Ueber eine Verallgemeinerung der Kreistheilung.

Von

L. STICKELBERGER in Freiburg i. Br.

Unter den merkwürdigen Beziehungen zwischen Algebra und Zahlentheorie, welche Gauss in der siebenten Section der *Disquisitiones arithmeticae* aufgedeckt hat, findet sich schon eine solche zwischen einer Aufgabe der Kreistheilung und der Darstellung einer Zahl durch eine quadratische Form. In Artikel 358 ist für jede Primzahl $p = 3n + 1$ die Vertheilung der p ten Einheitswurzeln in drei Perioden, d. h. die algebraische Bestimmung dieser Perioden, abhängig gemacht von der Darstellung der Zahl $4p$ durch die Form $t^2 + 27u^2$. In der ersten Abhandlung über die biquadratischen Reste hat Gauss einen ähnlichen Zusammenhang zwischen der Darstellung einer Primzahl $p = 4n + 1$ durch die Form $x^2 + y^2$ und der Vertheilung der p ten Einheitswurzeln in vier Perioden nachgewiesen, und zugleich die Reste der ungeraden unter den darstellenden Zahlen nach den Moduln 4 und p bestimmt.

Bevor noch die genannte Gauss'sche Abhandlung selbst erschienen war, hat Jacobi auf Grund der Gauss'schen Anzeige vom Jahre 1825, in welcher auf die Kreistheilung ausdrücklich hingewiesen war, dessen Idee erfasst, wie aus der 1827 erschienenen Note: „*De residuis cubicis commentatio numerosa*“ hervorgeht. Dieser folgte 1832 die: „*Observatio arithmetica de numero classium divisorum quadraticorum formae $y^2 + Az^2$* “, in welcher auf die aus der Kreistheilung gewonnene Darstellung gewisser Primzahlpotenzen durch die genannte Form eine Vermuthung gegründet wird, die sich später so glänzend bestätigen sollte, und 1837 die Note: „*Ueber die Kreistheilung und ihre Anwendung auf die Zahlentheorie*“.

Inzwischen hatte auch Cauchy sich mit Anwendungen der Kreistheilung auf die Zahlentheorie beschäftigt, namentlich in dem 1830 der Académie des sciences vorgelegten, aber erst 1840 veröffentlichten: „*Mémoire sur la théorie des nombres*“; besonders ist hervorzuheben, dass Cauchy auch beliebig zusammengesetzte Determinanten behandelt.

Während es sich bis dahin immer nur um die Darstellung von Potenzen der Primzahlen $p = mx + 1$ durch die Hauptform der Determinante $-m$ handelte, trat 1848 Eisenstein mit einer Abhandlung hervor: „*Zur Theorie der quadratischen Zerfällungen der Primzahlen $8n + 3$, $7n + 2$, $7n + 4$* “, in der mittels, allgemeinerer Principien, welche einige Aehnlichkeit mit denen der Kreistheilung haben,“ ein von Herrn Stern durch Induction gefundener Satz über die Primzahlen $8n + 3$ bewiesen wird und analoge Sätze über die beiden andern im Titel genannten Arten von Primzahlen gewonnen werden. Im Jahre 1852 gab sodann Herr Kummer in einer Abhandlung: „*Ueber die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*“ eine Verallgemeinerung der Kreistheilung, welche sich auf die von Jacobi durch $\psi(\alpha)$ bezeichneten Zahlen bezieht.

Der vorliegenden Abhandlung, welche durch die für 1885 und 1888 ausgeschriebene Preisfrage der königlichen Gesellschaft der Wissenschaften zu Göttingen veranlasst ist, liegt eine Verallgemeinerung der Kreistheilungsresolvente zu Grunde, nämlich eine aus m ten und p ten Einheitswurzeln gebildete Zahl, welche ganz ähnliche Eigenschaften besitzt wie die gewöhnliche Resolvente; dabei bedeutet p eine Primzahl und m eine beliebig zusammengesetzte, aber durch p nicht theilbare Zahl. Zu diesen Resolventen stehen die Kummer'schen Zahlen Ψ in ähnlicher Beziehung, wie die Jacobi'schen ψ zu den gewöhnlichen Resolventen. Ferner zerlegen sich unsere Resolventen stets in zwei Factoren, deren einer entweder eine gewöhnliche Resolvente oder gleich $-p$ ist, während der andere nur von den m ten Einheitswurzeln abhängt und in gleicher Weise gebaut ist wie die besonderen von Eisenstein untersuchten Summen, weshalb wir denselben als Eisenstein'sche Summe bezeichnen.

Die Analogie der gewöhnlichen und der verallgemeinerten Resolventen bewährt sich auch bei der Zerlegung derselben in ihre idealen Factoren; wenn p für den Modul m zum Exponenten f gehört, so verhält sich die allgemeine Resolvente ähnlich wie ein Product von f gewöhnlichen Resolventen. Vollständiger wird die Analogie, wenn man eine beliebige „Gruppe“ von Resten nach dem Modul m betrachtet; sobald die Primzahl p dieser Gruppe angehört, kann man ein Product von Resolventen herstellen, dessen ideale Primfactoren von jenem Exponenten f gar nicht explicite abhängen, und das Gleiche gilt auch von dem Reste dieses Productes nach der niedrigsten Potenz eines idealen Primfactors von p , durch die das Product nicht theilbar ist.

Ist die Zahl m so beschaffen, dass $-m$ eine Fundamentaldeterminante quadratischer Formen ist, und besteht die Restgruppe aus denjenigen (ungeraden positiven) Zahlen, für die das Jacobi'sche

Zeichen $\left(\frac{-m}{k}\right)$ den Werth $+1$ hat, so werden unsere allgemeineren Producte wie die von Jacobi und Cauchy betrachteten zweiwerthig und geben daher die Darstellung einer gewissen Potenz von p durch die Hauptform jener Determinante; zugleich genügen die darstellenden Zahlen zwei linearen Congruenzen nach dem Modul p , von denen jedoch nur eine von der gewählten Wurzel der Congruenz $x^2 + m \equiv 0 \pmod{p}$ unabhängig ist. Da der Exponent jener Potenz gleich der Classenanzahl der quadratischen Formen ist, so ist die Analogie mit den Sätzen von Jacobi und Cauchy eine vollständige; zur wirklichen Herstellung der quadratischen Zerfällungen reichen freilich unsere Formeln so wenig aus wie die der genannten Mathematiker, sobald die Classenanzahl grösser als Eins ist.

Diese Resultate habe ich im Jahre 1888 der Gesellschaft der Wissenschaften vorgelegt in einer Abhandlung: „*Theorie der Eisenstein'schen Summen u. s. w.*“, von welcher die gegenwärtige eine Umarbeitung ist. In der neuen Fassung treten die Eisenstein'schen Summen mehr zurück als in der frühern, nachdem es mir seither gelungen ist, die Zerlegung der Resolventen in ihre idealen Primfactoren auf neuem Wege, nämlich ohne die Hilfe jener Summen, zu bewerkstelligen. Dieser neue Beweis findet sich in § 6; er umfasst zugleich den in § 5 gegebenen; wiewohl also § 5 an sich entbehrlich ist, mochte ich ihn nicht beseitigen, da er immerhin das Verständniss von § 6 nicht unwesentlich erleichtern dürfte. Auch sonst ist die Anordnung des zweiten Theils wesentlich geändert und § 4 beträchtlich verkürzt, während in § 1–3 nur untergeordnete redactionelle Aenderungen vorgenommen sind.

Die Theorie der idealen Zahlen ist in derjenigen Form benutzt, die ihr Herr Dedekind zuerst in der zweiten Auflage der Dirichlet'schen Vorlesungen über Zahlentheorie gegeben hat. Die wenigen speciell auf Kreistheilungskörper bezüglichen Sätze, welche hier gebraucht werden, finden sich in der dritten Auflage desselben Werkes in der Fussnote zu Seite 587 angegeben.

§ 1.

Restsysteme.

1. Sei Ω ein beliebiger endlicher Zahlkörper, $\mathfrak{o}$ die Gesamtheit der ganzen Zahlen in Ω , und $\mathfrak{p}$ ein solches Ideal in $\mathfrak{o}$, welches in der rationalen Primzahl p aufgeht; eine übersichtliche Darstellung aller nach dem Modul $\mathfrak{p}$ incongruenten Zahlen von $\mathfrak{o}$ erhalten wir dann in folgender Weise. Ist ω_1 irgend eine durch $\mathfrak{p}$ nicht theilbare Zahl, und durchläuft x_1 p ganze rationale nach p incongruente Werthe, so

stellt $x_1 \omega_1$ p Zahlen dar, die nach p incongruent sind. Ist ω_2 keiner von diesen congruent, und durchläuft auch x_2 ein gewöhnliches Restsystem (mod. p), so nimmt $x_1 \omega_1 + x_2 \omega_2$ p^2 Werthe an, die nach p incongruent sind. Durch Fortsetzung dieses Verfahrens erhält man schliesslich f Zahlen $\omega_1, \omega_2, \dots, \omega_f$ von der Art, dass

$$(1) \quad \omega = x_1 \omega_1 + x_2 \omega_2 + \dots + x_f \omega_f$$

p^f incongruente Zahlen liefert, wenn $x_1, x_2, \dots, x_f$ die Zahlen $0, 1, \dots, p-1$ durchlaufen, und dass jede Zahl in $\mathfrak{o}$ einer von diesen p^f Zahlen congruent ist nach p . Wir nennen f den Grad des Ideals $\mathfrak{p}$. Solche f Zahlen kann man namentlich unter den Zahlen jedes Fundamentalsystems von $\mathfrak{o}$ finden; die übrigen $n - f$ Basiszahlen kann man dann um Zahlen der Form (1) so vermehren, dass sie durch p theilbar werden.

Die einzige Bedingung, der die Zahlen $\omega_1, \dots, \omega_f$ zu genügen haben, wenn f als bekannt angesehen wird, ist die, dass sie *unabhängig* seien nach dem Modul p . Wir nennen nämlich irgendwelche g Zahlen $\omega_1, \dots, \omega_g$ unabhängig (mod. p), wenn kein Aggregat der Form $x_1 \omega_1 + \dots + x_g \omega_g$ durch p theilbar ist, ohne dass die einzelnen Zahlen $x_1, \dots, x_g$ durch p theilbar sind. Ein einfaches Kriterium der Unabhängigkeit lässt sich für den Fall angeben, wo p ein *Primideal* ist, was wir von jetzt an voraussetzen.

2. Sind nämlich zunächst $\omega_1, \dots, \omega_g$ von einander abhängig, besteht also eine Congruenz

$$x_1 \omega_1 + x_2 \omega_2 + \dots + x_g \omega_g \equiv 0 \pmod{p},$$

in welcher die ganzen rationalen Zahlen x nicht alle durch p theilbar sind, so ergeben sich durch Potenzirung die weiteren Congruenzen

$$x_1 \omega_1^{(1)} + x_2 \omega_2^{(1)} + \dots + x_g \omega_g^{(1)} \equiv 0,$$

$$x_1 \omega_1^{(2)} + x_2 \omega_2^{(2)} + \dots + x_g \omega_g^{(2)} \equiv 0,$$

$$\dots \dots \dots \dots \dots \dots \dots \dots \dots$$

wobei zur Abkürzung

$$(2) \quad \omega^{(h)} = \omega^{p^h}$$

gesetzt ist. Daher muss die Determinante

$$(3) \quad \begin{vmatrix} \omega_1 & \omega_2 & \dots & \omega_g \\ \omega_1^{(1)} & \omega_2^{(1)} & \dots & \omega_g^{(1)} \\ \dots & \dots & \dots & \dots \\ \omega_1^{(g-1)} & \omega_2^{(g-1)} & \dots & \omega_g^{(g-1)} \end{vmatrix}$$

durch p theilbar sein. Um nun zu beweisen, dass diese Bedingung auch hinreicht, nehmen wir $g \leq f$ an, da überhaupt nicht mehr als f unabhängige Zahlen existiren; wir setzen ferner voraus, dass die analoge

Determinante aus den Zahlen $\omega_1, \dots, \omega_{g-1}$ durch $\mathfrak{p}$ nicht theilbar sei, da wir andernfalls auf diese die folgenden Schlüsse anwenden könnten. Dann sind aber $\omega_1, \dots, \omega_{g-1}$ sicher unabhängig, und die Determinante, welche aus (3) hervorgeht, wenn man ω_g durch eine willkürliche Zahl ω von $\mathfrak{p}$ ersetzt, ist in Bezug auf ω wirklich vom Grade p^{g-1} . Diese Determinante wird durch $\mathfrak{p}$ theilbar einerseits für

$$\omega \equiv x_1 \omega_1 + \dots + x_{g-1} \omega_{g-1},$$

andererseits für

$$\omega \equiv \omega_g;$$

da aber der Modul $\mathfrak{p}$ als Primideal vorausgesetzt ist, können nicht alle diese $p^{g-1} + 1$ Zahlen incongruent sein, vielmehr ist ω_g congruent einer der übrigen p^{g-1} Zahlen. Wir haben also den Satz gewonnen:

I. Für ein Primideal $\mathfrak{p}$ als Modul sind g Zahlen $\omega_1, \omega_2, \dots, \omega_g$ abhängig oder unabhängig, je nachdem die Determinante (3) durch $\mathfrak{p}$ theilbar ist oder nicht.

Für den Fall $g=f$ ist diese Bedingung von Herrn Hensel abgeleitet in § 2 der Abhandlung: „Untersuchung der ganzen algebraischen Zahlen eines Gattungsbereiches u. s. w.“^{*)}. Aus dem Obigen folgt auch:

Sind $\omega_1, \dots, \omega_g$ unabhängig, so sind die p^g Zahlen $x_1 \omega_1 + \dots + x_g \omega_g$ die Wurzeln der Congruenz

$$(4) \quad \begin{vmatrix} \omega & \omega_1 & \dots & \omega_g \\ \omega^{(1)} & \omega_1^{(1)} & \dots & \omega_g^{(1)} \\ \dots & \dots & \dots & \dots \\ \omega^{(g)} & \omega_1^{(g)} & \dots & \omega_g^{(g)} \end{vmatrix} \equiv 0 \pmod{\mathfrak{p}}.$$

3. Die p^g Zahlen $x_1 \omega_1 + \dots + x_g \omega_g$ haben die Eigenschaft, sich durch Addition zu reproduciren. Für $g=f$ reproduciren sie sich $(\text{mod. } \mathfrak{p})$ auch durch Multiplication. Soll für einen kleineren Werth von g den p^g Zahlen auch diese Eigenschaft zukommen, so müssen zufolge bekannter Schlüsse die $p^g - 1$ Zahlen, die nach Ausscheidung der Null übrig bleiben, Wurzeln der binomischen Congruenz

$$\omega^{p^g-1} \equiv 1 \pmod{\mathfrak{p}}$$

sein. Diese Congruenz hat aber dann und nur dann die verlangte Anzahl von Wurzeln, wenn $p^g - 1$ ein Theiler von $p^f - 1$ und mithin auch g ein Theiler von f ist.

II. Ein System von p^g Zahlen, welche sich durch Addition und Multiplication reproduciren nach dem Modul $\mathfrak{p}$, besteht aus den Wurzeln der Congruenz

$$(5) \quad \varrho^{p^g} \equiv \varrho \pmod{\mathfrak{p}},$$

in welcher g irgend einen Divisor von f , dem Grade des Primideals $\mathfrak{p}$, bezeichnet.

^{*)} Journal f. r. u. a. Math. Bd. 101.

Ist der Divisor g beliebig gewählt, und bedeuten $\varrho_1, \varrho_2, \dots$ Wurzeln der Congruenz (5), so kann man den Begriff der Unabhängigkeit so abändern, dass man h Zahlen $\omega_1, \dots, \omega_h$ abhängig oder unabhängig nennt, je nachdem zwischen ihnen eine Relation der Form

$$\varrho_1 \omega_1 + \varrho_2 \omega_2 + \dots + \varrho_h \omega_h \equiv 0 \pmod{p}$$

besteht oder nicht. In diesem Sinne unabhängige Zahlen giebt es genau $\frac{f}{g}$; auch gewinnt man leicht eine Bedingung der Unabhängigkeit, welche der früheren ganz analog ist.

4. Seien wieder in dem ursprünglichen Sinne $\omega_1, \dots, \omega_f$ unabhängig $\pmod{p}$, sodass die Congruenz

$$(6) \quad \omega \equiv x_1 \omega_1 + \dots + x_f \omega_f \pmod{p}$$

für eine beliebig gegebene Zahl ω von $\mathfrak{o}$ durch ganze rationale Zahlen $x_1, \dots, x_f$ befriedigt wird; diese Zahlen, die Coordinaten von ω in Bezug auf den Modul p und die Basis $\omega_1, \dots, \omega_f$, sind nach dem Modul p bestimmt, sobald $\omega \pmod{p}$ gegeben ist; da sie rational sind, genügt es aber, sie $\pmod{p}$ zu bestimmen. Eine solche Bestimmung gewinnt man leicht, wenn man die Congruenz (6) $f-1$ Mal auf die p te Potenz erhebt; denn dadurch erhält man f lineare Congruenzen, deren Determinante nach Satz I durch p nicht theilbar ist. Daher werden $x_1, \dots, x_f$ linearen homogenen Functionen von $\omega, \omega^{(1)}, \dots, \omega^{(f-1)}$ congruent $\pmod{p}$, wenn wir uns wieder der Bezeichnung (2) bedienen.

Allgemeiner kann man, wenn $\beta_1, \dots, \beta_f$ beliebige Zahlen von $\mathfrak{o}$ bedeuten, die lineare Function $\beta_1 x_1 + \dots + \beta_f x_f$ in die Form

$$(7) \quad \Phi(\omega) \equiv \alpha_0 \omega + \alpha_1 \omega^{(1)} + \dots + \alpha_{f-1} \omega^{(f-1)} \pmod{p}$$

bringen; das Umgekehrte ergibt sich unmittelbar. Beide Ausdrücke, die also von gleicher Allgemeinheit sind, kann man betrachten als Darstellungen einer Function $\Phi(\omega)$, deren Werthe dem Gebiete $\mathfrak{o}$ angehören und zugleich mit ω nach dem Modul p bestimmt sind, und die ausserdem die Congruenz

$$(8) \quad \Phi(\omega + \omega') \equiv \Phi(\omega) + \Phi(\omega') \pmod{p}$$

befriedigt. Denn aus diesen Bedingungen folgt in bekannter Weise

$$\Phi(x_1 \omega_1 + \dots + x_f \omega_f) \equiv x_1 \Phi(\omega_1) + \dots + x_f \Phi(\omega_f) \pmod{p}.$$

Giebt man speciell den Zahlen $\Phi(\omega_1), \dots, \Phi(\omega_f)$ ganze rationale Werthe, so ist allgemein

$$\Phi(\omega)^p \equiv \Phi(\omega) \pmod{p};$$

stellt man aber $\Phi(\omega)$ in der Form (7) dar, so zerfällt diese Congruenz in f einzelne:

$$\alpha_1 \equiv \alpha_0^p, \alpha_2 \equiv \alpha_1^p, \dots, \alpha_0 \equiv \alpha_{f-1}^p \pmod{p},$$

und diese ergeben

$$\alpha_1 \equiv \alpha_0^p, \alpha_2 \equiv \alpha_0^{p^2}, \dots, \alpha_{f-1} \equiv \alpha_0^{p^{f-1}} \pmod{p},$$

(9) $\omega + \omega^p + \dots + \omega^{p^{f-1}}$
congruent sind Modulo $\mathfrak{p}$, so wird vermöge dieser Nebenbedingung

$$\omega + \omega^p + \dots + \omega^{p^{f-1}}$$

congruent sind Modulo $\mathfrak{p}$, so wird vermöge dieser Nebenbedingung

$$\Phi(\omega) \equiv S(\alpha\omega) \pmod{p}.$$

$$\Phi(\omega + \omega') \equiv \Phi(\omega) + \Phi(\omega') \pmod{p}$$

Diese Zahl α ist (mod. p) bestimmt, sobald Φ gegeben ist, sie vertritt die f rationalen Zahlen $\Phi(\omega_1), \dots, \Phi(\omega_f)$. Setzt man der Reihe nach $\Phi(\omega)$ congruent $x_1, x_2, \dots, x_f$, so erhält man f specielle Werthe von α , die wir durch $\eta_1, \eta_2, \dots, \eta_f$ bezeichnen. Die Congruenz

$$x_i \equiv S(\eta_i \omega) \equiv S(\eta_i(x_1 \omega_1 + \dots + x_r \omega_r)) \pmod{p}$$

zerlegt sich in die folgenden:

$$(10) \quad \left. \begin{aligned} S(\eta_i \omega_i) &\equiv 1 \\ S(\eta_i \omega_k) &\equiv 0 \end{aligned} \right\} \pmod{p},$$

$$\left. \begin{aligned} \eta_1 \omega_1 + \dots + \eta_f \omega_f &\equiv 1 \\ \eta_1 \omega_1^p + \dots + \eta_f \omega_f^p &\equiv 0 \\ \vdots & \\ \eta_1 \omega_1^{f-1} + \dots + \eta_f \omega_f^{f-1} &\equiv 0 \end{aligned} \right\} (\text{mod. } p).$$

*) Abhandl. der k. Ges. d. W. zu Göttingen, Bd. 29 (1882).

5. Die Function $S(\omega)$ kann nach Definition nur einer der Zahlen $0, 1, \dots, p - 1$ congruent sein nach dem Modul p oder $\mathfrak{p}$; da sie nach dem letzteren einer ganzen Function p^{f-1} ten Grades von ω congruent ist, so kann sie denselben Werth höchstens für p^{f-1} incongruente Werthe von ω annehmen. Lässt man daher ω ein volles Restsystem nach dem Modul $\mathfrak{p}$ durchlaufen, so muss $S(\omega)$ jeden jener p Werthe, und jeden p^{f-1} Mal annehmen.

IV. *Durchläuft ω ein vollständiges Restsystem nach dem Primideal f ten Grades $\mathfrak{p}$ als Modul, so nimmt die Function $S(\omega)$ jeden der Werthe $0, 1, \dots, p - 1$ genau p^{f-1} Mal an.*

Bringt man die Congruenz

$$S(\omega) \equiv S(\omega^p) \pmod{\mathfrak{p}},$$

auf welcher der letzte Schluss beruht, in die Form

$$S(\omega - \omega^p) \equiv 0 \pmod{\mathfrak{p}},$$

so ist in gleicher Weise zu schliessen, dass man jede der p^{f-1} Wurzeln der Congruenz $S(\tau) \equiv 0 \pmod{\mathfrak{p}}$ p Mal erhält, wenn man $\tau \equiv \omega - \omega^p$ setzt und ω ein vollständiges Restsystem durchlaufen lässt.

Ähnlich wie den Satz IV erhält man den allgemeineren Satz:

V. *Bezeichnet g einen Divisor von f , und lässt man ω ein volles Restsystem nach dem Modul $\mathfrak{p}$ durchlaufen, so wird der Ausdruck*

$$\omega + \omega^{p^g} + \omega^{p^{2g}} + \dots + \omega^{p^{f-g}}$$

je p^{f-g} Mal congruent jeder der p^g Wurzeln der Congruenz

$$\varrho^{p^g} \equiv \varrho \pmod{\mathfrak{p}}.$$

Auch diesem Satze steht ein zweiter zur Seite in ähnlicher Weise wie dem Satze IV. Die hier angewandten Principien führen auch leicht zu einem viel allgemeineren Satze, den wir aber übergehen.

§ 2.

Restcharaktere.

1. Sei, wie in § 1, $\mathfrak{p}$ ein Primideal f ten Grades in dem endlichen Körper Ω , und seien m, n zwei complementäre Divisoren von $p^f - 1$, also

$$(1) \quad p^f - 1 = mn.$$

Da die Congruenz $\omega^{mn} \equiv 1 \pmod{\mathfrak{p}}$ mn Wurzeln besitzt, so schliesst man in bekannter Weise, dass ω^n , wenn ω jene mn Werthe durchläuft, nur m incongruente Werthe annimmt, nämlich die Wurzeln der Congruenz

$$(2) \quad \tau^m \equiv 1 \pmod{\mathfrak{p}},$$

aber jeden dieser Werthe n Mal. Demnach können die Zahlen ω classificirt werden nach den Resten von ω^n ; jede der m Classen enthält n Zahlen, und eine der Classen, für welche nämlich $\omega^n \equiv 1$ ist, besteht aus den m ten Potenzresten.

Enthält der Körper Ω eine primitive m te Einheitswurzel Θ , so sind die Wurzeln von (2) die Potenzen von Θ ; in der That sind diese incongruent, da ihre Differenzen Divisoren von m sind. Wir bezeichnen nun durch $[\omega]$ diejenige Potenz von Θ , welche der Potenz ω^n congruent ist; die charakteristischen Eigenschaften dieses Symbols sind also

$$(3) \quad [\omega]^m = 1,$$

$$(4) \quad [\omega] \equiv \omega^n \pmod{p}.$$

Demnach ist stets

$$(5) \quad [1] = 1,$$

$$(6) \quad [\Theta] = \Theta^n,$$

und ferner, wenn die Primzahl p ungerade ist,

$$(7) \quad [-1] = (-1)^n;$$

Denn unter dieser Voraussetzung ist mindestens eine der Zahlen m, n gerade. Für $p = 2$ dagegen ist $[-1] = 1$. Weiter ist

$$(8) \quad [\omega] = [\omega_1] \quad \text{für} \quad \omega \equiv \omega_1 \pmod{p},$$

und allgemein

$$(9) \quad [\omega \omega_1] = [\omega] [\omega_1].$$

Das Symbol $[\omega]$ gehört daher zu den „Charakteren“ der durch die $p^n - 1$ Zahlclassen nach dem Modul p gebildeten Abel'schen Gruppe. Die Gesamtzahl dieser Charaktere ist nach Herrn Weber*) gleich $p^n - 1$; wir haben es aber hier nur mit den Potenzen eines derselben, nämlich mit $[\omega]^n$, zu thun. Diese m Charaktere bilden eine Untergruppe und zwar die einzige Untergruppe der Ordnung m , weil die ganze Gruppe aus den Potenzen eines einzigen primitiven Charakters besteht. Aus dem nämlichen Grunde sind diese Charaktere die einzigen dem Körper Ω angehörenden, wenn dieser keine höheren als die m ten Einheitswurzeln enthält.

Da die Zahl Θ nach dem Modul p zum Exponenten m gehört, so kann man nach dem von Gauss**) gelehrten Verfahren eine primitive Wurzel der Congruenz

$$\omega^{p^n-1} \equiv 1 \pmod{p}$$

so bestimmen, dass zugleich $\omega^n \equiv \Theta$ ist. Sei γ eine solche primitive Wurzel, also

*) Mathem. Ann. Bd. 20, S. 307.

**) Disq. arithm. art. 71.

$$(10) \quad \gamma^n \equiv \Theta \pmod{p}, \quad [\gamma] = \Theta.$$

Setzt man dann

$$\omega \equiv \gamma^{\text{Ind } \omega} \pmod{p},$$

so wird

$$\omega^n \equiv \gamma^{n \text{Ind } \omega} \equiv \Theta^{\text{Ind } \omega},$$

und folglich

$$(11) \quad [\omega] = \Theta^{\text{Ind } \omega}.$$

Da $[\omega]$ jeden der Werthe $1, \Theta, \dots, \Theta^{m-1}$ n Mal annimmt, falls ω ein Restsystem durchläuft, so ist

$$\sum [\omega]^a = n(1 + \Theta^a + \Theta^{2a} + \dots + \Theta^{(m-1)a}),$$

also gleich $p^f - 1$ oder 0 , je nachdem a durch m theilbar ist oder nicht.

2. Wir untersuchen jetzt speciell die Charaktere derjenigen $p^g - 1$ Zahlen ϱ , welche die Congruenz

$$(12) \quad \varrho^{p^g - 1} \equiv 1 \pmod{p}$$

befriedigen, in welcher wieder g einen ganzen rationalen Theiler von f bedeuten soll. Ist

$$\varrho_2 \equiv \varrho \varrho_1 \pmod{p},$$

so ist jede der Gleichungen

$$[\varrho_2]^a = [\varrho_1]^a, \quad [\varrho]^a = 1$$

eine Folge der andern; daher nimmt $[\varrho]^a$ alle überhaupt vorkommenden Werthe ebenso oft an wie den speciellen Werth 1 . Soll aber $[\varrho]^a = 1$ sein, so ist ϱ eine gemeinsame Wurzel der Congruenzen $\varrho^{an} \equiv 1$ und (12). Bezeichnet man also durch d den grössten gemeinsamen Theiler von an und $p^g - 1$, so wird $[\varrho]^a$ jeden seiner verschiedenen Werthe d Mal annehmen, und die

$$\frac{p^g - 1}{d} = e$$

verschiedenen Werthe werden die e ten Wurzeln der Einheit sein, weil $an \cdot e$ durch $p^g - 1$ theilbar und somit

$$([\varrho]^a)^e \equiv \varrho^{an \cdot e} \equiv 1 \pmod{p}$$

ist. Bequemer lässt sich das Ergebniss ausdrücken, wenn man den Bruch

$$(13) \quad \frac{an}{p^g - 1} = \frac{a}{m} \frac{p^f - 1}{p^g - 1} = \frac{a(1 + p^g + \dots + p^{f-g})}{m}$$

einführt; der wahre Nenner dieses Bruches, d. h. der Nenner des ihm gleichen reducirten Bruches, ist nämlich gleich e .

Ist e der wahre Nenner des Bruches (13), dann sind die Charaktere $[\varrho]^a$ aller Wurzeln der Congruenz (12) e te Einheitswurzeln, und zwar

tritt jede dieser Einheitswurzeln gleich oft auf. Daher ist auch $\sum [\epsilon]^a$ gleich $p^g - 1$ oder 0, je nachdem a durch $p^g - 1$ theilbar ist oder nicht.

Zu demselben Resultat führt die Gleichung (11). Die Potenz

$$\gamma^{1+p^g+\dots+p^{f-g}}$$

ist nämlich eine primitive Wurzel der Congruenz (12), und ihr Charakter hat den Werth

$$\Theta^{1+p^g+\dots+p^{f-g}}.$$

Für $g = 1$ lautet der vorige Satz:

Durchläuft z die rationalen Zahlen $1, 2, \dots, p-1$, so wird der Charakter $[z]^a$ nur dann beständig gleich 1, wenn a durch $p-1$, d. h. $a(1+p+p^2+\dots+p^{f-1})$ durch m theilbar ist; in diesem Falle ist $\sum [z]^a = p-1$, in jedem andern Falle hat die Summe den Werth Null.

Sei z. B. $m = 8$, $p \equiv 3 \pmod{8}$, $f = 2$, $g = 1$. Dann ist $\frac{n}{p-1} = \frac{p+1}{8}$, also $e = 2$ bei ungeradem, $e = 1$ bei geradem a . Dabei ist

$$[z] \equiv z^{\frac{p-1}{2} \frac{p+1}{4}} \equiv z^{\frac{p-1}{2}} \pmod{p}$$

d. h. der Charakter $[z]$ stimmt überein mit dem Legendre'schen Zeichen.

Ist dagegen $m = 7$, p congruent 2 oder 4 (mod. 7), $f = 3$, $g = 1$, so ist $p-1$ prim zu m , und daher n durch $p-1$ theilbar; somit ist hier für jeden Werth von a $e = 1$, $[z] = 1$.

Diese beiden Specialfälle sind von Eisenstein in § 1 und 7 der zu Anfang erwähnten Abhandlung betrachtet.

Allgemein sei noch erwähnt, dass e für jeden Werth von a gleich 1 ist, wenn $p^g - 1$ zu m theilerfremd ist.

§ 3.

Resolventen und Eisenstein'sche Summen.

1. Ist p eine Primzahl, m ein Theiler von $p-1$, sind Θ , ξ respective primitive m te und p te Einheitswurzeln, dann stellt der Ausdruck

$$\sum_{i=1}^{p-1} \Theta^{a \text{Ind}_p \xi^i} = F(\Theta^a, \xi)$$

die sogenannte Kreistheilungsresolvente dar, deren wichtigste Eigenschaften durch Jacobi, Cauchy und namentlich durch Herrn Kummer festgestellt worden sind; die hier gewählte Schreibweise ist besonders

von Eisenstein*) benutzt worden. Wegen der Eigenschaften der Indices ist $\Theta^{\text{Ind}z}$ einer der Charaktere, welche der Gruppe der Zahlclassen nach dem Modul p entsprechen, und wir können denselben leicht unter die in § 2 behandelten einreihen. In dem Körper, welcher aus Θ durch die rationalen Operationen entspringt — im Rationalitätsbereiche (Θ) nach der Terminologie des Herrn Kronecker — zerfällt nach der Kummer'schen Theorie die Primzahl p in $\varphi(m)$ ideale Factoren, wobei $\varphi(m)$ die Euler'sche zahlentheoretische Function bedeutet; für einen und nur für einen dieser Factoren ist, wenn $\frac{p-1}{m} = n$ gesetzt wird, die n te Potenz der primitiven Congruenzwurzel, auf welche sich die Indices beziehen, congruent Θ , und daher auch allgemein $z^n \equiv \Theta^{\text{Ind}z}$. Deshalb bezeichnet auch schon Cauchy zu Anfang seines Mémoire sur la theorie des nombres**) $\Theta^{\text{Ind}z}$ durch das Zeichen $\left[\frac{z}{p}\right]$; genauer wäre die Bezeichnung $\left[\frac{z}{p}\right]$. Die Eigenschaften des andern Factors ξ^z , welche beim Beweise der Haupteigenschaften der Resolvente gebraucht werden, sind

$$\xi^y \cdot \xi^z = \xi^{y+z}, \quad \xi^p = 1.$$

2. Von jetzt ab sei m nicht mehr ein Divisor von $p-1$, sondern erst von p^f-1 , sodass p nach dem Modul m zum Exponenten f gehört; wir setzen, wie in § 1:

$$(1) \quad p^f - 1 = mn.$$

Bezeichnet wiederum Θ eine primitive m te Wurzel der Einheit, so zerfällt in dem durch Θ bestimmten Körper die Zahl p (oder das Hauptideal $\wp p$) in $\frac{\varphi(m)}{f}$ verschiedene Primideale, welche sämmtlich conjugirt und vom Grade f sind. Unter diesen greifen wir irgend eines heraus, das wir durch $\wp$ bezeichnen. Als f unabhängige Zahlen bieten sich zunächst die Potenzen $1, \Theta, \Theta^2, \dots, \Theta^{f-1}$ dar; in speciellen Fällen kann es vortheilhaft sein, eine andere Wahl zu treffen.

Um nun die Kreistheilungsresolvente zu verallgemeinern, ersetzen wir den ersten Factor ihres allgemeinen Gliedes durch den in § 2 definirten Restcharakter $[\omega]^a$, indem wir zugleich ω ein vollständiges Restsystem mit Ausschluss der Null durchlaufen lassen. Der zweite Factor ξ^z aber ist zu ersetzen durch eine Function $\Psi(\omega)$, welche ungeändert bleibt, wenn ω durch eine nach $\wp$ congruente Zahl ersetzt wird, und welche ausserdem der Gleichung $\Psi(\omega) \Psi(\omega_1) = \Psi(\omega + \omega_1)$ genügt. Aus der vorigen Gleichung folgt aber $\Psi(\omega)^z = \Psi(z\omega)$, und

*) Allgem. Untersuchungen üb. d. F. dritten Grades u. s. w., Journal f. Math. Bd. 28, S. 289.

**) Mémoires de l'Acad. d. sc., t. 17 (1840).

speciell mit Rücksicht auf die erste Eigenschaft $\Psi(\omega)^p = 1$. Wir führen daher eine primitive p te Einheitswurzel ξ ein und setzen

$$\Psi(\omega) = \xi^{\Phi(\omega)};$$

dann ist zu fordern, dass $\Phi(\omega)$ stets ganz und rational sei, ferner bestimmt nach p , sobald ω nach p als Modul bestimmt ist, und ausserdem, dass

$$\Phi(\omega) + \Phi(\omega_1) \equiv \Phi(\omega + \omega_1) \pmod{p}$$

sei. Die allgemeinste derartige Function ist aber nach Satz III, § 1

$$\Phi(\omega) \equiv S(\alpha \omega).$$

3. Wir lassen zunächst α beliebig und bilden die Summe

$$(2) \quad F_\alpha(\Theta^\alpha, \xi) = \sum [\omega]^\alpha \xi^{S(\alpha \omega)},$$

in welcher ω ein vollständiges Restsystem nach dem Modul p mit Ausschluss der Null durchläuft; diese Summe bezeichnen wir als *verallgemeinerte Resolvente*, oft auch kurzweg als *Resolvente*. Sie ist der Werth, welchen die Summe $\sum t^{\text{ind } \omega} \xi^{S(\alpha \omega)}$ für $t = \Theta^\alpha$ annimmt; da aber Θ^α jede Wurzel der Gleichung $t^m = 1$ sein kann, so wollen wir unter $F_\alpha(t, \xi)$ den Rest der zuletzt angegebenen Summe nach dem Modul $t^m - 1$ verstehen, also eine ganze Function vom Grade $m - 1$, deren Coefficienten ganze ganzzahlige Functionen von ξ sind. Die *Coefficienten* dieser Function sind dann völlig bestimmt durch die *Werthe*, welche sie für $t = 1, \Theta, \dots, \Theta^{m-1}$ annimmt; aus diesem Grunde ist es auch vortheilhaft, von vornherein keinen Werth von α auszuschliessen, wiewohl namentlich der Werth $\alpha = 0$ vielfach einen Ausnahmefall bildet.

Für $\alpha \equiv 0 \pmod{p}$ erhält man

$$F_0(\Theta^\alpha, \xi) = \sum [\omega]^\alpha,$$

also gleich $p^f - 1$ oder 0, je nachdem α durch m theilbar ist oder nicht.

Ist dagegen α durch p nicht theilbar, so durchläuft $\omega_1 \equiv \alpha \omega$ zugleich mit ω ein volles Restsystem; da hierbei $[\omega_1] = [\alpha][\omega]$ ist, so ergibt sich

$$(3) \quad F_\alpha(\Theta^\alpha, \xi) = [\alpha]^{-\alpha} F_1(\Theta^\alpha, \xi).$$

Im Allgemeinen reicht es also aus, die besondere Function F_1 zu betrachten; wir schreiben deshalb zur Vereinfachung

$$(4) \quad F(\Theta^\alpha, \xi) = F_1(\Theta^\alpha, \xi) = \sum [\omega]^\alpha \xi^{S(\omega)}.$$

Als besonderer Fall der Gleichung (3) stellt sich die folgende dar, in welcher α eine durch p nicht theilbare ganze rationale Zahl bezeichnet:

$$(5) \quad F(\Theta^a, \xi) = [\xi]^{-a} F(\Theta^a, \xi);$$

nach § 2 folgt hieraus, dass die e^{te} Potenz von $F(\Theta^a, \xi)$ von ξ frei ist, wenn e den wahren Nenner des Bruches $\frac{a n}{p-1}$ bedeutet.

Setzt man weiter $\omega_1 \equiv \omega^p$, so durchläuft wiederum ω_1 zugleich mit ω ein vollständiges Restsystem nach p ; da

$$[\omega]^p = [\omega_1], \quad S(\omega) \equiv S(\omega_1) \pmod{p}$$

ist, so wird

$$(6) \quad F(\Theta^a, \xi) = F(\Theta^{ap}, \xi).$$

Weniger einfach gestaltet sich die Beziehung zwischen $F_\alpha(\Theta^a, \xi)$ und $F_\alpha(\Theta^{ap}, \xi)$, wenn α beliebig ist.

4. Wir gehen zur Untersuchung des Productes

$$F(\Theta^a, \xi) F(\Theta^b, \xi) = \sum_{\omega} \sum_{\omega_1} [\omega]^a [\omega_1]^b \xi^{S(\omega + \omega_1)}$$

über, und zwar ordnen wir die Glieder der Doppelsumme nach den Potenzen von ξ . Die Glieder, für welche $\omega + \omega_1$ durch p theilbar ist, liefern den Beitrag

$$[-1]^a \sum [\omega]^{a+b}.$$

Für die übrigen Glieder setzen wir

$$\left. \begin{aligned} \sigma &\equiv \omega + \omega_1 \\ \omega &\equiv \sigma \tau, \quad \omega_1 \equiv \sigma(1-\tau) \end{aligned} \right\} \pmod{p};$$

den $(p^f - 1)(p^f - 2)$ Werthepaaren ω, ω_1 , für die weder ω noch ω_1 noch $\omega + \omega_1$ durch p theilbar ist, entsprechen eindeutig die Combinationen von $p^f - 1$ Werthen von σ mit $p^f - 2$ Werthen von τ , indem τ keinen der Werthe 0, 1 annehmen darf. Durch diese Substitution wird aber

$$[\omega]^a [\omega_1]^b \xi^{S(\omega + \omega_1)} = [\tau]^a [1-\tau]^b \cdot [\sigma]^{a+b} \xi^{S(\sigma)}.$$

Im Ganzen erhält man also

$$(7) \quad F(\Theta^a, \xi) F(\Theta^b, \xi) = [-1]^a \sum [\omega]^{a+b} + \Psi_{a,b}(\Theta) F(\Theta^{a+b}, \xi),$$

wenn man zur Abkürzung

$$(8) \quad \Psi_{a,b}(\Theta) = \sum [\tau]^a [1-\tau]^b$$

setzt. Allgemein soll unter $\Psi_{a,b}(t)$ diejenige ganze Function $(m-1)$ ten Grades von t verstanden werden, welche nach dem Modul $t^m - 1$ der Summe

$$\sum t^{a \text{ Ind } \tau + b \text{ Ind } (1-\tau)}$$

congruent ist. Alsdann ist

$$\Psi_{a,b}(t^k) \equiv \Psi_{ak,bk}(t)$$

nach $t^m - 1$; ferner bleibt Ψ ungeändert, wenn man a, b um Vielfache von m ändert.

Die wichtigeren Fälle der Gleichung (7) sind folgende.

a) Wenn $a + b$ durch m nicht theilbar ist, so wird

$$(7a) \quad F(\Theta^a, \xi) F(\Theta^b, \xi) = \Psi_{a,b}(\Theta) F(\Theta^{a+b}, \xi);$$

denn unter dieser Annahme ist

$$\sum [\omega]^{a+b} = 0.$$

b) Wenn a durch m nicht theilbar ist, so ist

$$(7b) \quad F(\Theta^a, \xi) F(\Theta^{-a}, \xi) = [-1]^a p^f.$$

Denn zunächst ist

$$\sum [\omega]^0 = p^f - 1 \quad \text{und} \quad F(\Theta^0, \xi) = -1.$$

Ausserdem aber geht $\Psi_{a,b}(\Theta)$, wenn man $\tau \equiv (1 - \tau)\tau_1$ setzt, wobei τ_1 ein volles Restsystem mit Ausschluss der Zahlen 0 und -1 durchläuft, über in

$$\sum [\tau_1]^a = \sum [\omega]^a - [-1]^a = -[-1]^a,$$

und somit die rechte Seite der Gleichung (7) in $[-1]^a (p^f - 1 + 1)$, w. z. b. w. Die Gleichung (7b) kann man zufolge (5) auch in die Form setzen

$$(7c) \quad F(\Theta^a, \xi) F(\Theta^{-a}, \xi^{-1}) = p^f,$$

in welcher die beiden Factoren der linken Seite conjugirt imaginär sind.

5. Die complexen Zahlen $\Psi_{a,b}$ sind von Herrn Kummer als Verallgemeinerung der in der Kreistheilung auftretenden $\psi(\Theta)$ eingeführt und in ihre idealen Primfactoren zerlegt in § 2 der Abhandlung „Ueber die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen“^{*)}. Man kann sie in sechs im Allgemeinen verschiedenen Formen darstellen mittelst der Substitutionen $\tau \equiv 1 - \tau_1$, $\tau \equiv \frac{1}{\tau_1}$. Setzt man nämlich

$$(9) \quad a + b + c \equiv 0 \pmod{m},$$

so erhält man die Gleichungen

$$(10) \quad \Psi_{a,b} = \Psi_{b,a},$$

$$(11) \quad [-1]^a \Psi_{b,c} = [-1]^b \Psi_{c,a} = [-1]^c \Psi_{a,b},$$

von denen im Grunde schon vorhin unter b) Gebrauch gemacht ist. Bei Herrn Kummer a. a. O. fehlen die Vorzeichen, weil m und p ungerade sind, sodass n gerade und $[-1] = +1$ ist; das Nämliche gilt übrigens auch für $p = 2$.

^{*)} Journal f. r. u. a. Mathem. 44, S. 106—121.

Sehr leicht ergeben sich die Gleichungen

$$(12) \quad \Psi_{a,b}(\Theta) = \Psi_{a,b}(\Theta^p),$$

$$(13) \quad \Psi_{a,b}(\Theta) \Psi_{a,b}(\Theta^{-1}) = p^f,$$

die letztere mit der Beschränkung, dass keine der Zahlen $a, b, a+b$ durch m theilbar sein darf. Endlich drücken sich genau wie in der gewöhnlichen Theorie gewisse Potenzen und Producte von Resolventen $F(\Theta^a, \xi)$ durch die Zahlen Ψ aus; namentlich ist, wenn durch ca das kleinste gemeinsame Vielfache von a und m bezeichnet und $c > 2$ angenommen wird,

$$(14) \quad F(\Theta^a, \xi)^c = [-1]^a p^f \Psi_{a,a} \Psi_{a,2a} \dots \Psi_{a,(c-2)a};$$

der Fall $c = 2$ erledigt sich unmittelbar durch die Formel (7b). Uebrigens wird in der Folge von den Zahlen Ψ kein weiterer Gebrauch gemacht.

6. Wenn es Exponenten k giebt, für welche $ap^k \equiv -a \pmod{m}$ ist, so ist der kleinste g unter diesen Exponenten ein Divisor von f . Die Gleichungen (6) und (7b) liefern dann zunächst

$$F(\Theta^a, \xi)^2 = [-1]^a p^f.$$

Ist nun der Quotient $\frac{f}{g}$ gerade, so ist

$$an = (p^g - 1) \frac{a(p^g + 1)}{m} (1 + p^{2g} + \dots + p^{f-2g})$$

durch $p - 1$ theilbar; folglich ist $[-1]^a = +1$ und

$$F(\Theta^a, \xi) = \pm p^{\frac{1}{2}f}.$$

Wir werden weiterhin unter der Annahme $ap^{\frac{1}{2}f} \equiv -a \pmod{m}$ das Vorzeichen in der letzten Gleichung allgemein bestimmen.

Ist dagegen $\frac{f}{g}$ ungerade, so ist jedenfalls auch $ap^f \equiv -a \pmod{m}$; da aber $p^f \equiv 1$ ist, so muss $2a$ durch m theilbar sein. Sehen wir von dem Falle $a \equiv 0 \pmod{m}$ ab, so muss m gerade, mithin p ungerade, und ausserdem $a \equiv \frac{m}{2} \pmod{m}$ sein. Dann ist aber $a(p+1)$ durch m theilbar, also $g = 1$ und f ungerade; weiter ist

$$\begin{aligned} an &= \frac{1}{2} mn = \frac{p-1}{2} (1 + p + \dots + p^{f-1}) \\ &\equiv \frac{p-1}{2} \pmod{(p-1)}. \end{aligned}$$

Somit wird hier

$$\begin{aligned} F(-1, \xi)^2 &= (-1)^{\frac{p-1}{2}} p^f, \\ F(-1, \xi) &= p^{\frac{f-1}{2}} \sqrt[(-1)^{\frac{p-1}{2}} p]. \end{aligned}$$

7. Ist g ein beliebiger Divisor von f , dann können wir die Summation nach ω in zwei einfachere zerlegen, indem wir die Zahlen ω nach den Werthen der Verbindung

$$(15) \quad \omega + \omega^{p^g} + \omega^{p^{2g}} + \dots + \omega^{p^{f-g}} \equiv \varrho$$

classificiren. Nach Satz V, § 1 umfasst jede Classe p^{f-g} Zahlen ω ; für alle diese hat auch $S(\omega)$ den nämlichen Werth, da

$$(16) \quad S(\omega) \equiv \varrho + \varrho^p + \dots + \varrho^{p^{g-1}} \equiv T(\varrho)$$

ist; ϱ aber durchläuft alle Wurzeln der Congruenz

$$(17) \quad \varrho^{p^g} \equiv \varrho \pmod{p}.$$

Ist nun ϱ von Null verschieden, so können wir durch die Substitution $\omega \equiv \varrho \tau$ die Congruenz (15) in

$$(18) \quad \tau + \tau^{p^g} + \tau^{p^{2g}} + \dots + \tau^{p^{f-g}} \equiv 1$$

überführen. Da in dieser ϱ nicht mehr vorkommt, so sind einfach alle Wurzeln von (17) mit allen von (18) zu multipliciren. Nur für $\varrho \equiv 0$ muss man auf die ursprüngliche Congruenz (15) zurückgehen, von den Wurzeln derselben aber $\omega \equiv 0$ weglassen. Bedient man sich wieder der durch die Gleichung (2) § 1 definirten Abkürzung und setzt ferner

$$M_0(\Theta^a) = \sum [\omega]^a, \quad (\omega + \omega^{(g)} + \dots + \omega^{(f-g)} \equiv 0),$$

$$(19) \quad M(\Theta^a) = \sum [\tau]^a, \quad (\tau + \tau^{(g)} + \dots + \tau^{(f-g)} \equiv 1),$$

$$(20) \quad G(\Theta^a, \xi) = \sum [\varrho]^a \xi^{T(\varrho)}$$

so erhält man jetzt

$$F(\Theta^a, \xi) = M_0(\Theta^a) + M(\Theta^a) G(\Theta^a, \xi).$$

Bei dieser Umformung ist nur die Gleichung $\xi^p = 1$ benutzt, sodass sie für $\xi = 1$ gültig bleibt. Daher kann man durch Subtraction die Grösse $M_0(\Theta^a)$ fortschaffen und hat dann

$$(21) \quad F(\Theta^a, \xi) - F(\Theta^a, 1) = M(\Theta^a) (G(\Theta^a, \xi) - G(\Theta^a, 1)).$$

Die durch $G(\Theta^a, 1)$ bezeichnete Summe hat aber nach § 2 den Werth $p^g - 1$ oder Null, je nachdem an durch $p^g - 1$ theilbar ist oder nicht; im ersten Falle reducirt sich der zweite Factor rechter Hand in Gleichung (21) auf $-p^g$. Aehnliches gilt von der linken Seite, nur das es auf die Theilbarkeit von an durch $p^f - 1$, d. h. von a durch m , ankommt. Sieht man also von dem Falle $a \equiv 0 \pmod{m}$ ab, so hat man den Satz:

Je nachdem an durch $p^g - 1$ theilbar ist oder nicht, wird

$$(21a) \quad F(\Theta^a, \xi) = -p^g M(\Theta^a)$$

oder

$$(21b) \quad F(\Theta^a, \xi) = M(\Theta^a) G(\Theta^a, \xi).$$

8. Der Factor $G(\Theta^a, \xi)$ besitzt ganz ähnliche Eigenschaften wie der Ausdruck $F(\Theta^a, \xi)$. In der That übertragen sich die Beweise in 3. und 4. dieses Paragraphen ohne Weiteres auf die Summe G , weil die Zahlen g sich durch Addition und Multiplication reproduciren. Namentlich ist also

$$(22) \quad G(\Theta^a, \xi^s) = [\varepsilon]^{-a} G(\Theta^a, \xi),$$

$$(23) \quad G(\Theta^a, \xi) = G(\Theta^{ap}, \xi),$$

$$(24) \quad G(\Theta^a, \xi) G(\Theta^{-a}, \xi^{-1}) = p^g;$$

bei der letzten Gleichung ist der bereits erledigte Fall

$$an \equiv 0 \pmod{(p^g - 1)}$$

anzunehmen.

Der andere Factor $M(\Theta^a)$ ist als specieller Werth der ganzen Function $(m-1)$ ten Grades $M(t) \equiv \sum t^{\text{Ind } \tau} \pmod{(t^m - 1)}$ aufzufassen, wobei τ durch die Congruenz (18) beschränkt ist. Da die einfachsten derartigen Summen von Eisenstein untersucht sind (vgl. den Schluss von § 2), bezeichnen wir sie allgemein als *Eisenstein'sche Summen*. Die zunächst sich darbietenden Eigenschaften derselben sind folgende:

$$(25) \quad a) \quad M(\Theta^a) = M(\Theta^{ap}).$$

b) Das Product $M(\Theta^a) M(\Theta^{-a})$ hat den Werth:

$$(26a) \quad p^{f-g}, \text{ wenn } an \text{ durch } p^g - 1 \text{ nicht theilbar ist;}$$

$$(26b) \quad p^{f-2g}, \text{ wenn } an \text{ durch } p^g - 1, \text{ aber nicht durch } p^f - 1 \text{ theilbar ist;}$$

$$(26c) \quad p^{2f-2g}, \text{ wenn } an \text{ durch } p^f - 1 \text{ theilbar ist.}$$

Die Entwicklungen in 7. und 8. gelten auch dann, wenn man statt von der Resolvente F von der Summe G ausgeht; neben der Zahl g ist dann noch ein Theiler h derselben einzuführen. Das Resultat lässt sich so aussprechen:

Zu jedem Divisor g des Grades f des Ideals $\mathfrak{p}$ gehört eine bestimmte „Resolvente“; wenn g durch h theilbar ist und G, H die zu den Zahlen g, h gehörigen Resolventen bezeichnen, so ist auch G durch H theilbar und der Quotient eine nur von Θ abhängende „Eisenstein'sche Summe.“

Die Modification, die dieser Satz erleidet, wenn an durch $p^h - 1$ theilbar ist, ist dabei ausser Acht gelassen.

9. Den wichtigsten Fall der Eisenstein'schen Summen erhält man, indem man $g = 1$ nimmt; in diesem Falle wird $G(\Theta^a, \xi)$ eine *gewöhnliche* Resolvente. Setzt man also

$$(27) \quad G(\Theta^a, \xi) = \sum [\varepsilon]^a \xi^{\varepsilon} \quad (\varepsilon = 1, 2, \dots, p-1),$$

$$(28) \quad M(\Theta^a) = \sum [\tau]^a \quad (\tau + \tau^p + \dots + \tau^{p^{f-1}} \equiv 1 \pmod{p}),$$

so hat man, von $a \equiv 0 \pmod{m}$ abgesehen,

$$(29a) \quad F(\Theta^a, \xi) = -p M(\Theta^a)$$

oder

$$(29b) \quad F(\Theta^a, \xi) = G(\Theta^a, \xi) M(\Theta^a),$$

je nachdem an durch $p-1$ theilbar ist oder nicht. Entsprechend ist auch

$$(30a) \quad M(\Theta^a) M(\Theta^{-a}) = p^{f-2}$$

oder

$$(30b) \quad M(\Theta^a) M(\Theta^{-a}) = p^{f-1},$$

während allgemein die Gleichung (25) gilt.

Die Congruenz $S(\omega) \equiv 0 \pmod{p}$ hat $f-1$ unabhängige Lösungen $\omega_1, \dots, \omega_{f-1}$. Nehmen wir zu diesen eine Lösung ω_0 der Congruenz $S(\omega) \equiv 1$ hinzu, so können wir alle Lösungen dieser letzteren durch $\omega_0 + x_1 \omega_1 + \dots + x_{f-1} \omega_{f-1}$ darstellen, wodurch

$$M(\Theta^a) = \sum [\omega_0 + x_1 \omega_1 + \dots + x_{f-1} \omega_{f-1}]^a$$

wird. Dabei sind dann $\omega_0, \omega_1, \dots, \omega_{f-1}$ f unabhängige Zahlen von bestimmter Beschaffenheit.

Auf diese Summe kann aber die allgemeinere

$$\overline{M}(\Theta^a) = \sum [\omega_0 + x_1 \omega_1 + \dots + x_{f-1} \omega_{f-1}]^a,$$

in welcher $\omega_0, \omega_1, \dots, \omega_{f-1}$ beliebige nach dem Modul p unabhängige Zahlen sind, in folgender Weise zurückgeführt werden. Sind $\eta_0, \eta_1, \dots, \eta_{f-1}$ die durch die Congruenzen (11) § 1 definirten complementären Zahlen, so sind die p^{f-1} Zahlen $\omega = \omega_0 + x_1 \omega_1 + \dots + x_{f-1} \omega_{f-1}$ die Wurzeln der Congruenz $S(\eta_0 \omega) \equiv 1 \pmod{p}$. Setzt man daher $\eta_0 \omega \equiv \tau$, so erhält man

$$\overline{M}(\Theta^a) = [\eta_0]^{-a} M(\Theta^a),$$

womit die Abhängigkeit der Summe $\overline{M}(\Theta^a)$ von der Wahl der Zahlen $\omega_0, \omega_1, \dots, \omega_{f-1}$ klar gelegt ist. Die Gleichungen (30) gelten für $\overline{M}$ unverändert, während (25) durch

$$\overline{M}(\Theta^a) = \overline{M}(\Theta^{ap}) [\eta_0]^{a(p-1)}$$

zu ersetzen ist.

Die Gleichungen (30) kann man auch nach Eisenstein direct beweisen durch ein Verfahren, welches im Grunde mit dem bei den Resolventen benutzten identisch ist; wir verzichten auf die Wiederholung des Beweises und fügen lieber einige Bemerkungen hinzu über die Art, wie Eisenstein in den beiden von ihm behandelten Fällen die f Zahlen $\omega_0, \omega_1 \dots \omega_{f-1}$ gewählt hat. Er hat die Wahl so getroffen, dass jene Zahlen sämmtlich für gewisse $\frac{\varphi(m)}{f}$ der primitiven Einheitswurzeln θ den nämlichen Werth und somit im Ganzen nur f verschiedene Werthe annehmen. Eine solche Wahl kann zwar practisch bequem sein, ist aber ohne principielle Wichtigkeit und ist auch nicht immer möglich. Wir geben nur kurz die Bedingung der Möglichkeit an nebst einem Falle, in dem diese Bedingung nicht erfüllt ist. Sie lautet: es darf keine niedrigere als die f te Potenz von p ein f ter Potenzrest sein; sie ist nicht erfüllt für $m = 15, p = 4$. Vgl. *Frobenius und Stickelberger „Ueber Gruppen von vertauschbaren Elementen“* § 3.*)

10. Wir können jetzt auch den in 6. erwähnten Fall vollständig erledigen, in dem

$$ap^{\frac{1}{2}f} \equiv -a \pmod{m}$$

ist, ohne dass a durch m theilbar wäre. Setzen wir nämlich

$$(31) \quad g = \frac{1}{2}f, \quad a(p^g + 1) = ml,$$

mithin

$$an = (p^g - 1)l,$$

so ist für alle Wurzeln der Congruenz (17) $[\theta]^a = 1$, und folglich nach Gleichung (21 a)

$$F(\theta^a, \xi) = -p^g M(\theta^a),$$

$$M(\theta^a) = \sum [\tau]^a$$

mit der Bedingung

$$\tau + \tau^{p^g} \equiv 1 \pmod{p}.$$

Setzt man nun

$$\tau^{p^g-1} \equiv \sigma,$$

so liefert die Bedingung für τ die Congruenzen

$$\sigma\tau \equiv 1 - \tau, \quad \tau(1 + \sigma) \equiv 1,$$

während

$$(32) \quad \sigma^{p^g+1} \equiv 1 \pmod{p}$$

ist. Es findet daher ein eindeutiges Entsprechen zwischen den Wurzeln

*) Journal f. Math. 86, S. 228.

der Congruenzen für τ und σ statt, wobei aber $\sigma = -1$ auszuschliessen ist. Zugleich wird

$$[\tau]^a \equiv \tau^{i(p^g-1)} \equiv \sigma^i.$$

Ist nun h der wahre Nenner des Bruches

$$\frac{l}{1+p^g} = \frac{a}{m},$$

so wird σ^i , während σ *alle* Wurzeln der Congruenz (32) durchläuft, je $(1+p^g):h$ Mal jeder der h ten Einheitswurzeln congruent; die Summe aller dieser Einheitswurzeln ist folglich gleich Null. Wegen des oben erwähnten Ausschlusses von $\sigma \equiv -1$ wird also

$$\begin{aligned} M(\Theta^a) &= \sum [\tau]^a = -(-1)^i, \\ (33) \quad F(\Theta^a, \xi) &= (-1)^i p^g = (-1)^i p^{\frac{1}{2}f}. \end{aligned}$$

Eine Ausnahme bildet der Fall $p=2$, wenn zugleich a ungerade ist. In der That sollte vorhin eigentlich diejenige Potenz von Θ ausgeschlossen werden, welche $\equiv (-1)^i \pmod{p}$ ist; diese ist aber *dann* nicht -1 , sondern $+1$, wenn l, m zugleich ungerade sind. Wegen Gleichung (31) erfordert dies, dass a und $p^g + 1$ ungerade seien, mithin $p=2$. Ueberhaupt ist für $p=2$ und $a \left(p^{\frac{1}{2}f} + 1 \right) \equiv 0 \pmod{m}$

$$F(\Theta^a, \xi) = + p^{\frac{1}{2}f}.$$

11. Wir betrachten zum Schlusse zwei einfache Beispiele.

Beispiel 1. Für $m=15$, $p=2$, $f=4$ hat man die viergliedrigen Perioden

$$\eta = \Theta + \Theta^2 + \Theta^4 + \Theta^8, \quad \eta_1 = \Theta^{14} + \Theta^{13} + \Theta^{11} + \Theta^7$$

zu betrachten, welche die Wurzeln der Gleichung

$$\eta^2 - \eta + 4 = 0$$

sind. Für denjenigen Primfactor p von 2, für den

$$\eta \equiv 0, \quad \eta_1 \equiv 1 \pmod{p}$$

ist, wird

$$(34) \quad \Theta^4 + \Theta + 1 \equiv 0 \pmod{p}.$$

Setzt man jetzt

$$\omega \equiv x_0 + x_1 \Theta + x_2 \Theta^2 + x_3 \Theta^3, \pmod{p},$$

so wird

$$S(\omega) \equiv \omega + \omega^2 + \omega^4 + \omega^8 \equiv x_3, \pmod{p}.$$

Zugleich ist $[\omega] \equiv \omega$. Nimmt man also $g=1$, so sind die Zahlen τ einfach diejenigen Potenzen von Θ , in deren mittels (34) auf den dritten Grad reducirten Ausdrücken Θ^3 einen ungeraden Coefficienten hat. Die Rechnung giebt als Exponenten dieser Potenzen

$$3, 6, 7, 9, 11, 12, 13, 14$$

und somit für $g = 1$:

$$M(t) = (t^3 + t^6 + t^9 + t^{12}) + (t^7 + t^{11} + t^{13} + t^{14}).$$

Die besonderen Werthe sind

$$\begin{aligned} M(\Theta) &= M(\Theta^2) = M(\Theta^4) = M(\Theta^8) = -\eta, \\ M(\Theta^7) &= M(\Theta^{11}) = M(\Theta^{13}) = M(\Theta^{14}) = -\eta_1, \\ M(\Theta^3) &= -2, \\ M(\Theta^5) &= +2. \end{aligned}$$

Beispiel 2. $m = 15$, $p = 19$, $f = 2$. Wählt man denjenigen Primfactor p , für den

$$\begin{aligned} \Theta + \Theta^4 &\equiv 2, & \Theta^2 + \Theta^8 &\equiv 9, & \Theta^7 + \Theta^{13} &\equiv 6, & \Theta^{11} + \Theta^{14} &\equiv 3, \\ \Theta^3 + \Theta^{12} &\equiv 4, & \Theta^6 + \Theta^9 &\equiv -5, & \Theta^5 &\equiv 7, & \Theta^{10} &\equiv -8 \end{aligned}$$

ist, so wird zugleich

$$\Theta^2 - 2\Theta + 7 \equiv 0;$$

diese Congruenz geht für

$$\Theta - 1 = \xi$$

über in

$$\xi^2 + 6 \equiv 0.$$

Setzt man nun $\omega = x + y\xi$, so wird einerseits

$$\omega + \omega^p \equiv 2x,$$

andererseits

$$[\omega] \equiv \omega^{24} \equiv (x + y\xi)^5 (x - y\xi).$$

Die Ausführung der Rechnung liefert allgemein

$$\begin{aligned} M(t) &\equiv 3(t + t^4) + (t^2 + t^8) + (t^7 + t^{13}) + (t^{11} + t^{14}) + 2(t^3 + t^{12}) \\ &\quad + 2t^5 + t^{10}, \end{aligned}$$

und im Besondern

$$\begin{aligned} M(\Theta) &= 2(\Theta + \Theta^4) - 3(\Theta^2 + \Theta^8) - 2(\Theta^7 + \Theta^{13}) - (\Theta^{11} + \Theta^{14}), \\ M(\Theta^3) &= -1, \\ M(\Theta^5) &= -2 + 3\Theta^5. \end{aligned}$$

§ 4.

Arithmetische Eigenschaften der Facultäten.

In den folgenden Paragraphen bedürfen wir einiger Eigenschaften der Facultäten, die wir hier im Zusammenhange entwickeln wollen. Wir gehen aus von der Darstellung der ganzen positiven Zahl a in dem System, dessen Basis p ist; wir setzen also

$$(1) \quad a = a_0 + a_1 p + a_2 p^2 + \dots$$

mit der Bedingung, dass $a_0, a_1, \dots$ Zahlen der Reihe $0, 1, \dots, p-1$ sind. Bekanntlich findet man dieselben durch wiederholte Division gemäss den Gleichungen

$$(2) \quad \begin{aligned} a &= a_0 + p q_1, \\ q_1 &= a_1 + p q_2, \\ q_2 &= a_2 + p q_3, \\ &\dots \end{aligned}$$

Aus diesen ergibt sich unmittelbar die bekannte Gleichung

$$(3) \quad a - (a_0 + a_1 + a_2 + \dots) = (p-1)(q_1 + q_2 + \dots),$$

auf welcher u. A. die Neunerprobe beruht.

Von jetzt an sei wieder p eine Primzahl, die zunächst auch gleich Zwei sein darf; wir wollen das Verhalten des Productes $1.2 \dots a = a!$ zu p untersuchen. Durch p theilbar sind in demselben die Factoren $p, 2p, \dots, q_1 p$, deren Product $p^{q_1} q_1!$ ist. Das Product der übrigen Factoren ist nach p congruent

$$(1.2 \dots (p-1))^{q_1} \cdot 1.2 \dots a_0$$

oder nach dem Wilson'schen Satze congruent $(-1)^{q_1} a_0!$. Somit haben wir

$$\frac{a!}{(-p)^{q_1} q_1!} \equiv a_0! \pmod{p}.$$

Aus gleichen Gründen ist

$$\frac{q_1!}{(-p)^{q_2} q_2!} \equiv a_1! \pmod{p}$$

u. s. w. Durch Multiplication erhalten wir

$$(4) \quad \frac{a!}{(-p)^{q_1+q_2+\dots}} \equiv a_0! a_1! a_2! \dots \pmod{p}.$$

Damit ist nicht allein die höchste in $a!$ aufgehende Potenz von p bestimmt, welche sich schon bei Legendre findet, sondern zugleich der Rest nach der nächst höheren Potenz.

Die Gleichung (4) gestattet eine Umformung, die auf der Einführung einer primitiven p ten Einheitswurzel ξ beruht*). Aus der Gleichung

$$p = (1 - \xi)(1 - \xi^2) \dots (1 - \xi^{p-1})$$

wird bekanntlich geschlossen, dass der Quotient $p : (1 - \xi)^{p-1}$ eine algebraische Einheit ist, für welche man zunächst den Ausdruck

$$1 \cdot (1 + \xi)(1 + \xi + \xi^2) \dots (1 + \xi + \dots + \xi^{p-2})$$

*) Diese Umformung und der anschliessende Satz sind neu hinzugefügt.

erhält; nach dem Modul $1 - \xi$ ist dieser congruent $1 \cdot 2 \dots (p-1)$, und man hat also mit Rücksicht auf den Wilson'schen Satz

$$(5) \quad \frac{-p}{(1-\xi)^{p-1}} \equiv +1 \pmod{(1-\xi)}.$$

Dieselbe Congruenz erhält man auch, indem man die Gleichung $\xi = 1 + (\xi - 1)$ auf die p te Potenz erhebt und rechts den binomischen Satz anwendet.

Erhebt man jetzt die Congruenz (5) auf die Potenz $q_1 + q_2 + \dots$ und multiplicirt sie mit (4), so erhält man

$$(6) \quad \frac{a!}{(1-\xi)^{a-(a_0+a_1+\dots)}} \equiv a_0! a_1! \dots \pmod{(1-\xi)},$$

wofür man auch schreiben kann

$$(7) \quad \frac{(1-\xi)^a}{a!} \equiv \frac{(1-\xi)^{a_0}}{a_0!} \frac{(1-\xi)^{a_1}}{a_1!} \dots \pmod{(1-\xi)^{1+a_0+a_1+\dots}},$$

In diesen Congruenzen ist der Satz enthalten, der uns in § 6 wesentliche Dienste leisten wird:

I. *Bedeutet a eine positive ganze rationale Zahl, p eine rationale Primzahl, ξ eine primitive p te Einheitswurzel, so ist der Bruch $\frac{(1-\xi)^a}{a!}$ gleich einem Bruche, dessen Nenner zu p theilerfremd ist.*

In dieser Form gilt der Satz auch für $a = 0$; ist $a > 0$, so enthält der Zähler des zweiten Bruches noch die Potenz $(1-\xi)^{a_0+a_1+\dots}$, also genau die erste, so oft a eine genaue Potenz von p ist.

Zwischen den Werthen von $a!$, welche den Werthen $a = 0, 1, \dots, p-1$ entsprechen, bestehen noch Relationen nach dem Modul p , welche an bekannte Eigenschaften von $\Gamma(\lambda)$ erinnern, wenn λ das Intervall von 0 bis 1 durchläuft. Zunächst ist nach dem Wilson'schen Satze

$$(8) \quad a!(p-1-a)! \equiv (-1)^{1+a} \pmod{p},$$

eine von Jacobi vielfach benutzte Relation.

Ist ferner a eine jener p Zahlen und q irgend eine ganze positive durch p nicht theilbare Zahl, und setzt man zur Abkürzung

$$b_0 = E\left(\frac{a}{q}\right), \quad b_1 = E\left(\frac{a+p}{q}\right), \quad \dots, \quad b_{q-1} = E\left(\frac{a+(q-1)p}{q}\right),$$

wobei $E(x)$ die grösste x nicht übersteigende ganze Zahl bedeutet, so sind $b_0, b_1, \dots, b_{q-1}$ ebenfalls Zahlen jener Reihe, und man kann den Bruch

$$(9) \quad F(a) = q^a \frac{b_0! b_1! \dots b_{q-1}!}{a!}$$

nach dem Modul p vollständig bestimmen. Ist nämlich $a \geq 1$ und k diejenige unter den Zahlen $0, 1, \dots, q-1$, für die $a + kp$ durch q theilbar, also gleich qb_k ist, so hat man

$$E\left(\frac{a+kp}{q}\right) = E\left(\frac{a-1+kp}{q}\right) + 1,$$

während für die übrigen Zahlen i jener Reihe

$$E\left(\frac{a+ip}{q}\right) = E\left(\frac{a-1+ip}{q}\right)$$

ist. Daher ist

$$\frac{F(a)}{F(a-1)} = q \cdot \frac{b_k}{a} = \frac{a+kp}{a} \equiv 1 \pmod{p},$$

folglich auch

$$F(a) \equiv F(a-1) \pmod{p}$$

und

$$(10) \quad F(a) \equiv F(0) \pmod{p}.$$

Diese Relation lässt sich bequemer und zugleich etwas allgemeiner schreiben, wenn man für irgend einen reellen positiven Werth von x durch $P(x)$ das Product der ganzen positiven Zahlen bezeichnet, die x nicht übertreffen, also

$$(11) \quad P(x) = 1 \cdot 2 \cdot 3 \cdots E(x)$$

setzt; für $0 \leq x < 1$ soll $P(x) = 0! = 1$ sein. Der Ausdruck

$$(9a) \quad F(x) = q^{E(x)} \cdot \frac{P\left(\frac{x}{q}\right) P\left(\frac{x+p}{q}\right) \cdots P\left(\frac{x+(q-1)p}{q}\right)}{P(x)}$$

ist dann, so lange $0 \leq x < p$ bleibt, nach dem Modul p von x unabhängig, also

$$F(x) \equiv P\left(\frac{p}{q}\right) P\left(\frac{2p}{q}\right) \cdots P\left(\frac{(q-1)p}{q}\right) \pmod{p}.$$

Hier kann man, wenn q ungerade ist, zufolge der Gleichung

$$E\left(\frac{ip}{q}\right) + E\left(\frac{(q-i)p}{q}\right) = p - 1$$

und der Congruenz (8) die Glieder paarweise zusammenfassen, wodurch man erhält

$$(12) \quad F(x) \equiv (-1)^{\frac{q-1}{2} + \sum E\left(\frac{ip}{q}\right)} \quad (i = 1, 2, \dots, \frac{q-1}{2}).$$

Auf gleiche Weise erhält man bei geradem q

$$(13) \quad \begin{aligned} F(x) &\equiv \frac{p-1}{2}! (-1)^{\frac{q-2}{2} + \sum E\left(\frac{ip}{q}\right)} \quad (i = 1, 2, \dots, \frac{q-2}{2}) \\ &\equiv \frac{1}{\frac{p-1}{2}} (-1)^{\frac{q}{2} + \sum E\left(\frac{ip}{q}\right)} \quad (i = 1, 2, \dots, \frac{q}{2}). \end{aligned}$$

Ist die Zahl q zusammengesetzt, so lässt sich das zu q gehörige Product $F(x)$ aus den analogen zusammensetzen, welche zu den einzelnen Factoren von q gehören. Wir wollen daher jetzt q als *Primzahl* voraussetzen. Für $q = 2$ haben wir dann unmittelbar

$$(14) \quad 2^{E(x)} P\left(\frac{x}{2}\right) P\left(\frac{x+p}{2}\right) \equiv P(x) P\left(\frac{p}{2}\right) \pmod{p}.$$

Bei ungeradem q dagegen bleibt noch der Factor

$$(-1)^{\sum E\left(\frac{p}{q}\right)}$$

zu bestimmen; derselbe ist aber durch Gauss' dritten Beweis des Reciprocitätsgesetzes*) bekannt, nämlich gleich dem Restcharakter $\left(\frac{p}{q}\right)$, wobei aber der Fall $p = 2$ auszuschliessen ist, der für unsere Relationen ohne jede Bedeutung ist. Wir haben somit, wenn p, q ungerade Primzahlen sind

$$(15) \quad q^{E(x)} P\left(\frac{x}{q}\right) P\left(\frac{x+p}{q}\right) \dots P\left(\frac{x+(q-1)p}{q}\right) \equiv (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \cdot P(x) \pmod{p}.$$

Die Beziehungen dieser Sätze zum quadratischen Reciprocitätsgesetze werde ich an anderer Stelle erörtern. Erwähnen muss ich hier noch, dass in Jacobi's Vorlesungen über Zahlentheorie 1836/7, die mir in der zweiten Hälfte der siebziger Jahre durch das Borchardt'sche Heft oder eine Abschrift desselben bekannt geworden sind, die Fälle behandelt werden, in denen $p \pm 1$ durch q theilbar ist.

§ 5.

Zur Theorie der Kreistheilung.

Um das Verständniss der allgemeinen Theorie des folgenden Paragraphen zu erleichtern, betrachten wir in dem gegenwärtigen die Factorenzerlegung der gewöhnlichen Kreistheilungsresolvente, wie sie Herr Kummer ermittelt hat, in grösster Allgemeinheit am Schlusse der Abhandlung: „*Theorie der idealen Zahlen, welche u. s. w.*“ Die Methode, die wir anwenden, liefert nicht allein die Kummer'schen Resultate in directerer Weise, sondern giebt auch eine Vervollständigung derselben und ist ausserdem leichter auf unsere verallgemeinerten Resolventen zu übertragen.

Sei p eine ungerade Primzahl, m ein Divisor von $p - 1 = mn$; seien ferner Θ , ξ primitive m te und p te Einheitswurzeln, $\wp$ ein in p aufgehendes Primideal des Körpers Ω , welcher aus der algebraischen Zahl Θ entspringt, endlich $[e]$ diejenige Potenz von Θ , welche nach

*) Werke II, S. 6.

**) Abhandl. der k. pr. Acad. d. W. 1856.

p congruent ist der n ten Potenz der ganzen rationalen Zahl z . Statt der Resolvente

$$(1) \quad F(\Theta^a, \xi) = \sum_1^{p-1} [z]^a \xi^z$$

betrachten wir zunächst die Function einer Unbestimmten u :

$$F(\Theta^a, 1+u) = \sum_1^{p-1} [z]^a (1+u)^z.$$

Vermöge der Definition des Zeichens $[z]$ und des binomischen Lehrsatzes erhalten wir

$$\begin{aligned} F(\Theta^a, 1+u) &\equiv \sum z^{an} (1+u)^z \\ &\equiv \sum_y \frac{u^y}{y!} \sum_z z^{an} \cdot z(z-1) \dots (z-y+1) \pmod{p}, \end{aligned}$$

wo z wie vorher die Werthe $1, 2, \dots, p-1$, y aber die Werthe $0, 1, \dots, p-1$ annimmt. Nehmen wir jetzt, was keine wesentliche Beschränkung einschliesst,

$$(2) \quad 0 < a \leq m,$$

so ist die ganze Function $z^{an} \cdot z(z-1) \dots (z-y+1)$ vom Grade $an+y$ und enthält kein von z freies Glied; so lange daher $an+y < p-1$ ist, ist aus bekannten Gründen die Summe ihrer Werthe für die genannten Werthe von z durch p theilbar, während sie congruent -1 wird für $an+y = p-1$. In der Entwicklung von $F(\Theta^a, 1+u)$ sind somit die Coefficienten derjenigen Potenzen von u , deren Exponenten kleiner als $p-1-an = n(m-a)$ sind, sämmtlich durch p theilbar, während der Coefficient der eben bezeichneten Potenz congruent ist $\frac{-1}{(p-1-an)!}$. Wir drücken dies durch die Congruenz aus:

$$\begin{aligned} (3) \quad F(\Theta^a, 1+u) &\equiv - \frac{u^{p-1-an}}{(p-1-an)!} \\ &\equiv (an)! (-u)^{p-1-an} \pmod{p, u^{p-an}}. \end{aligned}$$

Wollen wir nun $1+u = \xi$ einsetzen, so müssen wir gleichzeitig von dem Körper Ω zu demjenigen Körper $\bar{\Omega}$ vom Grade $(p-1)\varphi(m)$ übergehen, welcher aus den Einheitswurzeln Θ, ξ entspringt. Bezeichnet $\bar{p}$ die Gesamtheit der ganzen Zahlen dieses Körpers, so ist

$$\bar{p}p = \bar{p}^{p-1},$$

während $1-\xi$ nur die erste Potenz des neuen Primideals $\bar{p}$ enthält. Vermöge dieser Bemerkungen geht die letzte Congruenz über in

$$(4) \quad F(\Theta^a, \xi) \equiv (an)! (1-\xi)^{p-1-an} \pmod{\bar{p}^{p-an}}.$$

Damit ist nicht allein die höchste in F aufgehende Potenz des Primideals $\bar{p}$, sondern zugleich der Rest nach der nächst höheren Potenz bestimmt.

Die übrigen Primfactoren erledigen sich leicht, indem man a durch den kleinsten positiven Rest $a^{(k)}$ von ak und gleichzeitig Θ durch Θ^k ersetzt, wobei $kk' \equiv 1 \pmod{m}$ angenommen wird. Bezeichnet man durch $\mathfrak{p}_k, \bar{\mathfrak{p}}_k$ diejenigen Ideale, in welche durch diese Substitution die früheren $\mathfrak{p}, \bar{\mathfrak{p}}$ übergehen, so erhält man:

$$(5) \quad F(\Theta^a, \xi) \equiv (a^{(k)}n)! (1 - \xi)^{p-1-a^{(k)}n} \pmod{\bar{\mathfrak{p}}_k^{p-a^{(k)}n}}.$$

Nimmt man zu diesen Congruenzen die Gleichung

$$(6) \quad F(\Theta^a, \xi) F(\Theta^{-a}, \xi^{-1}) = p$$

hinzu, so lässt sich die Frage beantworten, wie weit durch diese Bedingungen die Zahl $F(\Theta^a, \xi)$ bestimmt ist; dabei wird angenommen, dass a eine feste durch m nicht theilbare Zahl sei, indem der Fall $a \equiv 0 \pmod{m}$ sich von selbst erledigt. Giebt es neben $F(\Theta^a, \xi)$ eine zweite Zahl, welche dieselben Bedingungen befriedigt, so enthalten beide nur die Primideale $\bar{\mathfrak{p}}_k$ und jedes derselben in der gleichen Potenz; ihr Quotient ε ist daher eine algebraische Einheit, und zwar eine solche, welche mit der conjugirt imaginären das Product Eins giebt; nach einem Kronecker'schen Satze*) ist daher ε eine Wurzel aus Eins, und zwar, weil rational aus Θ, ξ gebildet, von der Form $\pm \Theta^v \xi^z$; das doppelte Vorzeichen ist dabei überflüssig, sobald m gerade ist. Zufolge der Congruenz (4) muss aber auch $\varepsilon \equiv 1 \pmod{\bar{\mathfrak{p}}}$, d. h. $\pm \Theta^v \equiv 1 \pmod{\mathfrak{p}}$ sein, was nur möglich ist, wenn $\pm \Theta^v = 1$ ist. Daher ist durch die Gleichung (6) und die Congruenzen (5) die complexe Zahl $F(\Theta^a, \xi)$ bis auf eine Potenz von ξ bestimmt. Nimmt man die Bedingung hinzu, dass F^m die Grösse ξ nicht enthält, so bestimmt sich auch noch diese Potenz von ξ .

Setzt man $m - a$ für a , so ergibt sich aus (4) die Congruenz

$$(4a) \quad F(\Theta^{-a}, \xi) \equiv (p - 1 - an)! (1 - \xi)^{an} \pmod{\bar{\mathfrak{p}}^{1+an}},$$

welche für $0 \leq a < m$ gilt. Wenn a zwischen 0 und m liegt, so erhält man durch Multiplication

$$\begin{aligned} F(\Theta^a, \xi) F(\Theta^{-a}, \xi) &\equiv (an)! (p - 1 - an)! (1 - \xi)^{p-1} \\ &\equiv -(-1)^{an} (1 - \xi)^{p-1} \pmod{\bar{\mathfrak{p}}^p}. \end{aligned}$$

Da die linke Seite den Werth $(-1)^{an} p$ hat, so folgt hieraus

$$p \equiv -(1 - \xi)^{p-1} \pmod{\bar{\mathfrak{p}}^p},$$

in Uebereinstimmung mit Formel (5) § 4.

*) Journal f. Mathematik, Bd. 53, S. 176 ff.

Unsere Formel (3) ist, von der Bezeichnung abgesehen, in einer vollständiger enenthalt, die Jacobi in der Note: „*Ueber die Kreistheilung u. s. w.*“*) angiebt; während aber Jacobi die Entwicklung bis zu den Gliedern mit u^{p-1} treibt, haben wir uns mit dem ersten durch p nicht theilbaren Gliede begnügt und durch die Substitution $u = \xi - 1$ die Relation (4) gewonnen, welche unmittelbarer als die Jacobi'sche die von diesem „lange vergeblich gesuchte“ Analogie zwischen Resolventen und Euler'schen Integralen zweiter Gattung zum Ausdruck bringt. Unsere Congruenz liefert denn auch, ohne jede Benutzung der Jacobi'schen Zahlen ψ , die Beweise der von Jacobi a. a. O. mitgetheilten Sätze über Producte von Resolventen, wobei die auftretenden algebraischen Einheiten sich in ähnlicher Weise wie oben (S. 348) bestimmen; namentlich sei auf Jacobi's „allgemeine Formel“ S. 168 hingewiesen, bei deren Beweis die Formeln (12) und (13) des § 4 Verwendung finden.

Die Congruenz (4) führt auch zur Bestimmung des Vorzeichens der Gauss'schen Summen für den einfachsten Fall. Setzt man nämlich $m = 2$, $n = \frac{p-1}{2}$, mithin $p = p$, so fällt $[s]$ mit dem Legendre'schen Zeichen $\left(\frac{z}{p}\right)$ zusammen, und jene Congruenz verwandelt sich in

$$F(-1, \xi) = \sum \left(\frac{z}{p}\right) \xi^z \equiv \frac{p-1}{2}! (1 - \xi)^{\frac{p-1}{2}} \pmod{(1 - \xi)^{\frac{p+1}{2}}},$$

während zugleich

$$F(-1, \xi)^2 = (-1)^{\frac{p-1}{2}} p$$

ist. Denselben Bedingungen genügt aber auch die Zahl

$$\Phi(\xi) = \xi^{\frac{p-1}{2} \frac{p^2-1}{8}} (1 - \xi) (1 - \xi^2) \dots \left(1 - \xi^{\frac{p-1}{2}}\right);$$

bezüglich der Congruenz wird dies in gleicher Weise erkannt, wie wir die Relation (5) § 4 bewiesen haben. Zunächst muss also $F(-1, \xi) = \pm \Phi(\xi)$ sein; das Vorzeichen bestimmt sich dadurch, dass der Quotient nach dem Vorhergehenden congruent $+1$ sein muss nach dem Modul $1 - \xi$. Man hat also

$$\sum \left(\frac{z}{p}\right) \xi^z = \xi^{\frac{p-1}{2} \frac{p^2-1}{8}} (1 - \xi) (1 - \xi^2) \dots \left(1 - \xi^{\frac{p-1}{2}}\right),$$

woraus sich alles andere in bekannter Weise ergibt. Unser Beweis ist dem Wesen nach identisch mit dem von Herrn Kronecker**) angegebenen.

*) Journal f. Math. 30, S. 169.

**) Journal de math. (2) t. 1; 1856.

§ 6.

Congruenzbedingungen für die verallgemeinerten Resolventen.

Wir gehen jetzt zu der verallgemeinerten Resolvente

$$(1) \quad F(\Theta^a, \xi) = \sum [\omega]^a \xi^s$$

über, wie sie durch Gleichung (4) § 3 definirt ist; zur Abkürzung ist dabei s statt $S(\omega)$ geschrieben. Bei gegebenem a ist $F(\Theta^a, \xi)$ eine ganze Zahl desjenigen Körpers $\overline{\Omega}$ vom Grade $(p-1)\varphi(m)$, der aus den Einheitswurzeln Θ, ξ oder ihrem Producte $\Theta\xi$ entspringt, und sie enthält keine anderen Potenzen von Primidealen als solche, die in p^f aufgehen. Bezeichnet man auch hier durch $\overline{p}$ die Gesamtheit der ganzen Zahlen in $\overline{\Omega}$, so gilt wie in § 5 die Gleichung

$$(2) \quad \overline{p} \cdot \overline{p} = \overline{p}^{p-1},$$

während $1 - \xi$ die erste Potenz des neuen Primideals $\overline{p}$ enthält.

1. Was nun den ersten Factor des allgemeinen Gliedes von F anlangt, so haben wir

$$[\omega] \equiv \omega^n \pmod{p},$$

und daher nach bekannter Schlussweise

$$[\omega]^{p^f} \equiv \omega^{np^f} \pmod{p^{f+1}};$$

da aber $p^f \equiv 1 \pmod{m}$ und $[\omega]^m = 1$ ist, so wird auch

$$(3) \quad [\omega] \equiv \omega^{np^f} \pmod{p^{f+1}}.$$

Eine Vereinfachung lässt sich hier dadurch erzielen, dass man ω selbst passend auswählt. Setzt man nämlich zunächst

$$\omega^{p^f} \equiv \omega_1 \pmod{p^{f+1}},$$

so ist $\omega_1 \equiv \omega \pmod{p}$ und daher

$$\omega_1^{p^f} \equiv \omega^{p^f} \equiv \omega_1 \pmod{p^{f+1}}.$$

Die Congruenz

$$(4) \quad \omega^{p^f} \equiv \omega \pmod{p^{f+1}}$$

hat daher jedenfalls die p^f Zahlen ω_i zu Wurzeln. Sie hat aber auch keine andern Wurzeln; denn ist ω eine solche, so ist eben nach (4) ω einer p^f ten Potenz congruent. Daraus folgt:

I. Wählt man die Zahlen ω des Restsystems so, dass sie die Congruenz (4) befriedigen, dann ist

$$(5) \quad [\omega] \equiv \omega^n \pmod{p^{f+1}}.$$

Da sich ferner die Zahlen ω , von Null abgesehen, durch Multiplication reproduciren, so erhält man für jede ganze positive durch $p^f - 1$ nicht theilbare Zahl t die Congruenz

$$(6) \quad \sum \omega^t \equiv 0 \pmod{p^{f+1}},$$

während in dem ausgeschlossenen Falle die Summe congruent $p^f - 1$ ist.

2. Eine genauere Bestimmung der rationalen ganzen Zahl $s = S(\omega)$ wird geliefert durch den folgenden Hilfssatz.

II. Bezeichnet $\mathfrak{p}$ ein solches Primideal eines beliebigen Körpers Ω , dessen Norm gleich der f ten Potenz der rationalen Primzahl p ist, ferner $\Phi(x_1, x_2, \dots, x_f)$ eine ganze und ganzzahlige cyklische Function von f Veränderlichen, und h eine ganze positive Zahl, dann ist für jede ganze Zahl ω von Ω die Zahl

$$\Phi(\omega^{p^h}, \omega^{p^{h+1}}, \dots, \omega^{p^{h+f-1}})$$

einer rationalen Zahl congruent nach dem Modul p^{h+1} .

Setzt man nämlich

$$(7) \quad \Phi(x_1, x_2, \dots, x_f)^p = \Phi(x_1^p, x_2^p, \dots, x_f^p) + p\Psi(x_1, x_2, \dots, x_f),$$

so ist Ψ eine Function derselben Art wie Φ . Ist daher der Satz für einen bestimmten Werth von h giltig, so sind für

$$x_1 = \omega^{p^h}, \quad x_2 = \omega^{p^{h+1}}, \quad \dots$$

Φ, Ψ rationalen Zahlen congruent nach p^{h+1} , folglich Φ^p und $p\Psi$ ebenfalls rationalen Zahlen congruent nach p^{h+2} ; daraus folgt unmittelbar die Richtigkeit unseres Satzes für $h+1$. Der Fall $h=0$ ist bekannt; der Beweis beruht ebenfalls auf der Gleichung (7).

Wählen wir nun die Zahlen ω wieder so, dass sie die Congruenz (4) befriedigen, so erhalten wir unmittelbar den speciellen Satz:

III. Genügen die Zahlen ω wiederum der Congruenz (4), dann ist die Summe

$$(8) \quad \omega + \omega^p + \dots + \omega^{p^f-1} = \sigma$$

einer rationalen Zahl s congruent nach dem Modul p^{f+1} .

3. Wir wählen jetzt s überdies positiv, und entwickeln ξ^s nach Potenzen von $(\xi - 1)$ bis zu einer später zu bestimmenden Grenze, setzen also

$$\begin{aligned} \xi^s &\equiv \sum_0^l \frac{s(s-1)\dots(s-k+1)}{1 \cdot 2 \dots k} (\xi - 1)^k \\ &\equiv \sum \frac{(\xi - 1)^k}{k!} s(s-1)\dots(s-k+1) \pmod{(\xi - 1)^{l+1}}. \end{aligned}$$

Diese Congruenz bleibt auch giltig für den Modul $\bar{p}^{l+1}$, wenn $\bar{p}$ das zu Anfang definirte Primideal bedeutet. Ferner ist nach Satz III. s der Summe σ congruent nach dem Modul p^{f+1} oder $\bar{p}^{(f+1)(p-1)}$, während $(\xi - 1)^k : k!$ nach Satz I. § 4 gleich ist einem Bruche, dessen Nenner

zu p theilerfremd ist. Daher kann man in der vorigen Darstellung von ξ^s nach dem Modul $\bar{p}^{1+l}$ geradezu s durch σ ersetzen, wenn man den Exponenten l der Bedingung

$$(9) \quad (f+1)(p-1) > l$$

unterwirft. Auf diese Weise erhält man unter Benutzung bekannter Eigenschaften der Binomialcoefficienten

$$\begin{aligned} \xi^s &\equiv \sum_0^l \binom{\sigma}{k} (\xi - 1)^k \\ &\equiv \sum \binom{\omega}{x_0} \binom{\omega^p}{x_1} \dots \binom{\omega^{p^{f-1}}}{x_{f-1}} (\xi - 1)^{x_0+x_1+\dots+x_{f-1}} \pmod{\bar{p}^{1+l}}; \end{aligned}$$

dabei sind $x_0, x_1, \dots, x_{f-1}$ Zahlen der Reihe $0, 1, \dots$, deren Summe kleiner oder gleich l ist. Zu beachten ist hierbei, dass die einzelnen Binomialcoefficienten wie $\binom{\omega}{x}$ auch Potenzen von p im Nenner enthalten, die aber durch die hinzutretende Potenz von $(\xi - 1)$ compensirt sind. Setzt man nun für eine Unbestimmte w :

$$w(w-1)\dots(w-x+1) = \sum C_{x,y} w^{x-y} \quad (0 \leq y \leq x),$$

so ist $C_{x,0} = 1$, während die folgenden Coefficienten ganze Zahlen sind. Für ξ^s ergibt sich also die Darstellung

$$(10) \quad \sum_x \sum_y C_{x_0,y_0} C_{x_1,y_1} \dots \omega^{(x_0-y_0)+(x_1-y_1)p+\dots} \frac{(\xi-1)^{x_0+x_1+\dots}}{x_0! x_1! \dots} \pmod{\bar{p}^{1+l}};$$

die Summationsbedingungen ergeben sich unmittelbar aus dem Vorangehenden.

4. Wir setzen nun die Werthe (5) und (10) für $[\omega]$ und ξ^s in die allgemeine Resolvente ein. Nehmen wir noch

$$(11) \quad 0 < a \leq m$$

an und bringen an in die Form

$$(12) \quad an = b_0 + b_1 p + \dots + b_{f-1} p^{f-1},$$

mit der Bedingung, dass $b_0, b_1, \dots, b_{f-1}$ Zahlen der Reihe $0, 1, \dots, p-1$ seien, so wird der vollständige Exponent von ω in dem allgemeinen Glied von F :

$$\begin{aligned} t &= (b_0 + x_0 - y_0) + (b_1 + x_1 - y_1) p + \dots + (b_{f-1} + x_{f-1} - y_{f-1}) p^{f-1} \\ &= t_0 + t_1 p + \dots + t_{f-1} p^{f-1}. \end{aligned}$$

Die Zahlen $t_i = b_i + x_i - y_i$ sind wegen der Summationsbedingungen und der Annahme (11) nicht negativ und auch nicht sämmtlich gleich Null. Führen wir nun die Summation nach ω aus, so wird nach (6)

genau durch die $\sum E\left(\frac{p a_i}{m}\right)$ te Potenz des Primideals $\bar{p}$ theilbar und ist nach der nächst höheren Potenz congruent

$$(-1)^{1+\sum E\left(\frac{p a_i}{m}\right)} \frac{1}{\pi\left(P \frac{p a_i}{m}\right)} (1-\xi) \sum E\left(\frac{p a_i}{m}\right).$$

6. Der Uebergang zu den conjugirten Idealen geschieht wie in § 5. Man ersetzt a durch ak , Θ durch Θ^k , wobei die Zahlen k, k' die Bedingung $kk' \equiv 1 \pmod{m}$ befriedigen. Sind nun $a_0^{(k)}, \dots, a_{f-1}^{(k)}$ die kleinsten positiven Reste von $ak, \dots, akp^{f-1}$, ferner $\mathfrak{p}_k, \bar{\mathfrak{p}}_k$ die Ideale der Körper $\Omega, \bar{\Omega}$, in welche $\mathfrak{p}, \bar{\mathfrak{p}}$ durch jene Veränderung übergehen, so hat die höchste in $F(\Theta^{-a}, \xi)$ aufgehende Potenz von $\bar{\mathfrak{p}}_k$ den Exponenten

$$(19) \quad \sum_i E\left(\frac{p a_i^{(k)}}{m}\right) = \frac{p-1}{m} \sum_i a_i^{(k)} \quad (i = 0, 1, \dots, f-1).$$

Da allgemein $\mathfrak{p}_k = \mathfrak{p}_{kp}$ ist, so erhält man hieraus den Satz:

Durchläuft k $\varphi(m)$ Zahlen, welche incongruent nach m und prim zu m sind, erhebt man ferner jedes der Primideale $\bar{\mathfrak{p}}_k$ auf die Potenz $E\left(\frac{p a^{(k)}}{m}\right)$, wobei $a^{(k)}$ den kleinsten positiven Rest von ak nach m bedeutet, so ist das Product dieser Potenzen ein Hauptideal, nämlich $\bar{\mathfrak{p}} F(\Theta^{-a}, \xi)$. *)

Die Frage, wie weit durch die Gleichung

$$F(\Theta^a, \xi) F(\Theta^{-a}, \xi^{-1}) = p^f$$

und die in diesem Paragraphen hergeleiteten Congruenzbedingungen die Zahl $F(\Theta^a, \xi)$ bei gegebenem a bestimmt ist, beantwortet sich ähnlich wie die in § 5 aufgeworfene dahin, dass $F(\Theta^a, \xi)$ bis auf p te Einheitswurzeln bestimmt ist; aber auch diese bestimmen sich, wenn man die Bedingung hinzufügt, dass F^m die Grösse ξ nicht enthält. Die letzte Folgerung gilt nicht für $p = 2$; in diesem Falle lässt sich das Vorzeichen von F auf dem angegebenen Wege nicht bestimmen.

Wenn $\sum a_i$ durch m oder, was dasselbe heisst, an durch $p-1$ theilbar ist, so tritt eine Vereinfachung insofern ein, als dann schon $F(\Theta^a, \xi)$ von ξ frei ist. Entsprechend wird dann auch $\sum b_i$ durch $p-1$ theilbar, und man kann statt des Ideales $\bar{\mathfrak{p}}$ wieder $\mathfrak{p}$ einführen.

*) Vgl. Kummer, Journal f. Math. 35, S. 364–367; 44, S. 121.

Namentlich wird also $F(\Theta^{-a}, \xi)$ genau durch $p^{\frac{1}{m}\sum a_i}$ theilbar und ist nach der nächst höheren Potenz von p congruent

$$- (-p)^{\frac{1}{m}\sum a_i} \frac{1}{\prod P\left(\frac{p^{a_i}}{m}\right)}.$$

Als leicht zu verfolgende Beispiele seien angeführt

$$1) \ m = 11, \ p \equiv 3, 4, 5, 9 \pmod{11};$$

$$2) \ m = 15, \ p \equiv 2 \text{ oder } 8 \pmod{15}.$$

7. Die Betrachtungen, welche wir bisher in Betreff der Resolvente $F(\Theta^a, \xi)$ angestellt haben, übertragen sich mit geringen Abänderungen auf die Resolventen, welche nach § 3, 8 den verschiedenen Divisoren g von f entsprechen. Sei g ein solcher Divisor und an durch $p^g - 1$ nicht theilbar (andernfalls ist einfach $G(\Theta^a, \xi) = -1$), so wird man die Zahlen ϱ so wählen, dass sie die Congruenz

$$(20) \quad \varrho^{p^g} \equiv \varrho \pmod{p^{g+1}}$$

befriedigen; dann wird

$$[\varrho] \equiv \varrho^n \pmod{p^{g+1}};$$

$$\varrho + \varrho^p + \dots + \varrho^{p^{g-1}} = \sigma$$

aber wird einer rationalen Zahl s congruent nach demselben Modul. Setzt man nun

$$(21) \quad an = B_0 + B_1 p + \dots + B_{g-1} p^{g-1} + C_0(p^g - 1),$$

wo $B_0, B_1, \dots$ Zahlen der Reihe $0, 1, \dots, p-1$ sind, so wird vermöge der früheren Schlüsse

$$(22a) \quad G(\Theta^a, \xi) \equiv (-1)^{g-1} \prod B_i! (1 - \xi)^{\sum (p-1-B_i)} \pmod{p^{1+\sum (p-1-B_i)}},$$

$$(22b) \quad G(\Theta^{-a}, \xi) \equiv (-1)^{1+\sum B_i} \frac{1}{\prod B_i!} (1 - \xi)^{\sum B_i} \pmod{p^{1+\sum B_i}}.$$

Die Gleichung (21) lässt sich, da

$$\frac{n}{p^g - 1} = \frac{1 + p^g + \dots + p^{f-g}}{m}$$

ist, auf die Form

$$\frac{a(1 + p^g + p^{2g} + \dots + p^{f-g})}{m} = \frac{B_0 + B_1 p + \dots + B_{g-1} p^{g-1}}{p^g - 1} + C_0$$

bringen, in welcher das erste Glied rechter Hand zwischen 0 und 1 liegt. Bezeichnet man also durch A_i den kleinsten positiven Rest von

$$\alpha(p^i + p^{i+g} + \dots + p^{i+f-g})$$

nach dem Modul m , so wird

$$(23) \quad B_{g-i-1} = \frac{pA_i - A_{i+1}}{m} = E\left(\frac{pA_i}{m}\right),$$

$$(24) \quad B_{g-i-1}! = P\left(\frac{pA_i}{m}\right),$$

$$(25) \quad \sum B_i = \frac{p-1}{m} \sum A_i.$$

An die Congruenzen (22) knüpfen sich analoge Betrachtungen wie früher an (15); es scheint überflüssig, bei diesen besonders zu verweilen.

§ 7.

Anwendung auf die Theorie der quadratischen Formen.

1. Nachdem die verschiedenen in § 3 definirten Resolventen vollständig in ihre idealen Primfactoren zerlegt sind, kann man natürlich dasselbe auch für beliebige Producte, bez. Quotienten leisten; insbesondere für solche, die von ξ frei sind; in jedem Falle geben unsere Formeln zugleich den Rest nach der niedrigsten in der betreffenden Zahl nicht aufgehenden Potenz von $\bar{p}$ oder p . Beispielsweise sei auf Gleichung (7a) § 3 hingewiesen. Wir wollen sogleich zu solchen Producten übergehen, bei denen die verschiedenen Exponenten von Θ aus einem unter ihnen durch Multiplication mit Zahlen einer Restgruppe entspringen.

Sei also $\mathfrak{T}$ eine Gruppe von t Zahlen, die zu m theilerfremd sind und sich bis auf Vielfache von m durch Multiplication reproduciren. Sobald p dieser Restgruppe angehört, ist $t = fu$, und man kann bei geeigneter Wahl von $k_1, \dots, k_{u-1}$ die Gruppe darstellen durch

$$(1) \quad \begin{array}{ccccccc} 1, & p, & \dots, & p^{f-1}, \\ k_1, & k_1 p, & \dots, & k_1 p^{f-1}, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ k_{u-1}, & k_{u-1} p, & \dots, & k_{u-1} p^{f-1}. \end{array}$$

Das Product

$$(2) \quad (-1)^{t-u} F(\Theta^a, \xi) F(\Theta^{ak_1}, \xi) \dots F(\Theta^{ak_{u-1}}, \xi) = T(\Theta^a, \xi)$$

ist eine ganze ganzzahlige Function von Θ^a und ξ ; es bleibt ungeändert, wenn man Θ durch Θ^k ersetzt, falls k der Gruppe $\mathfrak{T}$ angehört. Dabei ist

$$(3) \quad T(\Theta^a, \xi) T(\Theta^{-a}, \xi^{-1}) = p^t.$$

Bedeutet ferner $a^{(k)}$ den kleinsten positiven Rest von ak nach m (den Fall $a \equiv 0$ schliessen wir wieder aus), so wird $T(\Theta^a, \xi)$ genau durch die

$$(4) \quad \sum E\left(\frac{p(m-a^{(k)})}{m}\right) = \frac{p-1}{m} \sum (m-a^{(k)})$$

te Potenz von $\bar{p}$ theilbar und ist nach der nächst höheren Potenz congruent

$$(5) \quad \prod P\left(\frac{pa^{(k)}}{m}\right) \cdot (1-\xi)^{\frac{p-1}{m} \sum (m-a^{(k)})}$$

In der Summe wie in dem Product durchläuft k die t Zahlen (1); aus diesen Congruenzen ist daher alles verschwunden, was sich auf den Exponenten f bezieht, zu dem p nach dem Modul m gehört. Nur der Ausdruck (2) von T ist von f abhängig; er enthält um so weniger Factoren, je grösser f ist; im Vergleich mit dem einfachsten Falle $f=1$ sind in dem allgemeinen je f Factoren durch einen ersetzt. Das Vorzeichen $(-1)^{t-u} = (-1)^u (f-1)$ ist der Gleichförmigkeit halber zugefügt; besser noch wäre es vielleicht, sowohl die gewöhnliche wie unsere allgemeine Resolvente mit -1 zu multipliciren.

Ist speciell $\sum k$ durch m theilbar, so kann man in (5) $(1-\xi)^{p-1}$ durch $-p$ ersetzen.

2. Wir betrachten jetzt besonders diejenige Gruppe der Ordnung $\frac{1}{2} \varphi(m)$, welche in der Theorie der quadratischen Formen von negativer Determinante eine so wichtige Rolle spielt und welche Cauchy in den Noten VII, VIII des früher angeführten Mémoire*) ausführlich discutirt hat. Sei nämlich m eine Zahl, die durch keine ungerade Quadratzahl ausser 1 theilbar und ausserdem entweder $\equiv 3 \pmod{4}$ oder $\equiv 4, 8 \pmod{16}$ ist; die quadratischen Formen $\alpha x^2 + \beta xy + \gamma y^2$ von der Determinante $\beta^2 - 4\alpha\gamma = -m$ sind dann nicht unter solchen von kleinerer Determinante enthalten. Setzt man nun mit Herrn Dedekind**) $(-m, p)$ gleich 0, +1, -1, je nachdem m durch die Primzahl p theilbar oder $-m$ quadratischer Rest oder Nichtrest von p ist (für $p=2$ je nachdem $-m \equiv 1$ oder $5 \pmod{8}$ ist), und ferner

$$(-m, p_1 p_2 p_3 \dots) = (-m, p_1) (-m, p_2) \dots,$$

so soll die Gruppe $\mathfrak{T}$ aus denjenigen $\frac{1}{2} \varphi(m)$ Zahlen bestehen, für die

$$(6) \quad (-m, k) = +1$$

ist.

Wir beweisen zunächst nach Cauchy, dass mit Ausnahme von $m=3, 4, 8$ stets die Summe der $\frac{1}{2} \varphi(m)$ Zahlen k durch m theilbar ist. Der Fall, in dem m eine Primzahl > 3 ist, erledigt sich un-

*) A. a. O., S. 525—588.

**) Zahlentheorie (3. Aufl.) S. 608.

mittelbar durch die Gruppeneigenschaft der k . Ist ferner q ein ungerader Primfactor von $m = qm'$, und $m' > 2$, so giebt es unter den Zahlen k je $\frac{1}{2} \varphi(m')$, welche einer bestimmten der Zahlen $1, 2, \dots, q-1$ congruent sind nach q ; daher ist

$$\sum k \equiv \frac{1}{2} \varphi(m') (1 + 2 + \dots + q-1) \equiv 0 \pmod{q}.$$

Für $m = 4m'$, $m' \equiv 1 \pmod{4}$ giebt es ebenso je $\frac{1}{2} \varphi(m')$ Zahlen k , die bez. congruent 1 oder 3 sind $\pmod{4}$, woraus $\sum k \equiv 0 \pmod{4}$ folgt. Aehnliches gilt für $m = 8m'$.

Wir wählen jetzt die Zahlen k zwischen 0 und m , und setzen

$$(7) \quad \sum k = mK.$$

Die Ergänzungen $k' = m - k$ gehören nicht der Gruppe $\mathfrak{L}$ an; setzen wir

$$(8) \quad \sum k' = mK',$$

so ist

$$(9) \quad K + K' = \frac{1}{2} \varphi(m).$$

Die Differenz $K' - K$ lässt sich bekanntlich auch durch Abzählung der zwischen 0 und $\frac{1}{2}m$ gelegenen Zahlen k und k' bestimmen, worauf wir hier nicht einzugehen brauchen. Dagegen entlehnen wir aus der Dirichlet'schen Theorie das Resultat, dass $K' - K$ gleich der Classenzahl der quadratischen Formen von der Determinante $-m$, und dass also $K' > K$ ist.

Weiter ist nach Cauchy

$$(10) \quad \sum \Theta^k - \sum \Theta^{k'} = \sum (-m, z) \Theta^z = \sqrt{-m}.$$

Nun sei p eine Primzahl, welche einer der Zahlen k congruent ist. Das Product (2) ist jetzt, wenn man wieder die Fälle $m=3, 4, 8$ ausschliesst, von ξ unabhängig und hat nur 2 verschiedene Werthe, indem

$$T(\Theta^k) = T(\Theta), \quad T(\Theta^{k'}) = T(\Theta^{-1})$$

ist. Die Verbindungen

$$T(\Theta) + T(\Theta^{-1}), \quad \frac{T(\Theta) - T(\Theta^{-1})}{\sqrt{-m}}$$

sind daher auch von Θ unabhängig, folglich rationale Zahlen. Setzen wir demgemäss

$$T(\Theta) = \frac{A + B\sqrt{-m}}{2},$$

so sind wegen der über m gemachten Voraussetzungen A, B ganze Zahlen; zugleich ist $A + mB \equiv 0 \pmod{2}$.

Unsere Relationen (3), (5) geben nun

$$\begin{aligned} 4p^{\frac{1}{2}\varphi(m)} &= A^2 + mB^2, \\ T(\Theta) &\equiv (-p)^K \prod P\left(\frac{pk}{m}\right) \pmod{\mathfrak{p}^{1+K}}, \\ T(\Theta^{-1}) &\equiv (-p)^K \prod P\left(\frac{pk'}{m}\right) \pmod{\mathfrak{p}^{1+K}}. \end{aligned}$$

Hiernach ist noch $T(\Theta)$ durch p^K theilbar. Setzen wir

$$(11) \quad T(\Theta) = (-p)^K \frac{C + D\sqrt{-m}}{2},$$

so ist der zweite Factor eine ganze algebraische Zahl und genügt den Bedingungen

$$(12) \quad 4p^{K'-K} = C^2 + mD^2,$$

$$(13) \quad \frac{C + D\sqrt{-m}}{2} \equiv 0 \pmod{\mathfrak{p}^{K'-K}},$$

$$(14) \quad \frac{C - D\sqrt{-m}}{2} \equiv \prod P\left(\frac{pk'}{m}\right) \equiv (-1)^{K'-K} \frac{1}{\prod P\left(\frac{pk}{m}\right)} \pmod{\mathfrak{p}},$$

aus denen noch

$$(15) \quad C \equiv \prod P\left(\frac{pk'}{m}\right) \pmod{p}$$

folgt. In diesen Producten durchläuft k , bez. k' diejenigen Zahlen der Reihe $1, 2, \dots, m-1$, welche prim zu m sind und die Gleichungen $(-m, k) = +1$, $(-m, k') = -1$ befriedigen; das Functionszeichen P ist durch die Gleichung (11), § 4 erklärt. Die gewonnenen Formeln leisten also für jede Primzahl p (einschliesslich $p=2$), für die $(-m, p) = +1$ ist, dasselbe, was die von Jacobi und Cauchy gegebenen für $p \equiv 1 \pmod{m}$.

In speciellen Fällen kann man den Congruenzen (13), (14) andere hinzufügen, die sich auf die Primfactoren von m als Moduln beziehen. Wir behandeln hier nur den Fall, wo m selbst eine Primzahl ist. Dann ist

$$F(\Theta^a, \xi) \equiv F(1, \xi) \equiv -1 \pmod{(1-\Theta)},$$

und folglich, wenn zunächst die Gruppe $\mathfrak{E}$ beliebig ist,

$$T(\Theta^a, \xi) \equiv (-1)^t \pmod{(1-\Theta)},$$

in unserem besonderen Falle aber

$$(16) \quad T(\Theta^a) \equiv (-1)^{\frac{1}{2} \varphi(m)} \pmod{(1-\Theta)}$$

oder

$$(17) \quad (-p)^{\kappa} C \equiv (-1)^{\frac{1}{2} \varphi(m)} \pmod{m}$$

§ 8.

Untersuchung der Eisenstein'schen Summen.

Wir wenden uns zum Schlusse nochmals zu den Eisenstein'schen Summen, welche in § 3 als Quotienten solcher Resolventen auftraten, die zu verschiedenen Divisoren des Exponenten f gehören; für den einen derselben wählen wir hier durchweg f selbst. Wenn also g einen Divisor von f bezeichnet, so haben wir wieder

$$F(\Theta^a, \xi) = -p^g M(\Theta^a)$$

oder

$$F(\Theta^a, \xi) = G(\Theta^a, \xi) M(\Theta^a),$$

je nachdem an durch $p^g - 1$ theilbar ist oder nicht; der triviale Fall $a \equiv 0 \pmod{m}$ ist dabei ausgeschlossen.

Nehmen wir zuerst den *zweiten* Fall, so brauchen wir neben den Resten a_i von ap^i nach dem Modul m noch die Reste der Summen $a(p^i + p^{i+g} + \dots + p^{i+f-g})$, die wir wie in § 6 durch A_i bezeichnen wollen. Dabei ist

$$(1) \quad a_0 + a_1 + \dots + a_{f-1} - (A_0 + \dots + A_{g-1}) = mq,$$

indem q eine ganze nicht negative Zahl bedeutet. Die höchste in $M(\Theta^a)$ aufgehende Potenz von $\bar{p}$ hat nun nach (22a), (25) § 6 den Exponenten

$$\sum (p-1-b_i) - \sum (p-1-B_i) = (p-1)(f-g-q).$$

Da $M(\Theta^a)$ von ξ frei ist, führen wir an Stelle von $\bar{p}^{p-1}$ das Ideal $\mathfrak{p}$ ein; mit Rücksicht auf die Formel (5) § 4 ergibt sich

$$(2) \quad M(\Theta^a) \equiv (-1)^g p^{f-g-q} \frac{P\left(\frac{pa_0}{m}\right) \dots P\left(\frac{pa_{f-1}}{m}\right)}{P\left(\frac{pA_0}{m}\right) \dots P\left(\frac{pA_{g-1}}{m}\right)} \pmod{\mathfrak{p}^{(f-g-q+1)}}.$$

Diese Formel bleibt auch im *ersten* Falle $an \equiv 0 \pmod{(p^g - 1)}$ bestehen, wenn man $A_0, A_1, \dots, A_{g-1}$ gleich Null und somit

$$(1a) \quad a_0 + a_1 + \dots + a_{f-1} = mq$$

setzt. Sie gilt sogar für $a \equiv 0 \pmod{m}$, wenn man sämtliche $a_i = 0$ setzt.

In den drei nachfolgenden Beispielen, von denen namentlich das dritte eigenen Werth haben dürfte, ist durchweg $g = 1$ angenommen.

Beispiel 1. Sei $m = 12$, $p = 12n + 5$, also $f = 2$; der Buchstabe n hat hier eine andere Bedeutung als in den früheren Paragraphen. Wegen

$$\Theta + \Theta^5 = \Theta^3 = \sqrt{-1}$$

ist $\Theta + \Theta^5$ einer rationalen Zahl congruent (mod. p); durch die Wahl der Congruenzwurzel ist der Primfactor bestimmt. Wir bestimmen $M(\Theta^a)$ für beliebige Werthe von a , nicht bloss für diejenigen, welche prim zu 12 sind. Zunächst ist

$$M(\Theta^0) = p.$$

Da ferner $6p \equiv 6 \pmod{12}$ und $6 + 6 = 1 \cdot 12$ ist, wird

$$M(\Theta^6) \equiv - \frac{p-1}{2}! \frac{p-1}{2}! \equiv +1 \pmod{p};$$

weil aber

$$M(\Theta^6) M(\Theta^{-6}) = M(\Theta^6)^2 = p^{f-2} = 1$$

ist, wird

$$M(\Theta^6) = +1.$$

Auf ähnliche Weise findet man

$$M(\Theta^4) = M(\Theta^8) = -1,$$

$$M(\Theta^2) = M(\Theta^{10}) = +1.$$

Dieselben Werthe erhält man auch aus Formel (33) § 3.

Für $a = 3$ hingegen ist $3p \equiv 3$, also $a_0 = a_1 = 3$, $A_0 = 6$, $q = 0$, während für $a = 9$, $a_0 = a_1 = 9$, $A_0 = 6$, $q = 1$ wird. Man hat somit

$$M(\Theta^3) M(\Theta^9) = p,$$

$$\begin{aligned} M(\Theta^3) &\equiv p \frac{(3n+1)!(3n+1)!}{(6n+2)!} \pmod{p^2} \\ &\equiv 0 \pmod{p}, \end{aligned}$$

$$M(\Theta^9) \equiv \frac{(6n+2)!}{(3n+1)!(3n+1)!} \pmod{p}.$$

Es sind also $M(\Theta^3)$, $M(\Theta^9)$ die beiden conjugirten Primfactoren von p nach der Gauss'schen Theorie, und es erübrigt noch, ihr Verhältniss zu den durch die Kreistheilung definirten Primfactoren zu bestimmen. Letztere werden gewöhnlich bestimmt durch die Relationen

$$(A + B\Theta^3)(A + B\Theta^9) = p,$$

$$A + B\Theta^3 \equiv 0,$$

$$A + B\Theta^9 \equiv - \frac{\frac{p-1}{2}!}{\frac{p-1}{4}! \frac{p-1}{4}!} \pmod{p}.$$

$$A \equiv -1 \pmod{4}.$$

Durch Vergleichung der beiderseitigen Bedingungen findet sich

$$M(\Theta^3) = -(A + B\Theta^3).$$

Nimmt man endlich $a = 1$, so wird zunächst $M(\Theta) = M(\Theta^5)$, hängt also nur von der vierten Einheitswurzel Θ^3 ab. Da

$$\left. \begin{aligned} M(\Theta) \cdot M(\Theta^{11}) &= p, \\ M(\Theta) &\equiv 0, \\ M(\Theta^{11}) &\equiv \frac{(6n+2)!}{n!(5n+2)!} \end{aligned} \right\} \pmod{p}$$

ist, so muss

$$M(\Theta) = (A + B\Theta^3)\Theta^{3h}$$

sein. Um die Einheitswurzel Θ^{3h} genauer zu bestimmen, benutzen wir die Relation (15) des § 4 für $q = 3$, $x = \frac{p}{4}$, und erhalten

$$3^{3n+1}n!(5n+2)!(9n+3)! \equiv (3n+1)! \pmod{p}$$

oder auch

$$(-3)^{3n+1}n!(5n+2)! \equiv -(3n+1)!(3n+1)! \pmod{p}.$$

Dadurch wird aber

$$M(\Theta^{11}) \equiv (-3)^{3n+1}(A + B\Theta^9) \pmod{p}$$

oder

$$\Theta^{-3h} \equiv (-3)^{\frac{p-1}{4}} \pmod{p}.$$

Die Potenz von $\Theta^3 = \sqrt[4]{-1}$, welche der $\frac{p-1}{4}$ ten Potenz einer Zahl congruent ist nach p , ist geradezu der biquadratische Restcharakter dieser Zahl; wir bezeichnen ihn durch doppelte Klammern, da er von unserm Charakter $[\omega]$ durchaus verschieden ist. Wir haben also endlich

$$\begin{aligned} \Theta^{-3h} &= \left(\left(\frac{-3}{p}\right)\right), \\ (3) \quad M(\Theta) &= \left(\left(\frac{-3}{p}\right)\right)^3 (A + B\Theta^3). \end{aligned}$$

Eine Prüfung der gewonnenen Resultate und zugleich eine Bestimmung des Restcharakters $\left(\left(\frac{-3}{p}\right)\right)$ ergibt sich aus den Congruenzen

$$(4) \quad M(\Theta^a) + M(\Theta^{a+4}) + M(\Theta^{a+8}) \equiv 0 \pmod{3},$$

$$(5) \quad M(\Theta^a) + M(\Theta^{a+3}) + M(\Theta^{a+6}) + M(\Theta^{a+9}) \equiv 0 \pmod{4},$$

die man leicht aus der Ganzzahligkeit der Coefficienten von $M(t)$ ableitet. Namentlich liefert die erste derselben für $a = 3$ die Congruenz

$$(A + B\Theta^3) + \left(\left(\frac{-3}{p}\right)\right)(A + B\Theta^9) \equiv 0 \pmod{3},$$

die durch Multiplication mit $A + B\Theta^3$ übergeht in

$$\left(\left(\frac{-3}{p}\right)\right) \equiv (A + B\Theta^3)^2 \pmod{3},$$

wie es das Reciprocitätsgesetz der biquadratischen Reste verlangt.

Beispiel 2. Sei jetzt $m = 12$, $p = 12n + 7$, $f = 2$, $g = 1$. Hier hängt $M(\Theta) = M(\Theta^7) = M(-\Theta)$ nur von Θ^2 , also im Grunde von dritten Einheitswurzeln ab, und ebenso alle $M(\Theta^a)$. Wir führen daher sogleich denjenigen Primfactor $(A + B\Theta^4)$ von p ein, welcher in der Kreistheilung auftritt und durch die Bedingungen

$$\left. \begin{aligned} A + B\Theta^4 &\equiv 0 \\ A + B\Theta^8 &\equiv -\frac{\frac{2p-2}{3}!}{\frac{p-1}{3}! \frac{p-1}{3}!} \pmod{p}, \\ A + B\Theta^4 &\equiv -1 \pmod{3} \end{aligned} \right\}$$

bestimmt ist.

Man hat im gegenwärtigen Falle

$$\begin{aligned} 2^{\frac{p-1}{2}} &\equiv \left(\frac{2}{p}\right) = (-1)^n \pmod{p}, \\ [2] &\equiv 2^{\frac{p-1}{3}(3n+2)} \equiv 2^{2\frac{p-1}{3}} \pmod{p}, \end{aligned}$$

und ferner nach (14), § 4 für $x = \frac{p}{6}$, bez. $\frac{p}{3}$ die Congruenzen

$$\left. \begin{aligned} 2^{2n+1} \cdot n! (7n+4)! &\equiv (2n+1)! (6n+3)! \\ 2^{4n+2} \cdot (2n+1)! (8n+4)! &\equiv (4n+2)! (6n+3)! \end{aligned} \right\} \pmod{p},$$

aus denen noch

$$2^{6n+3} \cdot n! (7n+4)! (8n+4)! \equiv (4n+2)! \pmod{p}$$

folgt. Durch ähnliche Schlüsse wie im vorigen Beispiel findet man mit Hilfe dieser Relationen

$$\begin{aligned} M(\Theta^6) &= -1, \\ M(\Theta^3) &= (-1)^{n+1} = \left(\frac{-2}{p}\right), \\ M(\Theta^4) &= -(A + B\Theta^4), \\ M(\Theta^2) &= [2]^2 (A + B\Theta^4), \quad M(\Theta^{10}) = [2] (A + B\Theta^8), \\ M(\Theta) &= \left(\frac{2}{p}\right) (A + B\Theta^4). \end{aligned}$$

Zur Prüfung dienen die Congruenzen (4), (5), welche zugleich eine Bestimmung des Restcharakters $[2]$ liefern. Namentlich giebt die zweite derselben für $a = 1$

$$(A + B\Theta^4) + [2](A + B\Theta^8) \equiv 0 \pmod{4},$$

wofür man auch

$$[2](A + B\Theta^4) + [2]^2(A + B\Theta^8) \equiv 0 \pmod{4}$$

schreiben kann. Daraus folgt zunächst

$$[2] \equiv (A + B\Theta^4)^2 \pmod{2},$$

im Einklang mit dem cubischen Reciprocitätsgesetze, wenn man die abweichende Bedeutung von $[2]$ berücksichtigt. Ausserdem lehren jene Congruenzen, dass $[2](A + B\Theta^4)$ auf die Form $C + D\sqrt{-3}$ gebracht werden kann, und dass dann C gerade ist; letzteres folgt auch aus

$$p = C^2 + 3D^2 \equiv 3 \pmod{4}.$$

Beispiel 3. Wir nehmen $m = 15$, $p = 15n + 4$, $f = 2$. Zunächst erhalten wir in bekannter Weise

$$M(\Theta^3) = -1.$$

Dagegen ist $M(\Theta^5)M(\Theta^{10}) = p$, und die Factoren hängen nur von dritten Einheitswurzeln ab. Bedeutet wieder $A + B\Theta^5$ denjenigen Primfactor von p , welcher durch $\mathfrak{p}$ theilbar und dabei $\equiv -1 \pmod{3}$ ist, so giebt unsre Congruenz (2) in bekannter Weise

$$M(\Theta^5) = -(A + B\Theta^5).$$

Für $M(\Theta)$ und die conjugirten Zahlen aber haben wir die Gleichungen

$$(6) \quad M(\Theta)M(\Theta^{14}) = M(\Theta^2)M(\Theta^{13}) = p$$

nebst den Congruenzen

$$\left. \begin{aligned} M(\Theta) = M(\Theta^4) &\equiv p \frac{n!(4n+1)!}{(5n+1)!} \\ M(\Theta^2) = M(\Theta^8) &\equiv p \frac{(2n)!(5n+1)!}{(7n+1)!} \end{aligned} \right\} \pmod{p^2},$$

$$\left. \begin{aligned} M(\Theta^7) = M(\Theta^{13}) &\equiv \frac{(7n+1)!}{(2n)!(5n+1)!} \\ M(\Theta^{11}) = M(\Theta^{14}) &\equiv \frac{(5n+1)!}{n!(4n+1)!} \end{aligned} \right\} \pmod{p}.$$

Ersetzt man Θ durch Θ^2 , wodurch $\mathfrak{p}$ in eines der drei andern Primideale übergeht, durch die p theilbar ist, so ergibt sich, dass $M(\Theta)$, $M(\Theta^2)$ durch dieselben zwei Primideale $\mathfrak{p}(\Theta)$, $\mathfrak{p}(\Theta^2)$ theilbar, mithin associirt sind; der Quotient $\varepsilon(\Theta)$ muss wegen (6) eine einfache Einheit, d. h. eine Potenz von $-\Theta$, sein und zugleich wegen $M(\Theta) = M(\Theta^4)$ die Gleichung $\varepsilon(\Theta) = \varepsilon(\Theta^{-2})$ befriedigen; er muss also eine dritte oder sechste Einheitswurzel sein. Die Bestimmung derselben wird durch die Congruenz (15), § 4 ermöglicht, wenn man in derselben $q = 5$, $x = \frac{p}{3}$ setzt; man erhält auf diese Weise

$$5^{5n+1} \cdot n!(4n+1)!(7n+1)!(10n+2)!(13n+3)! \equiv (5n+1)!$$

oder einfacher

$$5^{5n+1} n!(4n+1)!(7n+1)! \equiv (2n)!(5n+1)!(5n+1)! \pmod{p}.$$

Daher wird

$$\frac{M(\Theta^2)}{M(\Theta)} \equiv 5^{5n+1} = 5^{\frac{p-1}{3}} \equiv [5] \pmod{p}$$

oder vielmehr

$$M(\Theta^2) = [5] M(\Theta).$$

Somit bleibt $[5]^2 M(\Theta)$ ungeändert, wenn man Θ durch $\Theta^2, \Theta^4, \Theta^8$ ersetzt und lässt sich durch die Perioden

$$\Theta + \Theta^2 + \Theta^4 + \Theta^8, \quad \Theta^{14} + \Theta^{13} + \Theta^{11} + \Theta^7$$

linear ausdrücken, deren Werthe $\frac{1 + \sqrt{-15}}{2}, \frac{1 - \sqrt{-15}}{2}$ sind. Da die Form $x^2 + 15y^2$ für ungerade Werthe von x und y durch 8 theilbar ist, erkennt man leicht, dass

$$[5]^2 M(\Theta) = C + D \sqrt{-15}$$

sein muss; vollständiger hat man

$$C + D \sqrt{-15} = [5]^2 M(\Theta) = [5] M(\Theta^2) = [5]^2 M(\Theta^4) = [5] M(\Theta^8),$$

$$C - D \sqrt{-15} = [5]^2 M(\Theta^7) = [5] M(\Theta^{14}) = [5]^2 M(\Theta^{13}) = [5] M(\Theta^{11}).$$

Für die Zahlen C, D erhält man nun zunächst die Relationen¹

$$(7) \quad \left. \begin{aligned} C^2 + 15 D^2 &= p, \\ C + D \sqrt{-15} &\equiv 0, \\ C - D \sqrt{-15} &\equiv [5] \frac{(5n+1)!}{n! (4n+1)!} \end{aligned} \right\} \pmod{p},$$

$$(8) \quad 2C \equiv 5^{\frac{p-1}{3}} \frac{(5n+1)!}{n! (4n+1)!} \pmod{p}.$$

Weitere Bedingungen folgen aus den Congruenzen

$$M(\Theta) + M(\Theta^6) + M(\Theta^{11}) \equiv 0 \pmod{3},$$

$$M(\Theta) + M(\Theta^4) + M(\Theta^7) + M(\Theta^{10}) + M(\Theta^{13}) \equiv 0 \pmod{5},$$

die man auf gleichem Wege wie (4), (5) in Beispiel 1 erschliesst. Die erste derselben liefert, da jedenfalls

$$1 + [5] + [5]^2 \equiv 0, \quad ([5] - [5]^2) \sqrt{-15} \equiv 0 \pmod{3}$$

ist, nur eine Bedingung

$$(9) \quad C \equiv -1 \pmod{3};$$

die zweite aber, welche die Form

$$[5] C \equiv -(A + B \Theta^{10}) \pmod{5}$$

annimmt, lässt sich in zwei spalten, indem man sie quadriert und einbirt. Mit Rücksicht auf

$$C^2 = p - 15 D^2 \equiv -1 \pmod{5}$$

wird

$$[5]^2 \equiv -(A + B \Theta^{10})^2$$

oder

$$(10) \quad [5] \equiv -(A + B\Theta^5)^2 \pmod{5},$$

in Uebereinstimmung mit dem cubischen Reciprocitätsgesetze. Zugleich aber muss

$$(11) \quad C \equiv (A + B\Theta^{10})^3 \pmod{5}$$

sein. — Nun ist

$$p = (A + B\Theta^5)(A + B\Theta^{10}) \equiv (A + B\Theta^5)^6 \equiv -1 \pmod{5},$$

also $A + B\Theta^5$ eine der sechs Wurzeln der Congruenz $\omega^6 \equiv -1$, welche sich in zwei Reihen von je dreien ordnen:

$$\begin{array}{ccc} 2, & 2\Theta^5, & 2\Theta^{10}, \\ -2, & -2\Theta^5, & -2\Theta^{10}; \end{array}$$

wir haben also das Resultat:

Je nachdem $A + B\Theta^5$ einer Zahl der ersten, zweiten oder dritten Colonne dieser Tabelle congruent ist (mod. 5), ist der cubische Restcharakter $[5]$ gleich 1, Θ^{10} , Θ^5 ; dagegen ist C congruent -2 oder $+2$ (mod. 5), je nachdem $A + B\Theta^5$ einer Zahl der ersten oder zweiten Zeile congruent ist nach demselben Modul.

Freiburg i. Br., 31. März 1890.