité des substitutions*, 201—214, Ordre du groupe orthogonal).

lassen erkennen, dass jedem dieser Systeme  $\xi_i$  wirklich Substitutionen  $T$  zukommen, welche den Rest  $f$  in sich selbst transformiren.

Es frägt sich, wie viele verschiedene  $T$  können aus einem bestimmten Systeme  $\xi_i$  hervorgehen. Ist  $T_0$  eine erste dieser Substitutionen, so wird jedes überhaupt vorhandene  $T$  mit der ersten Verticalreihe  $\xi_i$  in ganz bestimmter Weise zusammengesetzt sein als Product aus  $T_0$  und aus zwei Substitutionen  $U$  und  $\mathfrak{Z}$  von der Form

$$U \equiv \begin{vmatrix} 1, & U_1, & \dots, & U_{n-1} \\ 0, & 1, & \dots, & 0 \\ \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & 1 \end{vmatrix}, \quad \mathfrak{Z} \equiv \begin{vmatrix} 1, & 0, & \dots, & 0 \\ 0, & t_1^1, & \dots, & t_1^{n-1} \\ \dots & \dots & \dots & \dots \\ 0, & t_{n-1}^1, & \dots, & t_{n-1}^{n-1} \end{vmatrix} \pmod{p'}.$$

Soll nun  $T$  den Rest  $f$  in sich selbst überführen, so ist nöthig, dass auch  $U, \mathfrak{Z}$  diesen Rest in sich selbst transformire. Hierzu wieder ist erforderlich, dass die Relationen  $U_h \equiv 0 \pmod{p'}$  gelten, und dass die Substitution  $\mathfrak{Z}$  auf den Rest  $F \pmod{p'}$  ohne Wirkung bleibe. Die Anzahl der verschiedenen  $T$  mit der ersten Verticalreihe  $\xi_i$ , welche  $f \pmod{p'}$  nicht ändern, wird daher gleich der Anzahl der verschiedenen  $\mathfrak{Z}$  sein, welche auf  $F \pmod{p'}$  ohne Wirkung sind, also gleich  $F(p')$ . Zieht man noch die Formel 4. (1) in Betracht, so kommt schliesslich

$$f(p') = p^{(n-1)t + \omega_1[(n-1)^2 - 1]} \cdot A \cdot f^{(1)}(p^{t - \omega_1}).$$

Wir setzen nun allgemein:

$$f(p') = p^{\frac{n(n-1)}{2}t + \sum_h^{1, n-1} \omega_h \left( \frac{(n-h)(n-h+1)}{2} - 1 \right)} \cdot f\{p\}. \quad \left( t > \sum_h^{1, n-1} \omega_h \right)$$

Für den Rest  $f^{(1)}$  bilden wir eine entsprechende Grösse  $f^{(1)}\{p\}$ . Die vorstehende Relation verwandelt sich alsdann in:

$$(p) \quad f\{p\} = A \cdot f^{(1)}\{p\},$$

und diese Formel bleibt auch für  $n = 1$  gültig, falls nur für eine Form  $F$  von Null Variablen  $F\{p\} = \frac{1}{2}$  genommen wird.



Es handelt sich jetzt um die Bestimmung der Grösse  $A$ . Nach dem Satze 4. (2) muss  $A \cdot p^{n-1}$  die Anzahl aller Lösungen von  $f(\xi_i) \equiv \alpha \pmod{p}$  ausdrücken. Bedeutet  $x$  den Index der ersten von den Zahlen  $\omega_1, \omega_2, \dots, \omega_{n-1}, \omega_n (= -\infty)$ , welche nicht verschwindet, so können wir  $f$  von dem Typus voraussetzen:

$$\left. \begin{aligned} f &\equiv \Phi + p^{\omega_x} \cdot f^{(x)} \\ \Phi &\equiv \alpha_1 \xi_1^2 + \alpha_2 \xi_2^2 + \dots + \alpha_x \xi_x^2 \end{aligned} \right\} \pmod{p}, \quad (\alpha_1 = \alpha)$$

wo ein jedes  $\alpha_1, \alpha_2, \dots, \alpha_x$  und ebenso der Rest  $f^{(x)}$  primitiv in Bezug auf  $p$  ist (*F. Q.*, p. 19). Wir erhalten dann  $f \equiv \Phi \pmod{p}$ , und  $A \cdot p^{x-1}$  muss die Anzahl der Lösungen von  $\Phi \equiv \alpha \pmod{p}$  geben. Nun lässt sich diese letztere Anzahl nach bekannten Sätzen herleiten.<sup>1</sup> Man gelangt so zu folgenden Beziehungen:

1) wenn  $x \equiv 0 \pmod{2}$ ,

$$A = (1 - \theta \cdot p^{-\frac{x}{2}}), \quad \theta = \left( \frac{(-1)^{\frac{x}{2}} \cdot \alpha_1 \alpha_2 \dots \alpha_x}{p} \right);$$

2) wenn  $x \equiv 1 \pmod{2}$ ,

$$A = (1 + \theta^1 \cdot p^{-\frac{x-1}{2}}), \quad \theta^1 = \left( \frac{(-1)^{\frac{x-1}{2}} \cdot \alpha_2 \alpha_3 \dots \alpha_x}{p} \right).$$

Im Falle  $x = 1$  hat man sich  $\theta^1 = 1$  zu denken.

Wir können weiter die Grösse  $f\{p\}$  auf  $f^{(x)}\{p\}$  zurückführen. Man findet:

$$f\{p\} = \mathfrak{A} \cdot f^{(x)}\{p\},$$

wenn  $\mathfrak{A}$  den folgenden Ausdruck bedeutet: im Falle  $x \equiv 0 \pmod{2}$ ,

$$\mathfrak{A} = 2 \left( 1 - \frac{1}{p^2} \right) \left( 1 - \frac{1}{p^4} \right) \dots \left( 1 - \frac{1}{p^{x-2}} \right) \cdot \left( 1 - \frac{\theta}{p^{\frac{x}{2}}} \right);$$

und im Falle  $x \equiv 1 \pmod{2}$ ,

$$\mathfrak{A} = 2 \left( 1 - \frac{1}{p^2} \right) \left( 1 - \frac{1}{p^4} \right) \dots \left( 1 - \frac{1}{p^{x-1}} \right).$$

<sup>1</sup> LEBESGUE, *Recherches sur les nombres*, § 5 (Journal de LIOUVILLE, T. 2, pp. 266—275). — C. JORDAN, *Comptes rendus*, 1866, I, pp. 687—690; *Traité des substitutions*, 197—200; Journal de LIOUVILLE, 2<sup>me</sup> série, T. 17, p. 372. — *F. Q.*, artt. VII—VIII.

Für ein  $x = 1$  stimmt diese Gleichung unmittelbar mit  $(p)$  überein, während sie für ein  $x > 1$  leicht aus  $(p)$  mit Hilfe eines Schlusses von  $x - 1$  auf  $x$  hervorgeht. Man braucht nur zu beachten, dass dem Reste  $f^{(1)}$  in derselben Weise die Zahl  $x - 1$  angehört wie dem Reste  $f$  die Zahl  $x$ .

Für alle ungeraden Primzahlen  $p$ , welche nicht in der Determinante  $\Delta$  der Form  $f$  aufgehen, wird  $x = n$ , also  $\alpha_1 \alpha_2 \dots \alpha_x \equiv \Delta \pmod{p}$ , während  $f^{(x)}$  sich als ein Rest von Null Variablen erweist. Für alle diese Primzahlen  $p$  kommt daher:

1) wenn  $n \equiv 0 \pmod{2}$ ,

$$f(p') = p^{\frac{n(n-1)}{2}t} \cdot \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p^4}\right) \dots \left(1 - \frac{1}{p^{n-2}}\right) \cdot \left\{1 - \left(\frac{(-1)^{\frac{n}{2}} \Delta}{p}\right) \frac{1}{p^{\frac{n}{2}}}\right\};$$

2) wenn  $n \equiv 1 \pmod{2}$ ,

$$f(p') = p^{\frac{n(n-1)}{2}t} \cdot \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p^4}\right) \dots \left(1 - \frac{1}{p^{n-1}}\right).$$

Um die Grössen  $f\{p\}$  vollständig darzustellen, wollen wir endlich  $f$  als *Hauptrest* für den Modul  $p'$  voraussetzen. Falls die Bezeichnungen aus 4. gelten, so heisst dieses,  $f$  soll den Typus haben:

$$f \equiv \{\Phi_1 + p^{v_1}[\Phi_2 + p^{v_2}[\Phi_3 + \dots + p^{v_{\lambda-1}}(\Phi_\lambda)]]\} \pmod{p'},$$

$$\Phi_k \equiv \alpha_1^{(k)} \xi_1^{(k)} \xi_1^{(k)} + \dots + \alpha_{x_k}^{(k)} \xi_{x_k}^{(k)} \xi_{x_k}^{(k)} \pmod{p^{t-v_{k-1}}},$$

wo die  $\alpha_k^{(k)}$  sämmtlich zu  $p$  prim sind (*F. Q.*, p. 19).

Für einen *Hauptrest*  $f$  wird die Grösse  $f\{p\}$  gleich einem Producte aus der Potenz  $2^{\lambda-1}$  und aus  $\lambda$  Factoren  $\mathfrak{A}_k$ , welche den  $\lambda$  einzelnen Resten  $\Phi_k$  entsprechen und folgende Bedeutung haben:

$$\mathfrak{A}_k = \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p^4}\right) \dots \left(1 - \frac{1}{p^{2\left[\frac{x_k}{2}\right]}}\right) \cdot \alpha_k,$$

wo  $\left[\frac{x_k}{2}\right]$  die grösste in  $\frac{x_k}{2}$  enthaltene ganze Zahl vorstellt, und  $\alpha_k = 1$  ist im Falle  $x_k \equiv 1 \pmod{2}$ , dagegen:

$$a_k = (1 + \theta_k \cdot p^{-\frac{x_k}{2}})^{-1}, \quad \theta_k = \left( \frac{(-1)^{\frac{x_k}{2}} \cdot \Delta(\Phi_k)}{p} \right),$$

wenn  $x_k \equiv 0 \pmod{2}$  ist.

Die Richtigkeit dieser Formeln ergibt sich sofort mit Hilfe eines Schlusses von  $\lambda - 1$  auf  $\lambda$ . Man bemerkt nämlich, dass dem Reste  $f^{(x)}(x = x_1)$  in derselben Weise die Zahl  $\lambda - 1$  zukommt wie dem Reste  $f$  die Zahl  $\lambda$ .

### 6. Der Fall der Primzahl 2.

Wir behandeln jetzt den Fall  $q = 2$ , welcher auf etwas umständlicherem Wege zu gleich einfachen Resultaten führt. Die Form  $f$  sei primitiv in Bezug auf 2. Wir machen für dieselbe von den in 4. angegebenen Bezeichnungen Gebrauch. Der Modul  $2^t$  sei grösser als die Potenz  $2^{1+\nu_{n-1}}$ ; man hat dann immer  $t \geq 2$ , und wenn  $\nu_{n-1} > 0$ , auch  $t \geq 3$ .

Wir werden die Grössen  $f(2^t)$  finden, indem wir  $f$  als *Hauptrest* für den Modul  $2^t$  annehmen, also für  $f$  den Typus zulassen:

$$f \equiv \{ \Phi_1 + 2^{\nu_{\lambda-1}} [ \Phi_2 + \dots + 2^{\nu_{\lambda-2}} (\Phi_\lambda) ] \} \pmod{2^t},$$

wo die einzelnen  $\Phi_k$  Reste vorstellen, die in Bezug auf 2 primitiv sind, und entweder dem Typus

$$(R_I) \quad \Phi_k \equiv \begin{vmatrix} \alpha_1^{(k)}, \\ \alpha_2^{(k)}, \\ \dots \\ \alpha_{x_k}^{(k)} \end{vmatrix} \pmod{2^{t-\nu_{\lambda k-1}}}$$

oder, wenn  $x_k$  gerade ist, auch dem Typus

$$(R_{II}) \quad \Phi_k \equiv \begin{vmatrix} 2\alpha_1^{(k)}, A_1^{(k)}, \\ A_1^{(k)}, 2\tilde{\alpha}_1^{(k)}, \\ \dots \\ \dots \\ 2\alpha_{\frac{x_k}{2}}^{(k)}, A_{\frac{x_k}{2}}^{(k)}, \\ A_{\frac{x_k}{2}}^{(k)}, 2\tilde{\alpha}_{\frac{x_k}{2}}^{(k)} \end{vmatrix} \pmod{2^{t-\nu_{\lambda k-1}}}$$

angehören (*F. Q.*, p. 23). Dabei bedeuten die  $\alpha_h^{(k)}$ , ebenso wie die  $A_h^{(k)}$ , lauter ungerade Grössen.

Wir geben jedem Reste  $\phi_k$  vom Typus (R<sub>I</sub>) eine Zahl  $\tau_k = 1$ , und jedem Reste  $\phi_k$  vom Typus (R<sub>II</sub>) eine Zahl  $\tau_k = 2$ . Die  $x_k - 1$  Invarianten  $\sigma$  eines Restes  $\phi_k$  nennen wir  $\rho_1^{(k)}, \rho_2^{(k)}, \dots, \rho_{x_k-1}^{(k)}$ . Es gelten dann folgende Beziehungen (*F. Q.*, art. IV), wenn  $\tau_k = 1$ :

$$\rho_h^{(k)} = 1;$$

wenn  $\tau_k = 2$ :

$$\rho_{2h_0-1}^{(k)} = 2, \quad \rho_{2h_0}^{(k)} = 1;$$

ferner:

$$\sigma_{(\theta_{k-1}+h)} = \rho_h^{(k)}, \quad (h=1, 2, \dots, x_{k-1})$$

und:

$$\sigma_{\theta_k} = 1,$$

sodass die Zahlen  $\tau_k$  durch die Invarianten  $\sigma_h$  bestimmt sind. In der That erhält man insbesondere:

$$\tau_k = \sigma_{(\theta_{k-1}+1)} = \sigma_{(\theta_k-1)}.$$

Ein Ausdruck von der Gestalt  $\frac{1}{\tau} \phi$  mag, je nachdem  $\tau = 1$  oder  $= 2$  ist, kurz mit (I) oder mit (II) bezeichnet werden. Wir schicken zunächst einige Bemerkungen über die Congruenzen

$$(I) \equiv m \pmod{4} \quad \text{und} \quad (II) \equiv m \pmod{2}$$

voraus.

(I). Für einen Ausdruck

$$\Psi \equiv \alpha_1 \xi_1^2 + \alpha_2 \xi_2^2 + \dots + \alpha_x \xi_x^2 \pmod{4}$$

mögen  $\Psi_0, \Psi_1, \Psi_2, \Psi_3$  die Anzahlen der Lösungen von

$$\Psi \equiv 0, 1, 2, 3 \pmod{4}$$

vorstellen. Diese 4 Anzahlen können leicht nach *F. Q.*, art. VIII, gefunden werden. Man setze nämlich

$$4\Psi_0 = \phi_0 + \phi_1 + \phi_2 + \phi_3,$$

$$4\Psi_1 = \phi_0 - i\phi_1 - \phi_2 + i\phi_3,$$

$$4\Psi_2 = \phi_0 - \phi_1 + \phi_2 - \phi_3,$$

$$4\Psi_3 = \phi_0 + i\phi_1 - \phi_2 - i\phi_3,$$

wo  $i = \sqrt{-1}$ , und bilde die Einheiten:

$$(I) \quad \varepsilon = (-1)^{\left[\frac{x}{2}\right]} \cdot (-1)^{\sum_k^{1,x} \frac{a_k-1}{2}},$$

$$\delta = (-1)^{\left[\frac{x}{4}\right]} \cdot (-1)^{\left[\frac{x}{2}\right] \left(\left[\frac{x}{2}\right] + \sum_k^{1,x} \frac{a_k-1}{2}\right)} \cdot (-1)^{\sum_{k' < k''}^{1,x} \frac{a_{k'}-1}{2} \cdot \frac{a_{k''}-1}{2}}$$

Als dann geben die Formeln *F. Q.*, p. 62 und p. 64:

$$\phi_0 = 2^{2x}, \quad \phi_2 = 0$$

und

$$\phi_h = \left(\frac{1+\varepsilon}{2} - \frac{1-\varepsilon}{2}i\right) \varepsilon^{\frac{h-1}{2}} \cdot \delta \cdot (-i)^{x^2 \left(\frac{h-1}{2}\right)^2} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{x-2\left[\frac{x}{2}\right]} \cdot 2^{\frac{3x}{2}}. \quad (h=1, 3)$$

Wir unterscheiden die folgenden Fälle:

1)  $x \equiv 0 \pmod{2}$ .

$$(A) \quad \varepsilon = 1; \quad \phi_1 = \delta \cdot 2^{\frac{3x}{2}}, \quad \phi_3 = \delta \cdot 2^{\frac{3x}{2}}.$$

$$4\psi'_0 = 2^{2x} + \delta \cdot 2^{\frac{3x}{2}+1},$$

$$4\psi'_2 = 2^{2x} - \delta \cdot 2^{\frac{3x}{2}+1},$$

$$4\psi'_1 = 4\psi'_3 = 2^{2x}.$$

$$(B) \quad \varepsilon = -1; \quad \phi_1 = -i\delta \cdot 2^{\frac{3x}{2}}, \quad \phi_3 = i\delta \cdot 2^{\frac{3x}{2}}.$$

$$4\psi'_0 = 4\psi'_2 = 2^{2x},$$

$$4\psi'_1 = 2^{2x} - \delta \cdot 2^{\frac{3x}{2}+1},$$

$$4\psi'_3 = 2^{2x} + \delta \cdot 2^{\frac{3x}{2}+1}.$$

2)  $x \equiv 1 \pmod{2}$ .

$$(A) \quad \varepsilon = 1; \quad \psi_1 = \delta \cdot \frac{1+i}{\sqrt{2}} \cdot 2^{\frac{3x}{2}}, \quad \psi_3 = \delta \cdot \frac{1-i}{\sqrt{2}} \cdot 2^{\frac{3x}{2}}.$$

$$4\psi'_0 = 4\psi'_1 = 2^{2x} + \delta \cdot 2^{\frac{3x+1}{2}},$$

$$4\psi'_2 = 4\psi'_3 = 2^{2x} - \delta \cdot 2^{\frac{3x+1}{2}}.$$

$$(B) \quad \varepsilon = -1; \quad \psi_1 = \delta \cdot \frac{1-i}{\sqrt{2}} \cdot 2^{\frac{3x}{2}}, \quad \psi_3 = \delta \cdot \frac{1+i}{\sqrt{2}} \cdot 2^{\frac{3x}{2}}.$$

$$4\psi'_0 = 4\psi'_3 = 2^{2x} + \delta \cdot 2^{\frac{3x+1}{2}},$$

$$4\psi'_2 = 4\psi'_1 = 2^{2x} - \delta \cdot 2^{\frac{3x+1}{2}}.$$

In Betreff der Einheiten  $\varepsilon$  und  $\delta$  erwähnen wir noch einige Punkte.

1) Der Rest  $l \equiv \alpha_1 + \alpha_2 + \dots + \alpha_x \pmod{4}$  ist durch die Einheit  $\varepsilon$  bestimmt.

Da nämlich immer  $\alpha_k \equiv 1 \pmod{2}$  ist, so kommt zunächst

$$l \equiv x \pmod{2}, \quad (-1)^l = (-1)^x.$$

Sind ferner von den Zahlen  $\alpha_1, \alpha_2, \dots, \alpha_x$  im Ganzen  $x_0 \equiv -1 \pmod{4}$  und  $x - x_0 \equiv 1 \pmod{4}$ , so folgt einerseits:

$$\varepsilon = (-1)^{\left[\frac{x}{2}\right] - x_0},$$

andererseits:

$$l \equiv (x - x_0) - x_0 \equiv x - 2x_0 \pmod{4},$$

mithin:

$$(-1)^{\left[\frac{l}{2}\right]} = (-1)^{\left[\frac{x}{2}\right] - x_0} = \varepsilon.$$

Im Speciellen findet man, wenn  $x \equiv 1 \pmod{2}$ :

$$l \equiv \varepsilon \pmod{4}.$$

2) Ersetzt man  $\psi$  durch  $-\psi$ , also  $\alpha_k \pmod{4}$  durch  $-\alpha_k \pmod{4}$ ,

so mögen an die Stelle von  $\varepsilon$  und  $\delta$  die Einheiten  $\varepsilon^-$  und  $\delta^-$  treten. Man erhält unmittelbar:

$$\varepsilon^- = \varepsilon \cdot (-1)^x, \quad \delta^- = \delta \cdot \varepsilon^{x-1},$$

also:

$$\begin{aligned} 1) \quad x \equiv 0 \pmod{2}, \quad \varepsilon^- &= \varepsilon, & \delta^- &= \delta \cdot \varepsilon; \\ 2) \quad x \equiv 1 \pmod{2}, \quad \varepsilon^- &= -\varepsilon, & \delta^- &= \delta. \end{aligned}$$

Dasselbe Resultat erschliesst man auch leicht aus der aufgestellten Tabelle, indem man die Beziehungen  $\psi_{-h}^1 = (-\psi)_h$  beachtet.

3) Wir wollen

$$\psi^1 \equiv \alpha_2 \xi_2^2 + \dots + \alpha_x \xi_x^2 \pmod{4}$$

setzen, und die Einheiten  $\varepsilon$  und  $\delta$ , welche zu  $\psi^1$  gehören, mit  $\varepsilon^1$  und  $\delta^1$  bezeichnen.

Mit Hilfe der Relationen

$$\left[ \frac{x}{2} \right] - \left[ \frac{x-1}{2} \right] \equiv x-1, \quad \left[ \frac{x}{4} \right] - \left[ \frac{x-1}{4} \right] \equiv (x-1) \left[ \frac{x-1}{2} \right] \pmod{2}$$

findet man:

$$\varepsilon = (-1)^{x-1} \cdot (-1)^{\frac{a-1}{2}} \cdot \varepsilon^1, \quad \delta = (-1)^{x \cdot \frac{a-1}{2}} \cdot \varepsilon^{(x-1) + \frac{a-1}{2}} \cdot \delta^1, \quad (a=a_1)$$

also:

$$\begin{aligned} 1) \quad x \equiv 0 \pmod{2}; \quad (A) \quad \varepsilon &= \varepsilon^1; & \delta &= \delta^1, & \alpha &\equiv -\varepsilon^1 \pmod{4}; \\ & & (B) \quad \varepsilon &= -\varepsilon^1; & \delta &= -(-1)^{\frac{a-1}{2}} \cdot \delta^1, & \alpha &\equiv \varepsilon^1 \pmod{4}. \\ 2) \quad x \equiv 1 \pmod{2}; \quad (A) \quad \alpha &\equiv -\varepsilon \pmod{4}; & \varepsilon^1 &= -\varepsilon, & \delta &= -\varepsilon \cdot \delta^1; \\ & & (B) \quad \alpha &\equiv \varepsilon \pmod{4}; & \varepsilon^1 &= \varepsilon, & \delta &= \delta^1. \end{aligned}$$

(II). Jetzt liege ein Ausdruck vor:

$$X \equiv (\alpha_1 \xi_1^2 + A_1 \xi_1 \tilde{\xi}_1 + \tilde{\alpha}_1 \tilde{\xi}_1^2) + \dots + \left( \alpha_x \xi_x^2 + A_x \xi_x \tilde{\xi}_x + \tilde{\alpha}_x \tilde{\xi}_x^2 \right) \pmod{2},$$

und es bedeute  $X_0$  und  $X_1$  die Anzahl der Lösungen von

$$X \equiv 0 \quad \text{und} \quad X \equiv 1 \pmod{2}.$$

Setzt man:

$${}_2X_0 = \chi_0 + \chi_1, \quad {}_2X_1 = \chi_0 - \chi_1,$$

ferner:

$$(II) \quad \theta = \left( \frac{2}{4a_1\tilde{a}_1 - A_1^2} \right) \cdots \left( \frac{2}{4a_{\frac{x}{2}}\tilde{a}_{\frac{x}{2}} - A_{\frac{x}{2}}^2} \right),$$

so kommt nach *F. Q.*, p. 65:

$$\chi_0 = 2^x, \quad \chi_1 = \theta \cdot 2^{\frac{x}{2}},$$

also:

$${}_2X_0 = 2^x + \theta \cdot 2^{\frac{x}{2}}, \quad {}_2X_1 = 2^x - \theta \cdot 2^{\frac{x}{2}}.$$

Nach diesen Vorbereitungen wollen wir versuchen, eine Formel aufzustellen, mit deren Hilfe die Grössen  $f(2')$  für Reste von  $n (> 1)$  Variablen auf entsprechende Grössen für Reste von weniger als  $n$  Variablen zurückgeführt werden können. Für Reste  $f$  von einer Variablen hat man einfach  $f(2') = 1$ .

Da wir  $f$  als Hauptrest für den Modul  $2'$  voraussetzen, so gilt jedenfalls eine Congruenz

$$f \equiv \Phi_1 + 2^{w_{x_1}} f^{(x_1)} \pmod{2'}, \quad (w_{x_1} \geq 1)$$

wo  $\Phi_1$  einen Rest vom Typus (R<sub>I</sub>) oder (R<sub>II</sub>) bedeutet. Wir unterscheiden zwei Fälle, je nachdem die Invariante  $\tau_1 = \sigma_1$  den Werth 1 oder 2 erhält.

$$(\underline{\sigma_1 = 1}).$$

Ist zunächst  $\sigma_1 = 1$ , so lässt  $f$  sich zugleich in der Form schreiben:

$$f \equiv \alpha \xi^2 + 2^{w_1} f^{(1)} \pmod{2'},$$

wo  $\alpha$  ungerade ist, und  $f^{(1)}$  einen in Bezug auf 2 primitiven Rest vorstellt,



welcher im Falle  $\omega_1 = 0$  ( $x_1 > 1$ ) eine erste Invariante  $\sigma$  gleich 1 ergibt. Ueberhaupt folgen die Invarianten  $\sigma_h^{(1)}$  und  $2^{\omega_h^{(1)}}$  von  $f^{(1)}$  aus den Gleichungen:

$$\sigma_{h-1}^{(1)} = \sigma_h, \quad \omega_{h-1}^{(1)} = \omega_h. \quad (h=2, 3, \dots, n-1)$$

Die Anzahl  $f(2^t)$  der incongruenten Substitutionen  $\mathbb{T}$  von einer Determinante  $\equiv 1 \pmod{2^t}$ , welche den Rest  $f$  in sich selbst überführen, drückt sich in ähnlicher Weise aus wie oben die Zahl  $f(p^t)$ . In der That, die erste Verticalreihe einer Substitution  $\mathbb{T}$  muss immer von  $n$  Zahlen  $\xi_i \pmod{2^t}$  gebildet sein, welche

$$(t) \quad f(\xi_i) \equiv \alpha \pmod{2^t}$$

liefern. Dazu tritt in den Fällen, wo  $x_1 > 1$  ist, noch die Bedingung, dass nicht zu gleicher Zeit die sämtlichen Congruenzen

$$(c) \quad \xi_1 \equiv 1, \xi_2 \equiv 1, \dots, \xi_{x_1} \equiv 1 \pmod{2}$$

bestehen dürfen (*F. Q.*, p. 172 und 128). Wir bezeichnen mit  $A \cdot 2^{(n-1)t}$ , je nachdem  $x_1 = 1$  oder  $> 1$  ist, entweder die Anzahl aller möglichen Lösungen  $\xi_i$  von (t), oder nur die Anzahl aller derjenigen Lösungen  $\xi_i$ , welche nicht zugleich die Congruenzen (c) erfüllen.

Die Betrachtungen in *F. Q.*, p. 172, zeigen, dass wirklich jedem dieser Systeme  $\xi_i$  Substitutionen  $\mathbb{T}$  entsprechen, welche den Rest  $f$  in sich selbst transformiren. Ebenso wie in 5. schliesst man dann, dass jedes solche System  $\xi_i$  zu genau soviel verschiedenen  $\mathbb{T}$  Veranlassung giebt, als verschiedene Substitutionen von einer Determinante  $\equiv 1 \pmod{2^t}$  existiren, welche auf den Rest  $2^{\omega_1} f^{(1)}$  ohne Wirkung sind. So gewinnt man die Beziehung:

$$f(2^t) = 2^{(n-1)t + \omega_1[(n-1)^2 - 1]} \cdot A \cdot f^{(1)}(2^{t-\omega_1}).$$

In Betreff der Grösse  $A$  unterscheiden wir die Fälle  $x_1 = 1$  und  $x_1 > 1$ .

1°. Ist zunächst  $x_1 = 1$ , so giebt unsere Annahme über  $t$ , (wenn  $n > 1$ ), jedenfalls  $t \geq 3$ . Nach dem Satze 4. (3) muss daher  $A \cdot 2^{3(n-1)}$  die Anzahl der Lösungen von  $f(\xi_i) \equiv \alpha \pmod{8}$  ausdrücken.

Indem man in  $f$  alle Glieder fortlässt, welche durch 8 theilbar sind, erlangt  $f$  entweder den Typus:

$$(1) \quad f \equiv \alpha \xi^2 \pmod{8}.$$

In diesem Falle hat man  $f \equiv \alpha \pmod{8}$ , sobald  $\xi \equiv 1 \pmod{2}$  ist. Die Anzahl der Lösungen von  $f \equiv \alpha \pmod{8}$  beträgt demnach  $4 \cdot 2^{3(n-1)}$  und man findet:

$$A = 4.$$

Oder  $f$  gehört einem der beiden Typen an:

$$(2) \quad \begin{aligned} f &\equiv \alpha \xi^2 + 4(I) \\ f &\equiv \alpha \xi^2 + 4(II) + 4(I) \end{aligned} \pmod{8}.$$

In dem Ausdrucke  $4(I)$  erscheint mindestens ein Glied  $4\alpha\mathfrak{y}^2 \equiv 4\mathfrak{y} \pmod{8}$ . Durch Änderung des Restes von  $\mathfrak{y} \pmod{2}$  können wir aus jeder Lösung von  $f \equiv \alpha \pmod{8}$  eine solche von  $f \equiv \alpha + 4 \pmod{8}$  herleiten, und umgekehrt. Diese zwei Congruenzen besitzen also gleich viel, nämlich  $2 \cdot 2^{3(n-1)}$  Lösungen, und man erhält:

$$A = 2.$$

Oder  $f$  gehört dem Typus an:

$$(3) \quad f \equiv \alpha \xi^2 + 4(II) \pmod{8}.$$

In diesem Falle hat  $f \equiv \alpha \pmod{8}$  stets  $\xi \equiv 1 \pmod{2}$  und  $(II) \equiv 0 \pmod{2}$  zur Folge. Bildet man für den Rest  $(II)$ , von  $x_2 = x$  Variablen, nach der Formel (II), eine Einheit  $\theta$ , so ergibt sich die Anzahl der Lösungen von  $(II) \equiv 0 \pmod{2}$  gleich  $2^{x-1} \left(1 + \theta \cdot 2^{\frac{-x}{2}}\right)$ , und man bekommt

$$A = 2 \left(1 + \frac{\theta}{2^{\frac{x}{2}}}\right).$$

Oder  $f$  gehört dem Typus an:

$$(4) \quad f \equiv \alpha \xi^2 + 2(I) \pmod{8}.$$

Dann ist  $f \equiv \alpha \pmod{8}$  identisch mit  $\xi \equiv 1 \pmod{2}$  und  $(I) \equiv 0 \pmod{4}$ . Gehören zu dem Reste  $(I)$  von  $x_2 = x$  Variablen, gemäss der Formel (I), zwei Einheiten  $\varepsilon$  und  $\delta$ , so liefert die obige Tabelle:

1)  $x \equiv 0 \pmod{2}$ ,

$$\begin{aligned} \varepsilon = 1, & \quad A = \left(1 + \frac{a}{2^{z-1}}\right); \\ \varepsilon = -1, & \quad A = 1. \end{aligned}$$

2)  $x \equiv 1 \pmod{2}$ ,

$$A = \left(1 + \frac{a}{2^{\frac{z-1}{2}}}\right).$$

Oder  $f$  gehört endlich dem Typus an:

$$(5) \quad f \equiv \alpha \xi^2 + 2(I) + 4(I)_1 \pmod{8}.$$

In diesem Falle enthält  $2(I)$  mindestens ein Glied  $2\alpha x^2 \equiv 2y \pmod{4}$ , mit dessen Hilfe die Lösungen von  $f \equiv 1$  und  $f \equiv 3 \pmod{4}$  einander eindeutig zugeordnet werden können; und ebenso erscheint in  $4(I)_1$  mindestens ein Glied  $4\alpha x^2 \equiv 4y \pmod{8}$ , in Folge dessen die Congruenzen  $f \equiv \alpha$  und  $f \equiv \alpha + 4 \pmod{8}$  gleichviel Lösungen zulassen. So findet man leicht:

$$A = 1.$$

2°. Jetzt sei  $x_1 > 1$ . Wir theilen für einen Moment die Systeme  $\xi_i$ , welche  $f(\xi_i) \equiv 1 \pmod{2}$  ergeben, in Systeme erster oder zweiter Art ein, je nachdem sie den Bedingungen (c) entgegen sind oder mit denselben harmoniren. Irgend ein System  $\xi_i \pmod{4}$  erster Art möge die Congruenz

$$(a) \quad f(\xi_i) \equiv \alpha \pmod{4}$$

erfüllen. Da ein solches System zugleich einen bestimmten Werth des Restes  $f(\xi_i) \pmod{8}$  ergibt, so wird es nur einer der beiden Congruenzen  $f(\xi_i) \equiv \alpha \pmod{8}$  und  $f(\xi_i) \equiv \alpha + 4 \pmod{8}$  Genüge leisten. Ist nun von den Zahlen  $\xi_1, \xi_2, \dots, \xi_{x_1}$  etwa  $\xi_k$  die erste, welche nicht ungerade ausfällt, und ändern wir den Rest  $\xi_k \pmod{4}$  in  $\xi_k + 2 \pmod{4}$ , so geht aus dem Systeme  $\xi_i \pmod{4}$  ein anderes System erster Art hervor, welches offenbar der anderen von diesen beiden Congruenzen genügen muss. So erhellt, dass diese zwei Congruenzen gleichviel Lösungen erster Art zulassen.

Beachtet man jetzt die Definition der Grösse  $A$  und den Satz 4. (3), so folgt, dass in allen Fällen die Anzahl der Lösungen erster Art von  $(\alpha)$  durch  $A \cdot 2^{2(n-1)}$  ausgedrückt ist. Man gelangt zu dieser Anzahl, indem man die Anzahl aller möglichen Lösungen dieser Congruenz um die Anzahl ihrer Lösungen zweiter Art vermindert.

Wir unterscheiden die Fälle  $x_1 \equiv 0 \pmod{2}$  und  $x_1 \equiv 1 \pmod{2}$ , schreiben aber der Einfachheit halber  $x$  für  $x_1$ .

1. Zunächst sei  $x \equiv 0 \pmod{2}$ . In diesem Falle treten überhaupt keine Lösungen zweiter Art auf, da die Congruenzen  $(c)$  stets  $f(\xi_i) \equiv x \pmod{2}$  nach sich ziehen.

Entweder ist nun  $f$  von dem Typus:

$$(1) \quad f \equiv (I) \pmod{4}.$$

Lassen wir dieselben Bezeichnungen wie oben für  $\Psi$  gelten, so liefert die aufgestellte Tabelle:

$$\begin{array}{lll} \varepsilon = 1, & A = 1; & [\delta = \delta^1, (-1)^{\frac{a-1}{2}} = -\varepsilon^1] \\ \varepsilon = -1, & A = \left(1 + \frac{\delta^1}{2^{\frac{x}{2}-1}}\right). & [\delta = -(-1)^{\frac{a-1}{2}} \cdot \delta^1, (-1)^{\frac{a-1}{2}} = \varepsilon^1] \end{array}$$

Oder  $f$  ist von dem Typus:

$$(2) \quad f \equiv (I) + 2(I)_1 \pmod{4}.$$

Alsdann erscheint in  $2(I)_1$  ein Glied  $2\alpha x^2 \equiv 2x \pmod{4}$ , welches bewirkt, dass  $f \equiv 1$  und  $f \equiv 3 \pmod{4}$  gleichviel Lösungen zulassen. Demnach kommt einfach:

$$A = 1.$$

2. Endlich sei  $x \equiv 1 \pmod{2}$ . Wir unterscheiden dieselben zwei Fälle. Entweder ist  $f$  von dem Typus:

$$(1) \quad f \equiv (I) \pmod{4}.$$

Identificiren wir den Rest  $(I)$  mit dem obigen Ausdrucke  $\Psi$ , so entsteht für Systeme  $\xi_i$  zweiter Art:

$$f(\xi_i) \equiv \alpha_1 + \alpha_2 + \dots + \alpha_x \equiv \varepsilon \pmod{4}.$$

Diese Systeme gehen also nur den Fall an, wo  $\alpha \equiv \varepsilon \pmod{4}$  ist. Mithin kommt:

$$\alpha \equiv -\varepsilon \pmod{4}, \quad A = \left(1 - \frac{\partial}{2^{\frac{x-1}{2}}}\right); \quad (\varepsilon^2 = -1, \partial = -\varepsilon \cdot \partial')$$

$$\alpha \equiv \varepsilon \pmod{4}, \quad A = \left(1 + \frac{\partial}{2^{\frac{x-1}{2}}} - \frac{1}{2^{x-2}}\right) = \left(1 - \frac{\partial}{2^{\frac{x-1}{2}}}\right) \left(1 + \frac{\partial'}{2^{\frac{x-3}{2}}}\right). \quad (\varepsilon^2 = 1, \partial = \partial')$$

Oder  $f$  ist vom Typus:

$$(2) \quad f \equiv (I) + 2(I)_1 \pmod{4}.$$

Als dann bewirkt ein jedes Glied  $2ax^2 \equiv 2x \pmod{4}$  aus  $2(I)_1$ , dass  $f \equiv 1$  und  $f \equiv 3 \pmod{4}$  sowohl gleichviel Lösungen erster, wie gleichviel Lösungen zweiter Art besitzen, und man findet:

$$A \equiv \left(1 - \frac{1}{2^{x-1}}\right).$$

$$\underline{(\sigma_1 = 2)}.$$

Wenn  $\sigma_1 = 2$  ist, so lässt  $f$  sich zugleich in der Form schreiben:

$$f \equiv 2(\alpha \xi^2 + A\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) + 2^{\omega_2} f^{(2)} \pmod{2^t},$$

wo  $\alpha$  und  $A$  ungerade sind, und  $f^{(2)}$  einen in Bezug auf 2 primitiven Rest bedeutet. Die Invarianten  $\sigma_h^{(2)}$  und  $2^{\omega_h^{(2)}}$  von  $f^{(2)}$  bestimmen sich aus den Gleichungen:

$$\sigma_{h-2}^{(2)} = \sigma_h, \quad \omega_{h-2}^{(2)} = \omega_h. \quad (h=3, 4, \dots, n-1)$$

Wir betrachten die  $f(2^t)$  Substitutionen  $\mathbb{T}$  von einer Determinante  $\equiv 1 \pmod{2^t}$ , welche den Rest  $f$  in sich selbst verwandeln. In jeder dieser Substitutionen muss die erste Verticalreihe von  $n$  Zahlen  $\xi_i \pmod{2^t}$  gebildet werden, welche

$$(t) \quad f(\xi_i) \equiv 2\alpha \pmod{2^t}$$

ergeben. Ferner dürfen diese Zahlen nicht zugleich alle Bedingungen

$$(e) \quad \xi_1 \equiv 0, \xi_2 \equiv 0, \dots, \xi_{x_1} \equiv 0 \pmod{2}$$

erfüllen (*F. Q.*, p. 175 und 129). Wir bezeichnen mit  $2A \cdot 2^{(n-1)t}$  die Anzahl aller Systeme  $\xi_i \pmod{2^t}$ , welche der Congruenz (*t*), aber nicht sämtlichen Congruenzen (*c*) genügen.

Jedes dieser Systeme  $\xi_i$  tritt wirklich in mindestens einer von den Substitutionen  $T$  als erste Verticalreihe auf (*F. Q.*, pp. 175—177), also etwa in einem  $T_0$ . Es fragt sich, für wieviel verschiedene  $T$  ein solches System  $\xi_i$  die erste Verticalreihe bildet; offenbar für alle diejenigen  $T$ , welche zusammengesetzt sind aus  $T_0$  und aus einer Substitution  $T'$  mit der ersten Verticalreihe  $1, 0, \dots, 0$ . Man hat also zu ermitteln, wie viele Substitutionen vom Typus

$$T' \equiv \begin{vmatrix} 1, U, \dots\dots\dots \\ 0, \eta_0, \dots\dots\dots \\ 0, \eta_1, \dots\dots\dots \\ \dots\dots\dots\dots\dots\dots \\ 0, \eta_{n-2}, \dots\dots\dots \end{vmatrix} \equiv 1 \pmod{2^t}$$

den Rest  $f$  in sich selbst transformiren.

Setzen wir

$$f^{(1)} \equiv (4\alpha\tilde{\alpha} - A^2)\eta_0^2 + 2^{2t+1} \cdot \alpha \cdot f^{(2)}(\eta_1, \dots, \eta_{n-2}) \pmod{2^{t+1}},$$

so entsteht zunächst die Bedingung

$$f^{(1)}(\eta_0, \eta_1, \dots, \eta_{n-2}) \equiv (4\alpha\tilde{\alpha} - A^2) \pmod{2^{t+1}}.$$

Dieser Congruenz mögen  $\frac{1}{2}A^{(1)} \cdot 2^{(n-2)t}$  verschiedene Systeme  $\eta_i \pmod{2^t}$  Genüge leisten. Durch Ueberlegungen, wie sie in *F. Q.*, pp. 176—177, angestellt sind, überzeugt man sich, dass wirklich jedem dieser Systeme  $\eta_i$  Substitutionen  $T$  zukommen, welche den Rest  $f$  in sich selbst transformiren; es fragt sich wieviele.

Die Gesamtheit aller solcher  $T$  wird hervorgehen, indem man eine beliebige unter ihnen, etwa  $T_0$ , mit allen Substitutionen

$$\mathfrak{Z} \equiv \begin{pmatrix} 1, & U, & V_1, & \dots, & V_{n-2} \\ 0, & 1, & \tilde{V}_1, & \dots, & \tilde{V}_{n-2} \\ 0, & 0, & t_1^1, & \dots, & t_1^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & t_{n-2}^1, & \dots, & t_{n-2}^{n-2} \end{pmatrix} \equiv 1 \pmod{2^t}$$

zusammensetzt, welche  $f \pmod{2^t}$  in sich selbst überführen. Für  $\mathfrak{Z}$  findet man  $2U \equiv 0, V_h \equiv 0, \tilde{V}_h \equiv 0 \pmod{2^t}$ ; und man erkennt, dass die Anzahl der verschiedenen  $\mathfrak{Z}$  durch  $2F(2^t)$  ausgedrückt ist, falls  $F$  den Rest  $2^{\omega_2} f^{(2)}$  bedeutet. So ergibt sich die Beziehung

$$f(2^t) = 2^{(n-1)t + (n-2)t + 1 + \omega_2(n-2)^2 \dots 1} \cdot A \cdot A^{(1)} \cdot f^{(2)}(2^{t-\omega_2}).$$

Nun hat man zugleich

$$f^{(1)}(2^{t+1}) = 2^{(n-2)(t+1) + (\omega_2+1)(n-2)^2 \dots 1} \cdot A^{(1)} \cdot f^{(2)}(2^{t-\omega_2});$$

also kommt endlich:

$$f(2^t) = 2^{(n-1)t - n(n-3)} \cdot A \cdot f^{(1)}(2^{t+1}).$$

Um die Grösse  $A$  zu finden, beachte man, dass das System der  $x_1$  Congruenzen (c) sich als identisch mit dem Systeme  $\frac{1}{2} \frac{\partial f}{\partial \xi_i} \equiv 0 \pmod{2}$  ( $i = 1, 2, \dots, n$ ) erweist. Nach 4. (4) muss infolgedessen  $A \cdot 2^{n-1}$  die Anzahl aller Lösungen von

$$(\alpha) \quad \frac{1}{2} f(\xi_i) \equiv 1 \pmod{2}$$

vorstellen, bei welchen die  $n$  Zahlen  $\frac{1}{2} \frac{\partial f}{\partial \xi_i}$  nicht sämtlich gerade sind. Wir wollen für  $x_1$  einfach  $x$  setzen.

Entweder ist  $\frac{1}{2} f$  vom Typus:

$$[I] \quad \frac{1}{2} f \equiv (II) \pmod{2}.$$

In diesem Falle liefern die Congruenzen (c) stets  $f \equiv 0 \pmod{4}$ ; sie

sind also nicht mit  $(\alpha)$  verträglich. Gehört zu  $(II)$  wie oben eine Einheit  $\theta$ , so kommt demnach:

$$A = \left(1 - \frac{\theta}{2^{\frac{x}{2}}}\right).$$

Oder  $\frac{1}{2}f$  ist vom Typus:

$$[2] \quad \frac{1}{2}f \equiv (II) + (I) \pmod{2}.$$

Dann erscheint in  $(I)$  ein Glied  $\alpha x^2 \equiv x \pmod{2}$ , welches zur Folge hat, dass  $\frac{1}{2}f \equiv 0$  und  $\frac{1}{2}f \equiv 1 \pmod{2}$  gleichviel Lösungen zulassen, man betrachte diese Congruenzen für sich oder zusammen mit den Congruenzen  $(c)$ . Man erhält also:

$$A = \left(1 - \frac{1}{2^x}\right).$$

Die Grösse  $A^{(1)}$  bestimmt sich mit Hilfe der Formeln aus  $(\sigma_1 = 1)$ . Im Falle [1] findet man, wenn  $x = 2$ :  $A^{(1)} = 4$ , und wenn  $x > 2$ :

$$A^{(1)} = 2 \left(1 + \frac{\theta^1}{2^{\frac{x}{2}-1}}\right), \quad \text{wobei} \quad \theta = \left(\frac{2}{4a\tilde{a} - A^2}\right) \cdot \theta^1;$$

im Falle [2] wird immer  $A^{(1)} = 2$ .

Wir setzen jetzt allgemein:

$$f(2^t) = 2^{\frac{n(n-1)}{2}t + \sum_h^{1, n-1} \omega_h \left(\frac{(n-h)(n-h+1)}{2} - 1\right)} \cdot \prod_h^{1, n-1} \sigma_h \cdot f\{2\}. \quad \left(t > 1 + \sum_h^{1, n-1} \omega_h\right)$$

Unsere Recursionsformeln gehen dann in

$$f\{2\} = A \cdot f^{(1)}\{2\}$$

über, und auf Grund der gefundenen Werthe von  $A$  können wir den vollständigen Ausdruck der Grösse  $f\{2\}$  hinschreiben.



Es bedeute, wie bisher,  $f$  einen aus  $\lambda$  Gliedern bestehenden Hauptrest, wo  $\lambda$  gleich ist der um 1 vermehrten Anzahl aller durch 2 theilbaren Grössen  $2^{\omega_h}$  ( $h = 1, \dots, n - 1$ ). Ferner bezeichne  $\mu - 1$  die Anzahl aller Grössen aus der Reihe  $\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}$  ( $h = 1, \dots, n - 1$ ), welche den Factor 4 enthalten, und  $\nu - 1$  die Anzahl aller Grössen dieser Reihe, welche durch 8 aufgehen.

Die Grösse  $f\{2\}$  ist dann gleich einem Producte aus der Potenz  $\frac{2^{(2\mu-1)+(\nu-1)}}{\Pi\sigma_h}$  und aus  $\lambda$  Factoren  $\mathfrak{A}_k$ , welche den  $\lambda$  einzelnen Resten  $\Phi_k$  entsprechen, und folgendermaassen bestimmt werden:

(I). So oft  $\Phi_k$  ein Rest vom Typus  $(R_I)$  ist, nehme man:

$$\mathfrak{A}_k = \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{2^4}\right) \dots \left(1 - \frac{1}{2^{2^{\left[\frac{x_k-1}{2}\right]}}}\right) \cdot \alpha_k,$$

und setze  $\alpha_k = 1$ , falls die Zahlen  $\tau_{k-1} \cdot 2^{\omega_{h_{k-1}}}$  und  $2^{\omega_{h_k}} \cdot \tau_{k+1}$  nicht beide durch 4 theilbar sind; andernfalls aber bilde man für  $\Phi_k$ , gemäss den Formeln (I), zwei Einheiten  $\varepsilon_k$  und  $\delta_k$ , und setze:

1) wenn  $x_k \equiv 0 \pmod{2}$ ,

je nachdem  $\varepsilon_k = 1$  oder  $= -1$  ist,

$$\alpha_k = \left(1 + \delta_k \cdot 2^{-\frac{x_k}{2} + 1}\right)^{-1} \quad \text{oder} \quad = 1;$$

2) wenn  $x_k \equiv 1 \pmod{2}$ ,

$$\alpha_k = \left(1 + \delta_k \cdot 2^{-\frac{x_k-1}{2}}\right)^{-1}.$$

(II). So oft  $\Phi_k$  ein Rest vom Typus  $(R_{II})$  ist, nehme man:

$$\mathfrak{A}_k = \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{2^4}\right) \dots \left(1 - \frac{1}{2^{x_k}}\right) \cdot \alpha_k,$$

und setze  $\alpha_k = 1$ , falls die Zahlen  $\tau_{k-1} \cdot 2^{\omega_{h_{k-1}}}$  und  $2^{\omega_{h_k}} \cdot \tau_{k+1}$  nicht beide durch 4 theilbar sind; andernfalls aber bilde man für  $\Phi_k$ , gemäss der Formel (II), eine Einheit  $\theta_k$ , und setze:

$$\alpha_k = \left(1 + \theta_k \cdot 2^{-\frac{x_k}{2}}\right)^{-1}.$$

Die Richtigkeit dieser Ausdrücke ergibt sich mit Hilfe eines Schlusses von  $n - 1$  auf  $n$ .

Wir erwähnen noch folgende Relation. Bedeutet  $M - 1$  die Anzahl aller durch 4 theilbaren Grössen  $\tau_k \cdot 2^{u_k} \cdot \tau_{k+1}$ , so hat man

$$2^{n-1} = 2^{M-1} \cdot \frac{\sigma_1 \sigma_2 \dots \sigma_{n-1}}{\tau_1 \tau_2 \dots \tau_\lambda}.$$

Die Congruenzen  $f(\xi_i) \equiv m \pmod{2^i}$  sind sehr eingehend von Herrn C. JORDAN in der Abhandlung *Sur la forme canonique des congruences du second degré et le nombre de leurs solutions*<sup>1</sup> untersucht worden. Die über diesen Gegenstand hier angestellten Betrachtungen sind indess wesentlich anderer Art. Die am Anfange gegebenen Werthe der Zahlen  $\Psi_h$  und  $X_h$  wird man auch aus Art. 8. des *Mémoire sur la représentation des nombres par des sommes de cinq carrés*<sup>2</sup> von H. SMITH ableiten können.

### 7. Die Grössen $f\{q\}$ in ihrer Abhängigkeit von den Characteren $C$ .

Die Einheiten, welche in den Grössen  $f\{q\}$  auftreten, sind offenbar Invarianten der Form  $f$ . Sie müssen sich daher mit Hilfe der besonderen Characteren  $C$  ausdrücken lassen, die wir in 2. aufgezählt haben.

Um dieses darzuthun setzen wir  $f$ , wie in 2., als charakteristische Form ihres Genus voraus. Die aus den ersten  $h$  Reihen von  $f$  gebildeten symmetrischen Minoren mögen also Werthe  $\sigma_h d_{h-1} \varphi_h$  von solcher Art liefern, dass ein jedes  $\varphi_h$  relativ prim zu  $2o_1 o_2 \dots o_{n-1}$  und zu  $\varphi_{h-1} \cdot \varphi_{h+1}$  ausfällt. Ferner sei  $f$  primitiv.

Bedeutet  $q$  zunächst irgend eine ungerade Primzahl, die nicht in  $\Delta$  aufgeht, so hängt  $f\{q\}$ , ausser von der Zahl  $n$ , nur in dem Falle eines geraden  $n$ , noch von einer Einheit  $\theta$  ab. Man findet dieselbe gleich

$$\left( \frac{(-1)^{\frac{n}{2}} \Delta}{q} \right) = \left( \frac{(-1)^{\frac{n}{2}-1} o_1 o_3 \dots o_{n-3} o_{n-1}}{q} \right).$$

Ist weiter  $q = p$  irgend eine ungerade Primzahl aus  $\Delta$ , so sind, laut Voraussetzung, sämtliche Zahlen  $\varphi_h$  zu  $p$  prim. Wir besitzen also in  $f$  eine *Grundform* für den Modul  $p$  (*F. Q.*, pp. 35—36). Die Classe  $f$

<sup>1</sup> Journal de LIOUVILLE, Deuxième Série, T. XVII, 1872, pp. 368—402.

<sup>2</sup> Mémoires présentés à l'Académie des Sciences de Paris, T. XXIX, N° 1.

liefert infolgedessen für einen jeden Modul  $p'$  unter anderen Resten auch folgenden Hauptrest:

$$\varphi \equiv \left( \begin{array}{c} \frac{\sigma_1 \varphi_1}{\sigma_0 \varphi_0}, \\ \\ o_1 \cdot \frac{\sigma_2 \varphi_2}{\sigma_1 \varphi_1}, \\ \dots \\ \dots \\ o_1 o_2 \dots o_{n-1} \cdot \frac{\sigma_n \varphi_n}{\sigma_{n-1} \varphi_{n-1}} \end{array} \right) \pmod{p'}.$$

In dem Ausdrücke von  $f\{p\} = \varphi\{p\}$  gehört zu jeder von den  $\lambda$  Zahlen  $x_k$ , welche gerade ausfällt, eine Einheit  $\theta$ . Setzt man  $\theta_{k-1} = r$ ,  $\theta_k = s$ , und ist also  $s - r = x_k \equiv 0 \pmod{2}$ , so nimmt eine solche Einheit den Werth an:

$$\left( \frac{(-1)^{\frac{s-r}{2}} o_{r+1} o_{r+3} \dots o_{s-3} o_{s-1} \cdot \sigma_r \varphi_r \sigma_s \varphi_s}{p} \right).$$

Endlich sei  $q = 2$ . Nach Voraussetzung sind alle Zahlen  $\varphi_h$  ungerade, und  $f$  stellt eine *Grundform* für den Modul 2 vor. Man gewinnt daher, nach *F. Q.*, pp. 34—36, einen Hauptrest

$$\varphi \equiv \{ \Phi_1 + 2^{\omega_1} [ \Phi_2 + \dots + 2^{\omega_{\lambda-1}} (\Phi_\lambda) ] \} \pmod{2^t}$$

der Classe  $f$ , indem man die Einzelreste  $\Phi_k$  in folgender Weise auswählt. Zur Abkürzung sei  $\theta_{k-1} = r$ ,  $\theta_k = s$ ; dann nehme man, wenn  $\tau_k = 1$ :

$$\left. \begin{array}{l} \frac{2^{e_r} \cdot \Phi_k}{o_1 o_2 \dots o_r} \equiv \psi_1 + o_{r+1} \psi_2 + \dots + o_{r+1} o_{r+2} \dots o_{s-1} \psi_{s-r} \\ \psi_i \equiv \frac{\varphi_{r+i}}{\varphi_{r+i-1}} \xi_i^2 \end{array} \right\} \pmod{2^{t-e_r}}.$$

und wenn  $\tau_k = 2$ , also jedenfalls  $s - r \equiv 0 \pmod{2}$ :

$$\left. \begin{array}{l} \frac{2^{e_r}}{o_1 o_2 \dots o_r} \cdot \Phi_k \equiv \psi_1 + o_{r+1} o_{r+2} \psi_2 + \dots + o_{r+1} o_{r+2} \dots o_{s-2} \frac{\psi_{s-r}}{2} \\ \psi_i \equiv \frac{2\varphi_{r+2i-1}}{\varphi_{r+2i-2}} \xi_i^2 + 2A_i \xi_i \eta_i + \frac{o_{r+2i-1} \varphi_{r+2i} - A_i^2 \varphi_{r+2i-2}}{2\varphi_{r+2i-1}} \eta_i^2 \end{array} \right\} \pmod{2^{t-e_r}},$$

wo die  $A_i$  irgend welche ungerade Zahlen bedeuten sollen.

So oft nun  $\tau_k = 1$  ist und die Zahlen  $\sigma_{r-1} 2^{er}$  und  $2^e \sigma_{s+1}$  beide durch 4 theilbar sind, kommen für den Ausdruck  $f\{2\}$  zwei aus den Coefficienten von  $\phi_k$  gebildete Einheiten  $\varepsilon$  und  $\delta$  in Betracht. Indem man wiederholt die für ungerade  $a$  und  $\alpha$  geltende Congruenz

$$\frac{aa-1}{2} \equiv \frac{a-1}{2} + \frac{a+1}{2} \pmod{2}$$

anwendet, ergibt sich  $\varepsilon$  als eine Potenz von  $-1$  mit dem Exponenten:

$$\frac{\varphi_r-1}{2} + \frac{\varphi_s-1}{2} + \sum \frac{o_{s-2u+1}+1}{2}, \quad (u=1, 2, \dots, \left[\frac{s-r}{2}\right])$$

während  $\delta$  aus zwei Potenzen von  $-1$  zusammengesetzt erscheint, von denen die eine den Exponenten:

$$\frac{\varphi_r-1}{2} \cdot \frac{\varphi_{r+1}-1}{2} + \frac{\varphi_{r+1}-1}{2} \cdot \frac{\varphi_{r+2}-1}{2} + \dots + \frac{\varphi_{s-1}-1}{2} \cdot \frac{\varphi_s-1}{2} + \sum_h^{r+1, s-1} \frac{\varphi_h-1}{2} \cdot \frac{o_h+1}{2}$$

und die andere den Exponenten:

$$\begin{aligned} & \frac{\varphi_r + (-1)^{s-r}}{2} \cdot \left( \frac{\varphi_s-1}{2} + \sum \frac{o_{s-2u+1}+1}{2} \right) + \frac{\varphi_s-1}{2} \cdot \sum \frac{o_{s-2v}+1}{2} \\ & + \sum \frac{o_{s-2u+1}+1}{2} \cdot \frac{o_{s-2v}+1}{2} \quad \left( \begin{array}{l} u, v, w=1, 2, \dots, \left[\frac{s-r}{2}\right] \\ u \leq v \end{array} \right) \end{aligned}$$

erhält.

Die erste Potenz aus  $\delta$  findet man mit Hilfe der Formeln aus F. Q., p. 85 gleich

$$\left| \left( \frac{\varphi_{r+1}}{\varphi_r} \right) (-1)^{\frac{l(l+1)}{2}} \right| \left| \left( \frac{\varphi_{s-1}}{\varphi_s} \right) (-1)^{\frac{l(l-1)}{2}} \right| \cdot \prod_h^{r+1, s-1} \left( \frac{\varphi_h}{o_h} \right),$$

während die zweite, ebenso wie die Einheit  $\varepsilon$  sich unmittelbar durch die Characteren  $(-1)^{\frac{\varphi_r-1}{2}}$  und  $(-1)^{\frac{\varphi_s-1}{2}}$  ausdrückt.

Es verdient beachtet zu werden, dass in  $f\{2\}$  die Einheiten  $\varepsilon$  und  $\delta$  nur in der Verbindung  $\frac{\delta + \delta^-}{2}$  auftreten, wo  $\delta^- = \delta \cdot \varepsilon^{\alpha-1}$  die zu  $-\phi_k$  gehörige Einheit  $\delta$  bedeutet,

So oft ferner  $\tau_k = 2$  ist, und die Zahlen  $\sigma_{r-1} 2^r$  und  $2^r \sigma_{s+1}$  beide durch 4 theilbar sind, begegnet man in  $f\{2\}$  einer aus den Coefficienten von  $\phi_k$  gebildeten Einheit

$$\theta = \left( \frac{2}{\sigma_{r+1} \sigma_{r+3} \dots \sigma_{s-3} \sigma_{s-1} \varphi_r \varphi_s} \right).$$

Wir bemerken schliesslich, dass die mit  $f = \sum a_{ik} x_i x_k$  adjungirte Form  $f' = \frac{(-1)^l}{d_{n-2}} \cdot \sum \frac{\partial \Delta}{\partial a_{n-i+1, n-k+1}} x'_i x'_k$  lauter Grössen  $f'\{q\}$  liefert, welche mit den Grössen  $f\{q\}$  identisch sind. Es erhellt dieses leicht aus dem Umstande, dass die Invarianten  $\sigma'_h, \sigma''_h$  und die Zahlen  $\varphi'_h$  der Form  $f'$  die Gleichungen erfüllen:

$$\sigma'_h = \sigma_{n-h}, \quad \sigma''_h = \sigma_{n-h}, \quad \varphi'_h = (-1)^l \cdot \varphi_{n-h}.$$

### 8. Ausdruck für die Formenanzahl eines Genus.

Irgend ein primitives Genus  $f$  sei definiert durch seine Invarianten  $I, \sigma_h, \sigma_h, C$ , welche allen für die Existenz des Genus nothwendigen Bedingungen genügen mögen. Wir bilden, nach den in 5., 6. und 7. angegebenen Regeln, die verschiedenen Grössen  $f\{q\}$ , welche zu unserem Genus gehören. Wir setzen ferner

$$\mathfrak{D} = \prod_h^{1, n-1} \sigma_h^{h(n-h)}$$

und

$$c_n = 2 \frac{\Gamma\left(\frac{1}{2}\right) \cdot \Gamma\left(\frac{2}{2}\right) \dots \Gamma\left(\frac{n}{2}\right)}{\left\{ \Gamma\left(\frac{1}{2}\right) \right\}^{\frac{n(n+1)}{2}}},$$

wo  $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$ ,  $\Gamma(1) = 1$ ,  $\Gamma(u+1) = u\Gamma(u)$ .

Wir wollen von dem Falle absehen, wo  $n = 2$  und  $(-1)^l \sigma_1 = \Delta$  eine negative Quadratzahl ist, das Genus also lauter zerlegbare Formen enthält.

Schliesst man diesen Fall aus, so besitzt das über alle möglichen Primzahlen  $q = 2, 3, 5, \dots$  erstreckte Product

$$1) \quad M = c_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \dots \sigma_{n-1}} \cdot \frac{1}{f\{2\}} \cdot \frac{1}{f\{3\}} \cdot \frac{1}{f\{5\}} \cdots \frac{1}{f\{q\}} \cdots$$

stets einen endlichen Werth.

Um dieses nachzuweisen, wollen wir in  $M$  die Grösse

$$\frac{\left(1 - \frac{1}{q^2}\right) \left(1 - \frac{1}{q^4}\right) \cdots \left(1 - \frac{1}{q^{2 \left[\frac{n-1}{2}\right]}}\right)}{f\{q\}} = E_q$$

als allgemeines Glied einführen. Solches kann leicht geschehen, indem man mit der Identität

$$1 = S_2 S_4 \dots S_{2 \left[\frac{n-1}{2}\right]} \cdot \prod_q \left(1 - \frac{1}{q^2}\right) \left(1 - \frac{1}{q^4}\right) \cdots \left(1 - \frac{1}{q^{2 \left[\frac{n-1}{2}\right]}}\right)$$

multipliziert, wo  $S_{2k}$  die Summe  $\sum_1^{2k} \frac{1}{z^{2k}}$  bedeutet. Man weiss, dass diese Summe den Werth  $\frac{1}{2} B_k \cdot \frac{(2\pi)^{2k}}{(2k)!}$  hat, falls unter  $B_k$  die  $k^{\text{te}}$  BERNOULLI'sche Zahl verstanden wird.

Für jede nicht in  $2\Delta$  enthaltene Primzahl  $p$  kommt, wenn  $n \equiv 1 \pmod{2}$ :

$$E_p = 1,$$

und wenn  $n \equiv 0 \pmod{2}$ :

$$E_p = \left\{ 1 - \left( \frac{(-1)^{\frac{n}{2}} \Delta}{p} \right) p^{-\frac{n}{2}} \right\}^{-1}. \quad \left(\frac{\Delta}{p}\right) = \left(\frac{(-1)^{\frac{n}{2}} \Delta}{p}\right)$$

Sind also die nicht in  $\Delta$  aufgehenden, ungeraden Primzahlen, ihrer Grösse nach geordnet:  $p, p', p'', \dots$ , so wird das unendliche Product:

$$E_p E_{p'} E_{p''} \dots,$$

je nachdem  $n \equiv 1 \pmod{2}$  oder  $n \equiv 0 \pmod{2}$ , gleich 1 oder gleich der Summe:

$$\sum \left( \frac{(-1)^{\frac{n}{2}} \Delta}{m} \right) \frac{1}{m^{\frac{n}{2}}},$$

wo  $m$  alle positiven und zu  $2\Delta$  relativ primen ganzen Zahlen durchläuft. Zur Bezeichnung dieser DIRICHLET'schen Summe mag das Symbol

$$D_n \left[ (-1)^{\frac{n}{2}} \Delta \right]$$

dienen.

Man setze nun:

$$c_n \cdot S_2 S_4 \dots S_{\left[\frac{n-1}{2}\right]} = c_n,$$

d. i., wenn  $n \equiv 1 \pmod{2}$ :

$$c_n = \left(\frac{1}{2}\right)^{\frac{n-3}{2}} \cdot B_1 B_2 \dots B_{\frac{n-1}{2}} \cdot \frac{1}{1 \cdot 2 \dots \frac{n-1}{2}},$$

und wenn  $n \equiv 0 \pmod{2}$ :

$$c_n = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot B_1 B_2 \dots B_{\frac{n-2}{2}} \cdot \frac{1}{\pi^2},$$

und lasse ferner  $\mathfrak{d}$  alle Primzahlen aus  $2\mathfrak{D}$  durchlaufen. Dann können wir endlich schreiben, wenn  $n \equiv 1 \pmod{2}$ :

$$2) \quad M = c_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \dots \sigma_{n-1}} \cdot \prod_{\mathfrak{d}} E_{\mathfrak{d}},$$

und wenn  $n \equiv 0 \pmod{2}$ :

$$2) \quad M = c_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \dots \sigma_{n-1}} \cdot \prod_{\mathfrak{d}} E_{\mathfrak{d}} \cdot D_n \left[ (-1)^{\frac{n}{2}-1} \cdot \mathfrak{D} \right].$$

Diese Ausdrücke zeigen in der That, dass  $M$  einen endlichen und positiven Werth annimmt.

Für ein Genus von binären zerlegbaren Formen gewinnt man ein ähnliches convergentes Product  $M$ , indem man  $\frac{1 - \frac{1}{q}}{f\{q\}}$  an die Stelle von  $\frac{1}{f\{q\}}$  treten lässt.

Wir behaupten nun:

*Die Formenanzahl unseres Genus besitzt den Ausdruck:*

$$M \cdot \Omega,$$

wo  $M$  das angegebene Product und  $\Omega$  eine positive unendliche Grösse bedeutet, die nur von  $n$  und  $I$  und von der Anzahl der Darstellungen der Zahl  $\circ$  durch die Formen des Genus abhängt.

In den Fällen eines definiten Genus ( $I = \circ$  oder  $I = n$ ) ist insbesondere dieses  $\Omega$  gleich der Anzahl aller ganzzahligen  $n$ -reihigen Substitutionen von der Determinante 1, und mithin  $M$  gleich der über alle Classen  $Cl$  des Genus erstreckten Summe  $\sum \frac{1}{t(Cl)}$ .

Wir werden uns begnügen, das vorstehende Resultat für die Fälle definiten (und zwar positiver) Genera zu erweisen. Dabei werden wir von den DIRICHLET'schen Methoden<sup>1</sup> Gebrauch machen, und in den Fällen  $n > 2$  einen Schluss von  $n - 1$  auf  $n$  zu Hülfe nehmen.

---

## Zweiter Theil.

### 9. Das Maass eines positiven Genus dargestellt durch einen gewissen Grenzwert.

Ein positives Genus  $G$  von  $n (\geq 2)$  Variablen sei definit durch seine Ordnung  $O$ :

$$d_0, \quad \begin{pmatrix} \sigma_1 & \sigma_2 & \dots & \sigma_{n-2} & \sigma_{n-1} \\ o_1 & o_2 & \dots & o_{n-2} & o_{n-1} \end{pmatrix}, \quad I = \circ$$

---

<sup>1</sup> DIRICHLET, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.* (CRELLE'S JOURNAL, Bd. XIX.)



und seine Charactere  $C$ . Wir setzen voraus, dass dieselben den für die Existenz des Genus nothwendigen Bedingungen genügen.  $d_0$  sei gleich 1, das Genus also primitiv.

Es sei  $\Delta$  die Determinante des Genus, und  $k$  eine beliebige zu  $2\Delta$  relativ prime ganze Zahl. Durch die Kenntniss der Invarianten  $O$  und  $C$  sind wir befähigt, die Reste unseres Genus für einen jeden beliebigen Modul hinzuschreiben. Insbesondere können wir also irgend einen Hauptrest  $\varphi$  in Bezug auf den Modul  $\sigma_1 \cdot 8\Delta R$  angeben. Der erste Coefficient von  $\varphi$  heisse  $\sigma_1 \alpha$ . Die Zahl  $\alpha$  ist dann sicher relativ prim zu  $8\Delta R$ .

Wir richten unser Augenmerk auf den quadratischen Character von  $\alpha$  in Bezug auf den Modul  $8\Delta R$ . Enthält  $\Delta$  im Ganzen  $\delta$  ungerade Primzahlen  $\delta$ , und  $R$  im Ganzen  $r$  ungerade Primzahlen  $r$ , so wird dieser Character durch die Gesammtheit der folgenden  $2 + \delta + r$  Symbole defnirt:

$$C(\alpha) \quad \left(-1\right)^{\frac{\alpha-1}{2}}, \quad \left(\frac{2}{\alpha}\right), \quad \left(\frac{\alpha}{\delta}\right), \quad \left(\frac{\alpha}{r}\right).$$

Diese Symbole können zum Theil Charactere des Genus vorstellen, zum Theil können sie bei anderer Wahl des Restes  $\varphi$  andere Werthe erlangen.<sup>1</sup>

<sup>1</sup> Man überzeugt sich leicht, dass in dieser Beziehung die nachstehenden Sätze gelten:

Eine jede Einheit  $\left(\frac{\alpha}{r}\right)$  kann sowohl gleich + 1 wie gleich - 1 ausfallen.

Eine Einheit  $\left(\frac{\alpha}{\delta}\right)$  hat einen festen Werth, wenn  $\sigma_1 \equiv 0 \pmod{\delta}$ , also  $\varphi$  von dem Typus  $\sigma_1 \alpha \xi^2 \pmod{\delta}$  ist. Sonst kann dieselbe beide Werthe  $\pm 1$  annehmen.

Was die Einheiten  $\left(-1\right)^{\frac{\alpha-1}{2}}$  und  $\left(\frac{2}{\alpha}\right)$  anlangt, so unterliegen dieselben keiner Beschränkung, wenn  $\sigma_1 = 2$  ist. Ebenso im Allgemeinen, wenn  $\sigma_1 = 1$  ist; nur bestehen hier die folgenden Ausnahmefälle:

1. Ist  $\varphi \equiv \alpha \xi^2 \pmod{8}$ , so sind beide Einheiten  $\left(-1\right)^{\frac{\alpha-1}{2}}$  und  $\left(\frac{2}{\alpha}\right)$  Charactere.
2. Ist  $\varphi \equiv \alpha \xi^2 \pmod{4}$ , oder  $\varphi \equiv \alpha \xi^2 + \beta \gamma^2 \pmod{4}$  und  $\alpha \equiv \beta \pmod{4}$ , oder  $\varphi \equiv \alpha \xi^2 + \beta \gamma^2 + \gamma \zeta^2 \pmod{4}$  und  $\alpha \equiv \beta \equiv \gamma \pmod{4}$ , so hat die Einheit  $\left(-1\right)^{\frac{\alpha-1}{2}}$  einen festen Werth.

Wie in 6. bezeichnen wir mit  $x$  den Index der ersten von den  $n$  Zahlen  $o_1, o_2, \dots, o_{n-1}, o_n (= 0)$ , welche gerade ausfällt.

Wir denken uns in jeder überhaupt existirenden Classe des Genus je eine Form ausgesucht, welche nach dem Modul  $\sigma_1 \cdot 8\Delta R$  den Rest  $\varphi$  lässt. Eine beliebige der so gewonnenen Formen sei  $f$ .

Wir bestimmen für die Variablen von  $f$  alle Systeme  $\xi_1, \xi_2, \dots, \xi_n$ , welche dem Ausdrucke  $f(\xi_i)$  einen Werth  $\sigma_1 m$  ertheilen, wo  $m$  prim zu  $8\Delta R$  ist und den Gleichungen

$$C(m) = C(\alpha)$$

genügt, welche aber dabei, falls  $x > 1$  ist, nicht die Bedingungen

$$(c) \quad \xi_1 \equiv \xi_2 \equiv \dots \equiv \xi_x \equiv \sigma_1 \pmod{2}$$

erfüllen. Ueber alle diese Werthsysteme  $\xi_i (\geq 0, 0, \dots, 0)$  erstrecken wir alsdann die Summe

$$\Xi = \rho \sum \frac{1}{\left\{ \frac{1}{\sigma_1} f(\xi_i) \right\}^{\frac{n}{2}(1+\rho)}},$$

und wir wollen den Grenzwert ermitteln, welchen diese Summe für ein positives, unendlich abnehmendes  $\rho$  erreicht.

Die definirten Werthsysteme  $\xi_i$  werden in einer gewissen Anzahl  $A$  von arithmetischen Progressionen

$$\xi_1 = 8\Delta R \cdot X_1 + v_1, \quad \xi_2 = 8\Delta R \cdot X_2 + v_2, \quad \dots, \quad \xi_n = 8\Delta R \cdot X_n + v_n$$

3. Ist  $\varphi \equiv a\xi^2 + 2\beta\gamma^2 \pmod{8}$  und setzt man  $(-1)^{\frac{a\beta+1}{2}} = \varepsilon$ , so können  $(-1)^{\frac{a-1}{2}}$  und  $\left(\frac{2}{a}\right)$  sich nur mit  $\varphi$  so ändern, dass  $\varepsilon^{\frac{a-1}{2}} \cdot \left(\frac{2}{a}\right)$  fest bleibt.

4. Wenn  $\varphi \equiv a\xi^2 + 2(\beta\gamma^2 + \gamma^2) \pmod{8}$ , so sind für die Einheiten  $(-1)^{\frac{a-1}{2}}$  und  $\left(\frac{2}{a}\right)$  nur drei von den vier Systemen  $\pm 1, \pm 1$  zulässig. Ist nämlich  $\beta \equiv -\gamma \pmod{4}$ , so kann der Fall nicht eintreten, dass  $(-1)^{\frac{a-1}{2}}$  ungeändert bleibt, während  $\left(\frac{2}{a}\right)$  in  $-\left(\frac{2}{a}\right)$  übergeht, und hat man  $\beta \equiv \gamma \equiv \theta \cdot a \pmod{4}$ ,  $\theta = \pm 1$ , so ist der Fall ausgeschlossen, dass  $(-1)^{\frac{a-1}{2}}$  in's Gegentheil umschlägt, während  $\left(\frac{2}{a}\right)$  sich in  $\theta \cdot \left(\frac{2}{a}\right)$  verwandelt.

enthalten sein. Man bezeichne mit  $2^{3(n-1)} \cdot A_2$ , wenn  $x > 1$ , die Anzahl aller derjenigen Lösungen  $\xi_i \pmod{8}$  von

$$\frac{1}{\sigma_1} \varphi(\xi_i) \equiv \alpha \pmod{8},$$

welche nicht zugleich den Bedingungen (c) genügen, und wenn  $x = 1$ , die Anzahl aller möglichen Lösungen dieser Congruenz; ferner mit  $2^{n-1} \cdot A_p$  die Anzahl aller Lösungen von

$$\varphi(\xi_i) \equiv \sigma_1 \alpha \pmod{p},$$

wenn  $p$  eine der ungeraden Primzahlen aus  $\Delta R$  bedeutet. In den Ausdrücken von  $A_2$  und  $A_p$  erscheint  $\alpha$ , wie wir wissen, nur in den Einheiten  $C(\alpha)$ . Dieser Umstand lässt erkennen, dass die Anzahl  $A$  den Werth hat:

$$A = (8\Delta R)^n \cdot \frac{1}{2} \prod_q \left\{ \frac{1}{2} \left( 1 - \frac{1}{q} \right) A_q \right\}, \quad (q=2, \vartheta, r)$$

wo  $q$  die  $1 + \vartheta + r$  Primzahlen von  $8\Delta R$  durchläuft.

Setzt man für die  $\xi_i$  zunächst nur alle diejenigen Systeme, welche in einer der  $A$  Progressionen vorkommen, so ergibt sich der Grenzwert der entstehenden Summe für ein  $\rho = +0$ , nach *F. Q.*, p. 148, gleich

$$e_n \cdot \frac{(8\Delta R)^{-n}}{\sqrt{\frac{\Delta}{\sigma_1^n}}},$$

wo

$$e_n = \frac{\left\{ \Gamma\left(\frac{1}{2}\right) \right\}^n}{\Gamma\left(1 + \frac{n}{2}\right)} = \pi^{\left[\frac{n}{2}\right]} \cdot \frac{2^{\left[\frac{n+1}{2}\right]}}{n(n-2)\dots\left(n-2\left[\frac{n-1}{2}\right]\right)}.$$

Für die ganze Summe  $\Xi$  wird daher

$$\text{Lim}(\Xi)_{(\rho=0)} = e_n \cdot \frac{(8\Delta R)_1}{2^{2+\vartheta+r}} \cdot \frac{\sigma_1^{\frac{n}{2}}}{\sqrt{\Delta}} \cdot \prod_q A_q, \quad (q=2, \vartheta, r)$$

wo  $(8\Delta R)_1$  das über alle Primzahlen  $q$  von  $8\Delta R$  erstreckte Product  $\prod \left(1 - \frac{1}{q}\right)$  bedeutet.

Eine Summe  $X$ , von ähnlicher Beschaffenheit wie  $\Xi$ , mag jetzt nur alle solchen Systeme  $\xi_i = x_i$  umfassen, in welchen die  $n$  Zahlen  $\xi_1, \xi_2, \dots, \xi_n$  keinen gemeinschaftlichen Theiler haben. Offenbar entstehen alle möglichen Systeme  $\xi_i$ , wenn wir diese besonderen Systeme  $x_i$  mit allen positiven und zu  $8\Delta R$  relativ primen Zahlen  $z$  multipliciren. Man findet daher

$$\bar{\Xi} = X \cdot \sum \frac{1}{z^{n(1+\rho)}},$$

und in der Grenze für  $\rho = 0$ :

$$\text{Lim} \left( \frac{\bar{\Xi}}{X} \right) = \sum \frac{1}{z^n}.$$

Die hier auftretende Summe hat bekanntlich den Werth:

$$(8\Delta R)_n \cdot S_n,$$

wenn  $S_n$  die Summe  $1 + \frac{1}{2^n} + \frac{1}{3^n} + \dots$  und  $(8\Delta R)_n$  das über alle Primzahlen  $q$  von  $8\Delta R$  erstreckte Product  $\prod \left( 1 - \frac{1}{q^n} \right)$  ausdrückt.

Wir bemerken noch, dass die Summe  $X$  sich in  $t(f)$  unter einander identische Summen  $X_0$  zerlegen lässt. Dabei ist unter  $t(f)$ , wie in 1., die Anzahl aller Substitutionen von der Determinante 1 verstanden, welche die Form  $f$  in sich selbst transformiren. (Solche Summen  $X_0$  haben dann auch in Fällen indefiniter Formen einen Sinn.)

Wir bilden endlich eine Doppelsumme:

$$S = \rho \cdot \sum \frac{1}{t(f)} \cdot \sum \frac{1}{\left| \frac{f(x_i)}{\sigma_1} \right|^{\frac{n}{2}(1+\rho)}},$$

erstreckt, einmal: über alle die inäquivalenten Formen  $f(\equiv \varphi, \text{ mod } \sigma_1 \cdot 8\Delta R)$ , die wir oben als Repräsentanten der einzelnen Classen des Genus aufgestellt hatten; und dann, für jede dieser Formen  $f$ : über alle solchen Systeme  $x_1, x_2, \dots, x_n$  ohne gemeinsamen Theiler, welche einer Congruenz

$$\frac{f(x_i)}{\sigma_1} \equiv \alpha z^2 \pmod{8\Delta R}$$

genügen, wo  $z$  zu  $8\Delta R$  relativ prim ist, und welche dabei, falls  $x > 1$ , nicht alle Bedingungen

$$(c) \quad x_1 \equiv x_2 \equiv \dots \equiv x_x \equiv \sigma_1 \pmod{2}$$

erfüllen.

Der Grenzwert  $l$  der früheren Summe  $X$  hatte sich als unabhängig von der speciellen Form  $f$  erwiesen. Infolgedessen muss der Grenzwert  $L$  dieser Doppelsumme gleich  $l \times \sum \frac{1}{t(f)}$  sein. Durch die hier erscheinende einfache Summe ist aber das Maass  $M$  unseres Genus dargestellt; man erhält demnach:

$$L = e_n \cdot \frac{(8\Delta R)_1}{2^{2+b+r}} \cdot \frac{1}{(8\Delta R)_n \cdot S_n} \cdot \frac{\sigma_1^{\frac{n}{2}}}{\sqrt{\Delta}} \cdot \prod_q A_q \cdot M. \quad (q=2, \delta, r)$$

Wir werden jetzt für  $L$  einen zweiten Ausdruck ableiten, und durch Vergleichung der beiden Ausdrücke werden wir dann die in 8. aufgestellten Formeln als richtig erkennen.

### 10. Bestimmung desselben Grenzwertes auf anderem Wege.

Wir haben soeben den Grenzwert  $L$  gefunden, indem wir uns die Summe  $S$  erst nach den einzelnen Formen  $f$ , und dann nach der numerischen Grösse der Zahlen  $\frac{f(x_i)}{\sigma_1}$  geordnet dachten. Nun handelt es sich in  $S$  um lauter positive Glieder; wir müssen daher zu demselben Grenzwert  $L$  gelangen, wenn wir die Summe  $S$  direct nach der Grösse der Zahlen  $\frac{1}{\sigma_1} f(x_i) = m$  anordnen. Durch ein solches Arrangement entsteht für  $S$  zunächst ein Ausdruck von der Gestalt:

$$\rho \sum \frac{M(m)}{m^{\frac{n}{2}(1+\rho)}}$$

wo die Summation alle positiven Zahlen  $m$  betrifft, die zu  $8\Delta R$  relativ prim sind und den Gleichungen:  $C(m) = C(\alpha)$  genügen.

Für jede dieser Zahlen  $m$  hat die Grösse  $M(m)$  folgende Bedeutung. Es bezeichne  $m(f)$ , wie oft eine bestimmte Form  $f$  die Zahl  $\sigma_1 m$  mit Hilfe von Systemen  $x_i$  darzustellen vermag, welche keinen gemeinsamen Theiler  $> 1$  haben, und ausserdem, falls  $x > 1$ , nicht alle Bedingungen (c) erfüllen. Dann ist:

$$M(m) = \sum \frac{m(f)}{t(f)},$$

wo die Summe sich über alle die Formen  $f$  erstreckt. Die Grösse  $M(m)$  bildet also, wie wir uns nach *F. Q.*, p. 142 ausdrücken, das Maass für alle die definirten Darstellungen  $x_i$  der Zahl  $\sigma_1 m$  durch die verschiedenen Formen  $f$  des Genus  $G$ .

Treten in der Zahl  $m$  im Ganzen  $\mu$  ungerade Primzahlen  $p_1, p_2, \dots, p_\mu$  auf, so erscheint, nach *F. Q.*, p. 143, dieses Maass  $M(m)$  als das  $2^\mu$ -fache von dem Maasse eines bestimmten positiven Genus  $G(m)$  von Formen mit  $n - 1$  Variablen, welches enge mit dem Genus  $G$  zusammenhängt. Von den Sätzen, welche diesen Zusammenhang feststellen, wollen wir hier soviel anführen, als für die Bestimmung der Grösse  $M(m)$  von Wichtigkeit ist (Vgl. *F. Q.*, art. XVIII).

(1). Es sei zunächst  $n = 2$ , in welchem Falle  $\Delta$  und  $\sigma_1$  identisch sind. Je nach der Beschaffenheit der Zahl  $m$  bieten sich zwei Möglichkeiten dar.

Entweder ist für die Zahl  $m$  die quadratische Congruenz

$$- \Delta \equiv z^2 \pmod{\sigma_1 m}$$

nicht lösbar. In diesem Falle existirt auch das Genus  $G(m)$  nicht, und man hat sein Maass gleich 0 zu setzen.

Oder diese Congruenz ist lösbar und besitzt  $2^\mu$  Lösungen  $z \pmod{\sigma_1 m}$ . Alsdann wird das Genus  $G(m)$  von der einen Form  $g = \xi^2$  gebildet und liefert das Maass 1.

In beiden Fällen kann man schreiben:

$$M(m) = \left\{ 1 + \left( \frac{-\Delta R^2}{p_1} \right) \right\} \left\{ 1 + \left( \frac{-\Delta R^2}{p_2} \right) \right\} \dots \left\{ 1 + \left( \frac{-\Delta R^2}{p_\mu} \right) \right\}.$$

Der zweite Fall ereignet sich beispielsweise, wenn man für  $\sigma_1 m$  den ersten Coefficienten einer der Formen  $f$  wählt, was man thun darf. Denn

nach Voraussetzung ist ein solcher Coefficient  $\equiv \sigma_1 \alpha \pmod{\sigma_1 \cdot 8\Delta R}$ . Man hat dann jedenfalls  $\left(\frac{-\Delta}{m}\right) = 1$ , worin eine Bedingung für die Einheiten  $C(m) = C(\alpha)$  liegt.

(2). Ist  $n > 2$ , so erkennt man zunächst, dass die Invarianten von  $G(m)$  durch die Zahl  $m[C(m) = C(\alpha)]$  und die Invarianten von  $G$  stets in solcher Weise ausgedrückt sind, dass das Genus  $G(m)$  wirklich existirt. Wir haben bereits bemerkt, dass dieses Genus sich als positiv erweist. Man findet es auch primitiv. Seine Invarianten  $o$  und  $\sigma$  erlangen die Werthe:

$$\left( \begin{array}{c} \sigma_2, \sigma_3, \dots, \sigma_{n-1} \\ \sigma_1 m \cdot o_2, o_3, \dots, o_{n-1} \end{array} \right).$$

Es sei  $\Delta^1 = \prod_h^{2, n-1} o_h^{n-h}$  und  $\mathfrak{D}^1 = \prod_h^{2, n-1} o_h^{(h-1)(n-h)}$ . Ferner fallen seine Characterere derart aus, dass für jede seiner Formen  $g = \sum_1^{n-1} c_{ik} \xi_i \xi_k$  die  $\frac{n(n-1)}{2}$  Congruenzen:

$$(z) \quad - o_1 c_{ik} \equiv z_i z_k \pmod{\sigma_1 m}$$

je  $2^n$  Lösungen zulassen.

Wir nehmen nun an, die Formeln aus 8. seien bereits für den Fall  $n - 1$  erwiesen, und wir wollen dieselben benutzen, um das Maass von  $G(m)$  aufzustellen. Wir bilden zu dem Behufe für irgend eine Form  $g$  dieses Genus alle Grössen  $g\{q\}$ , und wir schreiben:

$$\frac{\left(1 - \frac{1}{q^2}\right) \left(1 - \frac{1}{q^4}\right) \dots \left(1 - \frac{1}{q^{2\left[\frac{n}{2}\right]-2}}\right)}{g\{q\}} = E_q^1.$$

Für das Maass von  $G(m)$  erhalten wir dann einen Ausdruck:

$$c_{n-1} \cdot \frac{\sqrt{\mathfrak{D}^1} \cdot \sigma_1^{\frac{n-2}{2}} m^{\frac{n-2}{2}}}{\sigma_2 \sigma_3 \dots \sigma_{n-1}} \cdot E_2^1 E_3^1 E_5^1 \dots E_q^1 \dots,$$

wo  $c_{n-1}$  eine Constante bedeutet; und die Grösse  $M(m)$  ergibt sich gleich diesem Ausdrucke, multiplicirt mit  $2^n$ . Es sind jetzt die Grössen  $E_q^1$  zu ermitteln.

1) Ist zunächst  $q$  irgend eine ungerade Primzahl, die weder in  $\Delta R$ , noch in  $m$  aufgeht, so kommt, nach 8., wenn  $n \equiv 0 \pmod{2}$ :

$$E_q^1 = 1,$$

und wenn  $n \equiv 1 \pmod{2}$ :

$$E_q^1 = \left[ 1 - \left( \frac{(-1)^{\frac{n-1}{2}} \sigma_1 m \Delta^1}{q} \right) \frac{1}{q^{\frac{n-1}{2}}} \right]^{-1}.$$

In dem letzteren Falle hat man zugleich:  $\left(\frac{\Delta^1}{q}\right) = \left(\frac{\Delta R^2}{q}\right)$ . Bildet man das Product  $\prod E_q^1$  über alle nicht in  $2\Delta Rm$  aufgehenden Primzahlen  $q$  in ihrer natürlichen Reihenfolge, so kann man für dasselbe, je nachdem  $n \equiv 0 \pmod{2}$  oder  $n \equiv 1 \pmod{2}$  ist, entweder 1 oder die Summe  $D_{\frac{n-1}{2}} \left[ (-1)^{\frac{n-1}{2}} \sigma_1 m \Delta R^2 \right]$  setzen.

2) Ist weiter  $q = p$  eine der  $\mu$  ungeraden Primzahlen aus  $m$ , und  $p^d$  die höchste Potenz dieser Primzahl, welche  $m$  theilt, so besitzt das Genus  $G(m)$  Reste vom Typus:

$$g \equiv c \xi^2 + p^d (c_1 \xi_1^2 + \dots + c_{n-2} \xi_{n-2}^2) \pmod{p^d}, \quad (v > d)$$

wo die Grössen  $c, c_1, \dots, c_{n-2}$  sämmtlich zu  $p$  prim sind. Aus den Congruenzen ( $z$ ) erschliesst man das Bestehen einer Congruenz:

$$-o_1 c \equiv z^2 \pmod{p^d};$$

man findet ferner:

$$c c_1 \dots c_{n-2} \equiv \left( \frac{\sigma_1 m}{p^d} \right)^{n-2} \cdot \Delta^1 \pmod{p^{d-d}}.$$

Im Falle eines  $n \equiv 0 \pmod{2}$ , wo zugleich  $\left(\frac{o_1 \Delta^1}{p}\right) = \left(\frac{\Delta}{p}\right)$ , kommt also

$$\left( \frac{c_1 \dots c_{n-2}}{p} \right) = \left( \frac{-\Delta}{p} \right).$$

Die Formeln aus 5. und 8. geben in diesem Falle:

$$E_p^1 = \frac{1}{2} \left[ 1 + \left( \frac{(-1)^{\frac{n-2}{2}} c_1 \dots c_{n-2}}{p} \right) \frac{1}{p^{\frac{n-2}{2}}} \right] = \frac{1}{2} \left[ 1 + \left( \frac{(-1)^{\frac{n}{2}} \Delta R^2}{p} \right) \frac{1}{p^{\frac{n-2}{2}}} \right],$$



dagegen, wenn  $n \equiv 1 \pmod{2}$ :

$$E_r^n = \frac{1}{2}.$$

3) Ist endlich  $q$  eine der Primzahlen aus  $8\Delta R$ , so besitzt das gegebene Genus  $G$  für einen jeden Modul  $q'$  Hauptreste  $f_1$  mit einem ersten Coefficienten  $\sigma_1 m$ . Aus diesen Hauptresten entspringen, nach den Sätzen aus *F. Q.*, art. XVIII, in einfacher Weise Hauptreste des Genus  $G(m)$ .

Bedeutet  $q$  zunächst eine der ungeraden Primzahlen  $\vartheta, r$ , so hat ein  $f_1$  den Typus:

$$f_1 \equiv \sigma_1 m \xi^2 + \frac{o_1 f^{(1)}}{\sigma_1 m} \pmod{q'}.$$

Der hier auftretende Rest  $f^{(1)} \pmod{q'^{-o_1}}$  bildet dann einen Rest des Genus  $G(m)$ .

Ist  $q = 2$ , so müssen die Fälle  $\sigma_1 = 1$  und  $\sigma_1 = 2$  unterschieden werden.

Im ersteren Falle hat ein  $f_1$  den Typus:

$$f_1 \equiv m \xi^2 + \frac{o_1 f^{(1)}}{m} \pmod{2^t},$$

wo  $f^{(1)}$  einen in Bezug auf 2 primitiven Rest vorstellt, welcher im Falle  $o_1 \equiv 1 \pmod{2}$  eine erste Invariante  $\sigma$  gleich 1 liefert. In diesem  $f^{(1)} \pmod{2^{t-o_1}}$  finden wir einen Rest von  $G(m)$ .

Im zweiten Falle ( $\sigma_1 = 2$ ) hat  $f_1$  den Typus:

$$f_1 \equiv 2(m\xi^2 + A\xi\tilde{\xi} + \tilde{m}\tilde{\xi}^2) + \frac{o_1 o_2 f^{(2)}}{m} \pmod{2^t},$$

wo  $A$  ungerade und  $f^{(2)}$  primitiv in Bezug auf 2 ist, und man gewinnt in

$$f^{(1)} \equiv \frac{(4m\tilde{m} - A^2)}{o_1} \eta^2 + 2o_2 f^{(2)} \pmod{2^{t+1}}$$

einen Rest des Genus  $G(m)$ .

In allen Fällen ergibt sich nun, nach 5. und 6., wenn  $t$  gross genug gewählt ist, die Beziehung:

$$f\{q\} = A_q \cdot f^{(1)}\{q\},$$

wobei  $A_q$  mit der in 9. auf diese Weise bezeichneten Grösse identisch ist.

Für die Ausdrücke  $E_q$  und  $E_q^1$  folgt hieraus, wenn  $n \equiv 0 \pmod{2}$  und  $> 2$ , die Gleichung:

$$E_q^1 = A_q E_q,$$

und wenn  $n \equiv 1 \pmod{2}$ :

$$E_q^1 = \frac{A_q E_q}{1 - \frac{1}{q^{\frac{n-1}{2}}}}.$$

Im Falle  $n = 2$  findet man in ähnlicher Weise:  $f\{q\} = A_q$ , also, da hier  $E_q = \frac{1}{f\{q\}}$  ist:  $A_q E_q = 1$ .

Fassen wir alles Vorhergehende zusammen, so können wir die Grösse  $M(m)$ , wenn  $n > 2$  ist, in folgender Form schreiben:

$$c_{n-1} \cdot \frac{\sqrt{\mathfrak{D}^1} \cdot \sigma_1^{\frac{n-2}{2}} m^{\frac{n-2}{2}}}{\sigma_2 \sigma_3 \dots \sigma_{n-1}} \cdot \prod_q A_q E_q \cdot (m), \quad (q=2, \partial, r)$$

wobei im Falle eines geraden  $n$ :

$$(m) = \prod_p \left\{ 1 + \left( \frac{(-1)^{\frac{n}{2}} \Delta R^2}{p} \right)^{\frac{1}{\frac{n-2}{2}}} \right\}, \quad (p=p_1, p_2, \dots, p_n)$$

und im Falle eines ungeraden  $n$ :

$$(m) = \frac{1}{(8\Delta R)_{n-1}} \cdot D_{\frac{n-1}{2}} \left[ (-1)^{\frac{n-1}{2}} \sigma_1 m \Delta R^2 \right].$$

Dieser Ausdruck bleibt nun auch für  $n = 2$  gültig, wenn  $c_1 = 1$  genommen wird.

Wir vergleichen jetzt den früher gefundenen Ausdruck von  $L$  mit dem Grenzwerte  $\text{Lim} \left( \rho \sum \frac{M(m)}{m^{\frac{n}{2}(1+\rho)}} \right)$ . Dadurch erhalten wir eine Beziehung

für das Maass  $M$  des gegebenen Genus. In dieselbe setzen wir

$$M = c_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \dots \sigma_{n-1}} \cdot \prod_q E_q \cdot D_R \cdot M_0, \quad (q=2, \partial, r)$$

wo  $D_R = 1$  sei für ein ungerades  $n$ , und gleich  $D_{\frac{n}{2}} \left[ (-1)^{\frac{n}{2}} \Delta R^2 \right]$  für ein gerades  $n$ , und wo  $\mathfrak{D} = \Delta \cdot \mathfrak{D}^1$  und

$$c_n = 2 \frac{c_1}{e_2} (n=2); = \frac{c_{n-1}}{e_n} \cdot \frac{2}{n} (n \equiv 0, \pmod{2}; n > 2); = \frac{c_{n-1}}{e_n} \cdot \frac{2}{n} \cdot S_{n-1} (n \equiv 1, \pmod{2})$$

die Grössen aus 8. bedeuten sollen. Die Grösse  $M_0$  erweist sich dann als unabhängig von der Zahl  $R$ , und es wird  $M_0 = 1$  sein müssen, damit die in 8. für  $M$  aufgestellten Ausdrücke in Wirklichkeit gelten.

Schreibt man noch  $\frac{2}{n}\rho$  für  $\rho$ , so lauten die Endformeln: wenn  $n = 2$ ,

$$(1) \quad 2 \cdot \frac{(8\Delta R)_1}{2^{2+\delta+\tau}} \cdot \frac{D_1(-\Delta R^2)}{(8\Delta R)_2 \cdot S_2} \cdot M_0 = \text{Lim} \rho \sum \frac{1}{m^{1+\rho}} \prod_p \left[ 1 + \left( \frac{-\Delta R^2}{p} \right) \right];$$

wenn  $n \equiv 0 \pmod{2}$  und  $> 2$ ,

$$(2) \quad \frac{(8\Delta R)_1}{2^{2+\delta+\tau}} \cdot \frac{D_n \left[ (-1)^{\frac{n}{2}} \Delta R^2 \right]}{(8\Delta R)_n \cdot S_n} \cdot M_0 \\ = \text{Lim} \left\{ \rho \sum \frac{1}{m^{1+\rho}} \prod_p \left[ 1 + \left( \frac{(-1)^{\frac{n}{2}} \Delta R^2}{p} \right)^{\frac{1}{\frac{n-2}{2}}} \right] \right\};$$

wenn  $n \equiv 1 \pmod{2}$ ,

$$(3) \quad \frac{(8\Delta R)_1}{2^{2+\delta+\tau}} \cdot \frac{(8\Delta R)_{n-1} \cdot S_{n-1}}{(8\Delta R)_n \cdot S_n} \cdot M_0 = \text{Lim} \left\{ \rho \sum \frac{1}{m^{1+\rho}} D_{\frac{n-1}{2}} \left[ (-1)^{\frac{n-1}{2}} \sigma_1 m \Delta R^2 \right] \right\}.$$

Dabei durchläuft  $m$ , wie erinnert werden mag, alle positiven und zu  $8\Delta R$  relativ primen ganzen Zahlen, für welche die  $2 + \delta + \tau$  Einheiten

$$U(m) \quad (-1)^{\frac{m-1}{2}}, \quad \left( \frac{2}{m} \right), \quad \left( \frac{m}{\delta} \right), \quad \left( \frac{m}{r} \right)$$

gewisse feste Werthe annehmen, die für ein  $n = 2$  jedenfalls der Bedingung  $\left( \frac{-\Delta R^2}{m} \right) = 1$  genügen.

Diese Zahlen  $m$  bilden offenbar die Individuen von  $(8\Delta R)^n \cdot \frac{(8\Delta R)_1}{2^{2+\delta+\tau}}$  arithmetischen Progressionen  $8\Delta R \cdot U + m_0$ , ( $U = 0, 1, \dots, \infty$ ) von der Differenz  $8\Delta R$ . Infolgedessen muss nach DIRICHLET die Gleichung bestehen:

$$(4) \quad \frac{(8\Delta R)_1}{2^{2+\delta+\tau}} = \text{Lim} \left( \rho \sum \frac{1}{m^{1+\rho}} \right).$$

Von derselben werden wir sofort Gebrauch machen, um in allen Fällen das Resultat  $M_0 = 1$  abzuleiten.

### 11. Beweis, dass $M_0 = 1$ ist.

Wir schicken die folgende Betrachtung voraus:

Es sei eine ganze positive oder negative Zahl  $N$  theilbar durch alle ungeraden Primzahlen, die unter einer gewissen Grenze  $G + 1$  liegen; ferner soll  $p$  die sämtlichen Primzahlen irgend einer zu  $2N$  relativ primen Zahl  $m$  durchlaufen; endlich sei  $\nu > 1$  und  $\gamma = \frac{1}{(\nu - 1)G^{\nu-1}}$ ; dann gelten die Ungleichungen:

$$1 - \gamma < D_\nu(N) < 1 + \gamma; \quad 1 < (2N)_\nu \cdot S_\nu < 1 + \gamma;$$

$$1 - \gamma < \prod \left[ 1 + \left( \frac{N}{p} \right) \frac{1}{p^\nu} \right] = \Pi_\nu < 1 + \gamma.$$

In der That, man erhält zunächst

$$D_\nu(N) = \sum \left( \frac{N}{m} \right) \frac{1}{m^\nu},$$

wo die Summation sich auf alle zu  $2N$  relativ primen und positiven Zahlen  $m$  bezieht. Die kleinste dieser Zahlen  $m$ , welche von 1 verschieden ist, besitzt mindestens den Werth  $G + 1$ . Die vorstehende Summe liegt daher zwischen den beiden Grössen:

$$1 \pm \left( \frac{1}{(G+1)^\nu} + \frac{1}{(G+2)^\nu} + \dots \right).$$

Da nun

$$\frac{1}{(G+k)^\nu} < \int_{G+k-1}^{G+k} \frac{dx}{x^\nu},$$

so folgt um so mehr:

$$1 - \int_G^\infty \frac{dx}{x^\nu} < D_\nu(N) < 1 + \int_G^\infty \frac{dx}{x^\nu}.$$

In derselben Weise ergeben sich die Ungleichungen für die Grösse  $(2N)_\nu \cdot S_\nu$ , welche den Werth der über alle Zahlen  $m$  erstreckten Summe  $\sum \frac{1}{m^\nu}$  ausdrückt.

Was endlich das Product  $\Pi_\nu$  anlangt, so kommt zunächst

$$\Pi_\nu \leq \Pi(1 + p^{-\nu}) < 1 + [(G + 1)^{-\nu} + (G + 2)^{-\nu} + \dots] < 1 + \gamma,$$

und dann

$$\Pi_\nu \geq \Pi(1 - p^{-\nu}) > \frac{1}{1 + [(G + 1)^{-\nu} + (G + 2)^{-\nu} + \dots]} > \frac{1}{1 + \gamma} > 1 - \gamma.$$

Auf Grund der vorstehenden Ungleichungen können wir jetzt in allen Fällen, wo  $n > 4$  ist, die Beziehung  $M_0 = 1$  nachweisen.

Wir wählen einfach die Zahl  $R$  derart, dass in  $\Delta R$  sämtliche ungeraden Primzahlen auftreten, die kleiner als eine Zahl  $G + 1$  sind. Unsere Ungleichungen liefern uns dann, wenn  $n$  ungerade und  $> 3$  ist, für alle Grössen:

$$D_{\frac{n-1}{2}} \left[ (-1)^{\frac{n-1}{2}} \sigma_1 m \Delta R^2 \right], \quad (8\Delta R)_n \cdot S_n, \quad \frac{1}{(8\Delta R)_{n-1} \cdot S_{n-1}},$$

und wenn  $n$  gerade und  $> 4$  ist, für alle Grössen:

$$\Pi \left[ 1 + \left( \frac{(-1)^{\frac{n}{2}} \Delta R^2}{p} \right)^{\frac{1}{p^{\frac{n-2}{2}}}} \right], \quad (8\Delta R)_n \cdot S_n, \quad \frac{1}{D_{\frac{n}{2}} \left[ (-1)^{\frac{n}{2}} \Delta R^2 \right]}$$

einmal obere und dann untere Grenzen. Indem wir erst diese oberen und dann diese unteren Grenzen einsetzen, und jedesmal die hervorgehende Ungleichung durch die Gleichung (4) dividiren, bekommen wir, wenn  $n \equiv 1 \pmod{2}$  und  $> 3$ :

$$\frac{1 - \gamma_{\frac{n-3}{2}}}{1 + \gamma_{\frac{n-2}{2}}} < M_0 < (1 + \gamma_{\frac{n-3}{2}})(1 + \gamma_{n-1}),$$

und wenn  $n \equiv 0 \pmod{2}$  und  $> 4$ :

$$\frac{1 - \gamma_{\frac{n-4}{2}}}{1 + \gamma_{\frac{n-2}{2}}} < M_0 < \frac{(1 + \gamma_{\frac{n-4}{2}})(1 + \gamma_{n-1})}{1 - \gamma_{\frac{n-2}{2}}},$$

wobei  $\gamma_h$  für  $\frac{1}{hG^h}$  gesetzt ist. Lassen wir jetzt die Zahl  $G$  in's Unendliche wachsen, so folgt in der That:  $M_0 = 1$ .

Es bleibt uns noch übrig, die Fälle  $n = 2, 3, 4$  zu untersuchen.

Ist  $n = 2$ , so nehme man  $R = 1$ , und betrachte zu gleicher Zeit alle die Grenzwerte  $L(m)$ , welche die rechte Seite der Gleichung (1) darstellt, wenn man den  $2 + \delta$  Einheiten  $C(m)$  alle die Werthsysteme beilegt, die der Bedingung  $\binom{-\Delta}{m} = 1$  genügen. Man bilde aus diesen  $2^{1+\delta}$  Grenzwerten ebensoviele lineare Combinationen:  $\sum c(m) \cdot L(m) = L_c$ ;  $c(m)$  bedeute hier ein beliebiges Glied des über alle Einheiten  $C(m)$  erstreckten Productes  $\prod[1 + C(m)]$ ; von je zwei Einheiten  $c(m)$ , die ein Product gleich  $\binom{-\Delta}{m}$  geben, soll aber immer nur eine beibehalten werden. Aus den Summen  $L_c$  folgen umgekehrt die Grössen  $L(m)$  mit Hilfe der Gleichungen  $2^{1+\delta} \cdot L(m) = \sum c(m) \cdot L_c$ . Die Grenzwerte  $L_c$  sind von DIRICHLET angegeben. Unter ihnen ist nur einer von Null verschieden, nämlich derjenige, welcher zu  $c = 1 = \binom{-\Delta}{m}$  gehört; dieser besitzt einen Ausdruck, aus welchem sofort  $M_0 = 1$  hervorgeht.

In den Fällen  $n = 3$  und  $n = 4$  gebe ich für die Relation  $M_0 = 1$  einen Beweis, welcher sich auf die Sätze aus der Anmerkung zu 9. stützt. Uebrigens liesse sich für diese Fälle noch dieselbe Methode verwerthen, welche in den Fällen  $n > 4$  angewandt wurde. Für  $n = 3$  sehe man auch: SMITH, *On the Orders and Genera of Ternary Quadratic Forms*, artt. 13—21 (Phil. Trans. CLVII, 1867) und: *F. Q.*, pp. 156—159; für  $n = 4$ : *F. Q.*, pp. 162—163, und: SMITH, *Sur la représentation des nombres par une somme de cinq carrés* (Mém. prés. T. XXIX).

Ist  $n = 3$ , so constatire man zunächst, dass dem speciellen Genus  $G$  von der Ordnung:

$$\begin{pmatrix} 1, & 1 \\ 1, & 1 \end{pmatrix}, \quad (J=1)$$

welches die Formen von der Determinante 1 enthält, ein  $M_0 = 1$ , d. i. ein  $M = \frac{1}{24}$  zukommt. Bekanntlich bilden alle Formen von  $G$  eine ein-

zige Classe, welche durch  $f = x_1^2 + x_2^2 + x_3^2$  repräsentirt wird,<sup>1</sup> und dieses  $f$  lässt in der That genau 24 Transformationen von der Determinante 1 in sich selbst zu. Die Anwendung der Gleichung (3) auf  $G$  liefert:

$$(R) \quad \frac{(2R)_1}{2^{2+r}} \cdot \frac{(2R)_2 \cdot S_2}{(2R)_3 \cdot S_3} = \text{Lim} \left\{ \rho \sum \frac{1}{m^{1+\rho}} D_1(-mR^2) \right\},$$

wo  $m$  alle positiven und zu  $2R$  relativ primen Zahlen mit festen Einheiten:

$$\left(-1\right)^{\frac{m-1}{2}}, \quad \left(\frac{2}{m}\right), \quad \left(\frac{m}{r_1}\right), \quad \left(\frac{m}{r_2}\right), \dots, \left(\frac{m}{r_r}\right)$$

zu durchlaufen hat. Dabei ist nach 9. Anm. die Einheit  $\left(-1\right)^{\frac{m-1}{2}}$  stets gleich  $+1$  zu nehmen; während die übrigen Einheiten ganz nach Belieben gewählt werden dürfen.

Die vorstehende Formel benutzen wir, um für ein beliebiges ternäres Genus  $G$  von einer Ordnung

$$\begin{pmatrix} \sigma_1 & \sigma_2 \\ \rho_1 & \rho_2 \end{pmatrix} \quad (J = \rho_1^2 \rho_2)$$

die Relation  $M_0 = 1$  abzuleiten. Nach (3) genügt die Grösse  $M_0$  eines solchen Genus jedenfalls einer Gleichung

$$(\Delta) \quad \frac{(2\Delta)_1}{2^{2+b}} \cdot \frac{(2\Delta)_2 \cdot S_2}{(2\Delta)_3 \cdot S_3} \cdot M_0 = \text{Lim} \left\{ \rho \sum \frac{1}{m^{1+\rho}} D_1(-\sigma_1 \Delta m) \right\} = \{m\},$$

wo  $m$  alle positiven und zu  $2\Delta$  relativ primen Zahlen mit bestimmten festen Einheiten

$$C(m) \quad \left(-1\right)^{\frac{m-1}{2}}, \quad \left(\frac{2}{m}\right), \quad \left(\frac{m}{\delta_1}\right), \quad \left(\frac{m}{\delta_2}\right), \dots, \left(\frac{m}{\delta_b}\right)$$

durchläuft.

Wir betrachten zuerst den Fall, wo  $\sigma_1 \rho_2$  und  $\sigma_2 \rho_1$  beide vollständige Quadrate sind.

Das Genus  $G$  werde durch eine charakteristische Form  $f$  repräsentirt. Der erste Coefficient von  $f$  heisse  $\sigma_1 \varphi_1$ , und es sei  $\sigma_2 \varphi_2$  der erste

<sup>1</sup> Vgl. z. B. DIRICHLET in CRELLE'S JOURNAL, Bd. 40, S. 228.

Coefficient der zu  $f$  adjungirten Form. Die Zahlen  $\varphi_1$  und  $\varphi_2$  sind dann prim zu einander, und es gelten zwei Congruenzen

$$-o_1\sigma_2\varphi_2 \equiv X_1^2 \pmod{\sigma_1^2\varphi_1}$$

$$-o_2\sigma_1\varphi_1 \equiv X_2^2 \pmod{\sigma_2^2\varphi_2}.$$

Dieselben geben

$$-\left(\frac{-\varphi_2}{\varphi_1}\right) \cdot \left(\frac{-\varphi_1}{\varphi_2}\right) = (-1)^{\frac{\varphi_1+1}{2} \cdot \frac{\varphi_2+1}{2}} = -1,$$

also

$$\varphi_1 \equiv 1, \quad \varphi_2 \equiv 1 \pmod{4},$$

was nur mit  $\sigma_1 = 1$ ,  $\sigma_2 = 1$  verträglich ist. Denn hätte man etwa  $\sigma_2 = 2$ , so würde die zweite Congruenz zugleich  $-\varphi_1 \equiv 1 \pmod{4}$  liefern. Nach 7. besitzt nun unser Genus den Hauptrest  $\varphi_1\xi_1^2 + \frac{o_1\varphi_2}{\varphi_1}\xi_2^2 + \frac{o_1o_2}{\varphi_2}\xi_3^2 \pmod{4}$ .

Derselbe zeigt, dass in  $(\Delta)$  die Einheit  $(-1)^{\frac{m-1}{2}}$  allein gleich  $+1$  genommen werden darf. Setzt man  $\sigma_1\Delta = 2^{2h}R^2 (R \equiv 1, \pmod{2})$ , so kann daher der Grenzwert  $\{m\}$  nach der Formel (R) bestimmt werden, und man findet  $M_0 = 1$ .

Zweitens sei eine der Zahlen  $\sigma_1o_2$  und  $\sigma_2o_1$  kein vollständiges Quadrat.

Das Maass des Genus  $G$  stimmt, wie wir wissen, mit dem Maasse des adjungirten Genus von der Ordnung

$$\begin{pmatrix} \sigma_2, \sigma_1 \\ o_2, o_1 \end{pmatrix}$$

überein; ebenso liefern diese beiden Genera gleiche Grössen  $f\{g\}$ ; sie müssen also auch dasselbe  $M_0$  ergeben. Wir brauchen daher nur eines dieser Genera zu untersuchen, und können annehmen, es sei  $\sigma_1o_2$ , also auch  $\sigma_1\Delta$  kein vollständiges Quadrat.

Aus  $\sigma_1\Delta$  gehe durch Division mit einer möglichst hohen Potenz von 4 die Zahl  $d$  hervor. Wir betrachten irgend ein Genus  $\varphi_1$  der Ordnung

$$\begin{pmatrix} 1, 1 \\ 1, d \end{pmatrix};$$

denken uns aber im Falle  $d \equiv 1 \pmod{4}$ , (was dann sicher gestattet ist), die Characteren  $\left(\frac{\varphi_2}{d}\right)$  dieses Genus so ausgesucht, dass die Einheit



$\delta = (-1)^{\frac{d+1}{2}} \cdot \left(\frac{\varphi_2}{d}\right) = (-1)^{\frac{\varphi_1 d + 1}{2} \cdot \frac{\varphi_2 + 1}{2}}$  gleich  $+1$  wird. Die zu  $\varphi_1$  gehörige Grösse  $M_0$  lässt sich ebenfalls durch einen der Grenzwerte  $\{m\}$  darstellen; und zwar ist hier, nach den Sätzen aus 9. Anm., ein jeder der  $2^{2+b}$  Grenzwerte  $\{m\}$  in gleicher Weise verwendbar. Alle die Grenzwerte  $\{m\}$  müssen demnach untereinander gleich sein.

Bilden wir jetzt die Formel ( $\Delta$ ) für das zu  $\varphi_1$  adjungirte Genus  $\varphi_2$  der Ordnung

$$\begin{pmatrix} 1, & 1 \\ d, & 1 \end{pmatrix},$$

so ergeben sich die Grenzwerte  $\{m\}$  gleich gewissen Grenzwerten

$$\text{Lim} \left\{ \rho \sum \frac{1}{m^{1+\rho}} D_1(-d^2 m) \right\},$$

wo  $m$  wie vorher Reihen von positiven Zahlen mit festen Characteren  $C(m) = \pm 1$  zu durchlaufen hat. Hier ist für die Einheit  $(-1)^{\frac{m-1}{2}}$ , nach 9. Anm., stets der Werth  $+1$  zulässig. Wenn man  $d = R$ , resp.  $= 2R$  setzt, kann man also für den vorstehenden Grenzwert die Formel (R) benutzen, und man gelangt zu  $M_0 = 1$ .

Ist endlich  $n = 4$ , so haben wir einen Grenzwert

$$\text{Lim} \left[ \rho \sum \frac{1}{m^{1+\rho}} \prod_p \left\{ 1 + \left( \frac{-\Delta}{p} \right)^{\frac{1}{p}} \right\} \right] = \{m\}$$

zu ermitteln, wo  $m$  alle positiven und zu  $2\Delta$  relativ primen Zahlen mit festen Einheiten

$$C(m) \quad (-1)^{\frac{m-1}{2}}, \quad \left(\frac{2}{m}\right), \quad \left(\frac{m}{\delta_1}\right), \quad \left(\frac{m}{\delta_2}\right), \dots, \left(\frac{m}{\delta_b}\right)$$

durchläuft. Wir bilden aus  $\Delta$  durch Division mit einer möglichst hohen Potenz von 4 eine Zahl  $\Delta_0$ . Die Grösse  $M_0$  für irgend ein Genus der Ordnung

$$\begin{pmatrix} 1, & 1, & 1 \\ 1, & 1, & \Delta_0 \end{pmatrix}$$

hängt dann gleichfalls von irgend einem Grenzwerte  $\{m\}$  ab. Für ein

solches Genus unterliegen aber, nach den Sätzen aus 9. Anm., die Einheiten  $C(m)$  durchaus keiner Beschränkung. Alle die  $2^{2+b}$  Grenzwerte  $\{m\}$  müssen also untereinander gleich sein, und wir können sie gleich dem  $2^{2+b}$ ten Theile ihrer Summe setzen. Diese Summe wird durch einen ähnlichen Grenzwert gebildet, wo  $m$  alle möglichen positiven und zu  $2\Delta$  relativ primen Zahlen durchläuft. Dieser letzte Grenzwert gestattet nach *F. Q.*, p. 150 und 162 eine Transformation in:

$$\text{Lim} \left( \rho \sum \frac{1}{m^{1+\rho}} \cdot \frac{\sum \left(\frac{\Delta}{m}\right) m^{-2-\rho}}{\sum m^{-4-2\rho}} \right) = (2\Delta)_1 \cdot \frac{D_2(\Delta)}{(2\Delta)_4 \cdot S_4},$$

welche dann unmittelbar zu  $M_0 = 1$  führt.

Von den verschiedenen Darstellungen, deren das Maass eines Genus fähig ist, erscheint als die natürlichste die hier gegebene mit Hilfe eines unendlichen Productes, in welchem einer jeden Primzahl ein bestimmter Factor entspricht.<sup>1</sup> Ihre Bedeutung reicht über das specielle Gebiet der quadratischen Formen hinaus: es zeigt diese Darstellung, dass zur Lösung arithmetischer Probleme über Formenanzahlen ein Studium jener wichtigen Gruppenbildungen erforderlich ist, auf welche Herr CAMILLE JORDAN in N<sup>o</sup> 302 des *Traité des Substitutions* aufmerksam gemacht hat.

Ausdrücke für das Maass eines positiven Genus quadratischer Formen von  $n$  Variablen sind zuerst von HENRY J. STEPHEN SMITH in der Note *On the Orders and Genera of Quadratic Forms containing more than three Indeterminates*, (*Roy. Soc. Proc.* XVI, 1868, pp. 197—208), mitgetheilt. Die Formeln von SMITH sind ähnlich unseren Formeln (2) in 8., erschöpfen aber nicht alle Fälle; sie geben im Wesentlichen die Werthe der von uns  $E_q$  genannten Factoren für ungerade Primzahlen  $q$ , doch für die Primzahl 2 nur in den weniger verwickelten Fällen, wo das Genus eine ungerade Determinante besitzt.

In einem folgenden Aufsätze beabsichtige ich verschiedene Anwendungen der hier gefundenen Resultate auseinanderzusetzen.

<sup>1</sup> Ich habe auf diese Darstellung im 99. Bande des Journals für die reine und angewandte Mathematik hingewiesen.