Zur

Theorie der Modulargleichungen

der elliptischen Functionen

von

Julius König.

Der hohen philosophischen Fakultät zu Heidelberg

als Inauguraldissertation überreicht.

Heidelberg 1870.

Inhalt.

I.

Die Modulargleichungen

für einen beliebigen unparen Transformationsgrad.

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

$$du = \frac{dx}{\sqrt{(1-x^2)(1-c^2x^2)}}$$

$$du = \frac{ady}{\sqrt{(1-y^2)(1-k^2y^2)}}$$

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

$$\tau = \frac{b_0 + b_1\tau'}{a_0 + a_1\tau'}$$

oder

$$\tau' = \frac{b_0 - a_0\tau}{a_1\tau - b_1}$$

sein, wo noch

$$a_0 b_1 - a_1 b_0 = n$$

eine positive ganze Zahl, der Grad der Transformation ist.

Solcher Zahlensysteme a_0, a_1, b_0, b_1, welche obenstehender Gleichung genügen, gibt es unendlich viele; doch lassen sich dieselben bekanntlich immer in eine endliche Anzahl von Classen eintheilen; eine jede solche enthält wohl abermals unendlich viele Transformationen, doch nur jene, die durch lineare Transformation in einander übergehn. Es ist für

$$n = a\alpha\, b\beta \ldots -,$$

diese Classenzahl

$$a^{\alpha-1}\, b^{\beta-1} \ldots (a+1)\,(b+1) \ldots .$$

ein Ausdruck, der, sobald n keinen quadratischen Theiler enthält, gleichbedeutend wird mit der Summe aller Divisoren von n. —

Wir schreiben

$$\sqrt[4]{c} = u \quad , \quad \sqrt[4]{k} = v$$

wo die linken Seiten in bestimmter Weise definirte, eindeutige Grössen sind; dann existirt immer eine algebraische Gleichung — die zur Transformation n^{ten} Grades gehörige Modulargleichung, die wir durch

$$\Theta_n (u\ ,\ v) = o$$

bezeichnen wollen, deren Lösungen die v sind, die je einem Repräsentanten sämmtlicher Classen entsprechen. — Es sind diese Wurzeln Ausdrücke, deren transzendente Form die Transformationstheorie der elliptischen Functionen gibt. Der Grad der Modulargleichung ist dem gesagten entsprechend, der oben angeführte Ausdruck der Classenanzahl.

Man weiss ferner von der Modulargleichung, dass sie sich nicht ändert, wenn man u mit v und v mit $\left(\frac{2}{n}\right)$u vertauscht, wo $\left(\frac{2}{n}\right)$ das bekannte Legendre'sche Zeichen ist. — Ebenso bleibt die Gleichung dieselbe, wenn man auf c und k dieselbe lineare Transformation anwendet.

Die Transformatien pqten Grades lässt sich in der Weise ausgeführt denken, dass man die Transformationen des pten und qten Grades nacheinander anwendet. — Bei Anwendung dieses Princips ist es nur für Primzahlen nothwendig, die Modulargleichungen in der vorhergegangenen Weise zu definiren. Seien die Wurzeln der Modulargleichung, die zum Grade p gehört,

$$\Theta_p\ (w\ ,\ u) = o$$

$$w_p^{(1)}\ ,\ w_p^{(2)}\ ,\ \ldots\ ,\ w_p^{(p+1)}$$

so wird die Gleichung

$$\Theta_q\left(v, w_p^{(1)}\right) \cdot \Theta_p\left(v, w_p^{(2)}\right) \ldots \Theta_p\left(v, w_p^{(p+1)}\right) = 0$$

jene vierten Wurzeln der zu den Repräsentanten sämmtlicher Classen gehörigen Integralmoduln, welche die Transformation

pqten Grades besitzt, als Lösungen enthalten. D. h. die Modulargleichung, welche zum Grade pq gehört

$$\Theta_{pq}(v , u) = 0$$

ist das Eliminationsresultat aus

$$\Theta_{p}(v , w) = 0$$

und

$$\Theta_{q}(w , u) = 0$$

Man übersieht leicht, wie diese Definitionen vollständig übereinstimmen, so lange der Transformationsgrad keinen quadratischen Theiler enthält. In diesem Falle jedoch wird die Modulargleichung, als Resultante betrachtet, eine Reihe von Wurzeln mehrfach enthalten. Wir betrachten die Gleichung erst nach Hinwegschaffung dieser gleichen Wurzeln und dann wird sie mit der durch unmittelbare Zusammensetzung erhaltenen übereinstimmen müssen. [1])

II.

Reihenentwicklung

der Wurzeln der Modulargleichung.

Um die Wurzeln der Modulargleichung in Reihen zu entwickeln, untersuchen wir die Werte, welche v annimmt, wenn u unendlich klein wird; nach bekannten algebraischen Sätzen erhält man hieraus die Reihen für v, welche nach Potenzen von u fortschreiten. Es ist dann in der leichtesten Weise möglich durch Linearsubstitutionen Reihenentwicklungen mit anderem Argument zu erhalten.

Sei zuerst der Grad der Transformation eine Primzahl p, dann ist für einen Repräsentanten einer der $p+1$ nicht äquivalenten Klassen

$$v = u^{p} \operatorname{snc}.\frac{4C}{p} \operatorname{snc}.\frac{8C}{p} \ldots \operatorname{snc}.\frac{2(p-1)C}{p}$$

[1]) Siehe in Bezug auf die hier angeführten Sätze, sowie die durchweg gebrauchten Bezeichnungen das Werk meines hochverehrten Lehrers, Prof. Königsberger: Die Transformation, die Multiplication und die Modulargleichungen der elliptischen Funktionen, Leipzig 1868.

und es ist dieser Ausdruck für

$$\text{Lim. } u = 0$$

zu untersuchen. Man hat

$$\text{snc.}\frac{2Cx}{\pi} = \frac{2}{\sqrt{c}}\sqrt[4]{q}\,\cos. x \prod \frac{1 + 2q^{2n}\cos. 2x + q^{4n}}{1 + 2q^{2n-1}\cos. 2x + q^{4n-2}}$$

nun werden für unendlich kleine c die vollständigen elliptischen Integrale C und C^1 sich den Grenzen $\frac{\pi}{2}$ und ∞ nähern; daraus ergibt sich

$$\text{Lim. } q = \lim e^{\frac{\pi C'}{C}} = 0$$

und

$$\lim. \text{ snc.}\frac{2Cx}{\pi} = \lim. \frac{2}{\sqrt{c}}\sqrt[4]{q}\,\cos. x$$

Setzt man hierin für x der Reihe nach die Werthe

$$\frac{2\pi}{p}, \frac{4\pi}{p}, \ldots \frac{(p-1)\pi}{p}$$

ein, und multiplicirt, so wird

$$\text{Lim. snc.}\frac{4C}{p} \cdots \text{snc.}\frac{2(p-1)C}{p} =$$

$$= \text{Lim. } \frac{2^{\frac{p-1}{2}}}{u^{p-1}}\sqrt[4]{q}^{\frac{p-1}{2}} \cos. \frac{2\pi}{p} \cdots \cos. \frac{(p-1)\pi}{p}$$

Ferner ist

$$u = \sqrt[4]{c} = \sqrt{2}\sqrt[8]{q}\,\{(1+q^2)(1+q^4)\cdots\}^2(1-q)(1-q^3)\cdots$$

und

$$\cos\frac{2\pi}{p} \cdots \cos\frac{(p-1)\pi}{p} = \left(\frac{2}{p}\right)\frac{1}{2^{\frac{p-1}{2}}}$$

Mit Benützung dieser Relationen erhält man schliesslich das Resultat

$$(1,) \qquad \text{Lim. v.} = \left(\frac{2}{p}\right)\lim. \frac{u^p}{2^{\frac{p-1}{2}}}$$

Da die Modulargleichung sich durch Vertauschung von u und v mit v und $\left(\frac{2}{p}\right)$u nicht ändern darf, erhält man hieraus auch

$$\text{Lim. } u = \lim \frac{v^p}{2^{\frac{p-1}{2}}}$$

oder

$$\text{Lim. } v_s = \lim 2^{\frac{p-1}{2p}} u^{\frac{1}{p}} e^{\frac{2s\pi\iota}{p}} \qquad (2)$$

wo $s = 1, 2, \cdots p$. Die Formeln 1 und 2 enthalten demnach die Werthe aller $p + 1$ Wurzeln für unendlich kleine u.

Die Wurzelwerte einer algebraischen Gleichung

$$f(v, u) = 0$$

für $u = 0$ sind die ersten Glieder in der Reihenentwicklung der betreffenden Wurzeln nach Potenzen von u. Schreiben wir noch der Kürze wegen

$$a_p = 2^{\frac{p-1}{2p}}$$

$$b_p = \frac{1}{2^{\frac{p-1}{2}}}$$

dann ist

$$v_s = a_p u^{\frac{1}{p}} e^{\frac{2s\pi\iota}{p}} + a_p^{(1)} u^{\frac{2}{p}} + \cdots \quad s = 1 \cdots p$$

$$\left(\frac{2}{p}\right) v_{p+1} = b_p u^p + b_p^{(1)} u^{p+1}$$

Der transzendente Ausdruck für die durch v_s bezeichneten Wurzeln ist

$$v = u^p \text{ snc.} \frac{4C}{p} (\tau - 16\xi) \cdots \text{snc.} \frac{2(p-1)C}{p} (\tau - 16\xi)$$

und für v_{p+1}

$$v_{p+1} = u^p \text{ snc.} \frac{4C}{p} \cdots \text{snc.} \frac{2(p-1)}{p} C$$

Setzt man in diesen Ausdrücken statt des u $ue^{\frac{\pi\iota}{4}}$ so wird, da C nur von u^8 abhängt, dieses sich gar nicht ändern und die Wurzel durch diese Substitution nur mit einer 8ten Einheitswurzel multiplizirt werden. Dasselbe muss also auch der Fall sein, wenn die Wurzeln in der eben entwickelten Form als Potenzreihen entwickelt sind, und dies ist nur möglich, wenn alle Glieder in denen nicht u mit Exponenten von der Form $\frac{8m+1}{p}$ für die v_s, und $8m + p$ für v_{p+1} vorkömmt, verschwinden. Wir übergehn die Bestimmung der weiteren Coeffizienten der Reihe, da in den folgenden Entwicklungen nirgends davon Gebrauch zu machen ist [1]).

[1]) Die Entwicklung dieser Reihen für Primzahlgrade ist gegeben von Matthieu. Journal de l'école polytechnique. Cah. 42.

Es beginnt also die Entwicklung von p der Wurzeln mit $u^{\frac{1}{p}}$, und die der einzig übrigen mit u^{p} —

Man hat für 2 verschiedene Transformationsgrade p und q, wenn die zugehörigen Modulargleichungen

$$\Theta_p\,(w,u)=0$$
$$\Theta_q\,(v,w)=0$$

sind, demnach:

$$w_s = a_p\, u^{\frac{1}{p}}\, e^{\frac{2s\pi\iota}{p}} + \cdots \qquad s = 1 \cdots p$$

$$\left(\frac{2}{p}\right) w_{p+1} = b_p\, u^p + \cdots$$

und

$$v'_s = a_q\, w^{\frac{1}{q}}\, e^{\frac{2s'\pi\iota}{p}} + \cdots \qquad s' = 1 \cdots q$$

$$\left(\frac{2}{q}\right) v_{q+1} = b_q\, w_q + \cdots.$$

Die Wurzeln der zur Transformation pqten Grades gehörigen Modulargleichung

$$\Theta_{pq}\,(v,u)=0$$

werden nun folgende sein:

$$v_s = a_p^{\frac{1}{q}}\, a_q\, u^{\frac{1}{pq}}\, e^{\frac{2s\pi\iota}{pq}} + \cdots \qquad s = 1, \cdots pq$$

$$\left(\frac{2}{q}\right)_{v_{pq+s'}} = a_p^q\, b_q\, u^{\frac{q}{p}}\, e^{\frac{2s'\pi\iota}{p}} + \cdots \qquad s' = 1 \cdots p$$

$$\left(\frac{2}{p}\right)_{v_{pq+p+s''}} = a_q\, b_q^{\frac{1}{q}}\, u^{\frac{p}{q}}\, e^{\frac{2s''\pi\iota}{q}} + \cdots \qquad s'' = 1 \cdots q$$

$$\left(\frac{2}{pq}\right) v_{(p+1)\,q+1)} = b_p^q\, b_q\, u^{pq} + \cdots$$

In ganz ähnlicher Weise fortfahrend, wird es möglich sein, die Reihenentwicklungen festzustellen, wenn der Transformationsgrad eine beliebige ungrade Zahl ist. (Enthält derselbe quadratische Theiler, so sind wie bemerkt, die gleichen Wurzeln auszuschliessen). —

Für ein n ohne quadratische Theiler gelten nun folgende Sätze:

1) Die Coeffizienten des ersten Glieds in der Entwicklung der verschiedenen Wurzeln sind sämmtlich verschieden.
2) Ist d ein beliebiger Theiler des n, so gibt es immer d Wurzeln, deren Entwicklung mit $u^{\frac{n}{d^2}}$ beginnt. Dem

Zeichen nach gilt die Entwicklung für

$$\left(\frac{2}{\frac{n}{d}}\right) v = \left(\frac{2}{nd}\right);$$

die Summe der d ist eben der Grad der Gleichung.

Beide Sätze sind, wie man sich aus dem vorhergehenden unmittelbar überzeugt, richtig, wenn n aus ein oder zwei Primfactoren besteht. Die Coeffizienten von je d Wurzeln sind gebildet aus einer Zahl, die mit den verschiedenen dten Einheitswurzeln der Reihe nach multiplizirt ist. Sobald aber die Wurzeln — wie man sich ausdrücken kann — verschiedenen d entsprechen, ist der absolute Werth des 1. Coeffizienten ein verschiedener- — Die Sätze werden allgemein richtig sein, wenn wir nachweisen können, dass sie für ein n richtig sind, das aus $m+1$ Primfactoren besteht, sobald sie für ein aus m solchen bestehendes galten. —

Sei $n = dn'$; man habe ferner für den Transformationsgrad n' gezeigt, dass die Entwicklung von je d' Wurzeln mit

$$a_s^{(d')} w^{\frac{n'}{d'^2}} \qquad s = 1, \cdots d'$$

beginnt, sowie dass die a sämmtlich ungleich

Die Wurzeln der Gleichung

$$\Theta_d (w, u) = 0$$

sind nun wieder:

$$w_{s'} = a_d u^{\frac{1}{d}} e^{\frac{2s'\pi i}{d}} + \cdots \qquad s' = 1, \cdots d$$

$$\left(\frac{2}{d}\right) w_{d+1} = b_d u^d + \cdots$$

Das Einsetzen der ersten d Wurzeln im obigen gibt nun d'd Wurzeln deren Entwicklung mit

$$u^{\frac{n'}{dd'^2}} = u^{\frac{n}{d^2 d'^2}}$$

beginnt, und zwar gilt diese wieder für $\left(\frac{2}{ndd'}\right) v$; die Substitution der Wurzeln w_{d+1} gibt d' Wurzeln, deren Entwicklung mit

$$u^{\frac{n'd}{d'^2}} = u^{\frac{n}{d'^2}}$$

beginnt, und zwar ist diess $\left(\frac{2}{nd'}\right) v \cdots$ Die d' und d'd sind aber wieder sämmtliche Divisoren der Zahl n. — Auch die neuen Coeffizienten

$$a_s^{(d')} \quad a_d\, e^{\frac{2s'\pi i}{d}} \qquad s' = 1, \cdots d$$

können nicht gleich werden, wenn es unter denen für n' keine solchen gab. Abermals sind je d gleiche Zahlen, aber mit den verschiedenen dten Einheitswurzeln multiplicirt.

Die angeführten Sätze sind somit auch allgemein bewiesen.

Die Irreductibilität der Modulargleichungen folgt unmittelbar aus dem ersten derselben.

Die algebraische Gleichung $f(v,u) = 0$ vom Grade n ist irreductibel, wenn $v = \varphi(u)$ für jeden Punkt in der Ebene, mit Ausnahme der in endlicher Anzahl vorhandenen Verzweigungspuncte, für welche die Gleichung $f(v,u')$ gleiche Wurzeln erhält, n von einander verschiedene Werthe hat. Wir haben gezeigt, dass die Reihenentwicklung sämmtlicher Wurzeln der Modulargleichung verschieden ist. Die Modulargleichungen für einen unparen Transformationsgrad sind also immer irreductibel, da der 1te Satz auch dann noch gilt, wenn n einen quadratischen Theiler besitzt; wenn nur die gleichen Wurzeln die bei der Bildung der Modulargleichung als Resultante auftreten, weggeschafft wurden.

III.

Die Dimension der Modulargleichung.

Sei eine Gleichung gegeben:

$$f(v, u) = o$$

in welcher für $u = o$ auch $v = o$ ist und die Ableitung nach u verschwindet. Wir wählen in derselben jene Termen aus, die so beschaffen sind, dass es keine Glieder gibt, in denen beide Variabeln mit niedrigerem Exponenten vorkommen. Dann sind die Termen niedrigster Dimension jedenfalls in dieser Reihe.

$$A = A_o\, v^{p_o} u^{q_o} + A_1\, v^{p_1} u^{q_1} + \ldots + A_m\, v^{p_m} u^{q_m}$$

enthalten, von welcher man ausserdem weiss, dass die p eine steigende Reihe bilden wenn man nach fallenden q geordnet hat. Wäre zugleich p_1 und q_1 grösser oder kleiner als p_s und und q_s, so wäre ja für das eine der Glieder die oben ausgesprochene Bedingung nicht erfüllt. Nach den Untersuchungen von Puiseux [1]) gilt nun folgendes:

[1]) Recherches sur les fonctions algébriques, Liouville, XV.

Ist

$$q_{i+1} - q_i = \varphi_i \; r_i$$
$$p_i - p_{i+1} = \varphi_i \; s_i$$

wo φ_i den grössten gemeinschaftlichen Theiler beider Grössen darstellt, so gibt es φ_i Gruppen von r_i Wurzeln, deren Entwicklung mit einem Gliede

$$\alpha u^{\frac{r_i}{s_i}}$$

beginnt. Jede solche Gruppe erleidet eine cyclische Permutation, wenn man um den Punkt $u = o$ herumgeht.

Sei umgekehrt bloss ein Term jener Reihe Δ bekannt; man wisse ferner, dass die Entwicklung von je a_i Wurzeln mit

$$\alpha u^{\frac{b_i}{a_i}}$$

beginnt, wo $i = 1, \cdots m$.

Dann ist jedenfalls:

$$q_i - q_{i-1} = b_i \; \varphi_i$$
$$p_{i-1} - p_i = a_i \; \varphi_i$$

aber auch $\varphi_i \; a_i = a_i$

also $\varphi_i = 1$

und $q_i - q_{i-1} = b_i$

$$p_{i-1} - p_i = a_i$$

Aus der früher hergeleiteten Bedingung, dass die Reihe der p eine fallende, die der q eine steigende sei, erhält man ähnliche für a und b. Es ist

$$a_i = p_{i-1} - p_i$$
$$a_{i+1} = p_i - p_{i+1}$$

und da

aus $p_{i-1} < p_i < p_{i+1}$

$$p_i - p_{i+1} < p_{i-1} - p_i$$

folgt, auch

$$a_i > a_{i+1}$$

Sind nun die a in fallender Reihe geordnet, so müssen die b von selbst eine steigende Reihe bilden. In dieser Weise ist die Reihenfolge der Wurzeln eine fest bestimmte geworden, und man hat

$$q_i = q_{i-1} + b_i$$
$$p_i = p_{i-1} - a_i$$

oder wenn man den Term $A_o \; v^{p_o} \; u^{q_o}$ als bekannt annimmt

$$q_1 = q_0 + \sum_{s=1}^{s=i} b_s$$

$$p_1 = p_0 - \sum_{s=1}^{s=i} a_s$$

Die Modulargleichung für einen ungraden Transformationsgrad genügt nun den eben entwickelten Bedingungen. Ist d ein Divisor des n, so beginnt die Entwicklung von d Wurzeln mit einem Gliede, in dem der Exponent des u $\frac{\frac{n}{d}}{d}$ ist, wo $\frac{n}{d}$ und d relativ prim sind. Sind die Nenner jetzt in fallender Reihe geordnet, so bilden, wie man unmittelbar sieht, die Zähler eine steigende Reihe. Wir kennen auch den ersten Term der Reihe; er ist

$$v^{S(n)}$$

wenn $S_{(n)}$ die Summe aller Divisoren der Zahl n bedeutet. Man erhält also für $\mathcal{A}$, wenn die der Grösse nach geordneten Divisoren $d_1, d_2, \cdots$ sind (wo $d_1 = n$)

$$v^{S(n)} + \alpha_1 v^{S(n)-d_1} u + \alpha_2 v^{S(n)-d_1-d_2} u^{1+\frac{n}{d_2}} + \cdots$$

Welches ist nun der Term niedrigster Dimension in der Reihe $\mathcal{A}$ selbst? Wir bemerken früher noch, dass von diesen Termen keiner aus der Modulargleichung verschwinden darf, da dann die Wurzelentwicklungen, von denen wir ausgingen, nicht mehr statthaben könnten. — Die Hälfte der Anzahl der Divisoren von n ist bekanntlich grösser, ebenso viele kleiner als $\sqrt{n}$. So lange man nun im Exponenten von v Divisoren von n abzieht, die grösser als $\sqrt{n}$, und in dem von u solche addirt, die kleiner als $\sqrt{n}$ (wenn $d > \sqrt{n}$ ist eben $\frac{n}{d} < \sqrt{n}$) wird die Dimension der aufeinander folgenden Glieder immer geringer werden. — Bezeichnet man die Summe aller Divisoren, die kleiner als $\sqrt{n}$ mit $\psi(n)$ so ist das Glied niedrigster Dimension $\alpha u^{\psi(n)} v^{\psi(n)}$ —

Wenn n eine Primzahl, wird

$$\psi(n) = 1$$

und man hat den Satz, dass aus der zu einem Primzahlgrad ge-

hörenden Modulargleichung der Term $\alpha\, u\, v$ nicht verschwinden kann; — Sohncke [1]) erwähnt und gebraucht denselben in seiner Arbeit, während der dortige Beweis jedenfalls auf einem Irrthum beruht.

Aus dem Term niedrigster Ordnung erhält man nun sofort den Term höchster Ordnung. War jener

$$\alpha\, v\psi(n)\ u\varphi(n)$$

so muss dieser wenn wir noch die Summe der Divisoren die grösser sind als $\sqrt{n}$, d. i.

$$S(n) - \psi(n) = \varphi(n)$$

setzen $\alpha\ v\varphi(n)\ u\varphi(n)$

sein. Es ist Derjenige, welcher aus jenem entsteht, wenn man in der Modulargleichung u und v mit $\frac{1}{u}$ und $\frac{1}{v}$ vertauscht. Ein höheres Glied, z. B.

$$\alpha\, v\varphi(n) + a\ u\varphi(n) + b$$

kann nicht vorkommen; ihm entspräche durch abermalige Vornahme obiger Substitution

$$\alpha\, v\psi(n) - a\ u\psi(n) - b$$

ein Term niedrigerer Ordnung, als er überhaupt vorkommen kann.

Die grösste Dimension der Glieder der Modulargleichung ist also $2\varphi(n)$, die niedrigste $2\psi(n)$, wo $\varphi(n)$ und $\psi(n)$ die von Kronecker eingeführte Bedeutung besitzen.

IV.

Die Discriminante der Modulargleichungen.

Das Verschwinden der Discriminante ist bekanntlich die Bedingung dafür, dass eine Gleichung gleiche Wurzeln besitzt. Die Discriminante der Modulargleichung wird uns daher jene Integralmodulen liefern, welche durch eine Transformation n^{ten} Grades in sich selbst übergehn. Da diese nun, wenn n keinen quadratischen Theiler enthält, auch keine reelle Multiplication geben kann, werden jene Moduln die der complexen Multiplication

---

[1]) Sohncke, aequationes modulares pro transformatione functionum ellipticarum. Crelle, XVI. pag. 110.

sein, und zwar sämmtliche, die zur Transformation nten Grades gehören. Es ist also von Wichtigkeit, die Discriminante näher zu untersuchen, und ihre Factoren, wo möglich zu sondern.

Wir beschäftigen uns zuerst mit der Bestimmung des Grades der Discriminante. Die Modulargleichung besitzt die Form

$$v^{S(n)} + C_1 v^{S(n)-1} + \cdots + C_{S(n)} = 0$$

Die C sind hierin ganze Funktionen von u. Für das folgende ist es nothwendig den Grad von C_1 und $C_{S(n)}$ kennen zu lernen. Man weiss unmittelbar für letzteres, dass

$$C_{S(n)} = \pm u^{S(n)}$$

ist. — Aus den hervorgehenden Entwicklungen ist ferner bekannt, dass der Term

$$v^{S(n)-n} u$$

der Reihe derer niedrigster Ordnung angehört. Also ist

$$v^n u^{S(n)-1}$$

eines der Glieder aus der Reihe für die von höchster Dimension. Durch Vertauschung von u und v erhält man abermals einen Term dieser Reihe

$$v^{S(n)-1} u^n$$

und hieraus schliesst man, dass C_1 eine Function nten Grades von u ist.

Aus der Modulargleichung und ihrer Ableitung, nach v genommen, lässt sich nun nach Sylvester's dialytischer Methode die Discriminante als Determinante unmittelbar bilden. Sie besteht aus $2S(n) - 1$ Zeilen und Colonnen und lautet:

$$D = \begin{vmatrix} 1, C_1, C_2, \cdots C_{S(n)-1}, C_{S(n)}, 0, 0 \cdots 0 \\ 0, 1, C_1, \cdots\cdots\cdots, C_{S(n)}, 0 \cdots 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0, 0, 0, \cdots, 1, C_1, C_2, \cdots C_{S(n)} \\ S_{(n)}, (S_{(n)-1}) C_1, \cdots\cdots\cdots C_{S(n)-1}, 0 \cdots 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0, 0, \cdots\cdots\cdots S_{(n)}, (S_{(n)-1}) C_1, C_{S(n)-1} \end{vmatrix}$$

Aus derselben ist das höchste Glied zu suchen. Die in der Anzahl $S_{(n)} - 1$ vorhandenen $C_{S(n)}$ lassen sich nicht zusammenfassen, da die Unterdeterminante null würde. Man muss also eines derselben weglassen und zwar jenes, welches der dann entsprechenden Unterdeterminante den höchsten Grad gibt. Dies geschieht wenn man das $C_{S(n)}$ der ersten Zeile heraushebt,

dort dafür die 1 setzt; dann ist in der zurückgebliebenen Unterdeterminante das höchste Glied

$$(S_{(n)-1}\ C_1)^{S(n)}\ .$$

Würde man ein anderes $C^{S(n)}$ weglassen, so erhält man jedenfalls ein Glied von niedrigerem Grade, in dieser Unterdeterminante selbst wird jedes andre Glied statt C_n^2 den niedrigeren Factor $C_{s-1}\ C_{s+1}$ enthalten u. s w.

Hienach ist der Grad der Discriminante:

$$S_{(n)}\ (S_{(n)} - 2) + S_{(n)}\ n$$

ein Ausdruck der für primzahlige n sich auf

$$(n + 1)\ (2n - 1)$$

reduzirt.

Die Discriminante ist eine symmetrische Funktion der Wurzeln der Modulargleichung, die sich bei keiner Permutation derselben ändert. Sie ist aber auch eine ganze Function von u, die wir durch Benutzung der Entwicklungen für die Wurzeln der Modulargleichungen in Form einer Reihe erhalten können, indem wir sie als Product der quadrirten Wurzeldifferenzen bilden. — Wir bemerken noch, dass die Discriminante jedenfalls ein Ausdruck von der Form

$$u^{f(n)}\ (1 - u^8)^{f'(n)}\ g\,(u)$$

ist. — Wir wollen uns zuerst nun damit beschäftigen, die Anzahl der Grenzfälle

$$u = o\ ,\ u^8 = 1$$

zu bestimmen, und dann auf das Polynom g(u) eingehn, das die wirklichen Modulen der complexen Multiplication liefert.

V.

Die numerischen Funktionen f(n) und f'(n).

Wir haben früher gezeigt, dass sich sämmtliche Wurzeln der Modulargleichung nach gebrochenen Potenzen von u entwickeln lassen, und zwar, dass wenn d ein Divisor von n, die Entwicklung von je d Wurzeln mit $u^{\frac{n}{d^2}}$ beginnt. Wir bilden das Produkt der quadrirten Differenzen dieser Reihen, und suchen die

Potenz von u, mit welcher dasselbe als Factor austritt. Der Exponent ist eben f(n).

Man berücksichtige zuerst jenen Theil des Produkts, welcher entsteht, wenn man nur die Differenzen bildet, deren Entwicklung mit derselben Potenz des u beginnt. Die Potenz von u, die als Factor auftritt, ist

$$\Sigma\,(d-1)\,\frac{n}{d}$$

wo d der Reihe nach die Divisoren von n bedeutet. Es ist aber

$$\Sigma\,(d-1)\frac{n}{d} = \Sigma\, n\,\frac{d}{d} - \Sigma\,\frac{n}{d} = n\,S'(n) - S\,(n)$$

wenn S'(n) die Anzahl und S(n) wie früher die Summe der Divisoren von n bedeutet. —

Nun sind noch die quadrirten Differenzen aller Wurzeln zu bilden, die verschiedenen Gruppen (d) angehören.

Man hat z. B. d Wurzeln, deren Entwicklung mit $u^{\frac{n}{d^2}}$ und d' Wurz, die mit $u^{\frac{n}{d'^2}}$ beginnt, und zwar sei $d > d'$. Dann tritt aus dd' quadr. Wurzeldifferenzen der Factor

$$u^{\frac{2n}{d^2}}$$

$$u^{\frac{2\,d'\,n}{d}}$$

im ganzen

aus. d' und $\frac{n}{d}$ sind natürlich abermals Divisoren von n, und für dieselben folgt aus

$$d > d'$$

die Bedingung $\qquad d'.\,\frac{n}{d} < n$

Jede solche Zusammenstellung wird also eine Potenz von u als Factor der Discriminante auftreten lassen, deren Exponent das Doppelte des Produkts zweier Divisoren des n, die der Bedingung

$$d\,\delta < n$$

genügen, wo der Fall $d\,\delta = n$ ausgeschlossen bleibt. Es werden auch sämmtliche solche Produkte gebildet, d und d' waren ja willkürlich gewählt.

Noch fragt es sich, wie oft jedes solche Produkt vorkömmt. In jeder Art der Factorenzerlegung zweimal. Der Zusammenstellung von

d Wurzeln, die mit $u^{\frac{n}{d^2}}$ und

d' Wurzeln, die mit $u^{\frac{n}{d'^2}}$ beginnen,

entspricht noch die zweite von

d Wurzeln die mit $u^{\frac{n}{d^2}}$ und

$\frac{n}{d'}$ Wurzeln, die mit $u^{\frac{d'^2}{n}}$ anfangen.

Beide geben den Factor $u^{2d\delta}$ wo wieder

$$\delta = \frac{n}{d'}$$

ist. Nur wenn $d = \delta$ ist, fallen diese beiden Gruppen zusammen. Man erhält für f(n) die Formel [1])

$$f(n) = n\,S'(n) - S(n) + 2s(n) + 4\sigma(n)$$

wo die neueingeführten Funktionen s(n) und $\sigma(n)$ die folgende Bedeutung besitzen.

Es ist s(n) die Summe der Quadrate der Divisoren die kleiner als $\sqrt{n}$ und $\sigma(n)$ die Summe der Producte aller Pare von Divisoren, für die $d\,\delta < n$ ist.

Für Primzahlen wird einfach

$$f(n) = n + 1.$$

Um nun auch die Funktion f'(n) zu erhalten, werden wir ein analoges Verfahren in Bezug auf jene Reihenentwicklungen der Wurzeln einschlagen, die nach Potenzen von $u - \alpha$ fortschreiten, wo α eine beliebige 8te Einheitswurzel bedeutet. Der Einfachheit wegen führen wir zuerst die Rechnung für den Factor $u - 1$ durch. Die übrigen lassen sich unmittelbar ableiten.

Um nun zu diesen Reihen zu gelangen, kann man den zuerst gemachten ganz ähnliche Grenzbetrachtungen anstellen [2]), doch ergibt sich das gesuchte viel leichter in folgender Weise:

---

[1]) Diese Formel, sowie die für f'(n) und den Grad des Polynoms g(u) sind ohne Beweis mitgetheilt von Hermite (Sur la théorie des équations modulaires, Paris, 1859) doch haben sich in den dort gegebenen Ausdrücken leider Irrthümer eingeschlichen.

[2]) Matthien, a. a. O. p. 278.

Für den Fall einer Primzahl war

$$v'_1 = a_p u^{\frac{1}{p}} e^{\frac{2s\pi\iota}{p}} + \cdots \qquad s = 1, \cdots p$$

$$v'_{p+1} = b_p u^p + \cdots$$

wo

$$a_p = 2^{\frac{p-1}{p}} \quad \text{und} \quad b_p = \frac{1}{2^{\frac{p-1}{2}}}$$

Die Modulargleichung ändert sich nicht wenn man u^8 und v^8 mit $1-u^8$ und $1-v^8$ vertauscht. Man wird also abermals die Wurzeln der Modulargleichung erhalten (natürlich ohne dass das jetzige v_s das frühere v'_s sei), wenn man die erhaltenen Reihen in die 8te Potenz erhebt und dann die angeführte Vertauschung vornimmt. Das gibt

$$1 - v_s^8 = a_p^8 (1-u^8)^{\frac{1}{p}} e^{\frac{2s\pi\iota}{p}} + \cdots \qquad s = 1 \cdots p$$

$$1 - v_{p+1}^8 = b_p^8 (1-u^8)^p + \cdots$$

Man weiss nun [1]), dass für

$$u = 1$$

die Modulargleichung, je nachdem

$$\left(\frac{2}{p}\right) = \pm 1$$

ist, die Form

$$(v-1)^{p+1} = 0$$

oder

$$(v+1)^p (v-1) = 0$$

annimmt. Die Wurzeln $v_1, \cdots v_p$ sind also gleich $\left(\frac{2}{p}\right)$ und v_{p+1} immer gleich 1. —

Für lim. $u = 1$ ist also

$$\lim v_s = \left(\frac{2}{p}\right)$$

Man hat aber auch

$$\text{Lim } (1 - v_s^8) = \text{Lim.} \left[1 - \left\{\left(\frac{2}{p}\right) + v - \left(\frac{2}{p}\right)\right\}^8\right] =$$

$$= \text{Lim } 8 \left(1 - \left(\frac{2}{p}\right) v\right)$$

Und ebenso

$$\text{Lim } (1-u^8) = \text{Lim. } 8\,(1-u)$$

---

[1]) Sohncke, a. a. O. p. 112.

also

$$\text{Lim } 8\left(1-\left(\frac{2}{p}\right)v\right)=8^{\frac{1}{p}}\,a_p^8\,(1-u)^{\frac{1}{p}}\,e^{\frac{2s\pi i}{p}}$$

und da

$$\frac{8^{\frac{1}{p}}\,a_p^8}{8}=2^{\frac{p-1}{p}}=\alpha_p$$

ist,

$$\text{Lim}\left(v_s-\left(\tfrac{2}{p}\right)\right)=\text{Lim}\left(\frac{2}{p}\right)\alpha_p\,(u-1)^{\frac{1}{p}}\,e^{\frac{2s\pi i}{p}}$$

Aus diesem Grenzausdruck schliesst man wieder, dass die Reihenentwicklung die Form

$$1)\quad v_s=\left(\frac{2}{p}\right)+\left(\frac{2}{p}\right)\alpha_p\,(u-1)^{\frac{1}{p}}\,e^{\frac{2s\pi i}{p}}+\cdots\cdots$$
$$s=1\cdots p$$

hat. Für

$$v_{p+1}=b_p\,u^p+\cdots\cdots$$

hat man ganz ähnlich

$$1-v_{p+1}^8=b_p^8\,(1-u^8)^p+\cdots$$

und weiter

$$\text{Lim}\left\{-8\,(1-v_{p+1})\right\}=\text{Lim}\left\{8^p\,b_p^8\,(1-u)^p\right\}$$

woraus da

$$b_p=\frac{1}{2^{\frac{p-1}{2}}}$$

$$8^{p-1}\,b_p^8=\frac{1}{2^{p-1}}=\beta_p$$

die Reihenentwicklung

$$2)\quad v_{p+1}=1+\beta_p\,(u-1)^p+\cdots\cdots$$

folgt. — Aus der Entwicklung für Primzahlgrade setzt man nun leicht die übrigen zusammen. Man braucht dazu nur die Werthe von $w-1$ aus

$$1a)\ w_s=\left(\frac{2}{q}\right)+\left(\frac{2}{q}\right)\alpha_q\,(u-1)^{\frac{1}{q}}\,e^{\frac{2s\pi i}{q}}+\cdots\ s=1\cdots q$$

$$2a)\ w_{q+1}=1+\beta_q\,(u-1)^q+\cdots\cdots$$

in

$$1b)\ v_s=\left(\frac{2}{p}\right)+\left(\frac{2}{p}\right)\alpha_p\,(w-1)^{\frac{1}{p}}\,e^{\frac{2s\pi i}{p}}+\cdots\ s'=1,\cdots p$$

$$2b)\ v_{p+1}=1+\beta_p\,(w-1)^p+\cdots$$

einzusetzen. Dies ergibt für die Zusammenstellung von (1a) und (1b)

$$v_s = \left(\frac{2}{p}\right) + \left(\frac{2}{p}\right)\alpha_p\left\{\left(\frac{2}{q}\right)-1\right\}^{\frac{1}{p}} + \left(\frac{2}{p}\right)\alpha_p\left(\frac{2}{q}\right)\alpha_q^{\frac{1}{p}} \times$$
$$\times (u-1)^{\frac{1}{pq}} e^{\frac{2s\pi\iota}{pq}} + \cdots$$

wo $s = 1, \cdots pq$

Nun ist aber immer

$$\left(\frac{2}{p}\right) + \left(\frac{2}{p}\right)\alpha_p\left(\frac{2}{q}-1\right)^{\frac{1}{p}} = \left(\frac{2}{pq}\right)$$

wie man sich für jede Zusammenstellung von

$$\left(\frac{2}{p}\right) = \pm 1 \text{ und } \left(\frac{2}{q}\right) = \pm 1$$

unmittelbar überzeugen kann. Also

1c) $$v_s = \left(\frac{2}{pq}\right) + \left(\frac{2}{pq}\right)\alpha_p\,\alpha_q^{\frac{1}{p}}(u-1)^{\frac{q}{p}} e^{\frac{2s\pi\iota}{pq}} + \cdots$$
$$s = 1, \cdots pq$$

wo wir noch bemerken wollen, dass der Ausdruck

$$\alpha_p\,\alpha_q^{\frac{1}{p}}$$

in Bezug auf p und q symmetrisch ist.

Ebenso erhält man

2c) $$v_s' = \left(\frac{2}{p}\right) + \left(\frac{2}{p}\right) a_p\,\beta_q^{\frac{1}{p}}(u-1)^{\frac{q}{p}} e^{\frac{2s'\pi\iota}{p}} + \cdots$$
$$s'' = 1 \cdots p$$

3c) $$v_s'' = \left(\frac{2}{q}\right) + \left(\frac{2}{q}\right)\alpha_p\,\beta_p^{\frac{1}{q}}(u-1)^{\frac{p}{q}} e^{\frac{2s''\pi\iota}{q}} + \cdots$$
$$s'' = 1 \cdots q$$

4c) $$v = 1 + \beta_p\,\beta_q^p\,(u-1)^{pq} + \cdots$$

wo auch

$$\beta_p\,\beta_q^p = \beta_q\,\beta_p^q$$

ist. Aus diesen Reihen, die wir für aus 1 oder 2 Primfactoren bestehende n entwickelt haben, lassen sich nun wieder die beiden folgenden Sätze ablesen:

1) Ist d ein Theiler von n, so beginnt die Entwicklung von d Wurzeln mit

$$\left(\frac{2}{d}\right) + \left(\frac{2}{d}\right) C(u-1)^{\frac{n}{d2}} + \cdots$$

2) Die Coeffizienten des 2ten Gliedes sind sämmtlich ungleich.

Für die behandelten Fälle sieht man die Richtigkeit der

Sätze unmittelbar; sie gelten aber auch für $m + 1$ Primfactoren, wenn sie für m galten. Es ist wohl nicht nothwendig, die Rechnung durchzuführen, deren Mechanismus wieder genau der gebrauchte ist. —

Daraus erhält man nun den Exponenten von $u - 1$ in der Discriminante. Seine Zusammensetzung geschieht genau so wie die für u. Nur in der Zusammenstellung der Differenzen von verschiedenen d entsprechenden Wurzeln werden gewisse Posten wegbleiben. Es muss nämlich

$$\left(\frac{2}{d}\right) = \left(\frac{2}{d'}\right)$$

sein, da sonst das constante Glied nicht wegfällt, also $u - 1$ auch nicht als Factor auftritt. Demnach wird der gesuchte Exponent

$$n\,S'(n) - S(n) + 2s'(n) + 4\,\sigma'(n)$$

wenn der Accent die neue Beschränkung von $s(n)$ und $\sigma(n)$ andeutet. Man kann dieser Bedingung noch eine etwas andere Form geben, wenn man wieder

$$\delta = \frac{n}{d'}$$

setzt. Dann ist

$$\left(\frac{2}{d'}\right) = \left(\frac{2}{\frac{n}{\delta}}\right)\left(\frac{2}{\delta^2}\right) = \left(\frac{2}{n\,\delta}\right)$$

und die Bedingung lautet nun:

$$\left(\frac{2}{d}\right) = \left(\frac{2}{n\,\delta}\right).$$

$u\,e^{\frac{\pi\iota}{4}}$ für u gesetzt gibt, wie gezeigt worden, wieder die Wurzeln der Modulargleichung, nur mit 8ten Einheitswurzeln multiplizirt. Setzt man also in den Reihen für u

$$u\,e^{\frac{s\pi\iota}{4}} \qquad s = 1 \cdots, 8$$

so erhält man die Entwicklungen für das Argument

$$u - e^{\frac{s\pi\iota}{4}}$$

Der Factor in der Discriminante hat immer genau denselben Ausdruck; also ist auch der Exponent von $u^8 - 1$ in derselben

$$f'(n) = nS'(n) - S(n) + 2s'(n) + 4\sigma'(n)$$

was wenn n eine Primzahl in

$$n + \left(\frac{2}{n}\right)$$

übergeht

VI.

Das Polynom g(u).

Man kennt den Grad der Discriminante, sowie den Werth von f(n) und f'(n). Der Grad von g(u) bestimmt sich daraus unmittelbar. — g(u) kann bloss solche n enthalten, deren Exponent $\equiv$ o mod. 8 ist; denn durch Multiplication des u mit einer 8ten Einheitswurzel, tritt nur ein constanter Factor zur Discriminante. Der Grad von g(u) ist 8 ν und zwar folgt aus

$$S(n)\,(S(n)-2) + S(n).n = f(n) + 8f'(n) + 8\nu$$

$$\nu = \frac{S(n)\,(S(n)-2) + S(n).n - f(n) - 8f'(n)}{8}$$

für eine Primzahl

$$\nu = \frac{n^2-1}{4} - \left(n + \left(\tfrac{2}{n}\right)\right).$$

Zur weiteren Untersuchung genügen die bisher gebrauchten Methoden nicht. Man kann nun aber die Wurzeln der Modulargleichung auch als Functionen des Moduls der zugehörigen Thetafunctionen betrachten und zwar sind diese wenn man mit Hermite

$$u = \varphi(\tau)$$

setzt, sämmtlich gegeben durch den Ausdruck

$$\left(\frac{2}{t}\right)\varphi\left(\frac{t\tau - 16\xi}{t'}\right)$$

wo $tt' = n$ und ξ mod. t' zu betrachten ist.

Ferner weiss man, dass jene τ, welche complexe Multiplication liefern, einer ganzzahligen quadratischen Gleichung

$$A\tau^2 + 2B\tau + C = o$$

mit negativer Determinante genügen.

Transformirt man die Form (A, B, C) durch die Substitution

$$\begin{vmatrix} a_o & , & a_1 \\ b_o & , & b_1 \end{vmatrix}$$

in (A', B', C'), so ist das Resultat dasselbe, wie wenn man

$$\tau' = \frac{b_0 + b_1 \tau}{a_0 + a_1 \tau}$$

setzt. Daraus schliessen wir, dass jene quadratischen Gleichungen, denen Formen derselben Klasse entsprechen, solche τ liefern, die durch lineare Substitution ineinander übergehn, dass es also gestattet sein wird, die zu betrachtenden Gleichungen mit andern zu vertauschen, wenn nur

$$(A, B, C) \text{ und } (A^1, B^1, C')$$

in dieselbe Klasse gehören.

Hievon soll sogleich Gebrauch gemacht werden indem wir die Gleichungen, welche die τ liefern, so wählen, dass der 1te Coeffizient prim zu n sei. Soll nun complexe Multiplication stattfinden, so müssen 2 Wurzeln der Modulargleichung gleich werden. Sei die eine

$$\varphi\left(\frac{t\tau - 16\xi}{t^1}\right)$$

und setzt man jetzt

$$\frac{t\tau - 16\xi}{t^1} = \omega$$

also

$$\tau = \frac{t'\omega + 16\xi}{t}$$

so geht $A\tau^2 + 2B\tau + C = 0$
über in

$$At'^2\omega^2 + 2(A\xi' + Bt) + \frac{A\xi'^2 + 2Bt\xi + Ct^2}{t'} = 0$$

die abermals eine complexe Multiplication — natürlich auch nten Grades liefert.

An die Stelle von ξ kann aber ebenso gut jede andere Wurzel der Congruenz

$$A\xi^2 + 2Bt\xi + Ct^2 \equiv 0 \bmod t'$$

treten, wie auch die ξ nur solche sein können, die dieser Congruenz genügen.

Dieselbe hat aber, wenn sie überhaupt möglich ist, da A und t' der Annahme nach relativ prim sind, 2λ Wurzeln, wo λ die Anzahl der in t' enthaltenen Primfactoren. Somit ist gezeigt worden, dass wenn die Modulargleichung über-

haupt gleiche Wurzeln zulässt, ihre Zahl nur eine Potenz von 2 sein kann.

Die Gleichung $g(u) = o$ hat aber zu Wurzeln sämmtliche Moduln der complexen Multiplication; jeder Factor ist mit einem Exponenten 2^{λ} versehen; $g(u)$ ist ein vollständiges Quadrat $h^2(u)$.

Für eine Primzahltransformation wird $h(u)$ dann nur verschiedene Wurzeln besitzen.

C. F. Winter'sche Buchdruckerei.