16.

Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind.

(Von Herrn *C. G. J. Jacobi*, Professor ordin. an der Universität zu Königsberg in Pr.)

(Gelesen in der Akademie der Wissenschaften den 16. Mai 1839.)

Gauſs hat in seinen Untersuchungen über die biquadratischen Reste die complexen Zahlen von der Form $a+b\sqrt{-1}$ als Moduln oder Divisoren eingeführt. Indem er dieses that, konnte er über den biquadratischen Character zweier complexen Primzahlen von der Form $a+b\sqrt{-1}$ in Bezug auf einander ein Reciprocitätsgesetz von solcher Einfachheit und Vollendung aufstellen, wie das berühmte Fundamentaltheorem über quadratische Reste, das von ihm sogenannte Kleinod der höhern Arithmetik besitzt. Aber wie einfach jetzt auf eine solche Einführung der complexen Zahlen als Moduln erscheinen mag, so gehört sie nicht desto weniger zu den tiefsten Gedanken der Wissenschaft; ja ich glaube nicht, dafs zu einem so verborgenen Gedanken die Arithmetik allein geführt hat, sondern dafs er aus dem Studium der elliptischen Transcendenten geschöpft worden ist, und zwar der besondern Gattung derselben, welche die Rectification von Bogen der Lemniscata giebt. In der Theorie der Vervielfachung und Theilung von Bogen der Lemniscata spielen nämlich die complexen Zahlen von der Form $a+b\sqrt{-1}$ genau die Rolle gewöhnlicher Zahlen. Wie man durch rationale Ausdrücke die trigonometrischen Functionen des $n$fachen Kreisbogens darstellt, so kann man vermittelst rationaler Formeln den Bogen der Lemniscata mit einer complexen Zahl $a+b\sqrt{-1}$ multipliciren; wie man den Kreisbogen durch Auflösung einer Gleichung vom n^{ten} Grade in n Theile theilt, so theilt man den Bogen der Lemniscata in $a+b\sqrt{-1}$ Theile durch Auflösung einer Gleichung vom Grade $aa+bb$. So wie man einen Kreisbogen, wenn man ihn in 15 Theile theilen soll, in 3 und in 5 Theile theilt und aus beiden Theilungen die gesuchte findet, so hat man einen Bogen der Lemniscata, um ihn in 17 Theile zu theilen, in $1+4\sqrt{-1}$ und in $1-4\sqrt{-1}$ Theile zu theilen und setzt die Theilung in 17 Theile

aus beiden zusammen. So wird man bei Untersuchung jener besondern Gattung elliptischer Integrale, wenn man nur einigermafsen in ihre Natur eindringt, mit Nothwendigkeit darauf hingedrängt, die Zahlen $a+b\sqrt{-1}$ als Divisoren einzuführen. Mögen nun auch jene Untersuchungen der Integralrechnung viel complicirter und schwieriger erscheinen als jener einfache Gedanke der Zahlenlehre, so ist es doch nicht immer das einfache, welches sich zuerst darbietet. *Gaufs* versichert in den *Disquisitiones arithm.* die Methode seiner Kreistheilung auf die Theilung der ganzen Lemniscata anwenden zu können und verspricht hierüber ein *amplum opus* zu einer Zeit, in welcher er sich sicher noch nicht, seinen eigenen spätern Angaben zufolge, mit den biquadratischen Resten beschäftigt hatte. Auch ist es nicht unwahrscheinlich, dafs er die Fundamentaltheoreme über biquadratische Reste aus dieser Quelle geschöpft hat. Erst *Abel* hat dieses Versprechen von *Gaufs* eingelöst, indem er wenigstens die ersten Grundzüge dieser Ausdehnung der *Gaufs*'schen Methoden der Kreistheilung auf die Theilung der Lemniscata in seinen ersten, im gegenwärtigen Journal publicirten Arbeiten über die elliptischen Transcendenten gab. Eine eben so interessante als schwierige Aufgabe dürfte es sein, dieser Theilung des Lemniscatenbogens in $a+b\sqrt{-1}$ Theile und der Zusammensetzung der p^{ten} Theile des Bogens aus seiner Theilung in $a+b\sqrt{-1}$ und in $a-b\sqrt{-1}$ Theile einen geometrischen Sinn abzugewinnen. Die Geometrie hat in neuerer Zeit mit Glück dem Imaginären auch auf ihrem Gebiete einen Platz angewiesen; es ist zu erwarten, dafs sie bei dem bewundernswürdigen Aufschwung, welchen sie unter *Steiners* Händen genommen hat, sich auch dieser abstruseren Ideen bemächtigen wird.

Es hat keines neuen Gedankens bedurft, um die kubischen Reciprocitätsgesetze zu finden; man hatte hierzu nur nöthig auf ganz analoge Weise complexe Zahlen von der Form $\frac{a+b\sqrt{-3}}{2}$, oder solche, die aus den Cubikwurzeln der Einheit zusammengesetzt sind, als Moduln oder Divisoren einzuführen. Auch diese Untersuchungen kann man mit der Theorie besonderer elliptischer Integrale in Verbindung setzen. Das Reciprocitätsgesetz für kubische Reste, welches ich in einer frühern Note mitgetheilt habe, ist noch einfacher wie das von *Gaufs* für die biquadratischen Reste aufgestellte, und ergiebt sich ganz unmittelbar aus bekannten Formeln der Kreistheilung.

Nachdem *Gauſs* in seiner zweiten Abhandlung über biquadratische Reste die Elemente der complexen Zahlen von der Form $a+b\sqrt{-1}$ abgehandelt, bleibt es übrig, unter den Methoden und Resultaten der Arithmetik diejenigen auszumitteln, welche auch für diese complexe Zahlen ihre Gültigkeit haben. So zum Beispiel sieht man leicht, daſs die *Lagrange*sche Methode, die quadratischen Formen zu reduciren, auch auf solche Ausdrücke $pyy+qyz+rzz$ sich ausdehnen läſst, in welchen p, q, r, y, z complexe Zahlen der angegebenen Art bedeuten. Um die einfachste complexe Form zu nehmen, $yy-\sqrt{-1}.zz$, kann man beweisen, daſs jede Zahl $a+b\sqrt{-1}$, welche solche Form theilt, wiederum dieselbe Form haben müsse, und der Beweis ist vollkommen dem Beweise des bekannten Satzes analog, daſs jede Zahl, welche die Form $yy+zz$ theilt, wiederum die Summe zweier Quadrate ist. Ist $p=aa+bb$ eine Primzahl von der Form $8n+1$, so beweist man aus den Elementen der Theorie dieser complexen Zahlen sogleich, daſs $\sqrt{-1}$ quadratischer Rest von $a+b\sqrt{-1}$ ist, oder, was dasselbe ist, $a+b\sqrt{-1}$ Theiler einer Form $yy-\sqrt{-1}.zz$ ist, also nach dem eben bemerkten Satze selber diese Form hat. Zertheilt man diese Form in die beiden Factoren $y+\sqrt[4]{-1}.z$ und $y-\sqrt[4]{-1}.z$, und setzt

$$y = y'+y''\sqrt{-1}, \quad z = z'+z''\sqrt{-1},$$

wo y', y'', z', z'' reelle ganze Zahlen bedeuten, so erhält man $a+b\sqrt{-1}$ in zwei Factoren,

$$y'+y''\sqrt{-1}+\sqrt[4]{-1}\,[z'+z''\sqrt{-1}],$$
$$y'+y''\sqrt{-1}-\sqrt[4]{-1}\,[z'+z''\sqrt{-1}],$$

zerfällt, das ist in zwei complexen Zahlen, welche aus den 8ten Wurzeln der Einheit zusammengesetzt sind. Schreibt man α für die 8te Wurzel der Einheit oder für $\sqrt[4]{-1}$, und setzt

$$\Phi\alpha = y'+y''\alpha^2+z'\alpha+z''\alpha^3,$$

so wird

$$a+b\sqrt{-1} = a+b\alpha^2 = \Phi\alpha.\Phi\alpha^5$$

und, wenn man α^3 für α setzt,

$$a-b\sqrt{-1} = a-b\alpha^2 = \Phi\alpha^3.\Phi\alpha^7.$$

Die Primzahl $p=aa+bb$, von der Form $8n+1$, ist daher immer das Product der vier complexen Zahlen

$$\Phi\alpha.\Phi\alpha^3.\Phi\alpha^5.\Phi\alpha^7.$$

Man sieht leicht, daſs das Product $\Phi\alpha.\Phi\alpha^3$ die Form $c+d\sqrt{-2}$ und das Product $\Phi\alpha.\Phi\alpha^7$ die Form $e+f\sqrt{2}$ erhält. Die drei Arten, auf

welche man die vier Factoren in zwei Paare ordnen kann, geben daher die Darstellungen derselben Primzahl in den drei Formen a^2+b^2, c^2+2d^2, e^2+2f^2, welche hier aus einer gemeinschaftlichen Quelle abgeleitet sind, so dafs die sechs Zahlen a, b, c, d, e, f auf rationale Art durch vier andre Zahlen y', y'', z', z'' ausgedrückt werden. Man kann diese Zerfällung der Primzahlen von der Form $8n+1$ in vier complexe Factoren, welche aus acht Wurzeln der Einheit zusammengesetzt sind, auch durch die gewöhnlichen Methoden der Arithmetik ableiten. Ganz durch dieselben Methoden beweist man auch, dafs die Primzahlen von der Form $12n+1$ sich in vier complexe Factoren zerfällen lassen, welche aus 12^{te} Wurzeln der Einheit zusammengesetzt sind; die drei verschiedenen Arten, wie man diese vier Factoren zu zwei Paaren ordnen kann, geben die Darstellungen der Primzahl durch die drei Formen a^2+b^2, c^2+3d^2, e^2-3f^2. Man kann für die Auffindung dieser Zerfällungen leichte Vorschriften angeben, nach welchen Herr Oberlehrer *Zornow* in Königsberg mir für die Primzahlen von der Form $8n+1$ und $12n+1$ bis 1000 diese Zerfällungen zu berechnen die Güte gehabt hat.

Zu gleicher Zeit, als ich diese Betrachtungen anstellte, richtete ich meine Aufmerksamkeit auf gewisse Eigenschaften der complexen Zahlen, auf welche die Theorie der Kreistheilung führt. Ich habe in der erwähnten Note bemerkt, dafs wenn λ ein Theiler von $p-1$ ist, sich die Primzahl p und in der Regel auf mehrere verschiedene Arten als Product zweier complexen Zahlen darstellen läfst, welche aus λ^{ten} Wurzeln der Einheit zusammengesetzt sind. Es ereignet sich nun, und man kann dies durch die Theorie der Kreistheilung selbst beweisen, dafs man mehrere dieser complexen Zahlen mit einander multipliciren und das Product wieder durch andre complexe Zahlen derselben Art dividiren kann, so dafs der Quotient ebenfalls eine ganze complexe Zahl wird, ohne dafs man sieht, wie die complexen Zahlen des Nenners sich gegen die des Zählers fortheben. Eine genaue Betrachtung dieses merkwürdigen Umstandes führte mich zu der Ueberzeugung, dafs diese complexe Factoren der Primzahl p im Allgemeinen selbst wieder zusammengesetzt sein müssen, so dafs, wenn man sie in die wahren complexen Primzahlen auflöst, die complexen Primzahlen, welche die Factoren des Nenners bilden, gegen die Primfactoren des Zählers sich einzeln aufheben lassen. Da ich auf ganz anderem Wege zu diesem Resultate bereits für $\lambda = 8$ und $\lambda = 12$ gekommen war,

so wagte ich den etwas mühsamen Versuch mit $\lambda = 5$, und in der That gelang es mir für die Primzahlen von der Form $5n+1$, mit welchen ich den Versuch anstellte, jeden ihrer beiden aus 5^{ten} Wurzeln der Einheit zusammengesetzten Factoren noch einmal in zwei ganze Factoren derselben Art zu zerfällen; worauf es dann nicht schwer war einen allgemeinen Beweis für diese Zerfällbarkeit zu finden. So lassen sich also die Primzahlen von der Form $5n+1$, $8n+1$, $12n+1$ als Producte von vier ganzen complexen Zahlen darstellen, welche respective aus 5^{te}, 8^{te}, 12^{te} Wurzeln der Einheit zusammengesetzt sind. Es erhellt übrigens, dafs für die Primzahlen von der Form $5n+1$ durch eine andre paarweise Verbindung der vier Factoren ihre Darstellung in der Form $a^2 - 5b^2$ erhalten wird.

Die neuen Factoren sind nothwendig Primzahlen. Ist nämlich $f\alpha$ einer derselben, wo α für die drei Arten Primzahlen respective eine primitive 5^{te}, 8^{te}, 12^{te} Wurzel der Einheit ist, so kann $f\alpha$ nicht als Product zweier ganzer complexen Zahlen derselben Art $\varphi\alpha$ und $\psi\alpha$ dargestellt werden, wenn nicht eine derselben so beschaffen ist, dafs das Product ihrer vier Werthe der Einheit gleich ist. Denn man sieht leicht, dafs das Product der vier Werthe von $f\alpha$, $\varphi\alpha$, $\psi\alpha$ eine reelle Zahl ist, und da das Product der vier Werthe von $f\alpha$ eine Primzahl ist, so können nicht die beiden andern Producte reelle Zahlen geben, welche beide zugleich von der Einheit verschieden sind, da ihr Product der Primzahl gleich wird.

Zwischen diesen Primzahlen $f\alpha$ hat man in der Theorie der Reste der 5^{ten}, 8^{ten} und 12^{ten} Potenzen die Reciprocitätsgesetze aufzusuchen, und es würde vielleicht thunlich sein, dieselben durch blofse Induction zu finden, nachdem man ihre wahre Form kennt, wenn nicht solche Induction überaus beschwerlich wäre. Wenn man die Reciprocitätsgesetze auf zusammengesetzte Zahlen ausdehnt, ganz ähnlich wie ich es in der früher der Akademie mitgetheilten Note in Bezug auf die quadratischen, kubischen und biquadratischen Reste gethan habe, so können unmittelbar aus der Theorie der Kreistheilung die einfachen Reciprocitätssätze, in Bezug auf die Reste der 5^{ten}, 8^{ten} und 12^{ten} Potenzen, für den besondern Fall abgeleitet werden, wenn die eine Zahl reell ist. Ob es möglich sein wird, vermittelst neuer Kunstgriffe aus derselben Quelle die allgemeineren Sätze für je zwei complexe Zahlen abzuleiten, mufs von späteren Untersuchungen zu entscheiden vorbehalten bleiben.