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_0052
LOG Titel: §. 44. Zweiter Theil des Beweises
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

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

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.