19.

Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt.

(Von Herrn Dr. *G. Eisenstein* zu Berlin.)

§. 1.

Unter den elliptischen Functionen, welche wegen der Willkürlichkeit des elliptischen Moduls ein unendliches Gebiet von transcendenten Functionen umfassen, giebt es eine gewisse Classe, welche, neben den allgemeinen von *Jacobi* und *Abel* aufgestellten Eigenschaften aller elliptischen Functionen, noch besondere characteristische Eigenthümlichkeiten besitzt, durch die sie in sehr nahe Beziehung mit der Zahlentheorie versetzt wird, namentlich mit der Theorie der zweigliedrigen complexen ganzen Zahlen, welche aus den binären quadratischen Formen mit negativer Determinante entspringen. Es sind hiermit diejenigen elliptischen Functionen gemeint, von denen *Jacobi*, seiner Bezeichnungsweise gemäfs, sagt:

„Dafs bei ihnen der Modul durch die Transformation in sein Complement, oder auch in sich selbst zurückkehrt,"

und die sich auch als solche bezeichnen lassen,

„Welche eine complexe Periodicität und eine complexe Multiplication besitzen."

Unter einer complex periodischen Function ist hier eine solche zu verstehen, welche unverändert bleibt, wenn ihr Argument um ein beliebiges *complexes* ganzes Vielfache einer gewissen Gröfse, des Moduls der Periodicität, vermehrt wird. Der Character der complexen Multiplication, auf welchen auch schon *Abel* und *Jacobi* aufmerksam gemacht haben (Gegenw. Journal 3. Bd. S. 181, 195) besteht darin, dafs die Function für ein *complexes* ganzes Vielfache des Arguments sich algebraisch in die Function des einfachen Arguments ausdrücken läfst, während dies im *Allgemeinen* bei den elliptischen Functionen nur für einen *reellen* ganzen Werth des Multiplicators des Arguments gültig ist. Jede der in dieser Classe enthaltenen elliptischen Functionen entspricht einer anderen Gattung von complexen Zahlen; die lemniscatischen

Functionen, welche allen andern unter ihnen vorangehen, entsprechen den von *Gaufs* eingeführten complexen ganzen Zahlen von der Form $a+b\sqrt{-1}$.

Auf alle hier besonders hervorgehobenen Functionen lassen sich ferner, in Rücksicht auf ihre Theilung, die *Gaufs*ischen Principien der Kreistheilung mit gröfserer oder geringerer Leichtigkeit anwenden *). Dafs dies bei den lemniscatischen Functionen (und mit diesen haben wir es zunächst nur zu thun) möglich ist, hat schon *Gaufs* in seinen „Disquisitiones Arithm." angedeutet. *Abel,* indem er die Elemente **) der Lemniscatentheilung aufstellte, begnügte sich damit, die algebraische Auflösbarkeit der Gleichungen zu zeigen, von denen die Theilung abhängt, ohne näher in den speciellen Character der Resultate und deren Verknüpfung mit andern Gebieten der Mathematik einzugehen. Im Grunde erscheint bei *Abel* der vorliegende Fall nur als Beispiel für seine allgemeine Theorie der algebraisch lösbaren Gleichungen (4. Band dieses Journals Seite 131), und es wird daher die Untersuchung nicht weiter verfolgt, als sie sich für alle algebraischen Gleichungen durchführen läfst, in denen jede Wurzel als rationale Function einer Wurzel dargestellt werden kann.

Indem ich zuerst von den biquadratischen Resten aus auf diesen Gegenstand geführt wurde, habe ich in die von *Abel* ihren Grundzügen nach gegebene Theorie weiter einzudringen und namentlich dieselbe für zahlentheoretische Anwendungen fruchtbar zu machen gesucht. Als erstes Resultat dieser Untersuchungen ergaben sich meine neueren Beweise des biquadratischen Fundamentaltheorems. Die ferneren Ergebnisse meiner Forschungen erlaube ich mir hier und in einigen folgenden Abhandlungen den Freunden der Wissenschaft vorzulegen.

Ehe ich zu dem eigentlichen Gegenstand übergehe, wird es gut sein, auf eine allgemeine Schwierigkeit aufmerksam zu machen, mit welcher man in diesen Gebieten stets zu kämpfen hat. Es giebt sehr viele Sätze bei den elliptischen Functionen, welche eine blofse *Möglichkeit* behaupten, so zu sagen blofse Existenzsätze, und welche nicht den individuellen Character des Resultats erkennen lassen. So weifs man z. B., dafs sich die elliptischen Functionen eines vielfachen Arguments in die des einfachen ausdrücken lassen, und zwar

---

*) Die Theilung, welche hier gemeint wird, ist nicht mit der allgemeinen Theilung für ein unbestimmtes Argument zu verwechseln, für welche *Jacobi* die Fundamentalformeln aufgestellt hat.

**) 3. Band dieses Journals S. 162. Vergl. auch *Dirichlet* im 24. Band dieses Journals S. 366.

algebraisch; man weifs, dafs die von *Jacobi* zwischen den beiden Moduln bei der Transformation aufgestellte Gleichung eine algebraische ist; man weifs, dafs jede Wurzel der Gleichung für die Theilung der Lemniscate einer rationalen Function irgend einer andern Wurzel gleich ist, u. s. w.: fragt man aber nach der speciellen Art der Zusammensetzung dieser und ähnlicher algebraischer oder rationaler Ausdrücke, und verlangt man dieselben namentlich in einer solchen fertigen Form, welche sich zum weitern Fortschliefsen benutzen läfst, so bleibt die Theorie meistens die Antwort schuldig; in noch höherem Grade zeigt sich dieser Umstand, wenn man über die elliptischen Functionen hinaus zu andern Transcendenten fortschreitet. Ja noch mehr, in besonderer Rücksicht auf unseren Gegenstand: man kennt nicht einmal die Gleichung selbst, von der die Lemniscatentheilung abhängt und welche man doch auflösen soll; man weifs nur, dafs sie überhaupt existirt; man kennt ihren Grad und einen gewissen Algorithmus, um sie zu bilden, wenn der Divisor *numerisch* gegeben ist: ganz anders ist dies bei der Kreistheilung, wo die aufzulösende Gleichung $\frac{x^p-1}{x-1}=0$ gleich von vorn herein vollständig gegeben ist, und wo die Relationen zwischen ihren Wurzeln ebenfalls vollkommen bekannt sind, indem jede Wurzel sich als Potenz einer von ihnen ausdrücken läfst. Bei vielen Untersuchungen ist es freilich hinreichend, überhaupt nur zu wissen, dafs sich eine Gröfse in eine gewisse andere Gröfse algebraisch u. s. w. ausdrücken läfst, ohne näher das *Wie?* zu kennen. Wo Dies jedoch nicht ausreicht, da könnte man zwei Wege einschlagen. Einmal könnte man sich bemühen, den angeregten Mangel, wenn es überhaupt ein solcher ist, zu ergänzen; ich habe aber diesen Weg bald verlassen, weil ich auf demselben nicht fortkommen konnte. Dann kann man aber auch nach solchen Principien forschen, welche möglichst fruchtbar sind und doch zugleich nur eine möglichst geringe, gleichsam an der Oberfläche bleibende Einsicht in diejenigen Beziehungen erheischen, welche man beim jetzigen Standpuncte der Wissenschaft nur ihrer blofsen Existenz nach anzuwenden vermag. Dies Letztere habe ich zu thun versucht, so weit es meine Kräfte erlaubten.

§. 2.

Gaufs eröffnet seine Untersuchungen über Kreistheilung mit dem Beweise der Irreductibilität der Gleichung $\frac{x^p-1}{x-1}=0$ für den einfachsten Fall, wenn p, der Divisor, die Anzahl der Theile, eine (reelle pos.) Primzahl ist:

es möchte daher passend sein, die analoge Frage auch bei der Theilung der ganzen Lemniscate an die Spitze zu stellen. Dies wird den Hauptgegenstand vorliegender Abhandlung ausmachen.

Zuvor will ich ins Gedächtnifs zurückrufen, was unter der Theilung der ganzen Lemniscate zu verstehen sei.

Man weifs, dafs bei einer solchen Theilung für den Divisor, oder was ihm analog ist, eine ganze *complexe* Zahl und im einfachsten Falle eine *complexe* Primzahl *) genommen werden kann, welche an die Stelle der reellen positiven Primzahl als der Anzahl der Theile in der Kreistheilung tritt. Die geometrischen Schwierigkeiten, welche der Begriff einer solchen complexen Division darbietet, will ich hier bei Seite stellen (Vergl. *Jacobi* im 19ten Bande dieses Journals Seite 314). In algebraischem Sinne hat man unter der ganzen Lemniscate oder ihrem Umfange denjenigen einfachsten Modul der Periodicität zu verstehen, welcher selbst und dessen ganze *complexe* Vielfache dem Argumente der lemniscatischen Function hinzugefügt werden können, ohne den Werth dieser Function zu ändern; jener Modul der complexen Periodicität ist, wenn man $\int_0^1 \frac{dx}{\sqrt{(1-x^4)}} = \varpi$ setzt, nicht 4ϖ, der Umfang der reellen geometrischen Lemniscate, sondern schon $(2+2i)\varpi$. Bezeichnet man denselben durch $C=(2+2i)\varpi$, so bedeutet die Theilung der ganzen Lemniscate, für den complexen Divisor m oder die Theilung derselben in m gleiche Theile, nichts anderes, als die Auffindung derjenigen Werthe der lemniscatischen Function, welche zunächst dem Argumente $\frac{C}{m}$ und dann auch den complexen Vielfachen $\frac{rC}{m}$ dieses Arguments entsprechen. Wegen der complexen Periodicität gehören zu congruenten Werthen von r (mod. m) gleiche Werthe der lemniscatischen Function; man hat daher nur die incongruenten zu betrachten, welche ein vollständiges Restensystem (mod. m) formiren; ihre Anzahl ist der Norm von m gleich, $= N(m) = p$. Schliefst man noch das durch den Modul m theilbare Glied aus, welches ein Vielfaches von C und für die lemniscatische Function den Werth Null giebt, so ziehen sich alle Werthe von r auf die $p-1$ Glieder eines reducirten Restensystems (mod. m) zurück. Die diesen wesent-

*) Also entweder eine solche von der Form $a+b\sqrt{-1}$, welche aus der Zerfällung einer reellen positiven Primzahl $p \equiv 1$ (mod. 4) in die Form $p=(a+b\sqrt{-1})(a-b\sqrt{-1})$ entspringt; oder eine reelle Primzahl $\pm q$, welche, abgesehn vom Zeichen, $\equiv 3$ (mod. 4) ist; beide Fälle werden vereinigt hier betrachtet; im ersten ist p, im zweiten q^2 die Norm.

lich verschiedenen Werthen von r entsprechenden lemniscatischen Functionen von $\frac{rC}{m}$ sind die Wurzeln einer algebraischen Gleichung $W=0$ vom $p-1$ten Grade mit ganzen complexen Coëfficienten. Nennt man $x=\varphi(t)$ die lemniscatische Function von t für eine unbestimmte Variabele t, $y=\varphi(mt)$ die von mt, so dafs

$$t=\int_0^x \frac{dx}{\sqrt{(1-x^4)}}, \qquad mt=\int_0^y \frac{dy}{\sqrt{(1-y^4)}},$$

und bezeichnet man durch $y=\frac{U}{V}$ diejenige rationale Function, durch welche y in x ausgedrückt wird, so ist U vom $p$ten Grade in x, durch x theilbar, und man findet die linke Seite W der eben erwähnten Gleichung $W=0$, wenn man U durch x dividirt, also $W=\frac{1}{x}U$; wie dies Alles durch *Abel* und *Jacobi* hinlänglich bekannt ist. Die auf diese Weise aus dem Zähler von y erhaltene Gleichung $W=0$ ist das Analogon zu der Gleichung $\frac{x^p-1}{x-1}=0$ oder zu den ähnlichen für die verschiedenen Arten der trigonometrischen Functionen, welche *Gaufs* am Anfange der siebenten Section seines Werkes im Vorbeigehen aufführt, und das sogenannte Problem der Theilung der ganzen Lemniscate fällt mit der algebraischen Auflösung dieser Gleichung zusammen.

Da ich mich mit der Untersuchung über die Irreductibilität der Fundamentalgleichung $W=0$ beschäftigen will, so ist zunächst zu erörtern, in welchem Sinne diese Frage hier aufgefafst werden mufs. Mit der Betrachtung der lemniscatischen Functionen ist man ganz und gar in das Gebiet der *complexen* ganzen Zahlen von der Form $a+b\sqrt{-1}$ versetzt, welche hier in jeder Hinsicht die Rolle der gewöhnlichen reellen ganzen Zahlen übernehmen. Wenn man also im Allgemeinen unter einer irreductibeln Gleichung mit ganzen Coëfficienten eine solche versteht, von welcher keine Wurzel zugleich Wurzel einer Gleichung niederen Grades mit ebenfalls ganzen Coëfficienten sein kann, so wird hier bei unserer Gleichung das Wort „ganz" beide Male in complexem Sinne zu nehmen sein; nämlich, wenn irgend eine Wurzel der Gleichung $W=0$ zugleich Wurzel einer Gleichung niederen Grades $Z=0$ ist, so mufs gezeigt werden, dafs Z *weder mit reellen, noch* (was mehr behauptet und das erste als speciellen Fall einschliefst) mit *complexen ganzen* Coëfficienten angenommen werden kann.

Die Einleitung zum Beweise dieses Satzes besteht in Folgendem. Hätte

Z ganze complexe Coëfficienten, so könnte man durch die Operation der Aufsuchung des gröfsten gemeinschaftlichen Theilers zwischen W und Z eine ganze Function mit ebenfalls ganzen oder sicher rationalen complexen Coëfficienten finden, welche in W algebraisch aufgeht. W, welches die Form

$$W = x^{p-1} + A_1 x^{p-5} + A_2 x^{p-9} + \ldots + A_{\frac{1}{4}(p-1)}$$

hat, wo $A_1, A_2, \ldots$ sämmtlich ganze complexe Zahlen sind, zerfiele demnach in das Product zweier ganzen Functionen mit rationalen complexen Coëfficienten. Nach einem von *Gaufs* in den „Disq. Arithm. Art. 42." zunächst für reelle Zahlen aufgestellten Satze, dessen Beweis sich aber wörtlich auf complexe Zahlen anwenden läfst, müfsten sich die Factoren auf eine solche Form bringen lassen, dafs ihr höchstes Glied die Einheit zum Coëfficienten hat, und dafs alle übrigen Coëfficienten ganze complexe Zahlen sind. Es bliebe also nur noch die Unmöglichkeit einer Zerfällung von folgender Form nachzuweisen:

$$W = (x^\mu + a_1 x^{\mu-1} + a_2 x^{\mu-2} + \ldots.)(x^\nu + b_1 x^{\nu-1} + b_2 x^{\nu-2} + \ldots.),$$

wo $\mu + \nu = p-1$, $0 < \mu < p-1$, $0 < \nu < p-1$, und alle a und alle b ganze complexe Zahlen sind.

Bis hierher sind die Betrachtungen denen der Kreistheilung ganz analog und lassen sich auf jede Gleichung anwenden. Versucht man aber in derselben Weise wie bei *Gaufs* weiter zu gehen, so stöfst man auf Schwierigkeiten von der Art, wie sie schon in §. 1. angedeutet sind. Diese Schwierigkeiten, welche sich durch die ganze Theorie der Lemniscatentheilung hindurchziehen, liegen daran, dafs die ***Relationen*** zwischen den Wurzeln der Gleichung $W = 0$, wie folgenreich auch die Kenntnifs ihrer blofsen Existenz und ihres allgemeinen algebraischen Characters sein mag, doch viel zu complicirt und ihrer speciellen Beschaffenheit nach viel zu unbekannt sind, um jene Wurzeln einfachen Operationen (z. B. der Multiplication) mit derselben Leichtigkeit unterwerfen zu können, wie dies bei den Wurzeln der Einheit geschieht. Mit einem Worte: man kann nicht aus jenen Relationen *selbst* Vortheil ziehn, weil man sie nicht kennt, sondern nur aus allgemeinen Eigenschaften derselben, und man mnfs daher die Zahl der letztern zu vermehren suchen.

Der Beweis unseres Satzes gelingt, wenn man eine Eigenschaft der Coëfficienten $A_1, A_2, \ldots.$ zu Hülfe nimmt, welche ich bei einer früheren Gelegenheit schon, wenigstens für eine zweigliedrige (nicht reelle) complexe Primzahl m aufgestellt und bewiesen habe. Nämlich den Satz, dafs sämmt-

liche Coëfficienten $A_1, A_2, \ldots A_{\frac{1}{4}(p-1)}$ durch m theilbar sind, und dafs der letzte, abgesehn von einer complexen Einheit, welche als Factor hinzutreten kann, m selbst gleich ist. Dieser Satz läfst sich auch so aussprechen: Nennt man zwei ganze Functionen von x, wie $a+a'x+a''x^2+\ldots$ und $b+b'x+b''x^2+\ldots$ congruent (mod. m), wenn einzeln und für alle Coëfficienten $a \equiv b$, $a' \equiv b'$, $a'' \equiv b''$, ... (mod. m) ist, so hat man $W \equiv x^{p-1}$ (mod. m) und $A_{\frac{1}{4}(p-1)} = \varepsilon m$, wo ε eine complexe Einheit ist. Die höchst einfache Methode, durch welche ich aus dieser Eigenschaft der Coëfficienten von W die Irreductibilität der Gleichung $W=0$ ziehe, liefert zugleich den Beweis des folgenden allgemeineren Satzes, welcher die Irreductibilität einer sehr ausgedehnten Gattung von algebraischen Gleichungen ausspricht:

„Wenn in einer ganzen Function $F(x)$ von x von beliebigem Grade „der Coëfficient des höchsten Gliedes $=1$ ist, und alle folgenden Coëfficienten „ganze (reelle, complexe) Zahlen sind, in welchen eine gewisse (reelle resp. „complexe) Primzahl m aufgeht, wenn ferner der letzte Coëfficient $=\varepsilon m$ ist, „wo ε eine nicht durch m theilbare Zahl vorstellt: so ist es unmöglich $F(x)$ „auf die Form

$$(x^\mu + a_1 x^{\mu-1} + \ldots + a_\mu)(x^\nu + b_1 x^{\nu-1} + \ldots + b_\nu)$$

„zu bringen, wo μ und $\nu \geqq 1$, $\mu+\nu =$ dem Grad von $F(x)$, und alle a „und b (reelle resp. complexe) *ganze* Zahlen sind; und die Gleichung $F(x)=0$ „ist demnach irreductibel."

Wäre obige Zerfällung von $F(x)$ möglich, so hätte man zunächst $a_\mu b_\nu =$ dem letzten Coëfficienten von $F(x)$, also $=\varepsilon m$: folglich müfste, da m als Primzahl vorausgesetzt worden ist, eine der beiden Zahlen a_μ, b_ν, $=\varepsilon'$, die andere $=\varepsilon'' m$ sein, wo ε', ε'' zwei Factoren, deren Product $=\varepsilon$ ist, welche also beide nicht durch m theilbar sind. Es sei, da die Wahl willkürlich ist, $a_\mu = \varepsilon'$, $b_\nu = \varepsilon'' m$. Nach den gemachten Voraussetzungen ist ferner $F(x) \equiv x^{\mu+\nu}$ (mod. m); es wäre also

$$(x^\mu + a_1 x^{\mu-1} + \ldots + \varepsilon')(x^\nu + b_1 x^{\nu-1} + \ldots + \varepsilon'' m) \equiv x^{\mu+\nu} \text{ (mod. } m),$$

folglich auch, nach Weglassung des durch m theilbaren Gliedes $\varepsilon'' m$ im zweiten Factor links:

$$(x^\mu + a_1 x^{\mu-1} + \ldots + \varepsilon')(x^\nu + b_1 x^{\nu-1} + \ldots + b_{\nu-1} x) \equiv x^{\mu+\nu}.$$

Der Coëfficient von x ist hier $\varepsilon' b_{\nu-1}$, und da ein Glied mit der ersten Potenz von x rechts nicht vorkommt, so ist $\varepsilon' b_{\nu-1}$, also auch $b_{\nu-1}$ durch m theilbar. Läfst man wiederum das Glied $b_{\nu-1} x$ aus dem zweiten Factor links weg, so

erhält man eine dritte Congruenz, aus der zu sehen, dafs $b_{\nu-2}$ durch m theilbar sein mufs; der zweite Factor links kann daher abermals um ein Glied $b_{\nu-2}x^2$ vermindert werden. So fortfahrend, zeigt sich nach und nach, dafs sämmtliche $b \equiv 0 \pmod{m}$ sein müssen, und man wird zuletzt zu der Congruenz

$$(x^\mu + a_1 x^{\mu-1} + \ldots + \varepsilon').x^\nu \equiv x^{\mu+\nu} \pmod{m}$$

geführt. Diese ist aber offenbar unmöglich, da sich links multiplicando das *nicht* durch m theilbare Glied $\varepsilon' x^\nu$ ergiebt, zu welchem sich rechts kein entsprechendes findet. Demnach kann auch die ursprüngliche Zerfällung von $F(x)$ ohne Widerspruch nicht angenommen werden, und es ergiebt sich die Richtigkeit des obigen Satzes.

Die Gleichung $W = 0$ befindet sich unmittelbar in dem Falle des allgemeinen Satzes *), und ihre Irreductibilität ist somit erwiesen. Die Gleichung $\frac{x^p - 1}{x - 1} = 0$, wo p eine positive ungerade Primzahl, läfst sich durch eine leichte Substitution ebenfalls auf die Form bringen, welche der Satz verlangt. Man setze $x - 1 = z$, so wird $x = z + 1$ und man bekommt die Gleichung

$$z^{p-1} + pz^{p-2} + \tfrac{1}{2}p(p-1)z^{p-3} + \ldots + p = 0,$$

in der alle Coëfficienten durch p theilbar sind und der letzte $= p$ selbst ist. Dies giebt also, wenn man will, einen neuen und höchst einfachen Beweis der Irreductibilität der Gleichung $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$; und zwar setzt dieser Beweis im Unterschiede mit früheren **) nicht die Kenntnifs der Wurzeln und ihrer gegenseitigen Abhängigkeit voraus. — Die analogen Gleichungen für die trigonometrischen Functionen sind ebenfalls sämmtlich in dem allgemeinen Satze enthalten.

Der obige Satz läfst sich noch leicht dahin verallgemeinern: dafs die Gleichung $F(x) = 0$ auch dann noch irreductibel ist, wenn nur ein einziger der durch m theilbaren Coëfficienten in $F(x)$ nicht mit m^2 aufgeht, und es braucht dies nicht gerade der letzte zu sein, so dafs jede Gleichung mit ganzen Coëfficienten irreductibel ist, in welcher, aufser dem ersten, sämmtliche Coëfficienten durch m, aber nicht sämmtlich durch m^2 theilbar sind.

Ich will gelegentlich den häufig vorkommenden Satz beweisen, dafs bei einem Producte zweier ganzen ganzzahligen Functionen $S(x)T(x)$, welches $\equiv 0 \pmod{m \text{ Primzahl}}$ ist, nothwendig einer der beiden Factoren durch m

*) Siehe §. 3.

**) Aufser dem Beweise von *Gaufs* ist mir nur der von *Kronecker* im 29ten Bande dieses Journals Seite 280 bekannt.

theilbar sein mufs. Wäre dies nicht der Fall, d. h. wären in *keinem* der beiden Factoren *sämmtliche* Coëfficienten durch m theilbar, so müfste es in *jedem* derselben eine *niedrigste* Potenz von x geben (diese kann auch x^0 sein), deren Coëfficient nicht durch m theilbar ist. Es sei dies x^σ in $S(x)$ und x^τ in $T(x)$, den Fall σ oder $\tau = 0$ nicht ausgeschlossen, so dafs die Coëfficienten von $x^{\sigma-1}$, $x^{\sigma-2}$ etc. in $S(x)$ und die von $x^{\tau-1}$, $x^{\tau-2}$ etc. in $T(x)$ wirklich durch m theilbar sind; in dem Producte $S(x)T(x)$ wäre dann der Coëfficient von $x^{\sigma+\tau} \equiv$ dem Producte der beiden Coëfficienten von x^σ und x^τ in $S(x)$ resp. $T(x)$; dieser Coëfficient wäre also nicht durch m theilbar, was der Voraussetzung widerstreitet, nach welcher alle Coëfficienten des entwickelten Productes $\equiv 0 \pmod m$ sein sollen. — Aus diesem Satze folgt durch wiederholte Anwendung der weiter oben benutzte, welcher sich, wenigstens für reelle Zahlen, wie bemerkt, in „Disq. Arith. 42." findet. Es ist offenbar nur zu beweisen, dafs in einer Gleichung von der Form

$$k.(x^{\mu+\nu} + c_1 x^{\mu+\nu-1} + \ldots + c_{\mu+\nu})$$
$$= (a_0 x^\mu + a_1 x^{\mu-1} + \ldots + a_\mu).(b_0 x^\nu + b_1 x^{\nu-1} + \ldots + b_\nu) = S(x)\,T(x),$$

wo k und alle a, b, c ganze (reelle oder complexe) Zahlen sind, der Multiplicator k immer so auf die beiden ganzen Functionen S und T vertheilt werden kann, dafs k dem Producte zweier ganzen Factoren $k_1 k_2$ gleich wird, von denen der eine k_1 in $S(x)$, der andere k_2 in $T(x)$ aufgeht. Dies ergiebt sich daraus, dafs für jeden Primfactor m von k, $S(x)T(x) \equiv 0 \pmod m$ ist, also nach dem Obigen entweder $S(x)$ oder $T(x)$ mit m aufgeht. Dividirt man wirklich m weg, so erhält man eine neue Gleichung von derselben Form, in welcher $\frac{k}{m}$ an die Stelle von k getreten ist, nämlich entweder

$$\frac{k}{m}.(x^{\mu+\nu} + \text{etc.}) = \frac{1}{m} S(x).T(x) \quad \text{oder} \quad \frac{k}{m}(x^{\mu+\nu} + \text{etc.}) = S(x).\frac{1}{m} T(x),$$

je nachdem S oder T durch m theilbar ist. In dieser Gleichung kann man abermals einen neuen oder denselben Primfactor von $\frac{k}{m}$ fortheben, je nachdem m nur in der ersten Potenz, oder im Quadrat u. s. w. in k aufgeht. Durch wiederholte Anwendung dieses Verfahrens wird man endlich alle gleichen und ungleichen Primfactoren von k, also das ganze k selbst erschöpft und weggeschafft haben, und es hat sich zugleich k in der angegebenen Weise auf die beiden Factoren S und T vertheilt. Zuletzt erhält man dann eine Gleichung von der Form

$$x^{\mu+\nu} + \text{etc.} = (a_0' x^\mu + a_1' x^{\mu-1} + \text{etc.})(b_0' x^\nu + b_1' x^{\nu-1} + \text{etc.});$$

wo alle Coëfficienten ganz sind und wo, wegen $a_0' b_0' = 1$, $a_0' = b_0' = 1$ angenommen werden kann. Dem Wesen nach ist dieses Verfahren von demjenigen bei *Gauſs* nicht verschieden. Die Grundbetrachtungen über solche Congruenzen, deren Elemente ganze *Functionen* sind, findet man auch in *Schoenemann's* Abhandlung in diesem Journal Band 31. Seite 269 ff.

Aus der bewiesenen Irreductibilität der Gleichung $W = 0$ kann man die gewöhnlichen Folgerungen für die Wurzeln derselben ziehen. Wenn eine ganze Function mit rationalen complexen Coëfficienten und von niederem Grade als dem $p-1$ten, für eine Wurzel der Gleichung $W = 0$ verschwindet, so verschwinden ihre sämmtlichen Coëfficienten; und wenn zwei solche Functionen für eine Wurzel jener Gleichung gleich werden, so müssen ihre entsprechenden Coëfficienten übereinstimmen. Wenn irgend eine ganze Function mit rationalen complexen Coëfficienten für eine solche Wurzel verschwindet, so ist sie durch W algebraisch theilbar und verschwindet also für alle Wurzeln der Gleichung $W = 0$; sind zwei dergleichen ganze Functionen für eine Wurzel einander gleich, so gilt dies ebenfalls für alle Wurzeln, da ihre Differenz durch W theilbar ist, u. s. w. Für die Gleichung $W = 0$ insbesondere ergiebt sich wegen der speciellen Eigenschaften ihrer Wurzeln noch Folgendes. Diese Wurzeln sind in der Form $\varphi\left(\frac{rC}{m}\right)$ enthalten, wo r die $p-1$ Glieder eines reducirten Restensystems (mod. m) durchläuft; welche man alle als *ungerade* Zahlen voraussetzen kann. Diese Wurzeln sind auch $\varphi\left(\frac{rkC}{m}\right)$, wo k eine beliebige nicht durch m theilbare complexe ganze Zahl ist. Hat man nun eine Relation, wie $F(k) = 0$, zwischen diesen Wurzeln, in der letzteren Form, wo $F(k)$ eine ganze Function der Wurzeln mit rationalen complexen Coëfficienten bedeutet, und findet diese Relation für irgend einen Werth von k Statt, so muſs sie für jeden Werth von k richtig bleiben: denn da $\varphi\left(\frac{rkC}{m}\right)$ für jeden ungeraden Werth von r als rationale Function von $\varphi\left(\frac{kC}{m}\right)$ also, nach Wegschaffung des Nenners mit Hülfe der Gleichung $W = 0$, auch als ganze Function mit rationalen (nicht ganzen) Coëfficienten von $\varphi\left(\frac{kC}{m}\right)$ dargestellt werden kann, so verwandelt sich der ganze Ausdruck $F(k)$ in eine ganze Function von der *einen* Gröfse $\varphi\left(\frac{kC}{m}\right)$; wobei die Coëfficienten rational und von k *unabhängig* sind. Verschwindet aber eine solche Function für *einen*

Werth von k, so mufs sie wegen der Irreductibilität für jeden Werth von k verschwinden. Die Einführung des Factors k unter dem Zeichen φ kommt, wie man leicht sieht, auf eine sogenannte cyclische Permutation der Wurzeln hinaus; in jeder Relation von der angegebenen Art kann man also die Wurzeln *cyclisch* permutiren; woraus natürlich *nicht* folgt, dafs *jede* Permutation der Wurzeln erlaubt wäre.

§. 3.

Die Grundlage des Beweises der Irreductibilität der Gleichung $W=0$ bildet die oben erwähnte Eigenschaft der Coëfficienten der Function W. Ich habe, wie bemerkt, den Beweis dieser Eigenschaft für den einen Fall gegeben, wenn m eine zweigliedrige complexe Primzahl $a+bi$, also $a^2+b^2=p$ eine reelle Primzahl $\equiv 1 \pmod 4$ ist; es bleibt noch der Fall $m=\pm q$, wo q eine reelle positive Primzahl $\equiv 3 \pmod 4$ ist. Ich habe auch die Schwierigkeit angedeutet *), welche sich der früheren Methode in diesem zweiten Falle entgegenstellt, obwohl der Satz selbst richtig bleibt **). Es ist daher nöthig, im Folgenden einen neuen Beweis aufzustellen, der beide Fälle zugleich umfafst; um so mehr, da dieser Satz als Ausgangspunct auch für fast alle ferneren Untersuchungen in diesem Felde dient, und da es wichtig ist, in der Folge von einer besonderen Rücksichtsnahme auf die Unterscheidung der beiden eben erwähnten Fälle der Primzahl m befreit zu sein.

1) Entwickelt man für einen beliebigen ungeraden Werth von m die rationale Function von x, welche $y=\varphi(mt)$ in $x=\varphi(t)$ ausdrückt, nämlich $y=\frac{A_{\frac{1}{4}(p-1)}x+\text{etc.}}{1+B_1x^4+\text{etc.}}=\frac{U}{V}=\frac{xW}{V}$, in eine unendliche Reihe nach steigenden Potenzen von x, so werden die Coëfficienten dieser Reihe sämmtlich zu ganzen complexen Zahlen, da das niedrigste Glied des Divisors $=1$ ist, also bei der wirklichen Division von U durch V kein numerischer Nenner in den Coëfficienten eintreten kann. Setzt man demnach

$$y=R=c_1x+c_5x^5+c_9x^9+\ldots+c_{4\mu+1}x^{4\mu+1}+\text{in inf.},$$

so sind $c_1=A_{\frac{1}{4}(p-1)}$, $c_5=A_{\frac{1}{4}(p-5)}-B_1A_{\frac{1}{4}(p-1)}$, u. s. w., wie bemerkt, sämmtlich ganze Zahlen. Es kommt hier wenig darauf an, ob diese Reihe convergirt, oder nicht, da ich nicht ihre Summe, sondern nur ihre Coëfficienten

*) Gegenw. Journal Band 30. Seite 188.

**) Er ist aber nicht mehr richtig, wenn man für m eine reelle positive Primzahl $\equiv 1$ (mod. 4) setzen wollte.

betrachte; übrigens convergirt die Reihe bekanntlich sicher, wenn der analytische Modul von $x <$ als der kleinste unter den Moduln der Wurzeln der Gleichung $V = 0$ ist, was aber für die hier Statt findenden Untersuchungen gleichgültig ist.

2) Man kann dieselbe Reihe R auf einem ganz anderen Wege als dem der Division erhalten, wenn man direct nach der Methode der unbestimmten Coëfficienten und mit Hülfe der Gleichung

$$\int_0^y \frac{\partial y}{\sqrt{(1-y^4)}} = m \int_0^x \frac{\partial x}{\sqrt{(1-x^4)}}$$

y nach Potenzen von x entwickelt. Man findet auf diesem Wege, dafs $c_1 = m$, $c_5 = \frac{1}{10}(m - m^5)$, etc. und dafs der allgemeine Coëfficient die Form

$$c_{4\mu+1} = \frac{1}{\varrho}(\alpha_1 m + \alpha_5 m^5 + \alpha_9 m^9 + \ldots\ldots + \alpha_{4\mu+1} m^{4\mu+1}) = \frac{1}{\varrho} f(m)$$

hat, wo alle α und der Nenner ϱ nur von μ abhängige von m unabhängige ganze Zahlen sind, und wo man natürlich immer annehmen kann, dafs ϱ keinen Factor enthält, der in allen α zugleich aufgeht. Um dieses Resultat ohne viele Rechnung übersehen zu können, entwickele man $\varphi(mt)$ nach Potenzen von mt und setze statt der Potenzen von t in dieser Entwicklung die ihnen gleichen Reihen nach $x = \varphi(t)$. Es sei

$$\int_0^x \frac{\partial x}{\sqrt{(1-x^4)}} = t = x + \beta_5 x^5 + \beta_9 x^9 + \text{etc.},$$
$$t^\nu = x^\nu + \beta^{(\nu)}_{\nu+4} x^{\nu+4} + \beta^{(\nu)}_{\nu+8} x^{\nu+8} + \text{etc.},$$

endlich

$$x = \varphi(t) = t + \gamma_5 t^5 + \gamma_9 t^9 + \text{etc.},$$

wobei sämmtliche β und γ rein numerische und rationale Werthe haben und die $\beta^{(\nu)}$ nur von ν abhangen und ebenfalls rational sind. Da $y = \varphi(mt)$ ist, so erhält man hiernach

$$\begin{aligned} y &= mt + \gamma_5 m^5 t^5 + \gamma_9 m^9 t^9 + \ldots\ldots + \gamma_{4\mu+1} m^{4\mu+1} t^{4\mu+1} + \text{etc.} \\ &= m(x + \beta_5 x^5 + \beta_9 x^9 + \ldots\ldots + \beta_{4\mu+1} x^{4\mu+1} + \text{etc.}) \\ &\quad + \gamma_5 m^5 (x^5 + \beta^{(5)}_9 x^9 + \ldots\ldots + \beta^{(5)}_{4\mu+1} x^{4\mu+1} + \text{etc.}) \\ &\quad + \gamma_9 m^9 (x^9 + \ldots\ldots + \beta^{(9)}_{4\mu+1} x^{4\mu+1} + \text{etc.}) \\ &\quad + \text{etc.} \end{aligned}$$

und hier ist der Coëfficient von $x^{4\mu+1}$:

$$c_{4\mu+1} = \beta_{4\mu+1} . m + \gamma_5 \beta^{(5)}_{4\mu+1} . m^5 + \gamma_9 \beta^{(9)}_{4\mu+1} . m^9 + \ldots\ldots + \gamma_{4\mu+1} . m^{4\mu+1};$$

welcher in der That von der oben angegebenen Form ist. Die so gefundene

Reihe für y gilt natürlich für jeden beliebigen unbestimmten Werth von m, sie läfst sich aber nur dann durch eine rationale Function $\frac{U}{V}$ summiren, oder besser als aus der Entwicklung einer solchen hervorgehend betrachten, wenn m eine *ganze* und *ungerade* complexe Zahl ist.

3) $f(m)$ ist eine ganze ganzzahlige Function von m, welche den Factor m enthält. Da man nun für ganze ungerade Werthe von m bereits weifs, dafs $c_{4\mu+1}$ einer ganzen Zahl gleich ist, nämlich aus der Entwicklung von $y = \frac{U}{V}$ durch Division, so folgt, dafs $c_{4\mu+1}$ in allen den Fällen durch m theilbar ist, wenn m Primzahl, und der Nenner ϱ den Factor m *nicht* enthält. Ich behaupte, dafs ϱ überhaupt nur solche ungerade complexe Primfactoren enthalten kann, deren Norm $\leqq 4\mu+1$ ist. In der That sei n irgend ein ungerader complexer Primtheiler von ϱ, also irgend ein Primtheiler, mit Ausnahme von $1+i$; da $\frac{1}{\varrho} f(m)$ eine ganze Zahl für alle ungeraden (auch zusammengesetzten) Werthe von m ist, so hat man $f(m) \equiv 0 \pmod{\varrho}$, also auch $\pmod{n}$ für dieselben Werthe von m; da aber n ungerade ist, so kann man zu jeder beliebigen ganzen Zahl eine ihr congruente $\pmod{n}$ ungerade Zahl finden und es wird daher die Congruenz $f(m) \equiv 0 \pmod{n}$ für alle ganzen complexen Werthe von m ohne Ausnahme erfüllt. Betrachtet man auf die gewöhnliche Weise nur die incongruenten Wurzelwerthe, so hat die Congruenz $f(z) \equiv 0 \pmod{n}$ genau $N(n)$ Wurzeln, nämlich alle Glieder eines vollständigen Restensystems $\pmod{n}$. Da nun keine Congruenz mehr Wurzeln haben kann, als ihr Grad beträgt, der hier $4\mu+1$ ist, so hat man, wie behauptet worden war, $N(n) \leqq 4\mu+1$. Es folgt hieraus *a fortiori*, dafs sämmtliche Nenner ϱ der ersten Coëfficienten c_1, c_5 bis $c_{4\mu+1}$ nur solche complexe Primfactoren haben, deren Norm $\leqq 4\mu+1$ ist, und die der Coëfficienten c_1, c_5 bis $c_{4\mu-3}$ nur solche, deren Norm $< 4\mu+1$ ist. Dieser an sich wichtige Satz dient hier nur als Lemma, er wird in der Folge noch mannigfaltige Anwendungen finden.

4) Nehmen wir jetzt die Voraussetzung wieder auf, welche wir einen Augenblick fallen liefsen, dafs m Primzahl sein soll, und setzen wie immer $N(m) = p$, so zeigt sich, dafs m in keinem der Nenner ϱ der ersten Coëfficienten c_1, c_5 bis c_{p-4} aufgehen kann und dafs c_p der erste ist, welcher m in seinem Nenner enthalten könnte. Es sind daher nach der obigen Bemerkung am Anfange von 3) die Coëfficienten aller Potenzen von x unter x^p

durch m theilbare ganze Zahlen, und die Reihe selbst hat die Form $y = R = m.S + x^p.T$, wo S und T Reihen nach x mit ganzen Coëfficienten sind, und noch zu bemerken ist, dafs der Coëfficient der ersten Potenz von x in S, $= 1$ ist.

Multiplicirt man jetzt in der gefundenen Gleichung

$$\frac{U}{V} = \frac{xW}{V} = m.S + x^p.T,$$

mit V auf die rechte Seite hinüber, so ergiebt sich

$$U = xW = m.VS + x^p.VT,$$

und man sieht, dafs alle Coëfficienten in U, den von x^p allein ausgeschlossen, durch m theilbar sein müssen, weil auf der rechten Seite, wenn man entwickelt, wirklich alle Glieder mit niedrigeren Potenzen als x^p den Factor m enthalten. Es ist also

$$A_{\frac{1}{2}(p-1)} \equiv A_{\frac{1}{2}(p-5)} \equiv \ldots \equiv A_2 \equiv A_1 \equiv 0 \pmod{m}.$$

Diese Congruenzen in Verbindung mit der Bemerkung, dafs $A_{\frac{1}{2}(p-1)} = c_1 = m$ ist, enthalten die zu beweisende Eigenschaft.

5) Es läfst sich hiermit die Relation verbinden, die zwischen den Coëfficienten des Zählers U und denen des Nenners V Statt findet. Nimmt man nämlich im Allgemeinen U von der Form $\varepsilon(A_{\frac{1}{2}(p-1)} + \ldots + x^p)$ an, so wird $V = 1 + A_1 x^4 + \ldots + A_{\frac{1}{2}(p-1)}$. Diese Relation findet sich schon bei *Jacobi*, nur nicht die Bestimmung der complexen Einheit ε, welche für meine Untersuchungen von grofser Wichtigkeit ist. Für einen primären Werth von m, d. h. für $m \equiv 1 \pmod{2+2i}$ ist $\varepsilon = 1$ und man hat daher den Satz:

„Dafs für jede primäre complexe Primzahl m, gleichviel ob eingliedrig „oder zweigliedrig, die lemniscatische Function $\varphi(mt)$ von mt in $\varphi(t)$ „durch den Bruch

$$\varphi(mt) = \frac{\varphi(t)^{N(m)} + m.P}{1 + m.Q}$$

„ausgedrückt wird, wo P und Q ganze complex-ganzzahlige Functionen „von $\varphi(t)$ sind."

Zur Erläuterung dieses Beweises möge noch Folgendes hinzugefügt werden.

6) Da für eine primäre Primzahl m, deren Norm p ist, $U \equiv x^p$ und $V \equiv 1 \pmod{m}$ gefunden wurde, so erhält man, wenn man in die Gleichung $U = VR$ substituirt, $x^p \equiv R \pmod{m}$; d. h. alle Coëfficienten der Reihe

$R = c_1 x + c_5 x^5 +$ etc. bis ins Unendliche mit alleiniger Ausnahme von c_p sind durch m theilbar, und c_p ist $\equiv 1 \pmod{m}$. Das erstere, nämlich die Theilbarkeit der Coëfficienten durch m gilt auch für eine *nicht* primäre Primzahl m; dann ist aber nicht mehr $c_p \equiv 1$, sondern im Allgemeinen einer gewissen complexen Einheit congruent.

7) Nimmt man als bewiesen an, dafs in der Reihe R alle Coëfficienten, aufser c_p, durch m theilbar sind, so läfst sich hieraus die Congruenz $c_p \equiv 1 \pmod{m}$ für einen *primären* Werth von m, ohne besondere auf diesen Fall bezügliche Voraussetzung über U und V, auf folgende Art ableiten, welche wegen des Princips für allgemeinere Untersuchungen nützlich ist. Man hat $R \equiv c_p x^p \pmod{m}$, und da $U = VR$, so folgt $U \equiv c_p x^p . V$. Diese letztere Congruenz enthält nur endliche geschlossene Ausdrücke (ganze Functionen), und man darf daher statt x einen speciellen Werth, z. B. $x = 1$ setzen; was bei einer Congruenz mit unendlichen Reihen keinesweges erlaubt sein würde: denn ganz abgesehen von der Frage, betreffend die Convergenz, so hat auch eine unendliche Reihe im Allgemeinen keinen bestimmten arithmetischen Character, da sie, aus lauter rationalen Termen bestehend, doch recht wohl eine irrationale so gut als eine rationale Zahl ausdrücken kann *). Setzt man also $x = 1$ in der zuletzt erhaltenen Congruenz $U \equiv c_p x^p . V$, so ergiebt sich $u \equiv c_p v$, wenn durch $\frac{u}{v}$ der Werth von y bezeichnet wird, der $x = 1$ entspricht; es ist also c_p der Werth des Ausdrucks $\frac{u}{v} \pmod{m}$. Da $x = 1$ dem Werthe $t = \int_0^1 \frac{\partial x}{\sqrt{(1-x^4)}} = \varpi$ entspricht, und da die lemniscatische Function sich nicht ändert, wenn t um ganze complexe Vielfache von $(2+2i)\varpi = C$ wächst, so ist $\frac{u}{v} = \varphi(m\varpi) = \varphi(\varpi)$, also ebenfalls $= 1$, wenn $m \equiv 1 \pmod{2+2i}$; in diesem Falle also $c_p \equiv 1 \pmod{m}$. Im Allgemeinen ist $\frac{u}{v} = \varphi(m\varpi) = \varphi(i^\mu \varpi) = i^\mu \varphi(\varpi) = i^\mu$ also $c_p \equiv i^\mu \pmod{m}$, wenn $m \equiv i^\mu \pmod{2+2i}$, und bekanntlich ist jede ungerade Zahl irgend einer Potenz von i congruent $\pmod{2+2i}$, so dafs diese Annahme alle Fälle umfafst.

---

*) Die Betrachtung solcher Congruenzen, in denen unendliche Reihen vorkommen, scheint, wenn man sie auf sichere Principien zurückführt, sehr fruchtbar für die Zahlentheorie werden zu können. Vielleicht sollte die VIII. Section der *Disq.* auch dergleichen enthalten.

8) In der Entwicklung von $\frac{\partial y}{\partial x} = \frac{\partial R}{\partial x}$ sind alle Coëfficienten ohne Ausnahme durch m theilbar; denn durch das Differentiiren nach x tritt $(4\mu+1).c_{4\mu+1}$ an die Stelle von $c_{4\mu+1}$, und in diesem Producte ist für alle von p verschiedenen Werthe des Index $4\mu+1$ der zweite Factor, für $4\mu+1=p$ der erste Factor durch m theilbar. Die Entwicklung von $\frac{1}{m}\frac{\partial y}{\partial x}$ enthält demnach lauter ganze Coëfficienten, also auch die Entwicklung des gleichgeltenden Ausdrucks $\frac{\sqrt{(1-y^4)}}{\sqrt{(1-x^4)}}$. Letztere wird erhalten, wenn man die beiden Quadratwurzeln entwickelt, welche beide mit $+1$ anfangen, und statt der Potenzen von y die entsprechenden Potenzen der Reihe R setzt. Da $R \equiv x^p \pmod{m}$ ist, so vernachlässigt man nur Vielfache von m, wenn man hierbei x^p an die Stelle von y schreibt; man erhält so

$$\frac{1}{m}\frac{\partial y}{\partial x} \equiv \sqrt{\left(\frac{(1-x^4)^p}{1-x^4}\right)} \equiv \sqrt{\left(\frac{(1-x^4)^p}{1-x^4}\right)} \equiv (1-x^4)^{\frac{1}{4}(p-1)} \pmod{m}.$$

Dafs die bei der Entwicklung der Quadratwurzeln vorkommenden Nenner, welche nur Potenzen von 2 sein können, unberücksichtigt bleiben dürfen und der Strenge des Raisonnements keinen Abbruch thun, davon will ich der Kürze wegen die weitere Ausführung einer Gelegenheit überlassen, bei welcher ich überhaupt die algebraischen Functionen in dieser Hinsicht untersuchen werde. Man kann bei Congruenzen immer solche Nenner vernachlässigen, in denen der Modul nicht als Factor enthalten ist und braucht zu dem Ende den Begriff der Congruenz nur dahin zu erweitern, dafs man unter $\frac{a}{b} \equiv \frac{c}{d} \pmod{m}$, wo b und d beide nicht durch m aufgehen, nichts anders verstehen will, als $ad-bc \equiv 0 \pmod{m}$ *). — Setzt man $p = mm' = (a+bi)(a-bi)$, so ist in der gefundenen Congruenz $\frac{1}{m}\frac{\partial y}{\partial x} \equiv (1-x^4)^{\frac{1}{4}(p-1)} \pmod{m}$ der Coëfficient von x^{p-1} links $= m'c_p$, welches $\equiv m' \pmod{m}$ ist für einen primären Werth von m. Bezeichnet man durch

$$\Gamma = \frac{(-1)^{\frac{1}{4}(p-1)}(\frac{1}{2}(p-1))!}{(\frac{1}{4}(p-1))!(\frac{1}{4}(p-1))!} = (-1)^{\frac{1}{4}(p-1)} \cdot \frac{\frac{1}{2}(p-1).\frac{1}{2}(p-3)\ldots.\frac{1}{4}(p+3)}{1.2\ldots.\frac{1}{4}(p-1)}$$

den entsprechenden Coëfficienten rechts in $(1-x^4)^{\frac{1}{4}(p-1)}$, so hat man $m' \equiv \Gamma \pmod{m}$. Es ist dies der von *Gaufs* gefundene und am Schlusse der

*) Zwei algebraische Ausdrücke sind überhaupt congruent (mod. m), wenn das Resultat der Elimination aus den beiden irreductibeln Gleichungen mit ganzen Coëfficienten, welchen sie genügen, in homogener Form $\equiv 0 \pmod{m}$ ist.

ersten Abtheilung seiner biquadratischen Reste bewiesene merkwürdige Satz. Bemerkenswerth ist die Form, in welcher er hier auftritt, da eine primäre Primzahl in Bezug auf ihre conjugirte Primzahl als Modul bestimmt wird; man kann ihm leicht die gewöhnliche Form geben, wenn man auf beiden Seiten mit m' multiplicirt; dies giebt m'^2, d. h. $(a-bi)^2 \equiv \Gamma.(a-bi) \pmod{p}$, also $a^2-b^2 \equiv a\Gamma$ und $2ab \equiv b\Gamma \pmod{p}$, folglich, wenn b von Null verschieden ist, $2a \equiv \Gamma \pmod{p}$, wie bei *Gaufs*. Da m primär ist so hat man $a \equiv 1$ oder $\equiv -1 \pmod{4}$, je nachdem $p \equiv 1$ oder $\equiv 5 \pmod{8}$. Ich will hiermit nur ein ganz neues Princip zum Beweise solcher Sätze andeuten und überlasse einer späteren Gelegenheit die weitere Ausführung, welche sich an eine allgemeinere Betrachtung der am Anfang erwähnten Classe elliptischer Functionen anschliefst. Ich bemerke noch, dafs, wenn man auch die anderen Coëfficienten von $\frac{1}{m}\frac{\partial\gamma}{\partial x}$ betrachten will, allgemein $\frac{4\mu+1}{m}c_{4\mu+1} \equiv$ dem Coëfficienten von $x^{4\mu}$ in $(1-x^4)^{\frac{1}{2}(p-1)} \pmod{m}$ gefunden wird; hierdurch wird $c_{4\mu+1}$ in Bezug auf den Modul m^2 bestimmt. Man könnte noch weiter gehen und den allgemeinen Coëfficienten der Reihe R auch in Bezug auf m^3 und höhere Potenzen von m als Moduln bestimmen.

9) Dafs der Nenner ϱ des allgemeinen Coëfficienten $c_{4\mu+1}$ in der Form $\frac{1}{\varrho}f(m)$ keine andern complexen Primfactoren enthält, als solche, deren Norm $\leqq 4\mu+1$ ist, sieht man auch auf folgende, mehr elementare Weise ein, ohne den Satz über die gröfste Anzahl der Wurzeln einer Congruenz und ohne die Voraussetzung, dafs die Coëfficienten von U und V ganze Zahlen sind, und dafs V mit 1 anfängt, zu Hülfe zu nehmen. Aus der Art und Weise, wie die Potenzen einer gegebenen Reihe und die durch Umkehrung entstehende Reihe gebildet werden, geht hervor, dafs mit Beibehaltung der Bezeichnung in (2.), die Coëfficienten $\beta^{(\nu)}_{\nu+4}$, $\beta^{(\nu)}_{\nu+8}$, ... bis $\beta^{(\nu)}_{\nu+4\mu}$ für jeden ganzen positiven Werth von ν, und die Coëfficienten γ_5, γ_9, ... bis $\gamma_{4\mu+1}$ in Rücksicht der Primfactoren keine anderen Nenner enthalten können, als solche, die schon in β_5, β_9, ... $\beta_{4\mu+1}$ vorkommen. Es folgt dies aus einer wiederholten Anwendung des Satzes, dafs die Summe und das Product zweier Brüche in ihrem Nenner nur solche Primfactoren enthalten können, welche schon in den Nennern der beiden gegebenen Brüche aufgehen; denn für jede Reihe von der Form

$$t = x + \alpha x^2 + \beta x^3 + \ldots + \lambda x^{h+1} + \text{in. inf.}\ ^*)$$

*) Wenn die erste Potenz von x einen von 1 verschiedenen Coëfficienten hat, so tritt dieser oder doch sein Zähler bei der Umkehrung der Reihe noch als Nenner hinzu.

sind alle in der Entwicklung von t^ν bis zu dem Gliede mit $x^{h+\nu}$ und alle in der umgekehrten Reihe für x nach t bis zu dem Gliede mit t^{h+1} enthaltenen Coëfficienten *ganze ganzzahlige* Functionen der h Gröfsen $\alpha, \beta, \ldots . \lambda$, welche in der ursprünglichen Reihe bis zum Gliede mit x^{h+1} als Coëfficienten vorkommen, und wenn die letzteren als rational vorausgesetzt werden, so kann jeder Primfactor im Nenner des Werthes einer solchen Function nur aus den Nennern der ursprünglichen Elemente $\alpha, \beta, \ldots . \lambda$ entspringen, welche man als auf ihre kleinste Benennung gebracht annehmen darf. Für den hier vorliegenden Fall ist also, in Rücksicht auf die Bildungsweise von $c_{4\mu+1}$ in 2), nur zu zeigen, dafs die Coëfficienten der Reihe für $t = \int_0 \frac{\partial x}{\sqrt{(1-x^4)}}$ bis zu dem Gliede mit $x^{4\mu+1}$ incl. als *nothwendigen* Nenner, d. h. als einen solchen, der sich nicht fortheben läfst, keinen complexen Primfactor enthalten können, dessen Norm $> 4\mu+1$ ist, d. h. keine reelle positive Primzahl $\equiv 1 \pmod 4$, welche $> 4\mu+1$ und keine reelle positive Primzahl $\equiv 3 \pmod 4$, deren Quadrat $> 4\mu+1$ ist. Aus der Form des allgemeinen Coëfficienten

$$\beta_{4\mu+1} = \frac{1.3.5 \ldots . (2\mu-1)}{2.4.6 \ldots . 2\mu} \frac{1}{4\mu+1} = \frac{1.2.3.4 \ldots . (2\mu)}{(2.3 \ldots . 2\mu)^2} \frac{1}{4\mu+1}$$
$$= \frac{(2\mu)!}{2^{2\mu}(\mu!)^2} \frac{1}{4\mu+1} = \Delta,$$

ist schon beim blofsen Anblick ersichtlich, dafs derselbe überhaupt keinen Divisor $> 4\mu+1$ im Nenner enthält. Es bleibt also nur noch zu zeigen, dafs der Ausdruck Δ auch keine Primzahl $\equiv 3 \pmod 4$, deren Quadrat $> 4\mu+1$ ist, als nothwendigen Nenner enthält. Es läfst sich nun leicht untersuchen, wie oft *irgend* eine Primzahl q, d. h. in einer wie hohen Potenz sie im Zähler und im Nenner von Δ enthalten ist. Nach einem schon von ***Legendre*** angewandten Principe enthält das Product $1.2.3 \ldots . z$ resp. eine Anzahl von $E\left(\frac{z}{q}\right)$, $E\left(\frac{z}{q^2}\right)$, $E\left(\frac{z}{q^3}\right)$, etc. Zahlen, welche respective durch q, q^2, q^3, etc. theilbar sind, wo allgemein $E(u)$ die gröfste in u enthaltene ganze Zahl bedeutet, und es ist daher der Exponent der höchsten in jenem Producte aufgehenden Potenz von q, $= E\left(\frac{z}{q}\right) + E\left(\frac{z}{q^2}\right) + E\left(\frac{z}{q^3}\right) +$ etc. Setzt man zuerst $z = 2\mu$, dann $z = \mu$, um den Factor $\frac{(2\mu)!}{(\mu!)^2}$ von Δ zu untersuchen, so zeigt sich, dafs die Differenz

$$E\left(\frac{2\mu}{q}\right)+E\left(\frac{2\mu}{q^2}\right)+E\left(\frac{2\mu}{q^3}\right)+\ldots.$$
$$-2E\left(\frac{\mu}{q}\right)-2E\left(\frac{\mu}{q^2}\right)-2E\left(\frac{\mu}{q^3}\right)-\ldots.,$$

je nachdem sie positiv oder negativ ist, anzeigt, wie oft q respective im Zähler oder im Nenner von $\frac{(2\mu)!}{(\mu!)^2}$ nach allen Reductionen verbleibt. Jene Differenz, welche δ bezeichnen mag, ist aber nie negativ, weil allgemein $E(2u) \geqq 2E(u)$, und zwar kann die Differenz $E(2u)-2E(u)$ überhaupt nur die beiden Werthe 0 oder 1 haben: denn setzt man $u=E(u)+r$, wo $0 \leqq r < 1$, so folgt $2u = 2E(u)+2r$; entweder ist nun $2r$ auch noch <1, wenn $r<\frac{1}{2}$, und dann hat man $E(2u) = 2E(u)$, oder es ist $2r \geqq 1$ aber noch <2, wenn $\frac{1}{2} \leqq r < 1$, und dann hat man $E(2u) = 2E(u)+1$ *). Da der Werth von δ nur positiv oder Null sein kann, und zwar für jede *beliebige* Primzahl q, so geht hervor, dafs, wie auch sonst bekannt, $\frac{(2\mu)!}{(\mu!)^2}$ einer ganzen Zahl M gleich ist; diese geht durch q^δ und keine höhere Potenz von q auf, und es kann $\Delta = \frac{M}{2^{2\mu}} \cdot \frac{1}{4\mu+1}$ aufser der Primzahl 2 nur Theiler von $4\mu+1$ als nothwendige Primfactoren des Nenners enthalten. Da also die Nichttheiler von $4\mu+1$ hierdurch beseitigt sind, so sei q Theiler von $4\mu+1$ und $4\mu+1 = q.k$. Wenn aufserdem $q^2 > 4\mu+1$ vorausgesetzt wird, so ist $k<q$, also geht q nur in der ersten und keiner höheren Potenz in $4\mu+1$ auf, und q kann daher sicher fortgehoben werden, wenn nur mindestens $\delta = 1$ und nicht $=0$ ist. Unter der Voraussetzung $q^2 > 4\mu+1$ besteht ferner δ nur aus den beiden Gliedern $E\left(\frac{2\mu}{q}\right)-2E\left(\frac{\mu}{q}\right)$, weil dann *a fortiori* $2\mu < q^2$ ist und somit alle folgenden Glieder verschwinden; hier kann also δ nur die beiden Werthe 0 oder 1 haben, und zwar ist $\delta = 0$ oder $=1$, je nachdem der Rest von $\mu \pmod q$ unter oder über $\frac{1}{2}q$ liegt; nach diesen beiden Fällen wird also q im Nenner von Δ verbleiben oder *nicht* verbleiben; nun findet gerade der erste oder zweite dieser beiden Fälle Statt, je nachdem $q \equiv 1$ oder $\equiv 3 \pmod 4$ ist. Denn erstlich für $q \equiv 1 \pmod 4$ folgt aus $4\mu+1 = qk$, dafs auch $k \equiv 1 \pmod 4$; setzt man also $q = 4h+1$, $k = 4l+1$, so erhält man $\mu = \frac{1}{4}(qk-1) = ql+h$, wo der Rest h sogar $< \frac{1}{4}q$ ist. Zweitens für $q \equiv 3 \pmod 4$ ist auch

*) *Gaufs* hat dies bei seinem dritten Beweise des quadratischen Fundamentaltheorems angewendet.

$k \equiv 3 \pmod 4$, also wenn man $q = 4h+3$, $k = 4l+3$ setzt, so folgt $\mu = \frac{1}{4}(qk-1) = ql+3h+2$, wo der Rest $3h+2 > \frac{1}{2}q$ ist. Aus diesem Allen geht hervor, dafs unter sämmtlichen Primzahlen, deren Quadrat $> 4\mu+1$ ist, nur diejenigen im Nenner von Δ nothwendiger Weise zurückbleiben, welche in $4\mu+1$ aufgehen und zugleich von der Form $4h+1$ sind. Diese bleiben aber auch wirklich nach allen Reductionen zurück und aufser ihnen nur Primzahlen, welche die Quadratwurzel aus $4\mu+1$ nicht übersteigen. Da in jeder Zahl höchstens *eine* Primzahl aufgehen kann, welche ihre Quadratwurzel übersteigt, so ist es besser, dieses Resultat so auszusprechen: Wenn $4\mu+1$ einen ihre Quadratwurzel übersteigenden Primfactor enthält, so bleibt dieser im Nenner von Δ, oder er hebt sich fort, je nachdem er von der Form $4h+1$ oder $4h+3$ ist.

(Die Fortsetzung folgt im nächsten Heft.)