Ueber die Entwickelungscoefficienten der lemniscatischen Functionen*).

Von

A. Hurwitz in Zürich.

Die folgenden Untersuchungen beziehen sich auf gewisse Zahlen, welche ähnliche Eigenschaften besitzen, wie die Bernoulli'schen Zahlen. Die letzteren lassen sich bekanntlich durch die Gleichung

$$\sum \frac{1}{r^{2n}} = \frac{(2\pi)^{2n}}{(2n)!} B_n \qquad (n = 1, 2, 3, \ldots)$$

definiren, wobei die Summe über alle positiven und negativen reellen ganzen Zahlen r mit Ausschluss der Null zu erstrecken ist und die Zahl π als Werth des Integrales

$$\pi = 2 \int_0^1 \frac{dx}{\sqrt{1 - x^2}}$$

aufgefasst werden kann. In ähnlicher Weise können und sollen die hier zu untersuchenden Zahlen $E_1, E_2, E_3, \ldots$ durch die Gleichung

$$\text{(D)} \qquad \sum \frac{1}{(r + is)^{4n}} = \frac{(2\omega)^{4n}}{(4n)!} E_n \quad (n = 1, 2, 3, \ldots)$$

definirt werden. Dabei ist die Summe auf alle complexen ganzen Zahlen $r + is$ mit Ausschluss der Null auszudehnen; ferner bedeutet ω den Werth des Integrales

$$\omega = 2 \int_0^1 \frac{dx}{\sqrt{1 - x^4}} = 2{,}622057 \ldots .$$

Die Zahlen E_n nehmen also, ihrer Definition nach, eine entsprechende Stellung in der Theorie der Gaussischen complexen ganzen Zahlen

*) Vgl. eine vorläufige Mittheilung in den Nachrichten der k. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Classe. 1897, pag. 273.

ein, wie die Bernoulli'schen Zahlen in der Theorie der reellen ganzen Zahlen.

Die Zahlen E_n sind übrigens, ebenso wie die Bernoulli'schen Zahlen, positive reelle rationale Zahlen. Es wird sich dies weiterhin als unmittelbare Folge der Thatsache ergeben, dass die Zahlen E_n im Wesentlichen mit den Entwickelungscoefficienten einer gewissen lemniscatischen Function, d. h. einer doppeltperiodischen Function, deren Periodenparallelogramm ein Quadrat ist, identisch sind. Hierin liegt eine weitere Analogie der Zahlen E_n mit den Bernoulli'schen Zahlen. Denn die letzteren sind bekanntlich im Wesentlichen die Entwickelungscoefficienten einer einfach periodischen Function, der Cotangente.

Aber auch eine tiefer liegende Eigenschaft der Bernoulli'schen Zahlen, nämlich diejenige, welche sich auf ihre Partialbruchzerlegung bezieht und in dem v. Staudt-Clausen'schen Satze ihren Ausdruck findet, besitzt ihr völlig entsprechendes Gegenbild bei den Zahlen E_n. Dieses nachzuweisen, also die Herleitung desjenigen Satzes über die Zahlen E_n, welcher dem v. Staudt-Clausen'schen Satze von den Bernoulli'schen Zahlen entspricht, bildet das Hauptziel der folgenden Untersuchungen. Dabei sind die Methoden, deren ich mich bediene, zum Theil von allgemeinem Charakter, so dass dieselben auch über den vorliegenden speciellen Zweck hinaus bei Untersuchungen ähnlicher Art brauchbar sein dürften.

§ 1.

Ganzzahlige Potenzreihen.

Um den Gang der Untersuchung später nicht unterbrechen zu müssen, schicke ich hier einige allgemeine Sätze über Potenzreihen voraus, welche weiterhin zur Anwendung gelangen. Diese Sätze beziehen sich auf Potenzreihen einer complexen Variabeln u, welche die Gestalt

$$(1) \qquad \mathfrak{P} = c_0 + c_1 \frac{u}{1!} + c_2 \frac{u^2}{2!} + \cdots + c_n \frac{u^n}{n!} + \cdots$$

besitzen, wo $c_0, c_1, c_2, \ldots c_n, \ldots$ ganze rationale Zahlen bezeichnen.

Zur Abkürzung will ich eine derartige Potenzreihe „ganzzahlig" nennen.

Der Inbegriff aller ganzzahligen Potenzreihen bildet einen „Integritätsbereich", d. h. Summe, Differenz und Product irgend zweier ganzzahligen Potenzreihen sind wiederum ganzzahlige Reihen. Oder in anderer Ausdrucksweise: im Systeme aller ganzzahligen Potenzreihen sind Addition, Subtraction und Multiplication unbeschränkt ausführbare Operationen. Für die Addition und Subtraction leuchtet

diese Thatsache unmittelbar ein. Für die Multiplication folgt sie aus der Bemerkung, dass das Product der Reihe (1) in die Reihe

$$\mathfrak{P}_1 = d_0 + d_1 \frac{u}{1!} + d_2 \frac{u^2}{2!} + \cdots + d_n \frac{u^n}{n!} + \cdots \tag{2}$$

durch die Reihe

$$\mathfrak{P}_2 = e_0 + e_1 \frac{u}{1!} + e_2 \frac{u^2}{2!} + \cdots + e_n \frac{u^n}{n!} + \cdots \tag{3}$$

vorgestellt ist, wenn man allgemein

$$e_n = c_0 d_n + n_1 c_1 d_{n-1} + n_2 c_2 d_{n-2} + \cdots + c_n d_0$$

setzt, unter $n_1, n_2, \ldots$ die Binomialcoefficienten zur Basis n verstanden.

In dem Systeme der ganzzahligen Reihen sind aber überdies auch die Operationen der Differentiation und der Integration von $u = 0$ ab unbeschränkt ausführbar.

Denn bedeutet $\mathfrak{P}$ die ganzzahlige Reihe (1), so sind offenbar auch

$$\frac{d\mathfrak{P}}{du} = c_1 + c_2 \frac{u}{1!} + \cdots + c_{n+1} \frac{u^n}{n!} + \cdots$$

und

$$\int_0^u \mathfrak{P}\, du = c_0 u + c_1 \frac{u^2}{2!} + \cdots + c_{n-1} \frac{u^n}{n!} + \cdots$$

ganzzahlige Reihen.

Die Division ist im Gebiete der ganzzahligen Reihen nicht unbeschränkt ausführbar, und hierauf gründet sich die Definition:

„Eine ganzzahlige Reihe $\mathfrak{P}_1$ heisst durch eine andere $\mathfrak{P}$ theilbar, wenn der Quotient $\frac{\mathfrak{P}_1}{\mathfrak{P}}$ ebenfalls eine ganzzahlige Reihe ist."

Die Theilbarkeit einer Reihe $\mathfrak{P}_1$ durch eine andere $\mathfrak{P}$ deute ich auch an durch die Congruenz

$$\mathfrak{P}_1 \equiv 0 \pmod{\mathfrak{P}},$$

und allgemeiner schreibe ich

$$\mathfrak{P}_1 \equiv \mathfrak{P}_2 \pmod{\mathfrak{P}},$$

wenn $\mathfrak{P}_1 - \mathfrak{P}_2$ durch $\mathfrak{P}$ theilbar ist.

Im Folgenden werde ich namentlich solche Congruenzen zu betrachten haben, deren Modul $\mathfrak{P}$ sich auf eine ganze nicht verschwindende Zahl m reducirt. Offenbar ist eine derartige Congruenz

$$\mathfrak{P} \equiv \mathfrak{P}_1 \pmod{m},$$

wo $\mathfrak{P}$ und $\mathfrak{P}_1$ die Reihen (1) und (2) bezeichnen mögen, völlig gleichbedeutend mit den unzählig vielen gewöhnlichen Congruenzen

$$c_n \equiv d_n \pmod{m} \qquad (n = 0, 1, 2, \ldots).$$

Wenn die ganzzahlige Reihe (1) Divisor jeder beliebigen ganzzahligen Reihe, also insbesondere auch Divisor der Zahl 1, sein soll, so ist

offenbar erforderlich, dass $c_0 = 1$ ist. Diese nothwendige Bedingung ist aber auch hinreichend, wie aus der Gleichung

$$\frac{1}{\mathfrak{P}(u)} = 1 + [1 - \mathfrak{P}(u)] + [1 - \mathfrak{P}(u)]^2 + \cdots$$

hervorgeht. In dem Gebiete der ganzzahligen Reihen spielen also diejenigen Reihen, welche sich für $u = 0$ auf 1 reduciren, die Rolle der Einheiten. Diese Reihen will ich deshalb „Einheitsreihen" nennen.

Von Wichtigkeit wird weiterhin der folgende

Satz I. *Ist $\mathfrak{P}$ eine ganzzahlige Reihe, die mit u verschwindet, also kein constantes Glied enthält, so ist für jede positive Zahl m*

$$\mathfrak{P}^m \equiv 0 \pmod{m!}. \tag{4}$$

Die Behauptung des Satzes, dass $\frac{1}{m!}\mathfrak{P}^m$ ganzzahlig ist, bedarf für $m = 1$ keines Beweises. Daher genügt es die Richtigkeit des Satzes nachzuweisen unter der Voraussetzung, dass der Satz schon für den Fall bewiesen sei, wo die Zahl $m - 1$ an die Stelle der Zahl m tritt. Nun ist aber

$$\frac{1}{m!}\mathfrak{P}^m = \int_0^u \frac{1}{(m-1)!}\mathfrak{P}^{m-1}\cdot\mathfrak{P}'\,du,$$

und da $\frac{1}{(m-1)!}\mathfrak{P}^{m-1}$ und $\mathfrak{P}'$ ganzzahlige Reihen sind, so folgt aus der vorstehenden Gleichung, dass $\frac{1}{m!}\mathfrak{P}^m$ ebenfalls ganzzahlig ist, w. z. b. w.

An den Satz I knüpft sich ein anderer, welcher ebenfalls Bezug hat auf die m^{te} Potenz einer ganzzahligen Reihe ohne constantes Glied. Es sei

$$\mathfrak{P} = c_1 u + c_2\frac{u^2}{2!} + \cdots + c_n\frac{u^n}{n!} + \cdots$$

eine solche Reihe und es werde

$$\mathfrak{P}^m \equiv C_m\frac{u^m}{m!} + C_{m+1}\frac{u^{m+1}}{(m+1)!} + \cdots + C_k\frac{u^k}{k!} + \cdots$$

gesetzt. Dann ist $\frac{C_m}{m!} = c_1^m$, $\frac{C_{m+1}}{(m+1)!} = m c_1^{m-1}\cdot\frac{c_2}{2!}$, u. s. w.; allgemein ist $\frac{C_k}{k!}$ eine ganze ganzzahlige Function von c_1 $\frac{c_2}{2!}, \cdots \frac{c_{k-m+1}}{(k-m+1)!}$ und folglich wird der Nenner von $\frac{C_k}{k!}$, wenn man diese Zahl auf die kleinste Benennung bringt, keinen Primfactor enthalten, der grösser ist als $k - m + 1$. Wenn daher $k!$ durch eine Primzahl $p > k - m + 1$ theilbar ist, so muss p nothwendig in C_k aufgehen. Somit gilt der

Satz II. *Wenn die Reihe*

$$C_m\frac{u^m}{m!} + C_{m+1}\frac{u^{m+1}}{(m+1)!} + \cdots + C_k\frac{u^k}{k!} + \cdots$$

die m^{te} Potenz einer ganzzahligen Reihe ist, so enthält C_k jede Primzahl als Factor, die zwischen $k - m + 1$ und $k + 1$ liegt.

Eine unmittelbare Folge des Satzes I ist der weitere Satz:

Setzt man in einer beliebigen ganzzahligen Reihe an Stelle von u eine andere ganzzahlige Reihe ohne constantes Glied und ordnet sodann nach Potenzen von u, so erhält man wiederum eine ganzzahlige Reihe.

Wenn beispielsweise $\mathfrak{P}(u)$ eine mit u verschwindende ganzzahlige Reihe ist, so wird die Entwickelung von $e^{\mathfrak{P}(u)}$ nach Potenzen von u eine ganzzahlige Reihe, und zwar offenbar eine Einheitsreihe sein. Ebenso ist die Entwickelung des Logarithmus einer Einheitsreihe eine ganzzahlige Reihe, und man erkennt hieraus, dass die aus der Function $e^{\mathfrak{P}(u)}$ entspringende Reihe die allgemeinste Einheitsreihe vorstellt. —

Man kann dieser ganzen Betrachtung eine andere, für manche Zwecke geeignetere Wendung geben, indem man an die Stelle der Potenzreihen die analytischen Functionen setzt, welche sie definiren. Dann hat man es offenbar mit dem Inbegriff derjenigen analytischen Functionen zu thun, welche an der Stelle $u = 0$ regulär sind und an dieser Stelle ebenso wie alle ihre Ableitungen ganzzahlige Werthe annehmen.

Von dieser Auffassung ausgehend, beweist man leicht noch die folgenden Sätze, welche ich hier anführe, weil sie weiterhin — freilich in speciellerer Form — zur Geltung kommen.

Erstens: Es sei $\varphi(u)$ eine analytische Function, welche an der Stelle $u = 0$ regulär ist und einer Differentialgleichung der Gestalt

$$\varphi^{(n)}(u) = G\left(\varphi(u),\ \varphi'(u),\ \ldots\ \varphi^{(n-1)}(u)\right) \tag{5}$$

genügt. Dabei soll G eine ganze rationale Function der eingeklammerten Argumente bedeuten mit Coefficienten, welche ganzzahlige Reihen sind. Wenn dann

$$\varphi(0),\ \varphi'(0),\ \ldots\ \varphi^{(n-1)}(0)$$

ganze Zahlen sind, so ist die Entwickelung von $\varphi(u)$ nach Potenzen von u eine ganzzahlige Reihe.

In der That ergiebt sich successive, indem man die Differentialgleichung (5) wiederholt nach u differenzirt, dass

$$\varphi^{(n)}(0),\ \varphi^{(n+1)}(0),\ \varphi^{(n+2)}(0),\ \ldots$$

sämmtlich ganze Zahlen sind*).

*) Der Satz gilt, falls $\varphi(0) = 0$ ist, auch dann noch, wenn die rechte Seite der Differentialgleichung (5) eine ganze rationale Function von

$$\varphi(u),\ \varphi'(u),\ \ldots\ \varphi^{(n-1)}(u)$$

der Gestalt

$$\sum A \frac{(\varphi)^r}{r!} (\varphi')^{r_1} \ldots (\varphi^{(n-1)})^{r_{n-1}}$$

ist, wobei die Coefficienten A ganzzahlige Reihen bedeuten.

Zweitens: Durch Umkehrung der Reihe

$$t = \mathfrak{P}(u) = u + c_2 \frac{u^2}{2!} + \cdots + c_n \frac{u^n}{n!} + \cdots$$

möge die Reihe

$$u = \mathfrak{P}_1(t) = t + d_2 \frac{t^2}{2!} + \cdots + d_n \frac{t^n}{n!} + \cdots$$

entstehen. Wenn nun $\mathfrak{P}(u)$ eine ganzzahlige Reihe ist, so gilt das Nämliche von der Reihe $\mathfrak{P}_1(t)$.

Es ist nämlich $\frac{d^n u}{dt^n} \cdot \left(\frac{dt}{du}\right)^{2n-1}$ eine ganze ganzzahlige Function von $\frac{dt}{du}, \frac{d^2t}{du^2}, \cdots \frac{d^n t}{du^n}$ und folglich (wie die Annahme $t = u = 0$ ergiebt) d_n eine ganzzahlige Function von $c_2, \ldots c_n$, woraus die Richtigkeit der Behauptung folgt.

Schliesslich bemerke ich noch, dass die vorstehenden Betrachtungen und Sätze ohne wesentliche Aenderung auch dann noch gelten, wenn man an die Stelle der „ganzzahligen" Reihen diejenigen Potenzreihen (1) treten lässt, für welche $c_0, c_1, c_2, \ldots$ complexe ganze Zahlen $a + ib$ im Gaussischen Sinne oder, noch allgemeiner, ganze algebraische Zahlen eines endlichen Zahlkörpers sind.

§ 2.

Die Zahlen E_n als Entwickelungscoefficienten.

Aus der Definitionsgleichung (D) der Zahlen E_n ist ersichtlich, dass diese Zahlen bei der Entwickelung der Weierstrass'schen Function

$$(6) \qquad \wp(u) = \frac{1}{u^2} + \sum \left\{ \frac{1}{(u-(r+is)\omega)^2} - \frac{1}{((r+is)\omega)^2} \right\}$$

nach aufsteigenden Potenzen von u zum Vorschein kommen werden. In der That ergiebt sich ohne Schwierigkeit, dass

$$(7) \quad \wp(u) = \frac{1}{u^2} + \frac{2^4 E_1}{4} \cdot \frac{u^2}{2!} + \frac{2^6 E_2}{8} \cdot \frac{u^6}{6!} + \cdots + \frac{2^{4n} E_n}{4n} \cdot \frac{u^{4n-2}}{(4n-2)!} + \cdots$$

ist. Durch die Substitution $x = \frac{1}{\sqrt{s}}$ erhält man für die reelle Periode ω die Darstellung

$$\omega = 2\int_0^1 \frac{dx}{\sqrt{1-x^4}} = 2\int_1^\infty \frac{ds}{\sqrt{4s^3-4s}}.$$

Folglich haben die Invarianten von $\wp(u)$ die Werthe

$$g_2 = 4, \quad g_3 = 0,$$

und die Differentialgleichung der Function $\wp(u)$ lautet daher:

$$\wp'^2(u) = 4\wp^3(u) - 4\wp(u). \tag{8}$$

Aus dieser Gleichung ergiebt sich zunächst in bekannter Weise eine Recursionsformel für die Zahlen $E_1, E_2, E_3, \ldots$. Man differenzire nämlich (8) nach u, wodurch man

$$\wp''(u) = 6\wp^2(u) - 2$$

findet; hierin setze man nach (7)

$$\wp(u) = \frac{1}{u^2} + \sum_1^\infty \frac{2^{4n} E_n}{4n} \cdot \frac{u^{4n-2}}{(4n-2)!},$$

$$\wp''(u) = \frac{6}{u^4} + \sum_1^\infty \frac{2^{4n} E_n}{4n} \cdot \frac{u^{4n-4}}{(4n-4)!}.$$

Der Vergleich der Coefficienten der einzelnen Potenzen von u ergiebt dann

$$E_1 = \frac{1}{10}$$

und

$$(2n-3)(4n-1)(4n+1)E_n = 3\sum_{r+s=n} (4r-1)(4s-1)(4n)_{4r} \cdot E_r E_s \tag{9}$$

$$(n = 2, 3, 4, \ldots)$$

wobei die Summation auf alle positiven Zahlen r, s auszudehnen ist, welche der Bedingung $r + s = n$ genügen. Unter $(4n)_{4r}$ ist der $4r^{\text{te}}$ Binomialcoefficient zur Basis $4n$ zu verstehen.

Aus der Formel (9) geht hervor, dass die Zahlen E_n positive, reelle rationale Zahlen sind. Am Schlusse dieser Arbeit findet man eine Tabelle der Zahlen E_n, die ich auf Grund der Formel (9) hergestellt habe.

§ 3.

Die Function $\varphi(u)$.

Die Function

$$\varphi(u) = \sqrt{\frac{1}{\wp(u)}} = u + k_1 \frac{u^5}{5!} + k_2 \frac{u^9}{9!} + \cdots + k_n \frac{u^{4n+1}}{(4n+1)!} + \cdots \tag{10}$$

befriedigt die Differentialgleichung

$$\varphi'^2(u) = 1 - \varphi^4(u). \tag{11}$$

Sie ist diejenige eindeutige doppeltperiodische Function, welche Eisenstein seinen Untersuchungen über die biquadratischen Reste zu Grunde gelegt hat*). Die Werthe

*) Eisenstein, Beiträge zur Theorie der elliptischen Functionen I. (Crelle's Journal, Bd. 30 oder Mathematische Abhandlungen, Berlin 1847, pag. 129.)

$$2\omega, \quad (1+i)\omega$$

bilden ein Paar primitiver Perioden von $\varphi(u)$. Das Additionstheorem dieser Function spricht sich in der Gleichung aus:

$$\varphi(u+v) = \frac{\varphi(u)\,\varphi'(v) + \varphi(v)\,\varphi'(u)}{1+\varphi^2(u)\,\varphi^2(v)}. \tag{12}$$

Ferner geht aus (10) hervor, dass

$$\varphi(iu) = i\varphi(u) \tag{13}$$

ist. Durch Differentiation von (11) ergiebt sich

$$\varphi''(u) = -2\varphi^3(u), \tag{14}$$

und diese Differentialgleichung hat die Gestalt (5) in § 1. Daraus folgt, dass die Entwickelungscoefficienten

$$k_0 = 1,\ k_1,\ k_2, \ldots k_n, \ldots$$

der Function $\varphi(u)$ sämmtlich reelle ganze Zahlen sind.

Bemerkenswerth und für die weiteren Untersuchungen wichtig ist die Thatsache, dass sich die Entwickelungscoefficienten der Functionen $\frac{1}{\varphi(u)}$ und $\frac{1}{2}\varphi^2(u)$ in einfacher Weise durch die Zahlen E_n ausdrücken lassen. Die Entwickelungen dieser Functionen will ich in folgender Form ansetzen:

$$\sqrt{\varphi(u)} = \frac{1}{\varphi(u)} = \frac{1}{u} + \frac{F_1}{4}\cdot\frac{u^3}{3!} + \frac{F_2}{8}\cdot\frac{u^7}{7!} + \cdots + \frac{F_n}{4n}\frac{u^{4n-1}}{(4n-1)!} + \cdots, \tag{15}$$

$$\frac{1}{2\varphi(u)} = \frac{1}{2}\varphi^2(u) = e_0\frac{u^2}{2!} + e_1\frac{u^6}{6!} + e_2\cdot\frac{u^{10}}{10!} + \cdots + e_n\frac{u^{4n+2}}{(4n+2)!} + \cdots. \tag{16}$$

Um die Entwickelungscoefficienten F_n, e_n durch die Zahlen E_n auszudrücken, gehe ich aus von der Gleichung

$$\frac{1+i}{\varphi\left((1+i)u\right)} = \frac{\varphi'(u)}{\varphi(u)}, \tag{17}$$

welche aus (12) und (13) leicht folgt. Durch Quadrirung von (17) ergiebt sich

$$2i\wp\left((1+i)\,u\right) = \frac{1}{\varphi^2(u)} - \varphi^2(u) = \wp(u) - \varphi^2(u),$$

oder

$$\frac{1}{2}\varphi^2(u) = \frac{1}{2}\wp(u) - i\wp\left(1+i)u\right). \tag{18}$$

Benutzt man nun die Gleichung (7), so folgt:

$$e_{n-1} = 2^{4n-1}\left(1-(1+i)^{4n}\right)\frac{E_n}{4n}, \qquad (n=1,2,3\ldots) \tag{19}$$

wobei man beachten möge, dass $(1+i)^{4n}$ reell, nämlich $=(-4)^n$ ist.

Andererseits erhält man durch Differentiation aus (17)

$$\frac{d}{du}\left(\frac{1}{\varphi\left((1+i)u\right)}\right) = \frac{1}{1+i}\,\frac{\varphi\varphi'' - \varphi'^2}{\varphi^2} = -\frac{1}{1+i}\left(\frac{1}{\varphi^2} + \varphi^2\right)$$

oder, wenn man u durch $\frac{u}{1+i}$ ersetzt und (18) berücksichtigt,

$$\frac{d}{du}\left(\frac{1}{\varphi(u)}\right) = -\frac{1}{(1+i)^2}\left(2\varphi\left(\frac{u}{1+i}\right) - 2i\varphi(u)\right),$$

und endlich

$$\frac{1}{\varphi(u)} = \int\left\{\varphi(u) + i\varphi\left(\frac{u}{1+i}\right)\right\} du. \tag{20}$$

Hieraus folgt nun

$$F_n = (1+i)^{4n}\left[(1+i)^{4n} - 2\right] E_n. \qquad (n = 1, 2, 3, \ldots) \tag{21}$$

§ 4.

Die complexe Multiplication für die Function $\varphi(u)$.

Die Function $\varphi(u)$ lässt bekanntlich „complexe Multiplication" zu. Die hierauf bezüglichen Sätze stelle ich, soweit sie im Folgenden Anwendung finden, in diesem Paragraphen zusammen*). Es bezeichne $m = a + ib$ eine complexe ganze Zahl, die ungerade, d. h. durch $1 + i$ nicht theilbar ist. Ueberdies sei m primär, d. h. m genüge der Congruenz

$$m = a + ib \equiv 1 \pmod{2 + 2i}.$$

(Unter vier associirten ungeraden Zahlen m, $-m$, im, $-im$ ist stets eine und nur eine primär). Die Function $\varphi(mu)$ ist nun, wie aus functionentheoretischen Gründen unmittelbar folgt, rational durch $\varphi(u)$ darstellbar. Und zwar hat man, wenn zur Abkürzung

$$\varphi(mu) = y, \qquad \varphi(u) = x \tag{22}$$

gesetzt wird,

$$y = \frac{mx + a_1x^5 + a_2x^9 + \cdots + x^\mu}{1 + b_1x^4 + b_2x^8 + \cdots + mx^{\mu-1}} = \frac{U(x)}{V(x)}. \tag{23}$$

Der Grad μ des Zählers $U(x)$ ist die Norm der Zahl m, also

$$\mu = a^2 + b^2.$$

Ferner sind die Coefficienten $a_1, a_2, \ldots b_1, b_2, \ldots$ sämmtlich complexe ganze Zahlen. Zwischen ihnen besteht zunächst die Beziehung, dass die Coefficienten von $U(x)$ in umgekehrter Ordnung geschrieben genau mit den Coefficienten von $V(x)$ übereinstimmen, so dass

$$V(x) = x^\mu U\left(\frac{1}{x}\right)$$

*) Vgl. wegen dieser Sätze: Eisenstein, l. c.

ist. Sodann sind diese Coefficienten so beschaffen, dass die ganze Function

$$D(x) = V(x)\,U'(x) - U(x)\,V'(x) \tag{24}$$

lauter durch m theilbare Coefficienten besitzt.

Setzt man

$$U(x) = \sum_{k=0,1,2,\cdots} a_k x^{4k+1}, \quad V(x) = \sum_{k=0,1,2,\cdots} b_k x^{4k}, \qquad (a_0 = m,\ b_0 = 1)$$

so ergiebt sich nach kurzer Rechnung

$$D(x) = \sum_{k,h} (4h - 4k + 1)\, a_h b_k x^{4(k+h)} = \sum_{r=0,1,2,\cdots} c_r x^{4r}.$$

Die Coefficienten von $D(x)$ haben also der Reihe nach die Werthe

$$\begin{aligned}
c_0 &= a_0 = m,\\
c_1 &= 5a_1 - 3a_0 b_1,\\
c_2 &= 9a_2 + a_1 b_1 - 7a_0 b_2,\\
c_3 &= 13a_3 + 5a_2 b_1 - 3a_1 b_2 - 11a_0 b_3,\\
&\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\\
c_r &= (4r+1)a_r + (4r-7)a_{r-1}b_1 + \cdots + (-4r+1)a_0 b_r.\\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

Wenn nun m eine zweigliedrige complexe Primzahl ist, so wird $\mu = N(m)$ eine reelle Primzahl von der Form $4k+1$. In diesem Falle ist keine der Zahlen 5, 9, 13, ... $\mu - 4$ durch m theilbar. Daher folgt aus der Thatsache, dass $c_0, c_1, c_2, \ldots$ durch m theilbar sind, successive $a_1 \equiv 0$, $a_2 \equiv 0$, $a_3 \equiv 0, \ldots a_{\frac{\mu-5}{4}} \equiv 0 \pmod{m}$. D. h. es sind alle Coefficienten des Zählers mit Ausnahme des Coefficienten von x^μ, welcher gleich 1 ist, durch m theilbar.

Wenn zweitens $m = -q$ ist, wo q eine reelle Primzahl von der Form $4k+3$ bezeichnet, so ist die erste Zahl der Reihe 5, 9, 13, ..., welche durch m theilbar ist, offenbar gleich $3q$. In diesem Falle sind also wenigstens die ersten $\frac{3q-1}{4}$ Coefficienten des Zählers $U(x)$, nämlich

$$a_0,\ a_1,\ a_2, \ldots a_{\frac{3q-5}{4}}$$

durch $m = -q$ theilbar.

§ 5.

Der Nenner der Zahl E_n.

Die Zahl E_n ist eine reelle positive rationale Zahl und lässt sich also auf die Form bringen

$$E_n = \frac{Z_n}{N_n}, \tag{25}$$

wo Z_n, N_n positive ganze Zahlen ohne gemeinsamen Theiler sind.

Mit den bisher entwickelten Hülfsmitteln gelingt es nun, Näheres über die Primfactoren des Nenners N_n festzustellen.

Zu diesem Zwecke betrachte ich die Function

$$F(u) = m^2 \wp(mu) - \wp(u) = \frac{m^2}{\varphi^2(mu)} - \frac{1}{\varphi^2(u)}, \tag{26}$$

wobei m eine ungerade primäre complexe ganze Zahl bedeutet. Die Entwickelung dieser Function nach aufsteigenden Potenzen von u lautet:

$$F(u) = \sum_1^\infty 2^{4n}(m^{4n}-1)\frac{E_n}{4n}\frac{u^{4n-2}}{(4n-2)!}. \tag{27}$$

Andererseits ist nach dem vorigen Paragraphen:

$$F(u) = \frac{m^2 V^2(x)}{U^2(x)} - \frac{1}{x^2} = \frac{[mV(x)x - U(x)][mV(x)x + U(x)]}{x^2 U^2(x)} \tag{28}$$

$$= \frac{[(mb_1 - a_1)x^2 + (mb_2 - a_2)x^6 + \cdots][2m + (mb_1 + a_1)x^4 + (mb_2 + a_2)x^8 + \cdots]}{[m + a_1 x^4 + a_2 x^8 + \cdots + x^{\mu-1}]^2}.$$

Ersetzt man in dieser Gleichung u durch mu, so geht

$$x = \varphi(u) = u + k_1\frac{u^5}{5!} + k_2\frac{u^9}{9!} + \cdots$$

in eine durch m theilbare ganzzahlige Reihe über. Dasselbe gilt von allen Potenzen von x, so dass die Gleichung (28), nachdem man Zähler und Nenner rechts durch m^2 dividirt hat, die Form erhält

$$F(mu) = \frac{\mathfrak{P}_1(u)}{\mathfrak{P}_2(u)},$$

wo $\mathfrak{P}_1(u)$ und $\mathfrak{P}_2(u)$ ganzzahlige Reihen sind, von denen die letztere das Anfangsglied 1 besitzt, also eine Einheitsreihe ist. Folglich ist $F(mu)$ selbst eine ganzzahlige Reihe. Man erkennt somit:

Wenn m eine ungerade complexe ganze Zahl bezeichnet, so ist

$$(2m)^{4n-2}(m^{4n}-1)\frac{E_n}{n} = G_{m,n} \tag{29}$$

eine ganze Zahl.

Die beim Beweise gemachte Voraussetzung, dass m primär sei, darf unterdrückt werden, weil die linke Seite von (29) höchstens das Vorzeichen ändert, wenn man m durch eine associirte Zahl $i^s . m$ ersetzt.

Für den Fall, wo $m = -q$ ist, unter q eine Primzahl der Form $4k+3$ verstanden, lässt sich der vorstehende Satz noch wesentlich verschärfen. Auf der rechten Seite der Gleichung (28) ist dann nämlich im Nenner

$$m + a_1 x^4 + a_2 x^8 + \cdots + x^{\mu-1}$$

eine durch m theilbare ganzzahlige Reihe. In der That sind die Coefficienten

$$a_1, a_2, \ldots, a_{\frac{3q-5}{4}}$$

durch m theilbar und die Glieder $a_r x^{4r}$, in welchen $r \geqq \frac{3q-1}{4}$, also $4r$ sicher $> q$ ist, sind ebenfalls durch m theilbar, weil $\frac{x^{4r}}{(4r)!}$ nach § 1 eine ganzzahlige Reihe ist und $(4r)!$ den Factor q mindestens ein Mal enthält. Aus entsprechenden Gründen ist jeder Factor im Zähler auf der rechten Seite der Gleichung (28) eine durch m theilbare ganzzahlige Reihe. Hieraus folgt nun, dass in dem jetzt betrachteten Falle schon $F(u)$ eine ganzzahlige Reihe ist, oder:

Wenn q eine reelle Primzahl von der Form $4k+3$ bezeichnet, so ist

$$2^{4n}(q^{4n}-1) \cdot \frac{E_n}{4n} = H_{q,n} \tag{30}$$

eine ganze Zahl.

Aus dieser Thatsache geht zunächst hervor, dass der Nenner von E_n eine Primzahl q von der Form $4k+3$ nicht als Factor enthalten kann. Denn aus der Gleichung

$$E_n = \frac{n H_{q,n}}{2^{4n-2}(q^{4n}-1)}$$

ist ersichtlich, dass $2^{4n-2}(q^{4n}-1)$ ein Multiplum des Nenners N_n ist. Wäre also N_n durch q theilbar, so müsste auch $2^{4n-2}(q^{4n}-1)$ durch q theilbar sein, was aber offenbar nicht der Fall ist.

Die Annahme, p sei eine Primzahl von der Form $4k+1$, welche im Nenner N_n von E_n aufgeht, zieht folgende Consequenzen nach sich. Es sei p^α die höchste Potenz von p, welche in N_n enthalten ist, so dass $\alpha \geqq 1$ sein wird; ferner sei $p^{\alpha'}$ die höchste Potenz von p, welche in n aufgeht, wobei $\alpha' \geqq 0$. Aus der Gleichung (29) folgt nun

$$(2m)^{4n-2}(m^{4n}-1) Z_n = n N_n G_{m,n} \equiv 0 \pmod{p^{\alpha+\alpha'}}. \tag{31}$$

Hier wähle ich für m eine ungerade Primitivwurzel (mod. $p^{\alpha+\alpha'}$), also eine solche ungerade (reelle) ganze Zahl, für welche keine niedrigere Potenz als die mit dem Exponenten

$$\varphi(p^{\alpha+\alpha'}) = p^{\alpha+\alpha'-1}(p-1)$$

congruent 1 (mod. $p^{\alpha+\alpha'}$) ist. Da die Factoren $(2m)^{4n-2}$ und Z_n theilerfremd zu p sind (denn Z_n und N_n haben keinen gemeinsamen Theiler), so folgt aus (31)

$$m^{4n} - 1 \equiv 0 \pmod{p^{\alpha+\alpha'}}$$

und daher

$$4n = M \cdot p^{\alpha+\alpha'-1}(p-1), \tag{32}$$

wo M eine ganze Zahl bezeichnet. Die höchste Potenz von p, welche $4n$ theilt, ist aber $p^{\alpha'}$; folglich ist $\alpha = 1$. Ferner zeigt die Gleichung (32), dass $4n$ durch $p-1$ theilbar ist.

Die Resultate dieses Paragraphen fasse ich in folgenden Satz zusammen:

„Jede ungerade Primzahl p, welche im Nenner der Zahl E_n aufgeht, ist nothwendig von der Form $4k+1$ und so beschaffen, dass $p-1$ ein Divisor von $4n$ ist; sie kann ferner nur in erster, nicht in höherer Potenz im Nenner von E_n aufgehen."

§ 6.

Erster Ansatz zur Partialbruchzerlegung der Zahl E_n.

Bezeichnet p eine Primzahl, welche im Nenner einer rationalen Zahl R entweder gar nicht oder nur in der ersten Potenz enthalten ist, so kann man die ganze Zahl ε so bestimmen, dass der Nenner der Zahl

$$R - \frac{\varepsilon}{p}$$

den Primfactor p sicher nicht enthält. Die Zahl ε ist (mod. p) völlig bestimmt; sie ist $\equiv 0 \pmod{p}$, wenn der Nenner von R nicht durch p theilbar ist; andernfalls ist ε incongruent 0 (mod. p).

Die Anwendung dieser Bemerkung auf die Zahl $R = E_n$ führt zunächst zu folgendem Ergebniss: Aus den Divisoren $\delta, \delta', \delta'', \ldots$ der Zahl n bilde man die Zahlen

$$4\delta + 1,\ 4\delta' + 1,\ 4\delta'' + 1,\ \ldots \tag{33}$$

und bezeichne diejenigen unter ihnen, welche Primzahlen sind, mit

$$p_1, p_2, \ldots, p_r. \tag{34}$$

Dann hat die Partialbruchzerlegung von E_n jedenfalls die Gestalt

$$E_n = G + \frac{\varepsilon_0}{2^\alpha} + \frac{\varepsilon_1}{p_1} + \frac{\varepsilon_2}{p_2} + \cdots + \frac{\varepsilon_r}{p_r} = G + \frac{\varepsilon_0}{2^\alpha} + \sum \frac{\varepsilon}{p}, \tag{35}$$

wo G eine ganze Zahl, 2^α die höchste Potenz von 2, welche im Nenner von E_n aufgeht, und $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ ganze Zahlen bezeichnen.

Die nähere Bestimmung der Zähler $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ ist nun das Ziel dieses und der beiden folgenden Paragraphen.

Es bedeute p irgend eine der Primzahlen $p_1, p_2 \ldots p_r$ und es sei ε der zugehörige Zähler.

Die Primzahl p zerlege man in ihre primäre complexe Primfactoren

$$p = m \cdot m' = (a + ib)(a - ib) \tag{36}$$

und multiplicire dann die Gleichung (35) mit m. Man erkennt so, dass nach dem Modul m die Congruenz gilt*)

$$mE_n \equiv \frac{\varepsilon}{m'} \equiv \frac{\varepsilon}{m' + m} \equiv \frac{\varepsilon}{2a} \pmod{m}, \tag{37}$$

die nun zur näheren Bestimmung des Zählers ε dienen wird.

Die Gleichung (23), in welcher

$$\mu = N(m) = a^2 + b^2 = p$$

zu setzen ist, ergiebt, in Rücksicht darauf, dass die Coefficienten $a_1, a_2, \ldots, b_1, b_2, \ldots$ sämmtlich durch m theilbar sind, die Congruenz:

$$\frac{y}{x} = \varphi(mu) \cdot \frac{1}{\varphi(u)} \equiv \varphi^{p-1}(u) \equiv -\frac{1}{(p-1)!}\varphi^{p-1}(u) \pmod{m}, \tag{38}$$

wobei von dem Wilson'schen Satze $(p-1)! \equiv -1 \pmod{m}$ Gebrauch gemacht ist. Die linke Seite der vorstehenden Congruenz entwickele ich nach Potenzen von u, indem ich nach (10) und (15)

$$\varphi(mu) = mu + \sum_1^\infty m^{4n+1} k_n \frac{u^{4n+1}}{(4n+1)!},$$

$$\frac{1}{\varphi(u)} = \frac{1}{u} + \sum_1^\infty \frac{F_n}{4n} \frac{u^{4n-1}}{(4n-1)!}$$

setze. In dem Producte dieser beiden Reihen ist der Coefficient von $\frac{u^{4n}}{(4n)!}$ gleich

$$\begin{aligned} &mF_n + k_1 \frac{m^5}{5}(4n)_4 F_{n-1} + k_2 \frac{m^9}{9}(4n)_8 F_{n-2} + \cdots \\ &\cdots + k_{n-1} \frac{m^{4n-3}}{4n-3}(4n)_{4n-4} F_1 + k_n \cdot \frac{m^{4n+1}}{4n+1}. \end{aligned} \tag{39}$$

Hier sind nun alle Glieder vom zweiten ab congruent 0 (mod. m). Denn in dem Producte

$$k_r \frac{m^{4r+1}}{(4r+1)}(4n)_{4r} F_{n-r}$$

$$= k_r \cdot (4n)_{4r} \cdot \frac{m^{4r}}{(4r+1)} \cdot mE_{n-r}(1+i)^{4(n-r)}\left((1+i)^{4(n-r)} - 2\right)$$

*) Die Congruenz $r \equiv s \pmod{m}$, in welcher r und s rationale Zahlen bezeichnen, bedeutet, dass die Differenz $r - s$ einen durch m theilbaren Zähler besitzt, vorausgesetzt, dass diese Differenz auf die Form eines Bruches gebracht ist, dessen Zähler und Nenner theilerfremd sind.

enthält mE_{n-r} sicher nicht den Factor m im Nenner, und $\frac{m^{4r}}{(4r+1)}$ enthält in reducirter Form den Factor m mindestens ein Mal im Zähler. Anderenfalls würde nämlich m^{4r} ohne Rest in $4r+1$ aufgehen müssen, also auch p^{4r} ohne Rest in $4r+1$, während doch

$$p^{4r} \geqq 5^{4r} = (1+4)^{4r} > 1 + 16r$$

ist.

Die Zahl (39) ist also nach dem Modul m congruent

$$mF_n = m(1+i)^{4n}\left((1+i)^{4n} - 2\right)E_n.$$

Da nun $4n$ Multiplum von $p-1$ ist, so hat man nach dem Fermat'schen Satze $(1+i)^{4n} \equiv 1 \pmod{m}$ und folglich

$$mF_n \equiv -mE_n \pmod{m}.$$

Die Congruenz (38) besagt nun, dass der Coefficient von $\frac{u^{4n}}{(4n)!}$ in der Entwickelung von $\frac{\varphi(mu)}{\varphi(u)} \pmod{m}$ denselben Werth hat, wie der entsprechende Coefficient in der Entwickelung von $-\frac{1}{(p-1)!}\varphi^{p-1}(u)$. Bezeichnet also $-c_n$ diesen letzteren Coefficienten, so ist

$$mE_n \equiv c_n \pmod{m},$$

folglich nach (37)

$$\varepsilon \equiv (2a) \cdot c_n \pmod{m}$$

und da beide Seiten dieser Congruenz reell sind, so gilt die nämliche Congruenz auch (mod. p). Hiermit ist folgender Satz bewiesen:

Ist $\frac{\varepsilon}{p}$ irgend einer der Brüche, welche in der Partialbruchzerlegung (35) *der Zahl E_n auftreten, so gilt die Congruenz*

(40) $$\varepsilon \equiv 2a \cdot c_n \pmod{p}.$$

Dabei bedeutet a den reellen Theil des primären complexen Primfactors $m = a + ib$ der Zahl p und c_n den Coefficienten von $\frac{u^{4n}}{(4n)!}$ in der Entwickelung der Function

$$\frac{1}{(p-1)!}\varphi^{p-1}(u).$$

§ 7.

Entwickelung der Ableitungen von $\varphi^2(u)$ nach den Potenzen von $\varphi^2(u)$.

Die Bestimmung der Reihe $\frac{1}{(p-1)!}\varphi^{p-1}(u) \pmod{p}$ gelingt nun vermöge derjenigen Gleichungen, welche die Potenzen von $\varphi^2(u)$ durch die Differentialquotienten von $\varphi^2(u)$ ausdrücken und umgekehrt diese durch jene.

Die gemeinsame Quelle dieser Gleichungen (deren Existenz übrigens auch aus allgemeinen functionentheoretischen Gründen folgt) bildet

das Additionstheorem (12) der Function $\varphi(u)$. Aus diesem ergiebt sich zunächst, wenn zur Abkürzung

$$\varphi^2(u) = z, \qquad \varphi^2(v) = t \tag{41}$$

gesetzt wird,

$$\begin{aligned} &\frac{1}{2}\left[\varphi^2(u+v) + \varphi^2(u-v)\right] \\ &= \frac{[\varphi(u)\varphi'(v) + \varphi'(u)\varphi(v)]^2 + [\varphi(u)\varphi'(v) - \varphi'(u)\varphi(v)]^2}{2.[1+\varphi^2(u)\varphi^2(v)]^2} \\ &= \frac{(z+t)(1-zt)}{(1+zt)^2}. \end{aligned} \tag{42}$$

Entwickelt man hier die linke Seite nach Potenzen von v, die rechte Seite nach Potenzen von z, so kommt

$$\sum_{r=0}^{\infty} \frac{d^{2r}z}{du^{2r}} \frac{v^{2r}}{(2r)!} = t + \sum_{r=1}^{\infty} (-1)^r \left\{(2r+1)t^{r+1} - (2r-1)t^{r-1}\right\} z^r,$$

oder, indem man berücksichtigt, dass

$$\frac{d^2\varphi^{2r}(v)}{dv^2} = 2r(2r-1)\varphi^{2r-2}(v) - 2r(2r+1)\varphi^{2r+2}(v),$$

also

$$\frac{d^2t^r}{dv^2} = -2r[(2r+1)t^{r+1} - (2r-1)t^{r-1}]$$

ist,

$$\sum_{r=0}^{\infty} \frac{d^{2r}z}{du^{2r}} \frac{v^{2r}}{(2r)!} = t + \sum_{r=1}^{\infty} (-1)^{r+1} \cdot \frac{z^r}{2r} \cdot \frac{d^2t^r}{dv^2}. \tag{43}$$

Differentiirt man nun endlich diese Gleichung $2n$ Mal nach v und setzt sodann $v = 0$, so ergiebt sich die gewünschte Darstellung der $2n^{\text{ten}}$ Ableitung von $z = \varphi^2(u)$ durch die Potenzen von z, nämlich:

$$\frac{d^{2n}z}{du^{2n}} = \left(\frac{d^{2n}t}{dv^{2n}}\right)_{v=0} + \sum_{r=1,2,\cdots} (-1)^{r+1} \cdot \frac{z^r}{2r} \left(\frac{d^{2n+2}(t^r)}{dv^{2n+2}}\right)_{v=0}. \tag{44}$$

Zur Vereinfachung führe ich hier die Entwickelungscoefficienten der Potenzen von $t = \varphi^2(v)$ ein, indem ich setze:

$$t^r = \varphi^{2r}(v) = \varepsilon_{2r}^{(2r)} \frac{v^{2r}}{(2r)!} + \varepsilon_{2r+4}^{(2r)} \frac{v^{2r+4}}{(2r+4)!} + \cdots + \varepsilon_{2k}^{(2r)} \frac{v^{2k}}{(2k)!} + \cdots. \tag{45}$$

Diese Entwickelung enthält nur solche Potenzen von v, deren Exponenten $\equiv 2r \pmod 4$ und $\geq 2r$ sind; es ist daher

$$\varepsilon_{2k}^{(2r)} = 0,$$

wenn r nicht $\equiv k \pmod 2$ ist und ebenso, wenn $r > k$ ist.

Die Gleichung (44) nimmt nun folgende definitive Gestalt an:

$$(46) \qquad \frac{d^{2n}\varphi^2(u)}{du^{2n}} = \varepsilon_{2n}^{(2)} + \sum_{r=1,2,\cdots} (-1)^{r+1} \cdot (2r-1)!\, \varepsilon_{2n+2}^{(2r)} \frac{\varphi^{2r}(u)}{(2r)!}.$$

Die Summe braucht man hier nur auszudehnen auf diejenigen Werthe von r, welche $\equiv n+1 \pmod 2$ und überdies $\leqq n+1$ sind; denn alle übrigen Glieder der Summe verschwinden.

Nach Satz I in § 1 ist $\frac{\varphi^{2r}(u)}{(2r)!}$ eine ganzzahlige Reihe; ferner ist nach Satz II in § 1 die Zahl $\varepsilon_{2n+2}^{(2r)}$ durch jede Primzahl theilbar, die zwischen $2n-2r+3$ und $2n+3$ liegt.

Wenn also $2n+1$, wie ich jetzt voraussetzen will, eine Primzahl ist, so wird $\varepsilon_{2n+2}^{(2r)}$ durch $2n+1$ theilbar sein, sobald $r \geqq 2$ ist. Daher gilt dann die Congruenz

$$\frac{d^{2n}\varphi^2(u)}{du^{2n}} \equiv \varepsilon_{2n}^{(2)} + \varepsilon_{2n+2}^{(2)} \frac{\varphi^2(u)}{2} \pmod{2n+1}.$$

Der Gleichung (16) zufolge ist $\varepsilon_{2k}^{(2)} = 0$, wenn k gerade und $\varepsilon_{2k}^{(2)} = 2 \cdot e_{\frac{k-1}{2}}$, wenn k ungerade. Unterscheidet man also die beiden Fälle, wo $2n+1 = p$ eine Primzahl der Form $4k+1$ und wo $2n+1 = q$ eine Primzahl von der Form $4k+3$ ist, von einander, so lautet die vorstehende Congruenz im ersten Falle:

$$(47) \qquad \frac{d^{p-1}\varphi^2(u)}{du^{p-1}} \equiv e_{\frac{p-1}{4}} \cdot \varphi^2(u) \pmod p$$

und im zweiten Falle

$$(48) \qquad \frac{d^{q-1}\varphi^2(u)}{du^{q-1}} \equiv 2 \cdot e_{\frac{q-3}{4}} \pmod q.$$

Die r-malige Differentiation dieser Congruenzen führt zu den weiteren:

$$(47') \qquad \frac{d^{p-1+r}\varphi^2(u)}{du^{p-1+r}} \equiv e_{\frac{p-1}{4}} \frac{d^r\varphi^2(u)}{du^r} \pmod p,$$

$$(48') \qquad \frac{d^{q-1+r}\varphi^2(u)}{du^{q-1+r}} \equiv 0 \pmod q.$$

Diese Congruenzen gelten für jeden positiven (ganzzahligen) Werth von r; die Congruenz (47') auch noch für $r = 0$, in welchem Falle sie mit (47) zusammenfällt.

§ 8.

Entwickelung der Potenzen von $\varphi^2(u)$ nach den Ableitungen von $\varphi^2(u)$.

Die Gleichungen, welche die Potenzen von $z = \varphi^2(u)$ durch die Ableitungen dieser Function darstellen, sind die Umkehrungen der Gleichungen (46). Man erhält sie in expliciter Form vermöge der Gleichung (43) auf folgende Weise. Man setze

$$t = \tau^2,$$

so dass (nach (10))

$$(49) \qquad \tau = \varphi(v) = v + k_1 \frac{v^5}{5!} + \cdots + k_n \frac{v^{4n+1}}{(4n+1)!} + \cdots$$

ist. Integrirt man sodann die beiden Seiten der Gleichung (43) zwei Mal zwischen den Grenzen 0 und v, so ergiebt sich zunächst

$$(50) \qquad \sum_{r=0}^{\infty} \frac{d^{2r}z}{du^{2r}} \cdot \frac{v^{2r+2}}{(2r+2)!} = \int_0^v dv \cdot \int_0^v \tau^2 dv + \sum_{r=1}^{\infty} (-1)^{r+1} \frac{z^r}{2r} \cdot \tau^{2r}.$$

Durch Umkehrung der Gleichung (49) lässt sich nun v in eine nach Potenzen von τ fortschreitende Reihe entwickeln und diese Reihe ist nach § 1 ganzzahlig*). Daher hat man für jeden positiven ganzzahligen Werth von r:

$$(51) \qquad \frac{v^{2r}}{(2r)!} = \eta_{2r}^{(2r)} \cdot \frac{\tau^{2r}}{(2r)!} + \eta_{2r+4}^{(2r)} \frac{\tau^{2r+4}}{(2r+4)!} + \cdots + \eta_{2k}^{(2r)} \frac{\tau^{2k}}{(2k)!} + \cdots,$$

wo die Entwickelungscoefficienten $\eta_{2k}^{(2r)}$ ganze Zahlen sind. Analog wie bei der Reihe (45) ist auch hier

$$\eta_{2k}^{(2r)} = 0,$$

wenn r nicht $\equiv k \pmod 2$, oder wenn $r > k$ ist.

Entwickelt man nun in der Gleichung (50) Alles nach Potenzen von τ und vergleicht sodann die Coefficienten von τ^{2n} so ergiebt sich

$$(52) \qquad (-1)^{n+1} \cdot \frac{z^n}{2n} = \sum_{r=0,1,2,\cdots} \frac{\eta_{2n}^{(2r+2)}}{(2n)!} \frac{d^{2r}z}{du^{2r}} - A_{2n},$$

wobei A_{2n} den Coefficienten von τ^{2n} in der Entwickelung

$$\int_0^v dv \int_0^v \tau^2 dv = A_2\tau^2 + A_4\tau^4 + \cdots + A_{2n}\tau^{2n} + \cdots$$

*) Die betreffende Reihe ist die folgende:

$$v = \int_0^\tau \frac{d\tau}{\sqrt{1-\tau^4}} = \tau + \frac{1}{2} \cdot 4! \frac{\tau^5}{5!} + \cdots + \frac{1.3.5\ldots 2n-1}{2.4.6\ldots 4n} \cdot (4n)! \frac{\tau^{4n+1}}{(4n+1)!} + \cdots.$$

bedeutet. Um den Werth von A_{2n} zu bestimmen, differenzire ich vorstehende Gleichung zwei Mal nach v; hierdurch entsteht

$$\tau^2 = -A_2(2.3\tau^4 - 2.1) - A_4(4.5\tau^6 - 4.3\tau^2) - \cdots$$
$$\cdots - A_{2n}\left(2n(2n+1)\tau^{2n+2} - 2n(2n-1)\tau^{2n-2}\right) - \cdots$$

und durch Coefficientenvergleichung findet sich nun leicht

$$A_{2n} = 0 \quad \text{oder} \quad A_{2n} = \frac{1.5.9\ldots(2n-3)}{3.7.11\ldots(2n-1)} \cdot \frac{1}{2n}$$

je nachdem n ungerade oder gerade ist. Demnach nimmt nun die Gleichung (52), mit Unterscheidung der Fälle n gerade und n ungerade, die folgende definitive Form an:

Es ist

$$(53)\quad \varphi^{2n}(u) = \frac{-1}{(2n-1)!} \sum_{r=1,2,\cdots} \eta_{2n}^{(2r)} \frac{d^{2r-2}\varphi^2(u)}{du^{2r-2}} + \frac{1.5.9\ldots(2n-3)}{3.7.11\ldots(2n-1)},$$

wenn n gerade ist; dagegen

$$(54)\qquad \varphi^{2n}(u) = \frac{1}{(2n-1)!} \sum_{r=1,2,\cdots} \eta_{2n}^{(2r)} \frac{d^{2r-2}\varphi^2(u)}{du^{2r-2}},$$

wenn n ungerade ist.

Vermöge dieser Gleichungen lässt sich das Ergebnis des vorigen Paragraphen erheblich verallgemeinern.

Sei zunächst p eine Primzahl von der Form $4k+1$. Die in (53) und (54) auftretende Zahl n werde der Bedingung $2n < p$ unterworfen, so dass $(2n-1)!$ theilerfremd zu p ist.

Nun differenzire ich die Gleichungen (53) und (54) $p-1$ Mal nach u und benutze sodann die Congruenz (47'), der zufolge sich die Ableitungen von $\varphi^2(u)$ bis auf den Factor $e_{\frac{p-1}{4}} \pmod p$ reproduciren. Auf diese Weise ergiebt sich der Satz:

Ist $2n < p$, so gilt die Congruenz

$$(55)\quad \frac{d^{p-1}\varphi^{2n}(u)}{du^{p-1}} \equiv e_{\frac{p-1}{4}} \left(\varphi^{2n}(u) - \frac{1.5.9\ldots(2n-3)}{3.7.11\ldots(2n-1)}\right) \pmod p,$$

oder die Congruenz

$$(56)\qquad \frac{d^{p-1}\varphi^{2n}(u)}{du^{p-1}} \equiv e_{\frac{p-1}{4}} \cdot \varphi^{2n}(u) \pmod p,$$

je nachdem n gerade oder ungerade ist.

In entsprechender Weise ergiebt sich für eine Primzahl q von der Form $4k+3$ der Satz:

Ist $2n < q$, so gilt die Congruenz:

$$\frac{d^{q-1}\varphi^{2n}(u)}{du^{q-1}} \equiv (-1)^{n+1} \cdot \frac{2}{(2n-1)!}\, e_{\frac{q-3}{4}} \eta_{2n}^{(2)} \pmod{q}. \tag{57}$$

Für $n = 1$ geht (56) in die Congruenz (47) und (57) in die Congruenz (48) über.

§ 9.

Die Entwickelungscoefficienten der Potenzen von $\varphi^2(u)$.

Die im vorigen Paragraphen aufgestellten Congruenzen enthalten gewisse Eigenschaften der Entwickelungscoefficienten der Function $\varphi^{2n}(u)$, wie ich jetzt des Näheren darlegen will.

Zur Abkürzung setze ich

$$C_n = \frac{1.5.9\ldots(2n-3)}{3.7.11\ldots(2n-1)} \text{ oder } C_n = 0, \tag{58}$$

je nachdem n gerade oder ungerade ist. Dann lassen sich die beiden Congruenzen (55) und (56) in die folgende:

$$\frac{d^{p-1}\varphi^{2n}(u)}{du^{p-1}} \equiv e_{\frac{p-1}{4}} \left(\varphi^{2n}(u) - C_n\right) \pmod{p} \tag{59}$$

vereinigen. Hier bedeutet n eine beliebige positive ganze Zahl und p irgend eine Primzahl von der Form $4k+1$, die grösser als $2n$ ist. Nun ist nach Gleichung (45)

$$\varphi^{2n}(u) = \varepsilon_{2n}^{(2n)} \frac{u^{2n}}{(2n)!} + \varepsilon_{2n+4}^{(2n)} \frac{u^{2n+4}}{(2n+4)!} + \cdots + \varepsilon_{2k}^{(2n)} \frac{u^{2k}}{2k!} + \cdots. \tag{60}$$

Indem man diese Entwickelung in die Congruenz (59) einführt, ergiebt sich durch Coefficientenvergleichung:

$$\varepsilon_{p-1}^{(2n)} \equiv -e_{\frac{p-1}{4}} \cdot C_n \pmod{p} \tag{61}$$

und $\varepsilon_{2k+p-1}^{(2n)} \equiv e_{\frac{p-1}{4}} \varepsilon_{2k}^{(2n)} \pmod{p}$, welch' letztere Congruenz durch wiederholte Anwendung zu

$$\varepsilon_{2k+r(p-1)}^{(2n)} \equiv \left(e_{\frac{p-1}{4}}\right)^r \varepsilon_{2k}^{(2n)} \pmod{p} \quad (k = 1, 2, \ldots) \tag{62}$$

führt, unter r eine positive ganze Zahl verstanden.

Durch die Congruenz (62) werden die Reste der Entwickelungscoefficienten von $\varphi^{2n}(u)$ nach dem Modul p zurückgeführt auf die Reste derjenigen unter ihnen, deren Index nicht grösser als $p-1$ ist.

Für das Hauptziel dieser Arbeit ist der Fall $2n = p-1$ von besonderer Wichtigkeit. In diesem Falle ist

$$\varepsilon_{p-1}^{(2n)} = \varepsilon_{p-1}^{p-1} = (p-1)! \equiv -1 \pmod{p}$$

und die Congruenz (61) lehrt also, dass

$$e_{\frac{p-1}{4}} \equiv \frac{3.7.11\ldots(p-2)}{1.5.9\ldots(p-4)} \pmod{p} \tag{63}$$

ist. Nach einem bekannten Satze von Gauss*) ist die rechte Seite dieser Congruenz $\equiv 2a \pmod{p}$, wenn $a+bi$ den primären complexen Primfactor von p bezeichnet. Daher ist auch

$$e_{\frac{p-1}{4}} \equiv 2a \pmod{p}. \tag{64}$$

Endlich sind im Falle $2n = p-1$ alle Coefficienten $\varepsilon_{2k}^{(2n)}$, deren Index $2k$ unter $p-1$ liegt gleich Null. Folglich sind, in Rücksicht auf (62), sämmtliche Coefficienten $\varepsilon_{2k}^{(2n)}$ durch p theilbar, deren Indices $2k$ nicht Multipla von $p-1$ sind. Dieselbe Congruenz (62) liefert, indem man $k = \frac{p-1}{2}$ setzt und sodann $r-1$ an Stelle von r schreibt:

$$\varepsilon_{r(p-1)}^{(p-1)} \equiv -\left(e_{\frac{p-1}{4}}\right)^{r-1} \equiv -(2a)^{r-1} \pmod{p}. \tag{65}$$

Diese Resultate fasse ich in folgenden Satz zusammen:

Bezeichnet p eine Primzahl von der Form $4k+1$ und $a+ib$ den primären complexen Primfactor derselben, so gilt die Congruenz

$$\frac{\varphi^{p-1}(u)}{(p-1)!} \equiv \sum_{r=1}^{\infty} (2a)^{r-1} \cdot \frac{u^{r(p-1)}}{(r(p-1))!} \cdot \pmod{p}. \tag{66}$$

Der Vollständigkeit halber will ich noch die Congruenz (57) in ähnlicher Weise entwickeln, wie es soeben mit den Congruenzen (55) und (56) geschehen ist.

Die Congruenz (57) besagt, dass

$$\varepsilon_{q-1}^{(2n)} \equiv (-1)^{n+1} \cdot \frac{2}{(2n-1)!}\, e_{\frac{q-3}{4}} \cdot \eta_{2n}^{(2)} \pmod{q} \tag{67}$$

ist, und dass alle Coefficienten $\varepsilon_{2k}^{(2n)}$, deren Indices $2k$ grösser als $q-1$ sind, den Factor q haben. Die in (67) auftretenden Coefficienten $\eta_{2n}^{(2)}$ sind durch die Gleichung

$$\frac{v^2}{2} = \eta_2^{(2)} \frac{\tau^2}{2!} + \eta_6^{(2)} \cdot \frac{\tau^6}{6!} + \cdots + \eta_{2k}^{(2)} \frac{\tau^{2k}}{(2k)!} + \cdots \tag{68}$$

*) Theoria residuorum biquadraticorum, Commentatio prima. Werke Bd. II pag. 90.

definirt, wobei

$$(69)\quad v=\int_0^{\tau}\frac{d\tau}{\sqrt{1-\tau^4}}=\tau+\frac{1}{2}\,\frac{\tau^5}{5}+\cdots+\frac{1.3.5\ldots(2k-1)}{2.4.6\ldots 2n}\,\frac{\tau^{4k+1}}{4k+1}+\cdots$$

ist. Da nun v^2 der Differentialgleichung

$$(1-\tau^4)\,\frac{d^2v^2}{d\tau^2}-2\tau^3\,\frac{dv^2}{d\tau}=2$$

genügt, so kann man die Coefficienten $\eta_{2k}^{(2)}$ recurrent berechnen. Man findet auf diese Weise, dass das Quadrat des elliptischen Integrales (69) folgende Entwickelung besitzt

$$(70)\quad v^2=\tau^2+\frac{3}{5}\cdot\frac{\tau^6}{3}+\frac{3.7}{5.9}\cdot\frac{\tau^{10}}{5}+\cdots+\frac{3.7\ldots(4n-1)}{5.9\ldots(4n+1)}\,\frac{\tau^{4n+2}}{2n+1}+\cdots,$$

dass also

$$\eta_{2k}^{(2)}=0$$

oder

$$\eta_{2k}^{(2)}=(2k)!\,\frac{3.7\ldots(2k-3)}{5.9\ldots(2k-1)}\cdot\frac{1}{2k}$$

ist, je nachdem k eine gerade oder eine ungerade Zahl bezeichnet.

Hiernach nimmt die Congruenz (67) (welche für ein gerades n eine Identität vorstellt) für den Fall, wo n ungerade ist, die Gestalt an

$$(71)\quad \varepsilon_{q-1}^{(2n)}\equiv 2e_{\frac{q-3}{4}}\cdot\frac{3.7\ldots(2n-3)}{5.9\ldots(2n-1)}\pmod q.$$

Wenn hier $2n$ den grössten zulässigen Werth $q-1$ erhält, so ergiebt sich, weil

$$\varepsilon_{q-1}^{(q-1)}=(q-1)!\equiv -1\pmod q$$

ist,

$$e_{\frac{q-3}{4}}\equiv -\frac{1}{2}\cdot\frac{5.9\ldots(q-2)}{3.7\ldots(q-4)}\pmod q$$

oder

$$(72)\quad e_{\frac{q-3}{4}}\equiv\frac{1.5\ldots(q-6)}{3.7\ldots(q-4)}\pmod q,$$

und die Congruenz (71) lässt sich in Folge dessen auch so schreiben:

$$(73)\quad \varepsilon_{q-1}^{(2n)}\equiv -\frac{(2n+3)(2n+7)\ldots(q-2)}{(2n+1)(2n+5)\ldots(q-4)}\pmod q.$$

§ 10.

Die Partialbruchzerlegung der Zahl E_n.

Aus den Congruenzen (40) und (66) geht nun hervor, dass

$$\varepsilon \equiv (2a)^{\frac{4n}{p-1}} \pmod{p}$$

ist und dass folglich die Partialbruchzerlegung der Zahl E_n die Gestalt hat:

$$E_n = G + \frac{\varepsilon_0}{2^\alpha} + \sum \frac{(2a)^{\frac{4n}{p-1}}}{p}. \tag{74}$$

Hier ist die Summe über diejenigen Primzahlen p von der Form $4k+1$ auszudehnen, für welche $p-1$ ein Divisor von $4n$ ist, und für jede einzelne dieser Primzahlen p bedeutet a den reellen Theil ihres primären complexen Primfactors $a+ib$. Die Zahl a kann hiernach auch definirt werden als die Basis des ungeraden Quadrates bei der Zerlegung von p in die Summe zweier Quadrate:

$$p = a^2 + b^2,$$

und zwar diese Basis mit solchem Vorzeichen genommen, dass die Congruenz

$$a \equiv b + 1 \pmod{4}$$

besteht.

Es erübrigt noch, den auf die Primzahl 2 bezüglichen Theil $\frac{\varepsilon_0}{2^\alpha}$ der Partialbruchzerlegung von E_n zu bestimmen. Zu diesem Zwecke bediene ich mich der Recursionsformel (9).

Aus dieser Formel ergiebt sich leicht, dass $\frac{\varepsilon_0}{2^\alpha} = \frac{1}{2}$, oder was dasselbe besagt, dass

$$2E_n \equiv 1 \pmod{2} \tag{75}$$

ist. In der That: die Formel (9) lässt sich, je nachdem n gerade oder ungerade ist, in die Gestalt bringen:

$$(2n-3)(16n^2-1).(2E_n) \tag{76}$$

$$= 3\left\{\sum_{r=1}^{\frac{n}{2}-1}(4r-1)(4n-4r-1)(4n)_{4r}(2E_r).(2E_{n-r}) + (2n-1)^2(4n)_{2n}\frac{1}{2}(2E_{\frac{n}{2}})^2\right\}$$

respective

$$(2n-3)(16n^2-1)(2E_n) = 3\cdot\sum_{r=1}^{\frac{n-1}{2}}(4r-1)(4n-4r-1)(4n)_{4r}(2E_r)(2E_{n-r}). \tag{77}$$

Hierbei ist, wie man leicht erkennt, der Factor $(4n)_{2n} \cdot \frac{1}{2}$ in (76) eine ganze Zahl. Nimmt man nun an, die Congruenz (75) sei schon für die Zahlen $E_1, E_2, \ldots E_{n-1}$ als richtig nachgewiesen, so folgt aus (76) resp. (77)

$$2E_n \equiv \sum_{r=1}^{\frac{n}{2}-1} (4n)_{4r} + \frac{1}{2}(4n)_{2n} = \frac{1}{8}[(1+1)^{4n} + (1+i)^{4n} + (1-1)^{4n} + (1-i)^{4n} - 8] \pmod 2$$

resp.

$$2E_n \equiv \sum_{r=1}^{\frac{n-1}{2}} (4n)_{4r} = \frac{1}{8}[(1+1)^{4n} + (1+i)^{4n} + (1-1)^{4n} + (1-i)^{4n} - 8] \pmod 2$$

oder

$$2E_n \equiv 1 \pmod 2.$$

Da aber für $E_1 = \frac{1}{10}$ die Congruenz (75) erfüllt ist, so gilt sie allgemein.

Hiermit ist nun das Hauptziel dieser Untersuchung erreicht:

Die Partialbruchzerlegung der Zahl E_n lautet wie folgt:

$$E_n = G_n + \frac{1}{2} + \sum \frac{(2a)^{\overline{p-1}}}{p}. \tag{78}$$

Dabei bezeichnet G_n eine ganze Zahl und die Summe ist über diejenigen Primzahlen p von der Form $4k+1$ zu erstrecken, für welche $p-1$ ein Divisor von $4n$ ist. Die der einzelnen Primzahl p entsprechende Zahl a ist die Basis des ungeraden Quadrates in der Zerlegung

$$p = a^2 + b^2,$$

und zwar mit solchem Vorzeichen genommen, dass

$$a \equiv b + 1 \pmod 4$$

ist.

§ 11.

Die ganzzahligen Theile in der Partialbruchzerlegung der Zahlen E_n.

Vermöge der Gleichungen (76) und (77) gelingt es, den Rest der Zahl $2E_n$ nach dem Modul 16 zu bestimmen. Für die niedrigen Werthe von n findet man nach dem Modul 16:

$$2E_1 = \frac{1}{5} \equiv -3, \quad 2E_2 = \frac{3}{5} \equiv 7, \quad 2E_3 = \frac{3^4 \cdot 7}{5 \cdot 13} \equiv 7,$$

$$2E_4 = \frac{3^4 \cdot 7^2 \cdot 11}{5 \cdot 17} \equiv -1 \text{ u. s. w.}$$

Durch Fortsetzung der Rechnung wird man auf die Vermuthung geführt, dass vom Index $n = 3$ ab die Congruenz

$$2E_n \equiv 8n - 1 \pmod{16} \tag{79}$$

besteht, dass also $2E_n \equiv 7$ oder $-1 \pmod{16}$, je nachdem n ungerade oder gerade ist.

Diese Vermuthung bestätigt sich durch folgende Schlüsse. Aus den Gleichungen (76) und (77) folgen zunächst nach dem Modul 16 die Congruenzen:

$$(2n-3)(2E_n) \equiv (4n-1).3.\left\{\sum_{r=1}^{r=\frac{n}{2}-1}(4n)_{4r}(2E'_r)(2E_{n-r}) + \frac{1}{2}(4n)_{2n}(2E_{\frac{n}{2}})^2\right\}$$

resp.

$$(2n-3)(2E_n) \equiv (4n-1).3.\left\{\sum_{r=1}^{r=\frac{n-1}{2}}(4n)_{4r}(2E_r)(2E_{n-r})\right\},$$

und hieraus, durch Multiplication mit $4n+1$, in beiden Fällen

$$(4n+1)(2n-3).(2E_n) \equiv -\frac{3}{2}\sum_{r=1}^{r=n-1}(4n)_{4r}(2E_r)(2E_{n-r}).$$

Sei nun $n > 4$ und überdies die Congruenz (79) schon bewiesen für $n = 3, 4, \ldots n-1$. Dann folgt*)

$$\begin{aligned}(4n+1)(2n-3)(2E_n) &\equiv -\frac{3}{2}\Big[2.(4n)_4(2E_1)(2E_{n-1}) + 2(4n)_8(2E_2)(2E_{n-2}) \\ &\qquad + \sum_{r=3}^{r=n-3}(4n)_{4r}(2E_r)(2E_{n-r})\Big] \\ &\equiv +\frac{3}{2}\Big[2.(4n)_4.3.\big(8(n-1)-1\big) \\ &\qquad - 2.(4n)_8.7.\big(8(n-2)-1\big) \\ &\qquad - \sum_{r=3}^{r=n-3}(4n)_{4r}(8r-1)(8n-8r-1)\Big].\end{aligned}$$

Nach leichten Reductionen und unter Benutzung der Congruenz**)

---

*) Die folgenden Congruenzen beziehen sich sämmtlich auf den Modul 16, sofern nicht ein anderer Modul ausdrücklich angegeben ist.

**) Es ist

$$(4n)_{4r} = (2n)_{2r} \cdot \prod_{k=0}^{r-1}\frac{[4(n-k)-1][4(n-k)-3]}{(4k+1)(4k+3)},$$

und für jeden Werth von k

$$[4(n-k)-1][4(n-k)-3] \equiv (4k+1)(4k+3) \equiv 1.3 \pmod{16}.$$

$$(4n)_{4r} \equiv (2n)_{2r} \pmod{16}$$

kommt:

$$(4n+1)(2n-3)(2E_n)$$
$$\equiv 3\Big[(2n)_2(8n+5) + (2n)_4(8n+7) + (8n-1)\cdot\frac{1}{2}\sum_{r=3}^{r=n-3}(2n)_{2r}\Big].$$

Berücksichtigt man nun, dass

$$\frac{1}{2}\sum_{r=3}^{r=n-3}(2n)_{2r} = \frac{1}{2}\left[(1+1)^{2n} + (1-1)^{2n} - 2 - 2(2n)_2 - 2(2n)_4\right]$$
$$\equiv -1 - (2n)_2 - (2n)_4 \pmod{16},$$

so erkennt man, dass die vorhergehende Congruenz

$$\begin{aligned}(4n+1)(2n-3)(2E_n) &\equiv 3[6.(2n)_2 + 8(2n)_4 - (8n-1)]\\ &\equiv 2n(2n-1) + 2n(2n-1)(2n-2)(2n-3)\\ &\qquad + 8n + 3\\ &\equiv 2n(2n-1) + 4n(n-1) + 8n + 3\\ &\equiv 8n^2 + 2n + 3\end{aligned}$$

liefert. Da $8n^2 \equiv 8n \pmod{16}$, so ergiebt sich schliesslich

$$2E_n \equiv \frac{10n+3}{(4n+1)(2n-3)} \equiv \frac{10n+3}{-2n-3} \equiv 8n - 1 \pmod{16},$$

woraus nun die Gültigkeit der Congruenz (79) für $n \geqq 3$ folgt, da sie für $n = 3$, $n = 4$ feststeht.

Die Congruenz (79) giebt Aufschluss über das Verhalten der ganzzahligen Theile G_n der Partialbruchzerlegung (78) der Zahlen E_n in Bezug auf den Modul 8. Setzt man, unter der Voraussetzung $n > 2$, die Partialbruchzerlegung von E_n in (79) ein, so ergiebt sich zunächst

$$G_n \equiv 4n - 1 - \sum \frac{(2a)^{\frac{4n}{p-1}}}{p} \pmod{8}.$$

Die hier auftretenden Primzahlen p sind von der Form $4\delta + 1$, wo δ Divisor von n ist.

Der Exponent $\frac{4n}{p-1} = \frac{n}{\delta}$ wird daher, falls nicht $\delta = \frac{n}{2}$ oder $\delta = n$ ist, grösser als 2 und folglich das entsprechende Glied $\frac{(2a)^{\frac{n}{\delta}}}{p} \equiv 0 \pmod{8}$ sein. Für $\delta = \frac{n}{2}$ resp. $\delta = n$ ist der Exponent $\frac{n}{\delta}$ gleich 2 resp. 1; zugleich wird $p = 2n + 1$ resp. $p = 4n + 1$. Ich unterscheide nun folgende Fälle:

1. Fall. Weder $2n + 1$ noch $4n + 1$ ist eine Primzahl von der Form $4k + 1$. Dann ist

$$(80_1) \qquad G_n \equiv 4n - 1 \pmod{8}.$$

2. Fall. Es ist $2n+1$ eine Primzahl von der Form $4k+1$, $4n+1$ dagegen nicht. Dieser Fall kann nur für gerades n eintreten. Ferner ist nun der Exponent $\frac{4n}{p-1}$ stets >2, ausgenommen für $p=2n+1$. Also ist

$$G_n \equiv 4n - 1 - \frac{(2a)^2}{2n+1} \pmod 8.$$

Da $a \equiv 1 \pmod 2$, so wird $(2a)^2 \equiv 4 \pmod 8$; ferner ist

$$\frac{1}{2n+1} \equiv -2n+1 \pmod 8,$$

weil n gerade ist. Daher kommt:

$(80)_2$ $$G_n \equiv 3 \pmod 8.$$

3. Fall. Es ist $4n+1$ Primzahl, $2n+1$ dagegen nicht Primzahl von der Form $4k+1$. In diesem Falle ist

$$G_n \equiv 4n - 1 - \frac{2a}{4n+1} \pmod 8.$$

Nun folgt aus der Gleichung

$$4n+1 = a^2 + b^2,$$

dass

$$b^2 \equiv 4n \pmod 8,$$

und hieraus successive:

$$b \equiv 2n \pmod 4,$$

$$a \equiv b+1 \equiv 2n+1 \pmod 4,$$

$$\frac{2a}{4n+1} \equiv +2a \equiv 4n+2 \pmod 8$$

und schliesslich:

(80_3) $$G_n \equiv 5 \pmod 8.$$

4. Fall. Es sind $2n+1$ und $4n+1$ Primzahlen von der Form $4k+1$. Dieser Fall kann nur für gerades n eintreten. Die Glieder der Summe $\sum \frac{(2a)^{\frac{4n}{p-1}}}{p}$, welche den Primzahlen $p=2n+1$ und $p=4n+1$ entsprechen, werden respective $\equiv 4, 2 \pmod 8$, so dass jetzt

(80_4) $$G_n \equiv 1 \pmod 8$$

wird. —

Wenn n ungerade ist, so können nur die Fälle 1 und 3 stattfinden. Man hat demgemäss den Satz:

Ist $n > 1$ eine ungerade Zahl, so ist

$$G_n \equiv 5 \quad \textit{oder} \quad G_n \equiv 3 \pmod 8$$

je nachdem $4n+1$ eine Primzahl ist oder nicht.

Wenn n gerade ist, so kann jeder der vier Fälle eintreten. Die Congruenzen (80) ergeben jetzt den Satz:

Ist $n > 2$ eine gerade Zahl, so ist

$$G_n \equiv 1, 3, 5, 7 \pmod 8$$

je nachdem die Zahlen $2n+1$ und $4n+1$ beide Primzahlen sind, oder nur $2n+1$ oder nur $4n+1$ Primzahl ist oder endlich keine von beiden.

Betrachtet man die Reste der Zahlen $G_n \pmod 4$, so erhält man aus den beiden vorstehenden Sätzen (wenn man noch beachtet, dass $G_2 = -1 \equiv 3 \pmod 4$) das Resultat:

Ist $n > 1$, so lässt die Zahl G_n durch 4 dividirt den Rest 1 oder den Rest 3, je nachdem $4n+1$ Primzahl ist oder nicht.

Dass die Zahlen G_n, abgesehen von $G_1 = 0$, sämmtlich ungerade sind, ist eine selbstverständliche Folge der vorstehenden Sätze.

§ 12.

Die Entwickelungscoefficienten der Function $\frac{1}{2}\varphi^2(u)$.

Die Congruenzen (62) und (67) bestehen unter der Voraussetzung, dass $2n < p$ resp. $2n < q$ ist.

Diese Voraussetzung ist für $n = 1$ stets erfüllt. In diesem Falle ist überdies, wie schon oben bemerkt wurde, $\varepsilon_{2k}^{(2n)} = \varepsilon_{2k}^{(2)} = 0$ oder $= 2e_{\frac{k-1}{2}}$, je nachdem k gerade oder ungerade ist. Daher führt die Annahme $n = 1$ zu folgendem Satze über die Entwickelungscoefficienten der Function $\frac{1}{2}\varphi^2(u)$, welche durch die Gleichung (16), nämlich

$$\frac{1}{2\wp(u)} = \frac{1}{2}\varphi^2(u) = e_0\frac{u^2}{2!} + e_1\frac{u^6}{6!} + \cdots + e_n\frac{u^{4n+2}}{(4n+2)} + \cdots$$

definirt sind:

Bezeichnet p eine Primzahl $\equiv 1 \pmod 4$ und ist $p' = \frac{p-1}{4}$, so besteht die Congruenz

$$e_{n+p'} \equiv e_{p'}\, e_n \pmod p, \qquad (n = 0, 1, 2, \ldots) \tag{81}$$

durch welche die Reste der Zahlen $e_n \pmod p$ auf die der ersten $p'-1$ unter ihnen zurückgeführt werden. Ueberdies ist nach (63) und (64)

$$e_{p'} \equiv \frac{3.7.11\ldots(p-2)}{1.5.9\ldots(p-4)} \equiv 2a \pmod p.$$

Bezeichnet andererseits q eine Primzahl $\equiv 3 \pmod 4$ *und ist* $q' = \frac{q-3}{4}$, *so ist nach* (72)

$$e_{q'} = \frac{1 \cdot 5 \cdot 9 \ldots (q-6)}{3 \cdot 7 \cdot 11 \ldots (q-4)} \pmod q$$

und die Zahlen $e_{q'+1}, e_{q'+2}, \ldots$ *sind sämmtlich durch* q *theilbar.*

Diese Eigenschaften der Zahlen e_n lassen sich, vermöge der Gleichung (19), auf die Zahlen E_n übertragen.

Beispielsweise ergiebt sich so, dass der Zähler der Zahl

$$\left(1 - (1+i)^{4n}\right) \frac{E_n}{n}$$

den Factor q besitzt, sobald $n > \frac{q+1}{4}$ ist. Indessen dürften diese Sätze nur ein untergeordnetes Interesse beanspruchen, da für die Zahlen E_n allgemeinere Congruenzen zu gelten scheinen, welche jene Sätze in sich enthalten.

Zur Berechnung der Zahlen e_n kann man sich einer Recursionsformel bedienen, die sich folgendermassen ergiebt. Die Function $z = \varphi^2(u)$ genügt der Differentialgleichung

$$\left(\frac{dz}{du}\right)^2 = 4(z - z^3), \tag{82}$$

aus welcher durch Differentiation

$$\frac{d^2 z}{du^2} = 2 - 6z^2 \tag{83}$$

folgt. Setzt man hier

$$z = 2 \sum_{n=0}^{\infty} e_n \frac{u^{4n+2}}{(4n+2)!},$$

so ergiebt sich durch Coefficientengleichung

$$e_{n+1} = -12 \sum (4n+4)_{4r+2} e_r e_s, \quad (n = 0, 1, 2, \ldots) \tag{84}$$

wobei die Summe über alle nicht negativen Zahlen r, s zu erstrecken ist, welche die Bedingung $r + s = n$ befriedigen.

Die Recursionsformel (84) vereinfacht sich noch etwas, wenn man

$$e_n = (-12)^n \cdot \partial_n \quad (n = 0, 1, 2, \ldots) \tag{85}$$

setzt. Man erhält dann offenbar für die Zahlen ∂_n die Gleichung

$$\partial_{n+1} = \sum (4n+4)_{4r+2} \partial_r \partial_s, \quad (n = 0, 1, 2, \ldots) \tag{86}$$

aus welcher hervorgeht, dass diese Zahlen positive ganze Zahlen sind.

I. Tabelle der Zerfällungen $p = a^2 + b^2$, $\left(a \equiv b + 1 \pmod 4\right)$,

p	a	b	$2a$
5	−1	2	− 2
13	3	2	6
17	1	4	2
29	−5	2	− 10
37	−1	6	− 2
41	5	4	10

II. Tabelle der Zahlen $E_n = G_n + \frac{1}{2} + \sum \frac{(2a)^{\frac{4n}{p-1}}}{p}$.

(Wegen des raschen Anwachsens der ganzzahligen Theile G_n sind diese nur bis $n = 6$ in der Tabelle angegeben.)

$$E_1 = \frac{1}{10} = \frac{1}{2} - \frac{2}{5}$$

$$E_2 = \frac{3}{10} = -1 + \frac{1}{2} + \frac{2^2}{5}$$

$$E_3 = \frac{3^4 . 7}{10 . 13} = 5 + \frac{1}{2} - \frac{2^3}{5} + \frac{6}{13}$$

$$E_4 = \frac{3^4 . 7^2 . 13}{10 . 17} = 253 + \frac{1}{2} + \frac{2^4}{5} + \frac{2}{17}$$

$$E_5 = \frac{3^6 . 7^2 . 11}{10} = 39299 + \frac{1}{2} - \frac{2^5}{5}$$

$$E_6 = \frac{3^7 . 7^3 . 11^2 . 19}{10 . 13} = 13265939 + \frac{1}{2} + \frac{2^6}{5} + \frac{6^2}{13}$$

$$E_7 = \frac{3^9 . 7^4 . 11^2 . 19 . 23}{10 . 29} = G_7 + \frac{1}{2} - \frac{2^7}{5} - \frac{10}{29}$$

$$E_8 = \frac{3^{10} . 7^4 . 11^2 . 19 . 23 . 223}{10 . 17} = G_8 + \frac{1}{2} + \frac{2^8}{5} + \frac{2^2}{17}$$

$$E_9 = \frac{3^{14} . 7^5 . 11^3 . 19 . 23 . 31 . 61}{10 . 13 . 37} = G_9 + \frac{1}{2} - \frac{2^9}{5} + \frac{6^3}{13} - \frac{2}{37}$$

$$E_{10} = \frac{3^{13} . 7^5 . 11^3 . 19^2 . 23 . 31 . 2381}{10 . 41} = G_{10} + \frac{1}{2} + \frac{2^{10}}{5} + \frac{10}{41}$$

$$E_{11} = \frac{3^{15} . 7^6 . 11^4 . 19^4 . 23 . 31}{10} = G_{11} + \frac{1}{2} - \frac{2^{11}}{5}$$

$$E_{12} = \frac{3^{16} . 7^5 . 11^4 19^2 . 23^2 . 31 . 43 . 1162253}{10 . 13 . 17} = G_{12} + \frac{1}{2} + \frac{2^{12}}{5} + \frac{6^4}{13} + \frac{2^3}{17}$$

III. Tabelle der Zahlen e_n.

Reste nach dem Modul p:	$p=5$ $(p'=1)$	$p=13$ $(p'=3)$	$p=17$ $(p'=4)$	$p=29$ $(p'=7)$	$p=37$ $(p'=9)$	$p=41$ $(p'=10)$
$e_0 = 1$	1	1	1	1	1	1
$e_1 = -2^3.3^2$	−2	6	−4	15	2	10
$e_2 = 2^8.3^3.7$	−1	−2	2	12	25	4
$e_3 = -2^{10}.3^5.7^2.11$	2	6	−2	−1	1	23
$e_4 = 2^{16}.3^6.7^2.11.41$	1	10	2	13	9	0
$e_5 = -2^{19}.3^8.7^4.11^2.19$	−2	1	−8	7	1	−14
$e_6 = 2^{24}.3^9.7^8.11^2.19.23.113$	−1	10	4	12	14	38
$e_7 = -2^{25}.3^{11}.7^4.11^2.19.23.223.257$	2	−5	−4	−10	25	−6
$e_8 = 2^{32}.3^{12}.7^5.11^3.19.23.31.61.109$	1	6	4	24	18	10
$e_9 = -2^{35}.3^{14}.7^5.11^4.19^2.23.31^2.2381$	−2	−5	1	25	−2	−4
$e_{10} = 2^{40}.3^{15}.7^6.11^3.19^4.23.31.397.2113$	−1	9	8	10	−4	10
$e_{11} = -2^{42}.3^{17}.7^6.11^4.19^2.23^2.31.43.241.1162253$	2	10	−8	15	24	18