ÜBER EINE DIOPHANTISCHE GLEICHUNG VON RAMANUJAN-NAGELL UND IHRE VERALLGEMEINERUNG

HELMUT HASSE

TADASI NAKAYAMA zum Gedächtnis

Inhalt

In der vorliegenden Arbeit berichte ich über in der Literatur verstreute Ergebnisse zu einer, wie mir scheint, reizvollen und interessanten zahlentheoretischen Fragestellung. Ich verankere diese Fragestellung in der Theorie der imaginär-quadratischen Zahlkörper, gewinne von dort aus einen systematischen Ansatz zur Behandlung, und leite die hauptsächlichsten Ergebnisse nach einer einheitlichen Methode her. Als bescheidene eigene Beiträge haben sich dabei die Kriterien §5, VI und §6, X zu den in der Literatur vorhandenen hinzugesellt.

§1. Einleitung: Die Ramanujan-Nagellsche Gleichung (Basis 2, Diskriminante -7)

1. Ramanujan [1] hat vermutet, dass die diophantische Gleichung

$$x^2 + 7 = 2^{n+2}$$

nur die folgenden fünf Lösungen hat:

$$n = 1, \quad 2, \quad 3, \quad 5, \quad 13,$$
$$x = 1, \quad 3, \quad 5, \quad 11, \quad 181.$$

Received March 23, 1965.

Diese Vermutung wurde erstmalig von Nagell [2] bewiesen.

Diophantische Gleichungen dieser Art, bei denen eine Unbekannte x in rationaler, die andere n in exponentieller Form eingeht, waren meines Wissens bisher nicht untersucht worden, von einem allgemeinen Endlichkeitssatz abgesehen, über den in § 3 zu sprechen sein wird.

Ein Ansatz zur Behandlung der Ramanujan-Nagellschen Gleichung ergibt sich durch Betrachtung im quadratischen Zahlkörper der Diskriminante -7. In ihm lässt sich die Gleichung wie folgt schreiben:

$$2^n = \frac{x^2+7}{2^2} = \omega\bar{\omega} \qquad \text{mit} \qquad \omega = \frac{x+\sqrt{-7}}{2},$$

wobei das Vorzeichen von x offen gelassen sei. Nun besteht in diesem Zahlkörper eindeutige Primzahlzerlegung, und die einzigen Einheiten sind ± 1. Die Primzerlegung der Basis 2 ist:

$$2 = \omega_1\bar{\omega}_1 \qquad \text{mit} \qquad \omega_1 = \frac{1+\sqrt{-7}}{2}.$$

Für eine Lösung der Gleichung ist demnach notwendig und hinreichend:

$$\pm\omega = \omega_1^n$$

bei geeignetem Vorzeichen von x. Setzt man in Basisdarstellung

$$\omega_1^n = \frac{x_n + y_n\sqrt{-7}}{2},$$

so erhält diese Bedingung durch Koordinatenvergleich die rationale Gestalt:

$$y_n = \pm 1 \qquad \text{und dann} \qquad x_n = \pm x.$$

Es soll also n so beschaffen sein, dass $y_n = \pm 1$ wird, und dann findet man das zugehörige x aus $x_n = \pm x$.

2. Die hierbei auftretenden ganzrationalen Koordinaten x_n, y_n der Potenzfolge ω_1^n genügen den linearen Rekursionsformeln zweiter Ordnung:

$$x_{n+2} = x_{n+1} - 2x_n \qquad \text{mit} \qquad x_1 = 1,\ x_0 = 2,$$
$$y_{n+2} = y_{n+1} - 2y_n \qquad \text{mit} \qquad y_1 = 1,\ y_0 = 0.$$

Diese werden in irrationaler Gestalt gelöst durch:

$$x_n = \omega_1^n + \bar{\omega}_1^n, \qquad y_n = \frac{\omega_1^n - \bar{\omega}_1^n}{\sqrt{-7}} = \frac{\omega_1^n - \bar{\omega}_1^n}{\omega_1 - \bar{\omega}_1}.$$

Hier kommt es auf die Folge y_n an. Die Frage lautet, wie gesagt, für welche n in ihr $y_n = \pm 1$ wird.

Rekursive Zahlfolgen zweiter Ordnung vom Typus y_n werden in der Literatur auch als *Lehmersche Zahlfolgen zweiter Art* bezeichnet. Das bekannteste Beispiel ist die *Fibonaccische Zahlfolge* 0, 1, 1, 2, 3, 5, 8, 13, . . . ; sie entspricht der Irrationalität $\varepsilon_1 = \frac{1+\sqrt{5}}{2}$ in der Rolle des obigen $\omega_1 = \frac{1+\sqrt{-7}}{2}$. Während es sich bei ihr um die *Grundeinheit* ε_1 des *reell*-quadratischen Zahlkörpers von $\sqrt{5}$ handelt, ist der hier zugrunde liegende Zahlkörper von $\sqrt{-7}$ *imaginär*-quadratisch, besitzt also nur triviale Einheiten (Einheitswurzeln ± 1). Man kann jedoch die Zahl ω_1 als eine *modifizierte Einheit* in einem Sinne ansehen, der in der Klassen-körpertheorie von Bedeutung geworden ist, bei dem nämlich die Einheitenbedingung—zugeordneter Divisor 1—dadurch gelockert ist, dass der zugeordnete Divisor nur aus festen Primdivisoren—hier aus den Primdivisoren von 2—zusammengesetzt sein soll. Für einen imaginär-quadratischen Zahlkörper, in dem die Primzahl 2 zerlegt ist:

$$2 \equiv \mathfrak{d}\bar{\mathfrak{d}} \text{ mit zwei koujugierten Primdivisoren } \mathfrak{d},\ \bar{\mathfrak{d}},$$

hat die so modifizierte Einheitengruppe bezüglich der durch die rationalen modifizierten Einheiten $-1, 2$ erzeugten Untergruppe den Rang 1, wird nämlich erzeugt durch Hinzunahme der frühesten Potenz von $\mathfrak{d}$, die ein Hauptdivisor ist:

$$\omega_1 \cong \mathfrak{d}^e,$$

wobei der Exponent e ein Teiler der Divisorenklassenzahl h des quadratischen Zahlkörpers ist.

Im Falle des Körpers von $\sqrt{-7}$ ist die Klassenzahl $h = 1$, also der Exponent $e = 1$, und somit $\omega_1 = \frac{1+\sqrt{-7}}{2}$ die einzige irrationale *modifizierte Grundeinheit.*

3. Der von Nagell [2] gegebene Beweis für die Ramanujansche Vermutung erfolgt durch Betrachtung der Binomialentwicklung von

$$\omega_1^n = \left(\frac{1+\sqrt{-7}}{2}\right)^n,$$

oder vielmehr der daraus gebildeten rationalen Entwicklung von

$$y_n = \frac{\omega_1^n - \bar{\omega}_1^n}{\sqrt{-7}}$$

nach Potenzen von 7, und zwar wird diese Entwicklung als Kongruenz nach einer hinreichend hohen Potenz von 7 betrachtet. In erster Näherung hat man

$$y_n \equiv \frac{n}{2^{n-1}} \text{ mod. } 7.$$

Als notwendige Bedingung für $y_n = \pm 1$ entnimmt man daraus

$$n \equiv 1, 2, 3, 5, 13 \text{ mod. } 6 \cdot 7$$

mit

$$y_n \equiv 1, 1, -1, -1, -1, \text{ mod. } 7.$$

Es wird dann in mühsamen Einzelrechnungen gezeigt, dass in jeder dieser fünf Restklassen nur die kleinste positive Zahl n zu $y_n = \pm 1$ führt.

Eine etwas andere Wendung dieses 7-adischen Beweises gaben Skolem-Chowla-Lewis [3]. Sie gehen aus von der Identität

$$\omega_1^3 = 1 - \bar{\omega}_1\sqrt{-7}$$

und arbeiten mit der daraus gebildeten Binomialentwicklung. Im Hinblick auf den speziellen und unorganischen Charakter der benutzten Identität erscheint diese Schlussweise nicht verallgemeinerungsfähig.

Dasselbe gilt auch für einen weiteren Beweis von Shapiro-Slotnick [4], der hier nur erwähnt sei. Erstaunlich an dieser Arbeit ist vor allem, dass auf einem der Zahlentheorie so fernstehendem Gebiet, wie dem dort behandelten der *error-correcting codes*, die Frage nach den Lösungen der Ramanujan-Nagell-schen Gleichung von Bedeutung ist.

Noch anders gingen Browkin-Schinzel [5] vor. Zunächst erhalten sie durch Betrachtung von y_n mod. 2^6 als notwendige Bedingung für $y_n = \pm 1$ die Kongruenz

$$n \equiv 13 \text{ mod. } 2^4, \text{ sofern nur } n \geqq 6.$$

Durch Betrachtung von y_n mod. 17— eine im Körper von $\sqrt{-7}$ träge Primzahl— zeigen sie dann weiter, dass notwendig auch

$$n \equiv 13 \equiv 4 \text{ mod. } 3^2$$

ist; dabei kommt 3^2 als die Ordnung der Restklasse ω_1 mod. 17 bezüglich der Untergruppe der rationalen Restklassen (Index $18 = 2 \cdot 3^2$) herein. Gebraucht wird davon nur

$$n \equiv 1 \text{ mod. } 3.$$

Schliesslich zeigen sie durch Betrachtung von y_n mod. 79 – eine im Körper von $\sqrt{-7}$ zerlegte Primzahl—, dass notweudig auch noch

$$n \equiv 13 \text{ mod. } 3 \cdot 13$$

ist; dabei kommt $3 \cdot 13$ wieder als die Ordnung der Restklasse ω_1 mod. 79 bezüglich der Untergruppe der rationalen Restklassen (Index $78 = 2 \cdot 3 \cdot 13$) herein, Hieraus wird dann mittels der in § 2 allgemein zu besprechenden Teilbarkeitsregeln für die Folge y_n geschlossen, dass für $n \geqq 6$ nur noch die eine weitere Lösung $n = 13$ vorhanden ist. Auch diese Schlussweise, die auf sehr speziellen Verhältnissen beruht, erscheint nicht verallgemeinerungsfähig.

Dagegen hat sich eine geschickte Systematisierung der in Einzelrechnungen zerfallenden Nagellschen Schlussweise, wie sie bald darauf von Chowla-Dunton-Lewis [6] gegeben wurde, als verallgemeinerungsfähig erwiesen. Ich komme darauf in § 5 zurück.

Einen völlig andersartigen Beweis des Nagellschen Satzes gab schliesslich Mordell [7]. Er unterscheidet die drei Fälle

$$n = 3n_0, \quad 3n_0 + 1, \quad 3n_0 + 2$$

und gibt

$$z = 2^{n_0}$$

die Rolle einer neuen Unbekannten, behandelt also die rationale diophantische Gleichung

$$\frac{x^2 + 7}{2^2} = z^3, \quad 2z^3, \quad 2^2 z^3.$$

Im ersten Falle zeigt er im Körper von $\sqrt{-7}$ ganz einfach, dass $\omega = \varphi^3$ (mit dem ω aus 1) nur die Lösungen $\varphi = \pm \omega_1$ hat, so dass notwendig $n_0 = 1$, $n = 3$ ist. In den beiden anderen Fällen schreibt er die Gleichung in der Form

$$x^2 = (2z)^3 - 7 \quad \text{bzw.} \quad (2x)^3 = (2^2 z)^3 - 2^2 \cdot 7$$

und arbeitet demgemäss in den Körpern von $\sqrt[3]{7}$ bzw. $\sqrt[3]{2^2 \cdot 7}$; sie haben beide die Klassenzahl 3, und ihre Grundeinheiten sind

$$2 - \sqrt[3]{7} \quad \text{bzw.} \quad \frac{-1 - \sqrt[3]{2^2 \cdot 7} + \sqrt[3]{2 \cdot 7^2}}{3}.$$

Die einigermassen komplizierten, recht unorganischen Rechnungen, durch die

festgestellt wird, dass notwendig $n = 1$, 13 bzw. $n = 2$, 5 ist, erschienen mir wegen des Heranziehens der kubischen Zahlkörper dem quadratischen Problem nicht adäquat, und das war für mich der Anlass, mich mit dem durch die Ramanujansche Vermutung und ihren Nagellschen Beweis aufgeworfenen Fragenkreis näher zu beschäftigen.

§ 2. Verallgemeinerung auf beliebige negative Diskriminanten $D \equiv 1$ mod. 2^3: Systematischer Ansatz zur Behandlung und erste notwendige Bedingungen für Lösbarkeit und Lösungen

1. Betrachtet wird von nun an die diophantische Gleichung

$$x^2 - D = 2^{m+2}$$

mit einer quadratischen Ringdiskriminate D, die den Bedingungen

$$D \equiv 1 \text{ mod. } 2^3, \qquad D < 0$$

genügt. Die Ringdiskriminante D hängt mit der zugeordneten quadratischen Körperdiskriminante wie folgt zusammen:

$$D = f^2 d \text{ mit } f \text{ prim zu } 2, \qquad d \equiv 1 \text{ mod. } 2^3 \text{ quadratfrei.}$$

Für die Behandlung der zu betrachtenden Gleichung wichtiger ist jedoch die Darstellung ven D in der Form:

$$D = 1 - 2^a A \text{ mit } a \geqq 3, \qquad A \text{ prim zu } 2, \qquad A > 0.$$

Der Zahlring mit der Diskriminante D besteht aus den ganzen Zahlen des Körpers von $\sqrt{d}$ mit rationalem Rest mod. f, gegeben in Basisdarstellung als

$$\frac{x + y\sqrt{D}}{2} = \frac{x + yf\sqrt{d}}{2} \qquad \text{mit} \qquad x \equiv y \text{ mod. } 2.$$

Die Quotienten der mod. f kongruenten Ringzahlen, als Hauptdivisoren betrachtet, bilden die Hauptklasse der Ringklasseneinteilung vom Führer f im Bereich der zu f primen Divisoren des Körpers von $\sqrt{d}$.

In diesem Zahlring lässt sich die zu betrachtende Gleichung wie folgt schreiben:

$$2^m = \frac{x^2 - D}{2^2} = \omega\bar{\omega} \qquad \text{mit} \qquad \omega = \frac{x + \sqrt{D}}{2}.$$

wobei zunächst das Vorzeichen x wieder offen gelassen sei.

Wegen der Bedingung $D \equiv 1 \bmod 2^3$ ist die Primzahl 2 im Körper von $\sqrt{d}$ zerlegt, und zwar in zwei zum Führer f prime, konjugierte Primdivisoren:

$$2 \cong \mathfrak{d}\bar{\mathfrak{d}}$$

Dabei sei $\mathfrak{d}$ von $\bar{\mathfrak{d}}$ durch die Normierungsvorschrift

$$D \equiv -1 \bmod \mathfrak{d}$$

unterschieden. Sei zuerst

$$\mathfrak{d}^e \sim 1 \bmod f$$

im Sinne der beschriebenen Ringklasseneinteilung, wobei e ein Teiler der Ringklassenanzahl h ist, so ist als früheste Potenz $\mathfrak{d}^e$ ein Hauptdivisor im Zahlring mit der Diskriminante D. Dieser Hauptdivisor kann wie folgt angesetzt werden:

$$\mathfrak{d}^e \cong \omega_1 = \frac{x_1 + y_1\sqrt{D}}{2} \text{ mit } x_1 \equiv y_1 \bmod 2^2, \quad y_1 > 0$$

und

$$2^e = \omega_1\bar{\omega}_1 = \frac{x_1^2 - y_1^2 D}{2^2}.$$

Dabei ist $x_1 \equiv y_1 \bmod 2^2$ eine Folge der getroffenen Normierung von z, und $y_1 > 0$ kann durch einen Vorzeichenfaktor an ω_1 erreicht werden.

Wegen der Bedingung $D < 0$ ist die so bestimmte Zahl ω_1, wie schon in § 1, 2 ausgeführt, die einzige irrationale modifizierte Grundeinheit im dortigen Sinne, hier im Zahlring mit der Diskriminante D.

Für eine Lösung der vorgelegten Gleichung sei jetzt das vorher noch offen gelassene Vorzeichen von x durch die Vorschrift

$$x \equiv 1 \bmod 2^2 \quad \text{oder also} \quad \omega \equiv 0 \bmod \mathfrak{d}$$

normiert. Da ω wegen des Koeffizienten 1 bei $\sqrt{D}$ nicht durch 2 teilbar ist, hat man dann $\omega \not\equiv 0 \bmod \bar{\mathfrak{d}}$. Im Hinblick auf $\omega\bar{\omega} = 2^m$ ist somit ω eine Potenz von $\mathfrak{d}$ allein, und zwar die Potenz

$$\omega \cong \mathfrak{d}^m.$$

Auf Grund der Minimalwahl von $\omega_1 \cong \mathfrak{d}^e$ ist dafür notwendig und hinreichend, dass m ein Vielfaches des Exponenten e ist:

$$m = ne \quad \text{und dann} \quad \pm\omega = \omega_1^n.$$

Setzt man in Basisdarstellung

$$\omega_1^m = \frac{x_n + y_n\sqrt{D}}{2},$$

so erhält diese Bedingung durch Koordinatenvergleich die rationale Gestalt:

$$y_n = \pm 1 \quad \text{und dann} \quad x_n = \pm x.$$

Damit ist die Bestimmung aller Lösungen m, x der vorgelegten Gleichung darauf zurückgeführt, diejenigen Vielfachen $m = ne$ des Exponenten e zu ermitteln, für welche die Potenz ω_1^n der modifizierten Grundeinheit die zweite Koordinate $y_n = \pm 1$ hat.

Das ist ganz analog zu dem in § 1, 1 für die spezielle Ramanujan-Nagellsche Gleichung festgestellten Sachverhalt, nur dass dort speziell $e = 1$ ist.

Im folgenden werden die Lösungen der vorgeleten Gleichung nur noch durch Mitteilung von m oder auch nur n mitgeteilt; das zugehörige x bestimmt sich ja dazu nach dem angegebenen Schema.

2. Für die weiteren Untersuchungen über die verbliebene Aufgabe sind folgende beiden allgemeinen Schlussverfahren nützlich.

a) Es gelten die *Teilbakeitsregeln:*

$$n \mid n' \implies y_n \mid y_{n'}$$

und schärfer

$$n = (n', n'') \implies y_n = (y_{n'}, y_{n''}).$$

Das ergibt sich ohne weiteres aus der auf der Hand liegenden Tatsache:

$$y_{n'} \equiv 0 \bmod y_n \iff \omega_1^{n'} \equiv \text{rationale Zahl mod. } y_n f.$$

Auf diese Weise erkennt man sofort, dass für das Vorhandensein einer Lösung notwendig ist:

$$y_1 = 1 \quad \text{(und dann } x_1 \equiv 1 \bmod. 2^2 \text{ normiert)}.$$

Anders gesagt: *Wenn überhaupt eine Lösung $m = ne$ vorhanden sein soll, so muss notwendig für das kleinstmögliche $n = 1$, also $m = e$ eine Lösung vorliegen.*

Dass $n = 1$, also $m = e$ keine Lösung zu sein braucht, zeigt das Beispiel:

$$D \equiv 10 \bmod. 2^4 - 1 \quad \text{(realisiert etwa durch } D = -95),$$

in dem, wie man leicht feststellt, durchweg

$$x^2 - D \equiv 2^{m+2} \mod 2^4 - 1$$

ist. Eine andere Serie solcher Beispiele, unter denen sich nach Dirichlet unendlich viele primzahlige befinden, ist:

$$D \equiv 31,\ 94,\ 121,\ 124,\ 151,\ 199,\ 229,\ 241 \mod 2^8 - 1.$$

Diese Beispiele wurden von Browkin-Schinzel [8] angegeben, eine Arbeit, auf die ich in § 4 noch zurückkommen werde.

b) Analog zu § 1, 2 hat man auch hier *lineare Rekursionsformeln zweiter Ordnung* für die Folgen x_n, y_n. Ich formuliere sie hier gleich *unter der für das Vorhandensein von Lösungen notwendigen Voraussetzung* $y_1 = 1$, *die im folgenden durchweg gemacht wird:*

$$\begin{Bmatrix} x_{n+2} \\ y_{n+2} \end{Bmatrix} = x_1 \begin{Bmatrix} x_{n+1} \\ y_{n+1} \end{Bmatrix} - 2^e \begin{Bmatrix} x_n \\ y_n \end{Bmatrix} \quad \text{mit} \quad \begin{Bmatrix} x_1 = x_1, & x_0 = 2 \\ y_1 = 1, & y_0 = 0 \end{Bmatrix}.$$

Sie beziehen sich auf die Potenzfolge ω_1^n mit

$$\omega_1 = \frac{x_1 + \sqrt{D}}{2}, \qquad \omega_1 \bar{\omega}_1 = \frac{x_1^2 - D}{2^2} = 2^e, \qquad x_1 \equiv 1 \mod 2^2.$$

Entsprechende Formeln bestehen auch für die Potenzfolgen $\omega_1^{2n_0}$, $\omega_1^{2n_0+1}$ mit

$$\omega_1^2 = \frac{x_2 + y_2\sqrt{D}}{2} = \frac{(x_1^2 - 2^{e+1}) + x_1\sqrt{D_1}}{2}.$$

Die auf die zweiten Koordinaten y_2 bezügliche Formel lautet:

$$\text{(R)} \qquad y_{n+4} = (x_1^2 - 2^{e+1}) y_{n+2} - 2^{2e} y_n \quad \text{mit} \quad \begin{Bmatrix} y_2 = x_1, & y_0 = 0 \\ y_3 = x_1^2 - 2^e, & y_1 = 1 \end{Bmatrix}.$$

Gerade diese letztere Rekursionsformel wird im folgenden von ausschlaggebender Bedeutung sein.

3. Die Voraussetzung, dass für $n = 1$ eine Lösung vorliegen soll, bedeutet das Bestehen der Gleichung:

$$x_1^2 - D = 2^{e+2}.$$

Mittels der in 1 eingeführten Darstellung

$$D = 1 - 2^a A \quad \text{mit} \quad a \geqq 3, \quad A \text{ prim zu } 2, \quad A > 0$$

erhält sie die Form:

$$x_1^2 - 1 + 2^a A = 2^{e+2}.$$

Aus dieser Form erkennt man, dass nur die beiden folgenden Fälle möglich sind:

Hauptfall $A > 1$; dann ist $e \geqq a$, $x_1 \not\equiv 1$ (und $\not\equiv -1$).

Grenzfall $A = 1$; dann ist $e = a - 2$, $x_1 = 1$.

Für den Hauptfall folgt das aus der Abschätzung

$$2^{e+2} > 2^a A > 2^{a+1}.$$

Für den Grenzfall folgt es daraus, dass die Gleichung

$$x_1^2 + y_1^2(2^a - 1) = 2^{e+2}$$

ersichtlich zuerst für $e + 2 = a$ eine Lösung hat, nämlich $x_1 = 1$, $y_1 = 1$.

Der Grenzfall entspricht für primzahlige $D = -p$ den Mersenneschen Primzahlen $p = 2^a - 1$. Unter ihn fällt speziell der Ramanujan-Nagellsche Fall $D = -7$; ich nenne ihn im folgenden kurz:

Spezialfall $A = 1$, $a = 3$, $e = 1$, $x_1 = 1$.

Im Grenzfall ist neben der vorausgesetzten Lösung

$$n = 1 \quad \text{mit} \quad y_1 = 1, \quad x_1 = 1$$

nach den Rekursionsformeln aus 2 auch

$$n = 2 \quad \text{mit} \quad y_2 = x_1 = 1, \; x_2 = 1 - 2^{a-1}$$

eine Lösung. Im folgenden wird der Grenzfall stets o h n e Einschluss des Spezialfalls verstanden:

Grenzfall $A = 1$, $a > 3$, $e = a - 2 > 1$ $x_1 = 1$.

4. Mittels der Teilbarkeitsregeln und Rekursionsformeln aus 2 ergeben sich fast unmittelbar die folgenden Tatsachen:

I. Im Hauptfall ist für $y_n = +1$ notwendig $n \equiv 1$ mod. 2.

Beweis. Aus $2 \mid n$ folgte $y_2 \mid y_n$, also für $y_n = \pm 1$ notwendig auch $y_2 = \pm 1$, während doch im Hauptfall $y_2 = x_1 \not\equiv \pm 1$ ist.

II. Im Hauptfall und Grenzfall ist für jede Lösung n notwendig $y_n = +1$, während im Spezialfall, von den beiden Lösungen $n = 1, 2$ mit $y_1, y_2 = +1$ abgesehen, für jede weitere Lösung n notwendig $y_n = (-1)^n$ ist.

Beweis. Nach der Rekursionsformel (R) hat man

$$y_{n+4} \equiv (x_1^2 - 2^{e+1}) y_{n+2} \mod 2^{2e},$$

also sicher

$$y_{n+4} \equiv y_{n+2} \mod 2^2$$

und damit

$$y_n \equiv \left\{ \begin{array}{llll} y_2 \mod 2^2 & \text{für} & n \equiv 0 \mod 2, & n \geqq 2 \\ y_3 \mod 2^2 & \text{für} & n \equiv 1 \mod 2, & n \geqq 3 \end{array} \right\}.$$

Hierin ist aber

$$y_2 = x_1 \equiv +1 \mod 2^2$$

$$y_3 = x_1^2 - 2^e \equiv \left\{ \begin{array}{lll} +1 \mod 2^2 & \text{für} & e > 1 \\ -1 \mod 2^2 & \text{für} & e = 1 \end{array} \right\},$$

woraus man die Behauptungen abliest.

III. Im Grenzfall gibt es nur die beiden trivialen Lösungen $n = 1, 2$ *mit* $y_n = +1$.

Beweis. Für $n \equiv 1 \mod 2$ hat man nach der Rekursionsformel (R) im Grenzfall:

$$y_{n+4} \equiv y_{n+2} \mod 2^{e+1},$$

also

$$y_n \equiv y_3 = 1 - 2^e \mod 2^{e+1} \quad \text{für} \quad n \geqq 3,$$

und daher sicher $y_n \neq 1$ für ungerade $n > 2$.

Für $n \equiv 0 \mod 2$ hat man nach den Teilbarkeitsregeln im Grenzfall:

$n \equiv 0 \mod 4 \Rightarrow y_4 = 1 - 2^{e+1} \mid y_n$, also $y_n \neq 1$,

$n \equiv 2 \mod 4 \Rightarrow y_{n/2} \mid y_n$, wobei nach dem zuvor Gezeigten $y_{n/2} \neq 1$ für $n \geqq 6$, also auch $y_n \neq 1$ für $n \geqq 6$.

Damit hat man $y_n \neq 1$ auch für gerade $n > 2$.

Da nach II nur $y_n = +1$ in Frage kommt, ergibt sich zusammengenommen die Behauptung.

IV. Im Spezialfall ist für jede von den beiden trivialen Lösungen $n = 1, 2$ *verschiedene Lösung notwendig* $n \equiv 1$ *mod.* 2.

Beweis. Für $n \equiv 0 \bmod. 2$ hat man nach der Rekursionsformel (R) im Spezialfall

$$y_{n+4} = (1 - 2^2)y_{n+2} - 2^2 y_n \quad \text{mit} \quad y_2 = 1,\ y_0 = 0.$$

Daraus folgt ersichtlich

$$y_n \equiv 1 - 2^2 \bmod. 2^3 \quad \text{für gerade } n \geqq 4,$$

und daher sicher $y_n \neq \pm 1$ für gerade $n \geqq 4$, woraus sich die Behauptung ergibt.

Nach den damit erhaltenen Ergebnissen I-IV bleiben nur noch zu behandeln:

Hauptfall mit $n \equiv 1$ *mod.* 2, $y_n = +1$,
Spezialfall mit $n \equiv 1$ *mod.* 2, $n \geqq 3$, $y_n = -1$

Das wird in den nachfolgenden §§ 4-6 durch Kongruenzbetrachtungen nach Primzahlpotenzmoduln geschehen, und zwar bieten sich dafür in natürlicher Weise die folgenden dem Problem eigentümlichen Primzahlen an:

die Primzahl 2,
die Primteiler der Diskriminante D,
die Primteiler der kleinsten Lösung x_1 (nur im Hauptfall).

Zuvor wird im folgenden § 3 noch kurz ausgeführt, dass die Lösungsanzahl der betrachteten diophantischen Gleichung auf Grund tiefliegender allgemeiner Sätze aus der Theorie der diophantischen Approximationen jedenfalls endlich ist.

§ 3. Endlichkeit der Lösungsanzahl

Schon Polya [9] hat aus dem *Thue-Siegelschen Satz* gefolgert, dass ganz allgemein für jede ganze Nichtquadratzahl D die rational-exponentiell diophantische Gleichung

$$x^2 - D = p_1^{n_1} \cdots p_r^{n_r}$$

mit gegebenen Primzahlen $p_1, \ldots, p_r$ nur endlich viele Lösungen $x;\ n_1, \ldots, n_r$ besitzt.

Man erhält das am einfachsten aus dem *Siegelschen Endlichkeitssatz* für ganzzahlige Lösungen rationaler diophantischer Gleichungen vom Geschlecht $g \geqq 1$, wobei nur dessen einfach zugänglicher elliptischer Spezialfall $g = 1$ gebraucht wird [10].

Gäbe es nämlich unendlich viele Lösungen $x;\ n_1, \ldots, n_r$, so wären dar-

unter auch unendlich viele mit

$$n_1 \equiv \nu_1, \ \ldots, \ n_r \equiv \nu_r \text{ mod. } 3$$

für mindestens ein System kleinster nicht-negativer Reste $\nu_1, \ldots, \nu_r$ mod. 3. Setzt man dann

$$P = p_1^{\nu_1} \cdots p_r^{\nu_r},$$

so hätte die rationale diophantische Gleichung

$$x^2 - DPy^3$$

vom Geschlecht 1 unendlich viele ganzzahlige Lösungen x, y.

Es ist das übrigens genau dieselbe Zurückfuhrung der gegebenen rational-exponentiellen auf eine rationale diophantische Gleichung, mittels derer Mordell [7] im Ramanujan-Nagellschen Spezialfall die in § 1, **3** geschilderte Bestimmung aller Lösungen durchgeführt hat.

§ 4. Notwendige Bedingung für die Lösungen durch Kongruenzbetrachtung nach Potenzen von 2 (Browkin-Schinzel [8])

Es wird hier für den Hauptfall eine Verschärfung der Bedingung $n \equiv 1$ mod. 2 aus § 2, I hergeleitet. Für den Spezialfall ist eine entsprechende Verschärfung der Bedingung $n \equiv 1$ mod. 2 aus § 2, IV nicht möglich (und im Hinblick auf den Nagellschen Satz, der in § 5, VII durch Kongruenzbetrachtung nach Potenzen von 7 bewiesen werden wird, auch nicht nötig).

V. Für die im Hauptfall allein in Frage kommenden Lösungen

$$n \equiv 1 \ mod.\ 2 \quad mit \quad y_n = +1$$

besteht (von der vorausgesetzten Lösung $n = 1$ abgesehen) notwendig die Kongruenz

$$n \equiv \frac{A}{A'} \ mod.\ 2^e \quad mit \quad A' = A - 2^{e-a+1}.$$

Beweis. Aus der Rekursionsformel (R) in § 2, **2** folgt die auch im Beweis von § 2, II zugrunde gelegte Kongruenz:

$$y_{n+4} \equiv (x_1^2 - 2^{e+1}) y_{n+2} \text{ mod. } 2^{2e}.$$

Hier lassen wir die Rekursion ablaufen. Für $n \equiv 1$ mod. 2 und $n \geqq 3$ ergibt das:

$$y_n \equiv (x_1^2 - 2^{e+1})^{\frac{n-3}{2}} y_3 = (x_1^2 - 2^{e+1})^{\frac{n-3}{2}} (x_1^2 - 2^e) \equiv (x_1^2 - 2^{e+1})^{\frac{n-1}{2}} + (x_1^2)^{\frac{n-3}{2}} 2^e \bmod. 2^{2e}.$$

Nach der vorausgesetzten, der Lösung $n = 1$ entsprechenden Gleichung

$$x_1^2 - 1 + 2^a A = 2^{e+2}$$

hat man hierin für die Basis des ersten Gliedes rechterhand:

$$x_1^2 - 2^{e+1} = 1 - 2^a A + 2^{e+1} = 1 - 2^a A',$$

wobei wegen $e \geqq a$ mit A auch A' prim zu 2 ist, und hieraus ergibt sich wegen $e \geqq a$ für die Basis des zweiten Gliedes rechterhand:

$$x_1^2 \equiv 1 \bmod. 2^a.$$

Zusammengenommen wird damit:

$$y_n \equiv (1 - 2^a A')^{\frac{n-1}{2}} + 2^e \bmod. 2^{e+a}.$$

Auf der rechten Seite dieser Kongruenz ist das erste Glied jedenfalls $\equiv 1$ mod. 2^a. Ersichtlich kann nur dann $y_n = 1$ sein, wenn die dyadische Ordnungszahl des nach Abspaltung von 1 verbleibenden Restes mit der dyadischen Ordnungszahl des zweiten Gliedes übereinstimmt und sich überdies dieser Rest mit dem zweiten Glied mod. 2^{e+a} annulliert. Setzt man

$$\frac{n-1}{2} = 2^\nu n_0 \quad \text{mit} \quad \nu \geqq 0,\ n_0 \text{ prim zu } 2,$$

so lautet jene Restabsp ltung folgendermassen:

$$(1 - 2^a A')^{\frac{n-1}{2}} \equiv 1 - 2^{a+\nu} n_0 A' \bmod. 2^{2a+\nu-1},$$

wie man leicht durch vollständige Induktion bestätigt. Demmach ist für $y_n = 1$ zunächst notwendig, dass

$$a + \nu = e$$

ist. Da dann $2a + \nu + 1 = e + a - 1$ ist, wird jedenfalls

$$y_n \equiv 1 - 2^{a+\nu} n_0 A' + 2^e \equiv 1 - 2^{a-1}(n-1)A' + 2^e \bmod. 2^{e+a-1}.$$

Demnach ist für $y_n = 1$ weiter notwendig, dass die Kongruenz

$$(n-1)A' \equiv 2^{e-a+1} \bmod. 2^e$$

besteht, und dies läuft nach der Definition von A' auf die Behauptung hinaus.

§ 5. Notwendige Bedingung für die Lösung durch Kongruenzbetrachtung nach Potenzen eines Primteilers von D (Eigene Untersuchung)

1. Die nach § 2, 4 noch zu betrachtenden Fälle:

Hauptfall mit $n \equiv 1 \bmod 2$, $y_n = +1$,

Spezialfall mit $n \equiv 1 \bmod 2$, $n \geqq 3$, $y_n = -1$

werden hier simultan behandelt.

Sei p ein Primteiler von D; es ist $p \neq 2$ wegen $D \equiv 1 \bmod 2^3$ und p kein Teiler von x_1 im Hinblick auf die vorausgesetzte Gleichung $x_1^2 - D = 2^{e+2}$. Man hat dann in erster Näherung:

$$\omega_1^n = \left(\frac{x_1 + \sqrt{D}}{2}\right)^n \equiv \left(\frac{x_1}{2}\right)^n + n\left(\frac{x_1}{2}\right)^{n-1}\frac{\sqrt{D}}{2} \bmod p$$

und daher

$$y_n = \frac{\omega_1^n - \bar{\omega}_1^n}{\sqrt{D}} \equiv n\left(\frac{x_1}{2}\right)^{n-1} \bmod p,$$

wie für den Spezialfall bereits in § 1, 3 vermerkt. Sei nun q *die in* $\frac{p-1}{2}$ *aufgehende Ordnung der Restklasse* $\frac{x_1}{2}$ *mod. p bezüglich der aus den beiden Restklassen* ± 1 *bestehenden Untergruppe, also jedenfalls*

$$\left(\frac{x_1}{2}\right)^q \equiv 1 \bmod p.$$

Dann kommt es für y_n mod. p nur auf n mod. $2qp$ an. Wie aus dem Ansatz

$$n \equiv i + 2qj \bmod 2qp \text{ mit } i \bmod 2q,\ j \bmod p$$

klar ist, durchläuft

$$y_n \equiv n\left(\frac{x_1}{2}\right)^{n-1} \equiv (i + 2qj)\left(\frac{x_1}{2}\right)^{i-1} \bmod p$$

für jede feste Restklasse i mod $2q$ bei laufendem j mod. p genau ein volles Restsystem mod. p. Seien insbesondere n_i $(i = 1, \ldots, q)$ die q kleinsten positiven Reste mod. $2qp$ mit

$$n_i \equiv 1 \bmod 2 \quad (\text{also } i \equiv 1 \bmod 2) \quad \text{und } y_{n_i} \equiv \left\{ \begin{array}{l} +1 \bmod p \text{ im Hauptfall} \\ -1 \bmod p \text{ im Spezialfall} \end{array} \right\}.$$

Dann liegt die erste Aussage des folgenden Satzes auf der Hand:

VI. Notwendig für eine Lösung n im Hauptfall, sowie im Spezialfall mit $n \geqq 3$ ist, dass n einer der q Restklassen

$$n \equiv n_i \text{ mod. } 2qp$$

angehört.

In jeder dieser Restklassen gibt es höchstens eine Lösung n.

Beweis. Es bleibt nur noch die zweite Aussage zu beweisen. Sei $n' > n$ mit $n' \equiv n \text{ mod. } 2qp$. Neben der hierin enthaltenen Kongruenz

$$n' \equiv n \text{ mod. } 2q$$

mit der Folgerelation

$$\left(\frac{x_1}{2}\right)^{n'} \equiv \left(\frac{x_1}{2}\right)^{n} \text{mod. } p$$

sei genauer

$$n' \equiv n \text{ mod. } p^r \text{ mit maximalem } r, \text{ wobei } r \geqq 1.$$

In

$$\omega_1^{n'} = \omega_1^n \omega_1^{n-n'} = \omega_1^n \left(\frac{x_1 + \sqrt{D}}{2}\right)^{n'-n} = \omega_1^n \left(\frac{x_1}{2}\right)^{n'-n} \left(1 + \frac{\sqrt{D}}{x_1}\right)^{n'-n}$$

ist dann, wie gleich begründet wird, einerseits

$$\left(\frac{x_1}{2}\right)^{n'-n} \equiv 1 \text{ mod. } p^{r+1},$$

andererseits

$$\left(1 + \frac{\sqrt{D}}{x_1}\right)^{n'-n} \equiv 1 + (n' - n)\frac{\sqrt{D}}{x_1} \text{ mod. } p^{r+1}.$$

Für ersteres potenziere man zunächst mit $2q$, dann r mal nacheinander mit p, und zuletzt noch mit $\frac{n'-n}{2qp^r}$; für letzteres potenziere man zunächst r mal nacheinander mit p und dann mit $\frac{n'-n}{p^r}$.

Unter Beachtung von

$$\omega_1^n \sqrt{D} \equiv \left(\frac{x_1}{2}\right)^n \sqrt{D} \text{ mod. } p$$

erhält man demnach

$$\omega_1^{n'} \equiv \omega_1^n + (n'-n)\omega_1^n \frac{\sqrt{D}}{x_1} \equiv \omega_1^n + (n'-n)\left(\frac{x_1}{2}\right)^{n-1}\frac{\sqrt{D}}{2} \text{ mod. } p^{r+1}.$$

Daraus ergibt sich

$$y_{n'} \equiv y_n + (n'-n)\left(\frac{x_1}{2}\right)^{n-1} \text{ mod. } p^{r+1},$$

und zwar formal zunächst nur mod. $p^r\sqrt{D}$, aber da alles rational, dann auch mod. p^{r+1}. Wären nun beide $y_n, y_{n'} = \left\{\begin{matrix} +1 \text{ im Hauptfall} \\ -1 \text{ im Spezialfall} \end{matrix}\right\}$, so folgte hieraus $n'-n \equiv 0$ mod. p^{r+1}, im Widerspruch zu der maximalen Wahl von r. Somit können nicht beide n, n' Lösungen sein, wie behauptet.

2. Aus VI folgt leicht der Nagellsche Satz:

VII. Im Spezialfall gibt es ausser den beiden trivialen Lösungen $n = 1, 2$ *nur noch die drei Lösungen* $n = 3, 5, 13$.

Beweis. Für $D = -7$ hat man $p = 7$, $x_1 = 1$, $q = 3$. Der Ansatz

$$n \equiv i + 6j \text{ mod. } 6 \cdot 7 \quad \text{mit} \quad i \equiv 1, 3, 5 \text{ mod. } 6, \quad j \text{ mod. } 7$$

ergibt

$$y_n \equiv (i+6j_i)\left(\frac{1}{2}\right)^{i-1} \equiv -1 \text{ mod. } 7$$

genau für

$$j_1 = 2,\ j_3 \equiv 0,\ j_5 \equiv 0 \text{ mod. } 7,$$

also

$$n_1 \equiv 13,\ n_3 \equiv 3,\ n_5 \equiv 5 \text{ mod. } 6 \cdot 7.$$

Die kleinsten positiven Reste 13, 3, 5 dieser Restklassen mod. $6 \cdot 7$ sind Lösungen. Nach VI sind sie dann die einzigen nicht-trivialen Lösungen.

Der vorstehende Beweis von VI ist durch Systematisierung und Verallgemeinerung der von Nagell für den Spezialfall verwendeten Schlussweise entstanden. Er ist für den Spezialfall wesentlich identisch mit dem Beweis von Chowla-Dunton-Lewis [6].

Mir scheint, dass die in der Ramanujanschen Vermutung zunächst sehr überraschende und unbegreifliche Fünfzahl der Lösungen einerseits durch die Abspaltung der allgemein im Grenzfall vorhandenen beiden trivialen Lösungen und andererseits durch die vorstehenden Beweise von VI und VII an Begreiflich-

keit gewinnt. Im übrigen nimmt ja der Spezialfall im Hinblick auf das Ergebnis § 2, III für den Grenzfall und das spätere Ergebnis § 6, IX für den Hauptfall tatsächlich eine singuläre Ausnahmestellung ein.

§ 6. Notwendige Bedingungen für die Lösungen durch Kongruenzbetrachtung nach Potenzen eines Primteilers von x_1 (kleinste positive Lösung) (Apéry [11] nebst eigener Ergänzung)

1. Nachdem der Spezialfall durch § 5, VII erledigt ist, braucht nur noch der Hauptfall betrachtet zu werden, in dem für eine Lösung notwendig ist:

$$n \equiv 1 \bmod. 2, \qquad y_n = +1, \qquad x_1 \neq \pm 1$$

Sei p ein (in diesem Falle sicher vorhandener) Primteiler von x_1; es ist $p \neq 2$ wegen $x_1 \equiv 1 \bmod. 2^2$ und p kein Teiler von D im Hinblick auf die vorausgesetzte Gleichung $x_1^2 - D = 2^{e+2}$. Man hat dann in erster Näherung:

$$\omega_1^n = \left(\frac{x_1 + \sqrt{D}}{2}\right)^n \equiv \left(\frac{\sqrt{D}}{2}\right)^n \bmod. p.$$

Für $n \equiv 1 \bmod. 2$ folgt daraus:

$$y_n = \frac{\omega_1^n - \bar{\omega}_1^n}{\sqrt{D}} \equiv \left(\frac{\sqrt{D}}{2}\right)^{n-1} \equiv \left(\frac{\sqrt{D}}{2^2}\right)^{\frac{n-1}{2}} \bmod. p.$$

Sei nun k *die in* $\frac{p-1}{2}$ *aufgehende Ordnung der Restklasse* $\frac{D}{2^2}$ *mod. p bezüglich der aus den beiden Restklassen* ± 1 *mod. p bestehenden Untergruppe*, so dass also zuerst

$$\left(\frac{D}{2^2}\right)^k \equiv \varepsilon \bmod. p \qquad \text{mit } \varepsilon^2 = 1$$

ist. Da für eine Lösung n notwendig $y_n \equiv 1 \bmod. p$ ausfällt, ergibt sich zunächst einmal:

VIII. Notwendig für eine Lösung n im Hauptfall ist, dass n der Restklasse

$$n \equiv 1 \ \textit{mod.}\ 2k$$

angehört, und wenn man dementsprechend

$$n = 2kt + 1$$

setzt, dass

$$\varepsilon^t = 1$$

ist.

In Verschärfung der zum Ausgang genommenen Kongruenz mod. p wird nunmehr die volle Binomialreihe betrachtet:

$$y_n = \frac{\omega_1^n - \bar{\omega}_1^n}{\sqrt{D}} = \sum_{\nu \geqq 0} \binom{n}{2\nu} \left(\frac{x_1}{2}\right)^{2\nu} \left(\frac{\sqrt{D}}{2}\right)^{n-1-2\nu} = \sum_{\nu \geqq 0} \binom{n}{2\nu} \left(\frac{x_1}{2}\right)^{2\nu} \left(\frac{D}{2^2}\right)^{\nu}.$$

Sie kann mit der Abkürzung

$$P_1 = \frac{x_1^2}{D}, \qquad \text{wo} \qquad P_1 \equiv 0 \bmod p^2,$$

in der folgenden Form geschrieben werden:

$$y_n \left(\frac{2^2}{D}\right)^{\frac{n-1}{2}} = \sum_{\nu \geqq 0} \binom{n}{2\nu} P_1^{\nu} = 1 + \sum_{\nu \geqq 1} \binom{n}{2\nu} P_1^{\nu}.$$

Dabei wurde aus einem nachher hervortretenden Grunde die obere Summationsbeschränkung $2\nu \leqq n$ fortgelassen, so dass sich die Reihe *formal* ins Unendliche erstreckt. Setzt man ferner die Definitionskongruenz von k in die Form:

$$\varepsilon \left(\frac{2^2}{D}\right)^k = 1 + P_2 \qquad \text{mit} \qquad P_2 \equiv 0 \bmod p,$$

so hat man nach VIII für den an y_n getretenen Faktor die Binomialreihe:

$$\left(\frac{2}{D}\right)^{\frac{n-1}{2}} = (1 + P_2)^t = \sum_{\nu \geqq 0} \binom{t}{\nu} P_2^{\nu} = 1 + \sum_{\nu \geqq 0} \binom{t}{\nu} P_2^{\nu}.$$

Die für eine Lösung $n = 2kt + 1$ notwendige (und auch hinreichende) Bedingung $y_n = 1$ transformiert sich damit in die Bedingung, dass t der folgenden ***Reihengleichung*** genügt:

$$(\Re) \qquad \sum_{\nu \geqq 1} \binom{2kt+1}{2\nu} P_1^{\nu} = \sum_{\nu \geqq 1} \binom{t}{\nu} P_2^{\nu}$$

2. Aus dieser Bedingung wird jetzt ein Ergebnis von Apéry [11] gefolgert, das unter allen bisher erzielten Ergebnissen zu der in dieser Arbeit behandelten Fragestellung am stärksten ist:

IX. Im Hauptfall kann es ausser der vorausgesetzten Lösung $n = 1$ höchstens noch eine weitere Lösung n geben, und zwar höchstens dann, wenn zwischen den p-adischen Ordnungszahlen

$$2h_1 = w_p(P_1) = 2w_p(x_1) \qquad \textit{und} \qquad h_2 = w_p(P_2) = w_p\left(\varepsilon \left(\frac{2^2}{D}\right)^k - 1\right)$$

die Ungleichung

$$2h_1 \leqq h_2$$

besteht.

Beweis. In den beiden unendlichen Reihen links und rechts in $(\mathfrak{R})$ werde t als Unbestimmte aufgefasst. Die Reihen sind dann *aktual* unendlich, indem die Binomialkoeffizienten $\binom{2kt+1}{2\nu}$ bzw. $\binom{t}{\nu}$ eine Folge von Polynomen der Grade 2ν bzw. ν bilden. Die Zahlnenner dieser Polynome sind $(2\nu)!$ bzw. $\nu!$. Nach der Theorie der p-adischen Exponentialreihe sind nun die p-adischen Reihen

$$\sum_{\nu \geqq 1} \frac{P_1^\nu}{(2\nu)!} \quad \text{und} \quad \sum_{\nu \geqq 1} \frac{P_2^\nu}{\nu!}$$

konvergent, und ihre Anfangsglieder haben jeweils niedrige p-adische Ordnungszahl als alle ihre weiteren Glieder. Demnach kann man die beiden Reihen aus $(\mathfrak{R})$ als Potenzreihen in t mit ganz-p-adischen Zahlkoeffizienten auffassen, die sogar sämtlich durch p teilbar sind; noch genauer bestehen für diese beiden Potenzreihen nach dem Gesagten die Kongruenzen:

$$(\mathfrak{R}) \qquad \begin{aligned} &\sum_{\nu \geqq 1} \binom{2kt+1}{2\nu} P_1^\nu \equiv kt(2kt+1)P_1 \bmod p^{2h_1+1}, \\ &\sum_{\nu \geqq 1} \binom{t}{\nu} P_2^\nu \equiv tP_2 \bmod p^{h_2+1}. \end{aligned}$$

Bei dieser Auffassung wird die Reihengleichung $(\mathfrak{R})$ zu einer p-adischen Potenzreihengleichung. Ihre Lösungen im ursprünglichen Sinne durch natürliche Zahlen t sind gewiss auch ganz-p-adische Lösungen der p-adischen Potenzreihengleichung (aber nicht notwendig umgekehrt). Es genügt demnach zu zeigen, dass die p-adische Potenzreihengleichung ausser der $n=1$ entsprechenden Lösung $t=0$ höchstens noch e i n e weitere ganz-p-adische Lösung besitzt.

Der Lösung $t=0$ entspricht der in allen Binomialkoeffizienten links und rechts auftretende Linearfaktor t. Durch Wegdivision dieses Faktors werden die Kongruenzen $(\mathfrak{R})$ zu:

$$(\mathfrak{R}') \qquad \begin{aligned} &\sum_{\nu \geqq 1} \frac{1}{t} \binom{2kt+1}{2\nu} P_1^\nu \equiv k(2kt+1)P_1 \bmod p^{2h_1+1}, \\ &\sum_{\nu \geqq 1} \frac{1}{t} \binom{t}{\nu} P_2^\nu \equiv P_2 \bmod p^{h_2+1}. \end{aligned}$$

Ist zunächst $2h_1 > h_2$, so ist die erste Reihe sicher $\equiv 0 \bmod. p^{h_2+1}$, während die zweite Reihe $\equiv P_2 \not\equiv 0 \bmod. p^{h_2+1}$ ist. Demnach können die beiden Reihen für kein ganz-p-adisches t einander gleich werden.

Ist ferner $2h_1 \leqq h_2$, so dividiere man beide Reihen noch durch P_1. Dadurch werden die beiden Kongruenzen $(\mathfrak{R}')$ zu

$$(\mathfrak{R}'') \qquad \sum_{\nu \geqq 1} \frac{1}{t}\binom{2kt+1}{2\nu} P_1^{\nu-1} \equiv 2k^2t + k \bmod. p.$$

$$\sum_{\nu \geqq 1} \frac{1}{t}\binom{t}{\nu} \frac{P_2^{\nu}}{P_1} \equiv \frac{P_2}{P_1} \bmod. p^{h_2-2h_1+1}, \qquad \text{also sicher mod. } p.$$

Die Forderung, dass die beiden Reihen für ein ganz-p-adisches t einander gleich werden, bekommt daher, indem man alle sicher durch p teilbaren Glieder auf die rechte Seite nimmt, die Gestalt

$$2k^2t + \left(k - \frac{P_2}{P_1}\right) = p \sum_{\nu \geqq 0} c_\nu t^\nu$$

mit ganz-p-adischen c_ν. Eine derartige Gleichung hat aber höchstens eine ganz-p-adische Lösung. Denn gäbe es zwei verschiedene t, t', so sei

$$t - t' \equiv 0 \bmod. p^r \qquad \text{mit maximalem } r\ (\geqq 0).$$

Da dann auch durchweg $t^\nu - t'^\nu \equiv 0 \bmod. p^r$ ist, folgte durch Subtraktion der beiden Gleichungen

$$2k^2(t - t') \equiv 0 \bmod. p^{r+1}.$$

Da $2k$ als Teiler von $p-1$ prim zu p ist, widerspricht das der maximalen Wahl von r.

3. Aus dem vorstehenden Beweis lässt sich, wie ich ergänzend ausführen möchte, noch eine zu § 5, VI analoge Kongruenzaussage über die möglicherweise vorhandene Lösung $n > 1$ herausholen:

X. Die im Falle $2h_1 \leqq h_2$ möglicherweise vorhandene Lösung $n > 1$ liegt notwendig in der Restklasse

$$n \equiv \frac{P_2}{kP_1} = \frac{\varepsilon(2^2 - D)}{kx_1^2} \quad \textit{mod.}\ p^{2h_1-1}.$$

Beweis. Es genügt, durch schärfere Abschätzung der vorstehend vernachlässigten Reihenglieder mit $\nu \geqq 2$ zu zeigen, dass die im Modul der Kongruenzen

$(\mathfrak{R})$, $(\mathfrak{R}')$, $(\mathfrak{R}'')$ auftretende zusätzliche Potenz p^1 durch p^{2h_1-1} ersetzt werden kann. Denn dann kann aus $(\mathfrak{R}'')$ durch Vergeich der rechten Seiten für eine eventuelle Lösung $n>1$ unter Beachtung von $n=2kt+1$ auf die behauptete Kongruenz geschlossen werden.

Die erforderliche schärfere Abschätzung, sogar mit p^{h_2} statt p^1 für die zweite Reihe, erhält man durch Betrachtung der Glieder mit $\nu \geqq 2$ linkerhand in $(\mathfrak{R}'')$ wie folgt.

Zweite Reihe. Zu betrachten sind die Glieder

$$G_\nu'' = \frac{1}{t}\binom{t}{\nu}\frac{P_2^\nu}{P_1} \quad \text{mit } \nu \geqq 2.$$

Bekanntlich [12] ist

$$w_p\left(\binom{t}{\nu}\right) \geqq \operatorname{Max}\,(w_p(t) - w_p(\nu), 0)$$

und daher

$$w_p\left(\frac{1}{t}\binom{t}{\nu}\right) \geqq \operatorname{Max}(-w_p(\nu), -w_p(t)) = -\operatorname{Min}(w_p(\nu), w_p(t)).$$

Dabei ist

$$\nu \geqq p^{w_p(\nu)} \geqq 1 + w_p(\nu)(p-1) \geqq 1 + 2\,w_p(\nu), \text{ also } w_p(\nu) \leqq \frac{\nu-1}{2},$$

daher auch

$$\operatorname{Min}\,(w_p(\nu), w_p(t)) \leqq \frac{\nu-1}{2},$$

und somit

$$w_p\left(\frac{1}{t}\binom{t}{\nu}\right) \geqq -\frac{\nu-1}{2}.$$

Demnach wird

$$w_p(G_\nu'') \geqq -\frac{\nu-1}{2} + \nu h_2 - 2h_1 = \nu\left(h_2 - \frac{1}{2}\right) - 2h_1 + \frac{1}{2} \geqq 2h_2 - 1 - 2h_1 + \frac{1}{2}$$

$$= 2h_2 - 2h_1 - \frac{1}{2}$$

oder also

$$w_p(G_\nu'') \geqq 2h_2 - 2h_1 \text{ für } \nu \geqq 2,$$

wie behauptet.

Erste Reihe. Zu betrachten sind die Glieder

$$G'_\nu = \frac{1}{t}\binom{2kt+1}{2\nu} P_1^{\nu-1} = \frac{n}{2\nu}\frac{1}{t}\binom{2kt}{2\nu-1} P_1^{\nu-1} \quad \text{mit } \nu \geqq 2.$$

Zunächst ist

$$w_p\left(\frac{n}{2\nu}\right) \geqq -w_p(2\nu) = -w_p(\nu) \geqq \left\{\begin{matrix} -\frac{\nu-1}{2} & \text{für } w_p(2\nu)>0 \\ 0 & \text{für } w_p(2\nu)=0 \end{matrix}\right\},$$

ersteres nach dem vorher Gezeigten. Analog wie vorher ist ferner

$$w_p\left(\frac{1}{t}\binom{2kt}{2\nu-1}\right) \geqq -\operatorname{Min}(w_p(2\nu-1),\ w_p(t)),$$

dabei

$$w_p(2\nu-1) \leqq \frac{2\nu-2}{2} = \nu-1,$$

daher sicher

$$\operatorname{Min}((w_p(2\nu-1),\ w_p(t)) \leqq \left\{\begin{matrix} \nu-1 & \text{für } w_p(2\nu-1)>0 \\ 0 & \text{für } w_p(2\nu-1)=0 \end{matrix}\right\}.$$

Schliesslich ist ersichtlich entweder $w_p(2\nu)=0$ oder $w_p(2\nu-1)=0$ (oder beides). Demnach wird in jedem Falle

$$w_p(G'_\nu) \geqq -(\nu-1)+(\nu-1)2h_1 = (\nu-1)(2h_1-1) \geqq 2h_1-1 \quad \text{für } \nu \geqq 2,$$

wie behauptet.

§ 7. Schluss: Bemerkungen über Verallgemeinerung auf ungerade Primzahlbasen, auf positive Diskriminanten, sowie über effektive Entscheidung der Lösbarkeit

1. Es liegt nahe, die vorstehend ausführlich behandelte Fragestellung auf Primzahlbasen $l \neq 2$ zu verallgemeinern. Die zu behandelnde diophantische Gleichung lautet dann.

$$x^2 - D = l^m \text{ mit } D \text{ prim zu } l,\ \left(\frac{D}{l}\right) = 1,\ D<0.$$

Auch für diese Gleichung wurde von Apéry [13] durch eine zu § 6, 2 ganz analoge

Schlussweise bewiesen, dass in jedem Falle höchstens zwei Lösungen vorhanden sind: ein Ausnahmefall von der Art des Ramanujan-Nagellschen Spezialfalles tritt hier nicht auf. Es dürfte nicht schwer sein, dies Ergebnis durch Kongruenzkriterien für die Lösungsexponenten n analog zu den hier in §§ 4-6 hergeleiteten zu ergänzen.

Speziell im Falle $D=-1$, also $l\equiv 1 \bmod 2^2$, ist für die Lösbarkeit notwendig, dass die Gleichung

$$x^2+1=l$$

lösbar ist. Man weiss bis heute nicht, ob es unendlich viele Primzahlen l mit dieser Eigenschaft gibt.

Was die zu $D\equiv 1 \bmod 2^3$ analoge Forderung $\left(\frac{D}{l}\right)=1$ betrifft, so sorgt sie dafür, dass l im quadratischen Zahlkörper von $\sqrt{D}$ in zwei konjugierte Primdivisoren zerfällt und somit die durch Zulassung von Primdivisoren von l modifizierte Einheitengruppe überhaupt einen unendlichen Zyklus nicht-rationaler modifizierter Einheiten enthält. Lässt man diese Forderung fallen, wie es von einem elementarzahlentheoretischen Standpunkt aus angebracht erscheinen mag und auch von einigen Autoren getan wurde, so lässt sich in den hinzukommenden Fällen die Entscheidung über die Lösbarkeit und die Bestimmung der Lösungsgesamtheit in ganz elementarer Weise vollständig durchführen.

2. Viel schwieriger dürfte eine Verallgemeinerung auf Diskriminanten $D>0$ sein. Dann ist nämlich die durch Zulassung von Primteilern von l modifizierte Einheitengruppe in bezug auf ihre rationale Untergruppe nicht mehr zyklisch, sondern vom Rang 2. Es kommt nämlich zu der hier interessierenden modifizierten Grundeinheit ω_1 die gewöhnliche Grundeinheit ε_1 hinzu. Die für alles weitere grundlegende Reduktion der Fragestellung in § 2, **1** beruhte nun aber wesentlich auf der Zyklizität der genannten Gruppe. Im nicht-zyklischen Falle würden durch das Hereinspielen von ε_1 erhebliche Komplikationen eintreten. Einige Ergebnisse hierzu siehe bei Chowla-Dunton-Lewis [14].

Ganz Entsprechendes gilt in noch stärkerem Masse auch für die Verallgemeinerung auf aus mehreren Primzahlpotenzen zusammengesetzte Zahlen $p_1^{n_1}\cdots p_r^{n_r}$ anstelle von l^m, wie sie bei dem Endlichkeitsnachweis in § 3 zugrunde gelegt wurde.

3. Schliesslich sei noch auf das Problem der effektiven Entscheidung über

die Lösbarkeit hingewiesen. Dieses Problem konnte Schinzel [15] mittels eines tiefliegenden Hilfssatzes von Gelfond [16] lösen, nämlich durch die untere Abschätzung

$$|y_n| > |\omega_1|^{n-\log^2+\varepsilon n} \quad \text{für} \quad n \geqq n_0(\varepsilon)$$

bei beliebig vorgebbarem $\varepsilon > 0$, in der die Schranke $n_0(\varepsilon)$ effektiv angebbar ist. Man beachte dabei

$$|\omega_1|^2 = \omega_1\bar{\omega}_1 = 2^e \quad (\text{bzw. } l^e).$$

Die Bedeutung der über den Apéryschen Satz § 6, IX hinaus hergeleiteten Kongruenzbedingungen aus §§ 4-6 liegt darin, dass man mit ihrer Hilfe bei numerisch bekannter, aber sehr grosser Schranke $n_0(\varepsilon)$ die Suche nach der möglicherweise vorhandenen Lösung $n > 1$ auf einen Bruchteil aller möglichen Werte reduzieren kann.

Literaturverzeichnis

[1] S. Ramanujan, Coll. Papers, Cambridge Univ. Press (1927), 327.

[2] T. Nagell, The diophantine equation $x^2+7=2^n$, Norsk Mat. Tidsskr. **30** (1948), 62-64; Ark. f. Mat. **4** (1960), 185-187.

[3] Th. Skolem-S. Chowla-D. J. Lewis, The diophantine equation $2^{n+2}-7=x^2$ and related problems, Proc. Amer. Math. Soc. **10** (1959), 663-669.

[4] H. S. Shapiro-D. L. Slotnick, On the mathematical theory of error-correcting codes, IBM Journal **3** (1959), 25-34.

[5] J. Browkin-A. Schinzel, Sur les nombres de Mersenne qui sont triangulaires, Comptes Rendus Paris (Ser. math., phys., astr.) **242** (1956), 1780-1781.

[6] S. Chowla-M. Dunton-D. J. Lewis, All integer solutions of $2^n-7=x^2$ are given by $n=3, 4, 5, 7, 15$, Kongl. Norske Vidensk. Selsk. Forhandl. (Trondheim) B **33** (1960), Nr, 9, 37-38.

[7] L. J. Mordell, The diophantine equation $2^n=x^2+7$, Arkiv f. Mat. **4** (1962), 455-460.

[8] J. Browkin-A. Schinzel, On the equation $2^n-D=y^2$, Bull, Acad. Pol. Sci. **8** (1960), 311-318.

[9] Siehe dazu E. Landau, Vorlesungen über Zahlentheorie **3**, Leipzig 1927, Satz 698.

[10] Siehe dazu etwa H. Hasse, Rein-arithmetischer Beweis des Siegelschen Endlichkeitssatzes für binäre diophantische Gleichungen im Spezialfall des Geschlechts 1, Abh. Deutsche. Akad. d. Wis., Kl. Math. Nat. 1951, Nr. **2** (1952), 1-19.

[11] R. Apéry, Sur une équation diophantienne, Comptes Rendus Paris (Sér. math., phys., astr.) **251** (1960), 1263-1264.

[12] Siehe etwa E. Artin-H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln, Abh. Math. Sem. Hamburg **6** (1928), 146-162.

[13] R. Apéry, Sur une équation diophantienne., Comptes Rendus Paris (Ser. math., phys.,

astr.) **251** (1960), 1451–1452.

[14] S. Chowla-M. Dunton-D. J. Lewis, Linear recurrences of order two, Pacific Journ. Math. **11** (1961), 833–845.

[15] A. Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant, Arkiv f. Mat. **4** (1962), 413–416.

[16] A. Gelfond, Transcendental and algebraic numbers, New-York (1960), 1–190.

Universität zu Hamburg