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_0091
LOG Titel: §. 83. Lösung der Pell'schen Gleichung für positive Determinanten in positiven Zahlen durch die Betrachtung der Perioden der reducirten Formen.
LOG Typ: chapter

äquivalent, oder nicht äquivalent. Im erstern Fall ergiebt sich offenbar zugleich eine Substitution, durch welche die eine Form in die andere übergeht (vergl. §. 66).

Beispiel: Die beiden gegebenen Formen seien (713, 60, 5) und (62, 95, 145), welche dieselbe Determinante $D = 35$ haben. Die erste geht durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix}$ in die reducirte Form (5, 5, — 2), die zweite durch die Substitution $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$ in die reducirte Form (— 2, 5, 5) über (§. 76). Diese beiden reducirten Formen gehören aber derselben zweigliedrigen Periode (5, 5, — 2), (— 2, 5, 5) an, und zwar geht die erstere durch die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix}$ in die letztere über. Mithin sind die beiden gegebenen Formen (713, 60, 5) und (62, 95, 145) äquivalent, und da $\begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix}$ die inverse Substitution von $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$ ist, so geht die erstere dieser beiden Formen durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix} \begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix} = \begin{pmatrix} -3, & -5 \\ +41, & +68 \end{pmatrix}$ in die letztere über.

§. 83.

Durch unsere letzten Untersuchungen ist das erste der beiden in §. 59 aufgestellten Hauptprobleme auch für Formen von *positiver* Determinante gelöst; das zweite haben wir in §. 62 auf die Auflösung der unbestimmten Gleichung

$$t^2 - Du^2 = \sigma^2$$

zurückgeführt, und es bleibt daher, um in der Theorie der Formen von positiver Determinante zu demselben Abschluss zu kommen, wie früher für negative Determinanten, nur noch übrig, diese Gleichung für jeden positiven (nicht quadratischen) Werth der Determinante D vollständig aufzulösen. *Fermat* hat diese Gleichung den Mathematikern zuerst vorgelegt, worauf ihre Lösung von dem Engländer *Pell* angegeben wurde; allein obwohl seine Methode die Lösung in jedem Fall wirklich giebt, so lag doch in ihr nicht den Nachweis, dass sie immer zum Ziele führen muss, und dass die Gleichung ausser der evidenten Auflösung $t = \pm \sigma$, $u = 0$ noch andere Auflösungen besitzt. Diese Lücke ist erst von *Lagrange* *) ausgefüllt, und hierin besteht wohl eine der bedeutend-

*) *Solution d'un Problème d'Arithmétique*, Miscellanea Taurinensia, Tom. IV. (Œuvres de Lagrange, publ. par Serret, T. I. 1867. p. 669.) —

sten Leistungen des grossen Mathematikers auf dem Gebiete der Zahlentheorie, da die von ihm zu diesem Zweck eingeführten Principien in hohem Grade der Verallgemeinerung fähig und deshalb auch auf ähnliche höhere Probleme anwendbar sind *).

Wir schlagen hier einen ganz andern Weg ein, der sich den zunächst vorangehenden Untersuchungen unmittelbar anschliesst. Der Zusammenhang zwischen der obigen unbestimmten Gleichung und dem zweiten Hauptproblem in der Theorie der Aequivalenz war folgender. Ist (a, b, c) eine Form von der Determinante D und vom Theiler σ, und ist $\binom{\alpha, \beta}{\gamma, \delta}$ irgend eine eigentliche Substitution, durch welche (a, b, c) in sich selbst übergeht so ist stets

$$\alpha = \frac{t - bu}{\sigma}, \quad \beta = -\frac{cu}{\sigma}, \quad \gamma = \frac{au}{\sigma}, \quad \delta = \frac{t + bu}{\sigma},$$

wo t, u zwei der Gleichung

$$t^2 - Du^2 = \sigma^2$$

genügende ganze Zahlen bedeuten; und umgekehrt, jeder Auflösung t, u der unbestimmten Gleichung entspricht durch die vorstehenden Formeln eine Substitution $\binom{\alpha, \beta}{\gamma, \delta}$, durch welche die Form (a, b, c) in sich selbst übergeht. Wir haben nun durch die letzten Untersuchungen, wie sich gleich zeigen wird, ein Mittel gewonnen, alle Transformationen $\binom{\alpha, \beta}{\gamma, \delta}$ einer reducirten Form von positiver Determinante D in sich selbst direct zu finden, und folglich können wir hieraus auch alle Auflösungen t, u der unbestimmten Gleichung ableiten. Wir schicken der Ausführung dieser Untersuchung noch eine Bemerkung über die Perioden der reducirten Formen voraus.

Wir wissen, dass die Reihe der positiven Zahlen k, welche die Elemente des Kettenbruchs bilden, in den die erste Wurzel ω_0

Sur la solution des problèmes indéterminés du second degré, Mém. de l'Ac. de Berlin T. XXIII. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Elémens d'Algèbre par L. Euler* §§. II, VIII. — Das Verdienst, die tiefe Bedeutung der Pell'schen Gleichung für die allgemeine Auflösung der unbestimmten Gleichungen zweiten Grades zuerst dargethan zu haben, gebührt *Euler*; man vergl.: *De solutione problematum Diophanteorum per numeros integros*, Comm. Petrop. VI. p. 175. *De resolutione formularum quadraticarum indeterminatarum per numeros integros*, Nov. Comm. Petrop. IX. p. 3. *De usu novi algorithmi in problemate Pelliano solvendo*, Nov. Comm. Petrop. XI. p. 28. *Nova subsidia pro resolutione formulae* $axx + 1 = yy$, Opusc. anal. I. p. 310. — Man vergleiche ferner *Gauss: D. A.* artt. 197—202.

*) Siehe Supplement VIII.

einer reducirten Form φ_0 entwickelt wird, eine gerade Anzahl von Gliedern

$$k_0, \; k_1 \ldots k_{2n-1}$$

enthält, nach welchen dieselben Glieder periodisch wiederkehren; und zwar ist diese Anzahl $2n$ die der reducirten Formen, welche mit φ_0 in einer Periode enthalten sind. Wir haben aber oben (§. 79) an einzelnen Beispielen gesehen, dass die Zahlen k aus kleineren Perioden bestehen können; wir fanden z. B. aus der zehngliedrigen Formenperiode der Determinante $D = 13$ folgende Zahlen:

$$\begin{array}{lllll} \delta_0 = +1, & \delta_1 = -6, & \delta_2 = +1, & \delta_3 = -1, & \delta_4 = +1; \\ \delta_5 = -1, & \delta_6 = +6, & \delta_7 = -1, & \delta_8 = +1, & \delta_9 = -1; \end{array}$$

und also

$$k_0 = 1, \quad k_1 = 6, \quad k_2 = 1, \quad k_3 = 1, \quad k_4 = 1;$$

und hierauf wiederholt sich schon dieselbe Reihe

$$k_5 = 1, \quad k_6 = 6, \quad k_7 = 1, \quad k_8 = 1, \quad k_9 = 1.$$

Es ist nun wichtig zu untersuchen, wann dies eintreten kann. Es sei daher $2n$ die Gliederanzahl der Formenperiode und m die Gliederanzahl irgend einer Periode in der Reihe der Zahlen k. Dann ist, indem wir die früheren Bezeichnungen für die Formen und ihre ersten Wurzeln beibehalten, wenn m gerade ist,

$$\omega_m = (k_m, k_{m+1} \ldots) = (k_0, k_1 \ldots)$$

und folglich $\omega_m = \omega_0$, und also auch φ_m identisch mit φ_0 und daher nothwendig m ein Multiplum von $2n$; es existirt also jedenfalls keine kleinere Periode von gerader Gliederanzahl als die der ganzen Formenperiode entsprechende. Ist dagegen m ungerade, so ist $2m$ ebenfalls die Gliederanzahl einer Periode in der Reihe der Zahlen k, und folglich ist nach dem eben Bewiesenen $2m$ ein Multiplum von $2n$, also m mindestens $= n$; der Fall, dass die Periode der Zahlen k kürzer ist als die aus $2n$ Gliedern bestehende Periode der Formen, kann also nur dann eintreten, wenn n eine *ungerade* Zahl ist, indem dann, wie wir ja auch an dem obigen Beispiel sehen, die Periode der Zahlen k aus n Gliedern bestehen kann; es ist dann $\omega_n = -\omega_0$, und also $c_n = -c_0$, $b_n = b_0$, $a_n = -a_0$. Doch muss man sich hüten zu glauben, dass diese Erscheinung jedesmal wirklich eintreten *muss*, wenn n ungerade ist; denn wir haben nur gezeigt, dass sie in diesem Fall allein eintreten *kann*. Für $D = 19$ z. B. sind die beiden Formenperioden sechsgliedrig (§. 79), also ist $n = 3$; aber die Perioden der Zahlen k sind nicht dreigliedrig, sondern sechsgliedrig *).

---

*) Die Erscheinung, dass die Kettenbruch-Entwicklung nur halb so lang ist, als die Periode der Form, wird, wie oben gezeigt ist, nur dann eintreten, wenn die Formen (a, b, c) und $(-a, b, -c)$ äquivalent sind, und man erkennt leicht (aus §. 82), dass sie dann auch stets eintreten muss. Führt man nun die Untersuchung über die Aequivalenz dieser beiden Formen genau ebenso durch wie in §. 62, so erhält man das Resultat: Die Coefficienten einer jeden Substitution $\binom{\lambda, \mu}{\nu, \varrho}$, durch welche eine Form (a, b, c) von der Determinante D und vom Theiler σ in die Form $(-a, b, -c)$ übergeht, sind in den Formeln

$$\lambda = \frac{t - bu}{\sigma}, \quad \mu = \frac{cu}{\sigma}, \quad \nu = \frac{au}{\sigma}, \quad \varrho = -\frac{t + bu}{\sigma} \tag{I}$$

enthalten, wo t, u zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung

$$t^2 - Du^2 = -\sigma^2 \tag{II}$$

Genüge leisten; und umgekehrt, giebt es zwei solche ganze Zahlen t, u, so liefern jene Formeln (I) stets eine Substitution von der angegebenen Beschaffenheit. Die erwähnte Erscheinung wird daher stets und nur dann auftreten, wenn die Gleichung (II) *möglich* ist; tritt sie daher in der Periode irgend einer Form auf, so wird sie auch in allen Perioden derjenigen Formen auftreten, welche zu derselben *Ordnung* gehören (§. 61); ist ferner die Gleichung $t^2 - Du^2 = -1$ möglich, so wird sie bei allen Perioden dieser Determinante D auftreten. Dies ist z. B. stets der Fall, wenn $D = p^{2s+1}$ und p eine positive Primzahl $\equiv 1 \pmod{4}$ ist; denn sind T, U die *kleinsten* positiven Zahlen, welche der Gleichung $T^2 - DU^2 = +1$ genügen (§. 84), so ist T ungerade, U gerade, und

$$\frac{T-1}{2} \cdot \frac{T+1}{2} = D\left(\frac{U}{2}\right)^2;$$

da die beiden Factoren linker Hand relative Primzahlen sind, so ist einer und nur einer von ihnen durch D theilbar; wäre nun $T - 1 = 2Df^2$, $T + 1 = 2g^2$, $U = 2fg$, so wäre $g^2 - Df^2 = +1$, und $f < U$, gegen die Voraussetzung; es muss daher $T - 1 = 2f^2$, $T + 1 = 2Dg^2$, $U = 2fg$, und also $f^2 - Dg^2 = -1$ sein, w. z. b. w. Zugleich leuchtet ein, dass $T + U\sqrt{D} = (f + g\sqrt{D})^2$ ist, was nur ein specieller Fall eines allgemeineren Satzes ist.

Besonders interessante Resultate erhält man, wenn man, falls die Gleichung (II) möglich ist, die Perioden von *ambigen* Formen betrachtet (§. 78). Um uns auf den einfachsten Fall zu beschränken, nehmen wir an, die Gleichung $t^2 - Du^2 = -1$ sei möglich; ist nun λ die grösste in $\sqrt{D}$ enthaltene ganze Zahl, also $\varphi_0 = (1, \lambda, \lambda^2 - D)$ eine reducirte und zugleich ambige Form, deren Periode $2n$ Glieder enthält (§. 79), so muss n ungerade $= 2m + 1$, und $\varphi_n = (-1, \lambda, D - \lambda^2)$, also $\varphi_{2m} = (D - \lambda^2, \lambda, -1)$ sein, und hieraus folgt leicht, dass $\varphi_m = (a, b, -a)$, $\varphi_{3m+1} = (-a, b, a)$, also $D = a^2 + b^2$ ist, wo a ungerade und relative Primzahl zu b ist, weil φ_0 eine ursprüngliche Form der ersten Art ist. Da wir vorhin gesehen haben, dass dieser

Um nun die unbestimmte Gleichung $t^2 - Du^2 = \sigma^2$ zu lösen, in welcher D eine beliebige nicht quadratische positive Zahl, und entweder $D \equiv 0 \pmod{\sigma^2}$, oder $4D \equiv \sigma^2 \pmod{4\sigma^2}$ ist, nehmen wir eine beliebige *reducirte* Form (a, b, c) von der Determinante D und vom Theiler σ. (Dass eine solche stets existirt, leuchtet aus §§. 61, 76 unmittelbar ein.) Wir nehmen ferner, was stets gestattet ist, *a positiv*, und folglich *c negativ* an; dann ist die erste Wurzel ω dieser Form positiv, und folglich

$$\omega = (k_0, \; k_1 \ldots k_{2hn-2}, \; k_{2hn-1}, \; \omega),$$

wo $2n$ die Gliederanzahl der Formenperiode, und h eine beliebige positive ganze Zahl ist. Setzt man nun

$$\frac{\gamma}{\alpha} = (k_0, \; k_1 \ldots k_{2hn-2}); \quad \frac{\delta}{\beta} = (k_0, \; k_1 \ldots k_{2hn-1})$$

d. h. (nach §. 23)

$$\alpha = [k_1 \ldots k_{2hn-2}], \quad \beta = [k_1 \ldots k_{2hn-2}, \; k_{2hn-1}],$$
$$\gamma = [k_0, \; k_1 \ldots k_{2hn-2}], \quad \delta = [k_0, \; k_1 \ldots k_{2hn-2}, \; k_{2hn-1}],$$

so ist nach den schon öfter benutzten Sätzen $\alpha\delta - \beta\gamma = 1$ und

$$\alpha + \beta\omega = [k_1 \ldots k_{2hn-2}, \; k_{2hn-1}, \; \omega]$$
$$\gamma + \delta\omega = [k_0, \; k_1 \ldots k_{2hn-2}, \; k_{2hn-1}, \; \omega]$$

und folglich

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (k_0, \; k_1 \ldots k_{2hn-2}, \; k_{2hn-1}, \; \omega) = \omega,$$

woraus unmittelbar folgt (§. 73), dass die Form (a, b, c) durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in sich selbst übergeht.

Setzt man daher für h der Reihe nach alle positiven ganzen Zahlen 1, 2, 3 ..., so erhält man durch die Zähler und Nenner der Näherungsbrüche vom Range $2hn - 1$ und $2hn$ jedesmal eine entsprechende Transformation $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ der Form (a, b, c) in sich selbst (wenn $n = 1$ ist und $h = 1$ genommen wird, hat man $\alpha = 1$, $\beta = k_1$, $\gamma = k_0$, $\delta = k_0 k_1 + 1$ zu setzen); die vier Coefficienten $\alpha, \beta, \gamma, \delta$ sind immer *positiv*, und da ausserdem mit wachsendem h auch nothwendig die Zähler und Nenner der Näherungsbrüche

Fall stets eintritt, wenn D eine Primzahl $\equiv 1 \pmod 4$ ist, so liegt hierin ein neuer Beweis des Fermat'schen Satzes (§. 68), und zugleich eine directe Methode, die Zerlegung einer solchen Primzahl D in zwei Quadrate aus der Entwicklung von $\sqrt{D}$ in einen Kettenbruch abzuleiten (vergl. *Gauss*: *D. A.* art. 265; *Legendre*: *Théorie des Nombres* 3me éd. Tom. I. §. VII. (52)). Dies Resultat steht in der engsten Beziehung zu der biquadratischen Hülfsgleichung, welche bei der Theilung des Kreises in D gleiche Theile auftritt.

beständig wachsen, so entsprechen zwei verschiedenen Werthen von h auch zwei verschiedene Substitutionen $\binom{\alpha,\ \beta}{\gamma,\ \delta}$.

Umgekehrt wollen wir nun zeigen, dass man auf diese Weise *alle* die Transformationen $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ der Form (a, b, c) in sich selbst erhält, in denen die vier Coefficienten α, β, γ, δ sämmtlich *positiv* sind. Denn es sei $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ eine solche Substitution, so ist (§. 73)

$$\alpha\delta - \beta\gamma = 1 \text{ und } \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

also auch

$$\beta\omega^2 + (\alpha - \delta)\,\omega - \gamma = 0,$$

und zwar müssen dieser quadratischen Gleichung beide Wurzeln der Gleichung genügen. Da nun die eine zwischen 1 und $+\infty$, die andere zwischen -1 und 0 liegt, so muss die linke Seite dieser Gleichung für $\omega = 1$ negativ, für $\omega = -1$ positiv ausfallen; hieraus folgt, dass

$$\gamma + \delta > \alpha + \beta, \quad \beta + \delta > \alpha + \gamma$$

ist, wo die Ungleichheitszeichen die Gleichheit ausschliessen. Da wir beweisen wollen, dass $\gamma : \alpha$ und $\delta : \beta$ zwei auf einander folgende Näherungsbrüche eines regelmässigen Kettenbruchs $(k_0, k_1 \ldots)$ sind, so haben wir vor allem zu zeigen, dass $\gamma \geqq \alpha$ und $\delta > \gamma$ ist; dies ergiebt sich in der That aus den vorstehenden Ungleichungen. Wäre nämlich $\delta \leqq \gamma$, so würde aus der zweiten Ungleichung folgen, dass $\alpha < \beta$ und also auch $\alpha\delta < \beta\gamma$ sein müsste, während doch $\alpha\delta = \beta\gamma + 1$ ist; also ist gewiss $\delta > \gamma$. Wäre ferner $\gamma < \alpha$, also $\alpha = \gamma + \varrho$, wo ϱ eine positive ganze Zahl bedeutet, so würde aus der ersten Ungleichheit folgen, dass $\delta > \beta + \varrho$, also auch

$$\alpha\delta - \beta\gamma > (\beta + \gamma)\,\varrho + \varrho^2$$

wäre; dies ist aber wieder unmöglich, da die linke Seite $= 1$, die rechte aber mindestens $= 3$ ist, weil β, γ, ϱ positive ganze Zahlen bedeuten; also ist in der That $\gamma \geqq \alpha$.

Hieraus folgt nun weiter, dass man

$$\frac{\gamma}{\alpha} = (\gamma', m \ldots q, r)$$

setzen kann, wo die Elemente γ', $m \ldots q$, r sämmtlich positiv sind, und zwar kann man es so einrichten, dass ihre Anzahl ungerade ist, weil man eventuell wieder r in $r - 1 + \frac{1}{1}$ auflösen kann. Nehmen wir ferner zunächst an, dass $\alpha > 1$ ist, so ist auch $\gamma > \alpha$ und γ nicht theilbar durch α, und folglich enthält der Kettenbruch mindestens drei Elemente. Bilden wir daher den unmittelbar vorausgehenden Näherungsbruch

$$\frac{\varphi}{f} = (\gamma', m \ldots q),$$

so folgt aus $\alpha\varphi - f\gamma = 1$ und $\alpha\delta - \beta\gamma = 1$, dass man wieder $\beta = f + \alpha\beta'$, $\delta = \varphi + \gamma\beta'$ setzen kann, und hierin wird β' eine *positive* ganze Zahl sein. Wäre nämlich $\beta' = 0$, so wäre $\delta = \varphi$, und da φ gewiss $< \gamma$ ist, so wäre $\delta < \gamma$, während doch $\delta > \gamma$ ist; wäre ferner β' negativ, so wäre auch δ negativ, gegen unsere Voraussetzung, dass $\alpha, \beta, \gamma, \delta$ positive ganze Zahlen sind. Es ist daher

$$\frac{\delta}{\beta'} = (\gamma', m \ldots q, r, \beta')$$

und folglich, ähnlich wie früher,

$$\omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (\gamma', m \ldots q, r, \beta', \omega),$$

wo nun die Anzahl der positiven Elemente $\gamma', m \ldots q, r, \beta'$ gerade ist*). In dem bisher ausgeschlossenen Fall $\alpha = 1$ erhält man ein ganz ähnliches Resultat, denn dann ist

$$\omega = \frac{\gamma + (\beta\gamma + 1)\omega}{1 + \beta\omega} = (\gamma, \beta, \omega).$$

Wir erhalten daher für ω stets einen regelmässigen periodischen Kettenbruch

$$\omega = (\gamma', m \ldots q, r, \beta'; \gamma', m \ldots)$$

in welchem die Anzahl der Glieder $\gamma', m \ldots q, r, \beta'$ eine gerade ist. Da nun ein Werth ω nur auf eine einzige Weise in einen regelmässigen Kettenbruch entwickelt werden kann, so müssen die Zahlen $\gamma', m \ldots$ der Reihe nach mit den Zahlen $k_0, k_1 \ldots$ übereinstimmen; und da wir uns oben überzeugt haben, dass jede Periode der Zahlen k, deren Gliederzahl gerade ist, entweder mit der Reihe der den sämmtlichen $2n$ Formen entsprechenden Zahlen k identisch ist oder aus einer mehrmaligen Wiederholung dieser kleinsten Periode von gerader Gliederanzahl besteht, so ist also $r = k_{2hn-2}$, $\beta' = k_{2hn-1}$, wo h irgend eine positive ganze Zahl bezeichnet, und folglich

---

*) Dasselbe ergiebt sich auch unmittelbar daraus, dass die grössten in den Brüchen $\gamma : \alpha$, $\beta : \alpha$ enthaltenen ganzen Zahlen γ', β' zufolge der obigen Ungleichungen positiv sind (vergl. §. 81).