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_0054
LOG Titel: §. 46. Jacobi's Verallgemeinerung des Symbols von Legendre. Verallgemeinerter Reciprocitätssatz
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 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.