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_0060
LOG Titel: §. 52. Aufstellung der Linearformen, in denen die Primzahlen enthalten sind, von welchen eine gegebene Zahl quadratischer Rest oder Nichtrest ist
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

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.