Mathematische Mittheilungen

von

A. Meyer.

III. Ueber eine Eigenschaft der Pell'schen Gleichung.

Den Satz, um welchen es sich handelt, habe ich zwar bereits in meiner Dissertation (1871) aufgestellt*) und zum Beweise einer Eigenschaft indefiniter ternärer quadratischer Formen benutzt. Indessen habe ich mich damals auf Betrachtung ungerader Zahlen beschränkt. Wenn ich jetzt wieder auf denselben Gegenstand zurückkomme, so geschieht es nicht bloss um jene Beschränkung aufzuheben, sondern auch um die früher gegebene Darstellung noch in einigen Punkten zu verbessern. Die Benutzung dieser Erweiterung für die Theorie der ternären Formen behalte ich mir dagegen für eine spätere Gelegenheit vor.

Der zu beweisende Satz lautet folgendermassen:

Ist D eine positive ganze Zahl, 2^σ die grösste in D aufgehende Potenz von 2, $\sigma \leqq 4$, S^2 das grösste in D aufgehende ungerade Quadrat und $D = 2^\sigma S^2 D_1$, so gibt es stets mit $2D$ theilerfremde Zahlen ξ, η von der Beschaffenheit, dass für alle Primzahlen p, q, die den Congruenzen

$$p \equiv \xi,\ q \equiv \eta \pmod{8 S D_1}$$

*) Verwandte Untersuchungen finden sich in Legendre's Théorie des nombres, Art. 46, und in einer Abhandlung von Arndt, Crelle's J. Bd. 31, pag. 343.

genügen, die Pell'sche Gleichung

$$(1) \quad t^2 - p\,q\,D\,u^2 = 1$$

eine Fundamentalauflösung $t = T$, $u = U$ besitzt, für welche weder $T+1$ noch $T-1$ durch pq theilbar ist.

1. Es seien p, q zwei verschiedene in $2D$ nicht aufgehende Primzahlen, ihr Product $pq = a$. Gesetzt, $T \mp 1$ sei durch a theilbar, so kann man setzen, wenn

1) $\sigma = 0$ und je nachdem T ungerade oder gerade ist:

$$a) \quad T = 2a\lambda \pm 1\ ,\ U = 4v$$

$$b) \quad T = a\lambda \pm 1\ ,\ U = v.$$

Im Falle *a)* ergibt sich aus der Gleichung $T^2 - aDU^2 = 1$

$$\lambda(a\lambda \pm 1) = 4Dv^2 = 4S^2 D_1 v^2.$$

Nun sind λ und $a\lambda \pm 1$ relativ prim; somit muss λ von der Form $\delta'\mu^2$ sein, wo δ' und μ bezw. Theiler von D_1 und $2Sv$ sind. Setzt man daher

$$\lambda = \delta'\mu^2,\ D_1 = \delta\delta',\ 2Sv = \mu\nu,$$

so erhält man

$$(\alpha) \qquad \delta\nu^2 - a\delta'\mu^2 = \pm 1.$$

Im Falle *b)* ergibt sich in derselben Weise

$$\lambda(a\lambda \pm 2) = Dv^2 = S^2 D_1 v^2$$

$$\lambda = \delta'\mu^2,\ D_1 = \delta\delta',\ Sv = \mu\nu$$

$$(\beta) \qquad \delta\nu^2 - a\delta'\mu^2 = \pm 2.$$

In den übrigen Fällen ($\sigma > o$) muss T immer ungerade sein. Setzt man demnach

$$T = 2a\lambda \pm 1,$$

so wird

$$4\lambda(a\lambda \pm 1) = 2^\sigma D_1 S^2 U^2.$$

Ist nun

2) $\sigma = 1$, so muss U gerade sein. Es sei $U = 2v$, so wird

$$\lambda(a\lambda \pm 1) = 2 D_1 (Sv)^2,$$

und man wird wieder setzen können

$$\lambda = 2\delta'\mu^2 \text{ oder } = \delta'\mu^2,\ D_1 = \delta\delta',\ Sv = \mu\nu,$$

woraus sich bezw. die Gleichungen ergeben

$$(\alpha) \qquad \delta\nu^2 - 2a\delta'\mu^2 = \pm 1$$

$$(\beta) \qquad \delta(2\nu)^2 - 2a\delta'\mu^2 = \pm 2.$$

3) $\sigma = 2$. U wird wieder gerade $= 2v$ und

$$\lambda(a\lambda \pm 1) = 4 D_1 (Sv)^2.$$

Setzt man, da λ, wenn gerade, durch eine gerade Potenz von 2 theilbar sein muss,

$$\lambda = 4\delta'\mu^2 \text{ oder } = \delta'\mu^2,\ D_1 = \delta\delta',\ Sv = \mu\nu,$$

so ergibt sich bezw.

$$\delta\nu^2 - a\delta'(2\mu)^2 = \pm 1,\ \delta(2\nu)^2 - a\delta'\mu^2 = \pm 1.$$

4) $\sigma > 2$; also

$$\lambda(a\lambda \pm 1) = 2^{\sigma-2} D_1 (SU)^2.$$

Setzt man, je nachdem λ gerade oder ungerade,

$$\lambda = 2^{\sigma-2}\delta'\mu^2 \text{ oder } = \delta'\mu^2,\ D_1 = \delta\delta',\ SU = \mu\nu,$$

so geht die vorige Gleichung bezw. über in

$$\delta\nu^2 - 2^{\sigma-2} a\delta'\mu^2 = \pm 1 \text{ oder } 2^{\sigma-2}\delta\nu^2 - a\delta'\mu^2 = \pm 1.$$

Ist σ gerade, so lassen sich beide Gleichungen in die Form bringen

$$(\alpha) \qquad \delta x^2 - a\delta' y^2 = \pm 1.$$

Ist dagegen σ ungerade, so sind diese Gleichungen bezw. von der Form

$$(\alpha) \qquad \delta x^2 - 2a\delta' y^2 = \pm 1 \ (x = v,\ y = 2^{\frac{\sigma-3}{2}} \mu)$$

$$(\beta) \qquad \delta x^2 - 2a\delta' y^2 = \pm 2 \ (x = 2^{\frac{\sigma-1}{2}} v,\ y = \mu).$$

Aus Vorstehendem ergibt sich also das Resultat:

Jedesmal, wenn $T \mp 1$ durch $a = pq$ theilbar ist, findet eine der Gleichungen statt ($D_1 = \delta\delta'$):

$$(2) \begin{cases} \delta x^2 - a\delta' y^2 = \pm 1 \text{ oder } \pm 2, \text{ wenn } \sigma = 0 \\ \delta x^2 - a\delta' y^2 = \pm 1 \quad \text{„} \quad \sigma > 0 \text{ und gerade} \\ \delta x^2 - 2a\delta' y^2 = \pm 1 \text{ oder } \pm 2 \quad \text{„} \quad \sigma \text{ ungerade.} \end{cases}$$

Lässt sich also durch passende Wahl der Primzahlen p, q bewirken, dass keine dieser Gleichungen stattfinden kann, so kann auch nicht $T \equiv \pm 1$ (mod. pq) sein. Dass für $\sigma \leqq 4$ solche Primzahlen existiren, soll nun nachgewiesen werden.

2. Zunächst betrachte ich von den Gleichungen (2) die folgenden

$$(\alpha_1) \qquad x^2 - aD_1 y^2 = 1,\ x^2 - 2aD_1 y^2 = 1,$$

welche der Annahme $\delta = 1$, $\delta' = D_1$, $T \equiv 1$ (mod. a) entsprechen. Man bestätigt leicht aus den Werthen von x und y, dass dann in allen oben betrachteten Fällen die Gleichungen gelten,

wenn σ gerade:

$$T = 2x^2 - 1,\ 2^{\frac{\sigma}{2}} SU = 2xy,\ T + U\sqrt{aD} = (x + y\sqrt{aD_1})^2;$$

wenn σ ungerade:

$$T = 2x^2 - 1,\ 2^{\frac{\sigma-1}{2}} SU = 2xy,\ T + U\sqrt{aD} = (x + y\sqrt{2aD_1})^2$$

Ist $\sigma = 0, 1$ oder 3, und y durch S theilbar, so wäre diesen Gleichungen zufolge T, U nicht Fundamentalauflösung von (1); somit findet in diesem Fall die Gleichung (α_1) nicht statt.

Ist $\sigma = 2$ oder > 3, so gilt dies nur, so lange als y ausserdem durch $2^{\frac{\sigma}{2}}$ $(2^{\frac{\sigma-1}{2}})$ theilbar ist, was sich für $\sigma = 2$ oder 4 dadurch bewirken lässt, dass man $a \equiv D_1 \pmod 4$ setzt; denn alsdann folgt aus der Gleichung $x^2 - a D_1 y^2 = 1$, dass x ungerade, y durch 4 theilbar sein muss.

Sei jetzt y nicht durch S theilbar. Nun ist aber $x y$ durch S theilbar, somit x wenigstens durch eine in S aufgehende Primzahl s, welche zudem nicht in D_1 enthalten sein kann, wenn eine der Gleichungen (α_1) möglich sein soll. Aus eben diesen Gleichungen folgt dann für das Legendre'sche Symbol bezw.

$$\left(\frac{-aD_1}{s}\right) = +1 \text{ oder } \left(\frac{-2aD_1}{s}\right) = +1.$$

Sind daher $s_1, s_2, \ldots . s_m$ die in S aufgehenden Primzahlen, welche nicht zugleich in D_1 aufgehen, so braucht man nur a so zu bestimmen, dass die Gleichungen

$$(A) \qquad \left(\frac{a}{s_k}\right) = -\left(\frac{-2^{\sigma} D_1}{s_k}\right) \quad (k = 1, 2, 3, \ldots . m)$$

und, wenn $\sigma = 2$ oder 4, ausserdem die Congruenz

$$(A') \qquad a \equiv D_1 \pmod 4$$

erfüllt sind, um die Gleichungen (α_1) unmöglich zu machen, so lange $\sigma \leqq 4$.

3. Um zweitens von den Gleichungen (2) die folgenden

(α_2) $\quad x^2 - a D_1 y^2 = -1$ oder ± 2, $x^2 - 2 a D_1 y^2 = -1$ oder ± 2

unmöglich zu machen, nehme man, wenn $\sigma = 0, 1$ oder 3 ist,

(B) $\quad p \equiv 5$ oder $\equiv q + 4 \pmod 8$, $q \equiv 3 \pmod 4$.

Ist $\sigma = 2$ oder 4, so kommt nur die Gleichung

$$x^2 - a D_1 y^2 = -1$$

in Betracht und es genügt, mit Rücksicht auf (A'), zu setzen

(B') $\quad p \equiv -D_1,\ q \equiv 3 \pmod 4$.

Enthält jedoch D_1 einen Primfactor der Form $4n + 3$, so bedarf es für $\sigma = 2$ oder 4 der Festsetzung (B') nicht, und enthält D_1 einen Primfactor d der Form $8n + 3$ oder $8n + 5$ oder $8n + 7$, so können für $\sigma = 0, 1$ oder 3 ausser den vorigen Annahmen über p und q noch die folgenden getroffen werden

$$p \equiv 1 \text{ oder } q \pmod 8$$

und $\quad q \equiv 5$ oder 7, 3 oder 7, 3 oder 5 $\pmod 8$

je nachdem $\quad d \equiv 3, 5, 7 \pmod 8$.

Da p und q vertauscht werden dürfen, so folgt, dass dann sämmtliche 16 Combinationen $p, q \equiv 1, 3, 5, 7 \pmod 8$ zulässig sind, mit Ausnahme der folgenden vier:

$$p \equiv 1 \text{ oder } d,\ q \equiv 1 \text{ oder } d \pmod 8.$$

Enthält endlich D_1 Primfactoren von wenigstens zwei der Formen $8n + 3, 5, 7$, so sind die Gleichungen (α_2) unmöglich.

4. Es sei ferner D_1 das Product aus n verschiedenen (ungeraden) Primzahlen $d_1, d_2, \ldots . d_n$. Der Kürze wegen möge, wenn σ gerade ist, die Form $\delta x^2 - a\delta' y^2$, und wenn σ ungerade ist, die Form $\delta x^2 - 2a\delta' y^2$ mit $f(\delta)$ bezeichnet werden. Nach obigen Festsetzungen über p und q reducirt sich dann die Aufgabe darauf, p und q weiter so zu wählen, dass wenn $\sigma = 0, 1$ oder 3, keine der

Zahlen ± 1, ± 2, und, wenn $\sigma = 2$ oder 4, keine der Zahlen ± 1 durch eine der $2^n - 1$ Formen $f(\delta)$ dargestellt werden kann, die man erhält, wenn man δ sämmtliche Theiler von D_1, welche > 1 sind, durchlaufen lässt.

Die 2^n Formen $f(\delta)$, inclus. $f(1)$, deren Gesammtheit F heissen mag, sind alle eigentlich primitiv und ambig (formae ancipites). Durch Zusammensetzung zweier Formen $f(\delta)$ und $f(\delta_1)$ entsteht eine Form $f(\delta_2)$, die ebenfalls zum System F gehört, und zwar ist $\delta_2 = \varepsilon^{-2} \delta \delta_1$, wenn ε den grössten gemeinschaftlichen Theiler von δ und δ_1 bezeichnet. Die Formen $f(\delta)$ bilden also eine Gruppe, woraus folgt, dass jeder Combination von quadratischen Charakteren in Bezug auf die Primfactoren $d_1, d_2, \ldots . d_n$, wenn überhaupt, gleichviel Formen in F entsprechen, wie der «Hauptcombination»

$$\left(\frac{f}{d_1}\right) = +1, \left(\frac{f}{d_2}\right) = +1. \ldots\ldots \left(\frac{f}{d_n}\right) = +1,$$

zu welcher z. B. $f(1)$ gehört.

Es soll nun gezeigt werden, dass man die quadratischen Charaktere von a in Bezug auf die Primfactoren von D_1 so wählen kann, dass jeder der 2^n Combinationen dieser Charaktere eine (und somit nur eine) Form des Systems F entspricht (in welchem Falle das System F generisch getrennt heisse), oder, was dasselbe ist, dass der Hauptcombination keine Form von F ausser $f(1)$ angehört. Angenommen nämlich, diese Behauptung sei bewiesen für eine aus $n-1$ verschiedenen ungeraden Primfactoren bestehende Zahl $D'_1 = d_1 d_2 \ldots . d_{n-1}$, so lässt sich zeigen, dass sie auch für $D_1 = d_1 d_2 \ldots . d_{n-1} d_n$ gilt:

Aus dem System F' der 2^{n-1} zu D'_1 gehörigen Formen

$$f'(\delta) = \delta x^2 - a'\delta' y^2 \text{ (bezw. } \delta x^2 - 2a'\delta' y^2)$$

leitet sich das System F ab, indem man in $f'(\delta)$ das eine Mal den Coefficienten von y^2, das andere Mal den Coefficienten von x^2 mit d_n multiplicirt und a' durch a ersetzt, so dass aus jeder Form $f'(\delta)$ der Determinante $a'D'_1$ zwei Formen, $f(\delta)$ und $f(\delta d_n)$, der Determinante aD_1 entstehen. Sind nun, wie der Voraussetzung zufolge möglich ist, die Charaktere von a' in Bezug auf $d_1, d_2, \ldots d_{n-1}$ so bestimmt, dass $f'(1)$ die einzige Form des Systems F' ist, deren Charaktere in Bezug auf $d_1, d_2, \ldots . d_{n-1}$ sämmtlich positiv sind, so setze man

$$(C) \qquad \left(\frac{a}{d_1}\right) = \left(\frac{a'd_n}{d_1}\right), \ \ldots\ldots \left(\frac{a}{d_{n-1}}\right) = \left(\frac{a'd_n}{d_{n-1}}\right).$$

Dann sind die Charaktere der Formen $f(\delta)$ und $f'(\delta)$ in Bezug auf $d_1, \ldots . d_{n-1}$ dieselben, also auch nur für die Form $f(1)$ sämmtlich positiv.

Für die Charaktere der Formen $f(\delta d_n)$ der zweiten Gruppe erhält man

$$\left(\frac{f(\delta d_n)}{d_k}\right) = \left(\frac{f'(\delta)}{d_k}\right)\left(\frac{d_n}{d_k}\right) \quad (k = 1, 2, 3, \ldots n-1).$$

Unter den 2^{n-1} Formen $f'(\delta d_n)$ gibt es nur eine, deren schon fixirte Charaktere alle positiv sind, nämlich die Form $f(\delta_1 d_n) = \delta_1 d_n x^2 - a\delta'_1 y^2$ (bezw. $\delta_1 d_n x^2 - 2a\delta'_1 y^2$), welche derjenigen Form $f'(\delta_1)$ des Systems F' entspricht, für welche

$$\left(\frac{f'(\delta_1)}{d_k}\right) = \left(\frac{d_n}{d_k}\right) \quad (k = 1, 2, 3, \ldots . n-1).$$

Wird nun der noch nicht bestimmte Charakter

$$(C') \qquad \left(\frac{a}{d_n}\right) = -\left(\frac{-\delta'_1}{d_n}\right)$$

gesetzt, so wird $\left(\frac{f(\delta_1 d_n)}{d_n}\right) = -1$ und hat keine dieser 2^{n-1} Formen $f(\delta d_n)$ lauter positive Charaktere in Bezug auf $d_1, d_2, \ldots . d_n$.

Hiemit ist der Satz bewiesen, da er für $D_1 = 1$ evident ist.

Bemerkung. Durch die Festsetzungen *(C)* und *(C')* sind zwar die n Charaktere $\left(\frac{a}{d_k}\right)$ vollständig bestimmt für eine bestimmte Aufeinanderfolge der Factoren d_k; verschiedenen Anordnungen können aber verschiedene Bestimmungen entsprechen, z. B. für

$$D_1 = d_1 \cdot d_2 \cdot d_3\,; \left(\frac{d_2}{d_1}\right) = +1\,, \left(\frac{d_3}{d_1}\right) = -1\,, \left(\frac{d_3}{d_2}\right) = +1\,;$$

$$d_1 \equiv d_2 \equiv d_3 \equiv 3 \pmod 4$$

entspricht den Aufeinanderfolgen

$d_1\, d_2\, d_3$, $d_2\, d_1\, d_3$ die Bestimmung	$\left(\frac{a}{d_1}\right) = -1$,	$\left(\frac{a}{d_2}\right) = -1$,	$\left(\frac{a}{d_3}\right) = +1$
$d_1\, d_3\, d_2$, $d_3\, d_1\, d_2$ „	-1	$+1$	-1
$d_2\, d_3\, d_1$, $d_3\, d_2\, d_1$ „	$+1$	-1	-1.

Aber auch alle übrigen Festsetzungen mit Ausnahme der folgenden

$$\left(\frac{a}{d_1}\right) = \left(\frac{a}{d_2}\right) = \left(\frac{a}{d_3}\right) = -1$$

ertheilen dem System F in diesem Fall lauter verschiedene Gesammtcharaktere.

5. Nach dieser Festsetzung der Charaktere von $a = pq$ bleiben noch die Charaktere einer der Zahlen p, q in

Bezug auf die Primfactoren von D_1 willkürlich. Da jede Form, welche die Zahl $+1$ darstellt, in's Hauptgeschlecht gehört, lässt sich nunmehr $+1$ durch keine der Formen $f(\delta)$, ausser $f(1)$, darstellen. Der letztere Fall, d. h. die Gleichung $f(1) = 1$, ist durch die Festsetzungen *(A)* und *(A')* bereits beseitigt und die Aufgabe darauf reducirt, die Charaktere von p in Bezug auf die Primfactoren von D_1 so zu bestimmen, dass für $\sigma = 0, 1$ oder 3 die Zahlen $-1, \pm 2$, für $\sigma = 2$ oder 4 die Zahl -1 durch keine Form $f(\delta)$ $(\delta > 1)$ dargestellt werden kann.

Enthält D_1 bloss Primfactoren der Form $8n+1$, so kann keine der Zahlen $-1, \pm 2$ durch eine Form $f(\delta)$ $(\delta > 1)$ dargestellt werden; ebenso können die Zahlen $-1, +2, -2$ nicht dargestellt werden, wenn D_1 bezw. bloss Primfactoren der Form $4n+1$, $8n \pm 1$, $8n+2 \pm 1$ enthält.

6. Ist nun $\sigma = 2$ oder 4 und enthält D_1 Primfactoren der Form $4n+3$, so gibt es eine einzige Form $f(\delta)$, deren Charaktere in Bezug auf $d_1, d_2 \ldots d_n$ mit denjenigen von -1 stimmen und diese einzige noch zulässige Gleichung $\delta x^2 - a\delta' y^2 = -1$ wird auch noch unmöglich, wenn man der schon eingeführten Bedingung *(A')* noch die folgende hinzufügt:

$$\left(\frac{\delta}{p}\right) = -\left(\frac{-1}{p}\right) = -(-1)^{\frac{p-1}{2}}.$$

7. Ist $\sigma = 0, 1$ oder 3 und enthält D_1 abgesehen von Primfactoren der Form $8n+1$ nur solche der Form $8n+5$, so fällt die Zahl -1, weil durch keine Form $f(\delta)$ $(\delta > 1)$ darstellbar, ausser Betracht und $+2$ und -2 könnten nur noch durch eine und dieselbe bestimmte Form $f(\delta)$ dargestellt werden. Macht man dann für dieses δ

$$p \equiv 3 + 2\left(\frac{\delta}{p}\right) \text{ (mod. 8)}, \; q \text{ beliebig} \equiv 1, 3, 5, 7 \text{ (mod. 8)}$$

oder $\quad p \equiv q + 2 + 2\left(\frac{\delta}{pq}\right), \; q \equiv 3 \text{ oder } 7 \text{ (mod. 8)},$

so wird diese eine übrig gebliebene Gleichung unmöglich. Zusammen mit der Bedingung in Art. 3, wonach die Combination $p \equiv q \equiv 1$ (mod. 4) ausgeschlossen ist, und wenn man die Vertauschbarkeit von p und q berücksichtigt, gibt dies die Regel:

Von den Werthen $p, q \equiv 1, 3, 5\ 7$ (mod. 8) sind alle diejenigen auszuschliessen, für welche wenigstens eine der Congruenzen stattfindet:

$$p \equiv 3 - 2\left(\frac{\delta}{p}\right), \; q \equiv 3 - 2\left(\frac{\delta}{q}\right), \; pq \equiv 3 - 2\left(\frac{\delta}{pq}\right) \text{ (mod. 8)}.$$

Ist ferner $\sigma = 0$, 1 oder 3 und enthält D_1 abgesehen von Primfactoren der Form $8n+1$ nur Primfactoren (d) der Form $8n+7$ $(8n+3)$, so fällt die Zahl 2 (bezw. -2) ausser Betracht und die Zahlen -1 und -2 $(+2)$ haben mit einer und derselben Form $f(\delta)$ $(\delta > 1)$ gleiche Charaktere in Bezug auf die Primfactoren von D_1. Um dann auch diese letzte Gleichung $f(\delta) = -1$ oder -2 $(+2)$ unmöglich zu machen, schliesse man von den Werthsystemen $p, q \equiv 1, 3, 5, 7$ (mod. 8) alle diejenigen aus, für welche wenigstens eine der Congruenzen (mod. 8) stattfindet:

$$(D) \quad p \equiv \frac{d+1}{2} - \left(\frac{\delta}{p}\right)\frac{d-1}{2}, \; q \equiv \frac{d+1}{2} - \left(\frac{\delta}{q}\right)\frac{d-1}{2}$$

$$pq \equiv \frac{d+1}{2} - \left(\frac{\delta}{pq}\right)\frac{d-1}{2}.$$

In dieser Regel ist auch die vorige (für $d = 8n+5$) mit inbegriffen; auch ist dabei die Bedingung am Schluss von Art. 3 schon berücksichtigt.

8. Ist endlich $\sigma = 0, 1$ oder 3 und enthält D_1 Primfactoren von wenigstens zwei der Formen $8n + 3, 5, 7$, so sind die Gesammtcharaktere der Zahlen $-1, +2, -2$ in Bezug auf die Primfactoren von D_1 unter sich und von denjenigen der Zahl 1 verschieden und somit gibt es drei unter sich und von $f(1)$ verschiedene Formen des Systems F: $f(\delta), f(\delta_1), f(\delta_2)$, denen bezw. dieselben Charaktere zukommen, und es bleibt demnach übrig, die Gleichungen

$$(\gamma) \qquad f(\delta) = -1,\ f(\delta_1) = 2,\ f(\delta_2) = -2$$

unmöglich zu machen. Hier ist $f(\delta_2)$ aus $f(\delta)$ und $f(\delta_1)$ zusammengesetzt, also (Art. 4) $\delta_2 = \varepsilon^{-2}\delta\delta_1$. Zur Abkürzung setze man

$$\left(\frac{\delta}{p}\right) = \vartheta_5(p),\ \left(\frac{\delta_1}{p}\right) = \vartheta_7(p),\ \left(\frac{\delta_2}{p}\right) = \vartheta_3(p),\ (\vartheta_3 = \vartheta_5\vartheta_7);$$

ferner führe man eine Zahl N ein, indem man setzt:

$$N = 1, \text{ wenn } \left(\frac{\delta}{pq}\right) = +1,\ \left(\frac{\delta_1}{pq}\right) = +1$$

$$N = 3, \quad \text{„} \quad \left(\frac{\delta}{pq}\right) = -1,\ \left(\frac{\delta_1}{pq}\right) = -1$$

$$N = 5, \quad \text{„} \quad \left(\frac{\delta}{pq}\right) = +1,\ \left(\frac{\delta_1}{pq}\right) = -1$$

$$N = 7, \quad \text{„} \quad \left(\frac{\delta}{pq}\right) = -1,\ \left(\frac{\delta_1}{pq}\right) = +1,$$

so dass also $N \equiv \left(\frac{\delta}{pq}\right)\left\{3 - 2\left(\frac{\delta_1}{pq}\right)\right\} \pmod 8$,

bezeichne den kleinsten positiven Rest des Products Npq mit r und bestimme den Werth je eines der Symbole $\vartheta_r(p)$ nach folgender Tafel:

I.

$Nq \equiv 1$	3	5	7
$p \equiv 1$	*	-1	-1	-1
3	-1	*	$+1$	$+1$
5	-1	$+1$	*	$+1$
7	-1	$+1$	$+1$	*

d. h. man setze $\vartheta_r(p) = -1$, wenn entweder $p \equiv 1$ oder $Nq \equiv 1$, sonst $\vartheta_r(p) = +1$. Der Asterisk * entspricht dem Symbol $\vartheta_1(p)$ und bedeutet, dass die betreffende Combination unbrauchbar ist.*) Man überzeugt sich nun leicht, dass durch diese Festsetzung jede der Gleichungen (γ) unmöglich gemacht wird.

9. Aus den bisherigen Entwicklungen ergibt sich zur Bestimmung der Zahlen p, q (mod. $8 S D_1$), d. h. der Zahlen ξ, η folgendes Verfahren:

Man gebe den Symbolen $\left(\frac{a}{s_1}\right), \left(\frac{a}{s_2}\right), \ldots \left(\frac{a}{s_m}\right)$ die durch die Gleichungen (A) vorgeschriebenen Werthe und den Symbolen $\left(\frac{a}{d_1}\right), \left(\frac{a}{d_2}\right), \ldots \left(\frac{a}{d_n}\right)$ irgend ein System von Werthen, für welche das System F (Art. 4) generisch getrennt ist. Weiter sind dann nach den verschiedenen oben unterschiedenen Fällen noch folgende Bestimmungen zu treffen:

---

*) Für die Symbole ϑ gelten noch folgende Relationen:

Ist $p_1 \equiv 4 D_1 + p$, $q_1 \equiv 4 D_1 + q$ (mod. $8 D_1$) und haben N_1 und r_1 dieselbe Bedeutung für p_1 und q_1 wie N und r für p und q, so ist $N_1 = N$, $r_1 = r$, $\vartheta_r(p_1) = \left(\frac{-1}{r}\right) \vartheta_r(p)$. Ist ferner $p_1 \equiv 4 D_1 - p$, $q_1 \equiv 4 D_1 - q$ (mod. $8 D_1$), so ist $N_1 = N$, $r_1 = r$, $\vartheta_r(p_1) = \left(\frac{-2}{r}\right) \vartheta_r(p)$.

1) wenn $\sigma = 0, 1$ oder 3 und

a) wenn D_1 bloss Primfactoren der Form $8n+1$ enthält, bestimme man p, q gemäss den Congruenzen *(B)* des Art. 3;

b) wenn D_1 abgesehen von Primfactoren der Form $8n+1$ nur Primfactoren d von einer der drei Formen $8n+3, 5, 7$ enthält, berechne man δ (Art. 7) und schliesse alle Werthsysteme für p, q aus, für welche wenigstens eine der Congruenzen *(D)* stattfindet;

c) wenn D_1 Primfactoren von wenigstens zwei der Formen $8n+3, 5, 7$ enthält, berechne man $\delta, \delta_1, \delta_2$ (Art. 8) und (aus den Werthen der Symbole $\left(\frac{a}{d_k}\right)$ mit Hilfe des quadratischen Reciprocitätsgesetzes $\left(\frac{\delta}{a}\right), \left(\frac{\delta_1}{a}\right)\left(\frac{\delta_2}{a}\right)$, N, wähle für $a = pq$ irgend einen Werth (mod. 8), für welchen die Congruenz $a \equiv N$ (mod. 8) nicht stattfindet, bestimme mittelst Tafel I den Werth von ϑ_r und diesem gemäss p, endlich q (mod. $8SD_1$).

2) wenn $\sigma = 2$ oder 4 und

a) wenn D_1 bloss Primfactoren der Form $4n+1$ enthält, mache man nach Art. 3 *(B')* $p \equiv q \equiv 3$ (mod. 4);

b) wenn D_1 Primfactoren der Form $4n+3$ enthält, bestimme man δ (Art. 6) und mache $pq \equiv D_1$ (mod. 4), $\left(\frac{-\delta}{p}\right) = -1$.

Dass vorstehende Forderungen in der That erfüllt werden können, ist leicht zu übersehen, ergibt sich auch

sofort aus der Anzahl der Werthsysteme $\xi, \eta \pmod{8 S D_1}$, welche denselben genügen. Diese Anzahl soll jetzt noch berechnet werden.

10. Zu diesem Zwecke betrachte ich zunächst folgende Aufgabe:

Die Anzahl $\mathfrak{A}$ derjenigen mit $2 D_1$ theilerfremden Zahlen a eines vollständigen Restsystems in Bezug auf den Modul $8 D_1$ zu bestimmen, für welche die Symbole $\left(\frac{a}{d_1}\right), \left(\frac{a}{d_2}\right), \ldots\ldots \left(\frac{a}{d_n}\right)$ vorgeschriebene Werthe (± 1) haben und für welche

1°) $$a \equiv \frac{d+1}{2} - \left(\frac{\delta}{a}\right) \frac{d-1}{2} \pmod 8 \qquad (D)$$

oder

2°) $$a \equiv \left(\frac{\delta}{a}\right)\left\{3 - 2\left(\frac{\delta_1}{a}\right)\right\} \pmod 8 \qquad (E)$$

ist, wo wie früher δ und δ_1 verschiedene Theiler von D_1 sind, d aber irgend eine ungerade Zahl sein kann.

Aufl: Die Anzahl der Zahlen a eines vollständigen Restsystems mod. $8 D_1$, welche zu $8 D_1$ prim sind und vorgeschriebene quadratische Charaktere in Bezug auf die n Primfactoren von D_1 haben, ist

$$2^{-n} \varphi(8 D_1) = 2^{-n+2} \varphi(D_1) = 2^{-n+2} (d_1 - 1)(d_2 - 1) \ldots\ldots (d_n - 1).$$

1°. Bezeichnet man den Ausdruck $\frac{d+1}{2} - \left(\frac{\delta}{a}\right) \frac{d-1}{2}$ mit N, so ist, wenn $\delta \equiv 1 \pmod 4$, $N \equiv 1$ oder $d \pmod 8$, je nachdem $\left(\frac{a}{\delta}\right) = +1$ oder $= -1$, und es gibt dann unter je vier Werthen $a \equiv 1, 3, 5, 7 \pmod 8$, für welche $\left(\frac{a}{\delta}\right)$ denselben Werth hat, immer genau einen, welcher der Congruenz *(D)* genügt.

Ist $\delta \equiv 3 \pmod 4$ und $\left(\frac{a}{\delta}\right) = +1 (-1)$, so ist $N \equiv 1$ *(d)* oder $\equiv d$ (1) (mod. 8), je nachdem $a \equiv 1$ oder $\equiv 3$ (mod. 4) ist. Ist nun $d \equiv 1 \pmod 4$, so gibt es unter je vier Werthen $a \equiv 1, 3, 5, 7 \pmod 8$, für welche $\left(\frac{a}{\delta}\right)$ denselben Werth hat, wieder genau einen, für welchen $a \equiv N \pmod 8$ ist. Ist dagegen $d \equiv 3 \pmod 4$, so gibt es deren zwei oder keinen, je nachdem $\left(\frac{a}{\delta}\right) = +1$ oder $= -1$. Diese Anzahl ist also gleich

$1 + \left(\frac{a}{\delta}\right)$ od. gleich 1, je nachdem $d \equiv \delta \equiv 3 \pmod 4$ ist oder nicht.

Daher ist bezw. die gesuchte Anzahl

$$\mathfrak{A} = 2^{-n}\left(1 + \left(\frac{a}{\delta}\right)\right)\varphi(D_1) \text{ oder } = 2^{-n}\varphi(D_1).$$

2°. Die linke Seite der Congruenz *(E)* werde wieder mit N bezeichnet und wie früher $\delta\,\delta_1 = \varepsilon^2\delta_2$ gesetzt, so dass

$$N \equiv 3\left(\frac{\delta}{a}\right) - 2\left(\frac{\delta_2}{a}\right) \equiv 3(-1)^{\frac{a-1}{2}\cdot\frac{\delta-1}{2}}\left(\frac{a}{\delta}\right) - 2(-1)^{\frac{a-1}{2}\cdot\frac{\delta_2-1}{2}}\left(\frac{a}{\delta_2}\right) \pmod 8.$$

In folgender Tafel sind die Werthe von N nach den Vorzeichen von $\left(\frac{a}{\delta}\right)$, $\left(\frac{a}{\delta_2}\right)$ und den Resten von $\delta, \delta_2, a \pmod 4$ zusammengestellt. Die erste Zahl gibt den Rest von N (mod. 8) für $a \equiv 1$, die zweite für $a \equiv 3 \pmod 4$.

$\left(\frac{a}{\delta}\right)$	$\left(\frac{a}{\delta_2}\right)$	$\delta \equiv 1,\ \delta_2 \equiv 1$		$\delta \equiv 1,\ \delta_2 \equiv 3$		$\delta \equiv 3,\ \delta_2 \equiv 1$		$\delta \equiv 3,\ \delta_2 \equiv 3$	
+	+	1	1	1	5	1	3	1	7
+	−	5	5	5	1	5	7	5	3
−	+	3	3	3	7	3	1	3	5
−	−	7	7	7	3	7	5	7	1

In der ersten und zweiten Columne (für $\delta \equiv 1$) stimmt von je vier Werthen $a \equiv 1, 3, 5, 7 \pmod 8$, die demselben Werthsystem $\left(\frac{a}{\delta}\right)$, $\left(\frac{a}{\delta_2}\right)$ entsprechen, immer nur je einer mit der Congruenz $a \equiv N \pmod 8$, in der dritten und vierten dagegen (für $\delta \equiv 3$) je zwei oder keiner, je nachdem $\left(\frac{a}{\delta}\right) = +1$ oder $= -1$. Diese Anzahl wird also ausgedrückt durch

1 oder $1 + \left(\frac{a}{\delta}\right)$, je nachdem $\delta \equiv 1$ oder $\equiv 3 \pmod 4$.

Somit ist bezw.

$$\mathfrak{A} = 2^{-n} \varphi(D_1) \text{ oder } = 2^{-n}\left(1 + \left(\frac{a}{\delta}\right)\right) \varphi(D_1).$$

Aus diesen Ausdrücken für $\mathfrak{A}$ lässt sich das Symbol $\left(\frac{a}{\delta}\right)$ noch wegschaffen, wenn man in den Congruenzen *(D)* und *(E)* der Zahl δ ihre frühere Bedeutung (Art. 7 und 8) gibt. Für die Congruenz *(D)* und $d \equiv 3 \pmod 4$ ist $\delta x^2 - a\delta' y^2$ oder $\delta x^2 - 2a\delta' y^2$, je nachdem σ gerade oder ungerade, diejenige Form des generisch getrennten Systems F, deren Charaktere in Bezug auf die Primfactoren von D_1 mit denjenigen der Zahl -1 stimmen. Dasselbe gilt für *(E)*. Daher ist für $\delta \equiv 3 \pmod 4$

$$\left(\frac{\delta}{\delta'}\right) = \left(\frac{-1}{\delta'}\right) \text{ und } \left(\frac{-a\delta'}{\delta}\right) = \left(\frac{-1}{\delta}\right), \text{ bezw. } \left(\frac{-2a\delta'}{\delta}\right) = \left(\frac{-1}{\delta}\right);$$

also

$$\left(\frac{a}{\delta}\right) = \left(\frac{\delta'}{\delta}\right) = (-1)^{\frac{\delta'-1}{2}} \left(\frac{\delta}{\delta'}\right) = +1, \text{ bezw. } \left(\frac{a}{\delta}\right) = \left(\frac{2}{\delta}\right),$$

oder in einer Formel

$$\left(\frac{a}{\delta}\right) = \left(\frac{2}{\delta}\right)^{\sigma};$$

somit

$$\mathfrak{A} = 2^{-n}\left(1 + \left(\frac{2}{\delta}\right)^{\sigma}\right)\varphi(D_1),$$

wenn in *(D)* $d \equiv \delta \equiv 3 \pmod 4$ oder in *(E)* $\delta \equiv 3 \pmod 4$; sonst

$$\mathfrak{A} = 2^{-n}\varphi(D_1).$$

Hieraus folgt, dass die Anzahl der zu $2 S_1 D_1$ theilerfremden Zahlen eines vollständigen Restsystems in Bezug auf den Modul $8 S_1 D_1$ ($S_1 = s_1 s_2 \ldots s_m$), für welche die Symbole $\left(\frac{a}{s_1}\right), \ldots \left(\frac{a}{s_m}\right)$; $\left(\frac{a}{d_1}\right), \ldots \left(\frac{a}{d_n}\right)$ vorgeschriebene Werthe haben und welche den Congruenzen *(D)* und *(E)* bezw. nicht genügen, gleich

$$2^{-m-n}\left(3 - \left(\frac{2}{\delta}\right)^{\sigma}\right)\varphi(S_1 D_1)$$

ist, wenn in *(D)* $d \equiv \delta \equiv 3 \pmod 4$, in *(E)* $\delta \equiv 3 \pmod 4$, sonst gleich

$$2^{-m-n} \cdot 3\,\varphi(S_1 D_1).$$

11. Es bleibt noch übrig, zu jedem (mod. $8 S_1 D_1$) gegebenen a die Anzahl der zugehörigen p (mod. $8 S_1 D_1$) zu berechnen, da durch die p die zugehörigen q (mod. $8 S_1 D_1$) eindeutig bestimmt sind.

Ist a (mod. $8 S_1 D_1$) gegeben, so ist auch die Zahl δ (Art. 7 und 8) bestimmt, also auch $\left(\frac{\delta}{a}\right)$, und es fragt sich im Falle 1 *b)* von Art. 9, welches diejenigen mit $2 S_1 D_1$ theilerfremden Zahlen p seien, für welche keine der Congruenzen

$$p \equiv \frac{d+1}{2} - \left(\frac{\delta}{p}\right)\frac{d-1}{2},\quad q \equiv \frac{d+1}{2} - \left(\frac{\delta}{q}\right)\frac{d-1}{2} \pmod 8$$

stattfindet. Durch diese Congruenzen sind für $\left(\frac{a}{\delta}\right) = +1$, $a \equiv d \pmod 8$ und für $\left(\frac{a}{\delta}\right) = -1$, $a \equiv 1 \pmod 8$ die Werthe $p \equiv 1$ und $p \equiv d \pmod 8$ ausgeschlossen, dagegen kann $\left(\frac{\delta}{p}\right)$ beliebig gleich ± 1 sein. In den übrigen Fällen ist dagegen p beliebig $\equiv 1, 3, 5, 7 \pmod 8$ und $\left(\frac{\delta}{p}\right)$ vorgeschrieben. Hieraus folgt, dass zu jedem Werthe von a im Ganzen $2\,\varphi(S_1 D_1)$ Werthe von p gehören (mod. $8\,S_1 D_1$). Dieselbe Anzahl ergibt sich auch im Falle 1 *c)* von Art. 9. Dann ist nämlich für jeden zulässigen Werth von a die Zahl p beliebig $\equiv 1, 3, 5$ oder $7 \pmod 8$, aber der Werth eines der Symbole $\left(\frac{\delta}{p}\right), \left(\frac{\delta_1}{p}\right), \left(\frac{\delta_2}{p}\right)$ vorgeschrieben. Die übrigen Fälle des Art. 9 bedürfen keiner besondern Discussion. Bezeichnet man die Anzahl der zu D_1 gehörigen generisch getrennten Systeme F (Art. 4) mit ν, so erhält man demnach für die Anzahl Z der gesuchten Werthsysteme von $p, q \pmod{8\,S_1 D_1}$, insofern man je zwei Werthsysteme $p \equiv \xi$, $q \equiv \eta$ und $p \equiv \eta$, $q \equiv \xi \pmod{8\,S_1 D_1}$ als verschieden betrachtet (der Fall $p \equiv q \pmod{8\,D_1}$ kann nicht vorkommen), wenn $\sigma = 2$ oder 4:

$$Z = 2^{-m-n+2}\,\nu\,\varphi^2(S_1 D_1);$$

wenn $\sigma = 0$, 1 oder 3 und D_1 nur Primfactoren der Form $4n+1$ enthält:

$$Z = 3 \cdot 2^{-m-n+1}\,\nu\,\varphi^2(S_1 D_1);$$

wenn $\sigma = 0$, 1 oder 3 und D_1 mindestens einen Primfactor der Form $4n+3$ enthält:

$$Z = 2^{-m-n+1}\left(3\nu - \Sigma\left(\frac{2}{\delta}\right)^{\sigma}\right)\varphi^2(S_1 D_1),$$

wo die Summation $\Sigma\left(\frac{2}{\delta}\right)^{\sigma}$ sich auf alle δ (Art. 7 und 8) erstreckt, welche $\equiv 3 \pmod 4$ sind. Da die Anzahl dieser Summanden höchstens $= \nu$ ist, so ist $3\nu - \Sigma\left(\frac{2}{\delta}\right)^{\sigma} \geqq 2\nu$.

Die Anzahl der Werthepaare $\xi, \eta \pmod{8SD_1}$, deren Existenz der Satz behauptet, beträgt demnach, wenn man zwei Paare ξ, η und η, ξ nicht als verschieden betrachtet, mindestens $2^{-m-n+1}\nu\varphi^2(SD_1)$, wo $\nu \geqq 1$. Nach dem bekannten Satze von der arithmetischen Progression ist damit auch die Existenz unendlich vieler Paare von Primzahlen p und q nachgewiesen, für welche die Pell'sche Gleichung die im Lehrsatze ausgesprochene Eigenschaft besitzt.

Ausser den hier abgeleiteten Werthsystemen $\xi, \eta \pmod{8SD_1}$ gibt es aber im Allgemeinen noch andere, denen dieselbe Eigenschaft zukommt. So ist z. B. die oben zur Vereinfachung der Betrachtungen eingeführte Bedingung, nach welcher den Symbolen $\left(\frac{a}{d_k}\right)$ nur solche Werthe ertheilt werden, für welche das System F generisch getrennt ist, keineswegs nothwendig. Die obigen Vorschriften liefern für $D = 15$ z. B. 128 verschiedene Werthepaare $\xi, \eta \pmod{120}$, während es deren mindestens 240 gibt.