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_0177
LOG Titel: §. 158. Jede Classe des Hauptgeschlechtes entsteht durch Duplication
LOG Typ: chapter

$-bc \equiv \mathfrak{A}^2$ (*mod. a*), $-ca \equiv \mathfrak{B}^2$ (*mod. b*), $-ab \equiv \mathfrak{C}^2$ (*mod. c*), *so ist die obige Gleichung in relativen Primzahlen x, y, z der Art lösbar, dass*

$$\mathfrak{A}z \equiv by \text{ (mod. } a), \quad \mathfrak{B}x \equiv cz \text{ (mod. } b), \quad \mathfrak{C}y \equiv ax \text{ (mod. } c)$$

wird.

§. 158.

Mit Hülfe dieses Satzes lässt sich nun das oben (§. 155) erwähnte grosse Theorem von *Gauss* leicht beweisen:

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Als Repräsentanten der dem Hauptgeschlechte der Determinante D angehörenden Classe wählen wir eine Form (A, B, C), deren erster Coefficient A relative Primzahl zu $2D$ ist (§. 93). Da die Zahl A durch diese Form darstellbar ist, und alle Einzel-Charaktere derselben den Werth $+1$ haben, so ist A quadratischer Rest von jeder in D aufgehenden ungeraden Primzahl, und auch von 4 oder von 8, falls D durch 4 oder 8 theilbar ist (§. 122); mithin ist (nach §. 37) A quadratischer Rest von D selbst (umgekehrt ergiebt sich leicht, zum Theil mit Hülfe des Reciprocitätssatzes, dass die Form (A, B, C) gewiss dem Hauptgeschlecht angehört, wenn A relative Primzahl zu $2D$, quadratischer Rest von D, und, falls D negativ sein sollte, positiv ist). Ja, man kann sogar voraussetzen, dass A quadratischer Rest von $4D$ ist, d. h. dass $A \equiv 1$ (mod. 4), oder $A \equiv 1$ (mod. 8) ist, je nachdem D ungerade oder gerade ist. Dies ist in der That von selbst der Fall, wenn $D \equiv 3$ (mod. 4), oder $D \equiv 0$ (mod. 8) ist; sollte ferner A in den übrigen Fällen dieser Bedingung nicht genügen, wäre also $A \equiv 3$ (mod. 4), $\equiv 7$ (mod. 8), $\equiv 3$ (mod. 8), $\equiv 5$ (mod. 8), je nachdem $D \equiv 1$ (mod. 4), $\equiv 2$ (mod. 8), $\equiv 6$ (mod. 8), $\equiv 4$ (mod. 8), so kann man die Form (A, B, C) durch eine Substitution $\binom{\alpha, \; -1}{1, \;\; 0}$ in eine Form transformiren, deren erster Coefficient $A' = A\alpha^2 + 2B\alpha + C$ relative Primzahl zu $2D$ ist und zugleich die verlangte Eigenschaft besitzt; da nämlich $AA' = (A\alpha + B)^2 - D$ ist, so braucht man α nur so zu wählen, dass $A\alpha + B$ im ersten Falle gerade, in den drei übrigen Fällen aber ungerade wird, was sich stets in der Art erreichen lässt, dass $A\alpha + B$ zugleich relative Primzahl zu D wird.