Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0039
LOG Titel: Dritter Abschnitt Von den quadratischen Besten.
LOG Typ: chapter

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Dritter Abschnitt.

Von den quadratischen Resten.

§. 32.

Wir behandeln im Folgenden ausführlich die Theorie der Congruenzen von der Form

$$x^2 \equiv D \pmod{k}, \qquad (1)$$

in welcher wir stets D als *relative Primzahl* gegen den Modul k voraussetzen. Es würde sich leicht zeigen lassen, dass jede beliebige Congruenz zweiten Grades auf diesen Fall zurückgeführt werden kann; doch wollen wir uns dabei nicht aufhalten. So oft nun die Congruenz (1) möglich ist, d. h. so oft sie Wurzeln hat, heisst die Zahl D *quadratischer Rest der Zahl* k; im entgegengesetzten Fall heisst D *quadratischer Nichtrest der Zahl* k. Man lässt auch häufig, wenn kein Missverständniss zu befürchten ist, das Beiwort „quadratisch" fort und nennt kurz die Zahl D *Rest* oder *Nichtrest* von k, je nachdem die Congruenz (1) möglich ist oder nicht. Unmittelbar leuchtet hieraus ein, dass zwei nach dem Modul k congruente Zahlen entweder beide Reste von k, oder beide Nichtreste von k sind; d. h. alle in einer und derselben *Classe* enthaltenen Zahlen haben denselben Charakter; je nachdem eine von ihnen Rest oder Nichtrest des Modul k ist, sind sie alle Reste oder alle Nichtreste von k.

Die Theorie der quadratischen Reste zerfällt nun in zwei Haupttheile; man kann nämlich einmal die Frage aufwerfen:

Wenn der Modul k gegeben ist, welches sind dann die sämmtlichen incongruenten quadratischen Reste von k? und wie viele Wurzeln hat die einer jeden dieser Zahlen entsprechende Congruenz?

Bei weitem schwieriger ist aber die Beantwortung der folgenden zweiten Hauptfrage:

Wenn die Zahl D gegeben ist, welches sind dann die Moduln k, für welche die Congruenz (1) *möglich ist, d. h. welches sind die Zahlen k, von denen die gegebene Zahl D quadratischer Rest ist?*

§. 33.

Wir beschäftigen uns zuerst mit der ersten Frage und beginnen die Untersuchung mit dem einfachsten Falle, mit dem nämlich, wo der Modul eine *ungerade Primzahl p* ist (der Fall $p = 2$ erledigt sich unmittelbar durch die Bemerkung, dass jede ungerade Zahl $\equiv 1^2$, also quadratischer Rest von 2 ist). Hier erhalten wir die vollständige Antwort sogleich durch die vorhergehende Theorie der binomischen Congruenzen (§. 31). In unserm Falle ist nämlich $n = 2$ der Grad der binomischen Congruenz, und da $p - 1$ gerade ist, so ist $\delta = 2$ der grösste gemeinschaftliche Divisor von n und $p - 1$; die Congruenz

$$x^2 \equiv D \pmod{p}$$

ist daher stets und nur dann möglich, wenn

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

und zwar hat sie jedesmal zwei incongruente Wurzeln; es giebt $\frac{1}{2}(p-1)$ quadratische Reste, und folglich, da die Anzahl aller incongruenten und durch p nicht theilbaren Zahlen gleich $p - 1$ ist, auch $\frac{1}{2}(p-1)$ Nichtreste von p. Da ferner nach dem Fermat'schen Satze

$$D^{p-1} - 1 = (D^{\frac{p-1}{2}} - 1)(D^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

ist, so folgt, dass

$$D^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

sein muss, so oft D ein Nichtrest von p ist. Je nachdem also

$D^{\frac{p-1}{2}} \equiv +1$ oder $\equiv -1$ ist, ist D ein Rest oder Nichtrest von p. Nennt man die Eigenschaft einer Zahl D, Rest oder Nichtrest von p zu sein, ihren *Charakter*, so ist derselbe also durch dieses Kriterium vollständig bestimmt*).

Es lässt sich indessen auch ganz elementar beweisen, dass die Anzahl sowohl der Reste als auch der Nichtreste $= \frac{1}{2}(p-1)$ ist. Quadrirt man nämlich die $\frac{1}{2}(p-1)$ Zahlen

$$1,\ 2,\ 3, \ldots \frac{p-1}{2},$$

so sind die Quadrate sämmtlich incongruent; denn sind r und s zwei verschiedene dieser Zahlen, so ist die Differenz ihrer Quadrate

$$r^2 - s^2 = (r+s)\,(r-s)$$

nicht theilbar durch p, da die Factoren $r+s$ und $r-s$ kleiner als p sind. Diese $\frac{1}{2}(p-1)$ Quadrate geben also wirklich $\frac{1}{2}(p-1)$ incongruente quadratische Reste; dagegen liefern die Quadrate der folgenden Zahlen

$$\frac{p+1}{2},\ \frac{p+3}{2} \cdots (p-1)$$

dieselben Reste wieder; denn es ist allgemein

$$(p-r)^2 = p^2 - 2rp + r^2 \equiv r^2 \pmod{p}.$$

Also ist $\frac{1}{2}(p-1)$ die Anzahl aller quadratischen Reste, und folglich auch die der quadratischen Nichtreste.

Da ein Product aus mehreren Factoren, die nicht durch p theilbar sind, dieselbe Eigenschaft hat, so kann man nach dem Charakter des Productes fragen, wenn die Charaktere der Factoren gegeben sind. Beschränken wir uns zunächst auf zwei Factoren, so sind folgende drei Fälle zu unterscheiden.

I. Das Product aus zwei Resten ist wieder ein Rest; denn sind a und a' Reste, so giebt es Zahlen x, x' von der Beschaffenheit, dass $a \equiv x^2 \pmod{p}$, $a' \equiv x'^2 \pmod{p}$; hieraus folgt aber $aa' \equiv (xx')^2 \pmod{p}$, d. h. aa' ist Rest von p.

II. Das Product aus einem Rest und einem Nichtrest ist ein Nichtrest. Denn wenn wir ein vollständiges System incongruenter

*) Dies Kriterium rührt wesentlich von *Euler* her; man vergl. z. B. die Abhandlung *Theoremata circa residua ex divisione potestatum relicta*, Nov. Comm. Petrop. VII, p. 49; aber es ist mir nicht geglückt, in seinen zahlreichen Arbeiten über diesen Gegenstand eine Stelle aufzufinden, wo dasselbe in voller Schärfe ausgesprochen wäre.

und durch p nicht theilbarer Zahlen bilden, so zerfällt dasselbe in zwei Gruppen, deren eine $\frac{1}{2}(p-1)$ Reste — wir wollen sie allgemein mit α bezeichnen — und deren zweite $\frac{1}{2}(p-1)$ Nichtreste β enthält. Multiplicirt man nun alle diese Zahlen α und β mit einem Reste a, so bilden die Producte $a\alpha$ und $a\beta$ wieder ein vollständiges System incongruenter (durch p nicht theilbarer) Zahlen, welches also wieder $\frac{1}{2}(p-1)$ Reste und $\frac{1}{2}(p-1)$ Nichtreste enthält. In der That sind nun (nach I.) die Producte $a\alpha$ sämmtlich wieder Reste; es müssen daher die anderen $\frac{1}{2}(p-1)$ Producte $a\beta$ sämmtlich Nichtreste sein; also ist das Product aus jedem Rest a und jedem Nichtrest β ein Nichtrest.

III. Das Product aus zwei Nichtresten ist ein Rest. Denn bildet man wieder das System der Reste α und Nichtreste β, und multiplicirt dieselben mit einem Nichtreste b, so sind die Producte $b\alpha$ (nach II.) sämmtlich Nichtreste; folglich müssen die übrigen $\frac{1}{2}(p-1)$ Producte $b\beta$ sämmtlich Reste sein.

Man kann diese wichtigen Sätze offenbar in den folgenden einen zusammenfassen:

Ein Product aus beliebig vielen durch die Primzahl p nicht theilbaren Zahlen ist Rest oder Nichtrest von p, je nachdem die Anzahl der Nichtreste, welche sich unter den Factoren finden, gerade oder ungerade ist.

Dieser Satz ergiebt sich auch unmittelbar aus dem oben aufgestellten Kriterium für den Charakter einer Zahl; denn da

$$(abc\ldots)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}}\, c^{\frac{p-1}{2}} \ldots$$

ist, so wird

$$(abc\ldots)^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

sein, je nachdem die Anzahl der Factoren $a^{\frac{p-1}{2}}$, $b^{\frac{p-1}{2}}$, $c^{\frac{p-1}{2}}\ldots$, welche $\equiv -1$ sind, eine gerade oder ungerade ist.

Man kann diesen Satz in Form einer Gleichung ausdrücken, wenn man sich eines von *Legendre**) in die Zahlentheorie eingeführten Zeichens bedient, welches in allen folgenden Untersuchungen eine grosse Rolle spielt. *Legendre* bezeichnet nämlich durch das Symbol

$$\left(\frac{m}{p}\right)$$

*) *Théorie des Nombres*, 3me éd. Tom. I. p. 197.

die positive oder negative Einheit, je nachdem die durch die Primzahl p nicht theilbare Zahl m quadratischer Rest oder Nichtrest von p ist; es ist daher stets

$$\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = +1 \quad \text{und} \quad m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}.$$

Den Satz über den Charakter eines Productes kann man dann offenbar durch die folgende Gleichung ausdrücken:

$$\left(\frac{mnl\ldots}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\left(\frac{l}{p}\right)\cdots$$

Es leuchtet ferner ein, dass, sobald $m \equiv n \pmod{p}$, auch

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$$

sein wird.

§. 34.

Es ist nun interessant zu sehen, dass die soeben gewonnenen Sätze, welche zum Theil als Resultate einer ausgedehnten Theorie, wie der der binomischen Congruenzen, erscheinen, sich aus den ersten Principien auf einem ganz elementaren Wege ableiten lassen, der zugleich einen neuen Beweis des Wilson'schen und Fermat'schen Satzes liefern wird.

Es sei D irgend eine durch die (ungerade) Primzahl p nicht theilbare Zahl, und r irgend eine der Zahlen

$$1, 2, 3 \ldots (p-1); \tag{1}$$

dann existirt in derselben Reihe stets eine und nur eine Zahl s von der Beschaffenheit, dass

$$rs \equiv D \pmod{p}$$

ist; denn diese Zahl s ist ja die Wurzel der Congruenz ersten Grades $rx \equiv D \pmod{p}$; je zwei solche Zahlen r und s der Reihe (1), deren Product $\equiv D$ ist, wollen wir *zusammengehörige* Zahlen nennen; offenbar ist durch eine dieser beiden Zahlen die andere ebenfalls bestimmt. Identisch können diese beiden Zahlen nur dann werden, wenn die Congruenz

$$x^2 \equiv D \pmod{p} \tag{2}$$

möglich ist. Danach theilen wir unsere Untersuchung in zwei Fälle ein.

Erstens: Die Congruenz (2) ist unmöglich. — Dann sind also je zwei zusammengehörige Zahlen von einander verschieden, und da zwei solche Paare stets identisch sind, sobald sie nur eine gemeinschaftliche Zahl haben, so zerfallen die sämmtlichen $p-1$ Zahlen (1) in $\frac{1}{2}(p-1)$ solche Paare zusammengehöriger Zahlen, und folglich ist ihr Product

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv D^{\frac{p-1}{2}} \pmod{p}. \qquad (3)$$

Zweitens: Die Congruenz (2) ist möglich. — Dann existirt also auch in der Reihe (1) mindestens eine Zahl ϱ von der Beschaffenheit, dass $\varrho^2 \equiv D$; sehen wir zu, ob ausser ϱ in der Reihe (1) noch eine solche Zahl σ existirt; dann muss $\sigma^2 \equiv \varrho^2$, folglich $(\sigma-\varrho)(\sigma+\varrho)$ durch p theilbar sein; da wir σ verschieden von ϱ voraussetzen, so ist $\sigma-\varrho$ nicht theilbar durch p, folglich muss $\sigma+\varrho$ theilbar durch p, also $\sigma = p-\varrho$ sein; und in der That ist wirklich $(p-\varrho)^2 \equiv D$. Trennen wir nun diese beiden (wirklich ungleichen) Zahlen ϱ und $\sigma = p-\varrho$, deren Product $\varrho\sigma \equiv -\varrho^2 \equiv -D$ ist, von den übrigen der Reihe (1), so zerfallen die letztern in $\frac{1}{2}(p-3)$ Paare zusammengehöriger Zahlen von der Beschaffenheit, dass jedes Paar aus zwei verschiedenen Zahlen besteht. Demnach ist in diesem Fall das Product aller Zahlen der Reihe (1):

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -D^{\frac{p-1}{2}} \pmod{p}. \qquad (4)$$

Nun giebt es aber einen Fall, in welchem die Congruenz (2) stets möglich ist, nämlich den, in welchem $D = 1 = 1^2$; wir erhalten daher zunächst aus (4) den Satz von *Wilson:*

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -1 \pmod{p}, \qquad (5)$$

und substituiren wir dies in die Congruenzen (3) und (4), so erhalten wir das Resultat, dass

$$D^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

ist, je nachdem die Congruenz (2) möglich oder nicht möglich ist. Da endlich ein dritter Fall nicht existiren kann, so erhalten wir allgemein

$$D^{p-1} = (D^{\frac{p-1}{2}})^2 \equiv (\pm 1)^2 \equiv +1 \pmod{p},$$

also den Satz von *Fermat.*

Durch diese einfache Betrachtung sind wir also sogleich bis zu denselben Sätzen in der Theorie der quadratischen Reste ge-

langt, welche vorher aus der allgemeinen Theorie der binomischen Congruenzen abgeleitet waren.

§. 35.

Wir wenden uns jetzt zu der Untersuchung des Falls, in welchem der Modul k der quadratischen Congruenz

$$x^2 \equiv D \pmod{k}$$

die Potenz einer Primzahl p ist; dabei müssen wir den Fall, in welchem $p = 2$, gesondert von den übrigen behandeln, in welchen p eine ungerade Primzahl ist*).

Ist zunächst p eine ungerade Primzahl, und $k = p^\pi$, wo π irgend eine positive ganze Zahl bedeutet, und nehmen wir an, die Congruenz

$$x^2 \equiv D \pmod{p^\pi} \qquad (1)$$

sei möglich, so überzeugt man sich leicht, dass sie im Ganzen zwei incongruente Wurzeln hat; denn ist α eine bestimmte, und x irgend eine Wurzel, so muss

$$x^2 - \alpha^2 = (x-\alpha)\ (x+\alpha) \equiv 0 \pmod{p^\pi}$$

sein; von den beiden Factoren $x-\alpha$ und $x+\alpha$ ist aber nur einer durch p theilbar; denn wären beide durch p theilbar, so wäre auch ihre Differenz 2α, und folglich auch α durch p theilbar, was nicht der Fall ist, da wir $D \equiv \alpha^2$ als nicht theilbar durch p vorausgesetzt haben. Da also einer der beiden Factoren relative Primzahl gegen p^π ist, so muss der andere für sich allein durch p^π theilbar sein. Es ist daher entweder

$$x \equiv \alpha \pmod{p^\pi}, \quad \text{oder} \quad x \equiv -\alpha \pmod{p^\pi};$$

also hat die Congruenz (1) entweder gar keine Wurzel, oder sie hat zwei incongruente Wurzeln α und $-\alpha$.

Es ist nun noch zu entscheiden, wann das Eine, wann das Andere Statt finden wird. Da nun jede Wurzel α der Congruenz (1) auch eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p} \qquad (2)$$

ist, so leuchtet ein, dass die Congruenz (1) nur dann möglich ist, wenn D quadratischer Rest von p ist; es fragt sich daher nur, ob

*) Die nachfolgenden Resultate lassen sich auch aus dem in §. 145 bewiesenen Satze ableiten.

auch umgekehrt, wenn D quadratischer Rest von p ist, hieraus die Möglichkeit der Congruenz (1) folgt. Um dies zu zeigen, brauchen wir nur nachzuweisen, dass, sobald die Congruenz (2) eine Wurzel α besitzt (also D quadratischer Rest von p ist), hieraus sich eine Wurzel der Congruenz (1) ableiten lässt, welche $\equiv \alpha \pmod{p}$ ist; und da Aehnliches von jeder Congruenz $x^2 \equiv D \pmod{k}$ gilt, wo D stets dieselbe Zahl, k aber irgend eine Potenz der Primzahl p ist, so braucht man nur zu zeigen, dass aus einer Wurzel α der Congruenz (1) sich eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p^{\pi+1}} \tag{3}$$

ableiten lässt, welche $\equiv \alpha \pmod{p^\pi}$ ist. Es sei daher

$$\alpha^2 \equiv D \pmod{p^\pi} \quad \text{oder} \quad \alpha^2 - D = hp^\pi,$$

so setzen wir

$$x = \alpha + p^\pi y,$$

woraus

$$x^2 - D = hp^\pi + 2\alpha p^\pi y + p^{2\pi} y^2 \equiv p^\pi (h + 2\alpha y) \pmod{p^{\pi+1}}$$

folgt; damit nun $x^2 \equiv D \pmod{p^{\pi+1}}$ werde, braucht y nur so bestimmt zu werden, dass

$$2\alpha y \equiv -h \pmod{p}$$

werde; da nun D, folglich auch α und also, da p ungerade ist, auch 2α eine durch p nicht theilbare Zahl ist, so lässt sich y stets so wählen, dass es dieser Congruenz ersten Grades genügt. Wir sehen also, dass aus der Möglichkeit der Congruenz (1) auch stets die Möglichkeit der Congruenz (3) folgt; durch dieselbe wiederholt angewendete Schlussweise ergiebt sich also auch, dass aus der Möglichkeit der Congruenz (2) stets die der Congruenz (1) folgt, und wir haben auch eine Methode gefunden, um aus einer Wurzel der Congruenz $x^2 \equiv D$ für den Modul p successive eine Wurzel derselben Congruenz für die Moduln p^2, $p^3 \ldots p^\pi$ zu gewinnen. Wir haben mithin folgendes Resultat:

Ist p eine ungerade Primzahl, und D eine durch p nicht theilbare Zahl, so ist für die Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{p^\pi}$$

erforderlich und hinreichend, dass

$$\left(\frac{D}{p}\right) = 1,$$

d. h. dass D quadratischer Rest von p sei; sobald diese Bedingung erfüllt ist, besitzt die vorgelegte Congruenz zwei incongruente Wur-

zeln α und $-\alpha$, welche gefunden werden können, sobald man eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p}$$

gefunden hat.

§. 36.

Wir gehen nun zu dem besondern Fall über, in welchem der Modul k eine Potenz der Primzahl 2 ist, so dass also D irgend eine ungerade Zahl bedeutet. Betrachten wir zunächst die Congruenz

$$x^2 \equiv D \pmod{4},$$

so erkennt man leicht, dass dieselbe stets und nur dann möglich ist, wenn

$$D \equiv 1 \pmod{4}$$

ist. Denn ist die Congruenz möglich, so ist x jedenfalls ungerade, und das Quadrat von $x = 2n+1$ ist $4n^2+4n+1 \equiv 1 \pmod{4}$; umgekehrt, ist $D \equiv 1 \pmod{4}$, so hat die Congruenz offenbar die beiden incongruenten Wurzeln $x \equiv 1$ und $x \equiv -1 \pmod{4}$.

Gehen wir nun zu der Congruenz

$$x^2 \equiv D \pmod{8}$$

über, so leuchtet ein, da das Quadrat einer jeden ungeraden Zahl $4n \pm 1$ gleich $16n^2 \pm 8n + 1 \equiv 1 \pmod{8}$ ist, dass diese Congruenz nur dann möglich ist, wenn

$$D \equiv 1 \pmod{8}$$

ist; und umgekehrt, sobald diese Bedingung erfüllt ist, hat die Congruenz die vier incongruenten Wurzeln $x \equiv 1$, $x \equiv 3$, $x \equiv 5$, $x \equiv 7$.

Betrachten wir jetzt die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo $\pi \geqq 3$ ist, so kann diese Congruenz nur dann möglich sein, wenn die Congruenz

$$x^2 \equiv D \pmod{8}$$

möglich ist; es ist daher erforderlich, dass

$$D \equiv 1 \pmod{8}$$

sei. Wir wollen nun umgekehrt zeigen, dass diese Bedingung

auch hinreicht, und dass dann die Congruenz stets 4 incongruente Wurzeln hat. Nehmen wir nämlich an, dies sei für den Modul 2^π schon bewiesen, so können wir zeigen, dass dasselbe auch für den Modul $2^{\pi+1}$ gilt. Es sei nämlich α eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{2^\pi}$$

also

$$\alpha^2 - D = h \cdot 2^\pi,$$

so setzen wir

$$x = \alpha + 2^{\pi-1} \cdot y;$$

dann wird

$$x^2 - D = h \cdot 2^\pi + 2^\pi \cdot \alpha y + 2^{2\pi-2} y^2.$$

Da nun $\pi \geqq 3$, so ist $2\pi - 2 \geqq \pi + 1$, folglich

$$x^2 - D \equiv 2^\pi (h + \alpha y) \pmod{2^{\pi+1}}.$$

Damit also $x^2 - D$ durch $2^{\pi+1}$ theilbar werde, braucht man nur y so zu wählen, dass

$$\alpha y \equiv -h \pmod{2}$$

werde. Dies ist aber stets möglich, da α eine ungerade Zahl ist; also folgt aus der Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo $\pi \geqq 3$ ist, stets die Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^{\pi+1}}.$$

Wir schliessen hieraus zunächst das folgende Resultat:

Damit die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

in welcher $\pi \geqq 3$ ist, Wurzeln habe, ist erforderlich und hinreichend, dass

$$D \equiv 1 \pmod{8}$$

sei.

Ist nun α eine Wurzel dieser Congruenz — und eine solche kann immer nach der obigen Methode gefunden werden —, so muss, wenn x irgend eine Wurzel derselben Congruenz bezeichnet,

$$x^2 - \alpha^2 = (x - \alpha)(x + \alpha) \equiv 0 \pmod{2^\pi}$$

sein. Da ferner α sowohl wie x ungerade Zahlen sein müssen, so sind die beiden Factoren $x - \alpha$ und $x + \alpha$ gerade Zahlen, und dann muss

$$\frac{x-\alpha}{2} \cdot \frac{x+\alpha}{2} \equiv 0 \pmod{2^{\pi-2}}$$

sein. Da nun die Differenz der beiden Factoren $\frac{1}{2}(x-\alpha)$ und $\frac{1}{2}(x+\alpha)$ eine ungerade Zahl ist, so muss einer von ihnen ungerade, und der andere folglich theilbar durch $2^{\pi-2}$ sein. Dies giebt folgende Fälle:

$$x \equiv \alpha \pmod{2^{\pi-1}} \quad \text{oder} \quad x \equiv -\alpha \pmod{2^{\pi-1}}$$

und diese liefern wieder folgende vier Fälle:

$$x \equiv \alpha \pmod{2^{\pi}}; \qquad x \equiv \alpha + 2^{\pi-1} \pmod{2^{\pi}};$$
$$x \equiv -\alpha \pmod{2^{\pi}}; \quad x \equiv -\alpha - 2^{\pi-1} \pmod{2^{\pi}}.$$

Und umgekehrt überzeugt man sich leicht, dass jede dieser vier in Bezug auf den Modul 2^{π} incongruenten Zahlen der Congruenz genügt.

Wir fassen die ganze Untersuchung in folgendem Satze zusammen:

Die Congruenz

$$x^2 \equiv D \pmod{2^{\pi}}$$

ist stets möglich, wenn $\pi = 1$, *und hat dann eine Wurzel; sie ist, wenn* $\pi = 2$, *stets und nur dann möglich, wenn* $D \equiv 1 \pmod{4}$ *und sie hat dann zwei Wurzeln; sie ist, wenn* $\pi \geqq 3$, *stets und nur dann möglich, wenn* $D \equiv 1 \pmod{8}$ *ist, und zwar hat sie dann vier Wurzeln.*

§. 37.

Es ist jetzt leicht, die Möglichkeit und die Anzahl der Wurzeln der Congruenz $x^2 \equiv D$ für einen beliebigen Modulus zu beurtheilen, der relative Primzahl zu D ist. Wir führen diese Untersuchung ganz allgemein in folgender Weise.

Es seien $a, b, c \ldots$ relative Primzahlen zu einander, und

$$f(x) \equiv 0 \pmod{abc \ldots} \tag{1}$$

eine beliebige zur Auflösung vorgelegte Congruenz, so lässt dieselbe sich stets auf die vollständige Auflösung der Congruenzen

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{a} \\ f(x) &\equiv 0 \pmod{b} \\ f(x) &\equiv 0 \pmod{c} \end{aligned}\right\} \tag{2}$$

u. s. w.

zurückführen. Zunächst leuchtet ein, dass jede Wurzel x der Congruenz (1) auch allen Congruenzen (2) genügen muss; es wird daher die Congruenz (1) unmöglich sein, wenn dies mit irgend einer der Congruenzen (2) der Fall ist. Umgekehrt, ist α irgend eine Wurzel der Congruenz $f(x) \equiv 0 \pmod{a}$, ebenso β irgend eine Wurzel der Congruenz $f(x) \equiv 0 \pmod{b}$, γ eine Wurzel der Congruenz $f(x) \equiv 0 \pmod{c}$ u. s. w., so bestimme man (nach §. 25) eine Zahl x durch das System von Congruenzen

$$\left.\begin{aligned} x &\equiv \alpha \pmod{a} \\ x &\equiv \beta \pmod{b} \\ x &\equiv \gamma \pmod{c} \end{aligned}\right\} \quad (3)$$

u. s. w.,

so wird

$$\begin{aligned} f(x) &\equiv f(\alpha) \equiv 0 \pmod{a} \\ f(x) &\equiv f(\beta) \equiv 0 \pmod{b} \\ f(x) &\equiv f(\gamma) \equiv 0 \pmod{c} \end{aligned}$$

u. s. w.

und folglich, da $a, b, c \ldots$ relative Primzahlen zu einander sind, auch

$$f(x) \equiv 0 \pmod{abc \ldots},$$

d. h. jede dem System (3) genügende Zahl x ist eine Wurzel der vorgelegten Congruenz (1). Da nun (nach §. 25) dem System (3) unendlich viele Zahlen x genügen, welche aber alle nach dem Modul $abc \ldots$ einander congruent sind, so liefert das System (3), eine und nur eine Wurzel x der Congruenz (1). Ist nun

λ die Anzahl aller incongruenten Wurzeln $\alpha \pmod{a}$
μ „ „ „ „ „ $\beta \pmod{b}$
ν „ „ „ „ „ $\gamma \pmod{c}$

u. s. w.

so kann man im Ganzen $\lambda\mu\nu \ldots$ verschiedene Systeme (3) bilden, welchen (nach §. 25) ebensoviele verschiedene Wurzeln x der Congruenz (1) entsprechen; und andere Wurzeln kann diese letztere nicht besitzen, weil, wie schon oben bemerkt ist, jede bestimmte Wurzel x der Congruenz (1) auch Wurzel aller Congruenzen (2) und folglich einem bestimmten $\alpha \pmod{a}$, einem bestimmten $\beta \pmod{b}$, einem bestimmten $\gamma \pmod{c}$ u. s. f. congruent sein muss. Mithin ist die Anzahl aller nach dem Modul $abc \ldots$ incongruenten Wurzeln der vorgelegten Congruenz $= \lambda\mu\nu \ldots$

Mit Hülfe dieses allgemeinen Resultates sind wir im Stande zu beurtheilen, ob die Congruenz

$$x^2 \equiv D \pmod{k},$$

in welcher D und k relative Primzahlen sind, möglich, und wie gross die Anzahl σ ihrer incongruenten Wurzeln ist. Bedeutet p jede beliebige in dem Modul k (also nicht in D) aufgehende ungerade Primzahl, so ist erforderlich, dass

$$\left(\frac{D}{p}\right) = +1$$

sei; ist diese Bedingung erfüllt, so hat die Congruenz $x^2 \equiv D$ in Bezug auf jeden Modulus von der Form p^π genau zwei incongruente Wurzeln. Ist daher der Modul k ungerade, und μ die Anzahl der von einander verschiedenen in k aufgehenden Primzahlen p, so ist

$$\sigma = 2^\mu.$$

Dasselbe ist der Fall, wenn der Modulus k das Doppelte einer ungeraden Zahl ist; denn die Congruenz $x^2 \equiv D \pmod 2$ hat stets eine und nur eine Wurzel.

Ist aber k das Vierfache einer ungeraden Zahl, so ist ausser den früheren μ Bedingungen noch erforderlich, dass $D \equiv 1 \pmod 4$ sei; da alsdann die Congruenz $x^2 \equiv D \pmod 4$ zwei Wurzeln besitzt, so ist

$$\sigma = 2^{\mu+1}.$$

Ist endlich $k \equiv 0 \pmod 8$, so ist ausser den früheren μ Bedingungen noch erforderlich, dass $D \equiv 1 \pmod 8$ sei; da dann die Congruenz $x^2 \equiv D \pmod{2^\pi}$, wo $\pi \geqq 3$, stets vier Wurzeln hat, so ist in diesem Fall

$$\sigma = 2^{\mu+2}.$$

§. 38.

Bevor wir diesen Gegenstand verlassen, wollen wir noch eine Anwendung von dem soeben gewonnenen Resultate auf eine Verallgemeinerung des Wilson'schen Satzes (§. 27) machen. Setzen wir $D = 1$, so ergiebt sich, dass die Congruenz

$$x^2 \equiv 1 \pmod{k} \qquad (1)$$

für jeden Modul k möglich ist; die Anzahl σ ihrer Wurzeln ist $= 1$, wenn $k = 1$ oder $k = 2$; sie ist $= 2$, wenn k eine Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder $= 4$ ist; in allen übrigen Fällen ist σ durch 4 theilbar. Schliessen wir die Fälle $k = 1$ und $k = 2$ aus, so zerfallen die σ Wurzeln in $\frac{1}{2}\sigma$ Paare von Wurzeln ϱ und $-\varrho$; denn mit ϱ ist gleichzeitig auch $-\varrho$ eine Wurzel, und da ϱ relative Primzahl zu k, und folglich 2ϱ nicht $\equiv 0 \pmod{k}$ sein kann, so sind je zwei solche Wurzeln ϱ und $-\varrho$ auch incongruent. Das Product $\varrho \times (-\varrho) = -\varrho^2$ zweier solcher Wurzeln ist $\equiv -1$, und folglich ist das Product aller σ Wurzeln $\equiv +1$ oder -1, je nachdem σ durch 4 theilbar ist oder nicht.

Unter den $\varphi(k)$ Zahlen z, welche nicht grösser als k und relative Primzahlen zu k sind, finden sich zunächst die σ Wurzeln der Congruenz (1); die übrigen $\varphi(k) - \sigma$ dieser Zahlen z (wenn noch solche vorhanden sind) lassen sich in Paare von je zwei solchen Zahlen r und s zerlegen, deren Product $rs \equiv 1$ ist; denn zu jeder Zahl r gehört (nach §. 22) eine solche Zahl s und nur eine, und ausserdem kann s nicht $\equiv r$ sein, weil sonst $r^2 \equiv 1$, und folglich r eine der σ Wurzeln der Congruenz (1) wäre. Mithin ist auch das Product aller dieser $\varphi(k) - \sigma$ Zahlen $\equiv 1$.

Multiplicirt man daher alle $\varphi(k)$ Zahlen z mit einander, so wird das Product $\equiv -1$, wenn k Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder $= 4$ ist, in allen übrigen Fällen aber $\equiv +1$. (In den beiden ausgeschlossenen Fällen $k = 1$ und $k = 2$ ist $\varphi(k) = 1$, und die einzige Zahl $z \equiv \pm 1$.) Dies ist der verallgemeinerte Wilson'sche Satz*).

§. 39.

Nachdem in den vorhergehenden Paragraphen die erste der beiden in §. 32 aufgeworfenen Fragen ihre vollständige Beantwortung gefunden hat, wenden wir uns jetzt zu der zweiten ungleich interessanteren, aber auch schwierigern Aufgabe:

Alle Moduln k zu finden, von welchen eine gegebene Zahl D quadratischer Rest ist.

*) *Gauss: D. A.* art. 78.

Bevor wir zu der Lösung derselben übergehen, wollen wir erwähnen, dass man häufig, namentlich in den älteren Schriften, eine andere Ausdrucksweise vorfindet. Die Moduln k, für welche eine Congruenz $f(x) \equiv 0 \pmod{k}$ möglich ist, nennt man auch *Divisoren der Form* $f(x)$, weil es Zahlen x giebt, für welche die *Form* $f(x)$ durch einen solchen Modul k theilbar wird; die von uns gesuchten Zahlen k sind daher die Divisoren der Form $x^2 - D$; sie stimmen vollständig überein mit den Divisoren der *Form* $t^2 - Du^2$, in welcher t, u zwei unbestimmte ganze Zahlen bedeuten, die aber immer relative Primzahlen zu einander sein müssen. Dass wirklich jeder Divisor der Form $x^2 - D$ auch ein Divisor der Form $t^2 - Du^2$ ist, leuchtet unmittelbar ein, da die letztere in die erstere übergeht, wenn man $t = x$, $u = 1$ setzt. Umgekehrt, ist k Divisor der Form $t^2 - Du^2$, so ist u jedenfalls relative Primzahl zu k (denn ginge irgend eine Primzahl gleichzeitig in k und u auf, so müsste sie auch in t^2 und folglich auch in t aufgehen, gegen die Voraussetzung, dass t, u relative Primzahlen sind), und man kann folglich eine Zahl x finden, welche der Congruenz $ux \equiv t \pmod{k}$ genügt; da nun $t^2 - Du^2 \equiv 0 \pmod{k}$, so ist auch $u^2(x^2 - D) \equiv 0 \pmod{k}$ und folglich, da u^2 relative Primzahl zu k ist, auch $x^2 - D \equiv 0 \pmod{k}$, d. h. jeder Divisor k der Form $t^2 - Du^2$, in welcher t und u relative Primzahlen zu einander sind, ist auch Divisor der Form $x^2 - D$.

Das allgemeine Problem wird daher häufig auch so ausgedrückt: es sollen alle Divisoren der Form $t^2 - Du^2$ gefunden werden, in welcher D eine gegebene, t und u dagegen zwei unbestimmte ganze Zahlen bedeuten, die relative Primzahlen zu einander sind.

Wir beschränken uns auch hier auf solche (immer mit *positivem* Vorzeichen genommene) Moduln k, die relative Primzahlen zu D sind; da ferner nach den vorhergehenden Untersuchungen die Möglichkeit der Congruenz $x^2 \equiv D \pmod{k}$ nur von der Beschaffenheit der in k aufgehenden Primzahlen abhängt und für einen Modul von der Form 2^n immer leicht beurtheilt werden kann, so kommt es nur darauf an, alle ungeraden (in D nicht aufgehenden) Primzahlen p zu finden, von welchen D quadratischer Rest ist. Bedenken wir ferner, dass (nach §. 33) der quadratische Charakter einer Zahl D in Bezug auf einen solchen Modulus p nur von den in D enthaltenen Factoren abhängt, so werden wir in letzter Instanz auf folgendes Problem geführt:

Alle ungeraden Primzahlen p zu finden, für welche irgend eine der drei Congruenzen

$$x^2 \equiv -1, \quad x^2 \equiv 2, \quad x^2 \equiv q \pmod{p}$$

möglich ist, wo q irgend eine gegebene positive ungerade Primzahl bedeutet.

§. 40.

Die Auffindung aller ungeraden Primzahlen p, für welche die Congruenz

$$x^2 \equiv -1 \pmod{p}$$

möglich ist, bietet keine Schwierigkeit mehr dar. Denn da (nach §. 33) allgemein

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \pmod{p}$$

ist, so erhält man speciell

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und folglich auch

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

In Worten lautet dieser wichtige Satz*) folgendermaassen:

Die Zahl -1 ist quadratischer Rest aller Primzahlen von der Form $4n+1$, dagegen quadratischer Nichtrest aller Primzahlen von der Form $4n+3$.

Dasselbe Resultat erhält man auch auf folgendem Wege. Ist die Congruenz $x^2 \equiv -1 \pmod{p}$ möglich, und x eine Wurzel derselben, so folgt hieraus durch Potenzirung

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und hieraus (nach dem Fermat'schen Satze §. 19) $(-1)^{\frac{p-1}{2}} = 1$ also $p = 4n+1$; d. h. die Zahl -1 ist quadratischer Nichtrest von allen Primzahlen von der Form $4n+3$. Ist umgekehrt p von der Form $4n+1$, so ist $x^{p-1}-1$ algebraisch theilbar durch x^4-1, also auch durch x^2+1; es ist folglich

$$x^{p-1} - 1 = (x^2+1)\,\psi(x),$$

*) *Euler: Demonstratio theorematis Fermatiani, omnem numerum primum formae $4n+1$ esse summam duorum quadratorum*, Nov. Comm. Petrop. V, p. 3.

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet; da nun (nach dem Fermat'schen Satze §. 19) die linke Seite dieser Gleichung für $p-1$ incongruente Werthe von x congruent Null wird, so wird (nach §. 26) auch x^2+1 für zwei incongruente Werthe von x congruent Null*), d. h. die Zahl -1 ist quadratischer Rest von allen Primzahlen von der Form $4n+1$. Der Satz ist also von Neuem bewiesen.

§. 41.

Wir gehen nun zu der Lösung der zweiten Aufgabe über, welche sich auf die Congruenz

$$x^2 \equiv 2 \pmod{p}$$

bezieht. *Fermat* hat, wahrscheinlich durch Induction, folgendes, zuerst von *Lagrange***) bewiesenes, Resultat gefunden:

Die Zahl 2 *ist quadratischer Rest aller Primzahlen von einer der beiden Formen* $8n+1$ *oder* $8n+7$, *dagegen Nichtrest aller Primzahlen von einer der beiden Formen* $8n+3$ *oder* $8n+5$.

Wir beweisen zuerst den zweiten Theil des Satzes, dass nämlich 2 Nichtrest aller Primzahlen p von der Form $8n\pm3$ ist. Offenbar ist derselbe für $p=3$ richtig, denn nur die Zahl 1 ist Rest von 3. Gesetzt nun, der Satz wäre nicht allgemein gültig, so müsste es doch eine *kleinste* Primzahl p von der Form $8n\pm3$ geben, für welche er unrichtig würde, für welche also die Congruenz

$$x^2 \equiv 2 \pmod{p}$$

möglich würde. Hierin kann man immer die Wurzel x kleiner als p und ungerade voraussetzen, denn wenn x gerade ist, so ist die andere Wurzel $x'=p-x$ ungerade. Wir können daher

$$x^2-2=pf$$

setzen, wo f positiv und kleiner als p ist; da ferner x^2 von der Form $8n+1$, also pf von der Form $8n-1$, und folglich f von der Form $8n\mp3$ ist, so hat die Zahl f mindestens einen Primfactor p' von einer der Formen $8n+3$ oder $8n-3$; denn ein Product aus lauter Factoren von der Form $8n\pm1$ würde wieder

*) Man findet auch leicht mit Hülfe des Wilson'schen Satzes (§. 27), dass diese Wurzeln $\equiv \pm 1.2.3\ldots\frac{1}{2}(p-1)$ sind.

**) *Recherches d'Arithmétique*, Nouv. Mém. de l'Acad. de Berlin. 1775. p. 349, 351.

dieselbe Form $8n \pm 1$ haben. Für diese Primzahl p', die jedenfalls $< p$ ist, würde dann ebenfalls $x^2 \equiv 2 \pmod{p'}$ sein; allein dies streitet mit unserer Voraussetzung, dass p die kleinste in der Form $8n \pm 3$ enthaltene Primzahl ist, von welcher die Zahl 2 quadratischer Rest ist. Mithin ist diese Voraussetzung überhaupt unzulässig, und es folgt, dass stets

$$\left(\frac{2}{p}\right) = -1 \text{ ist, wenn } p = 8n \pm 3.$$

Wir wollen jetzt zweitens beweisen, dass die Zahl 2 quadratischer Rest aller Primzahlen p von der Form $8n + 7$ ist; da nun (nach §. 40) -1 quadratischer Nichtrest aller dieser Primzahlen ist, so haben wir nur zu zeigen, dass die Zahl -2 ebenfalls Nichtrest aller dieser Primzahlen ist; statt dessen stellen wir uns die allgemeinere Aufgabe zu beweisen, dass -2 Nichtrest von allen in den beiden Formen $8n + 5$, $8n + 7$ enthaltenen Primzahlen ist, obgleich dies für die Primzahlen der Form $8n + 5$, von welchen (nach §. 40) -1 quadratischer Rest ist, schon im Vorhergehenden geschehen ist. Zunächst bemerken wir wieder, dass der Satz für die kleinste in einer dieser Formen enthaltene Primzahl 5 in der That richtig ist. Wenn nun der Satz nicht allgemein gültig ist, so sei p die kleinste ihm nicht gehorchende Primzahl, so dass also eine Zahl x existirt, für welche

$$x^2 + 2 \equiv 0 \pmod{p}$$

ist; auch hier können wir wieder annehmen, dass x kleiner als p und ungerade ist, so dass, wenn wir

$$x^2 + 2 = pf$$

setzen, die Zahl f positiv, ungerade und kleiner als p ausfällt. Da ferner $x^2 + 2 \equiv 3 \pmod{8}$ und $p \equiv 5$ oder $\equiv 7 \pmod{8}$ ist, so muss f entsprechend $\equiv 7$ oder $\equiv 5 \pmod{8}$ sein; und da ein Product aus lauter Factoren von den Formen $8n + 1$, oder $8n + 3$ stets wieder eine dieser Formen, niemals eine der Formen $8n + 5$ oder $8n + 7$ hat, so muss die Zahl f mindestens einen Primfactor p' von einer der Formen $8n + 7$, $8n + 5$ haben, für welchen der Satz ebenfalls unrichtig ist, da $x^2 + 2 \equiv 0 \pmod{p'}$ ist; allein, da $p' < p$, so streitet dies mit der Annahme, dass p die kleinste dem Satze nicht gehorchende Primzahl ist. Also ist die Annahme überhaupt nicht zulässig und folglich der Satz allgemeingültig, dass

$$\left(\frac{-2}{p}\right) = -1 \text{ für } p = 8n + 5 \text{ oder } = 8n + 7.$$

d. h. dass

$$\left(\frac{2}{p}\right) = -1 \text{ für } p = 8n+5$$

$$\left(\frac{2}{p}\right) = +1 \text{ für } p = 8n+7$$

ist.

Es bleibt jetzt nur noch zu beweisen übrig, dass 2 quadratischer Rest von allen Primzahlen p von der Form $8n+1$ ist; hierauf ist die vorhergehende Methode aus dem Grunde nicht anwendbar, weil die Annahme des Gegentheils sich nicht in Form einer Congruenz darstellen lässt, die dann zur Auffindung des Widerspruchs benutzt werden könnte. Allein in diesem Falle kann man direct, wie folgt, verfahren; da $p = 8n+1$ ist, so hat die Function $x^{p-1} - 1$ den Divisor $x^8 - 1$, also auch den Factor $x^4 + 1$, und hieraus folgt nach einem frühern Satze (§. 26), dass die Congruenz

$$x^4 + 1 \equiv 0 \pmod{p}$$

Wurzeln hat; ist nun x eine solche, so ist

$$x^4 + 1 = (x^2 \pm 1)^2 \mp 2x^2 \equiv 0 \pmod{p},$$

also

$$(x^2 \pm 1)^2 \equiv \pm 2x^2 \pmod{p};$$

es ist daher $\pm 2x^2$ und folglich auch ± 2 quadratischer Rest von p; in Zeichen

$$\left(\frac{\pm 2}{p}\right) = 1, \text{ wenn } p = 8n+1.$$

Hiermit ist der Satz in allen seinen Theilen bewiesen; wir können denselben in der einen Gleichung

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

zusammenfassen; denn je nachdem $p = 8n \pm 1$, oder $p = 8n \pm 3$ ist, wird $\frac{1}{8}(p^2 - 1)$ eine gerade oder ungerade Zahl.

§. 42.

Wir kommen nun zu der Untersuchung der dritten Frage: *von welchen ungeraden Primzahlen p ist die gegebene ungerade*

Primzahl q quadratischer Rest? Die vollständige Antwort hierauf wird durch einen der wichtigsten und interessantesten Sätze der Zahlentheorie gegeben, welcher seines eigenthümlichen Charakters wegen den Namen des *Reciprocitäts-Satzes* erhalten hat. Man kann ihn folgendermaassen aussprechen:

Sind p und q zwei positive ungerade Primzahlen, von denen mindestens eine die Form $4n+1$ hat, so ist q quadratischer Rest oder Nichtrest von p, je nachdem p quadratischer Rest oder Nichtrest von q ist; haben aber beide Primzahlen p und q die Form $4n+3$, so ist q quadratischer Rest oder Nichtrest von p, je nachdem p quadratischer Nichtrest oder quadratischer Rest von q ist.

Offenbar lässt sich dieser Satz durch die für beide Fälle gültige Gleichung

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ausdrücken; denn sobald mindestens eine der beiden Primzahlen p oder q die Form $4n+1$ hat, so ist die entsprechende der beiden Zahlen $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ eine gerade Zahl, so dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1, \text{ d. h. } \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

ist, worin der erste Fall seinen Ausdruck findet; sind dagegen beide Primzahlen p und q von der Form $4n+3$, so sind auch beide Zahlen $\frac{1}{2}(p-1)$ und $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ ungerade, so dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1, \text{ d. h. } \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

wird, worin der zweite Theil des Satzes ausgedrückt ist.

Ist z. B. $p=3$, $q=5$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Nichtrest von p, in Zeichen

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1.$$

Ist ferner $p=3$, $q=13$, so ist p quadratischer Rest von q und gleichzeitig q quadratischer Rest von p, in Zeichen

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = +1.$$

Ist dagegen $p=3$, $q=7$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Rest von p, in Zeichen

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

Dieser Satz wurde zuerst von *Legendre* durch Induction gefunden und ausgesprochen; allein erst *Gauss* hat denselben vollständig bewiesen, ja er hat nach einander sechs auf ganz verschiedenen Grundgedanken beruhende Beweise*) von diesem Satze gegeben, den er in etwas anderer Form aussprach und seiner Wichtigkeit wegen das *Theorema fundamentale* in der Theorie der quadratischen Reste nannte. Wir folgen hier zunächst dem *dritten* dieser sechs Beweise, der sich auf ein Lemma stützt, durch welches das Euler'sche Kriterium (§. 33) über den Charakter einer Zahl D in Bezug auf die Primzahl p in ein anderes umgeformt wird.

§. 43.

Wir haben früher (§. 33) gesehen, dass eine durch p nicht theilbare Zahl D quadratischer Rest oder Nichtrest von p ist, je nachdem

$$D^{\frac{p-1}{2}} \equiv +1 \text{ oder } \equiv -1 \pmod{p}$$

ist; betrachten wir nun die Producte

$$D,\quad 2D,\quad 3D \ldots \tfrac{1}{2}(p-1)D$$

aus dieser Zahl D und aus den ersten $\frac{1}{2}(p-1)$ ganzen positiven Zahlen, so werden die kleinsten positiven Reste

$$r_1,\quad r_2,\quad r_3 \ldots r_{\frac{p-1}{2}}$$

derselben, nach dem Modulus p genommen, erstens sämmtlich verschieden von einander und kleiner als p sein, und keiner von ihnen kann gleich Null sein. Wir theilen nun diese $\frac{1}{2}(p-1)$ Reste in zwei Abtheilungen, je nachdem sie grösser oder kleiner als $\frac{1}{2}p$ sind, und bezeichnen die erstern, deren Anzahl $= \mu$ sei, mit

$$\alpha_1,\quad \alpha_2 \ldots \alpha_\mu,$$

---

*) *D. A.* art. 125—145. — *D. A.* art. 262. — *Theorematis arithmetici demonstratio nova.* 1808. — *Summatio quarumdam serierum singularium.* 1808. — *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae.* 1817. — Vergl. §§. 48—51, 115.

die übrigen Reste, welche kleiner als $\frac{1}{2}p$ sind, und deren Anzahl $\lambda = \frac{1}{2}(p-1) - \mu$ ist, mit

$$\beta_1, \quad \beta_2 \ldots \beta_\lambda.$$

Nimmt man nun von den erstern μ Resten ihre Ergänzungen zur Zahl p, also die Zahlen

$$p-\alpha_1, \quad p-\alpha_2 \ldots p-\alpha_\mu,$$

so liegen dieselben, ebenso wie die λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$, auch zwischen den Grenzen 0 und $\frac{1}{2}p$; ausserdem sind sie alle von einander verschieden; endlich lässt sich aber auch zeigen, dass sie von den λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$ verschieden sind; denn wäre z. B. $p-\alpha = \beta$, also $\alpha+\beta = p \equiv 0 \pmod{p}$, so müsste auch, wenn α der Rest von sD, β der Rest von tD ist,

$$sD + tD = (s+t)D \equiv 0 \pmod{p}$$

und folglich $s+t$ durch p theilbar sein; allein da jede der beiden Zahlen s und t zwischen 0 und $\frac{1}{2}p$ liegt, so liegt $s+t$ zwischen 0 und p (mit Ausschluss dieser beiden Grenzen); es kann daher $s+t$ nicht theilbar durch p, und folglich auch nicht $p-\alpha = \beta$ sein.

Mithin haben die folgenden $\frac{1}{2}(p-1)$ Zahlen

$$p-\alpha_1, \quad p-\alpha_2 \ldots p-\alpha_\mu; \quad \beta_1, \quad \beta_2 \ldots \beta_\lambda$$

lauter von einander verschiedene Werthe, und da sie ihrem Werth nach zwischen 0 und $\frac{1}{2}p$ liegen, so müssen sie im Complex genommen identisch mit den $\frac{1}{2}(p-1)$ Zahlen

$$1, \quad 2, \quad 3 \ldots \tfrac{1}{2}(p-1)$$

sein, so dass ihr Product

$$(p-\alpha_1)(p-\alpha_2)\ldots(p-\alpha_\mu)\,\beta_1\beta_2\ldots\beta_\lambda = 1.2.3\cdots\tfrac{1}{2}(p-1)$$

ist. Werfen wir hieraus die Multipla von p weg, so erhalten wir die Congruenz

$$(-1)^\mu \alpha_1\alpha_2\ldots\alpha_\mu.\beta_1\beta_2\ldots\beta_\lambda \equiv 1.2.3\cdots\tfrac{1}{2}(p-1) \pmod{p};$$

da nun andererseits

$$\alpha_1\alpha_2\ldots\alpha_\mu.\beta_1\beta_2\ldots\beta_\lambda \equiv 1.2\cdots\tfrac{1}{2}(p-1)\,D^{\frac{p-1}{2}} \pmod{p}$$

ist, so folgt hieraus, dass

$$(-1)^\mu.1.2\cdots\tfrac{1}{2}(p-1).D^{\frac{p-1}{2}} \equiv 1.2.3\cdots\tfrac{1}{2}(p-1) \pmod{p}$$

und also auch

$$D^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}$$

oder, was dasselbe sagt, dass

$$\left(\frac{D}{p}\right) = (-1)^{\mu}$$

ist. Hierin besteht die Umformung des Kennzeichens, welches darüber entscheidet, ob eine Zahl D quadratischer Rest oder Nichtrest der ungeraden Primzahl p ist:

Man braucht nur nachzusehen, ob die Anzahl μ der kleinsten positiven Reste der Zahlen

$$D,\ 2D,\ 3D \ldots \tfrac{1}{2}(p-1)D,$$

die grösser als $\frac{1}{2}p$ ausfallen, gerade oder ungerade ist; je nachdem das Erstere oder Letztere eintritt, ist D quadratischer Rest oder quadratischer Nichtrest von p.

Mit Hülfe dieses Satzes ist man schon im Stande, für jedes wirklich gegebene D die Formen für die Primzahlen aufzustellen, von welchen D Rest oder Nichtrest ist. Um dies deutlicher zu zeigen, betrachten wir den allerdings schon früher (§. 41) vollständig durchgeführten Fall $D = 2$. Bilden wir die Zahlen

$$2,\ 4,\ 6 \ldots (p-1),$$

so ist jede derselben auch ihr eigener kleinster positiver Rest in Bezug auf den Modulus p, und die Anzahl μ derjenigen dieser Zahlen, welche $> \frac{1}{2}p$ sind, wird durch die Bedingungen

$$p-1-2\mu < \tfrac{1}{2}p < p+1-2\mu \quad \text{oder} \quad \frac{p-2}{4} < \mu < \frac{p+2}{4}$$

bestimmt; bezeichnen wir daher allgemein mit $[x]$ die grösste in der reellen Zahl x enthaltene *ganze* Zahl, so dass stets $0 \leqq x-[x] < 1$ ist, so erhalten wir

$$\mu = \left[\frac{p+2}{4}\right].$$

Je nachdem nun p von einer der Formen $8n+1$, $8n+3$, $8n+5$, $8n+7$ ist, wird $\mu = 2n,\ 2n+1,\ 2n+1,\ 2n+2$; es ist daher μ gerade und folglich

$$\left(\frac{2}{p}\right) = +1, \quad \text{wenn} \quad p \equiv \pm 1 \pmod{8};$$

und μ ist ungerade, also

$$\left(\frac{2}{p}\right) = -1, \quad \text{wenn} \quad p \equiv \pm 3 \pmod 8.$$

Auf diese Weise finden wir also eine vollständige Bestätigung des Resultats unserer frühern Untersuchung (§. 41), und ganz ebenso würde sich für jeden speciellen Werth von D die Untersuchung führen lassen, z. B. für die nächstliegenden Fälle $D = -1$, $D = 3$, $D = 5$ u. s. w.

§. 44.

Wir verlassen diese Anwendungen auf specielle Fälle und wenden uns zu einer weitern Umformung, bei welcher wir der spätern Bezeichnung wegen q statt D schreiben wollen. Bezeichnen wir wieder mit $[x]$ die grösste in dem Werth x enthaltene ganze Zahl, und setzen wir zur Abkürzung $p = 2p' + 1$, so können wir

$$q = p\left[\frac{q}{p}\right] + r_1$$

$$2q = p\left[\frac{2q}{p}\right] + r_2$$

$$\cdots\cdots\cdots\cdots$$

$$p'q = p\left[\frac{p'q}{p}\right] + r_{p'}$$

setzen, wo wie früher (§. 43)

$$r_1, \quad r_2 \ldots r_{p'}$$

zwischen den Grenzen 0 und p liegen; theilen wir wieder diese kleinsten Reste in zwei Abtheilungen

$$\alpha_1, \quad \alpha_2 \ldots \alpha_\mu$$

und

$$\beta_1, \quad \beta_2 \ldots \beta_\lambda,$$

von denen die ersteren $> \frac{1}{2}p$, die letzteren $< \frac{1}{2}p$ sind, und bezeichnen wir mit A die Summe der μ ersteren, mit B die Summe der λ letzteren, ferner mit M die Summe

$$M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{p'q}{p}\right],$$

so folgt durch Addition der vorstehenden Gleichungen

$$\frac{p^2-1}{8}\, q = pM + A + B;$$

da nun (nach §. 43) der Complex der Zahlen

$$p-\alpha_1,\quad p-\alpha_2 \ldots p-\alpha_\mu;\quad \beta_1,\ \beta_2 \ldots \beta_\lambda$$

mit dem Complex der Zahlen

$$1,\ 2,\ 3 \ldots \frac{p-1}{2}$$

vollständig übereinstimmt, so ist ihre Summe

$$\frac{p^2-1}{8} = \mu p - A + B;$$

zieht man diese Gleichung von der vorhergehenden ab, so erhält man

$$\frac{p^2-1}{8}(q-1) = (M-\mu)p + 2A.$$

Nun kommt es uns lediglich darauf an, zu erfahren, ob μ gerade oder ungerade ist; lassen wir daher alle Multipla von 2 fort, so erhalten wir, da $p \equiv -1 \pmod 2$ gesetzt werden kann,

$$\mu \equiv M + \frac{p^2-1}{8}(q-1) \pmod 2.$$

Je nachdem daher die zur Rechten befindliche Zahl gerade oder ungerade ist, wird q quadratischer Rest oder Nichtrest von p sein. Nehmen wir daher z. B. wieder den Fall $q = 2$, so ergiebt sich unmittelbar $M = 0$, also

$$\mu \equiv \frac{p^2-1}{8} \pmod 2,$$

folglich

$$\left(\frac{2}{p}\right) = (-1)^\mu = (-1)^{\frac{p^2-1}{8}};$$

dies ist aber genau die schon früher (§. 41) aufgestellte Formel.

Von jetzt an wollen wir die Untersuchung nur noch unter der Voraussetzung fortführen, dass q eine *ungerade*, also $q-1$ eine gerade Zahl ist; dann ist also

$$\mu \equiv M \pmod 2,\quad \left(\frac{q}{p}\right) = (-1)^M;$$

und es reducirt sich daher die ganze Frage darauf, zu entscheiden, ob die oben mit M bezeichnete Summe *gerade* oder *ungerade* ist.

Um dies weiter zu untersuchen, machen wir die fernere Annahme, es sei q *positiv* und *kleiner als* p. Dann leuchtet zunächst

ein, dass jedes Glied in der Reihe M höchstens um eine Einheit grösser ist als das unmittelbar vorhergehende, weil der Unterschied von zwei auf einander folgenden Brüchen

$$\frac{sq}{p} \quad \text{und} \quad \frac{(s+1)q}{p}$$

< 1 ist, und folglich höchstens *eine* ganze Zahl zwischen beiden liegen kann; da ferner der letzte Bruch

$$\frac{p'q}{p} = \frac{(p-1)q}{2p} = \frac{q-1}{2} + \frac{p-q}{2p}$$

ist, so ist der Werth des letzten Gliedes in der obigen Reihe

$$\left[\frac{p'q}{p}\right] = \frac{q-1}{2} = q'.$$

Mithin kommen in der Summe M nach und nach Glieder vor, welche die Werthe $0, 1, 2 \ldots q'$ besitzen; wir suchen nun gerade die Stellen auf, wo zwei auf einander folgende Glieder

$$\left[\frac{sq}{p}\right] \quad \text{und} \quad \left[\frac{(s+1)q}{p}\right]$$

wirklich um eine Einheit verschieden sind, so dass, wenn t irgend eine der Zahlen $1, 2 \ldots q'$ bedeutet,

$$\frac{sq}{p} < t < \frac{(s+1)q}{p}$$

wird (da q relative Primzahl zu p, und $s < p$ ist, so kann keiner der Brüche $sq:p$ eine ganze Zahl sein); hieraus folgt aber

$$s < \frac{tp}{q} < s+1, \quad \text{also} \quad s = \left[\frac{tp}{q}\right],$$

und folglich giebt es in der Reihe M jedesmal

$$\left[\frac{tp}{q}\right] - \left[\frac{(t-1)p}{q}\right]$$

Glieder, welche den Werth $(t-1)$ haben; und die Anzahl der letzten Glieder, welche den Werth q' haben, ist offenbar

$$p' - \left[\frac{q'p}{q}\right].$$

Multiplicirt man nun jedesmal die Anzahl einer solchen Gruppe von Gliedern, welche einen und denselben Werth haben, mit diesem Werth, so muss die Summe aller dieser Producte $= M$ werden Dies giebt

$$0\cdot\left[\frac{p}{q}\right]+1\cdot\left(\left[\frac{2p}{q}\right]-\left[\frac{p}{q}\right]\right)+2\cdot\left(\left[\frac{3p}{q}\right]-\left[\frac{2p}{q}\right]\right)+\cdots$$
$$+(q'-1)\cdot\left(\left[\frac{q'p}{q}\right]-\left[\frac{(q'-1)p}{q}\right]\right)+q'\cdot\left(\frac{p-1}{2}-\left[\frac{q'p}{q}\right]\right)$$
$$=-\left[\frac{p}{q}\right]-\left[\frac{2p}{q}\right]-\cdots-\left[\frac{q'p}{q}\right]+q'\cdot\frac{p-1}{2}.$$

Setzen wir daher

$$N=\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{q'p}{q}\right],$$

so erhalten wir das Resultat

$$M+N=\frac{p-1}{2}\cdot\frac{q-1}{2},$$

welches offenbar für *je zwei positive ungerade relative Primzahlen* p, q gültig ist; denn bei der Ableitung ist weiter Nichts vorausgesetzt, und da das Resultat vollkommen symmetrisch in Bezug auf die beiden Zahlen p, q ist, von welchen doch eine jedenfalls die kleinere sein muss, so ist auch die bei dem Beweise gemachte Annahme, es sei $p > q$, erlaubt.

Hiermit ist nun zwar die Summe M nicht selbst gefunden, sondern nur auf die Summe N zurückgeführt; aber dies genügt vollständig, um den Reciprocitäts-Satz daraus abzuleiten. Oben ist gezeigt, dass, wenn p eine positive ungerade Primzahl, und q irgend eine durch p nicht theilbare ungerade Zahl bedeutet, stets

$$\left(\frac{q}{p}\right)=(-1)^M$$

ist; nehmen wir daher jetzt ferner an, dass q ebenfalls eine positive ungerade Primzahl ist, so wird ebenso

$$\left(\frac{p}{q}\right)=(-1)^N,$$

und folglich, mit Rücksicht auf den so eben bewiesenen Satz,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{M+N}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

worin der Reciprocitäts-Satz besteht.

§. 45.

Wir betrachten zunächst ein Beispiel, um die Nützlichkeit des Reciprocitätssatzes für die Beurtheilung der Möglichkeit einer Congruenz von der Form

$$x^2 \equiv D \pmod{p}$$

nachzuweisen. Nehmen wir die Congruenz

$$x^2 \equiv 365 \pmod{1847},$$

so ist der Werth des Symbols

$$\left(\frac{365}{1847}\right)$$

zu ermitteln. Zunächst zerlegen wir 365 in Primfactoren, obgleich dies, wie wir später sehen werden, nicht nothwendig ist.

Aus dieser Zerlegung $365 = 5.73$ folgt unmittelbar

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right).$$

Da ferner 5 von der Form $4n+1$ ist, so ergiebt sich aus dem Reciprocitätssatze

$$\left(\frac{5}{1847}\right) = \left(\frac{1847}{5}\right)$$

und also, da $1847 \equiv 2 \pmod{5}$ ist,

$$\left(\frac{5}{1847}\right) = \left(\frac{2}{5}\right) = -1$$

nach §. 41; da ferner auch 73 von der Form $4n+1$ ist, so folgt wieder aus dem Reciprocitätssatze, und weil $1847 \equiv 22 \pmod{73}$ ist,

$$\left(\frac{73}{1847}\right) = \left(\frac{1847}{73}\right) = \left(\frac{22}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{11}{73}\right);$$

nun ist aber $73 \equiv 1 \pmod{8}$, also (nach §. 41)

$$\left(\frac{2}{73}\right) = 1, \quad \text{folglich} \quad \left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right);$$

nach dem Reciprocitätssatze ist aber wieder

$$\left(\frac{11}{73}\right) = \left(\frac{73}{11}\right) = \left(\frac{7}{11}\right),$$

und da beide Primzahlen 7 und 11 von der Form $4n+3$ sind, so ist abermals nach dem Reciprocitätssatze

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1,$$

folglich

$$\left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right) = \left(\frac{7}{11}\right) = -1$$

und also endlich

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) = (-1)(-1) = +1,$$

es ist also 365 quadratischer Rest der Primzahl 1847, d. h. die oben vorgelegte Congruenz ist möglich; und in der That ist

$$(\pm 496)^2 = 246016 = 365 + 133 \cdot 1847.$$

§. 46.

Der in dem eben behandelten Beispiel angewendete Algorithmus, welcher auch bei jedem ähnlichen Beispiel nach einer endlichen Anzahl von Operationen zum Ziele führt, lässt sich im Allgemeinen bedeutend abkürzen, wenn man sich einer zuerst von *Jacobi**) in die Zahlentheorie eingeführten Verallgemeinerung des Legendre'schen Symbols bedient; da der Gebrauch dieses Zeichens auch für unsere späteren Untersuchungen unerlässlich ist, so beschäftigen wir uns zunächst mit der Erklärung desselben und den Gesetzen, denen es gehorcht.

Es sei die *ungerade* Zahl P in ihre Primzahlfactoren p, p', p'' u. s. w. zerlegt, also

$$P = pp'p'' \ldots$$

und m irgend eine *relative Primzahl* zu P, so setzen wir mit *Jacobi*

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots;$$

offenbar ist der Werth dieses Symbols $= +1$ oder $= -1$, je nachdem die Anzahl derjenigen Primfactoren $p, p', p'' \ldots$, von welchen m quadratischer Nichtrest ist, gerade oder ungerade ist. Wenn m

*) Monatsbericht der Berliner Akademie. 1837.

quadratischer Rest von P, und also auch von jeder einzelnen der Primzahlen $p, p', p'' \ldots$ ist, so ist

$$\left(\frac{m}{p}\right) = \left(\frac{m}{p'}\right) = \left(\frac{m}{p''}\right) \cdots = 1,$$

und folglich auch

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right) \cdots = 1;$$

aber man darf diesen Satz durchaus nicht umkehren; sobald nämlich die Zahl m von zweien der Primfactoren $p, p', p'' \ldots$ (oder von vier, von sechs u. s. w.) quadratischer Nichtrest ist, so hat das Symbol den Werth $+1$, und doch ist m quadratischer Nichtrest von P. Im einfachsten Fall, wo P selbst eine ungerade Primzahl ist, stimmt die Bedeutung des Zeichens offenbar mit der frühern überein. Der Vollständigkeit wegen wollen wir ferner festsetzen, dass, wenn $P = 1$, das Symbol immer die positive Einheit bedeuten soll.

Aus dieser Definition des Zeichens ergeben sich nun folgende Sätze:

1. Ist m relative Primzahl gegen jede der beiden ungeraden Zahlen P und Q, also auch gegen die ungerade Zahl PQ, so ist

$$\left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{PQ}\right);$$

denn, wenn

$$P = pp'p'' \ldots$$
$$Q = qq'q'' \ldots$$

ist, wo $p, p' \ldots q, q' \ldots$ lauter Primzahlen bedeuten, so ist

$$\left(\frac{m}{PQ}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right) \cdots \left(\frac{m}{q}\right)\left(\frac{m}{q'}\right)\left(\frac{m}{q''}\right) \cdots$$
$$= \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right).$$

2. Sind die Zahlen $l, m, n \ldots$ relative Primzahlen gegen die ungerade Zahl P, so ist

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) \cdots = \left(\frac{lmn \ldots}{P}\right);$$

denn, wenn wieder

$$P = pp'p'' \ldots$$

ist, so ist

$$\left(\frac{l}{P}\right) = \left(\frac{l}{p}\right)\left(\frac{l}{p'}\right)\left(\frac{l}{p''}\right)\cdots$$
$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots$$
$$\left(\frac{n}{P}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p'}\right)\left(\frac{n}{p''}\right)\cdots$$

u. s. w.

Da nun ferner, wie früher (§. 33) bewiesen ist,

$$\left(\frac{l}{p}\right)\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\cdots = \left(\frac{lmn\cdots}{p}\right)$$

ist, und Aehnliches für die anderen Primfactoren p', p'' u. s. w. gilt, so erhält man durch Multiplication der vorangehenden Gleichungen

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right)\cdots = \left(\frac{lmn\cdots}{p}\right)\left(\frac{lmn\cdots}{p'}\right)\left(\frac{lmn\cdots}{p''}\right)\cdots,$$

worin der zu beweisende Satz besteht.

3. Ist m relative Primzahl zu der ungeraden Zahl P und $m \equiv m'$ (mod. P), also auch m' relative Primzahl zu P, so ist

$$\left(\frac{m}{P}\right) = \left(\frac{m'}{P}\right);$$

denn, wenn $P = pp'p'' \ldots$ ist, so ist auch

$$m \equiv m' \text{ (mod. } p), \quad m \equiv m' \text{ (mod. } p'),$$

u. s. w., also

$$\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right), \quad \left(\frac{m}{p'}\right) = \left(\frac{m'}{p'}\right),$$

u. s. w., und folglich

$$\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots = \left(\frac{m'}{p}\right)\left(\frac{m'}{p'}\right)\cdots,$$

was zu beweisen war. —

4. Die beiden letzten Sätze zeigen, dass das verallgemeinerte Symbol denselben Gesetzen gehorcht wie das einfache; wir wollen nun zeigen, dass auch die Werthe der Symbole

$$\left(\frac{-1}{P}\right), \quad \left(\frac{2}{P}\right)$$

nach den früheren Regeln zu bestimmen sind, und endlich, dass auch ein dem frühern ganz analoger Reciprocitätssatz Statt findet; um

aber den Gang der Beweise nicht zu unterbrechen, schicken wir folgende Bemerkungen voraus. Ist

$$R = r' r'' r''' \dots$$

eine beliebige ungerade Zahl, so sind $r' - 1$, $r'' - 1$, $r''' - 1 \dots$ lauter gerade Zahlen, und folglich ist jedes Product aus zweien oder mehreren dieser Differenzen $\equiv 0 \pmod 4$; bringt man daher R in die Form

$$R = (1 + (r' - 1))\ (1 + (r'' - 1))\ (1 + (r''' - 1)) \dots$$

und führt die Multiplication aus, so ergiebt sich

$$R \equiv 1 + (r' - 1) + (r'' - 1) + (r''' - 1) + \cdots \pmod 4,$$

oder kürzer

$$\frac{R-1}{2} \equiv \Sigma \frac{r-1}{2} \pmod 2,$$

wo das Summenzeichen sich auf den Buchstaben r bezieht, der die einzelnen Factoren r', r'', $r''' \dots$ durchlaufen muss.

Auf ganz ähnliche Weise ergiebt sich aus denselben Voraussetzungen noch ein zweites Lemma; es ist nämlich $r^2 \equiv 1 \pmod 8$ und folglich

$$R^2 = (1 + (r'^2 - 1))\ (1 + (r''^2 - 1))\ (1 + (r'''^2 - 1)) \dots$$
$$\equiv 1 + \Sigma\ (r^2 - 1) \pmod{64},$$

also

$$\frac{R^2-1}{8} \equiv \Sigma \frac{r^2-1}{8} \pmod 8$$

und um so mehr

$$\frac{R^2-1}{8} \equiv \Sigma \frac{r^2-1}{8} \pmod 2.$$

Nach diesen Vorbemerkungen kehren wir zu unserm Gegenstande zurück.

5. Ist P eine positive ungerade Zahl, so ist

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

Denn wenn P das Product aus den positiven Primzahlen p', p'', $p''' \dots$ ist, so ist

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p'}\right)\left(\frac{-1}{p''}\right)\left(\frac{-1}{p'''}\right) \cdots = (-1)^{\Sigma \frac{p-1}{2}},$$

wo der Summationsbuchstabe p alle Primfactoren p', p'', $p''' \dots$ durchlaufen muss; da nun nach dem ersten Lemma 4.

$$\Sigma \frac{p-1}{2} \equiv \frac{P-1}{2} \pmod 2$$

ist, so leuchtet die Richtigkeit des Satzes ein.

6. Ist P eine ungerade Zahl, so ist

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Denn mit Beibehaltung derselben Zeichen ist

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p'}\right)\left(\frac{2}{p''}\right)\left(\frac{2}{p'''}\right)\cdots = (-1)^{\Sigma\frac{p^2-1}{8}},$$

und da nach dem zweiten Lemma 4.

$$\Sigma \frac{p^2-1}{8} \equiv \frac{P^2-1}{8} \pmod 2$$

ist, so ergiebt sich unmittelbar die Richtigkeit des zu beweisenden Satzes.

7. Sind die beiden positiven ungeraden Zahlen P und Q relative Primzahlen zu einander, so ist

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Denn es sei P das Product aus den Primzahlen

$$p', p'', p''' \ldots \qquad (p)$$

und Q das Product aus den Primzahlen

$$q', q'' \ldots \qquad (q)$$

welche also von den Primzahlen $p', p'', p''' \ldots$ verschieden sind. Dann ist zufolge der Erklärung und nach 2.

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q'}\right)\left(\frac{P}{q''}\right)\cdots = \Pi\left(\frac{p}{q}\right),$$

wo das Productzeichen Π sich auf alle Combinationen einer jeden der Primzahlen p mit einer jeden der Primzahlen q bezieht; ganz ebenso ist aber

$$\left(\frac{Q}{P}\right) = \Pi\left(\frac{q}{p}\right)$$

und folglich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \Pi\left(\frac{p}{q}\right)\left(\frac{q}{p}\right),$$

wo das Productzeichen sich auf dieselben Combinationen bezieht; da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ist, so ergiebt sich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

wo wieder das Summenzeichen sich auf dieselben Combinationen jeder Primzahl p mit jeder Primzahl q erstreckt; es ist daher

$$\Sigma\frac{p-1}{2}\frac{q-1}{2} = \Sigma\frac{p-1}{2}\times\Sigma\frac{q-1}{2},$$

wo auf der rechten Seite das erste Summenzeichen sich auf alle Primzahlen p, das zweite sich auf alle Primzahlen q bezieht. Da nun nach dem ersten Lemma 4.

$$\Sigma\frac{p-1}{2} \equiv \frac{P-1}{2} \pmod 2$$

und

$$\Sigma\frac{q-1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

ist, so ergiebt sich

$$\Sigma\frac{p-1}{2}\frac{q-1}{2} \equiv \frac{P-1}{2}\frac{Q-1}{2} \pmod 2,$$

und hieraus

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}},$$

was zu beweisen war. —

Es bleibt uns nun noch eine Bemerkung über das Symbol zu machen übrig; wir haben oben dieses Zeichen nur unter der Voraussetzung definirt, dass die Zahl P eine *positive ungerade* Zahl, und dass die positive oder negative Zahl m *relative Primzahl zu* P ist; wir erweitern jetzt die Bedeutung des Zeichens dahin, dass P auch eine *negative ungerade* Zahl sein kann, immer aber mit der Beschränkung, dass m *relative Primzahl zu* P ist*); und zwar setzen wir fest, dass

$$\left(\frac{m}{-P}\right) = \left(\frac{m}{P}\right)$$

*) Später (Supplemente §. 116) werden wir festsetzen, dass das Symbol den Werth *Null* haben soll, sobald P eine ungerade Zahl, m aber keine relative Primzahl zu P ist.

sein soll. Dann leuchtet augenblicklich ein, dass die Sätze 1., 2., 3. und 6. ohne Beschränkung gültig bleiben; ferner, dass der Satz 5. nur dann richtig ist, wenn P positiv ist, dagegen für ein negatives P falsch wird; und endlich, dass der Satz 7. nur dann gültig bleibt, wenn mindestens eine der beiden Zahlen P und Q positiv ist, dagegen seine Gültigkeit verliert, wenn beide Zahlen P und Q negativ sind.

§. 47.

Die oben (§. 45) an einem Beispiel behandelte Aufgabe, den Werth des Legendre'schen Symbols zu bestimmen, bildet offenbar nur einen ganz speciellen Fall der allgemeinen Aufgabe, den Werth des Jacobi'schen Symbols zu bestimmen. Es zeigt sich nun, dass die damals nothwendige Zerlegung in Primzahlfactoren (abgesehen von dem Factor 2) ganz überflüssig geworden, und der anzuwendende Algorithmus demjenigen ganz ähnlich ist, durch welchen der grösste gemeinschaftliche Divisor zweier Zahlen gefunden wird. Einige Beispiele werden genügen, um diese einfachere Methode zu erläutern.

Beispiel 1: Nehmen wir das schon oben (§. 45) behandelte Beispiel, so können wir jetzt nach dem verallgemeinerten Reciprocitätssatze

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right)$$

setzen, weil 365 von der Form $4n+1$ ist. Da ferner $1847 \equiv 22 \pmod{365}$ ist, so ist nach §. 46, 3. und 2.

$$\left(\frac{1847}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right);$$

da ferner $365 \equiv 5 \pmod 8$, so ist nach §. 46, 6.

$$\left(\frac{2}{365}\right) = -1,$$

also

$$\left(\frac{365}{1847}\right) = -\left(\frac{11}{365}\right).$$

Nach dem verallgemeinerten Reciprocitätssatz ist nun wieder

$$\left(\frac{11}{365}\right) = \left(\frac{365}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

und folglich

$$\left(\frac{365}{1847}\right) = +1,$$

wie früher.

Beispiel 2: Nach dem verallgemeinerten Reciprocitätssatze ist

$$\left(\frac{195}{1901}\right) = \left(\frac{1901}{195}\right);$$

weil $1901 \equiv -49 \pmod{195}$, so ist

$$\left(\frac{1901}{195}\right) = \left(\frac{-49}{195}\right);$$

da ferner die Zahlen -49 und 195 nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, und, weil beide von der Form $4n+3$ sind, so ist

$$\left(\frac{-49}{195}\right) = -\left(\frac{195}{-49}\right) = -\left(\frac{195}{49}\right);$$

weil endlich $195 \equiv -1 \pmod{49}$, und 49 von der Form $4n+1$ ist, so ist

$$\left(\frac{195}{49}\right) = \left(\frac{-1}{49}\right) = +1,$$

also

$$\left(\frac{195}{1901}\right) = -1$$

d. h. 195 ist quadratischer Nichtrest der Primzahl 1901. Natürlich hätte sich die Auflösung abkürzen lassen durch Zerlegung in Factoren, nämlich durch die Bemerkung, dass $49 = 7 \cdot 7$ und folglich

$$\left(\frac{-49}{195}\right) = \left(\frac{-1}{195}\right) = -1$$

ist; überhaupt wird die Operation immer bedeutend abgekürzt, wenn man im Zähler oder Nenner des Symbols quadratische Factoren bemerkt, da diese sogleich fortgelassen werden können.

Beispiel 3: Da $74 = 2 \cdot 37$, und $101 \equiv 5 \pmod{8}$ ist, so ist

$$\left(\frac{74}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{37}{101}\right) = -\left(\frac{37}{101}\right);$$

dann ist ferner nach dem Reciprocitätssatze

$$\left(\frac{37}{101}\right) = \left(\frac{101}{37}\right) = \left(\frac{-10}{37}\right) = \left(\frac{10}{37}\right)$$

und, weil 37 von der Form $8n+5$ ist,

$$\left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right);$$

endlich ist wieder nach dem Reciprocitätssatze

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1$$

und folglich

$$\left(\frac{74}{101}\right) = -1.$$

Kürzer gelangt man durch folgende Kette zum Ziele:

$$\left(\frac{74}{101}\right) = \left(\frac{-27}{101}\right) = \left(\frac{101}{-27}\right) = \left(\frac{-7}{27}\right) = \left(\frac{27}{-7}\right) = \left(\frac{-1}{7}\right) = -1.$$

§. 48.

Wegen der Wichtigkeit des Reciprocitätssatzes theilen wir hier noch einen andern Beweis desselben mit, nämlich den *ersten* der von *Gauss* gegebenen sechs Beweise*); dies kann hier um so eher geschehen, als durch die im Vorhergehenden erörterte Verallgemeinerung des Legendre'schen Symbols mehrere der von *Gauss* unterschiedenen acht Fälle sich zusammenziehen lassen, wodurch der Beweis an Kürze und Uebersichtlichkeit bedeutend gewinnt**).

Das Wesen dieses Beweises besteht in der sogenannten vollständigen Induction; wenn nämlich der Satz für je zwei Primzahlen p, p' richig ist, welche kleiner sind, als eine bestimmte Primzahl q, so lässt sich zeigen, dass er auch für jede Combination einer solchen Primzahl p mit der Primzahl q selbst gelten muss; hieraus und weil der Satz für die beiden kleinsten ungeraden

*) *Disquisitiones Arithmeticae* artt. 135 — 144.

**) *Dirichlet: Ueber den ersten der von Gauss gegebenen Beweise des Reciprocitätsgesetzes in der Theorie der quadratischen Reste* (Crelle's Journal XLVII).

Primzahlen 3 und 5 wirklich richtig ist, folgt dann unmittelbar seine Allgemeingültigkeit

Von besonderer Wichtigkeit für diesen Nachweis ist nun die vorläufige Bemerkung, dass aus der angenommenen Richtigkeit des Reciprocitätssatzes für je zwei Primzahlen p, p', welche kleiner als die Primzahl q sind, mit Nothwendigkeit auch die Gültigkeit des verallgemeinerten Satzes (§. 46, 7.)

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

folgt, sobald die beiden ungeraden relativen Primzahlen P und Q (die nicht gleichzeitig negativ sein dürfen) nur solche Primzahlfactoren enthalten, die kleiner als q sind; denn der Beweis dieses verallgemeinerten Satzes gründete sich ausschliesslich auf die Richtigkeit des einfachen Satzes für alle die Paare von zwei Primzahlen, von denen die eine in P, die andere in Q aufgeht.

Bei dem Beweise nun, dass der Reciprocitätssatz für jede Combination von q mit einer Primzahl p gilt, welche kleiner als q ist, haben wir zwei Fälle zu unterscheiden. Der eine Fall und zwar der schwierigere findet Statt, wenn q die Form $4n+1$ hat, und zugleich p quadratischer Nichtrest von q ist; dann ist zu beweisen, dass auch q quadratischer Nichtrest von p ist. In irgend einem der andern Fälle, nämlich wenn q von der Form $4n+3$ ist, oder auch, wenn q zwar die Form $4n+1$ hat, dann aber p quadratischer Rest von q ist, kann man offenbar der Primzahl p immer ein solches Vorzeichen geben, dass, wenn man $\omega = \pm p$ setzt, wenigstens für eins der beiden Vorzeichen ω quadratischer Rest von q wird; dann ist also zu beweisen, dass

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)}$$

ist; dieser letztere Fall ist deshalb leichter zu behandeln, weil die Annahme sogleich einen Ansatz giebt, welcher nur ausgebeutet zu werden braucht. Wir beginnen daher mit diesem Theile des Satzes.

§. 49.

Es sei also $\omega = \pm p$ quadratischer Rest von q, so hat die Congruenz $x^2 \equiv \omega \pmod{q}$ zwischen 0 und q immer zwei Wurzeln x

deren Summe $= q$, und von denen folglich die eine, welche wir mit e bezeichnen wollen, eine gerade Zahl ist. Dann wird

$$e^2 - \omega = qf$$

sein, wo f eine ganze Zahl bedeutet, welche jedenfalls nicht $= 0$ ist, weil sonst die Primzahl ω eine Quadratzahl sein müsste. Diese Zahl f kann aber auch nicht negativ sein; denn sonst wäre ω positiv $= p$, und $p - e^2$ eine positive durch q theilbare Zahl, was aber unmöglich ist, da $p - e^2 < p$, und der Voraussetzung nach $p < q$ ist. Diese positive Zahl f muss ferner ungerade sein; denn da e gerade ist, so ist $e^2 - \omega$ ungerade, und folglich auch jeder Divisor von $e^2 - \omega$, also auch f ungerade. Endlich ist diese positive ungerade Zahl f nothwendig $< q - 1$; denn da $e \leqq q - 1$, und $p < q - 1$, so ist $qf = e^2 - \omega < (q-1)^2 + (q-1)$, d. h. $qf < q(q-1)$, also wirklich $f < q - 1$.

Nun sind zwei Fälle möglich:

1. Ist f nicht durch p theilbar, so folgt aus der Gleichung $e^2 - \omega = qf$, dass

$$\left(\frac{\omega}{f}\right) = +1,$$

und ferner, weil qf quadratischer Rest von p ist, dass

$$\left(\frac{q}{\omega}\right) = \left(\frac{f}{\omega}\right)$$

sein muss; da nun die beiden ungeraden Zahlen f und ω relative Primzahlen zu einander, beide kleiner als q, und endlich nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, d. h. es ist

$$\left(\frac{f}{\omega}\right)\left(\frac{\omega}{f}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}$$

und hieraus ergiebt sich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}.$$

Da ferner e eine gerade Zahl ist, so ist auch $-\omega \equiv qf \pmod 4$, also (nach dem ersten Lemma 4. in §. 46)

$$-\frac{\omega+1}{2} \equiv \frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod 2;$$

multiplicirt man diese Congruenz mit $\frac{1}{2}(\omega - 1)$, so erhält man auf

der linken Seite ein Product aus zwei successiven ganzen Zahlen, also gewiss eine gerade Zahl, und hieraus folgt unmittelbar

$$\frac{\omega-1}{2}\frac{f-1}{2} \equiv \frac{\omega-1}{2}\frac{q-1}{2} \pmod 2$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)},$$

was zu beweisen war.

2. Ist dagegen f theilbar durch p, so kann man $f = \omega\varphi$ setzen, wo φ eine ungerade Zahl bedeutet, die dasselbe Zeichen wie ω hat und ihrem absoluten Werthe nach $< q$ ist. Da nun $e^2 - \omega = q\omega\varphi$, so ist auch e theilbar durch ω und also $e = \varepsilon\omega$, wo ε wieder eine gerade Zahl ist. Hieraus ergiebt sich nun

$$\varepsilon^2\omega - 1 = q\varphi,$$

und es kann daher φ nicht durch ω theilbar sein. Nun war ω quadratischer Rest von $f = \omega\varphi$, und folglich auch von φ, also ist

$$\left(\frac{\omega}{\varphi}\right) = \left(\frac{\omega}{-\varphi}\right) = +1;$$

ausserdem folgt aus der vorhergehenden Gleichung, dass $-q\varphi$ quadratischer Rest von ω, dass also

$$\left(\frac{q}{\omega}\right) = \left(\frac{-\varphi}{\omega}\right)$$

ist; da endlich von den beiden ungeraden Zahlen $-\varphi$ und ω die eine positiv ist, und da sie relative Primzahlen zu einander und ausserdem beide $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatze

$$\left(\frac{-\varphi}{\omega}\right)\left(\frac{\omega}{-\varphi}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(\varphi+1)}$$

und folglich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(\varphi+1)}.$$

Da nun ε eine gerade Zahl und folglich $q\varphi \equiv -1 \pmod 4$ ist, so muss die eine der beiden Zahlen φ und q von der Form $4n+1$, die andere aber von der Form $4n+3$ sein, woraus folgt, dass

$$\frac{\varphi+1}{2} \equiv \frac{q-1}{2} \pmod 2$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)}$$

ist. Also ist auch für diesen Fall der Satz bewiesen.

§. 50.

Wir kommen nun zu dem zweiten Theile, in welchem vorausgesetzt wird, dass p Nichtrest von q, und q von der Form $4n+1$ ist, und in welchem bewiesen werden muss, dass q Nichtrest von p ist. Hier fehlt nun die Möglichkeit eines Ansatzes, und um diese zu gewinnen, kommt alles darauf an nachzuweisen, dass wenigstens eine Primzahl $p' < q$ existirt, von welcher q quadratischer Nichtrest ist, oder mit anderen Worten, dass die Primzahl q nicht von allen kleineren Primzahlen quadratischer Rest sein kann. Für den Fall, dass $q \equiv 5 \pmod 8$ ist, hat dieser Nachweis nicht die geringste Schwierigkeit; denn dann ist $\frac{1}{2}(q+1) \equiv 3 \pmod 4$, und folglich muss unter den Primfactoren dieser Zahl $\frac{1}{2}(q+1)$, welche natürlich alle $< q$ sind, mindestens einer p' von der Form $4n+3$ sein; dann ist aber $q \equiv -1 \pmod{p'}$ und folglich quadratischer Nichtrest einer kleinern Primzahl p'. Desto schwieriger war dieser Nachweis für den andern Fall zu führen, in welchem $q \equiv 1 \pmod 8$ ist; und *Gauss* selbst gesteht*), dass es ihm erst nach manchen vergeblichen Versuchen gelungen ist, diese capitale Schwierigkeit zu überwinden; er gelangte dazu durch folgende äusserst scharfsinnige Betrachtung.

Es sei $2m+1$ irgend eine ungerade Zahl, aber kleiner als q. Wenn nun q quadratischer Rest von allen ungeraden Primzahlen z ist, welche diese ungerade Zahl $2m+1$ nicht übertreffen, so ist nach früheren Sätzen (§. 37) die Primzahl q, da sie $\equiv 1 \pmod 8$ und also von jeder Potenz der Zahl 2 quadratischer Rest ist, auch quadratischer Rest von jeder Zahl, welche keine anderen ungeraden Primfactoren als die Primzahlen z enthält, und also z. B. von der Zahl

*) *D. A.* art. 125.

$$M = 1 \cdot 2 \cdot 3 \cdot 4 \ldots\ldots (2m)\ (2m+1);$$

es giebt daher positive Zahlen k von der Beschaffenheit, dass

$$q \equiv k^2 \pmod{M}$$

ist, und zwar muss k relative Primzahl zu M sein, weil $2m+1 < q$ und also auch q relative Primzahl zu M ist. Aus dieser Congruenz folgt nun weiter, dass in Bezug auf den Modul M

$$k(q-1^2)\ (q-2^2)\ (q-3^2) \ldots (q-m^2)$$
$$\equiv k(k^2-1^2)\ (k^2-2^2)\ (k^2-3^2) \ldots (k^2-m^2)$$
$$\equiv (k+m)\ (k+m-1) \ldots (k+1)\ k(k-1) \ldots (k-m+1)\ (k-m)$$

ist; da nun nach einem frühern Satze (§. 15) jedes Product von $(2m+1)$ successiven ganzen Zahlen durch M theilbar, und ausserdem k relative Primzahl zu M ist, so ist das Product

$$(q-1^2)\ (q-2^2)\ (q-3^2) \ldots (q-m^2)$$

theilbar durch das Product

$$M = (m+1)\ ((m+1)^2-1^2)\ ((m+1)^2-2^2) \ldots ((m+1)^2-m^2)$$

d. h. das Product

$$\frac{1}{m+1} \cdot \frac{q-1^2}{(m+1)^2-1^2} \cdot \frac{q-2^2}{(m+1)^2-2^2} \cdots \frac{q-m^2}{(m+1)^2-m^2}$$

ist nothwendig eine ganze Zahl.

Andererseits leuchtet ein, dass dies Product gewiss keine ganze Zahl ist, sobald für m die grösste ganze Zahl unterhalb $\sqrt{q}$ genommen wird; denn, wenn $m < \sqrt{q} < m+1$ ist, so sind alle Factoren dieses Productes echte Brüche. Da nun ausserdem $2m+1 < 2\sqrt{q}+1 < q$ ist, so kann für diese Zahl m die Annahme nicht zulässig sein, und wir haben daher folgenden Satz gewonnen:

Ist q eine Primzahl von der Form $8n+1$, so giebt es unterhalb $2\sqrt{q}+1$ und folglich auch unterhalb q mindestens eine ungerade Primzahl p', von welcher q quadratischer Nichtrest ist.

§. 51.

Nachdem für jede Primzahl q von der Form $4n+1$ die Existenz einer Primzahl $p' < q$ nachgewiesen ist, von welcher q quadratischer Nichtrest ist, gehen wir zum Beweise unseres zweiten Theiles über. Jede solche Primzahl p' muss Nichtrest von q sein;

denn wäre p' Rest von q, so würde aus dem schon von uns bewiesenen Theil (§. 49)

$$\left(\frac{q}{p'}\right) = (-1)^{\frac{1}{2}(p'-1)\cdot\frac{1}{2}(q-1)} = +1$$

folgen, was mit der Voraussetzung streitet. Mithin gilt für diese Primzahl p' das Reciprocitätsgesetz. Giebt es nun *ausser* p' noch *andere* ungerade Primzahlen $p < q$, welche Nichtreste von q sind, so ist nur zu beweisen, dass

$$\left(\frac{q}{pp'}\right) = +1$$

ist, weil hieraus sogleich folgt, dass q Nichtrest von p ist. Da nun der Voraussetzung nach p' und p quadratische Nichtreste von q sind, so ist pp' quadratischer Rest von q, und es giebt daher wieder eine gerade Zahl $e < q$ von der Beschaffenheit, dass

$$e^2 - pp' = q\varphi$$

und φ eine ganze Zahl ist; und weil die linke Seite dieser Gleichung eine ungerade Zahl darstellt, welche ihrem absoluten Werthe nach $< q^2$ ist, so ist φ ebenfalls eine ungerade Zahl und zwar $< q$. Je nach der Beschaffenheit dieser Zahl φ zerfällt nun der Beweis in drei Theile.

1. Ist φ weder durch p noch durch p' theilbar, so ist

$$\left(\frac{pp'}{\varphi}\right) = +1,$$

und da $q\varphi$ quadratischer Rest von pp' ist, auch

$$\left(\frac{q\varphi}{pp'}\right) = 1, \text{ also } \left(\frac{q}{pp'}\right) = \left(\frac{\varphi}{pp'}\right);$$

da ferner die beiden ungeraden relativen Primzahlen φ und pp' (von denen die letztere positiv ist) nur solche Primfactoren enthalten, welche $< q$ sind, so gilt für diese beiden Zahlen auch das verallgemeinerte Reciprocitätsgesetz, d. h. es ist

$$\left(\frac{\varphi}{pp'}\right)\left(\frac{pp'}{\varphi}\right) = (-1)^{\frac{1}{2}(\varphi-1)\cdot\frac{1}{2}(pp'-1)}$$

und folglich, mit Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(\varphi-1)\cdot\frac{1}{2}(pp'-1)}.$$

Da aber e eine gerade Zahl, so ist $q\varphi \equiv -pp' \pmod 4$, also, da $q \equiv 1 \pmod 4$ ist,

$$\varphi \equiv -pp' \pmod 4$$

$$\frac{\varphi-1}{2} \equiv -\frac{pp'+1}{2} \pmod 2$$

also

$$\frac{\varphi-1}{2} \cdot \frac{pp'-1}{2} \equiv 0 \pmod 2$$

und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

2. Ist φ durch p' theilbar, durch p nicht theilbar, so setze man $\varphi = p'\psi$, und, da auch e durch p' theilbar sein muss, $e = p'\varepsilon$; dann ist $\psi < q$ eine durch p nicht theilbare ungerade, und ε eine gerade Zahl, und es wird

$$p'\varepsilon^2 - p = q\psi.$$

Hieraus folgt nun zunächst wieder (da ψ relative Primzahl zu pp' ist)

$$\left(\frac{pp'}{\psi}\right) = +1,$$

ferner

$$\left(\frac{q\psi}{p}\right) = \left(\frac{p'}{p}\right), \quad \text{also} \quad \left(\frac{q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{\psi}{p}\right)$$

und

$$\left(\frac{q\psi}{p'}\right) = \left(\frac{-p}{p'}\right), \quad \text{also} \quad \left(\frac{q}{p'}\right) = \left(\frac{-p}{p'}\right)\left(\frac{\psi}{p'}\right)$$

und folglich

$$\left(\frac{q}{pp'}\right) = \left(\frac{p'}{-p}\right)\left(\frac{-p}{p'}\right)\left(\frac{\psi}{pp'}\right) = (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(p'-1)}\left(\frac{\psi}{pp'}\right);$$

da endlich ψ und pp' nur solche Primfactoren enthalten, die $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatz

$$\left(\frac{\psi}{pp'}\right)\left(\frac{pp'}{\psi}\right) = (-1)^{\frac{1}{2}(\psi-1)\cdot\frac{1}{2}(pp'-1)}$$

und hieraus in Verbindung mit zwei vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(p'-1)+\frac{1}{2}(\psi-1)\cdot\frac{1}{2}(pp'-1)}.$$

Da nun $\varepsilon^2 \equiv 0 \pmod 4$ und $q \equiv 1 \pmod 4$, so ist $\psi \equiv -p \pmod 4$, folglich

$$\tfrac{1}{2}(\psi-1) \equiv \tfrac{1}{2}(p+1) \pmod 2,$$

also

$$\tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(\psi-1)\cdot\tfrac{1}{2}(pp'-1)$$
$$\equiv \tfrac{1}{2}(p+1)\,[\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(pp'-1)] \pmod 2,$$

und da ferner (nach dem ersten Lemma 4. in §. 46)

$$\tfrac{1}{2}(pp'-1) \equiv \tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1) \pmod 2$$

ist, so ergiebt sich

$$\tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(\psi-1)\cdot\tfrac{1}{2}(pp'-1)$$
$$\equiv \tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p-1) \equiv 0 \pmod 2$$

und folglich

$$\left(\frac{q}{pp'}\right)=1,$$

was zu beweisen war.

Da bei diesem Beweise die Annahme, dass q Nichtrest von p' ist, gar nicht zur Anwendung gekommen ist, so wird durch einfache Vertauschung von p mit p' der Beweis für den Fall entstehen, dass φ durch p theilbar, durch p' nicht theilbar ist; denn im Uebrigen sind sowohl die Voraussetzungen als auch das zu beweisende Resultat vollständig symmetrisch in Bezug auf beide Primzahlen p und p'.

3. Ist φ sowohl durch p als auch durch p' und folglich (da p und p' verschiedene Primzahlen sind) auch durch pp' theilbar, so setze man $\varphi = pp'\psi$, und, da e dann ebenfalls durch pp' theilbar ist, $e = pp'\varepsilon$; dann bedeutet ψ eine ungerade Zahl $< q$, und ε eine gerade Zahl, und es wird

$$pp'\varepsilon^2-1 = q\psi.$$

Hieraus folgt, dass pp' relative Primzahl zu ψ und ausserdem quadratischer Rest von ψ, also

$$\left(\frac{pp'}{\psi}\right)=+1$$

ist; ebenso ergiebt sich aber, dass $-q\psi$ quadratischer Rest von pp', dass also

$$\left(\frac{q}{pp'}\right)=\left(\frac{-\psi}{pp'}\right)$$

ist; nach dem verallgemeinerten Reciprocitätssatze, welcher offenbar für die beiden Zahlen $-\psi$ und pp' gilt, ist ferner

$$\left(\frac{-\psi}{pp'}\right)\left(\frac{pp'}{-\psi}\right)=(-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)},$$

und hieraus ergiebt sich in Verbindung mit den beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)}.$$

Da aber ϵ eine gerade Zahl, und $q \equiv 1 \pmod 4$, so ist $\psi \equiv -1 \pmod 4$, also $\frac{1}{2}(\psi+1)$ eine gerade Zahl, und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

Hiermit ist nun auch der zweite Theil des Beweises vollständig geführt und dadurch die Allgemeingültigkeit des Reciprocitätssatzes von Neuem nachgewiesen (ein dritter Beweis findet sich in den Supplementen I. §. 115). Auf ähnliche Weise lassen sich auch die Sätze über die Charaktere der Zahlen -1 und 2 begründen, was dem Leser überlassen bleiben mag*).

§. 52.

Nach allen diesen Untersuchungen kehren wir nun zurück zu der Beantwortung der zweiten in §. 32 aufgeworfenen Frage, welche in §. 39 auf die folgende reducirt ist:

Von welchen ungeraden Primzahlen q ist die gegebene Zahl D quadratischer Rest?

Auch jetzt fragen wir nur nach denjenigen (positiv genommenen) Primzahlen q, welche nicht in D aufgehen, und setzen ausserdem der Einfachheit halber voraus, dass D kein Quadrat und auch durch kein Quadrat (ausser 1) theilbar ist, weil der allgemeinere Fall offenbar sogleich auf diesen einfachern reducirt werden kann. Es wird sich zeigen, dass nicht blos alle diese Primzahlen q (die *Divisoren der Form* $t^2 - Du^2$ nach §. 39), sondern überhaupt alle positiven Zahlen n, welche relative Primzahlen zu $2D$ sind und der Bedingung

$$\left(\frac{D}{n}\right) = +1$$

*) *Dirichlet* a. a. O.

genügen, in einer Anzahl von bestimmten Linearformen, d. h. von arithmetischen Reihen enthalten sind, deren Differenz entweder $= 2D$ oder $= 4D$ ist. Da wir vorausgesetzt haben, dass die positive oder negative Zahl D durch keine Quadratzahl theilbar ist, so wird, wenn wir das Product aller in D aufgehenden positiven ungeraden Primzahlen $p, p', p'' \ldots$ mit P bezeichnen, entweder $D = \pm P$, oder $D = \pm 2P$ sein; wenn D keine ungerade Primzahl p als Factor enthält (für welchen Fall das Resultat aber schon in den §§. 40, 41 oder allgemeiner in §. 46, 5. und 6. angegeben ist), wird $P = 1$ zu setzen sein. Wir unterscheiden im Ganzen vier Fälle.

I. $D = \pm P \equiv 1 \pmod 4$.

In diesem Falle ist, wenn n irgend eine *positive* Zahl bedeutet, die relative Primzahl zu $2D$ ist, zufolge des verallgemeinerten Reciprocitätssatzes (§. 46, 7.)

$$\left(\frac{D}{n}\right) = \left(\frac{n}{P}\right).$$

Da nun das Symbol rechts für alle Zahlen n, welche einer und derselben Classe (mod. P) angehören, nach §. 46, 3. einen und denselben Werth besitzt, so kommt es offenbar nur darauf an, ein vollständiges System von $\varphi(P)$ incongruenten Zahlen m (mod. P) zu betrachten, die relative Primzahlen zu P sind, und für jede den Werth des Symbols zu bestimmen. Es ist wichtig, dies etwas näher zu untersuchen.

Zunächst lässt sich beweisen, dass Zahlen b existiren, welche der Bedingung

$$\left(\frac{b}{P}\right) = -1 \qquad (1)$$

genügen. Denn da D nicht $= +1$ sein kann, und folglich P mindestens eine Primzahl p enthält, so wähle man einen beliebigen Nichtrest β von p, und bestimme b (nach §. 25) durch die Bedingungen

$$b \equiv \beta \pmod p, \quad b \equiv 1 \pmod{P'},$$

wo $P = pP'$ gesetzt ist, so wird

$$\left(\frac{b}{P}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{P'}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{P'}\right) = -1.$$

Nachdem dieser Punct absolvirt ist, erkennt man leicht, dass die Anzahl aller incongruenten Zahlen b (mod. P), welche der Be-

dingung (1) genügen, $= \frac{1}{2}\varphi(P)$, und folglich die Anzahl aller incongruenten Zahlen a (mod. P), für welche

$$\left(\frac{a}{P}\right) = +1 \tag{2}$$

ist, ebenso gross ist. Denn setzt man

$$S = \Sigma\left(\frac{m}{P}\right),$$

wo m das ganze System aller $\varphi(P)$ incongruenten Zahlen durchlaufen soll, so ist S gänzlich unabhängig von der Wahl der die einzelnen Zahlclassen repräsentirenden Individuen m; da nun, wenn b eine bestimmte Zahl von der Beschaffenheit (1) bedeutet, auch die Producte bm ein solches vollständiges System bilden, so ist auch

$$S = \Sigma\left(\frac{bm}{P}\right) = \left(\frac{b}{P}\right)\Sigma\left(\frac{m}{P}\right) = -S$$

und folglich

$$\Sigma\left(\frac{m}{P}\right) = 0, \tag{3}$$

mithin ist die Anzahl der Glieder dieser Summe, welche den Werth $+1$ haben, gleich der Anzahl derjenigen, welche den Werth -1 haben; d. h. die Anzahl der Zahlclassen a ist gleich derjenigen der Zahlclassen b.

Es leuchtet ferner ein, dass man die Repräsentanten m (oder a und b) sämmtlich *ungerade* wählen kann; denn ist m gerade, so ist $m + P$ eine in derselben Zahlclasse enthaltene ungerade Zahl. Dann wird also

$$\left(\frac{D}{n}\right) = +1, \quad \text{wenn} \quad n \equiv a \pmod{2P}$$

$$\left(\frac{D}{n}\right) = -1, \quad \text{wenn} \quad n \equiv b \pmod{2P}$$

und jede (positive) Zahl n, welche relative Primzahl zu $2D$ ist, ist in einer und nur einer dieser arithmetischen Reihen (von der Differenz $2D$) enthalten.

Beispiel 1. Ist $D = +P = 21$, also $\varphi(P) = 12$, so sind die sämmtlichen relativen Primzahlen zu P congruent

$$\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10;$$

bestimmt man nun für jede dieser Zahlen den Werth des Jacobi'schen Symbols nach §. 47, so ergiebt sich

$$a \equiv \pm 1, \pm 4, \pm 5; \quad b \equiv \pm 2, \pm 8, \pm 10;$$

es wird daher

$$\left(\frac{21}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 5, 17, 25, 37, 41 \pmod{42}$$

$$\left(\frac{21}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 11, 13, 19, 23, 29, 31 \pmod{42}.$$

Beispiel 2. Ist $D = -P = -15$, so sind die zu betrachtenden Zahlenclassen folgende $\pm 1, \pm 2, \pm 4, \pm 7$; diese zerfallen in $a \equiv +1, +2, +4, -7$, und $b \equiv -1, -2, -4, +7$. Es wird daher

$$\left(\frac{-15}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 17, 19, 23 \pmod{30}$$

$$\left(\frac{-15}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 7, 11, 13, 29 \pmod{30}.$$

Wir gehen nun über zu dem Fall

$$\text{II.} \quad D = \pm P \equiv 3 \pmod{4}.$$

Bedeutet n wieder eine *positive* relative Primzahl zu $2D$, so ist nach dem allgemeinen Reciprocitätssatz

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n-1}{2}} \left(\frac{n}{P}\right);$$

behalten wir dieselbe Bezeichnung wie im ersten Falle bei, so wird

$$\left(\frac{D}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1 \pmod{4} \quad \text{und} \quad n \equiv a \pmod{P}$$
$$\text{oder} \quad n \equiv 3 \pmod{4} \quad \text{und} \quad n \equiv b \pmod{P}$$

dagegen

$$\left(\frac{D}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 1 \pmod{4} \quad \text{und} \quad n \equiv b \pmod{P}$$
$$\text{oder} \quad n \equiv 3 \pmod{4} \quad \text{und} \quad n \equiv a \pmod{P}.$$

Einem jeden solchen Congruenzpaare entspricht aber (nach §. 25) eine bestimmte Classe von Zahlen $n \pmod{4P}$; man erhält daher $\varphi(P) = \frac{1}{2}\varphi(4P)$ solche Classen von Zahlen n, die der einen Kategorie angehören, und ebenso viele Classen von Zahlen n, die den entgegengesetzten Charakter haben; diese Classen bilden arithmetische Reihen von der Differenz $4D$. Dies Resultat gilt auch noch in dem Falle $D = -1$, obgleich dann keine Zahl b existirt.

Beispiel. Für $D = +15$ wird

$$\left(\frac{D}{n}\right) = +1, \text{ wenn } n \equiv 1 \pmod 4, \equiv +1, +2, +4, -7 \pmod{15}$$
$$\text{oder } n \equiv 3 \pmod 4, \equiv -1, -2, -4, +7 \pmod{15}$$

dagegen

$$\left(\frac{D}{n}\right) = -1, \text{ wenn } n \equiv 1 \pmod 4, \equiv -1, -2, -4, +7 \pmod{15}$$
$$\text{oder } n \equiv 3 \pmod 4, \equiv +1, +2, +4, -7 \pmod{15};$$

hieraus ergiebt sich

$$\left(\frac{15}{n}\right) = +1, \text{ wenn } n \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60}$$

$$\left(\frac{15}{n}\right) = -1, \text{ wenn } n \equiv 13, 19, 23, 29, 31, 37, 41, 47 \pmod{60}.$$

Die Rechnung gestaltet sich am einfachsten, wenn man die sämmtlichen positiven relativen Primzahlen zu $4P$ darauf prüft, ob sie der einen oder andern Kategorie angehören, und sie lässt sich noch durch manche Kunstgriffe abkürzen, die hier nicht erwähnt werden können.

III. $D = \pm 2P \equiv 2 \pmod 8$.

In diesem Falle ist, wenn n eine *positive* relative Primzahl zu D bedeutet,

$$\left(\frac{D}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right),$$

und folglich

$$\left(\frac{D}{n}\right) = +1, \text{ wenn } n \equiv \pm 1 \pmod 8, \equiv a \pmod P$$
$$\text{oder } n \equiv \pm 3 \pmod 8, \equiv b \pmod P$$

dagegen

$$\left(\frac{D}{n}\right) = -1, \text{ wenn } n \equiv \pm 1 \pmod 8, \equiv b \pmod P$$
$$\text{oder } n \equiv \pm 3 \pmod 8, \equiv a \pmod P$$

und jedem bestimmten Congruenzpaare entspricht eine bestimmte Zahlclasse $n \pmod{8P}$; die Zahlen n vertheilen sich daher in arithmetische Reihen von der Differenz $4D$; jeder der beiden Kategorien gehören gleich viele Zahlclassen an.

Beispiel. Ist $D = -6$, so ergiebt sich

$$\left(\frac{-6}{n}\right) = +1, \text{ wenn } n \equiv 1, 5, 7, 11 \pmod{24}$$

$$\left(\frac{-6}{n}\right) = -1, \text{ wenn } n \equiv 13, 17, 19, 23 \pmod{24}.$$

IV. $D = \pm 2P \equiv 6 \pmod{8}$

In diesem Falle ist

$$\left(\frac{D}{n}\right) = (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right),$$

und folglich

$$\left(\frac{D}{n}\right) = +1, \text{ wenn } n \equiv 1, 3 \pmod{8}, \equiv a \pmod{P}$$
$$\text{oder } n \equiv 5, 7 \pmod{8}, \equiv b \pmod{P}$$

dagegen

$$\left(\frac{D}{n}\right) = -1, \text{ wenn } n \equiv 1, 3 \pmod{8}, \equiv b \pmod{P}$$
$$\text{oder } n \equiv 5, 7 \pmod{8}, \equiv a \pmod{P}.$$

Die Zahlen n vertheilen sich wieder in arithmetische Reihen von der Differenz $4D$; jeder der beiden Kategorien gehören gleich viele Zahlclassen an.

Beispiel. Für $D = +6$ ergiebt sich

$$\left(\frac{6}{n}\right) = +1, \text{ wenn } n \equiv 1, 5, 19, 23 \pmod{24}$$

$$\left(\frac{6}{n}\right) = -1, \text{ wenn } n \equiv 7, 11, 13, 17 \pmod{24}.$$

Wir bemerken schliesslich, dass die vier Fälle sich zusammenfassen lassen, wenn man zwei positive oder negative Einheiten δ, ε einführt, so, dass $\delta = +1$ oder $= -1$, je nachdem $\pm P \equiv 1$ oder $\equiv 3 \pmod{4}$, und dass $\varepsilon = +1$ oder $= -1$, je nachdem D ungerade oder gerade ist. Die vier Fälle stellen sich dann folgendermassen dar:

$$D = \pm P \equiv 1 \pmod{4}, \quad \delta = +1, \quad \varepsilon = +1;$$
$$D = \pm P \equiv 3 \pmod{4}, \quad \delta = -1, \quad \varepsilon = +1;$$
$$D = \pm 2P \equiv 2 \pmod{8}, \quad \delta = +1, \quad \varepsilon = -1;$$
$$D = \pm 2P \equiv 6 \pmod{8}, \quad \delta = -1, \quad \varepsilon = -1.$$

Dann ist vermöge des allgemeinen Reciprocitätssatzes und der Ergänzungssätze (§. 46)

$$\left(\frac{D}{n}\right) = \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right),$$

wo n wieder irgend eine positive relative Primzahl zu $2D$ bedeutet.

Lässt man n ein vollständiges System incongruenter Zahlen nach dem Modulus $4D$ durchlaufen, welche zugleich positiv und relative Primzahlen zu $2D$ sind, so ergiebt sich in allen vier Fällen, dass die entsprechende Summe

$$\Sigma\left(\frac{D}{n}\right) = 0$$

ist; im ersten Falle genügt es schon, dass n ein solches vollständiges Restsystem nach dem Modulus $2D$ durchläuft.