Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Werk Id: PPN30976923X

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN30976923X|LOG_0157

OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

VIII. Ueber die Pell'sche Gleichung.

§. 141.

Bedeutet D eine positive ganze Zahl, die aber kein vollständiges Quadrat ist, so ist in §. 83 durch die Betrachtung der Perioden von reducirten quadratischen Formen, die zur Determinante D gehören, nachgewiesen, dass die Pell'sche oder Fermat'sche Gleichung

$$t^2 - Du^2 = 1$$

immer unendlich viele Lösungen in ganzen positiven Zahlen t, u besitzt, und es ist dort auch eine Methode gegeben, durch welche alle diese Lösungen gefunden werden können. Es hat durchaus keine Schwierigkeit, den Zusammenhang zwischen allen diesen Lösungen zu finden, sobald nur erst der Hauptpunct bewiesen ist, dass wirklich eine Lösung existirt, in welcher u von Null verschieden ist (§. 85); *Lagrange* gebührt das Verdienst, durch Einführung neuer Principien in die Zahlentheorie diese Schwierigkeit zuerst vollständig überwunden zu haben, und diese Principien sind später in hohem Grade verallgemeinert*). Wir wollen deshalb hier noch einen Beweis der Lösbarkeit der Pell'schen Gleichung

---

*) Vergl. drei Abhandlungen von *Dirichlet* in den Monatsberichten der Berliner Akademie vom October 1841, April 1842, März 1846; ferner die Comptes rendus der Pariser Akademie 1840, T. X, p. 286—288. — Vergl. *P. Bachmann: De unitatum complexarum theoria.* 1864.

mittheilen, welcher im Wesentlichen auf derselben Grundlage beruht.

Das Fundament dieses Beweises beruht auf der Thatsache, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche, abgesehen vom Vorzeichen,

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

ist; man überzeugt sich hiervon leicht, wenn man aus der Theorie der Kettenbrüche den Satz entlehnt, dass jeder Näherungswerth $x : y$, den man durch Entwicklung einer Grösse ω in einen Kettenbruch erhält, um weniger als y^{-2} von ω verschieden ist; nimmt man also $\omega = \sqrt{D}$, so giebt es, da $\sqrt{D}$ irrational ist, unendlich viele solche Zahlenpaare x, y von der Beschaffenheit, dass, abgesehen vom Vorzeichen,

$$\frac{x}{y} - \sqrt{D} < \frac{1}{y^2}, \text{ also } x - y\sqrt{D} = \frac{\delta}{y}$$

ist, wo δ einen positiven oder negativen echten Bruch bedeutet; hieraus folgt

$$x + y\sqrt{D} = \frac{\delta}{y} + 2y\sqrt{D},$$

und durch Multiplication

$$x^2 - Dy^2 = \frac{\delta^2}{y^2} + 2\delta\sqrt{D} < 1 + 2\sqrt{D}.$$

Um aber Nichts aus der Theorie der Kettenbrüche zu entlehnen, wollen wir diesen Satz noch auf einem andern und zwar ganz einfachen Wege beweisen. Es sei m irgend eine positive ganze Zahl, so legen wir der Zahl y der Reihe nach die $m + 1$ Werthe

$$0, 1, 2 \ldots (m-1), m$$

bei, und bestimmen für jeden dieser Werthe die zugehörige ganze Zahl x durch die Bedingung

$$0 \leqq x - y\sqrt{D} < 1,$$

welche offenbar jedesmal durch eine, und nur durch eine ganze Zahl x erfüllt wird. Theilen wir nun das Intervall von 0 bis 1 in m gleiche Intervalle, welche durch die Werthe

$$\frac{0}{m},\ \frac{1}{m},\ \frac{2}{m} \cdots \frac{m-1}{m},\ \frac{m}{m}$$

begrenzt werden, so muss, da die Anzahl $m+1$ der Zahlenpaare x, y grösser ist als die Anzahl m dieser Intervalle, wenigstens eines dieser Intervalle mehr als einen, also mindestens zwei von den Werthen $x - y\sqrt{D}$ enthalten, die zwei *verschiedenen* Werthen von y entsprechen. Wir bezeichnen diese beiden Werthe mit $x' - y'\sqrt{D}$ und $x'' - y''\sqrt{D}$; dann ist, abgesehen vom Vorzeichen, ihr Unterschied

$$(x' - x'') - (y' - y'')\sqrt{D} = x - y\sqrt{D} < \frac{1}{m},$$

und da y', y'' ungleich, nicht negativ und $\leqq m$ sind, so ist (abgesehen vom Vorzeichen) auch $y = y' - y'' \leqq m$ und von Null verschieden; mithin wird $x - y\sqrt{D}$ auch $< y^{-1}$ und von Null verschieden, weil $\sqrt{D}$ irrational ist. Hieraus folgt aber, wie oben, dass

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

und von Null verschieden wird.

Dass nun aber auch unendlich viele solche Zahlenpaare x, y existiren, ergiebt sich leicht; sind nämlich schon beliebig viele solche Zahlenpaare x, y gefunden, so kann man immer die ganze Zahl m so gross nehmen, dass m^{-1} kleiner wird als der kleinste der bisher gefundenen Werthe $x - y\sqrt{D}$; für diese Zahl m erhält man aber auf die angegebene Weise wieder ein Zahlenpaar x, y von der Beschaffenheit, dass $x - y\sqrt{D} < m^{-1}$ und folglich auch kleiner als alle früher gefundenen Werthe $x - y\sqrt{D}$ wird, woraus folgt, dass dieses Zahlenpaar x, y von den frühern verschieden ist; mithin ist die Anzahl dieser Zahlenpaare unbegrenzt.

§. 142.

Mit Hülfe dieses Resultates, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche der absolute Werth von $x^2 - Dy^2 < 1 + 2\sqrt{D}$ und von Null verschieden wird, lässt sich nun leicht beweisen, dass die Gleichung $t^2 - Du^2 = 1$ immer in ganzen Zahlen t, u lösbar ist, und zwar so, dass u von Null verschieden ausfällt.

Da die Anzahl der ganzen Zahlen, welche abgesehen vom Vorzeichen $< 1 + 2\sqrt{D}$ sind, endlich ist, so muss der Ausdruck $x^2 - Dy^2$ für unendlich viele Zahlenpaare x, y einer und derselben (von Null verschiedenen) Zahl k gleich werden; da ferner die Anzahl der verschiedenen Paare von Resten α, β, welche zwei Zahlen x, y (mod. k) lassen können, endlich, nämlich $= k^2$ ist, so leuchtet ebenso ein, dass mindestens ein solches Restsystem α, β unendlich oft auftreten muss, dass also unter den unendlich vielen Zahlenpaaren x, y, für welche $x^2 - Dy^2 = k$ wird, auch wieder unendlich viele Paare x, y sich finden müssen, in welchen $x \equiv \alpha$, $y \equiv \beta$ (mod. k) ist, wo α, β zwei bestimmte Reste bedeuten. Sind nun x', y' und x'', y'' irgend zwei solche Zahlenpaare, d. h. ist gleichzeitig

$$x'^2 - Dy'^2 = x''^2 - Dy''^2 = k$$

und

$$x' \equiv x'', \quad y' \equiv y'' \text{ (mod. } k\text{)},$$

so kann man

$$(x' - y'\sqrt{D})(x'' + y''\sqrt{D}) = k(t + u\sqrt{D})$$

setzen, wo t, u *ganze* Zahlen bedeuten, die offenbar der Gleichung

$$t^2 - Du^2 = 1$$

genügen; und zwar dürfen wir annehmen, dass u von Null verschieden ist; denn aus $u = 0$, $t = \pm 1$ ergiebt sich vermöge der obigen Gleichung $x' - y'\sqrt{D} = \pm(x'' - y''\sqrt{D})$; da aber unendlich viele solche Zahlenpaare x', y' und x'', y'' existiren, so können wir auch immer zwei solche auswählen, dass x'', y'' verschieden von $\pm x'$, $\pm y'$, und folglich u von Null verschieden ausfällt.

Hiermit ist also in der That bewiesen, dass immer eine Lösung t, u der vorstehenden Pell'schen Gleichung existirt, in welcher u von Null verschieden ist.

Hieraus lässt sich dann (wie in §. 85), ebenfalls ohne Hülfe der Theorie der reducirten Formen, zeigen, dass alle Auflösungen t, u sich aus der Gleichung

$$t + u\sqrt{D} = \pm(T + U\sqrt{D})^n$$

ergeben, wo T, U die kleinsten positiven ganzen Zahlen bedeuten, die der Gleichung genügen, und der Exponent n alle positiven und negativen ganzen Zahlen durchläuft. Nur in der einen Beziehung bleibt diese Theorie der Pell'schen Gleichung unvollständig, dass aus ihr keine directe Methode fliesst, diese kleinste positive Auflösung T, U unmittelbar zu finden. Hierzu und ebenso zur Beurtheilung der Aequivalenz zweier Formen und also auch der Darstellbarkeit einer Zahl durch eine Form bleibt die Theorie der reducirten Formen unentbehrlich.