SUB | NIEDERSÄCHSISCHE STAATS- UND UNIVERSITÄTSBIBLIOTHEK GÖTTINGEN

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_0051
LOG Titel: §. 43. Erster Theil des Beweises; Umformung des früheren' Kriteriums für den Charakter einer Zahl. Neuer Beweis des Satzes über die Zahl 2
LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

Dieser Satz wurde zuerst von *Legendre* durch Induction gefunden und ausgesprochen; allein erst *Gauss* hat denselben vollständig bewiesen, ja er hat nach einander sechs auf ganz verschiedenen Grundgedanken beruhende Beweise*) von diesem Satze gegeben, den er in etwas anderer Form aussprach und seiner Wichtigkeit wegen das *Theorema fundamentale* in der Theorie der quadratischen Reste nannte. Wir folgen hier zunächst dem *dritten* dieser sechs Beweise, der sich auf ein Lemma stützt, durch welches das Euler'sche Kriterium (§. 33) über den Charakter einer Zahl D in Bezug auf die Primzahl p in ein anderes umgeformt wird.

§. 43.

Wir haben früher (§. 33) gesehen, dass eine durch p nicht theilbare Zahl D quadratischer Rest oder Nichtrest von p ist, je nachdem

$$D^{\frac{p-1}{2}} \equiv +1 \text{ oder } \equiv -1 \pmod{p}$$

ist; betrachten wir nun die Producte

$$D,\quad 2D,\quad 3D \ldots \tfrac{1}{2}(p-1)D$$

aus dieser Zahl D und aus den ersten $\frac{1}{2}(p-1)$ ganzen positiven Zahlen, so werden die kleinsten positiven Reste

$$r_1,\quad r_2,\quad r_3 \ldots r_{\frac{p-1}{2}}$$

derselben, nach dem Modulus p genommen, erstens sämmtlich verschieden von einander und kleiner als p sein, und keiner von ihnen kann gleich Null sein. Wir theilen nun diese $\frac{1}{2}(p-1)$ Reste in zwei Abtheilungen, je nachdem sie grösser oder kleiner als $\frac{1}{2}p$ sind, und bezeichnen die erstern, deren Anzahl $= \mu$ sei, mit

$$\alpha_1,\quad \alpha_2 \ldots \alpha_\mu,$$

---

*) *D. A.* art. 125—145. — *D. A.* art. 262. — *Theorematis arithmetici demonstratio nova.* 1808. — *Summatio quarumdam serierum singularium.* 1808. — *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae.* 1817. — Vergl. §§. 48—51, 115.

die übrigen Reste, welche kleiner als $\frac{1}{2}p$ sind, und deren Anzahl $\lambda = \frac{1}{2}(p-1) - \mu$ ist, mit

$$\beta_1, \quad \beta_2 \ldots \beta_\lambda.$$

Nimmt man nun von den erstern μ Resten ihre Ergänzungen zur Zahl p, also die Zahlen

$$p-\alpha_1, \quad p-\alpha_2 \ldots p-\alpha_\mu,$$

so liegen dieselben, ebenso wie die λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$, auch zwischen den Grenzen 0 und $\frac{1}{2}p$; ausserdem sind sie alle von einander verschieden; endlich lässt sich aber auch zeigen, dass sie von den λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$ verschieden sind; denn wäre z. B. $p-\alpha = \beta$, also $\alpha+\beta = p \equiv 0 \pmod{p}$, so müsste auch, wenn α der Rest von sD, β der Rest von tD ist,

$$sD + tD = (s+t)D \equiv 0 \pmod{p}$$

und folglich $s+t$ durch p theilbar sein; allein da jede der beiden Zahlen s und t zwischen 0 und $\frac{1}{2}p$ liegt, so liegt $s+t$ zwischen 0 und p (mit Ausschluss dieser beiden Grenzen); es kann daher $s+t$ nicht theilbar durch p, und folglich auch nicht $p-\alpha = \beta$ sein.

Mithin haben die folgenden $\frac{1}{2}(p-1)$ Zahlen

$$p-\alpha_1, \quad p-\alpha_2 \ldots p-\alpha_\mu; \quad \beta_1, \quad \beta_2 \ldots \beta_\lambda$$

lauter von einander verschiedene Werthe, und da sie ihrem Werth nach zwischen 0 und $\frac{1}{2}p$ liegen, so müssen sie im Complex genommen identisch mit den $\frac{1}{2}(p-1)$ Zahlen

$$1, \quad 2, \quad 3 \ldots \tfrac{1}{2}(p-1)$$

sein, so dass ihr Product

$$(p-\alpha_1)(p-\alpha_2)\ldots(p-\alpha_\mu)\,\beta_1\beta_2\ldots\beta_\lambda = 1.2.3\cdots\tfrac{1}{2}(p-1)$$

ist. Werfen wir hieraus die Multipla von p weg, so erhalten wir die Congruenz

$$(-1)^\mu \alpha_1\alpha_2\ldots\alpha_\mu.\beta_1\beta_2\ldots\beta_\lambda \equiv 1.2.3\cdots\tfrac{1}{2}(p-1) \pmod{p};$$

da nun andererseits

$$\alpha_1\alpha_2\ldots\alpha_\mu.\beta_1\beta_2\ldots\beta_\lambda \equiv 1.2\cdots\tfrac{1}{2}(p-1)\,D^{\frac{p-1}{2}} \pmod{p}$$

ist, so folgt hieraus, dass

$$(-1)^\mu.1.2\cdots\tfrac{1}{2}(p-1).D^{\frac{p-1}{2}} \equiv 1.2.3\cdots\tfrac{1}{2}(p-1) \pmod{p}$$

und also auch

$$D^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}$$

oder, was dasselbe sagt, dass

$$\left(\frac{D}{p}\right) = (-1)^{\mu}$$

ist. Hierin besteht die Umformung des Kennzeichens, welches darüber entscheidet, ob eine Zahl D quadratischer Rest oder Nichtrest der ungeraden Primzahl p ist:

Man braucht nur nachzusehen, ob die Anzahl μ der kleinsten positiven Reste der Zahlen

$$D,\ 2D,\ 3D \ldots \tfrac{1}{2}(p-1)D,$$

die grösser als $\frac{1}{2}p$ ausfallen, gerade oder ungerade ist; je nachdem das Erstere oder Letztere eintritt, ist D quadratischer Rest oder quadratischer Nichtrest von p.

Mit Hülfe dieses Satzes ist man schon im Stande, für jedes wirklich gegebene D die Formen für die Primzahlen aufzustellen, von welchen D Rest oder Nichtrest ist. Um dies deutlicher zu zeigen, betrachten wir den allerdings schon früher (§. 41) vollständig durchgeführten Fall $D = 2$. Bilden wir die Zahlen

$$2,\ 4,\ 6 \ldots (p-1),$$

so ist jede derselben auch ihr eigener kleinster positiver Rest in Bezug auf den Modulus p, und die Anzahl μ derjenigen dieser Zahlen, welche $> \frac{1}{2}p$ sind, wird durch die Bedingungen

$$p-1-2\mu < \tfrac{1}{2}p < p+1-2\mu \quad \text{oder} \quad \frac{p-2}{4} < \mu < \frac{p+2}{4}$$

bestimmt; bezeichnen wir daher allgemein mit $[x]$ die grösste in der reellen Zahl x enthaltene *ganze* Zahl, so dass stets $0 \leqq x-[x] < 1$ ist, so erhalten wir

$$\mu = \left[\frac{p+2}{4}\right].$$

Je nachdem nun p von einer der Formen $8n+1$, $8n+3$, $8n+5$, $8n+7$ ist, wird $\mu = 2n,\ 2n+1,\ 2n+1,\ 2n+2$; es ist daher μ gerade und folglich

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

und μ ist ungerade, also