Zur Auflösbarkeit der Gleichung $x^2 - Dy^2 = -1$.

Von *P. Epstein* in Frankfurt a. M.

Während die Fermatsche Gleichung $x^2 - Dy^2 = 1$ für jeden Wert der Diskriminante D lösbar ist, ist dies bekanntlich bei der Gleichung $x^2 - Dy^2 = -1$ nicht der Fall. Zunächst muß D als Teiler von $x^2 + 1$ eine Summe von zwei Quadraten sein, aber diese Bedingung reicht nicht hin, wie schon das Beispiel $D = 34$ zeigt. Eine notwendige und hinreichende Bedingung liefert die Kettenbruchentwicklung von $\sqrt{D}$, nämlich: Die Gleichung ist dann und nur dann lösbar, wenn die primitive Periode des regulären Kettenbruchs für $\sqrt{D}$ eine ungerade Anzahl von Teilnennern besitzt.

Hiermit ist jedoch die Fragestellung nur verschoben. Es bleibt die Frage, welche Zahlen D eine derartige Kettenbruchentwicklung liefern, und dieses Problem ist bis jetzt nicht allgemein gelöst. Einige spezielle Klassen von Zahlen, für die die Gleichung lösbar ist, haben Legendre, Dirichlet u. a. angegeben.

Im folgenden wird ein allgemeiner Satz bewiesen, durch den man alle zulässigen Diskriminanten aufstellen kann, und daraus ein einfaches, zur Zerfällbarkeit in zwei Quadrate hinzukommendes notwendiges Kriterium für die Lösbarkeit der Gleichung abgeleitet.

1. Bei jeder auflösbaren Gleichung $x^2 - Dy^2 = -1$ muß nicht nur D, sondern auch y und y^2 eine Summe von zwei Quadraten sein. Setzt man also

$$y^2 = \alpha^2 + \gamma^2, \quad D = \beta^2 + \delta^2,$$

so wird

$$x^2 + 1 = (\alpha^2 + \gamma^2)(\beta^2 + \delta^2) = (\alpha\beta + \gamma\delta)^2 + (\alpha\delta - \beta\gamma)^2.$$

Diese Gleichung ist befriedigt, wenn $\alpha\delta - \beta\gamma = \pm 1$ ist; dann wird $x = \alpha\beta + \gamma\delta$. Wir haben also den Satz:

Bestimmt man vier Zahlen $\alpha, \beta, \gamma, \delta$ so, daß

$$\alpha^2 + \gamma^2 \text{ ein Quadrat}$$

und

$$\alpha\delta - \beta\gamma = \pm 1 \tag{1}$$

ist, so ist die Gleichung $x^2 - Dy^2 = -1$ lösbar für $D = \beta^2 + \delta^2$.

Verstehen wir unter β, δ ein bestimmtes Lösungspaar der Gleichung (1), so ist jedes andere Paar durch $\alpha m + \beta$, $\gamma m + \delta$ gegeben, und wir sehen:

Die Gleichung $x^2 - Dy^2 = -1$ *ist lösbar für alle Diskriminanten der Schar*

$$D = (\alpha m + \beta)^2 + (\gamma m + \delta)^2, \tag{2}$$

wenn darin $\alpha^2 + \gamma^2$ *ein Quadrat und* $\alpha\delta - \beta\gamma = \pm 1$ *ist.*

2. Wir zeigen nun, daß dieser Satz den allgemeinen Ausdruck für *jede* zulässige Diskriminante liefert. Zu diesem Ende ziehen wir die Kettenbruchentwicklung von $\sqrt{D}$ heran. Sie hat allgemein die Form

$$\sqrt{D} = (a, \overline{q_1, q_2, \ldots, q_n, q_n, \ldots, q_2, q_1, 2a}, \ldots). \tag{3}$$

Man wird alle möglichen zulässigen Diskriminanten erhalten, wenn man sich die Teilnenner $q_1, q_2, \ldots, q_n$ irgendwie gegeben denkt und a so bestimmt, daß D eine ganze Zahl wird. Das ist mit einer leichten Einschränkung bei der Wahl der Teilnenner q_i immer möglich. Es seien $\frac{A_k}{B_k}$ $(k = 1, 2, 3, \ldots, 2n)$ die Näherungsbrüche des symmetrischen Kettenbruchs

$$(q_1, q_2, \ldots, q_n, q_n, \ldots, q_2, q_1);$$

dann ist nach bekannten Sätzen:

$$\begin{gathered} A_{2n} = A_n^2 + A_{n-1}^2, \quad B_{2n-1} = B_n^2 + B_{n-1}^2, \\ A_{2n-1} = B_{2n} = A_n B_n + A_{n-1} B_{n-1}, \\ A_{2n} B_{2n-1} = B_{2n}^2 + 1. \end{gathered} \tag{4}$$

Aus

$$\sqrt{D} = (a, q_1, q_2, \ldots, q_1, a + \sqrt{D})$$

folgt

$$\sqrt{D} = a + \frac{(a + \sqrt{D}) B_{2n} + B_{2n-1}}{(a + \sqrt{D}) A_{2n} + A_{2n-1}} = a + \frac{(a + \sqrt{D}) B_{2n} + B_{2n-1}}{(a + \sqrt{D}) A_{2n} + B_{2n}}$$

und hieraus

$$D = a^2 + \frac{2a B_{2n} + B_{2n-1}}{A_{2n}}. \tag{5}$$

Es ist also a so zu bestimmen, daß

$$\frac{2a B_{2n} + B_{2n-1}}{A_{2n}} = b \tag{6}$$

eine ganze Zahl wird. Ist nun

1) $B_{2n-1} = B_n^2 + B_{n-1}^2$ gerade, so muß $A_{2n} = A_n^2 + A_{n-1}^2$ ungerade sein, sonst wäre nach der letzten Gleichung (4): $B_{2n}^2 \equiv -1 \bmod 4$.

2) Ist B_{2n-1} ungerade, so muß nach (6) ebenfalls A_{2n} ungerade sein. Nach der letzten Gleichung (4) ist dann B_{2n} gerade. Es folgt somit:

Damit der Kettenbruch (3) die Quadratwurzel aus einer ganzen Zahl darstellt, muß jedenfalls $A_{2n} = A_n^2 + A_{n-1}^2$ *ungerade* sein. Dann ist immer $B_{2n} B_{2n-1}$ gerade. Von den Zahlen A_n, A_{n-1} muß also eine gerade, die andere ungerade sein. Das ist aber immer erreichbar, denn wenn es bei vorgegebenen q_i bei dem Kettenbruch

$$\frac{A_n}{B_n} = (q_1, q_2, \ldots, q_n) \tag{7}$$

mit $q_n > 1$ nicht der Fall ist, so braucht man nur den Teilnenner q_n durch die zwei Teilnenner $(q_n - 1, 1)$ zu ersetzen.

Nunmehr lassen sich die ganzzahligen Werte von a und b, welche die Gleichung (6) befriedigen, mit Benutzung der letzten Gleichung (4) leicht angeben. Sie sind

$$\begin{aligned} a &= \tfrac{1}{2} B_{2n} B_{2n-1} + m A_{2n}, \\ b &= \quad B_{2n-1}^2 + 2m B_{2n}, \end{aligned} \tag{8}$$

worin m jede ganze Zahl bedeutet. Hiermit wird also

$$D = (mA_{2n} + \tfrac{1}{2}B_{2n}B_{2n-1})^2 + 2mB_{2n} + B_{2n-1}^2.$$

Die Diskriminante dieser quadratischen Funktion von m ist -4, mithin ist D als eine *Summe von zwei Quadraten* darstellbar. Man findet:

$$D = (\alpha m + \beta)^2 + (\gamma m + \delta)^2,$$

worin

$$\alpha = A_n^2 - A_{n-1}^2, \quad \gamma = 2A_nA_{n-1},$$
$$\beta = \tfrac{1}{2}(B_n^2 - B_{n-1}^2)B_{2n} + 2(-1)^n B_nB_{n-1},$$
$$\delta = B_nB_{n-1}B_{2n} - (-1)^n(B_n^2 - B_{n-1}^2)$$

und

$$\alpha\delta - \beta\gamma = (-1)^n$$

ist. Unter den gemachten Voraussetzungen (A_n und A_{n-1} teilerfremd und eins von ihnen gerade) sind α und γ immer teilerfremd, und es ist

$$\alpha^2 + \gamma^2 = (A_n^2 + A_{n-1}^2)^2 = A_{2n}^2.$$

Damit ist unser Satz bewiesen, der nunmehr in folgender Form ausgesprochen werden kann:

Um die Werte von D zu finden, für welche die Gleichung $x^2 - Dy^2 = -1$ lösbar ist, nehme man zwei teilerfremde positive Zahlen $u > v$ an, von denen eine gerade ist, bestimme die Zahlen

$$\alpha = u^2 - v^2, \quad \gamma = 2uv$$

und mit ihnen β und δ als Lösungen von

$$\alpha\delta - \beta\gamma = \varepsilon = \pm 1.$$

Dann gehört zu jedem Paar β, δ eine zulässige Diskriminante

$$D = \beta^2 + \delta^2,$$

und es sind

$$x = \alpha\beta + \gamma\delta, \quad y = u^2 + v^2$$

Lösungen der Gleichung $x^2 - Dy^2 = -1$.

3. Von jeder so bestimmten Diskriminante D kann man auch sogleich den Kettenbruch für $\sqrt{D}$ angeben. Wir nennen $(q_1, q_2, \ldots, q_n)$ den erzeugenden Kettenbruch von $\sqrt{D}$. Dann ist die Kettenbruchentwicklung von $\frac{u}{v} = \frac{A_n}{A_{n-1}}$ der umgekehrte erzeugende Kettenbruch $\frac{u}{v} = (q_n, q_{n-1}, \ldots, q_1)$, und mit ihm kann man dann sofort die Entwicklung von $\sqrt{D}$ hinschreiben.

Zu je zwei Zahlen u, v erhält man zwei Scharen von Diskriminanten, je nachdem man β und δ als Lösungen der Gleichung $\alpha\delta - \beta\gamma = +1$ oder $\alpha\delta - \beta\gamma = -1$ bestimmt. Dies hängt damit zusammen, daß man den Kettenbruch für $\frac{u}{v}$ entweder in der Form

$$\frac{u}{v} = (q_n, q_{n-1}, \ldots, q_1) \text{ mit } q_1 > 1$$

oder in der Form

$$\frac{u}{v} = (q_n, q_{n-1}, \ldots, q_1 - 1, 1)$$

ansetzen kann.

Beispiel. $u = 3$, $v = 2$, also $\alpha = 5$, $\gamma = 12$.

1) $\alpha\delta - \beta\gamma = 1$

$$\beta = 2 + 5m, \quad \delta = 5 + 12m$$
$$D = (5m + 2)^2 + (12m + 5)^2$$

$\frac{u}{v} = (1, 2)$ $\quad m = 0 \quad \sqrt{29} = (5, 2, 1, 1, 2, 10, \ldots)$

$\quad m = 1 \quad \sqrt{338} = (18, 2, 1, 1, 2, 36, \ldots)$

$\quad m = 2 \quad \sqrt{985} = (31, 2, 1, 1, 2, 62, \ldots)$

2) $\alpha\delta - \beta\gamma = -1$

$$\beta = 3 + 5m, \quad \delta = 7 + 12m$$
$$D = (5m + 3)^2 + (12m + 7)^2$$

$\frac{u}{v} = (1, 1, 1)$ $\quad m = 0 \quad \sqrt{58} = (7, 1, 1, 1, 1, 1, 1, 14, \ldots)$

$\quad m = 1 \quad \sqrt{425} = (20, 1, 1, 1, 1, 1, 1, 40, \ldots)$.

Für alle diese Diskriminanten hat die Gleichung $x^2 - Dy^2 = -1$ dieselbe Lösung $y = u^2 + v^2 = 13$.

4. Jede mögliche Diskriminante gehört nicht nur zu *einer* Schar von Diskriminanten, sondern sie kommt in unendlich vielen Scharen vor. Man kann nämlich den erzeugenden Kettenbruch bis in die Mitte von irgendeiner Periode ausdehnen und erhält jedesmal eine neue Schar. So gehört z. B. die Diskriminante 5 den folgenden Scharen an:

$(m + 2)^2 + 1$	$y = 1$
$(15m + 2)^2 + (8m + 1)^2$	$y = 17$
$(273m + 2)^2 + (136m + 1)^2$	$y = 305$

usf.

Jede Darstellungsform der Diskriminante liefert ein Lösungspaar der Gleichung, und so erhält man die Gesamtheit der Lösungen.

5. Wir haben gesehen, wie jede Lösung der Gleichung $x^2 - Dy^2 = -1$ mit der Zerlegung von D in zwei Quadrate zusammenhängt, nämlich: Ist $D = \beta^2 + \delta^2$ eine zulässige Diskriminante, so gehören zu jeder Lösung x, y zwei *pythagoreische Zahlen* α, γ so, daß $\alpha\delta - \beta\gamma = \varepsilon = \pm 1$ und $x = \alpha\beta + \gamma\delta$, $y^2 = \alpha^2 + \gamma^2$ ist. Wir brauchen nur positive Werte für $\alpha, \beta, \gamma, \delta$ in Betracht zu ziehen und sagen:

Die Lösung x, y gehört durch (α, γ) zu der Zerlegung (β, δ) von D.

Das hat natürlich nur Bedeutung, wenn sich D auf verschiedene Arten in zwei Quadrate zerlegen läßt, also wenn D nicht Potenz einer Primzahl der Form $4k + 1$ oder das Doppelte einer solchen Potenz ist. Dann aber besteht der Satz:

Für jede zulässige Diskriminante gibt es nur *eine* bestimmte Zerlegung $D = \beta^2 + \delta^2$, zu der sämtliche Lösungen der Gleichung $x^2 - Dy^2 = -1$ gehören. Diese Zerlegung nennen wir die Hauptzerlegung von D.

Zum Beweis dieses Satzes zeigen wir:

1) Eine Lösung x, y gehört zu einer bestimmten Zerlegung von D.

Würde nämlich x, y durch (α, γ) zu der Zerlegung (β, δ) und durch (α', γ') zu einer anderen Zerlegung (β', δ') von D gehören, so wäre

$$x = \alpha\beta + \gamma\delta = \alpha'\beta' + \gamma'\delta',$$
$$\alpha\delta - \beta\gamma = \varepsilon, \ \alpha'\delta' - \beta'\gamma' = \varepsilon',$$
$$D = \beta^2 + \delta^2 = \beta'^2 + \delta'^2.$$

Man findet daraus:

$$D\alpha = \beta x + \delta\varepsilon, \quad D\alpha' = \beta' x + \delta'\varepsilon'$$
$$D\gamma = \delta x - \beta\varepsilon, \quad D\gamma' = \delta' x - \beta'\varepsilon'$$

und weiter

$$\begin{aligned} D(\alpha\beta' - \beta\alpha') &= \varepsilon\delta\beta' - \varepsilon'\beta\delta' = \varepsilon(\delta\beta' - \varepsilon\varepsilon'\beta\delta') \\ D(\gamma\delta' - \delta\gamma') &= \varepsilon'\delta\beta' - \varepsilon\beta\delta' = \varepsilon'(\delta\beta' - \varepsilon\varepsilon'\beta\delta'). \end{aligned} \tag{9}$$

Nun ist

$$D^2 = (\beta^2 + \delta^2)(\beta'^2 + \delta'^2) = (\beta\beta' + \varepsilon\varepsilon'\delta\delta')^2 + (\delta\beta' - \varepsilon\varepsilon'\beta\delta')^2.$$

Aus (9) folgt, daß $\delta\beta' - \varepsilon\varepsilon'\beta\delta'$ durch D teilbar, aber aus der letzten Gleichung, daß es absolut $\leqq D$ ist, also ist entweder $\delta\beta' - \varepsilon\varepsilon'\beta\delta' = 0$ oder $\delta\beta' - \varepsilon\varepsilon'\beta\delta' = \pm D$. Aus $\delta\beta' = \varepsilon\varepsilon'\beta\delta'$ folgt aber, da $(\beta, \delta) = 1$ und $(\beta', \delta') = 1$ ist, $\beta = \beta'$, $\delta = \delta'$. Ist aber $\delta\beta' - \varepsilon\varepsilon'\beta\delta' = \pm D$, so muß nach der letzten Gleichung $\beta\beta' = -\varepsilon\varepsilon'\delta\delta'$, also $\beta = \delta'$, $\delta = \beta'$ sein. In beiden Fällen ergibt sich dieselbe Zerlegung von D.

2) Zwei verschiedene Lösungen gehören zu derselben Zerlegung von D.

Sei nämlich x_0, y_0 die kleinste positive Lösung und sie gehöre durch (α, γ) zu der Zerlegung (β, δ) von D. Aus ihr erhält man alle Lösungen durch

$$x_k + \sqrt{D}y_k = (x_0 + \sqrt{D}y_0)^{2k+1}.$$

Es ist daher

$$\begin{aligned} x_k + \sqrt{D}y_k &= (x_{k-1} + \sqrt{D}y_{k-1})(x_0^2 + Dy_0^2 + 2\sqrt{D}x_0y_0) \\ &= (x_{k-1} + \sqrt{D}y_{k-1})(2Dy_0^2 - 1 + 2\sqrt{D}x_0y_0), \end{aligned}$$

mithin

$$x_k = x_{k-1}(2Dy_0^2 - 1) + 2Dx_0y_0y_{k-1},$$

also ist

$$x_k + x_{k-1} \equiv 0 \bmod D$$

und damit

$$x_0 \equiv -x_1 \equiv x_2 \equiv -x_3 \equiv \cdots \equiv (-1)^k x_k \bmod D.$$

Wir können also schreiben

$$\begin{aligned} x_k &= \eta x_0 + nD \quad (\eta = \pm 1) \\ &= \eta(\alpha\beta + \gamma\delta) + n(\beta^2 + \delta^2) \\ &= (\eta\alpha + n\beta)\beta + (\eta\gamma + n\delta)\delta \end{aligned}$$

oder

$$x_k = \alpha_k\beta + \gamma_k\delta \tag{10}$$

mit

$$\alpha_k = \eta\alpha + n\beta, \quad \gamma_k = \eta\gamma + n\delta$$

und

$$\alpha_k\delta - \gamma_k\beta = \eta(\alpha\delta - \beta\gamma) = \eta\varepsilon = \pm 1. \tag{11}$$

Dann wird

$$\alpha_k^2 + \gamma_k^2 = \alpha^2 + \gamma^2 + 2\eta n(\alpha\beta + \gamma\delta) + n^2(\beta^2 + \delta^2)$$
$$= y_0^2 + 2\eta n x_0 + n^2 D,$$

also

$$D(\alpha_k^2 + \gamma_k^2) = 1 + x_0^2 + 2\eta n x_0 D + n^2 D^2$$
$$= 1 + (\eta x_0 + nD)^2 = 1 + x_k^2 = Dy_k^2,$$

d. h.

$$\alpha_k^2 + \gamma_k^2 = y_k^2. \tag{12}$$

Aus (10), (11), (12) ist ersichtlich, daß in der Tat die Lösung x_k, y_k durch (α_k, γ_k) zur gleichen Zerlegung (β, δ) gehört wie die Lösung x_0, y_0.

Damit ist gezeigt, daß für jede zulässige Diskriminante nur *eine* Zerlegung $D = \beta^2 + \delta^2$ für die Lösung der Gleichung $x^2 - Dy^2 = -1$ in Betracht kommt, und wenn wir, entsprechend den früheren Entwicklungen, unter α immer die ungerade der beiden Zahlen α, γ verstehen, so ist immer δ *ungerade.*

6. Es erhebt sich die Frage, wie man (ohne Kettenbruchentwicklung für $\sqrt{D}$) einer Zerlegung von D ansehen kann, ob sie eine Hauptzerlegung ist. Darüber möge folgendes gesagt werden. Bei einer Hauptzerlegung lassen sich die zugehörigen Zahlen (α, γ) durch $\alpha = u^2 - v^2$, $\gamma = 2uv$ ausdrücken, also ist

$$\delta u^2 - 2\beta uv - \delta v^2 = \varepsilon,$$

somit

$$\varepsilon\delta = (\delta u - \beta v)^2 - Dv^2$$

und

$$-\varepsilon\delta = (\delta v + \beta u)^2 - Du^2.$$

Hieraus sieht man zunächst:

Für jede zulässige Diskriminante mit der Hauptzerlegung $D = \beta^2 + \delta^2$ *sind außer der Gleichung* $x^2 - Dy^2 = -1$ *auch die Gleichungen* $x^2 - Dy^2 = \delta$ *und* $x^2 - Dy^2 = -\delta$ *lösbar.*

7. Weiter aber schließt man aus den obigen Gleichungen:

Für jede zulässige Diskriminante mit der Hauptzerlegung (β, δ) *muß* δ *quadratischer Rest von* D *sein.*

Es ist also jedenfalls die Gleichung $x^2 - Dy^2 = -1$ *nicht lösbar*, wenn bei allen primitiven Zerlegungen von D die ungeraden Bestandteile *quadratische Nichtreste* von D sind.

Beispiel. $D = 205 = 14^2 + 3^2 = 6^2 + 13^2$. Die Zahlen 3 und 13 sind Nichtreste von 5, also auch von 205, mithin ist $x^2 - Dy^2 = -1$ nicht lösbar.

Diese Bedingung für die Nichtlösbarkeit der Gleichung ist hinreichend, aber nicht notwendig. Es gibt Diskriminanten D, für die bei jeder Zerlegung die ungeraden Bestandteile quadratische Reste von D sind und doch die Gleichung $x^2 - Dy^2 = -1$ nicht lösbar ist.

Beispiel. $D = 689 = 13 \cdot 53 = 8^2 + 25^2 = 20^2 + 17^2$. Die Zahlen 17 und 25 sind quadratische Reste von D, aber $x^2 - Dy^2 = -1$ ist nicht lösbar.

8. Auf Grund der letzten Bedingung können wir den folgenden Satz beweisen:

Die Gleichung $x^2 - Dy^2 = -1$ *ist nicht lösbar für alle Diskriminanten* $D = 2p$, *wenn* p *eine Primzahl der Form* $8k + 1$ *und in der Zerlegung* $2p = A^2 + B^2$ *die eine Zahl* A *(und damit auch* B*)* $\equiv \pm 3 \bmod 8$ *ist.*

Beweis. Sei $p = a^2 + b^2$, a die ungerade, b die gerade Basis, so ist $A = a + b$, $B = a - b$. Wir zeigen, daß bei den genannten Diskriminanten stets A *quadratischer Nichtrest von* p, also auch von D ist. Zu diesem Zweck ziehen wir die von Gauß[1]) aufgestellten Kongruenzen für die Zahlen a und b heran. Wir setzen

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} = P, \qquad 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{4} = Q.$$

Dann ist

$$2aQ^2 \equiv (-1)^{\frac{p+3}{4}} P, \qquad \pm 2bQ^2 \equiv (-1)^{\frac{p-1}{4}} \bmod p,$$

also in unserem Fall ($p = 8k + 1$)

$$2aQ^2 \equiv -P, \qquad \pm 2bQ^2 \equiv 1,$$

mithin

$$2AQ^2 \equiv \mp (1 \pm P) \bmod p.$$

Nun ist $P^2 \equiv -1$, also $P \equiv \pm i$, also

$$2AQ^2 \equiv \mp (1 \pm i) \bmod p.$$

Hieraus folgt, da $2^{\frac{p-1}{2}} \equiv 1$, $Q^{p-1} \equiv 1$, $(-1)^{\frac{p-1}{2}} \equiv 1$ ist,

$$A^{\frac{p-1}{2}} \equiv (1 \pm i)^{\frac{p-1}{2}} \equiv (\pm 2i)^{\frac{p-1}{4}}$$

oder

$$A^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{8}} 2^{\frac{p-1}{4}} \bmod p. \tag{13}$$

Es ist also der quadratische Restcharakter von A zurückgeführt auf den *biquadratischen Restcharakter von* 2. Für diesen gilt aber nach Gauß:

$$2^{\frac{p-1}{4}} \equiv \quad 1 \text{ für die Primzahlen } p = a^2 + b^2 \text{ mit } b \equiv 0 \bmod 8,$$

$$2^{\frac{p-1}{4}} \equiv -1 \text{ für die Primzahlen } p = a^2 + b^2 \text{ mit } b \equiv 4 \bmod 8.$$

Hiermit erhält man

1) für $p = 16m + 1$, $(-1)^{\frac{p-1}{8}} = 1$, wenn $b \equiv 4 \bmod 8$ ist:

$$A^{\frac{p-1}{2}} \equiv -1 \bmod p,$$

2) für $p = 16m + 9$, $(-1)^{\frac{p-1}{8}} = -1$, wenn $b \equiv 0 \bmod 8$ ist:

$$A^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

In beiden Fällen ist also immer A quadratischer Nichtrest, also die Gleichung $x^2 - Dy^2 = -1$ nicht lösbar.

Die Bedingungen unter 1) und 2) sind aber gleichbedeutend mit der im Satz ausgesprochenen Bedingung $A \equiv \pm 3 \bmod 8$, denn

$$\text{für } p = 16m + 1 \text{ ist } a \equiv \pm 1 \bmod 8,$$

$$\text{für } p = 16m + 9 \text{ ist } a \equiv \pm 3 \bmod 8.$$

9. Die hier betrachteten Primzahlen lassen sich noch in anderer Weise einfach charakterisieren. Da sie $\equiv 1 \bmod 8$ sind, sind sie durch die Form $x^2 + 2y^2$ mit geradem y,

[1]) Theoria residuorum biquadraticorum, Commentatio prima = Werke II, S. 65—92.

also in der Form $c^2 + 8d^2$ darstellbar, und nun besteht der Satz, daß *immer und nur für die oben betrachteten Primzahlen d ungerade ist.*

Beweis. Sei also die Primzahl

$$p = a^2 + b^2 = c^2 + 8d^2,$$

so ist immer $b^2 \equiv 0 \bmod 8$, also b durch 4 teilbar. Wir setzen $b = 4b_0$, dann ist

$$a^2 - c^2 = 8(d^2 - 2b_0^2).$$

Ist k der größte gemeinsame Teiler von b_0 und d und sei

$$b_0 = kb_1, \quad d = kd_1,$$

so ist also

$$a^2 - c^2 = 8k^2(d_1^2 - 2b_1^2). \tag{14}$$

Sei 2^n die höchste in k enthaltene Potenz von 2, also

$$k = 2^n k_1 \text{ und } k_1 \text{ ungerade},$$

so muß von den Faktoren $a + c$ und $a - c$ der linken Seite von (14) einer durch k_1 teilbar, der andere zu k_1 relativ prim sein, weil sonst a und b gemeinsame Teiler hätten. Beide Faktoren sind gerade, aber einer von ihnen kann nur durch 2, nicht durch 4 teilbar sein, sonst würde a eine gerade Zahl sein. Mithin kann man bei geeigneter Wahl des Vorzeichens von c ansetzen:

entweder $\quad a + c = 2f, \quad a - c = 2^{2n+2}k_1^2 g$

oder $\quad a + c = 2k_1^2 f, \quad a - c = 2^{2n+2} g,$

und hierin ist f ungerade.

f und g sind Teiler der Form $d_1^2 - 2b_1^2$ mit den relativ primen Zahlen b_1 und d_1, also nach einem bekannten Satz von Lagrange wieder von der Form $x^2 - 2y^2$. Wir setzen daher:

$$\begin{aligned} &a + c = 2(q^2 - 2r^2), \quad && a - c = 2^{2n+2}k_1^2(s^2 - 2t^2) \\ \text{bzw. } &a + c = 2k_1^2(q^2 - 2r^2), && a - c = 2^{2n+2}(s^2 - 2t^2), \end{aligned} \tag{15}$$

und hier muß also q *ungerade* sein.

Ist jetzt

1) $n > 0$, also k und d *gerade* und $b = 4kb_0 \equiv 0 \bmod 8$, so ist nach (15):

$$\begin{aligned} a &= q^2 - 2r^2 + 2^{2n+1}k_1^2(s^2 - 2t^2) \\ \text{bzw. } a &= k_1^2(q^2 - 2r^2) + 2^{2n+1}(s^2 - 2t^2). \end{aligned} \tag{16}$$

Beidesmal ist $a \equiv 1 - 2r^2 \bmod 8$, also

$$a + b \equiv 1 - 2r^2 \equiv \begin{cases} +1 \bmod 8, & \text{wenn } r \text{ gerade} \\ -1 \bmod 8, & \text{wenn } r \text{ ungerade.} \end{cases}$$

Wir sehen, daß für unsere Primzahlen, bei denen $a + b \equiv \pm 3 \bmod 8$ ist, dieser Fall ($b \equiv 0 \bmod 8$ und d gerade) ausscheidet.

Ist aber

2) $n = 0$, also k *ungerade* und $k_1 = k$, so folgt jetzt aus (16):

$$a \equiv 1 - 2r^2 + 2s^2 - 4t^2 \bmod 8. \tag{17}$$

Nun war

$$\begin{aligned} d_1^2 - 2b_1^2 &= (q^2 - 2r^2)(s^2 - 2t^2) \\ &= (qs + 2rt)^2 - 2(qt + rs)^2, \end{aligned}$$

also, da q ungerade ist,

$$d_1^2 - 2b_1^2 \equiv s^2 - 2(t + rs)^2 \bmod 4,$$

mithin

(18) $$d_1 \equiv s \bmod 2, \quad b_1 \equiv t + rs \bmod 2.$$

Es sind zwei Fälle möglich:

α) d_1 *gerade*, also s gerade. Dann ist b_1 ungerade und $b = 4kb_1 \equiv 4 \bmod 8$. Dann ist nach (18) t ungerade und nach (17) $a \equiv -3 - 2r^2 \bmod 8$, also $a + b \equiv 1 - 2r^2 \bmod 8$. Das ist dieselbe Kongruenz wie vorhin, und auch dieser Fall scheidet für unsere Primzahlen aus.

β) d_1 *ungerade*, also d *ungerade*. Dann ist s ungerade und nach (18) $b_1 \equiv r + t \bmod 2$, also

$$b = 4kb_1 \equiv 4r + 4t \bmod 8.$$

Nach (17) wird $a \equiv 3 - 2r^2 - 4t^2 \bmod 8$, also

$$\begin{aligned} a + b &\equiv 3 - 2r(r-2) - 4t(t-1) \\ &\equiv 3 - 2r(r-2) \bmod 8, \quad \text{folglich} \end{aligned}$$

für gerade r: $\quad a + b \equiv 3 \bmod 8$

für ungerade r: $\quad a + b \equiv -3 \bmod 8$.

Wir erhalten also in der Tat nur in diesem einen Fall, wenn d *ungerade* ist, die Primzahlen der oben betrachteten Art mit $a + b \equiv \pm 3 \bmod 8$, und der Satz ist damit bewiesen.

Hiernach können wir den Satz in 8 über unsere Gleichung in der Form aussprechen:

I. *Die Gleichung* $x^2 - Dy^2 = -1$ *ist nicht lösbar für jede Diskriminante* $D = 2p$, *wenn* p *eine Primzahl der Form* $c^2 + 8d^2$ *mit ungeradem* d *ist.*

In dieser Fassung hat vor mehr als 20 Jahren Herr Brandt, damals Student in Straßburg, den Satz auf Grund einer großen Anzahl von Beispielen als Vermutung ausgesprochen. Ein Beweis konnte damals nicht geführt werden.

10. Für dieselben Primzahlen p gilt aber der weitere Satz:

II. *Die Gleichung* $x^2 - Dy^2 = -1$ *ist nicht lösbar für jede Diskriminante* $D = 2p^2$. Der Beweis ist sogar einfacher als der des vorigen Satzes, da er nicht von den Gaußschen Kongruenzen für die Basen a und b Gebrauch macht. Sei also wie bisher

$$p = a^2 + b^2 \text{ und } a \pm b \equiv \pm 3 \bmod 8.$$

Dann ist $p^2 = (a^2 - b^2)^2 + (2ab)^2$ und

$$\begin{aligned} D = 2p^2 &= (a^2 - b^2 + 2ab)^2 + (a^2 - b^2 - 2ab)^2 \\ &= M^2 + N^2. \end{aligned}$$

Nun ist $b^2 \equiv -a^2 \bmod p$, also $b \equiv \pm ia \bmod p$. Damit wird

$$M \equiv 2a^2(1 \pm i) \bmod p$$

$$M^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} a^{p-1}(1 \pm i)^{\frac{p-1}{2}}.$$

Aber es ist $2^{\frac{p-1}{2}} \equiv 1$, $a^{p-1} \equiv 1$, daher

$$M^{\frac{p-1}{2}} \equiv (1 \pm i)^{\frac{p-1}{2}} \equiv (\pm 2i)^{\frac{p-1}{4}} \quad \text{oder}$$

$$M^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{8}} 2^{\frac{p-1}{4}} \bmod p.$$

Die gleiche Kongruenz gilt für $N^{\frac{p-1}{2}}$, und sie ist dieselbe, wie die oben für $A^{\frac{p-1}{2}}$ gefundene. Daher gelten auch dieselben Folgerungen, d. h. die Gleichung ist in der Tat für die Diskriminante $D = 2p^2$ nicht lösbar.

11. Hieraus folgt aber nun unmittelbar:

III. Ist $p = a^2 + b^2 = c^2 + 8d^2$ eine Primzahl der bisher betrachteten Art, also *d ungerade, so ist die Gleichung* $x^2 - Dy^2 = -1$ *nicht lösbar für alle Diskriminanten* $D = 2p^n$.

Ist nämlich

1) n ungerade $= 2m - 1$, so ist

$$x^2 - Dy^2 = x^2 - 2p(p^{m-1}y)^2 = -1$$

nicht lösbar nach Satz I.

2) n gerade $= 2m$, so ist

$$x^2 - Dy^2 = x^2 - 2p^2(p^{m-1}y)^2 = -1$$

nicht lösbar nach Satz II.

12. Wir geben zum Schluß ein Verzeichnis der hier in Betracht kommenden Primzahlen bis $p = 1009$ und ihrer Zerlegung in $a^2 + b^2$ und $c^2 + 8d^2$.

$$\begin{aligned}
17 &= 1^2 + 4^2 = 3^2 + 8\cdot 1^2 & 449 &= 7^2 + 20^2 = 21^2 + 8\cdot 1^2\\
73 &= 3^2 + 8^2 = 1^2 + 8\cdot 3^2 & 601 &= 5^2 + 24^2 = 23^2 + 8\cdot 3^2\\
89 &= 5^2 + 8^2 = 9^2 + 8\cdot 1^2 & 617 &= 19^2 + 16^2 = 15^2 + 8\cdot 7^2\\
97 &= 9^2 + 4^2 = 5^2 + 8\cdot 3^2 & 641 &= 25^2 + 4^2 = 21^2 + 8\cdot 5^2\\
193 &= 7^2 + 12^2 = 11^2 + 8\cdot 3^2 & 673 &= 23^2 + 12^2 = 5^2 + 8\cdot 9^2\\
233 &= 13^2 + 8^2 = 15^2 + 8\cdot 1^2 & 769 &= 25^2 + 12^2 = 11^2 + 8\cdot 9^2\\
241 &= 15^2 + 4^2 = 13^2 + 8\cdot 3^2 & 929 &= 23^2 + 20^2 = 27^2 + 8\cdot 5^2\\
281 &= 5^2 + 16^2 = 9^2 + 8\cdot 5^2 & 937 &= 19^2 + 24^2 = 17^2 + 8\cdot 9^2\\
401 &= 1^2 + 20^2 = 3^2 + 8\cdot 7^2 & 977 &= 31^2 + 4^2 = 3^2 + 8\cdot 11^2\\
433 &= 17^2 + 12^2 = 19^2 + 8\cdot 3^2 & 1009 &= 15^2 + 28^2 = 19^2 + 8\cdot 9^2.
\end{aligned}$$

Frankfurt a. M., 30. September 1933.

Eingegangen 13. Dezember 1933.