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_0164
LOG Titel: §. 145. Lemma über die Congruenzen zweiten Grades
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

X. Ueber die Composition der binären quadratischen Formen.

§. 145.

Den Ausgangspunct für unsere Darstellung der von *Gauss**) gegründeten Theorie der Composition bildet folgendes Lemma:

Ist

$$bb \equiv D \pmod{a}, \quad b'b' \equiv D \pmod{a'}, \tag{1}$$

und haben die drei Zahlen a, a', $b + b'$ *keinen gemeinschaftlichen Theiler, so existirt in Bezug auf den Modulus* aa' *eine und nur eine Classe von Zahlen* B, *welche den drei Bedingungen*

$$B \equiv b \pmod{a}, \quad B \equiv b' \pmod{a'}, \quad BB \equiv D \pmod{aa'} \tag{2}$$

genügen.

Dies leuchtet unmittelbar ein, falls a und a' relative Primzahlen sind (§§. 25, 37); unter der allgemeineren Voraussetzung aber, dass a, a', $b + b'$ keinen gemeinschaftlichen Theiler haben, bestimme man (nach §. 24) drei ganze Zahlen h, h', h'', welche die Bedingung

$$ha + h'a' + h''(b + b') = 1 \tag{3}$$

befriedigen; dann werden alle durch die Congruenz

$$B \equiv hab' + h'a'b + h''(bb' + D) \pmod{aa'} \tag{4}$$

bestimmten Zahlen B und nur diese den Forderungen (2) genügen. Da nämlich

---

*) *D. A.* art. 234 seqq. — Vergl. *Lejeune Dirichlet: De formarum binariarum secundi gradus compositione.* 1851.