ZUR THEORIE DER QUADRATISCHEN RESTE,

VON

ERNST SCHERING.

GAUSS hat durch seine *Disquisitiones Arithmeticae* die Lehre von den ganzen Zahlen zu einer systematischen Wissenschaft erhoben. In diesem Werke gibt es wol nur eine Stelle, von welcher man behaupten kann, dass die systematische Anordnung durchbrochen ist, nemlich dort wo GAUSS zwischen die Untersuchung der Congruenzen ersten Grades und der Congruenzen zweiten Grades die Untersuchung der höheren Potenzreste einschaltet. Es erscheint mir, anstatt die höheren Potenzreste als das allgemeinere Gebiet, zu welchen die quadratischen Reste gehören, dort zu untersuchen, natürlicher, die quadratischen Congruenzen nicht nur für Primzahl-Moduln, welche von GAUSS fast ausschliesslich behandelt werden, sondern auch für zusammengesetzte Moduln vollständig zu erledigen.

Auf solche Weise erhält man nicht nur eine Reihe neuer Lehrsätze, sondern man gelangt auch unmittelbar zu der Charakteristik einer Zahl im Gebiete der quadratischen Reste in Bezug auf einen zusammengesetzten Modul, dieser Charakteristik, auf welche GAUSS bei seinem ersten Beweise für das Reciprocitäts-Gesetz in der Theorie der quadratischen Reste erst aufmerksam wurde, nachdem er das Reciprocitäts-Gesetz durch Induction gefunden hatte.

Die Wichtigkeit dieses ersten Beweises, welchen GAUSS am 8. April 1796 gefunden hat (Vergl. meine Bemerkungen Seite 475 zu GAUSS' *Werken* Band I), ist von DIRICHLET auch dadurch anerkannt, dass er der Wiedergabe desselben Beweises in übersichtlicher Form eine eigne Abhandlung gewidmet hat (Crelle's Journal Bd. XLVII, Berlin 1854, Seite

139 bis 150). Es mag deshalb mir gestattet sein, auf einigen Blättern den unmittelbaren Beweis eines von mir gefundenen für jene von GAUSS eingeführte Charakteristik geltenden besonders einfachen Satzes zusammenzustellen; eines Satzes, welcher sich dem grossen Meister bei Abfassung seiner Disquiss. Arithmm. wie auch später entzogen zu haben scheint, wol deshalb, weil er in jenem Werke die Behandlung der quadratischen Reste für zusammengesetzte Moduln vermieden hat.

Da für die Vergleichung der verschiedenen Beweise des Reciprocitäts-Satzes der Umfang der benutzten Theorien von besonderer Bedeutung ist, so will ich hervorheben, dass im Folgenden von dem Inhalte der Disquiss. Arithmm. nichts weiter vorausgesetzt wird als die erste Section, welche im Allgemeinen von den Congruenzen der Zahlen handelt, und die zweite Section, von den Congruenzen des ersten Grades, bis einschliesslich des Artikel 36.

Der in diesem Artikel bewiesene Lehrsatz lässt sich, mit Hinzufügung einer leicht zu erledigenden Vervollständigung so aussprechen: Ist zu jedem von mehreren mit einander theilerfremden Moduln A, B, C, D ... eine beliebige Zahl, beziehungsweise a, b, c, d .. vorgegeben, so lässt sich zum Producte ABCD .. der Moduln als neuer Modul immer ein und nur ein Rest z finden, welcher den einzelnen vorgegebenen Zahlen a, b, c, d .. nach den bezüglichen Moduln A, B, C, D congruent ist: $z \equiv a$ (mod. A), $z \equiv b$ (mod. B), $z \equiv c$ (mod. C) ...

Ausserdem wird nur noch der Artikel 38 vorausgesetzt. Dieser bestimmt die EULERsche Function $\varphi(A)$, nemlich die Anzahl der positiven Zahlen, welche zu einer gegebenen positiven Zahl A theilerfremd und nicht grösser als dieselbe sind. Der Ausdruck für die EULERsche Function wird im Folgenden nicht benutzt sondern nur der Begriff derselben.

Zunächst wollen wir für den Fall, dass der Modul m eine zusammengesetzte Zahl und dass die Zahl a zu m theilerfremd ist, die Anzahl der Wurzeln x in der Congruenz

$$xx \equiv a \pmod{m}$$

bestimmen. Einige hierzu in enger Beziehung stehende bekannte Sätze will ich der Vollständigkeit wegen mit aufnehmen.

N. 1. Die ungerade Zahl a ist dann und nur dann quadratischer Rest zum Modul 4, wenn sie die Form $a = 4k + 1$ hat. Für diesen

Fall besitzt die Congruenz $xx \equiv a \pmod 4$ zwei von einander verschiedene Auflösungen nemlich:

(I) $$x \equiv +1 \text{ und } x \equiv -1 \pmod 4.$$

N. 2. Die ungerade Zahl a ist dann und nur dann quadratischer Rest zu einer die Zahl 4 übertreffende Potenz von 2, wenn sie die Form $a = 8k + 1$ hat. In der That, besteht die Congruenz $a \equiv x_s x_s \pmod{2^s}$ und bestimmt man h durch die Congruenz

$$x_s h \equiv \frac{a - x_s x_s}{2^s} \pmod{2^{s-2}},$$

setzt man ferner $$x_\sigma = x_s + h 2^{s-1}$$

so wird $x_\sigma x_\sigma \equiv a \pmod{2^{2s-2}}$. Von der Potenz $2^s = 2^3$ gelangt man durch Wiederholung dieses Verfahren zu allen höheren Potenzen von 2 als Moduln.

N. 3. Für eine Zahl a von der Form $8k + 1$ hat die Congruenz $xx \equiv a \pmod{2^{\pi_0}}$, wenn $\pi_0 > 2$ ist, vier Auflösungen; bezeichnet x_0 eine derselben, so sind:

(II) $$x \equiv +x_0,\ x \equiv -x_0,\ x \equiv +x_0 + 2^{\pi_0 - 1},\ x \equiv -x_0 - 2^{\pi_0 - 1} \pmod{2^{\pi_0}}$$

jene vier von einander verschiedene Wurzeln. Die Zahl $xx - x_0 x_0$ wird nemlich, weil x und x_0 ungerade sind, nur dann durch 2^{π_0} theilbar, wenn entweder $x - x_0$ oder $x + x_0$ durch $2^{\pi_0 - 1}$ theilbar ist.

N. 4. Ist p eine ungerade Primzahl und ist die durch p nicht theilbare Zahl a quadratischer Rest zu p, so ist a auch quadratischer Rest zu jeder Potenz von p als Modul. In der That besteht die Congruenz $a \equiv x_s x_s \pmod{p^s}$ und bestimmt man h durch die Congruenz

$$2 x_s h \equiv \frac{a - x_s x_s}{p^s} \pmod{p^s}, \quad \text{setzt dann} \quad x_\sigma = x_s + h p^s$$

so wird $x_\sigma x_\sigma \equiv a \pmod{p^{2s}}$. Auf solche Weise gelangt man von der Potenz $p^s = p$ durch Wiederholung zu jeder Potenz von p.

N. 5. Ist p_λ eine ungerade Primzahl und ist die durch p_λ nicht theilbare Zahl a quadratischer Rest zu p_λ, so hat die Congruenz $xx \equiv a \pmod{p_\lambda^{\pi_\lambda}}$ zwei Auflösungen; ist x_λ eine derselben, so sind

(III) $$x \equiv +x_\lambda \text{ und } x \equiv -x_\lambda \pmod{p_\lambda^{\pi_\lambda}}$$

die beiden von einander verschiedenen Wurzeln, weil $xx - x_\lambda x_\lambda$ nur für diese beiden Fälle durch $p_\lambda^{\pi_\lambda}$ theilbar wird.

N. 6. Bezeichnet m eine zusammengesetzte positive Zahl, hat also die Form

$$m = 2^{\pi_0} p_1^{\pi_1} p_2^{\pi_2} \dots p_\mu^{\pi_\mu} \tag{IV}$$

worin $p_1, p_2, p_3, \dots p_\mu$ von einander verschiedene ungerade Primzahlen und $\pi_1, \pi_2, \pi_3, \dots \pi_\mu$ positive Zahlen bedeuten, während π_0 auch der Null gleich sein kann,

bezeichnet ferner a eine zu m theilerfremde Zahl,

so hat die Congruenz $xx \equiv a \pmod{m}$ entweder keine oder $\psi(m)$ von einander verschiedene Auflösungen, wenn nemlich

$$\begin{aligned} &\psi(m) = 2^n && \text{für} \quad \pi_0 < 2, \\ &\psi(m) = 2^{n+1} && \text{für} \quad \pi_0 = 2, \\ &\psi(m) = 2^{n+2} && \text{für} \quad \pi_0 > 2 \quad \text{gesetzt wird.} \end{aligned} \tag{V}$$

Das Bestehen der Congruenz $xx \equiv a \pmod{m}$ erfordert, dass a quadratischer Rest zu jeder der Primzahlen $p_1, p_2, p_3, \dots p_\mu$ und

wenn $\pi_0 = 2$ ist, dass noch $a \equiv 1 \pmod{4}$

wenn aber $\pi_0 > 2$ ist, dass auch $a \equiv 1 \pmod{8}$ sei.

Umgekehrt reichen diese Bedingungen auch zur Möglichkeit der Erfüllung jener Congruenz aus, denn man braucht nur mit Hülfe des oben angegebenen Satzes aus dem Art. 36 der Disquiss. Arithmn. die Zahl x so zu bestimmen,

dass sie je einer der beiden Congruenzen (III) für jedes $\lambda \equiv 1, 2, 3, \dots, \mu$;
(VI) und wenn $\pi_0 = 1$ ist, dass sie noch der Congruenz $x \equiv 1 \pmod{2}$;
wenn aber $\pi_0 = 2$ ist, dass x einer der beiden Congruenzen (I);
wenn endlich $\pi_0 > 2$ ist, dass x einer der vier Congruenzen (II) genüge.

Zugleich erkennt man unmittelbar, dass verschiedene Verbindungen der für x erforderlichen linearen Congruenzen auch einander nach dem Modul m incongruente Werthe für x ergeben, so dass also die Anzahl der verschiedenen Verbindungen der linearen Congruenzen gleich der Anzahl der Wurzeln der quadratischen Congruenz $xx \equiv a \pmod{m}$ ist, wie es der Lehrsatz zu Anfang dieser N. 6 ausspricht.

Beispiel: Es ist $\psi(60) = \psi(4 \cdot 3 \cdot 5) = 2^3 = 8$; in der That die Wurzeln der Congruenz $xx \equiv 1 \pmod{60}$ sind $x \equiv \pm 1, \pm 11, \pm 19,$

± 29 und von der Congruenz $xx \equiv -11 \pmod{60}$ sind $x \equiv \pm 7, \pm 13, \pm 17, \pm 23,$ die Wurzeln, während jede zu 60 theilerfremde Zahl a, welche weder congruent $+1$ noch congruent -11 ist, einen quadratischen Nichtrest zum Modul 60 bedeutet.

N. 7. Die Anzahl der zum Modul m theilerfremden quadratischen Reste ist $= \frac{\varphi(m)}{\psi(m)}$, wie sich unmittelbar ergibt, wenn man jeden der $\varphi(m)$ zum Modul m gehörenden theilerfremden Reste quadrirt und den Rest Modulo m bildet, denn es entsteht dadurch nach dem Lehrsatze in N. 6. aus je $\psi(m)$ der $\varphi(m)$ Reste immer wieder derselbe quadratische zu m theilerfremde Rest.

N. 8. Die Anzahl der zum Modul m theilerfremden quadratischen Nichtreste ist demnach $= \varphi(m) - \frac{\varphi(m)}{\psi(m)}$. Beispiel: Es ist $\varphi(60) = 16$, $\psi(60) = 8$ und, wie in N. 6. gefunden, gibt es zum Modul 60 nur die zwei theilerfremden quadratischen Reste $+1$ und -11, die übrigen 14 theilerfremden Reste $-1, +11, \pm 7, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29$ sind quadratische Nichtreste zum Modul 60.

N. 9. Die quadratische Congruenz $a \equiv xx \pmod{m}$ kann man als speciellen Fall der bilinearen Congruenz $a \equiv yz \pmod{m}$ auffassen. Benutzt man die letztere Congruenz, um für ein gegebenes, zu einem die Zahl 2 übertreffenden Modul m theilerfremdes, a sämmtliche $\varphi(m)$ theilfremden Reste als Werthe der y und z anzuordnen, so ergibt sich, dass dies für alle Reste, mit Ausschluss der Wurzeln x, möglich ist. Will man aber jene Anordnung auf sämmtliche $\varphi(m)$ Reste ausdehnen, so braucht man die quadratische Congruenz nur in die Form $a \equiv -x \ (m - x)$ zu setzen und erhält dann:

(VII)
$$\begin{aligned}
a &\equiv -\alpha_1 \cdot \alpha'_1 \pmod{m} \\
a &\equiv -\alpha_2 \cdot \alpha'_2 \\
&\cdots\cdots \\
a &\equiv -\alpha_{\frac{1}{2}\psi} \cdot \alpha'_{\frac{1}{2}\psi} \\
&\cdots\cdots \\
a &\equiv +\alpha_{\frac{1}{2}\psi+1} \cdot \alpha'_{\frac{1}{2}\psi+1} \\
&\cdots\cdots \\
a &\equiv +\alpha_{\frac{1}{2}\varphi} \cdot \alpha'_{\frac{1}{2}\varphi}
\end{aligned}$$

wenn nemlich

(VIII) $$\pm \alpha_1, \pm \alpha_2, .. \pm \alpha_{\frac{1}{2}\psi}$$

die $\psi(m)$ von einander verschiedenen Wurzeln x der Congruenz $xx \equiv a \pmod{m}$ bedeuten und

(VIII*) $$\alpha'_1 = m - \alpha_1,\ \alpha'_2 = m - \alpha_2, .. \alpha'_{\frac{1}{2}\psi} = m - \alpha_{\frac{1}{2}\psi}$$

gesetzt ist. Die Zahl $\alpha_{\frac{1}{2}\psi+1}$ wird als irgend ein von $\alpha_1, \alpha'_1, \alpha_2, \alpha'_2, .. \alpha_{\frac{1}{2}\psi}, \alpha'_{\frac{1}{2}\psi}$ verschiedener zum Modul m theilerfremde Rest ausgewählt, wenn solche noch vorhanden sind. Die durch die obige Congruenz bestimmte Zahl $\alpha'_{\frac{1}{2}\psi+1}$ muss dann offenbar von $\alpha_{\frac{1}{2}\psi+1}$ und von den vorgenannten $\psi(m)$ Resten verschieden sein. Sind damit noch nicht alle theilerfremden Reste berücksichtigt, so sei $\alpha_{\frac{1}{2}\psi+2}$ einer der übrigen. Der durch die obige Congruenz bestimmte Rest $\alpha'_{\frac{1}{2}\psi+2}$ ist dann ein von allen $2(\frac{1}{2}\psi + 1) + 1$ vorher schon in Betracht gezogenen Resten verschiedener zum Modul m theilerfremder Rest. Durch Fortsetzung dieses Verfahrens werden alle $\varphi(m)$ Reste in der Weise erschöpft werden, dass die in den vorstehenden Congruenzen (VII) auftretenden α und α' zusammen das vollständige System der $\varphi(m)$ zum Modul m theilerfremden Reste

(IX) $$r_1, r_2, r_3 \ldots r_{\varphi(m)}$$

ausmachen.

Multipliciren wir die entsprechenden Seiten der obigen Congruenzen (VII) mit einander, so erhalten wir:

(X) $$a^{\frac{1}{2}\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} . r_1 r_2 r_3 \ldots r_{\varphi(m)} \pmod{m}$$

wobei a als quadratischer Rest vorausgesetzt war.

Die Zahl 1 ist quadratischer Rest zu m, wendet man sie als Werth von a an, so erhält man aus der letzten Congruenz den Lehrsatz:

N. 10. Das Product der sämmtlichen $\varphi(m)$ zum Modul m theilerfremden Reste ist congruent $(-1)^{\frac{1}{2}\psi(m)}$,

(XI) $$r_1 . r_2 . r_3 \ldots r_{\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} \pmod{m}.$$

Der entstehende Rest wird (zufolge N. 6) nur dann zu -1, wenn m entweder gleich 4 oder gleich irgend einer Potenz einer ungeraden

Primzahl oder endlich gleich dem Doppelten einer solchen Potenz ist. Für alle andere Zahlen m entsteht der Rest $+1$. In dieser Form hat GAUSS die Verallgemeinerung des WILSON'schen Satzes ausgesprochen. Disquiss. Arr. Art. 78. Von dem Beweise hat er eine Andeutung gegeben.

Beispiel: Es ist $1 \equiv -1 \cdot 59 \equiv -11 \cdot 49 \equiv -19 \cdot 41 \equiv -29 \cdot 31 \equiv$ $\equiv 7 \cdot 43 \equiv 13 \cdot 37 \equiv 17 \cdot 53 \equiv 23 \cdot 47 \pmod{60}$ und $49 \equiv -7 \cdot 53 \equiv$ $-13 \cdot 47 \equiv -17 \cdot 43 \equiv -23 \cdot 37 \equiv 1 \cdot 49 \equiv 11 \cdot 59 \equiv 19 \cdot 31 \equiv 29 \cdot 41$.

N. 11. Wendet man die bilineare Congruenz $b \equiv y \cdot z \pmod{m}$ auf einen zu m theilerfremden quadratischen Nichtrest b an, um entsprechend wie in N. 9. das vollständige System der theilerfremden Reste für den Modul m zu ordnen, so treten keine Ausnahmefälle wie bei einem quadratischen Reste a ein, sondern in allen Congruenzen ist dasselbe Vorzeichen anzuwenden und man erhält

$$\text{(XII)} \qquad \begin{aligned} b &\equiv \beta_1 \cdot \beta'_1 \pmod{m} \\ b &\equiv \beta_2 \cdot \beta'_2 \\ b &\equiv \beta_3 \cdot \beta'_3 \\ &\cdots\cdots \\ b &\equiv \beta_{\frac{1}{2}\varphi} \cdot \beta'_{\frac{1}{2}\varphi} \end{aligned}$$

Hier bilden die $\beta_1 \ldots \beta_{\frac{1}{2}\varphi}$, $\beta'_1 \ldots \beta'_{\frac{1}{2}\varphi}$ wieder in einer besonderen Anordnung das vollständige System der zum Modul m theilerfremden Reste $r_1 \cdot r_2 \cdot r_3 \ldots r_{\varphi(m)}$. Multiplicirt man die entsprechenden Seiten dieser Congruenzen mit einander und berücksichtigt N. 10, so erhält man

$$\text{(XIII)} \qquad b^{\frac{1}{2}\varphi(m)} \equiv \beta_1 \ldots \beta_{\frac{1}{2}\varphi} \cdot \beta'_1 \ldots \beta'_{\frac{1}{2}\varphi} \equiv r_1 \cdot r_2 \cdot r_3 \ldots r_{\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} \pmod{m}.$$

Beispiel: Es ist (modulo 60): $7 \equiv 1 \cdot 7 \equiv 11 \cdot 17 \equiv 13 \cdot 19 \equiv 23 \cdot 29 \equiv$ $\equiv 31 \cdot 37 \equiv 41 \cdot 47 \equiv 43 \cdot 49 \equiv 53 \cdot 59$ und $11 \equiv 1 \cdot 11 \equiv 7 \cdot 53 \equiv 13 \cdot 47 \equiv$ $\equiv 17 \cdot 43 \equiv 19 \cdot 29 \equiv 23 \cdot 37 \equiv 31 \cdot 41 \equiv 49 \cdot 59$.

Die Vergleichung der N. 9, 10, 11 gibt den

N. 12. LEHRSATZ. *Ist a zum Modul m theilerfremder quadratischer Rest, so wird*

$$\text{(XIV)} \qquad a^{\frac{1}{2}\varphi(m)} \equiv +1 \pmod{m}.$$

Ist a zum Modul m theilerfremder quadratischer Nichtrest, so wird

$$\text{(XV)} \qquad a^{\frac{1}{2}\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} \pmod{m}.$$

Hat die bilineare Congruenz $a \equiv y \,.\, z \pmod{m}$ *in ganzen positiven unter* m *liegenden Zahlen* y *und* z, *von welchen* y *kleiner als* z *ist,* $\frac{1}{2}\varphi(m)$ *Auflösungen, so muss* a *quadratischer Nichtrest zu* m *sein.*

Beträgt die Anzahl jener Auflösungen aber weniger als $\frac{1}{2}\varphi(m)$ *und ist* a *theilerfremd zu* m, *so muss* a *quadratischer Rest zum Modul* m *sein, und die Anzahl jener Auflösungen wird* $\frac{1}{2}\varphi(m) - \frac{1}{2}\psi(m)$ *betragen.*

Beispiel: Wenn jede der zum Modul 60 theilerfremden Zahlen quadrirt wird, so entsteht entweder der Rest 1 oder 49, also ist 7 quadratischer Nichtrest zu 60. Es ist $\frac{1}{2}\varphi(60) = 8$, $\frac{1}{2}\psi(60) = 4$, $7^8 \equiv (-11)^4 = 14641 \equiv 1 \equiv (-1)^4 \pmod{60}$.

Es ist (mod. 50):

$1 \equiv -1 \,.\, 49 \equiv 3 \,.\, 17 \equiv 7 \,.\, 43 \equiv 9 \,.\, 39 \equiv 11 \,.\, 41 \equiv 13 \,.\, 27 \equiv 19 \,.\, 29 \equiv 21 \,.\, 31 \equiv 23 \,.\, 37 \equiv 33 \,.\, 47$; $3 \equiv 1 \,.\, 3 \equiv 7 \,.\, 29 \equiv 9 \,.\, 17 \equiv 11 \,.\, 23 \equiv 13 \,.\, 31 \equiv 19 \,.\, 37 \equiv 21 \,.\, 43 \equiv 27 \,.\, 39 \equiv 33 \,.\, 41 \equiv 47 \,.\, 49$; ferner ist $\frac{1}{2}\varphi(50) = 10$, $\frac{1}{2}\psi(50) = 1$, $11^5 = 161051 \equiv 1 \pmod{50}$, also $11^{10} \equiv +1$ und $11 \equiv 19^2 \pmod{50}$ aber $3^{10} = 59049 \equiv -1 \equiv (-1)^{\frac{1}{2}\psi(50)}$.

N. 13. Ausser der bilinearen Congruenz $a \equiv y \,.\, z \pmod{m}$ bietet für eine auf die Zahl a sich beziehende Anordnung der Reste zum Modul m die lineare Congruenz mit a als constanten Factor, zum Beispiel $a \,.\, u \equiv v \pmod{m}$, Gelegenheit. Wählt man der Einfachheit halber für u der Reihe nach die positiven unter den absolut kleinsten zum Modul m theilerfremden Reste, sie mögen mit $r_1, r_2, \ldots r_{\frac{1}{2}\varphi(m)}$ bezeichnet werden; so werden die zugehörigen v zum Modul m theilerfremd, und einander weder unmittelbar noch nach theilweiser Aenderung des Vorzeichens congruent sein. Nimmt man für v auch absolut kleinste Reste, für $r'_1, r'_2 \ldots$ absolut kleinste positive Reste und setzt

$$\text{(XVI)} \qquad \begin{aligned} a \,.\, r_1 &\equiv \eta_1 r'_1 \pmod{m} \\ a \,.\, r_2 &\equiv \eta_2 r'_2 \\ &\cdots\cdots \\ a \,.\, r_{\frac{1}{2}\varphi(m)} &\equiv \eta_{\frac{1}{2}\varphi(m)} r'_{\frac{1}{2}\varphi(m)} \end{aligned}$$

indem man für $\eta_1, \eta_2, \ldots \eta_{\frac{1}{2}\varphi(m)}$ keine andere Werthe als $+1$ oder -1 zulässt, so sind also die Zahlen $r'_1, r'_2, \ldots r'_{\frac{1}{2}\varphi(m)}$ abgesehen von der Reihenfolge dieselben wie $r_1, r_2, \ldots r_{\frac{1}{2}\varphi(m)}$. Multiplicirt man die entsprechenden Seiten dieser Congruenzen mit einander, dividirt dann die beiden Seiten der entstehenden Congruenz durch das zum Modul m

theilerfremde Product $r_1, r_2, \ldots r_{\frac{1}{2}\varphi(m)}$ oder $r'_1, r'_2, \ldots r'_{\frac{1}{2}\varphi(m)}$, so erhält man

(XVII) $$a^{\frac{1}{2}\varphi(m)} \equiv \eta_1 \cdot \eta_2 \cdots \eta_{\frac{1}{2}\varphi(m)} \pmod{m}$$

und demnach unter Benutzung von N. 12 den

N. 14. LEHRSATZ: *Die Anzahl* $\eta(a, m)$ *der aus den Producten von* a *multiplicirt in die positiven absolut kleinsten zum Modul* m *theilerfremden Reste sich wieder für den Modul* m *ergebenden absolut kleinsten aber negativen Reste oder die Anzahl der in absolut kleinsten positiven Resten* u, v *dargestellten Lösungen der Congruenz* $a \cdot u + v \equiv 0 \pmod{m}$ *wird eine gerade Zahl wenn* a *zum Modul* m *theilerfremder quadratischer Rest das heisst die Congruenz* $a \equiv xx \pmod{m}$ *lösbar ist, dagegen wenn diese Congruenz nicht lösbar, sondern wenn* a *zum Modul* m *theilerfremder quadratischer Nichtrest ist, so wird jene Anzahl* $\eta(a, m)$ *mit* $\frac{1}{2}\psi(m)$ *das heisst mit der Anzahl der in absolut kleinsten positiven Resten dargestellten Lösungen* w *der Congruenz* $aa \equiv ww \pmod{m}$ *gleichzeitig gerade oder ungerade.*

(XVIII) $a^{\frac{1}{2}\varphi(m)} \equiv +1 \equiv (-1)^{\eta(a, m)} \pmod{m}$, *wenn* a *theilerfremder quadratischer Rest zu* m;

(XIX) $a^{\frac{1}{2}\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} \equiv (-1)^{\eta(a, m)} \pmod{m}$, *wenn* a *theilerfremder quadratischer Nichtrest zu* m.

Für den besonderen Fall, dass m eine ungerade Primzahl ist, geht dieser Satz in den von GAUSS Januar 1808 aufgestellten Lehrsatz über, auf welchen er seinen dritten Beweis des Reciprocitäts-Gesetzes gründete (Art. 3. Seite 4, Band II meiner Redaction von GAUSS' Werken). Mein in der hier vorliegenden Abhandlung geführte Beweis geht für jenen besonderen Fall in den Beweis über, welchen DIRICHLET für den GAUSS'schen Satz in seinen frühesten Universitäts-Vorlesungen zu geben pflegte.

Beispiel. Für den Modul 60 ist 49 theilerfremder quadratischer Rest, aber 7 theilerfremder quadratischer Nichtrest, $\frac{1}{2}\varphi(60) = 8$, $\frac{1}{2}\psi(60) = 4$, $49^8 \equiv 11^8 \equiv (11^4)^2 \equiv (14641)^2 \equiv 1$, $7^8 \equiv 11^4 \equiv 1$, $\eta(49, 60) = 8$, $\eta(7, 60) = 4$, $49 \cdot 1 \equiv -11$, $49 \cdot 7 \equiv -17$, $49 \cdot 11 \equiv -1$, $49 \cdot 13 \equiv -23$, $49 \cdot 17 \equiv -7$, $49 \cdot 19 \equiv -29$, $49 \cdot 23 \equiv -13$, $49 \cdot 29 \equiv -19$,

$7 . 1 \equiv 7$, $7 . 7 \equiv -11$, $7 . 11 \equiv 17$, $7 . 13 \equiv -29$, $7 . 17 \equiv -1$, $7 . 19 \equiv 13$, $7 . 23 \equiv -19$, $7 . 29 \equiv 23$. Für den Modul 50 ist $11 \equiv 19^2$, also 11 theilerfremder quadratischer Rest aber 7 theilerfremder quadratischer Nichtrest, $\frac{1}{2}\varphi(50) = 10$, $\frac{1}{2}\psi(50) = 1$, $11^{10} \equiv 11^{5 \cdot 2} \equiv \equiv 161051^2 \equiv 1$, $7^{10} \equiv (-1)^5 \equiv -1$, $\eta(11, 50) = 6$, $\eta(7, 50) = 5$, $11 . 1 \equiv 11$, $11 . 3 \equiv -17$, $11 . 7 \equiv -23$, $11 . 9 \equiv -1$, $11 . 11 \equiv 21$, $11 . 13 \equiv -7$, $11 . 17 \equiv -13$, $11 . 19 \equiv 9$, $11 . 21 \equiv -19$, $11 . 23 \equiv 3$, $7 . 1 \equiv 7$, $7 . 3 \equiv 21$, $7 . 7 \equiv -1$, $7 . 9 \equiv 13$, $7 . 11 \equiv -23$, $7 . 13 \equiv \equiv -9$, $7 . 17 \equiv 19$, $7 . 19 \equiv -17$, $7 . 21 \equiv -3$, $7 . 23 \equiv 11$.

N. 15. Multiplicirt man beide Seiten so wie den Modul m in den Congruenzen (XVI) mit derselben positiven Zahl δ, setzt $M = \delta m$ und beachtet, dass die Gesammtheit der Producte

$$\delta . r_1, \ \delta . r_2, \ \delta . r_3, \ \ldots \ \delta . r_{\frac{1}{2}\varphi(m)}$$

die vollständige Reihe derjenigen zum Modul M gehörenden positiven absolut kleinsten $\frac{1}{2}\varphi\left(\frac{M}{\delta}\right)$ Reste bilden, welche mit M den grössten gemeinsamen Theiler δ besitzen, so erhält man den Satz:

Die zu Eingang der N. 14 *definirte Anzahl* $\eta(a, m)$ *oder* $\eta\left(a, \frac{M}{\delta}\right)$ *ist auch gleich der Anzahl der absolut kleinsten negativen Reste, welche sich für den Modul* M *aus den Producten der zu* M *theilerfremden Zahl* a *multiplicirt in die zum Modul* M *gehörenden mit ihm den grössten gemeinsamen Theiler* δ *besitzenden positiven absolut kleinsten* $\frac{1}{2}\varphi\left(\frac{M}{\delta}\right)$ *Resten ergeben.*

N. 16. Die zum Modul M gehörenden absolut kleinsten nothwendig positiv zu nehmenden Reste also die natürliche Zahlenreihe

entweder (XX) $1, 2, 3, 4, \ldots \frac{M-1}{2}$, wenn M ungerade ist,

oder (XXI) $1, 2, 3, 4, \ldots \frac{M}{2} - 1$, wenn M gerade ist,

kann auch aufgefasst werden als die Gesammtheit derjenigen zum Modul M gehörenden absolut kleinsten positiven Reste, welche mit M je einen

von allen unter $\frac{M}{2}$ liegenden Theilern δ der Zahl M als grössten gemeinsamen Theiler besitzen.

Multiplicirt man mit der zu M theilerfremden Zahl a jede Zahl des obigen Resten-Systems (XX) oder (XXI), bildet von diesen Producten die absolut kleinsten Reste für den Modul M, wendet die hier angedeutete Gruppirung jener Zahlen nach ihrem jedesmaligen mit M gemeinsamen grössten Theiler an und benutzt den in N. 15 aufgestellten Satz, so findet man den

N. 17. Lehrsatz: *Die Anzahl* $H(a, M)$ *der absolut kleinsten negativen Reste, welche in Bezug auf den Modul* M *den Producten*

$$\textit{entweder} \quad a.1,\ a.2,\ a.3,\ \ldots .\ a\frac{M-1}{2}, \quad \textit{wenn}\ M\ \textit{ungerade},$$

$$\textit{oder} \quad a.1,\ a.2,\ a.3,\ \ldots .\ a\left(\frac{M}{2}-1\right), \quad \textit{wenn}\ M\ \textit{gerade},$$

congruent sind, wird, wenn die Zahl a *zu* M *theilerfremd ist, gleich*

$$\text{(XXII)} \quad H(a, M) = \sum_{\delta}\eta\left(a, \frac{M}{\delta}\right) = \sum_{m}\eta(a, m), \quad 1 \leqq \delta < \frac{M}{2}, \quad 2 < m \leqq M = m\delta$$

worin die eine Summation über die sämmtlichen unter $\frac{M}{2}$ *liegenden Theiler* δ *des Modul* M, *die andere Summation über die sämmtlichen die Zahl* 2 *übertreffenden Theiler* m *des Modul* M *auszudehnen ist.*

Wählt man in diesem Satze die Zahl $a = -1$ und berücksichtigt, dass $\eta(-1, m) = \frac{1}{2}\varphi(m)$ ist, so erhält man den Euler'schen Summation's Satz für die φ Function. Von diesem Satze werden wir hier aber keinen Gebrauch zu machen haben.

Beispiel. Es ist: $H(7, 60) = 13$, $\sum_{\delta}\eta\left(7, \frac{60}{\delta}\right) = \eta(7, 60) + \eta(7, 30) +$ $+ \eta(7, 20) + \eta(7, 15) + \eta(7, 12) + \eta(7, 10) + \eta(7, 6) + \eta(7, 5) + \eta(7, 4) +$ $+ \eta(7, 3) = 4 + 2 + 0 + 2 + 2 + 1 + 0 + 1 + 1 + 0 = 13$ Ferner ist: $H(7, 45) = 9$, $\sum_{\delta}\eta\left(7, \frac{45}{\delta}\right) = \eta(7, 45) + \eta(7, 15) + \eta(7, 9) + \eta(7, 5) +$ $+ \eta(7, 3) = 4 + 2 + 2 + 1 + 0 = 9.$

N. 18. Ist M gerade, so wird für ein ungerades a

entweder $as \equiv +s' > 0$ und $a\left(\frac{M}{2} - s\right) \equiv \frac{M}{2} - s' > 0 \pmod{M}$

oder $as \equiv -s' < 0$ und $a\left(\frac{M}{2} - s\right) \equiv -\frac{M}{2} + s' < 0 \pmod{M}$

worin s und s' positive unter $\frac{M}{2}$ liegende Zahlen bedeuten.

Die absolut kleinsten negativen Reste werden also nicht anders als paarweise auftreten können, wenn jedes s von $\frac{M}{2} - s$ verschieden also $\frac{M}{2}$ ungerade ist.

Für ein geradzahliges $\frac{M}{2}$ wird

$$a\frac{M}{4} \equiv +\frac{M}{4} \pmod{M}, \text{ wenn } a \equiv 1 \pmod{4} \text{ ist,}$$

$$a\frac{M}{4} \equiv -\frac{M}{4} \pmod{M}, \text{ wenn } a \equiv 3 \pmod{4} \text{ ist.}$$

Wir erhalten demnach den Satz:

Für einen geradzahligen Modul M *und für ein ungerades* a *wird die Anzahl* $H(a, M)$ *der den Producten*

$$a.1, \quad a.2, \quad a.3, \quad \ldots. \quad a.\left(\frac{M}{2} - 1\right)$$

nach dem Modul M *congruenten absolut kleinsten negativen Reste*

eine gerade Zahl sein, $H(a, M) \equiv 0 \pmod{2}$ *wenn* $M \equiv 2 \pmod{4}$ *oder wenn zugleich* $M \equiv 0$ *und* $a \equiv 1 \pmod{4}$ *ist;*

dagegen wird sie ungeradzahlig, $H(a, M) \equiv 1 \pmod{2}$, *wenn zugleich* $M \equiv 0$ *und* $a \equiv 3 \pmod{4}$ *ist.*

Beispiele: $H(7, 30) = 8$, $H(5, 12) = 2$, $H(7, 60) = 13$.

N. 19. Aus der Verbindung der Lehrsätze in N. 17 und 14 folgt

(XXIII) $$H(a, M) = \sum_m \eta(a, m) \equiv \sum_m{}' \tfrac{1}{2}\psi(m) \pmod{2}$$

worin $\sum_m$ sich auf alle, die Zahl 2 übertreffenden, Theiler m von M, dagegen $\sum_m'$ sich nur auf diejenigen die Zahl 2 übertreffenden im Modul M enthaltenden Theiler m bezieht, zu welchen a quadratischer Nichtrest ist.

Wir haben also den Lehrsatz: Die Anzahl $H(a, M)$ derjenigen absolut kleinsten negativen Reste, welche nach dem Modul M den Producten

$$\text{entweder} \quad a.1,\ a.2,\ a.3,\ \ldots\ a\frac{M-1}{2}, \quad \text{wenn M ungerade,}$$

$$\text{oder} \quad a.1,\ a.2,\ a.3,\ \ldots\ a\left(\frac{M}{2}-1\right), \quad \text{wenn M gerade,}$$

congruent sind, wird, für ein zu M theilerfremdes a, gleichzeitig gerade oder ungerade mit der Gesammt-Anzahl aller in absolut kleinsten positiven Resten modulo m dargestellten Lösungen w der Congruenzen $1 \equiv ww \pmod{m}$ für die ganze Reihe derjenigen Moduln m, welche grösser als 2 und Theiler von M sind und zu welchen a quadratischer Nichtrest ist.

Beispiel: Es ist $7 \equiv 1.1 \pmod{6 \text{ und mod. } 3}$ für alle anderen Theiler von 60 ist 7 quadratischer Nichtrest. Ferner ist $1 \equiv 1.1 \pmod{4 \text{ und mod. } 5 \text{ und mod. } 10}$, $1 \equiv 1.1 \equiv 5.5 \pmod{12}$, $1 \equiv 1.1 \equiv 4.4 \pmod{15}$, $1 \equiv 1.1 \equiv 9.9 \pmod{20}$, $1 \equiv 1.1 \equiv 11.11 \pmod{30}$, $1 \equiv 1.1 \equiv 11.11 \equiv 19.19 \equiv 29.29 \pmod{60}$ also $\sum_m' \frac{1}{2}\psi(m) = \frac{1}{2}\psi(4) + \frac{1}{2}\psi(5) + \frac{1}{2}\psi(10) + \frac{1}{2}\psi(12) + \frac{1}{2}\psi(15) + \frac{1}{2}\psi(20) + \frac{1}{2}\psi(30) + \frac{1}{2}\psi(60) = 1 + 1 + 1 + 2 + 2 + 2 + 2 + 4 = 15$, endlich ist $H(7, 60) = 13 \equiv 15 \pmod{2}$.

N. 20. Wir beschränken jetzt unsere Untersuchung auf den Fall eines ungeraden M, welches also in der Form

$$\text{(XXIV)} \qquad M = P_1^{e_1} P_2^{e_2} \ldots P_\lambda^{e_\lambda} \ldots P_\nu^{e_\nu}$$

dargestellt werden kann, worin $P_1, P_2, \ldots P_\lambda, \ldots P_\nu$ von einander verschiedene positive Primzahlen und $e_1, e_2, \ldots e_\lambda, \ldots e_\nu$ irgend welche positive Zahlen bedeuten. Aus der Congruenz (XXIII) folgt dann, wenn

wir auch noch die in N. 6 gefundene Bestimmung von $\psi(m)$ und die übrigen dort ausgesprochenen Lehrsätze anwenden, die Congruenz:

$$\text{(XXV)} \qquad \mathrm{H}(a, \mathrm{M}) = \sum_m \eta(a, m) \equiv \sum_m{}' \tfrac{1}{2}\psi(m) \equiv \sum_m{}'' \tfrac{1}{2}\psi(m) = \sum_\lambda{}''' e_\lambda \pmod 2.$$

Hierin erstreckt sich die Summation $\sum_m$ über alle Theiler m von M, die Summation $\sum_m{}'$ über alle diejenigen in M enthaltenen Theiler m, zu welchen a quadratischer Nichtrest ist, die Summation $\sum_m{}''$ über alle diejenigen in M enthaltenen Theiler m, welche je einzeln keine verschiedene Primzahlen enthalten und zu welchen a quadratischer Nichtrest ist, endlich die Summation $\sum_\lambda{}''' e_\lambda$ über die in der Darstellung (XXIV) von M vorkommenden Exponenten derjenigen Primzahlen P_λ, zu welchen die Zahl a quadratischer Nichtrest ist.

Diese letzte Summe $\sum_\lambda{}''' e_\lambda$ bedeutet auch die Anzahl aller derjenigen gleichen und ungleichen in M enthaltenen Primfactoren, zu welchen a quadratischer Nichtrest ist. Die Congruenz (XXV) gibt also den Lehrsatz:

Die Anzahl $\mathrm{H}(a, \mathrm{M})$ *derjenigen Producte*

$$a \,.\, 1, \quad a \,.\, 2, \quad a \,.\, 3, \quad \ldots \; a\frac{\mathrm{M}-1}{2}$$

welche absolut kleinsten negativen Resten für den ungeradzahligen Modul M *congruent sind, wird für ein zu* M *theilerfremdes* a *gleichzeitig gerade oder ungerade mit der Anzahl aller derjenigen gleichen und ungleichen in* M *enthaltenen Primfactoren, zu welchen* a *quadratischer Nichtrest ist.*

Beispiel: Es ist $\mathrm{H}(7, 45) = 9$, $\sum_m{}' \tfrac{1}{2}\psi(m) = \tfrac{1}{2}\psi(5) + \tfrac{1}{2}\psi(15) + \tfrac{1}{2}\psi(45) = 1 + 2 + 2 = 5$; $\sum_m{}'' \tfrac{1}{2}\psi(m) = \tfrac{1}{2}\psi(5) = 1 \equiv 5 \equiv 9 \pmod 2$ für $a = 7$, $\mathrm{M} = 45$. Dagegen für $a = 11$, $\mathrm{M} = 45$ wird $\mathrm{H}(11, 45) = 10$, $\sum_m{}' \tfrac{1}{2}\psi(m) = \tfrac{1}{2}\psi(3) + \tfrac{1}{2}\psi(9) + \tfrac{1}{2}\psi(15) + \tfrac{1}{2}\psi(45) = 1 + 1 + 2 + 2 = 6$, $\sum_m{}'' \tfrac{1}{2}\psi(m) = \tfrac{1}{2}\psi(3) + \tfrac{1}{2}\psi(9) = 1 + 1 = 2 \equiv 6 \equiv 10 \pmod 2$.

N. 21. Es mag noch bemerkt werden, dass die oben benutzten Potenzen von a und b mit dem Exponenten $\frac{1}{2}\varphi(m)$ nicht wesentlich für diese Untersuchung sind, sondern hier nur gebraucht wurden, um an die üblichen Betrachtungen anzuschliessen. Ohne Herbeiziehung derselben wird die Entwickelung noch einfacher. Man hat dann den folgenden Lehrsatz aufzustellen:

Die Anzahl aller Lösungen der Congruenzen

(XXVI) $$-x\left(\frac{\mathrm{M}}{\delta}-x\right)\equiv a \pmod{\frac{\mathrm{M}}{\delta}}$$ *in ganzen positiven unter* $\frac{\mathrm{M}}{2\delta}$ *liegenden Zahlen* x,

(XXVII) $$1\equiv -x'\left(\frac{\mathrm{M}}{\delta}-x'\right) \pmod{\frac{\mathrm{M}}{\delta}}$$ *in ganzen positiven unter* $\frac{\mathrm{M}}{2\delta}$ *liegenden Zahlen* x',

(XXVIII) $au\equiv -v \pmod{\mathrm{M}}$ *in ganzen positiven unter* $\frac{\mathrm{M}}{2}$ *liegenden und mit* M *denselben beliebigen grössten unter* $\frac{\mathrm{M}}{2}$ *liegenden gemeinsamen Theiler* δ *enthaltenden Zahlen* u, v,

zusammengenommen ist für ein zu M *theilerfremdes* a *immer eine gerade Zahl.*

Es ist leicht zu sehen, dass man u und v anstatt aus dem System der absolut kleinsten positiven Reste des Modul M zu nehmen, sie auch aus irgend einem vollständigen halben Resten-System für den Modul M wählen kann, wenn man nemlich darunter ein System aller solcher Reste versteht, von denen keine zwei eine durch den Modul M theilbare Differenz oder Summe ergeben. Für den Fall, dass a und M ungerade Zahlen bedeuten, ist es häufig von Vortheil die sämmtlichen unter M liegenden positiven entweder geraden oder ungeraden Zahlen als ein solches vollständiges halbes Resten-System für den Modul M zu benutzen.

Der Beweis des Lehrsatzes ergibt sich aus der Multiplication der entsprechenden Seiten aller Congruenzen, welche zunächst entstehen, wenn man sämmtliche Lösungen in jene Congruenzen (XXVI), (XXVII), (XXVIII) einsetzt, nachdem man die beiden Seiten und den Modul der Congruenz $au\equiv -v \pmod{\mathrm{M}}$ für jede Lösung durch δ dividirt hat

und welche ferner noch entstehen, wenn man in die Congruenzen

(XXIX) $y \,.\, z \equiv a \pmod{\frac{M}{\delta}}$ ihre Lösungen durch ganze positive unter $\frac{M}{\delta}$ liegende und die Bedingung y kleiner als z erfüllende Zahlen y, z einsetzt, ebenso in

(XXX) $1 \equiv y' \,.\, z' \pmod{\frac{M}{\delta}}$ ihre Lösungen durch ganze positive unter $\frac{M}{\delta}$ liegende und die Bedingung y' kleiner als z' erfüllende Zahlen y', z' einsetzt und schliesslich in

(XXXI) $au \equiv v \pmod{M}$ ihre Lösungen durch ganze positive unter $\frac{M}{2}$ liegende und jenen grössten mit M gemeinsamen Theiler δ enthaltende Zahlen u, v einführt und beide Seiten und den Modul M dieser Congruenz für jede Lösung durch δ dividirt.

Die beiden Seiten der durch diese Multiplication sich ergebenden Congruenz besitzen nemlich, wie unmittelbar aus den Congruenz-Systemen (VII), (XII) und (XVI) hervorgeht, gleiche absolute zu $\frac{M}{\delta}$ theilerfremde Zahlenwerthe und müssen, da der Modul $\frac{M}{\delta}$ dieser Congruenz grösser als 2 ist, auch gleiche Vorzeichen haben.

N. 22. Die Begriffe der beiden Anzahlen, welche durch den Lehrsatz des N. 20 zu einander in Beziehung gesetzt werden, sind schon von Gauss aufgestellt. Nachdem er im März 1795 (wie er selbst in sein Handexemplar der Diss. Arr. eingeschrieben, G.-Werke Bd. I. Seite 476 meine Bemerkungen) das Reciprocitäts-Gesetz der quadratischen Reste durch Induction gefunden hatte, welches er in Art. 131 der im Jahre 1801 herausgegebenen Disquiss. Arr. unter verschiedenen Formen darstellt, gerieth er am 29. Apr. 1796 (G.-Werke Bd. I. Seite 476) auf die Betrachtung der Anzahl der in einer gegebenen ungeraden Zahl P enthaltenen gleichen und verschiedenen Primfactoren, zu welchen eine andere gegebene Zahl Q quadratischer Nichtrest ist In Art. 133 der Disquiss.

Arr. zeigt er, dass wenn zwischen allen in der einen gegebenen ungeraden Zahl Q enthaltenen Primzahlen einerseits und allen in der anderen gegebenen ungeraden Zahl P enthaltenen Primzahlen andererseits das Reciprocitäts-Gesetz für die quadratischen Reste besteht, dann auch das analoge Reciprocitäts-Gesetz für die eben definirte Anzahl (Q, P) und für diejenige entsprechende Anzahl (P, Q) gilt, welche sich auf dieselben beiden gegebenen Zahlen aber nach ihrer Umwechselung bezieht. Der Begriff der hier definirten Anzahl ist dann für GAUSS ein wesentliches Hülfsmittel, um in den Artikeln 134 bis 136 den vollständigen Beweis für das Reciprocitäts-Gesetz der quadratischen Reste durchzuführen.

JACOBI hat im Jahre 1837 (Monatsberichte der Akademie der Wissenschaft zu Berlin Seite 135 »Ueber die Kreistheilung und ihre Anwendung auf die Zahlentheorie»), wie es scheint ohne sich der betreffenden Stelle bei GAUSS bewusst zu sein, die gleichbedeutende Characteristik $\left(\frac{Q}{P}\right)$ eingeführt, welche den Werth entweder -1 oder $+1$ besitzt, je nachdem Q entweder zu einer ungeraden oder zu einer nicht ungeraden Anzahl von gleichen und verschiedenen in P enthaltenen Primfactoren quadratischer Nichtrest ist. JACOBI nennt dies das verallgemeinerte LEGENDRE'sche Zeichen und definirt es als das Product von allen LEGENDRE'schen Zeichen $\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\left(\frac{Q}{p_3}\right)\ldots\left(\frac{Q}{p_\nu}\right)$, worin die $p_1, p_2, p_3, \ldots p_\nu$ die Gesammtheit aller derjenigen gleichen und verschiedenen Primfactoren ausmachen, deren Product gleich P ist.

Auch der Begriff der anderen in dem Lehrsatze des N. 20 vorkommenden Anzahl, nemlich der Anzahl derjenigen absolut kleinsten negativen Reste, welche sich für eine zusammengesetzte ungerade Zahl M als Modul aus den Producten einer zu M theilerfremden Zahl a multiplicirt in jeden einzelnen absolut kleinsten positiven Rest ergeben, ist von GAUSS untersucht und dafür der Reciprocitäts-Satz bewiesen in Art. 2 der Abhandlung »Theorematis Fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae» 1817 Febr. (G.-Werke Bd. II. S. 52.).

Von dem in N. 20 ausgesprochenen Satze hat GAUSS den speciellen Fall, wenn M eine Primzahl bedeutet, aufgestellt und darauf schon seinen dritten Beweis des Reciprocitäts-Satzes gegründet; aber der allgemeine Lehrsatz für eine zusammengesetzte Zahl M scheint sich ihm entzogen zu haben.

Meine Auffindung dieses Satzes ist in den Monatsberichten der Akademie der Wissenschaften zu Berlin 1876 Seite 330 veröffentlicht. Herr KRONECKER hat hieran mehrere Entwickelungen angeschlossen, in welcher er auch ausspricht, dass er vor meiner Mittheilung diesen Satz selbst gefunden habe. Er stützt seinen Beweis des Satzes auf die Kenntniss des vorausbewiesenen Reciprocitäts-Satzes.

N. 23. Die in N. 21 aufgestellte Form des Lehrsatzes halte ich deshalb für beachtenswerth, weil darin und in dem Beweise wesentlich nur die Abzählung der Auflösungen von bilinearen und von linearen Congruenzen auftritt und weil in meinem Beweise (1879) des Reciprocitäts-Satzes für die quadratischen Reste keine andere Untersuchung als die Abzählung der Lösungen von linearen Congruenzen in Anwendung gebracht wird. Eine genaue Vergleichung dieses Beweises mit dem dritten (1808) und dem fünften (1817) Beweise von GAUSS, dem geometrischen Beweise von EISENSTEIN (1844), dem Beweise von Herrn ZELLER (1872), dem arithmetischen Beweise von Herrn KRONECKER (1876) und den beiden Beweisen von Sign. GENOCCHI (1852 und 1880) zeigt unter Benutzung des auf Seite 45 meiner Abhandlung »Bestimmung des quadratischen Rest-Characters» Göttingen 1879, ausgesprochenen Lehrsatzes, dass alle diese Beweise auf die Betrachtung der Anzahl verschiedenartiger Lösungen linearer Congruenzen zurückgeführt werden können.

N. 24. Es ist bemerkenswerth, dass diejenigen Gleichungen, welche den obigen bilinearen Congruenzen (VII) entsprechen, schon von EULER mehrfach, wenn auch nur für den Fall einer Primzahl m, angewendet worden sind: Observationes circa divisionem quadratorum per numeros primos. §. 20. §. 30. Op. anal. I. 1772. — Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta §. 29. §. 50. Op. anal. Exhib. 1772. Maji 18. — Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia §. 25. N. comment. Petrop. XVIII. 1773 Exhib. 1772. Maj 18. — Diese Abhandlungen sind abgedruckt: EULERI commentationes arithmeticae collectae. Edit. FUSS. Petrop. 1849. Tom. I. pag. 480, 482, 494, 505, 519. — EULER nennt für den Fall $a = 1$ und $m = p$ in der Gleichung $\alpha\alpha' \equiv 1 + np$ die Zahlen α und α' residua sociata.

Göttingen 1882 November 9.