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_0049
LOG Titel: §. 41. Die Zahl 2 ist quadratischer Rest aller Primzahlen van der Form ..... , NichtTest aller Primzahlen von der Form ....
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

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

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