Untersuchungen über die biquadratischen Reste und Nichtreste der Primzahlen von der Form $4n+1$.

§. 1.

Der erste Beweis des quadratischen Reziprozitätsgesetzes, wie ihn Legendre in seiner théorie des nombres gegeben hat, gilt in aller Strenge nur für die Primzahlen von der Form $4n+3$, $8n+5$ und diejenigen von der Form $8n+1$, welche Nichtreste zu 3 sind; die übrigen können nur insofern mit hinzugezogen werden, als eine spezielle Berechnung für jede einzelne darthut, daß sie Nichtrest zu irgend einer Primzahl $4n+3$ ist, oder durch Nachweisung der Allgemeingültigkeit dieses Postulates. Der Beweis selbst beruht auf einer Zerlegung der Gleichung $y^2 = px^2 + 1$ in zwei andere, wobei p das nichtquadratische Produkt der zu vergleichenden Primzahlen allein oder mit einer dritten bezeichnet. Die eben genannte Gleichung hängt wiederum ab von der Entwickelung der Quadratwurzel aus p in einen Kettenbruch. Um Wiederholungen zu vermeiden sollen zunächst die Grundgedanken von Legendre's Darstellung angegeben werden, und zwar mit einigen Erweiterungen, die für das Folgende wesentlich sind.

Es führt nemlich die Entwickelung von $\sqrt{p}$ in einen Kettenbruch zu Näherungswerthen $\frac{y}{x}$, die sämmtlich Gleichungen von der Form $y^2 = px^2 \pm r$ genügen. Die Reste r werden ebenso wie die Kettenbruchsnenner wiederkehrend periodisch gefunden, und zwar so, daß wenn

$$\sqrt{p} = a + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cdots + \cfrac{1}{\alpha_2 + \cfrac{1}{\alpha_1 + \cfrac{1}{2a + \cfrac{1}{\alpha_1 + \cdots}}}}}}$$

1

ist, den Näherungswerthen

$$\frac{a}{1}, \quad \frac{aa_1 + 1}{a_1}, \quad \ldots\ldots$$

die Reste

$$-r_0, \quad +r_1, \quad -r_2, \quad \ldots \quad \pm r_2, \quad \mp r_1, \quad \ldots\ldots$$

entsprechen. Unter den unbestimmten Gleichungen befinden sich auch solche von der besondern Form

$$(1.) \qquad y^2 = px^2 + 1,$$

die ebenfalls periodisch wiederkehren; jedoch soll weiterhin unter (1.) immer diejenige verstanden werden, in welcher y und x die kleinsten möglichen Werthe annehmen, mit Ausschluß von $y = 1$, $x = 0$. In besondern Fällen, wenigstens jedesmal dann, wenn p eine ungerade Primzahl von der Form $4n + 1$ ist, existiren ebenfalls periodisch wiederkehrend unzählig viele Gleichungen

$$(2.) \qquad y^2 = px^2 - 1,$$

deren kleinste aus der Gleichung (1.) leicht abgeleitet werden kann. Soll sie für zusammengesetzte Zahlen p möglich sein, so ist nothwendige Bedingung, daß p, außer dem Faktor 2^μ, nur Primzahlen von der Form $4n + 1$ enthalte, da niemals die Kongruenz $y^2 \equiv -1$, (mod. $4n + 3$) stattfinden kann. Hinreichend ist übrigens diese Bedingung keineswegs.

Von Legendre *) ist ferner bewiesen, daß, im Fall die Gleichung (2.) möglich ist, in der Mitte der ersten Periode der Näherungswerthe, ebenso auch in allen anderen, zwei derartige auf einander folgende vorhanden sein müssen, daß sie den Gleichungen

$$(a.) \qquad y_1^2 = px_1^2 \pm a \quad \text{und} \quad y_2^2 = px_2^2 \mp a$$

genügen; gleichzeitig ist a an die Bedingung geknüpft, daß $p = a^2 + b^2$ wird; ein Satz, aus dem die Zerlegung der Primzahlen $4n + 1$ in die Summe zweier Quadrate hervorgeht.

Wenn p ungerade ist, so läßt sich auch noch entscheiden, welcher Art die Größe a sein muß. Es sei nemlich in $p = a^2 + b^2$ die Größe a ungerade, b also gerade. Unter der Annahme, daß b der in der Mitte der Periode zweimal auftretende Rest ist, hätte man dann die Gleichungen

$$(b.) \qquad \left\{ \begin{array}{l} y_1^2 = px_1^2 \pm b \\ y_2^2 = px_2^2 \mp b, \end{array} \right\}$$

---

*) Diese Entwickelungen finden sich in der théorie des nombres, 3. ed. tom. I. pag. 49 — 71.

wobei $\frac{y_1}{x_1}$ und $\frac{y_2}{x_2}$ zwei auf einander folgende Näherungswerthe darstellten; bekanntlich würde in diesem Falle

$$y_1x_2 - y_2x_1 = \pm 1$$

gefunden werden. Durch Quadriren erhält man

$$y_1^2x_2^2 + y_2^2x_1^2 = 1 + 2y_1y_2x_1x_2. \qquad \text{(c.)}$$

Andrerseits folgt aus den Gleichungen (b.)

$$y_1^2y_2^2 - p(y_1^2x_2^2 + y_2^2x_1^2) + p^2x_1^2x_2^2 = -b^2,$$

oder da $-b^2 = -p + a^2$, durch Anwendung der Gleichung (c.)

$$y_1^2y_2^2 - p - 2py_1y_2x_1x_2 + p^2x_1^2x_2^2 = -p + a^2,$$

und hieraus

$$y_1y_2 - px_1x_2 = \pm a. \qquad \text{(d.)}$$

Nun sind y_1 und x_1, y_2 und x_2 als Näherungswerthe eines Kettenbruchs prim zu einander, und da b in den Gleichungen (b.) gerade ist, so müssen y_1, x_1, y_2, x_2 ungerade Zahlen sein, indem sie außerdem nur gleichzeitig gerade sein könnten, also nicht prim wären. Dazu ist aber nöthig, daß b mindestens den Faktor 4 enthalte, was für $p = 8n + 5$ nicht möglich ist. Im anderen Falle, nemlich $p = 8n + 1$, findet man dann aus der Gleichung (d.), daß $\pm a$ als die Differenz von zwei ungeraden Größen gerade ist, was der Voraussetzung widerspricht. Demnach sind, unter den angegebenen Bedingungen, nur die Gleichungen (a.) möglich, in welchen a eine ungerade Zahl bedeutet.

§. 2.

Nach diesen Voraussetzungen soll nun zu dem eigentlichen Gegenstande der vorliegenden Untersuchungen übergegangen werden, zur Bestimmung der biquadratischen Beziehungen zwischen ungeraden nicht komplexen Primzahlen von der Form $4n + 1$.

Legendre leitet in seinem Beweise des quadratischen Reziprozitätsgesetzes aus der Gleichung $y^2 = \alpha\beta\gamma x^2 + 1$, wo α eine Primzahl $4n + 1$, β und γ Primzahlen $4n + 3$ bedeuten, andere Gleichungen, wie z. B. $\alpha\beta \cdot u^2 = \gamma \cdot v^2 \pm 1$, ab, in denen die Größen α, β, γ theilweise von einander getrennt vorkommen. Mittelst des im Anfange angegebenen Postulates muß dann über die Existenz oder Nichtexistenz einer jeden von diesen Gleichungen entschieden werden, Bestimmungen, die leichter, wie es Gauss in den disquisitiones arithmeticae gethan hat, von dem Reziprozitätsgesetze erst abhängig zu machen sind, indem nemlich in der Gleichung $ax^2 + 2bxy + cy^2 = M$ die Bedingung erfüllt werden muß, daß $b^2 - ac$ quadratischer Rest zu M. Wenn $M = 1$ wird, so ist auf die quadratischen Beziehungen der Größen a, b, c

zu einander zurückzugehen. Inzwischen ist, wenn $b = 0$ gesetzt wird und a und c Primzahlen sind, die Eigenschaft der einen von diesen quadratischer Rest oder Nichtrest der andern zu sein, nicht immer allein hinreichend, die Möglichkeit einer aus den beiden Zahlen zu bildenden unbestimmten Gleichung des zweiten Grades darzuthun, so daß z. B. die Gleichung $au^2 - bv^2 = \pm 1$, worin a und b Primzahlen von der Form $4n + 1$ sein mögen, zu den unmöglichen gehören kann, obgleich a und b quadratische Reste zu einander sind. In diesem Falle kommt es vielmehr, wie bald dargethan werden soll, darauf an, ob die eine der beiden Primzahlen biquadratischer Rest oder Nichtrest der andern ist.

Es sei, wie schon oben festgestellt wurde,

$$(1.) \qquad y^2 = px^2 + 1$$

die Auflösung dieser unbestimmten Gleichung in den kleinsten Zahlenwerthen; ferner sei

$$p = \alpha\delta$$

das Produkt von zwei Primzahlen α und δ von der Form $4n + 1$, p also von derselben Form. Dann ist in (1.) y nothwendig ungerade, x gerade, so daß man daraus die Gleichung

$$\frac{y+1}{2} \cdot \frac{y-1}{2} = \alpha\delta\left(\frac{x}{2}\right)^2$$

ableiten kann. Die ganzen Zahlen $\frac{y+1}{2}$ und $\frac{y-1}{2}$, die sich um die Einheit unterscheiden, haben keinen gemeinsamen Faktor. Nimmt man demnach an, daß $\alpha\delta$ in $\frac{y-1}{2}$ aufgehe, so wird

$$\frac{y-1}{2} = \alpha\delta \cdot u^2, \quad \frac{y+1}{2} = v^2$$

zu setzen sein, wo auf den rechten Seiten die quadratischen Formen u^2 und v^2 genommen werden müssen, weil ihr Produkt ein Quadrat $\left(\frac{x}{2}\right)^2$ ist, während die Größen selbst keine gemeinschaftlichen Faktoren haben. Hieraus würde folgen

$$v^2 = \alpha\delta u^2 + 1,$$

eine Gleichung, die der Voraussetzung nach nicht stattfinden kann, weil sie eine Auflösung der Gleichung (1.) in kleineren Zahlen wäre. Es bleiben also zwei Fälle zu untersuchen, nemlich erstens der, daß $\alpha\delta$ in $\frac{y+1}{2}$ aufgeht, oder

$$\frac{y+1}{2} = a\delta u^2, \quad \frac{y-1}{2} = v^2$$

oder

$$v^2 = a\delta u^2 - 1 \qquad (2.)$$

zu setzen ist.

Der zweite Fall ist der, daß eine der beiden Primzahlen, z. B. a, in $\frac{y+1}{2}$, die andere δ in $\frac{y-1}{2}$ aufgeht, wobei

$$\frac{y+1}{2} = au^2, \quad \frac{y-1}{2} = \delta v^2,$$

genommen werden muß, also die Gleichung

$$au^2 - \delta v^2 = 1 \qquad (3.)$$

entsteht. Diese beiden Fälle schließen einander aus, und da der zweite nur dann eintreten kann, wenn a und δ quadratische Reste zu einander sind, so folgt nothwendig, daß die Gleichung (2.) bestehen muß, wenn a und δ quadratische Nichtreste zu einander sind. Die Umkehrung aber, daß die Gleichung (3.) stattfinden müßte, wenn a und δ quadratische Reste zu einander sind, ergiebt sich hieraus nicht.

Schon eine mäßig ausgedehnte Induktion innerhalb der Grenzen der Tafel X. in Legendre's théorie des nombres, tom. I. (wo die kleinsten Zahlenwerthe zur Auflösung der Gleichung $y^2 = px^2 \pm 1$ angegeben sind, aus denen man leicht entscheiden kann, ob auf der rechten Seite das obere oder untere Vorzeichen zu nehmen ist), und auf diejenigen Zahlen a und δ beschränkt, welche quadratische Reste zu einander sind, führt zu ganz anderen Bestimmungen. Die letztere Beschränkung rechtfertigt sich durch das in Bezug auf Nichtreste so eben gewonnene Resultat. Die Gleichung $y^2 = a\delta x^2 - 1$ ist hiernach möglich für folgende Zahlen

$$145 = 5 \cdot 29, \quad 445 = 5 \cdot 89, \quad 901 = 17 \cdot 53. \qquad (4.)$$

Die Gleichung $y^2 = a\delta x^2 - 1$ ist nicht möglich, oder die andere $au^2 - \delta v^2 = 1$ ist möglich für:

$$\left.\begin{array}{l} 205 = 5 \cdot 41, \ 221 = 17 \cdot 13, \ 305 = 5 \cdot 61, \ 377 = 13 \cdot 29, \\ 505 = 5 \cdot 101, \ 545 = 109 \cdot 5, \ 689 = 13 \cdot 53, \ 745 = 149 \cdot 5, \\ 793 = 13 \cdot 61, \ 905 = 5 \cdot 181. \end{array}\right\} \qquad (5.)$$

Es sind nun die biquadratischen Reste der hier vorkommenden Zahlen in der Tafel enthalten:

Zahlen.	Biquadratreste.
5	1.
13	1, 3, 9.
17	1, 4, 13, 16.
29	1, 7, 16, 20, 23, 24, 25.
41	1, 4, 10, 16, 18, 23, 25, 31, 37, 40.
53	1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49.
61	1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58.
89	1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44, 45, 50, 57, 64, 67, 73, 78, 81, 85, 87, 88.
101	1, 5, 16, 19, 24, 25, 31, 36, 37, 52, 54, 56, 58, 68, 71, 78, 79, 80, 81, 84, 87, 88, 92, 95, 97.
109	1, 3, 5, 7, 9, 15, 16, 21, 22, 25, 26, 27, 35, 38, 45, 48, 49, 63, 66, 73, 75, 78, 80, 81, 89, 97, 105.
149	1, 5, 6, 16, 17, 19, 25, 28, 29, 30, 31, 33, 36, 37, 49, 63, 67, 73, 80, 81, 83, 85, 88, 95, 97, 102, 104, 106, 107, 117, 123, 125, 127, 129, 140, 142, 145.
181	1, 3, 5, 9, 13, 14, 15, 16, 25, 27, 29, 34, 38, 39, 42, 43, 44, 45, 48, 59, 62, 65, 70, 73, 75, 80, 81, 82, 87, 102, 114, 117, 121, 125, 126, 129, 132, 135, 144, 145, 148, 161, 169, 170, 177.

Man sieht sogleich, daß zu (4.) diejenigen Zahlen gehören, welche beide zu einander biquadratische Nichtreste sind, zu (5.) diejenigen, wo wenigstens die eine biquadratischer Rest der andern ist. Zur bequemeren Uebersicht sind die Faktoren a und δ hier jedesmal so gestellt, daß der zweite Rest des ersten ist.

In der That läßt sich leicht darthun, daß zur Existenz der Gleichung

$$au^2 - \delta v^2 = 1$$

die Bedingung δ biquadratischer Rest zu a nothwendig ist. Beim Beweise sind zwei Fälle zu unterscheiden, je nachdem nemlich a von der Form $8n + 5$ oder $8n + 1$ ist.

Erster Fall. $a = 8n + 5$.

Aus $\delta v^2 \equiv -1$, (mod. a) ergiebt sich, daß δv^2 biquadratischer Nichtrest zu a sein muß, da alle Primzahlen von der Form $8n + 5$ den biquadratischen Nichtrest -1 haben. Da ferner, wie leicht ersichtlich, in der oben aufgestellten Gleichung u nur eine ungerade, v eine gerade Zahl sein kann, so hat u^2 die Form $8n + 1$, au^2 die Form $8n + 5$ ebenso wie a. Damit man die Differenz $+1$ erhalte, muß δv^2

von der Form $8n + 4$ sein, woraus man schließt, daß v den Faktor 2 einmal und nur einmal enthält. Bezeichnet man jetzt die ungeraden Primfaktoren dieser Größe mit k, k', k'', ..., so ist

$$v = 2kk'k'' \ldots\ldots$$

Es ist aber $\alpha u^2 \equiv 1$, (mod. k, k', k'', ...); man findet demnach, wenn man zur Abkürzung das Legendre'sche Zeichen $\left(\frac{p}{q}\right)$ anwendet, die Relationen

$$\left(\frac{\alpha}{k}\right) = 1, \quad \left(\frac{\alpha}{k'}\right) = 1, \quad \left(\frac{\alpha}{k''}\right) = 1, \ldots.$$

woraus sich mittelst des quadratischen Reziprozitätsgesetzes, da α von der Form $4n + 1$ ist,

$$\left(\frac{k}{\alpha}\right) = 1, \quad \left(\frac{k'}{\alpha}\right) = 1, \quad \left(\frac{k''}{\alpha}\right) = 1, \ldots.$$

ergiebt. Nimmt man, wegen $\alpha = 8n + 5$, hierzu die Relation

$$\left(\frac{2}{\alpha}\right) = -1$$

und multiplizirt, so erhält man

$$\left(\frac{2kk'k'' \ldots.}{\alpha}\right) = \left(\frac{v}{\alpha}\right) = -1.$$

Demnach ist v quadratischer, v^2 biquadratischer Nichtrest von α. Wäre jetzt δ ebenfalls biquadratischer Nichtrest zu α, so würde, wenn g eine primitive Wurzel von α bedeutet und $\delta \equiv g^\lambda$, (mod. α) gesetzt wird, der Index λ die Form $4n + 2$ haben, weil nemlich λ mit 2 theilbar sein muß, da nach Voraussetzung δ quadratischer Rest zu α ist. Ferner ist in $v^2 \equiv g^{\lambda'}$, (mod. α) der Index λ' ebenfalls von der Form $4n + 2$, so daß in $\delta v^2 \equiv g^{\lambda+\lambda'}$, (mod. α) der Index $\lambda + \lambda'$ mit 4 aufgehen und δv^2 biquadratischer Rest zu α sein müßte. Da man aber schon gefunden hat, daß δv^2 biquadratischer Nichtrest sein muß, so ist die für δ gemachte Annahme unmöglich, d. h. δ ist biquadratischer Rest zu α.

Zweiter Fall. $\alpha = 8n + 1$.

Hier findet man aus $\delta v^2 \equiv -1$, (mod. α), daß δv^2 biquadratischer Rest von α sein wird, weil dasselbe von -1 gilt. Ferner ist jetzt

$$v = 2^\mu \cdot kk'k'' \ldots.$$

zu setzen, wobei es, da 2 quadratischer Rest zu α ist, auf die Größe des Exponenten μ nicht ankommt. Wie oben ergiebt sich aus $\alpha u^2 \equiv 1$, (mod. v)

$$\left(\frac{\alpha}{k}\right) = 1, \left(\frac{\alpha}{k'}\right) = 1, \left(\frac{\alpha}{k''}\right) = 1, \ldots.$$

und durch Umkehrung

$$\left(\frac{k}{\alpha}\right) = 1, \left(\frac{k'}{\alpha}\right) = 1, \left(\frac{k''}{\alpha}\right) = 1, \ldots.$$

Multiplizirt man diese Relationen unter einander und mit

$$\left(\frac{2^{\mu}}{\alpha}\right) = 1,$$

so findet man

$$\left(\frac{2^{\mu} \cdot kk'k'' \ldots.}{\alpha}\right) = \left(\frac{v}{\alpha}\right) = 1.$$

Demnach ist jetzt v quadratischer, v^2 biquadratischer Rest zu α, und da schon bewiesen war, daß dasselbe von δv^2 gilt, so wird auch δ biquadratischer Rest zu α sein müssen. Man kann also folgenden Satz aufstellen:

(6.) „Wenn die Gleichung $\alpha u^2 - \delta v^2 = +1$ möglich sein soll, so muß wenigstens die eine der beiden Primzahlen biquadratischer Rest der andern sein."

Hieraus folgt ferner:

(7.) „Wenn beide Primzahlen α und δ biquadratische Nichtreste zu einander sind, so ist nur die Gleichung $y^2 = \alpha\delta x^2 - 1$ möglich."

§. 3.

Weit weniger einfach sind die Resultate, welche man aus der Gleichung (3.) in Bezug auf α ableiten kann. Es mag hierbei zunächst folgendes bemerkt werden. In einer Abhandlung von Dirichlet über die biquadratischen Reste (Crelle's Journal, Bd. III, S. 62 u. f. w.) ist gezeigt worden, welche Bedingungen dazu nöthig sind, daß eine Primzahl α von der Form $4n + 1$ zu der Primzahl δ von derselben Form biquadratischer Rest sei oder nicht sei. Von der Gleichung $t^2 + \alpha u^2 = \delta v^2$ ausgehend gelangt er, ohne den erst später von Gauss zu der Bestimmung der biquadratischen Reziprozitätsgesetze in diesen Theil der Zahlenlehre aufgenommenen Begriff der komplexen Primzahlen zu Hülfe zu nehmen, zu folgenden allgemeinen Resultaten.

Da $\left(\frac{\delta}{\alpha}\right) = 1$, $\left(\frac{\alpha}{\delta}\right) = 1$ vorausgesetzt werden muß, so ist $\delta \equiv \chi'^2$, (mod. α). Setzt man nun $\delta = \varphi'^2 + \psi'^2$, wo φ' eine ungerade, ψ' eine gerade Zahl bedeutet,

so ist $\left(\frac{\chi' \cdot \chi' + \psi'}{\alpha}\right) = +1$ oder $= -1$, und im ersten Falle α biquadratischer Rest, im zweiten Nichtrest zu δ. Nimmt man außerdem $\alpha = \varphi^2 + \psi^2$ und $\alpha \equiv \chi^2$, (mod. δ), so ist δ biquadratischer Rest oder Nichtrest zu α, je nachdem $\left(\frac{\chi \cdot \chi + \psi}{\delta}\right)$ $= +1$ oder $= -1$ ist. Man kann nun erstens annehmen, daß α biquadratischer Nichtrest zu δ und ebenso δ Nichtrest zu α ist. Dann hat man

$$\left(\frac{\chi'}{\alpha}\right) = -1, \left(\frac{\chi}{\delta}\right) = -1,$$

weil, wenn z. B. $\left(\frac{\chi'}{\alpha}\right) = 1$ wäre, man $\chi' \equiv r^2$, also $\chi'^2 \equiv r^4$, $\delta \equiv r^4$, (mod. α), hätte, was der Voraussetzung widerspricht. Hieraus folgt in Verbindung mit den so eben aufgestellten Relationen, daß

$$\left(\frac{\chi' + \psi'}{\alpha}\right) = +1, \left(\frac{\chi + \psi}{\delta}\right) = +1$$

sein muß.

Zweitens sei α biquadratischer Nichtrest zu δ, δ Rest zu α. Dann ist

$$\left(\frac{\chi'}{\alpha}\right) = +1, \left(\frac{\chi}{\delta}\right) = -1,$$

ferner

$$\left(\frac{\chi' \cdot \chi' + \psi'}{\alpha}\right) = -1, \left(\frac{\chi \cdot \chi + \psi}{\delta}\right) = 1,$$

also

$$\left(\frac{\chi' + \psi'}{\alpha}\right) = -1, \left(\frac{\chi + \psi}{\delta}\right) = -1.$$

Drittens sei α biquadratischer Rest zu δ und ebenso δ zu α. Dann ist

$$\left(\frac{\chi'}{\alpha}\right) = +1, \left(\frac{\chi}{\delta}\right) = +1,$$

und da hier

$$\left(\frac{\chi' \cdot \chi' + \psi'}{\alpha}\right) = 1, \left(\frac{\chi \cdot \chi + \psi}{\delta}\right) = 1$$

ist, so findet man

$$\left(\frac{\chi' + \psi'}{\alpha}\right) = +1, \left(\frac{\chi + \psi}{\delta}\right) = +1.$$

Eine Erweiterung dieser Resultate ergiebt sich aus der Betrachtung, daß

$$\chi'^2 \equiv \varphi'^2 + \psi'^2, \text{ (mod. } \alpha), \text{ oder}$$

$$(\chi' + \psi')(\chi' - \psi') \equiv \varphi'^2, \text{ (mod. } \alpha),$$

woraus folgt, daß $\chi' + \psi'$ und $\chi' - \psi'$ gleichzeitig quadratische Reste oder Nichtreste zu α sind. Dasselbe gilt für $\chi \pm \psi$ in Bezug auf δ. Das Gesetz, das man hieraus ableiten kann, ist ziemlich leicht zu übersehen. Der Fall, daß α in φ' (oder δ in φ) aufgeht, wobei $\chi' + \psi'$ oder $\chi' - \psi'$ ebenfalls mit α aufgehen würde, kann ohne Schwierigkeit für sich behandelt werden.

Es könnte nun scheinen, als ob im vorliegenden Falle, wo eine der Gleichung $t^2 + \alpha u^2 = \delta v^2$ ähnliche aber einfachere existirt, nemlich $\alpha u^2 - \delta v^2 = 1$, aus dieser letzteren auch einfachere Beziehungen als die eben angegebenen abgeleitet werden könnten. Dies ist auch in der That für δ bereits durchgeführt worden; ganz anders steht es mit der andern Primzahl α. Indem man nemlich

$$-1 + \alpha u^2 = \delta v^2 \text{ oder } i^2 + \alpha u^2 = \delta v^2$$

setzt, eine Gleichung, in der $i = \sqrt{-1}$ statt der allgemeinen Größe t auftritt, ist jede Art von Beweisführung, die der in der citirten Abhandlung auf der Zerlegung von t in seine Primfaktoren beruhenden analog wäre, unmöglich gemacht. Mittelst der Gleichung (3.) läßt sich nur noch zweierlei darthun.

Hat u die Form $4n + 1$ und enthält demnach unter seinen Primfaktoren solche von der Form $4n + 3$ stets paarweise oder als Quadrate, so ist in

$$\delta v^2 \equiv -1, \text{ (mod. } u)$$

δ entweder zu keinem Faktor von u oder zu je zweien quadratischer Nichtrest. Daraus folgt durch Umkehrung, daß man unter den Primfaktoren von u Nichtreste zu δ entweder gar nicht, oder immer paarweise antrifft, u demnach quadratischer, u^2 biquadratischer Rest zu δ sein wird. Andrerseits hat man

$$\alpha u^2 \equiv 1, \text{ (mod. } \delta),$$

d. h. αu^2 biquadratischer Rest zu δ, woraus man ableitet:

„Wenn u die Form $4n + 1$ hat, so ist α biquadratischer Rest zu δ."

Auf ganz ähnliche Weise ergiebt sich für $u = 4n + 3$, indem in dieser Größe Primfaktoren von derselben Form immer in ungerader Anzahl vorhanden sind, daß δv^2 wie auch δ zu einer ungeraden Anzahl von Primfaktoren von u Nichtrest ist. Durch Umkehrung findet man leicht, daß u quadratischer Nichtrest, u^2 also biquadratischer Nichtrest zu δ ist; und da αu^2 auch jetzt biquadratischer Rest zu δ sein muß, so hat man:

„Wenn u die Form $4n + 3$ hat, so ist α biquadratischer Nichtrest zu δ."

Einfachere Resultate lassen sich aber weder hieraus noch aus den übrigen Angaben dieses Paragraphen in einfacherer Weise ableiten.

§. 4.

Schon im ersten Paragraphen ist angegeben worden, daß zur Gleichung $y^2 = px^2 - 1$ nothwendig zwei andere $y^2 = px^2 \pm a$ gehören, wobei, vorausgesetzt daß p ungerade ist, die ungerade Zahl a so beschaffen sein muß, daß $p = a^2 + b^2$ gefunden wird. Man sieht leicht, daß $\pm a$ quadratischer Rest zu den in p enthaltenen Primzahlen ist. Setzt man im vorliegenden Falle

$$\alpha = a^2 + b^2, \; \delta = a'^2 + b'^2,$$

wo a und a' die ungeraden Theile bezeichnen, so findet man, daß sich das Produkt $\alpha\delta$ auf zweierlei Art als die Summe von zwei Quadraten darstellen läßt, nemlich

$$\alpha\delta = (aa' + bb')^2 + (ab' - a'b)^2$$
$$\alpha\delta = (aa' - bb')^2 + (ab' + a'b)^2.$$

Zur Abkürzung soll

$$aa' + bb' = A, \; aa' - bb' = A'$$
$$ab' - a'b = B, \; ab' + a'b = B'$$

also

$$\alpha\delta = A^2 + B^2 = A'^2 + B'^2$$

gesetzt werden. Auch hier sind A und A' ungerade.

Zunächst sei nun $a = kk'k'' \ldots .$, wo die Größen k lauter ungerade Primzahlen bedeuten; dann ist, da $\alpha \equiv b^2$, (mod. a)

$$\left(\frac{\alpha}{k}\right) = 1, \left(\frac{\alpha}{k'}\right) = 1, \left(\frac{\alpha}{k''}\right) = 1, \ldots .$$

und durch Umkehrung

$$\left(\frac{k}{\alpha}\right) = 1, \left(\frac{k'}{\alpha}\right) = 1, \left(\frac{k''}{\alpha}\right) = 1, \ldots .$$

oder

$$\left(\frac{kk'k'' \ldots .}{\alpha}\right) = \left(\frac{a}{\alpha}\right) = 1,$$

d. h. a ist quadratischer Rest zu α, und ganz ebenso a' zu δ. Ferner folgt aus den Kongruenzen

$$\alpha\delta \equiv B^2, \text{ (mod. } A), \quad \alpha\delta \equiv B'^2, \text{ (mod. } A'),$$

wenn $A = l \cdot l' \cdot l'' \ldots ., \; A' = m \cdot m' \cdot m'' \ldots .$ gesetzt wird,

$$\left(\frac{\alpha\delta}{l}\right) = 1, \left(\frac{\alpha\delta}{l'}\right) = 1, \ldots\ldots$$

$$\left(\frac{\alpha\delta}{m}\right) = 1, \left(\frac{\alpha\delta}{m'}\right) = 1, \ldots\ldots$$

Diese Kongruenzen lassen sich, indem man ± 1 mit $\varepsilon_1, \varepsilon_2, \ldots\ldots, \eta_1, \eta_2, \ldots\ldots$ bezeichnet, in andere zerlegen, die so lauten

$$\left(\frac{\alpha}{l}\right) = \varepsilon_1, \left(\frac{\delta}{l}\right) = \varepsilon_1, \left(\frac{\alpha}{l'}\right) = \varepsilon_2, \left(\frac{\delta}{l'}\right) = \varepsilon_2, \ldots\ldots$$

$$\left(\frac{\alpha}{m}\right) = \eta_1, \left(\frac{\delta}{m}\right) = \eta_1, \left(\frac{\alpha}{m'}\right) = \eta_2, \left(\frac{\delta}{m'}\right) = \eta_2, \ldots\ldots$$

aus denen sich ergiebt

$$\left(\frac{l}{\alpha}\right) = \varepsilon_1, \left(\frac{l'}{\alpha}\right) = \varepsilon_2, \ldots\ldots$$

$$\left(\frac{l}{\delta}\right) = \varepsilon_1, \left(\frac{l'}{\delta}\right) = \varepsilon_2, \ldots\ldots$$

$$\left(\frac{m}{\alpha}\right) = \eta_1, \left(\frac{m'}{\alpha}\right) = \eta_2, \ldots\ldots$$

$$\left(\frac{m}{\delta}\right) = \eta_1, \left(\frac{m'}{\delta}\right) = \eta_2, \ldots\ldots,$$

oder durch Multiplikation

$$\left(\frac{ll' \ldots\ldots}{\alpha}\right) = \left(\frac{A}{\alpha}\right) = \varepsilon_1 \varepsilon_2 \ldots\ldots$$

$$\left(\frac{ll' \ldots\ldots}{\delta}\right) = \left(\frac{A}{\delta}\right) = \varepsilon_1 \varepsilon_2 \ldots\ldots$$

$$\left(\frac{mm' \ldots}{\alpha}\right) = \left(\frac{A'}{\alpha}\right) = \eta_1 \eta_2 \ldots\ldots$$

$$\left(\frac{mm' \ldots\ldots}{\delta}\right) = \left(\frac{A'}{\delta}\right) = \eta_1 \eta_2 \ldots\ldots$$

Man schließt hieraus, „daß A gleichzeitig quadratischer Rest oder Nichtrest zu α und δ sein muß. Ebenso ist auch A' Rest oder Nichtrest zu δ, je nachdem es Rest oder Nichtrest zu α ist."

Es soll jetzt der früher ausgeschlossene Fall, daß α und δ quadratische Nichtreste zu einander sind, der Uebereinstimmung in der Beweisführung wegen, mit hinzugenommen werden.

Erster Fall. $\left(\frac{\alpha}{\delta}\right) = -1, \left(\frac{\delta}{\alpha}\right) = -1.$

Aus der Differenz

$$a'^2\alpha - b^2\delta = a^2a'^2 - b^2b'^2 = A \cdot A'$$

ergeben sich, wenn die Kongruenz

$$-b^2 \equiv a^2, \text{ oder } -b^2\delta \equiv a^2\delta, \text{ (mod. } \alpha)$$

berücksichtigt wird, die Relationen

$$AA' \equiv a'^2\alpha, \text{ (mod. } \delta), \quad AA' \equiv a^2\delta, \text{ (mod. } \alpha),$$

aus denen hervorgeht, daß AA' quadratischer Nichtrest, d. h. ein Faktor, z. B. A Nichtrest, der andere A' Rest zu α und zu δ sein muß. Ist aber $\left(\frac{A}{\alpha}\right) = -1$ und demnach $\left(\frac{A'}{\alpha}\right) = +1$, so folgt nach dem Obigen, daß gleichzeitig $\left(\frac{A}{\delta}\right) = -1$, $\left(\frac{A'}{\delta}\right) = +1$ gefunden wird, und umgekehrt.

„Wenn α und δ quadratische Nichtreste zu einander sind, so muß eine der Größen A, A' Rest, die andere Nichtrest zu α und gleichzeitig zu δ sein."

In der That waren in diesem Falle die Gleichungen $y^2 = \alpha\delta x^2 - 1$, $y^2 = \alpha\delta x^2 \pm A$ oder $y^2 = \alpha\delta x^2 \pm A'$ möglich, wobei sich in Betreff der letzteren über das Vorkommen von A oder A' von vornherein entscheiden läßt.

Zweiter Fall. $\left(\frac{\alpha}{\delta}\right) = 1, \left(\frac{\delta}{\alpha}\right) = 1.$

Eine der eben gegebenen Schritt für Schritt analoge Beweisführung läßt zunächst aus den Kongruenzen

$$AA' \equiv a'^2\alpha, \text{ (mod. } \delta), \quad AA' \equiv a^2\delta, \text{ (mod. } \alpha)$$

ersehen, daß AA' quadratischer Rest zu α und zu δ sein muß, woraus man den Satz ableitet:

„Wenn α und δ quadratische Reste zu einander sind, so sind A und A' gleichzeitig entweder Reste oder Nichtreste zu α und zu δ." (8.)

§. 5.

Wir wenden jetzt die Ergebnisse der bisherigen Betrachtungen auf die oben angegebenen Primzahlen an, um durch Induktion nähere Beziehungen aufzufinden.

Die Gleichung $y^2 = \alpha\delta x^2 - 1$ war möglich für

(I.) $145 = 5 \cdot 29,\ 445 = 5 \cdot 89,\ 901 = 17 \cdot 53.$

Man hat hier, $(\alpha\delta = A^2 + B^2 = A'^2 + B'^2)$

$$145 = 9^2 + 8^2 = 1^2 + 12^2$$
$$445 = 21^2 + 2^2 = 11^2 + 18^2$$
$$901 = 15^2 + 26^2 = 1^2 + 30^2,$$

und übersieht leicht, daß die ungeraden Größen A und A' quadratische Reste zu α und zu δ sind. Für eine dieser Größen ist dies übrigens schon durch die Möglichkeit der Gleichungen $y^2 = \alpha\delta x^2 \pm A$, oder $\pm A'$ festgestellt.

Die Zahlen, für welche die Gleichung $\alpha u^2 - \delta v^2 = 1$ möglich sein muß, zerfallen, je nachdem A und A' beide Reste oder beide Nichtreste sind, (es kommt nemlich hier wegen $\left(\frac{\alpha}{\delta}\right) = 1, \left(\frac{\delta}{\alpha}\right) = 1$ der Satz (8.) zur Anwendung) in zwei Klassen; in der ersten findet man die Zahlen

(II.) $505 = 5 \cdot 101,\ 689 = 13 \cdot 53,\ 793 = 13 \cdot 61,\ 905 = 5 \cdot 181,$

und zwar ist

$$505 = 21^2 + 8^2 = 19^2 + 12^2$$
$$689 = 25^2 + 8^2 = 17^2 + 20^2$$
$$793 = 27^2 + 8^2 = 3^2 + 28^2$$
$$905 = 29^2 + 8^2 = 11^2 + 28^2;$$

wobei A und A' beide als Reste zu α und zu δ gefunden werden; in der andern Klasse sind folgende enthalten:

(III.) $\left\{ \begin{array}{l} 205 = 5 \cdot 41,\ 221 = 17 \cdot 13,\ 305 = 5 \cdot 61,\ 377 = 13 \cdot 29 \\ 545 = 109 \cdot 5,\ 745 = 149 \cdot 5. \end{array} \right\}$

und zwar ist

$$205 = 13^2 + 6^2 = 3^2 + 14^2$$
$$221 = 11^2 + 10^2 = 5^2 + 14^2$$
$$305 = 17^2 + 4^2 = 7^2 + 16^2$$
$$377 = 19^2 + 4^2 = 11^2 + 16^2$$
$$545 = 23^2 + 4^2 = 17^2 + 16^2$$
$$745 = 27^2 + 4^2 = 13^2 + 24^2,$$

wobei A und A' beide als quadratische Nichtreste zu α und zu δ gefunden werden.

Nimmt man hinzu, daß in (I.) nur solche Primzahlen α und δ vorkommen, welche biquadratische Nichtreste, in (II.) nur solche, welche biquadratische Reste zu einander sind, während von denen in (III.) die eine biquadratischer Nichtrest der

andern und umgekehrt die letztere Rest zur ersten ist, so wird man durch Induktion zu folgendem Gesetze geführt werden, welches sich auf alle die Primzahlen bezieht, die schon quadratische Reste zu einander sind:

„Wenn bei der Zerlegung des Produkts zweier Primzahlen von der Form $4n + 1$ in die Summe von zwei Quadraten (auf zweierlei Weise möglich) die ungeraden Größen in diesen Ausdrücken quadratische Reste der Primzahlen sind, so sind die letzteren gleichzeitig biquadratische Reste zu einander oder nicht. Sind aber die ungeraden Größen quadratische Nichtreste der Primzahlen, so ist wenn die eine biquadratischer Rest der andern ist, umgekehrt die letztere Nichtrest der ersteren,"

ein Gesetz, welches die fraglichen Beziehungen der nicht komplexen ungeraden Primzahlen auf die einfachste Art regelt und eigenthümlicher Weise von der Form der Primzahlen ($8n + 1$ oder $8n + 5$) ganz unabhängig ist. Man kann noch bemerken, daß die hierbei unberücksichtigt gebliebenen Primzahlen, die schon quadratische Nichtreste zu einander sind, durch eine geringe Aenderung in der Fassung mit einbegriffen werden könnten.

Es sollen nun diese Ergebnisse der Induktion unter der Voraussetzung, daß immer $\left(\frac{\alpha}{\delta}\right) = 1, \left(\frac{\delta}{\alpha}\right) = 1$

oder

$$\alpha^{\frac{1}{2}(\delta-1)} \equiv 1, \text{ (mod. } \delta), \quad \delta^{\frac{1}{2}(\alpha-1)} \equiv 1, \text{ (mod. } \alpha)$$

also

$$\alpha^{\frac{1}{4}(\delta-1)} \equiv \pm 1, \text{ (mod. } \delta), \quad \delta^{\frac{1}{4}(\alpha-1)} \equiv \pm 1, \text{ (mod. } \alpha)$$

und

$$\alpha\delta = A^2 + B^2 = A'^2 + B'^2$$

ist, in folgender Ordnung bewiesen werden.

Erstens. A und A' sind quadratische Nichtreste zu α und zu δ, d. h.

$$\left.\begin{aligned}(aa' \pm bb')^{\frac{1}{2}(\alpha-1)} &\equiv -1, \text{ (mod. } \alpha)\\ (aa' \pm bb')^{\frac{1}{2}(\delta-1)} &\equiv -1, \text{ (mod. } \delta)\end{aligned}\right\} \qquad (9.)$$

woraus folgen soll, daß die eine der beiden Primzahlen, z. B. δ biquadratischer Rest zu α und α Nichtrest zu δ ist, oder umgekehrt, d. h.

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \pm 1, \text{ (mod. } \alpha)$$
$$\alpha^{\frac{1}{4}(\delta-1)} \equiv \mp 1, \text{ (mod. } \delta).$$

Zerlegt man $\alpha = a^2 + b^2$ in seine beiden komplexen Primfaktoren $(a + bi)$ und

$(a - bi)$, welche als primär angenommen werden können, indem man je nach der Form der ungeraden Zahl a das Vorzeichen, was immer möglich ist, so bestimmt, daß $a + bi \equiv 1$, (mod. $2 + 2i$) und $a - bi \equiv 1$, (mod. $2 - 2i$) ist, und setzt demnach

$$\alpha = (a + bi)\ (a - bi)$$

und ebenso

$$\delta = (a' + b'i)\ (a' - b'i);$$

so hat man

$$-bi \equiv a \text{ oder } b \equiv ai, \text{ (mod. } a + bi)$$
$$-bi \equiv -a \text{ oder } b \equiv -ai, \text{ (mod. } a - bi),$$

und ebenso

$$b' \equiv a'i, \text{ (mod. } a' + b'i), \quad b' \equiv -a'i, \text{ (mod. } a' - b'i).$$

Aus der ersten Kongruenz (9.) folgt dann

(10.) $$(aa' \pm ab'i)^{\frac{1}{2}(\alpha - 1)} \equiv -1, \text{ (mod. } a \pm bi).$$

Da aber bekanntlich a quadratischer Rest zu α ist, so hat man

$$a^{\frac{1}{2}(\alpha - 1)} \equiv 1, \text{ (mod. } \alpha),$$

woraus sich sofort ergiebt

$$a^{\frac{1}{2}(\alpha - 1)} \equiv 1, \text{ (mod. } a \pm bi).$$

Man sieht jetzt leicht, daß die Kongruenz (10.) durch folgende ersetzt werden kann:

$$(a' + b'i)^{\frac{1}{2}(\alpha - 1)} \equiv -1, \text{ (mod. } a + bi),$$

wo bloß die oberen Vorzeichen angegeben sind, weil sich die übrigen Fälle ohne Schwierigkeit daraus ableiten lassen. Da $\frac{1}{2}(\alpha - 1)$ eine gerade Zahl ist, so führt die Zerlegung der zuletzt angegebenen Relation auf bekannte Weise zu einer Kongruenz, die den biquadratischen Charakter der komplexen Zahl $a' + b'i$ bestimmt, nemlich zu

$$(a' + b'i)^{\frac{1}{4}(\alpha - 1)} \equiv \pm i, \text{ (mod. } a + bi);$$

bezeichnet man also die Größe ± 1 mit ε_1, ε_2 so findet man die vier Kongruenzen:

(11.)
$$\begin{cases} (a' + b'i)^{\frac{1}{4}(\alpha - 1)} \equiv \varepsilon_1 i, \text{ (mod. } a + bi) \\ (a' + b'i)^{\frac{1}{4}(\alpha - 1)} \equiv \varepsilon_2 i, \text{ (mod. } a - bi) \\ (a' - b'i)^{\frac{1}{4}(\alpha - 1)} \equiv -\varepsilon_1 i, \text{ (mod. } a - bi) \\ (a' - b'i)^{\frac{1}{4}(\alpha - 1)} \equiv -\varepsilon_2 i, \text{ (mod. } a + bi). \end{cases}$$

Es mag hierzu sogleich bemerkt werden, daß über die Vorzeichen ε_1 und ε_2 in der ersten und zweiten Kongruenz, ob sie gleich oder entgegengesetzt sind, nichts ausgemacht zu werden braucht; die Umkehrungen in der dritten und vierten sind nur eine einfache Folge der für Division mit komplexen Moduln geltenden Gesetze.

Um das biquadratische Reziprozitätsgesetz für komplexe Primzahlen, deren Norm eine Primzahl von der Form $4n + 1$ ist, hierauf anzuwenden, sind zwei Fälle zu unterscheiden.

Erster Fall. $\alpha = N(a + bi)$ und $\delta = N(a' + b'i)$ sind beide von der Form $8n + 5$.

Dann sind bekanntlich die Vorzeichen von $(a' + b'i)^{\frac{1}{4}(\alpha - 1)}$, (mod. $a + bi$) und $(a + bi)^{\frac{1}{4}(\delta - 1)}$, (mod. $a' + b'i$) entgegengesetzt, so daß man aus (11.) der Reihe nach erhält

$$\left.\begin{aligned} (a + bi)^{\frac{1}{4}(\delta - 1)} &\equiv -\varepsilon_1 i, \pmod{a' + b'i} \\ (a - bi)^{\frac{1}{4}(\delta - 1)} &\equiv -\varepsilon_2 i, \pmod{a' + b'i} \\ (a - bi)^{\frac{1}{4}(\delta - 1)} &\equiv \varepsilon_1 i, \pmod{a' - b'i} \\ (a + bi)^{\frac{1}{4}(\delta - 1)} &\equiv \varepsilon_2 i, \pmod{a' - b'i}. \end{aligned}\right\} \qquad (12.)$$

Durch Multiplikation der ersten und vierten Kongruenz in (11.) findet man aber

$$(a'^2 + b'^2)^{\frac{1}{4}(\alpha - 1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{a + bi}$$

oder

$$\delta^{\frac{1}{4}(\alpha - 1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{a + bi},$$

und ebenso aus der zweiten und dritten

$$\delta^{\frac{1}{4}(\alpha - 1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{a - bi},$$

woraus man schließt, daß $\delta^{\frac{1}{4}(\alpha - 1)} - \varepsilon_1 \varepsilon_2$ mit $(a + bi)$ und $(a - bi)$, also mit α theilbar sein muß. Dies führt zu der Kongruenz

$$\delta^{\frac{1}{4}(\alpha - 1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{\alpha}.$$

Andrerseits ergiebt sich aus der ersten und zweiten Kongruenz in (12.)

$$\alpha^{\frac{1}{4}(\delta - 1)} \equiv -\varepsilon_1 \varepsilon_2, \pmod{a' + b'i},$$

aus der dritten und vierten

$$\alpha^{\frac{1}{4}(\delta - 1)} \equiv -\varepsilon_1 \varepsilon_2, \pmod{a' - b'i}$$

und aus diesen letzteren selbst, da ihnen zufolge $\alpha^{\frac{1}{4}(\delta - 1)} + \varepsilon_1 \varepsilon_2$ mit $(a' + b'i)$ und $(a' - b'i)$ oder mit δ theilbar sein muß,

$$\alpha^{\frac{1}{4}(\delta - 1)} \equiv -\varepsilon_1 \varepsilon_2, \pmod{\delta}.$$

Wenn also A und A' quadratische Nichtreste zu α und δ sind, so hat man gleichzeitig

$$\delta^{\frac{1}{4}(\alpha - 1)} \equiv \pm 1, \pmod{\alpha} \text{ und } \alpha^{\frac{1}{4}(\delta - 1)} \equiv \mp 1, \pmod{\delta}.$$

Zweiter Fall. Die Normen α und δ sind nicht beide von der Form $8n + 5$.

Dann hat man

$$(a' + b'i)^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_1 i, \pmod{a + bi}$$
$$(a' + b'i)^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_2 i, \pmod{a - bi}$$
$$(a' - b'i)^{\frac{1}{4}(\alpha-1)} \equiv -\varepsilon_1 i, \pmod{a - bi}$$
$$(a' - b'i)^{\frac{1}{4}(\alpha-1)} \equiv -\varepsilon_2 i, \pmod{a + bi},$$

und wegen des biquadratischen Reziprozitätsgesetzes, nach welchem in diesem Falle $(a' + b'i)^{\frac{1}{4}(\alpha-1)}$, (mod. $a + bi$) und $(a + bi)^{\frac{1}{4}(\delta-1)}$, (mod. $a' + b'i$) dasselbe Vorzeichen haben,

$$(a + bi)^{\frac{1}{4}(\delta-1)} \equiv \varepsilon_1 i, \pmod{a' + b'i}$$
$$(a - bi)^{\frac{1}{4}(\delta-1)} \equiv \varepsilon_2 i, \pmod{a' + b'i}$$
$$(a - bi)^{\frac{1}{4}(\delta-1)} \equiv -\varepsilon_1 i, \pmod{a' - b'i}$$
$$(a + bi)^{\frac{1}{4}(\delta-1)} \equiv -\varepsilon_2 i, \pmod{a' - b'i}.$$

Wie oben ist

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{a + bi}$$
$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{a - bi}$$
$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_1 \varepsilon_2, \pmod{\alpha}$$

und

$$\alpha^{\frac{1}{4}(\delta-1)} \equiv -\varepsilon_1 \varepsilon_2, \pmod{a' + b'i}$$
$$\alpha^{\frac{1}{4}(\delta-1)} \equiv -\varepsilon_1 \varepsilon_2, \pmod{a' - b'i}$$
$$\alpha^{\frac{1}{4}(\delta-1)} \equiv -\varepsilon_1 \varepsilon_2, \pmod{\delta}.$$

so daß man auch hier findet

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \pm 1, \pmod{\alpha}$$
$$\alpha^{\frac{1}{4}(\delta-1)} \equiv \mp 1, \pmod{\delta}.$$

Das oben schon angegebene Gesetz gilt demnach für alle Normen α und δ.

Zweitens. A und A' sind quadratische Reste zu α und zu δ, d. h.

$$(aa' \pm bb')^{\frac{1}{2}(\alpha-1)} \equiv 1, \pmod{\alpha}$$
$$(aa' \pm bb')^{\frac{1}{2}(\delta-1)} \equiv 1, \pmod{\delta},$$

woraus folgen soll, daß wenn α biquadratischer Rest zu δ ist auch δ Rest zu α werden muß.

Ebenso, wie im vorigen Beweise findet man

$$(a' \pm b'i)^{\frac{1}{2}(\alpha-1)} \equiv 1, \pmod{a \pm bi}$$
$$(a \pm bi)^{\frac{1}{2}(\delta-1)} \equiv 1, \pmod{a' \pm b'i},$$

und hieraus, wenn wiederum ± 1 mit ε_1, ε_2 bezeichnet wird

$$\left.\begin{aligned}(a'+bi')^{\frac{1}{4}(\alpha-1)} &\equiv \varepsilon_1, \pmod{a+bi}\\ (a'+b'i)^{\frac{1}{4}(\alpha-1)} &\equiv \varepsilon_2, \pmod{a-bi}\\ (a'-b'i)^{\frac{1}{4}(\alpha-1)} &\equiv \varepsilon_1, \pmod{a-bi}\\ (a'-b'i)^{\frac{1}{4}(\alpha-1)} &\equiv \varepsilon_2, \pmod{a+bi}\end{aligned}\right\} \quad (13.)$$

Die rechten Seiten in der ersten und dritten, zweiten und vierten Kongruenz stimmen hier ganz überein, weil, wenn $(a'+b'i)^{\frac{1}{4}(\alpha-1)} - \varepsilon_1$ mit $(a+bi)$ theilbar ist, auch $(a'-b'i)^{\frac{1}{4}(\alpha-1)} - \varepsilon_1$ mit $(a-bi)$ theilbar sein muß.

Sind jetzt beide Normen α und δ von der Form $8n+5$, so erhält man durch das biquadratische Reziprozitätsgesetz

$$\left.\begin{aligned}(a+bi)^{\frac{1}{4}(\delta-1)} &\equiv -\varepsilon_1, \pmod{a'+b'i}\\ (a-bi)^{\frac{1}{4}(\delta-1)} &\equiv -\varepsilon_2, \pmod{a'+b'i}\\ (a-bi)^{\frac{1}{4}(\delta-1)} &\equiv -\varepsilon_1, \pmod{a'-b'i}\\ (a+bi)^{\frac{1}{4}(\delta-1)} &\equiv -\varepsilon_2, \pmod{a'-b'i};\end{aligned}\right\} \quad (14.)$$

sind sie nicht beide von dieser Form, so findet man

$$\left.\begin{aligned}(a+bi)^{\frac{1}{4}(\delta-1)} &\equiv \varepsilon_1, \pmod{a'+b'i}\\ (a-bi)^{\frac{1}{4}(\delta-1)} &\equiv \varepsilon_2, \pmod{a'+b'i}\\ (a-bi)^{\frac{1}{4}(\delta-1)} &\equiv \varepsilon_1, \pmod{a'-b'i}\\ (a+bi)^{\frac{1}{4}(\delta-1)} &\equiv \varepsilon_2, \pmod{a'-b'i}.\end{aligned}\right\} \quad (15.)$$

Aus den Kongruenzen (13.) folgt, in derselben Reihenfolge wie im ersten Falle:

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_1\,\varepsilon_2, \pmod{a+bi} \text{ und } \pmod{a-bi},$$

also

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv \varepsilon_1\,\varepsilon_2, \pmod{\alpha},$$

während man aus (14.) und (15.) übereinstimmend erhält

$$\alpha^{\frac{1}{4}(\delta-1)} \equiv \varepsilon_1\,\varepsilon_2, \pmod{\delta},$$

so daß, wenn α biquadratischer Rest zu δ, d. h.

$$\alpha^{\frac{1}{4}(\delta-1)} \equiv 1, \pmod{\delta},$$

also $\varepsilon_1\,\varepsilon_2 = 1$ ist, auch

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv 1, \pmod{\alpha}]$$

oder δ biquadratischer Rest zu α sein muß.

Drittens. A und A' sind ebenfalls quadratische Reste zu α und zu δ; es soll bewiesen werden, daß wenn α biquadratischer Nichtrest zu δ ist, auch δ Nichtrest zu α sein muß.

Der Beweis stimmt mit dem eben geführten ganz genau überein, nur hat man zuletzt

$$\alpha^{\frac{1}{4}(\delta-1)} \equiv -1, \text{ (mod. } \delta),$$

also $\varepsilon_1 \varepsilon_2 = -1$ zu setzen, woraus folgt, daß

$$\delta^{\frac{1}{4}(\alpha-1)} \equiv -1, \text{ (mod. } \alpha),$$

oder δ biquadratischer Nichtrest zu α ist.

Eine Abkürzung in der Fassung des so eben bewiesenen Gesetzes gewinnt man noch durch die Betrachtung, daß, wenn α und δ quadratische Reste zu einander sind, die Größen A und A' gleichzeitig quadratische Reste oder Nichtreste zu beiden Primzahlen sind, wie bereits bewiesen worden ist. Man braucht demnach $\alpha\delta$ nur einmal in die Summe zweier Quadrate zu zerlegen und zu untersuchen, ob die dabei erhaltene ungerade Zahl quadratischer Rest oder Nichtrest zu α (oder wenn man will zu δ) ist.

Was nun den Gang des Beweises überhaupt betrifft, so ist zu bemerken, daß das biquadratische Reziprozitätsgesetz zwischen komplexen Primzahlen dabei vorausgesetzt wird. Schon die größere Einfachheit des letzteren Gesetzes in Vergleich zu dem hier zwischen nicht komplexen Primzahlen aufgestellten rechtfertigt den eingeschlagenen Weg. Auch ist klar, daß durch die Nachweisung der biquadratischen Beziehungen zwischen den ungeraden Primzahlen α und δ, wenn man sie auf einem andern Wege festgestellt hätte, für die zwischen den komplexen Primzahlen bestehenden nichts Erhebliches gewonnen wäre, indem dann die Vorzeichen in

$$(a+bi)^{\frac{1}{4}(\delta-1)}, \text{ (mod. } a'+b'i) \text{ und } (a'+b'i)^{\frac{1}{4}(\alpha-1)}, \text{ (mod. } a+bi)$$

immer noch unbestimmt bleiben.

Im dritten Paragraphen sind andere Grundbedingungen der biquadratischen Beziehungen zwischen den beiden Primzahlen α und δ angegeben worden, die mit den eben bewiesenen im gewissen Sinne Aehnlichkeit haben. Wenn man mit geringen Aenderungen in den Bezeichnungen

$$\alpha \equiv c^2, \text{ (mod. } \delta)$$
$$\delta \equiv c'^2, \text{ (mod. } \alpha),$$

und $\alpha = a^2 + b^2$, $\delta = a'^2 + b'^2$ setzt, so ist

1. $\alpha^{\frac{1}{4}(\delta-1)} \equiv -1$, (mod. δ) und $\delta^{\frac{1}{4}(\alpha-1)} \equiv -1$, (mod. α),

wenn

$(c' \pm b')^{\frac{1}{2}(\alpha-1)} \equiv 1$, (mod. α) und $(c \pm b)^{\frac{1}{2}(\delta-1)} \equiv 1$, (mod. δ);

2. $\alpha^{\frac{1}{4}(\delta-1)} \equiv -1$, (mod. δ) und $\delta^{\frac{1}{4}(\alpha-1)} \equiv 1$, (mod. α),

wenn

$(c' \pm b')^{\frac{1}{2}(\alpha-1)} \equiv -1$, (mod. α) und $(c \pm b)^{\frac{1}{2}(\delta-1)} \equiv -1$, (mod. δ);

3. $\alpha^{\frac{1}{4}(\delta-1)} \equiv 1$, (mod. δ) und $\delta^{\frac{1}{4}(\alpha-1)} \equiv 1$, (mod. α),

wenn

$(c' \pm b')^{\frac{1}{2}(\alpha-1)} \equiv 1$, (mod. α) und $(c \pm b)^{\frac{1}{2}(\delta-1)} \equiv 1$, (mod. δ).

Man sieht, daß beide Zahlen α und δ zu einander biquadratische Reste oder Nichtreste sind, wenn von zwei bestimmten Größen $(c' \pm b')$ und $(c \pm b)$ die eine quadratischer Rest zu α, die andere zu δ ist; ferner daß die eine biquadratischer Rest zur andern, die zweite aber Nichtrest der ersten ist, wenn von den Größen $(c' + b')$ und $(c \pm b)$ die eine quadratischer Nichtrest zu α und die andere gleichzeitig Nichtrest zu δ ist. Es folgt daraus, daß

$$c' \pm b' \text{ und } aa' \pm bb' \quad (= A \text{ oder } A')$$

gleichzeitig quadratische Reste oder Nichtreste zu α sein werden, wie auch, daß

$$c \pm b \text{ und } aa' \pm bb'$$

gleichzeitig quadratische Reste oder Nichtreste zu δ sind. Könnte man umgekehrt diese Relationen beweisen, ohne von dem Principe der komplexen Zahlen Gebrauch zu machen, so würde das Reziprozitätsgesetz zwischen α und δ damit dargethan sein.

Ganz kurz soll noch angegeben werden, was sich aus dem Vorliegenden über das Stattfinden der Gleichungen

$$y^2 = a\delta x^2 - 1$$

und

$$au^2 - \delta v^2 = 1,$$

die einander, wie oben gezeigt worden, ausschließen, feststellen läßt.

Wenn die letztere Gleichung möglich ist und u die Form $4n + 1$ hat, so ist bewiesen worden, daß dann α und δ zu einander biquadratische Reste sind. Das Umgekehrte darf aber hiermit noch nicht als dargethan angenommen werden, indem für gewisse Zahlen α und δ etwa die Gleichung $y^2 = a\delta x^2 - 1$, für gewisse andere

$\alpha u^2 - \delta v^2 = 1$ möglich sein könnte. Demnach beschränkt sich das streng Bewiesene darauf, daß, wenn α biquadratischer Nichtrest zu δ und δ Rest zu α ist, wobei gleichzeitig A und A' quadratische Nichtreste zu α und zu δ sind, die Gleichung $\alpha u^2 - \delta v^2 = 1$ möglich sein muß. Denn $y^2 = \alpha\delta x^2 - 1$ kann nur dann bestehen, wenn es möglich ist den Gleichungen $y^2 = \alpha\delta x^2 \pm A$ (oder $\pm A'$) zu genügen, d. h. wenn wenigstens eine der Größen A und A' quadratischer Rest zu α und zu δ ist. Die Größe u muß in diesem Falle die Form $4n + 3$ haben. Die Gleichung $y^2 = \alpha\delta x^2 - 1$ dagegen ist stets möglich, wenn α und δ zu einander biquadratische Nichtreste sind.

§. 6.

Schließlich lassen sich den vorstehenden ganz ähnliche Betrachtungen auf die Gleichungen anwenden, mit deren Hülfe Legendre das quadratische Reziprozitätsgesetz zu beweisen suchte, wobei sich ergeben wird, weshalb dieselben den Beweis des Gesetzes nicht unmittelbar enthalten können.

Die zu Grunde gelegte Gleichung ist die immer mögliche

$$y^2 = \alpha\beta\gamma x^2 + 1, \tag{16.}$$

worin α eine Primzahl von der Form $4n + 1$, β und γ Primzahlen von der Form $4n + 3$ bedeuten. Da $\alpha\beta\gamma$ demnach die Form $4n + 1$ hat, so kann y nur eine ungerade, x eine gerade Zahl sein, woraus sich wie auf S. 4

$$\frac{y+1}{2} \cdot \frac{y-1}{2} = \alpha\beta\gamma \cdot \left(\frac{x}{2}\right)^2$$

ergiebt. Leicht leitet man die folgenden Zerlegungen ab

$$\frac{y \pm 1}{2} = \alpha u^2, \quad \frac{y \mp 1}{2} = \beta\gamma v^2, \quad \alpha u^2 - \beta\gamma v^2 = \pm 1,$$

$$\frac{y \pm 1}{2} = \alpha\beta u^2, \quad \frac{y \mp 1}{2} = \gamma v^2, \quad \alpha\beta u^2 - \gamma u^2 = \pm 1,$$

$$\frac{y \pm 1}{2} = \alpha\gamma u^2, \quad \frac{y \mp 1}{2} = \beta v^2, \quad \alpha\gamma u^2 - \beta v^2 = \pm 1;$$

wenn man wie oben die Gleichung (16.) als die kleinste ihrer Art bestimmt und berücksichtigt, daß $y^2 = \alpha\beta\gamma x^2 - 1$ nicht möglich ist.

Es scheint hieraus hervorzugehen, daß die zuerst angegeben Gleichung stattfinden müßte, wenn α entweder quadratischer Rest oder quadratischer Nichtrest zu β und zu γ ist, und demzufolge die übrigen immer dann und nur dann erhalten würden, wenn α nicht gleichzeitig quadratischer Rest oder Nichtrest zu β und zu γ ist; Bedingungen, die anders ausgedrückt aussagen würden, daß die Gleichung $\alpha u^2 - \beta\gamma v^2 = \pm 1$

jedesmal dem Falle entspräche, daß β und γ gleichzeitig quadratische Reste oder Nichtreste zu α sind.

Es mag nur der Fall hervorgehoben werden, daß man

$$\left(\frac{\alpha}{\beta}\right) = 1, \left(\frac{\alpha}{\gamma}\right) = 1$$

und demnach

$$\left(\frac{\beta}{\alpha}\right) = 1, \left(\frac{\gamma}{\alpha}\right) = 1$$

hat. Dann hätte man dieser Annahme gemäß

$$\alpha u^2 - \beta\gamma \cdot v^2 = +1, \qquad (17.)$$

eine Gleichung, in der $\beta\gamma$ ähnlich wie δ in den vorausgegangenen Entwickelungen von der Form $4n + 1$ ist, so daß u als eine ungerade, v als eine gerade Zahl angenommen werden muß. Hat man $\alpha = 8n + 5$, so enthält die gerade Zahl v den Faktor 2 nur einmal, so daß man $v = 2kk'k'' \ldots$ setzen kann, wenn unter $k, k', \ldots$ ungerade Primzahlen verstanden werden. Nun ist aber

$$\alpha u^2 \equiv 1, \pmod{k, k', \ldots},$$

also, wie auf S. 7, $kk'k'' \ldots$ quadratischer Rest, $2kk'k \ldots = v$ quadratischer Nichtrest, v^2 biquadratischer Nichtrest zu α; und da aus

$$\beta\gamma v^2 \equiv -1, \pmod{\alpha}$$

folgt, daß $\beta\gamma v^2$ biquadratischer Nichtrest und demnach $\beta\gamma$ biquadratischer Rest zu α ist, ein Resultat, daß man auch für $\alpha = 8n + 1$ ohne alle Schwierigkeit erhält, so muß man schließen, daß die Gleichung (17.) stets nur dann entstehen kann, wenn die Primzahlen β und γ nicht bloß quadratische, sondern beide gleichzeitig entweder biquadratische Reste oder Nichtreste zu α sind.
