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_0058
LOG Titel: §. 50. Lemma: ist q eine Primzahl von der Form 8n + 1, so giebt es unterhalb ..... mindestens eine ungerade Primzahl, von welcher q quadratischer 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

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

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.