Ueber die Discriminante der Modulargleichungen der elliptischen Functionen.

Von M. KRAUSE in Heidelberg.

Das allgemeine Problem der Transformationstheorie der elliptischen Functionen besteht bekanntlich darin, wenn die Differentialgleichungen:

$$dw = \frac{dx}{V(1-x^2)(1-c^2x^2)},$$

$$dw = \frac{ady}{V(1-y^2)(1-k^2y^2)}$$

gegeben sind, den Multiplicator a und den transformirten Integralmodul k so zu bestimmen, dass die aus der zweiten Gleichung herzuleitenden elliptischen Functionen sich rational durch die der ersten ausdrücken. Dann muss, wenn wir den Modul der zugehörigen Thetafunctionen mit τ , respective τ' bezeichnen,

$$(1) \quad \tau' = \frac{\beta_0 - \alpha_0 \tau}{\alpha_1 \tau - \beta_1}$$

sein, wobei:

$$\alpha_0 \beta_1 - \alpha_1 \beta_0 = n$$

eine positive ganze Zahl, der Grad der Transformation ist. Solcher Zahlensysteme $\alpha_0 \alpha_1 \beta_0 \beta_1$, welche obenstehender Gleichung genügen, giebt es unendlich viele, doch lassen dieselben sich immer in eine endliche Anzahl von Classen eintheilen. Eine jede solcher Classen enthält zwar wieder eine unendlich grosse Anzahl von Transformationszahlen, doch nur solche, die durch lineare Transformation in einander übergehen.

Nehmen wir an, dass n eine unpaare Zahl ohne quadratischen Theiler ist — eine Annahme, die im Folgenden beibehalten werden soll, — d. h. setzen:

$$n = a_0 \cdot \cdot \cdot a_p,$$

so ist die Zahl der Classen:

$$(a_0 + 1)(a_1 + 1) \cdot \cdot \cdot (a_p + 1),$$

überdies können als Repräsentanten einer jeden derselben Zahlen der Form gewählt werden:

$$\delta, 0, 16\xi, \delta_1,$$

wobei $\xi = 0, 1 \dots \delta_1 - 1$, $\delta \delta_1 = n$ und δ einen jeden Theiler von n bedeutet.

Ferner ist bekannt, dass, wenn wir eine Grösse q definiren, durch:

$$q = e^{\pi \tau i}$$

die vierte Wurzel aus dem Integralmodul c als eindeutige Function von τ durch den Ausdruck gegeben ist:

$$(2) \quad \sqrt[4]{c} = u = \sqrt[4]{2} \cdot \sqrt[4]{q} \frac{(1+q^2)(1+q^4)\dots}{(1+q)(1+q^3)\dots} = \varphi(\tau).$$

Alsdann ergibt sich für die vierte Wurzel desjenigen transformirten Integralmoduls, welcher den Transformationszahlen

$$\delta, 0, 16\xi, \delta_1,$$

entspricht, vorausgesetzt, dass ihr Vorzeichen auf eine gewisse eindeutige Weise bestimmt ist,

$$(3) \quad \sqrt[4]{k} = v = \left(\frac{2}{\delta}\right) \varphi\left(\frac{\delta\tau - 16\xi}{\delta_1}\right).$$

Lassen wir hierin $\delta, \delta_1, 16\xi$ alle den obigen Bedingungen genügenden Werthe annehmen, so werden die entsprechenden v Grössen Lösungen einer algebraischen Gleichung, der Modulargleichung, die in Bezug auf v vom

$$(a_0 + 1) \dots (a_p + 1)^{t_0}$$

Grade ist und deren Coefficienten ganze Functionen von u sind.

Die Discriminante derselben hat die Form:

$$D = u^N (u^8 - 1)^{N'} (a_0 + a_1 u^8 + \dots a_p u^{8p}),$$

wenn:

$$N = nS'(n) - S(n) + 2\Delta(n),$$

$$N' = nS'(n) - S(n) + 2\Delta'(n),$$

$$4v = S(n)^2 - S(n) - N - 4N'$$

ist.

Dabei haben die auf den rechten Seiten vorkommenden Grössen folgende Bedeutung. Es ist $S(n)$ gleich der Summe der Divisoren der Zahl n , $S'(n)$ gleich der Anzahl dieser Divisoren, ferner

$$\Delta(n) = \sum tt',$$

wenn t und t' alle die Divisoren von n bedeuten, für welche

$$tt' < n,$$

endlich

$$\Delta'(n) = \sum t_1 t_1',$$

wenn $t_1 t_1'$ dieselbe Bedingung wie tt' erfüllen und überdies noch:

$$\left(\frac{2}{t_1}\right)\left(\frac{2}{t_1'}\right) = 1 *).$$

*) Siehe in Bezug auf die hier angeführten-Sätze das Werk meines hochverehrten Lehrers, Herrn Prof. Koenigsberger, „Vorlesungen über die Theorie der elliptischen Functionen“, Leipzig 1874.

Die Discriminante gleich Null gesetzt, giebt diejenigen u Werthe, für welche zwei der v Werthe einander gleich werden. Wir bezeichnen letztere mit:

$$v_1 = \left(\frac{2}{\delta}\right) \varphi\left(\frac{\delta\tau - 16\xi_1}{\delta_1}\right),$$

$$v_2 = \left(\frac{2}{u}\right) \varphi\left(\frac{u\tau - 16\xi_2}{u_1}\right).$$

Nun gilt allgemein der Satz, dessen Beweis unmittelbar klar ist, dass die nothwendige und hinreichende Bedingung, damit zwei φ Functionen von verschiedenen Argumenten:

$$\varphi(\tau_1) \text{ und } \varphi(\tau_2),$$

abgesehen von achten Einheitswurzeln, einander gleich werden, ist:

$$(4) \quad \tau_1 = \frac{b_0 - a_0 \tau_2}{a_1 \tau_2 - b_1},$$

wobei die Zahlen $a_0 b_0 a_1 b_1$ zum ersten Fall der linearen Transformation gehören (siehe das oben citirte Werk II^{ter} Theil p. 112) und je nach der Wahl der achten Einheitswurzel verschiedene Bedingungen erfüllen. Wir werden diese Bedingungen später für den Fall zweier dieser achten Einheitswurzeln, nämlich ± 1 ausführlich aufstellen.

Setzen wir nun:

$$\tau_1 = \frac{\delta\tau - 16\xi_1}{\delta_1}; \quad \tau_2 = \frac{u\tau - 16\xi_2}{u_1},$$

so folgt: die nothwendige und hinreichende Bedingung, damit

$$\left(\frac{2}{\delta}\right) \varphi\left(\frac{\delta\tau - 16\xi_1}{\delta_1}\right) = \left(\frac{2}{u}\right) \varphi\left(\frac{u\tau - 16\xi_2}{u_1}\right)$$

werde, ist:

$$\frac{\delta\tau - 16\xi_1}{\delta_1} = \frac{b_0 - a_0 \frac{u\tau - 16\xi_2}{u_1}}{a_1 \frac{u\tau - 16\xi_2}{u_1} - b_1},$$

wobei also $a_0 b_0 a_1 b_1$ später noch aufzustellenden Bedingungen genügen müssen.

Wie wir sehen, erhalten wir auf diese Weise eine quadratische Gleichung in τ :

$$(5) \quad P\tau^2 + 2Q\tau + R = 0,$$

deren eine Lösung mindestens die Eigenschaft hat, dass für die ihr entsprechende $\varphi(\tau)$ Function zwei Wurzeln der Modulargleichung einander gleich werden.

Wir stellen uns nun die Aufgabe, die nothwendigen und hinreichenden Bedingungen zu finden, denen die P, Q, R genügen müssen, damit für die einer oder beiden Lösungen τ entsprechenden Functionen $\varphi(\tau)$ zwei Wurzeln der Modulargleichung, die zu einer rationalen

Transformation n^{ten} Grades gehört, einander gleich werden, vorausgesetzt, dass n eine unpaare Zahl ohne quadratischen Theiler ist.

Wir fanden:

$$\frac{\delta \tau - 16 \xi_1}{\delta_1} = \frac{b_0 - a_0 \left(\frac{u \tau - 16 \xi_2}{u_1} \right)}{a_1 \frac{u \tau - 16 \xi_2}{u_1} - b_1}.$$

Hieraus ergibt sich die Gleichung:

$$\alpha_1 \tau^2 + (\alpha_0 - \beta_1) \tau - \beta_0 = 0,$$

wenn:

$$\alpha_0 = u [a_0 \delta_1 - 16 \xi_1 a_1],$$

$$\alpha_1 = a_1 \delta u,$$

$$\beta_0 = b_0 \delta_1 u_1 + 16 \xi_2 a_0 \delta_1 - 16 \xi_1 b_1 u_1 - 16^2 \xi_1 \xi_2 a_1,$$

$$\beta_1 = \delta [b_1 u_1 + 16 \xi_2 a_1],$$

und daher

$$\alpha_0 \beta_1 - \alpha_1 \beta_0 = n$$

ist.

Die Determinante dieser Gleichung hat die Form:

$$\Delta = (a + n)(a - n),$$

wenn:

$$a = \frac{\alpha_0 + \beta_1}{2}$$

ist.

Nun muss wegen der Convergenz der ϑ Functionen der reelle Theil von $\frac{\tau}{i}$ positiv sein. Daraus folgt unmittelbar, dass Δ negativ sein muss, ferner dass nur diejenige der beiden τ Wurzeln gebraucht werden kann, für welche der Coefficient von i positiv ist.

Wir wollen zunächst das Verhalten von a in Bezug auf den Modul 16 untersuchen, oder, näher präcisirt, zusehen, welche Werthe r in:

$$a \equiv rn \pmod{16}$$

annehmen kann.

Dazu ist es nöthig, die schon vorhin angedeuteten Bedingungen aufzustellen, denen die Grössen $a_0 b_0 a_1 b_1$ genügen. Dieselben lauten:

$$\text{I. } \left(\frac{2}{\delta} \right) \left(\frac{2}{u} \right) = +1.$$

$$1) \ a_0 = 8A + 1; \ b_1 = 8B + 1; \ a_1 \equiv 0 \pmod{2}; \ b_0 \equiv 0 \pmod{16}; \\ A + B \equiv 0 \pmod{4};$$

$$2) \ a_0 = 8A + 7; \ b_1 = 8B + 7; \ a_1 \equiv 0 \pmod{2}; \ b_0 \equiv 0 \pmod{16}; \\ A + B \equiv 2 \pmod{4};$$

$$3) \ a_0 = 8A + 3; \ b_1 = 8B + 3; \ a_1 \equiv 0 \pmod{4}; \ b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 1 \pmod{4};$$

*) Hermite, Sur la théorie des équations modulaires etc. Paris 1859. p. 33.

$$4) a_0 = 8A + 3; \quad b_1 = 8B + 3; \quad a_1 \equiv 2 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 3 \pmod{4};$$

$$5) a_0 = 8A + 5; \quad b_1 = 8B + 5; \quad a_1 \equiv 0 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 1 \pmod{4};$$

$$6) a_0 = 8A + 5; \quad b_1 = 8B + 5; \quad a_1 \equiv 2 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 3 \pmod{4}.$$

$$\text{II. } \left(\frac{2}{\delta}\right) \left(\frac{2}{u}\right) = -1.$$

$$1) a_0 = 8A + 1; \quad b_1 = 8B + 1; \quad a_1 \equiv 0 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 0 \pmod{4};$$

$$2) a_0 = 8A + 1; \quad b_1 = 8B + 1; \quad a_1 \equiv 2 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 2 \pmod{4};$$

$$3) a_0 = 8A + 7; \quad b_1 = 8B + 7; \quad a_1 \equiv 0 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 2 \pmod{4};$$

$$4) a_0 = 8A + 7; \quad b_1 = 8B + 7; \quad a_1 \equiv 2 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}; \\ A + B \equiv 0 \pmod{4};$$

$$5) a_0 = 8A + 3; \quad b_1 = 8B + 3; \quad a_1 \equiv 0 \pmod{2}; \quad b_0 \equiv 0 \pmod{16}; \\ A + B \equiv 1 \pmod{4};$$

$$6) a_0 = 8A + 5; \quad b_1 = 8B + 5; \quad a_1 \equiv 0 \pmod{2}; \quad b_0 \equiv 0 \pmod{16}; \\ A + B \equiv 1 \pmod{4}.$$

Man findet diese Bedingungen unmittelbar, wenn man die an der citirten Stelle aufgestellten Relationen für die beiden achten Einheitswurzeln ± 1 näher untersucht.

Es ist nun:

$$2a = a_0 + \beta_1 = u[a_0\delta_1 - 16\xi_1 a_1] + \delta[b_1 u_1 + 16\xi_2 a_1],$$

d. h.

$$2a \equiv u a_0 \delta_1 + u_1 b_1 \delta \pmod{32}.$$

Es ist also die Congruenz zu untersuchen:

$$u a_0 \delta_1 + u_1 b_1 \delta \equiv 2rn \pmod{32};$$

a_0 und b_1 haben die Formen $8A + s$; $8B + s$, daraus folgt:

$$u a_0 \delta_1 + u_1 b_1 \delta \equiv 8[u\delta_1 A + u_1 \delta B] + s[u\delta_1 + u_1 \delta] \pmod{32}.$$

Wir untersuchen zunächst:

$$u\delta_1 + \delta u_1 \equiv 2rn \pmod{32}.$$

Es ergeben sich hierbei folgende Fälle:

$$\text{I. } \left(\frac{2}{\delta}\right)\left(\frac{2}{u}\right) = +1.$$

$$1) \ u = 8p_0 + k; \quad u_1 = 8p_1 + k_1; \quad \delta = 8p_2 + k; \quad \delta_1 = 8p_3 + k_1; \\ r = +1;$$

$$2) \ u = 8p_0 + k; \quad u_1 = 8p_1 + k_1; \quad \delta = 8p_2 - k; \quad \delta_1 = 8p_3 - k_1; \\ r = -1.$$

$$\text{II. } \left(\frac{2}{\delta}\right)\left(\frac{2}{u}\right) = -1.$$

$$1) \ u = 8p_0 + k; \quad u_1 = 8p_1 + k_1; \quad \delta = 8p_2 + k_1; \quad \delta_1 = 8p_3 + k; \\ r = \pm 9, \text{ je nachdem } k \mp k_1 \equiv 0 \pmod{4};$$

$$2) \ u = 8p_0 + k; \quad u_1 = 8p_1 + k_1; \quad \delta = 8p_2 - k_1; \quad \delta_1 = 8p_3 - k; \\ r = \mp 9; \text{ je nachdem } k \mp k_1 \equiv 0 \pmod{4};$$

$$3) \ u = 8p_0 + k; \quad u_1 = 8p_1 + k; \quad \delta = 8p_2 + k_1; \quad \delta_1 = 8p_3 + k_1; \\ r = \pm 9, \text{ je nachdem } k \mp k_1 \equiv 0 \pmod{4};$$

$$4) \ u = 8p_0 + k; \quad u_1 = 8p_1 - k; \quad \delta = 8p_2 + k_1; \quad \delta_1 = 8p_3 - k_1; \\ r = \pm 9, \text{ je nachdem } k \mp k_1 \equiv 0 \pmod{4}.$$

Weitere Fälle sind nicht möglich. Die Richtigkeit der Behauptungen folgt aus einer näher eingehenden Rechnung. Wir zeigen die Art derselben an dem Falle II, 2. Für diesen ist die Congruenz aufzulösen

$$(8p_0 + k)(8p_3 - k) + (8p_1 + k_1)(8p_2 - k_1) \equiv ruu_1 + r\delta\delta_1 \pmod{32},$$

oder

$$8[(p_3 - p_0) - r(p_1 - p_2)](k - k_1) - (k + k_1)^2 - 2(r - 1)kk_1 \equiv 0 \pmod{32}.$$

Sei nun:

$$k - k_1 \equiv 0 \pmod{4},$$

mithin

$$k + k_1 \equiv 2 \pmod{4},$$

so folgt daraus unmittelbar als einzige Lösung:

$$r = -9$$

Wir können die soeben gefundenen Resultate übersichtlicher darstellen:

Sei $u = 8p_0 + k$; $\delta = 8p_2 + k_1$; so ist, wenn:

$$(7) \quad \left\{ \begin{array}{l} \text{I. } \left(\frac{2}{\delta}\right)\left(\frac{2}{u}\right) = +1, \\ r = \mp 1, \text{ je nachdem } k \pm k_1 \equiv 0 \pmod{4}, \text{ wenn} \\ \text{II. } \left(\frac{2}{\delta}\right)\left(\frac{2}{u}\right) = -1, \\ r = \mp 9, \text{ je nachdem } k \pm k_1 \equiv 0 \pmod{4}. \end{array} \right.$$

Untersuchen wir jetzt die Congruenz:

$$2a \equiv 2rn \pmod{32},$$

so ergibt sich vermöge Rechnungen genau derselben Art für die in Formel (6) aufgestellten zwölf Fälle respective:

$$(8) \quad \left\{ \begin{array}{l} \text{I.} \\ 1) a \equiv \overline{+} n \pmod{16}; \quad 2) a \equiv \underline{+} n \pmod{16}; \\ 3) a \equiv \underline{+} 9n \pmod{16}; \quad 4) a \equiv \underline{+} n \pmod{16}; \\ 5) a \equiv \overline{+} 9n \pmod{16}; \quad 6) a \equiv \overline{+} n \pmod{16}. \\ \\ \text{II.} \\ 1) a \equiv \overline{+} 9n \pmod{16}; \quad 2) a \equiv \overline{+} n \pmod{16}; \\ 3) a \equiv \underline{+} 9n \pmod{16}; \quad 4) a \equiv \underline{+} n \pmod{16}; \\ 5) a \equiv \underline{+} n \pmod{16}; \quad 6) a \equiv \overline{+} n \pmod{16}. \end{array} \right.$$

Dabei ist in allen zwölf Fällen das obere oder das untere Zeichen zu nehmen, je nachdem

$$k \pm k_1 \equiv 0 \pmod{4}.$$

Wie wir sehen, zeigt sich das merkwürdige Resultat, dass a nur:

$$a \equiv \underline{+} n \pmod{8}$$

sein kann.

Je nachdem nun:

$$a \equiv \underline{+} 9n \pmod{16}$$

oder

$$a \equiv \underline{+} n \pmod{16}$$

ist, nimmt die Determinante eine der beiden Formen an:

$$(9) \quad \left\{ \begin{array}{l} \Delta = 16(3n - 8\delta)(n - 2\delta), \\ \Delta' = -32\delta(n - 8\delta). \end{array} \right.$$

Also finden wir: Damit eine Lösung von

$$P\tau^2 + 2Q\tau + R = 0$$

unseren früher aufgestellten Bedingungen genüge, ist eine nothwendige Bedingung, dass die Determinante der Gleichung sich in eine der beiden Formen bringen lässt:

$$Q^2 - PR = \Delta = 16(3n - 8\delta)(n - 2\delta)$$

oder

$$Q^2 - PR = \Delta' = -32\delta(n - 8\delta)$$

und negativ ist.

Es fragt sich jetzt, welchen weiteren Bedingungen die Coefficienten genügen müssen.

Es ergab sich für τ die Gleichung:

$$\alpha_1 \tau^2 + (\alpha_0 - \beta_1) \tau - \beta_0 = 0$$

oder

$$Pr^2 + 2Qr + R = 0,$$

wenn:

$$\begin{aligned} P &= a_1 \delta u, \\ 2Q &= u [a_0 \delta_1 - 16 \xi_1 a_1] - \delta [b_1 u_1 + 16 \xi_2 a_1], \\ R &= 16^2 \xi_1 \xi_2 a_1 + b_1 16 \xi_1 u_1 - 16 \xi_2 a_0 \delta_1 - b_0 \delta_1 u_1. \end{aligned}$$

Sei zunächst

$$\Delta = 16(3n - 8\delta)(n - 2\delta),$$

so zeigt die in (6) aufgestellte Tabelle, dass in allen diesen Fällen

$$a_1 \equiv 0 \pmod{4}; \quad b_0 \equiv 8 \pmod{16}$$

ist, mithin auch:

$$P \equiv 0 \pmod{4}; \quad R \equiv 8 \pmod{16}.$$

Es bleibt übrig Q zu betrachten und zwar untersuchen wir es nach dem Modul 8. Es ist:

$$2Q \equiv u a_0 \delta_1 - u_1 b_1 \delta \pmod{16} \equiv u a_0 \frac{n}{\delta} - \frac{n}{u} b_1 \delta \pmod{16} \equiv \frac{n}{\delta u} [u^2 a_0 - \delta^2 b_1] \pmod{16}.$$

Die Rechnung zeigt nun, dass:

$$u^2 a_0 - \delta^2 b_1$$

in allen möglichen vorkommenden Fällen congruent ist:

$$u^2 a_0 - \delta^2 b_1 \equiv 8 \pmod{16}.$$

Wir zeigen die Art derselben an einem Beispiele und wählen dazu Formel (6) II, 1). Dafür wird:

$$u^2 a_0 - \delta^2 b_1 \equiv 8 [k^2 A - k_1^2 B] + k^2 - k_1^2 \equiv k^2 - k_1^2 \pmod{16}.$$

Nun ist aber in diesem Falle

$$\left(\frac{2}{\delta}\right) \left(\frac{2}{u}\right) = -1,$$

mithin

$$k^2 - k_1^2 \equiv 8 \pmod{16},$$

also auch

$$u^2 a_0 - \delta^2 b_1 \equiv 8 \pmod{16}$$

q. e. d.

Hieraus folgt unmittelbar, dass auch

$$2Q \equiv 8 \pmod{16}$$

oder

$$Q \equiv 4 \pmod{8}$$

sein muss.

Ähnliche Resultate ergeben sich für:

$$\Delta' = -32\delta(n - 8\delta).$$

Man hat hierfür zwei Fälle zu unterscheiden, wie aus den aufgestellten Tabellen unmittelbar ersichtlich ist:

- a) $P \equiv 2 \pmod{4}; \quad Q \equiv 4 \pmod{8}; \quad R \equiv 8 \pmod{16};$
- b) $P \equiv 0 \pmod{2}; \quad Q \equiv 0 \pmod{8}; \quad R \equiv 0 \pmod{16}.$

Fassen wir die letzten Resultate zusammen, so ergibt sich:

Die nothwendigen Bedingungen, damit zu einer Lösung τ von:

$$P\tau^2 + 2Q\tau + R = 0$$

eine Function $\varphi(\tau)$ gehöre, die Wurzel der oben aufgestellten Discriminante

$$D = 0$$

ist, sind:

$$(10) \left\{ \begin{array}{l} 1) \text{ Die Determinante der Gleichung muss sich in eine der beiden Formen;} \\ \quad \Delta = 16(3n - 8\delta)(n - 2\delta) \\ \text{oder} \\ \quad \Delta' = -32\delta(n - 8\delta) \\ \text{bringen lassen und negativ sein.} \\ 2) \text{ Falls} \\ \quad \Delta = 16(3n - 8\delta)(n - 2\delta) \text{ ist,} \\ \text{muss sein:} \\ \quad P \equiv 0 \pmod{4}; \quad Q \equiv 4 \pmod{8}; \quad R \equiv 8 \pmod{16}. \\ \quad \text{Falls} \\ \quad \Delta' = -32\delta(n - 8\delta) \text{ ist,} \\ \text{muss sein:} \\ \quad P \equiv 2 \pmod{4}; \quad Q \equiv 4 \pmod{8}; \quad R \equiv 8 \pmod{16}, \\ \text{oder} \\ \quad P \equiv 0 \pmod{2}; \quad Q \equiv 0 \pmod{8}; \quad R \equiv 0 \pmod{16}. \end{array} \right.$$

Wir zeigen, dass diese aufgestellten Bedingungen auch die hinreichenden sind.

Dazu muss bewiesen werden, dass, falls sie gelten, $a_0 b_0 a_1 b_1 u u_1 \delta \delta_1 \xi_1 \xi_2$ so bestimmt werden können, dass sie allen Bedingungen Genüge leisten.

Wir fanden:

$$\begin{aligned} P &= a_1 \delta u, \\ 2Q &= u[a_0 \delta_1 - a_1 16 \xi_1] - \delta[b_1 u_1 + a_1 16 \xi_2], \\ R &= 16^2 \xi_1 \xi_2 a_1 + b_1 u_1 16 \xi_1 - a_0 \delta_1 16 \xi_2 - b_0 \delta_1 u_1, \\ &\quad a_0 b_1 - a_1 b_0 = 1. \end{aligned}$$

Setzen wir

$$Q^2 - PR = \Delta,$$

so ergeben sich hieraus für a_0 und b_1 die Gleichungen:

$$\begin{aligned} n^2 \delta^2 b_1^2 + 2n \delta b_1 [Qu + 16 \xi_2 P] &= u^2 \Delta + u^2 n^2 - (Qu + 16 \xi_2 P)^2, \\ n^2 u^2 a_0^2 - 2nu a_0 [Q\delta + 16 \xi_1 P] &= \delta^2 \Delta + \delta^2 n^2 - (Q\delta + 16 \xi_1 P)^2, \end{aligned}$$

mithin, da

$$n^2 + \Delta = a^2,$$

$$(11) \quad \begin{cases} n \delta b_1 = - (Qu + 16 \xi_2 P) \pm au, \\ nu a_0 = + (Q\delta + 16 \xi_1 P) \pm a\delta, \end{cases}$$

wobei zu bemerken ist, dass vermöge der ersten Bedingung a eine bis auf das Vorzeichen eindeutig bestimmte ganze Zahl ist.

Ferner ist a_1 bestimmt durch:

$$P = a_1 u \delta$$

und b_0 entweder aus

$$a_0 b_1 - a_1 b_0 = 1$$

oder

$$R = 16^2 \xi_1 \xi_2 a_1 + 16 \xi_1 b_1 u_1 - 16 \xi_2 a_0 \delta_1 - b_0 \delta_1 u_1.$$

Es handelt sich darum zunächst zu zeigen, dass $a_0 b_0 a_1 b_1$ sich als ganze Zahlen ausdrücken lassen.

Zu verfügen haben wir innerhalb gewisser Grenzen über $u \delta \xi_1 \xi_2$. Wir weisen nach, dass dieselben so gewählt werden können, dass $a_0 a_1 b_0 b_1$ zu ganzen Zahlen werden. In bestimmter, später ersichtlicher Weise geordnet sei:

$$n = a_1 \cdots a_f a_{f+1} \cdots a_g a_{g+1} \cdots a_h a_{h+1} \cdots a_k,$$

ferner:

$$P = a_1 \cdots a_f a_{f+1} \cdots a_g a_{g+1}^{r_{g+1}} \cdots a_h^{r_h} P',$$

wobei P' relativ prim zu n ist und

$$v_s \geq 2, \\ s = g+1, \dots, h.$$

Nun ist:

$$\Delta = Q^2 - PR = a^2 - n^2,$$

mithin:

$$(Q + a)(Q - a) = RP - n^2.$$

Hieraus folgt, dass sämtliche gemeinsamen Theiler von P und n in

$$(Q + a)(Q - a)$$

enthalten sind. Schliessen wir daher den Fall aus, dass P , Q , R einen gemeinsamen Theiler haben, der zugleich Theiler von n ist, so können wir setzen:

$$Q + a = a_1^{\lambda_1} \cdots a_f^{\lambda_f} a_{g+1}^{\lambda_{g+1}} \cdots a_h^{\lambda_h} Q',$$

$$Q - a = a_{f+1}^{\lambda'_{f+1}} \cdots a_g^{\lambda'_g} a_{g+1}^{\lambda'_{g+1}} \cdots a_h^{\lambda'_h} Q'',$$

wobei Q' und Q'' relativ prim zu P sind und überdies:

$$\lambda_s \geq 1; \quad \lambda_s + \lambda'_s \geq 2. \\ s = 1 \dots g \qquad s = g+1 \dots h$$

Alsdann setzen wir:

$$u = a_1 \cdots a_f a_{g+1}^{\mu_{g+1}} \cdots a_h^{\mu_h},$$

$$\delta = a_{f+1} \cdots a_g a_{g+1}^{\mu'_{g+1}} \cdots a_h^{\mu'_h}.$$

wenn $\mu_{g+1} \dots \mu_h$, respective $\mu'_{g+1} \dots \mu'_h$ die Werthe Eins oder Null haben, je nachdem das zugehörige λ respective λ' in $Q + a$ respective $Q - a$ von Null verschieden ist oder nicht.

Offenbar erfüllen dann u und δ die Bedingung, dass sie Theiler von n sind.

Wir zeigen, dass unter dieser Festsetzung aus;

$$n\delta b_1 = -(Qu + 16\xi_2 P) \pm au,$$

$$nu a_0 = (Q\delta + 16\xi_1 P) \pm a\delta$$

a_0 und b_1 sich als ganze Zahlen bestimmen lassen. Es wird dieses möglich sein, wenn zwei ganze Zahlen ξ_1, ξ_2 so gewählt werden können, dass sie kleiner als δ_1 resp. u_1 sind und den Congruenzen genügen:

$$16\xi_2 P_1 \delta + Q \mp a \equiv 0 \pmod{\delta u_1},$$

$$16\xi_1 P_1 u + Q \pm a \equiv 0 \pmod{\delta_1 u},$$

wenn

$$P = P_1 u \delta.$$

Es ist zunächst klar, dass nur die oberen Zeichen gewählt werden können, da n. A. $Q - a$ durch δ und $Q + a$ durch u theilbar ist. Es bleibt dieses auch dann richtig, wenn sowohl Q wie a durch $u\delta$ theilbar sind.

Also lauten die Congruenzen:

$$16\xi_2 P_1 \equiv \frac{-Q+a}{\delta} \pmod{u_1},$$

$$16\xi_1 P_1 \equiv \frac{-Q-a}{u} \pmod{\delta_1},$$

wobei

$$\frac{Q-a}{\delta} = a_{f+1}^{\lambda_{f+1}-1} \dots a_g^{\lambda_g-1} a_{g+1}^{\lambda'_{g+1}-\mu'_{g+1}} \dots a_h^{\lambda'_h-\mu'_h} Q'',$$

$$\frac{Q+a}{u} = a_1^{\lambda_1-1} \dots a_f^{\lambda_f-1} a_{g+1}^{\lambda_{g+1}-\mu_{g+1}} \dots a_h^{\lambda_h-\mu_h} Q'.$$

Die Congruenz

$$16\xi_2 P_1 \equiv \frac{-Q+a}{\delta} \pmod{u_1}$$

wird lösbar sein, wenn alle Theiler von P_1 und u_1 zu gleicher Zeit Theiler von $\frac{-Q+a}{\delta}$ sind. Nun sind diese sämmtlich enthalten unter den Grössen

$$a_{g+1}, \dots, a_h$$

und deren Combinationen.

Eine beliebige dieser Grössen wird Theiler von u_1 sein, falls das zugehörige λ in $Q + a$ gleich Null ist. Dann ist aber das entsprechende λ' in $Q - a$ grösser oder gleich 2, d. h. $\frac{Q-a}{\delta}$ ist auch durch dieselbe Grösse theilbar. Damit ist das Verlangte bewiesen.

Was von der Congruenz:

$$16 \xi_2 P_1 \equiv \frac{-Q+a}{\delta} \pmod{u_1}$$

gilt, gilt auch von

$$16 \xi_1 P_1 \equiv \frac{-Q-a}{u} \pmod{\delta_1}.$$

Sei nun der grösste gemeinsame Theiler von P_1 und $u_1: q$, von P_1 und $\delta_1: p$, so werden wir q Lösungen ξ_2 resp. p Lösungen ξ_1 erhalten, welche nach dem Modul u_1 respective δ_1 incongruent sind. Einer jeden derselben werden ganzzahlige a_0, b_1 entsprechen. Es fragt sich, ob alle oder, wenn nicht alle, welche von den Lösungen $\xi_1 \xi_2$ zu gebrauchen sind.

Untersuchen wir dazu, welches die Bedingungen sind, unter denen sich b_0 als ganze Zahl bestimmen lässt. Wir fanden für b_0 die Gleichungen:

$$b_0 = - \frac{R - 16 [b_1 \xi_1 u_1 - a_0 \xi_2 \delta_1] - 16^2 \xi_1 \xi_2 P_1}{\delta_1 u_1}$$

und

$$b_0 = - \left(\frac{1 - a_0 b_1}{P_1} \right).$$

Aus diesen beiden Gleichungen folgt, dass b_0 , falls es keine ganze Zahl ist, als Nenner höchstens die Grösse pq haben kann. Es fragt sich, ob nicht in jedem Falle $\xi_1 \xi_2$ so gewählt werden können, dass der Nenner fortfällt, d. h. dass:

$$(12) \quad R - 16 [b_1 \xi_1 u_1 - a_0 \xi_2 \delta_1] - 16^2 \xi_1 \xi_2 P_1 \equiv 0 \pmod{pq}$$

wird.

Wir schicken die Bemerkung voraus, dass P_1, u_1, δ_1 keinen gemeinsamen Theiler haben können.

In der That, wir haben gesetzt:

$$P = u \delta P_1,$$

wo P_1 , wenn anders es überhaupt Factoren von n enthält, nur solche enthält, die schon in u und δ enthalten sind.

Nun sei:

$$\delta = b_0 \cdots b_p c_0 \cdots c_r,$$

$$u = b_0 \cdots b_p d_0 \cdots d_s,$$

dann ist

$$\delta_1 = d_0 \cdots d_s \delta_1',$$

wo δ_1' relativ prim zu P_1 ist, ferner

$$u_1 = c_0 \cdots c_r u_1',$$

wo u_1' wiederum relativ prim zu P_1 ist. Hieraus folgt die Richtigkeit der Behauptung unmittelbar, da $c_0 \cdots c_r$ verschieden sind von $d_0 \cdots d_s$.

Vermöge dieses Satzes können wir die Congruenz schreiben:

$$R - 16 [b_1 \xi_1 u_1 - a_0 \xi_2 \delta_1] \equiv 0 \bmod pq,$$

oder, indem wir die Werthe von a_0 und b_1 einsetzen:

$$R - 16 \left[\left(\frac{-Q+a}{\delta} - 16 \xi_2 P_1 \right) \xi_1 - \left(\frac{Q+a}{u} + 16 \xi_1 P_1 \right) \xi_2 \right] \equiv 0 \bmod pq,$$

oder

$$16 \frac{-Q+a}{\delta} \xi_1 \equiv R - 16 \frac{Q+a}{u} \xi_2 \bmod pq,$$

Nun hat, wie bewiesen, $\frac{-Q+a}{\delta}$ den Theiler q , damit diese Congruenz möglich sei, muss also sein:

$$R - 16 \frac{Q+a}{u} \xi_2 \equiv 0 \bmod q.$$

Für ξ_2 haben sich q Lösungen der Form ergeben:

$$\xi_2' + \frac{k u_1}{q} \quad k = 0 \dots q-1,$$

wobei

$$\xi_2' < \frac{u_1}{q}$$

ist, mithin erhalten wir für k die Congruenz:

$$(13) \quad 16 \frac{Q+a}{u} \frac{k u_1}{q} \equiv R - 16 \frac{Q+a}{u} \xi_2' \bmod q.$$

Diese Congruenz hat aber stets eine und nur eine Lösung, die kleiner als q ist, da, wie aus dem Vorhergehenden unmittelbar folgt, $\frac{Q+a}{u}$ sowohl wie $\frac{u_1}{q}$ keinen gemeinsamen Theiler mit q hat.

Also giebt es nur einen Werth von ξ_2 , der kleiner als u_1 ist und der Congruenz genügt:

$$R - 16 \frac{Q+a}{u} \xi_2 \equiv 16 \frac{-Q+a}{\delta} \xi_1 \bmod pq,$$

und ebenso wird es nur einen hierzu gehörigen Werth ξ_1 geben, der kleiner als δ_1 ist.

Wählt man diese Werthe für ξ_1 und ξ_2 , so ergiebt sich b_0 als ganze Zahl und zwar nur dann.

Da nun vermöge der Wahl von u und δ a_1 auch eine ganze Zahl wird, so ergiebt sich zunächst, dass, falls die Coefficienten P, Q, R in

$$P\tau^2 + 2Q\tau + R = 0$$

der ersten der aufgestellten Bedingungen genügen — denn nur diese haben wir bisher benutzt — stets u, δ, ξ_1, ξ_2 so gewählt werden können, dass $a_0 b_0 a_1 b_1$ sich als ganze Zahlen ergeben.

Die Wahl von u und δ ist keine willkürliche. Eine Untersuchung ähnlicher Art, wie die vorhin angestellte, zeigt, dass sie eine eindeutig bestimmte ist.

Es bleibt übrig zu zeigen, dass vermöge der zweiten Bedingung, denen die P, Q, R genügen, auch die Form von $a_0 b_0 a_1 b_1$ die ver-

langte ist. Eine näher eingehende Betrachtung zeigt die Richtigkeit dieser Behauptung. Wir wollen sie nur für einen Fall wirklich durchführen, da sie für alle übrigen Fälle ganz ähnlich ist.

Sei

$$\Delta = 16 (3n - 8\delta) (n - 2\delta) = a^2 - n^2,$$

ferner

$$a \equiv -9n \pmod{16},$$

mithin

$$P \equiv 0 \pmod{4}; \quad Q \equiv 4 \pmod{8}; \quad R \equiv 8 \pmod{16}.$$

Wir fanden:

$$u_1 \delta b_1 = - (Q + 16 \xi_2 \delta P_1) + a,$$

$$\delta_1 u a_0 = (Q + 16 \xi_1 u P_1) + a,$$

also in unserem Falle:

$$u_1 \delta b_1 \equiv 7n - Q \pmod{16},$$

$$\delta_1 u a_0 \equiv 7n + Q \pmod{16}.$$

Sei nun:

$$\left(\frac{2}{\delta}\right) \left(\frac{2}{u}\right) = +1,$$

ferner:

$$u = 8p_0 + k; \quad u_1 = 8p_1 + k_1; \quad \delta = 8p_2 + k; \quad \delta_1 = 8p_3 + k_1,$$

so folgt, wenn wir

$$b_1 = 8B + l$$

setzen:

$$8[p_1 k l + k p_2 l + k_1 k B] + l k k_1 \equiv 56[p_0 k_1 + p_1 k] + 7 k k_1 - Q \pmod{16}.$$

Vermöge der Bedingung, welcher Q unterworfen ist, ist diese Congruenz nur möglich, wenn:

$$l - 7 \equiv 4 \pmod{8}, \text{ d. h. } l = 3$$

oder

$$b_1 = 8B + 3.$$

Ebenso würde sich ergeben:

$$a_0 = 8A + 3.$$

Addiren wir ferner die oberen Gleichungen, so wird:

$$u_1 \delta b_1 + u \delta_1 a_0 \equiv 2a \pmod{32} \equiv 14n \pmod{32}$$

oder

$$\delta^2 b_1 + a_0 u^2 \equiv 14 u \delta \pmod{32}.$$

Setzen wir hierin:

$$b_1 = 8B + 3; \quad a_0 = 8A + 3; \quad \delta = 8p_2 + k; \quad u = 8p_0 + k,$$

so ist diese Congruenz in die Form zu bringen:

$$4g - k(A + B - 1) \equiv 0 \pmod{4}, \text{ d. h. } A + B \equiv 1 \pmod{4}.$$

Ferner folgt aus:

$$P = a_1 \delta u$$

$$a_1 \equiv 0 \pmod{4},$$

aus:

$$b_0 = - \frac{R - 16 [b_1 \xi_1 u_1 - a_0 \xi_2 \delta_1] - 16 \xi_1 \xi_2 P_1}{\delta_1 u_1}$$

$$b_0 \equiv 8 \pmod{16}.$$

Vergleichen wir diese Resultate mit den in Formel (6) aufgestellten Bedingungen, so sehen wir, dass $a_0 b_0 a_1 b_1$ gerade diejenigen Formen haben, die sie nach jenen Formeln für

$a \equiv -9n \pmod{16}$; $\left(\frac{2}{\delta}\right)\left(\frac{2}{u}\right) = +1$; $k + k_1 \equiv 2 \pmod{4}$ haben müssen.

Also finden wir den *Lehrsatz*:

Die nothwendigen und hinreichenden Bedingungen, damit zu einer Wurzel von:

$$P\tau^2 + 2Q\tau + R = 0$$

eine Function $\varphi(\tau)$ gehöre, die Lösung der Discriminante

$$D = 0$$

ist, sind

1) Die Determinante der Gleichung muss sich in eine der beiden Formen:

$$\Delta = 16(3n - 8\delta)(n - 2\delta)$$

oder

$$\Delta' = -32\delta(n - 8\delta)$$

bringen lassen und negativ sein.

2) Falls $\Delta = 16(3n - 8\delta)(n - 2\delta)$ ist, muss sein:

$$P \equiv 0 \pmod{4}; \quad Q \equiv 4 \pmod{8}; \quad R \equiv 8 \pmod{16}.$$

Falls $\Delta' = -32\delta(n - 8\delta)$ ist, muss sein:

$$P \equiv 2 \pmod{4}; \quad Q \equiv 4 \pmod{8}; \quad R \equiv 8 \pmod{16}$$

oder

$$P \equiv 0 \pmod{2}; \quad Q \equiv 0 \pmod{8}; \quad R \equiv 0 \pmod{16}.$$

Zu gleicher Zeit sahen wir, dass stets zwei und nur zwei Wurzeln der zu dem Transformationsgrad n gehörigen Modulargleichung einander gleich werden, und fanden die Methode, dieselben zu bestimmen. Wir wollen letztere der Wichtigkeit der Sache wegen noch einmal angeben und zwar mit etwas veränderten Bezeichnungen.

Sei

$$Q^2 - RP = \Delta = a^2 - n^2,$$

$$n = a_0 \cdots a_m,$$

$$P = b_0^{\beta_0} \cdots b_e^{\beta_e} P',$$

wo die $b_0 \cdots b_e$ sämmtlich Theiler von n sind und P' relativ prim zu n ist, ferner

$$Q + a = c_0^{\xi_0} \cdots c_k^{\xi_k} Q',$$

$$Q - a = d_0^{\beta_0} \cdots d_i^{\beta_i} Q'',$$

wo die $c_0 \dots c_k$ $d_0 \dots d_i$ zu den $b_0 \dots b_e$ gehören und Q' und Q'' relativ prim zu P sind.

Dann setzen wir:

$$\begin{aligned} u &= c_0 \dots c_k, \\ \delta &= d_0 \dots d_i, \\ u_1 &= \frac{n}{u}; \quad \delta_1 = \frac{n}{\delta} \end{aligned}$$

und bestimmen die Lösungen ξ_1 und ξ_2 der Congruenzen

$$\begin{cases} 16 \xi_1 P_1 \equiv \frac{-Q-a}{u} \pmod{\delta_1}, \\ 16 \xi_2 P_1 \equiv \frac{-Q+a}{\delta} \pmod{u_1}, \end{cases}$$

wobei $P_1 u \delta = P$.

Es ergeben sich q Lösungen ξ_2 und p Lösungen ξ_1 , die nach dem Modul u_1 respective δ_1 incongruent sind, wenn q den grössten gemeinsamen Theiler von P_1 und u_1 , p den grössten gemeinsamen Theiler von P_1 und δ_1 bedeutet. Die Lösungen haben die Form:

$$\begin{aligned} \xi_2' + \frac{k u_1}{q}; \quad \xi_1' + \frac{k_1 \delta_1}{p}; \quad \xi_2' < \frac{u_1}{q}; \quad \xi_1' < \frac{\delta_1}{p}, \\ k = 0 \dots q-1, \quad k_1 = 0 \dots p-1. \end{aligned}$$

Die Grössen k und k_1 ferner sind eindeutig bestimmt aus:

$$\begin{aligned} R - 16 \frac{Q+a}{u} \xi_2' - 16 \frac{Q+a}{u} \frac{k u_1}{q} &\equiv 0 \pmod{q}, \\ R - 16 \frac{-Q+a}{\delta} \xi_1' - 16 \frac{-Q+a}{\delta} \frac{k_1 \delta_1}{p} &\equiv 0 \pmod{p}. \end{aligned}$$

Sind auf diese Weise u , u_1 , δ , δ_1 , ξ_1 , ξ_2 gefunden, so werden die beiden Wurzeln der Modulargleichung

$$\left(\frac{2}{\delta}\right) \varphi\left(\frac{\delta \tau - 16 \xi_1}{\delta_1}\right) \text{ und } \left(\frac{2}{u}\right) \varphi\left(\frac{u \tau - 16 \xi_2}{u_1}\right)$$

für diejenige Function $\varphi(\tau)$ einander gleich, deren zugehöriges τ eine Lösung der Gleichung:

$$P \tau^2 + 2 Q \tau + R = 0$$

ist.

Aus diesen Resultaten folgen mit Leichtigkeit eine Menge von Sätzen, die eine Verallgemeinerung derjenigen Sätze sind, die Hermite in seinem schon citirten Werke p. 35 sq. für eine Primzahltransformation ohne Beweis aufgestellt hat, doch unterlassen wir die Ableitung derselben.

Heidelberg, den 21. März 1875.