ÜBER DEN GRÖSSTEN PRIMTEILER SPEZIELLER POLYNOME ZWEITEN GRADES

VON

KURT MAHLER

OSLO
I KOMMISJON HOS MORTEN JOHANSEN
1935

ÜBER DEN GRÖSSTEN PRIMTEILER SPEZIELLER POLYNOME ZWEITEN GRADES

VON

KURT MAHLER

IN GRONINGEN

In der Arbeit: «Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \mp 1$ et leurs applications» (Videnskabsselskabets Skrifter, I. Mathem.-naturvid. Klasse. 1897. No. 2) zeigte C. Störmer, wie sich diejenigen Lösungen dieser Gleichung in natürlichen Zahlen finden lassen, für die in y allein solche Primzahlen aufgehen, die Teiler von D sind, und in der späteren Arbeit: «Solution d'un problème curieux qu'on rencontre dans la théorie élémentaire des logarithmes» (Nyt Tidsskrift f. Math. B. XIX) vereinfachte er diesen Beweis. Die angekündigte Verallgemeinerung seiner Untersuchungen auf die Gleichung $x^2 - Dy^2 = A$, wo A eine *beliebige* ganze rationale Zahl $\neq 0$ ist, ist dagegen nicht erschienen und anscheinend auch von andere Seite bisher nicht durchgeführt worden.

In der vorliegenden Arbeit wird das Problem wenigstens in einem speziellen Fall, nämlich unter der Annahme, *dass A quadratfrei und Teiler von $2D$ sei*, vollständig gelöst; es gibt dann entweder keine, eine oder zwei Lösungen in natürlichen Zahlen, und diese lassen sich auf finite Art bestimmen. Der Beweis ist dem Störmerschen vollständig nachgebildet, und beruht auf einem Hilfssatz von D. Schepel, der einen einfachen expliziten Ausdruck für die Lösungen der Gleichung $x^2 - Dy^2 = A$ vermittels der Fundamentallösung gibt. Auf Grund weiterer Ueberlegungen der Störmerschen Arbeit folgere ich aus meinem Ergebnis den Satz:

«*Ist A_0 eine der vier Zahlen $+1$, -1, $+2$, -2, D_1 quadratfrei und zu A_0 teilerfremd, x_0 eine natürliche Zahl und zu A_0*

teilerfremd, so ist für jedes $\varepsilon > 0$ *und hinreichend grosses* x_0 *der Ausdruck*

$$D_1 x_0^2 - A_0$$

durch mindestens eine Primzahl $p > \dfrac{\log\log x_0}{1+\varepsilon}$ *teilbar.*

Der Beweis dieses Satzes macht Gebrauch von einfachen Abschätzungen aus meiner Note: «Über den grössten Primteiler der Polynome $x^2 \mp 1$» (Archiv for Math. og Naturv. 1933. B. XLI. Nr. 1), wo ich die gleiche Frage schon für die beiden speziellen Polynome mit $D_1 = 1$ und $A_0 = \mp 1$ mittels des Störmerschen Satzes gelöst hatte. Man vergleiche auch die Arbeiten von S. Chowla in den Proc. Indian Acad. Sci. Sect. A, I (1934), 269—270 und 271—273, der gleichfalls und unabhängig von mir diese beiden speziellen Polynome untersuchte.

I.

Bezeichnungen: Der Kürze halber bezeichnet im Folgenden:

D eine natürliche Zahl, die kein Quadrat ist,

A eine quadratfreie ganze rationale Zahl ungleich Null, die in $2D$ aufgeht,

$X,\ Y$ Paare ganzer rationaler Zahlen mit

$$X^2 - DY^2 = A,$$

$\mathfrak{M}(D, A)$ die Menge aller dieser Paare,

$u,\ v$ das Paar natürlicher Zahlen mit kleinstem v, für das

$$u^2 - Dv^2 = A$$

ist; wir nennen dies das Fundamentalpaar von $\mathfrak{M}(D, A)$,

$x,\ y$ Paare ganzer rationaler Zahlen aus $\mathfrak{M}(D, A)$ mit $y \neq 0$ und der Eigenschaft, dass jeder Primteiler von y auch in D aufgeht,

$\mathfrak{N}(D, A)$ die Menge aller Paare $x,\ y$.

Wir stellen uns das Ziel:

«Zu gegebenen Werten von D und A ein Verfahren anzugeben, mittels dessen sich alle Elemente der Menge $\mathfrak{N}(D, A)$ bestimmen lassen.»

1) Für $A = 1$ wird die Frage gelöst durch folgenden Satz von C. Störmer (Videnskabsselskabets Skrifter, I. Math.-naturv. Klasse (1897), Nr. 2):

«*Die Menge* $\mathfrak{N}(D, 1)$ *ist entweder leer, oder sie besteht allein aus den Elementen*

$$x = \pm u, \quad y = \pm v,$$

wobei u, v *das Fundamentalpaar von*

$$u^2 - Dv^2 = 1$$

darstellt.»

In derselben Arbeit zeigt Störmer einen ganz analog lautenden Satz für die zweite Menge $\mathfrak{N}(D, -1)$; dieser Satz wird sich in der vorliegenden Arbeit als Spezialfall allgemeinerer Ergebnisse ergeben.

Das gestellte Problem lässt sich weiter in trivialer Weise lösen für $A = -D$. Denn aus

$$x^2 - Dy^2 = -D$$

folgt, dass x durch D teilbar ist, da wir ja $A = -D$ als quadratfrei voraussetzen. Aus dem gleichen Grund müssen x und y teilerfremd sein, weil das Quadrat ihres grössten gemeinsamen Teilers in D aufgeht. Da nun jeder Primteiler von y in D aufgehen soll und folglich auch in x, so kann nur $y = \pm 1$ sein; damit ergibt sich:

«*Die Menge* $\mathfrak{N}(D, -D)$ *besitzt allein die Elemente*

$$x = 0, \quad y = \pm 1.$$»

Auf analoge Weise zeigt man, dass die Menge $\mathfrak{N}(D, D)$ für $D \neq 2$ leer ist, dagegen für $D = 2$ allein aus den Elementen $x = \pm 2$, $y = \pm 1$ besteht.

2) Da nach § 1 die beiden Mengen $\mathfrak{N}(D, 1)$ und $\mathfrak{N}(D, -D)$ bekannt sind, so dürfen wir im Folgenden ohne Einschränkung der Allgemeinheit voraussetzen, dass

$$A \neq 1 \quad \text{und} \quad A \neq -D$$

sei. Die Ergebnisse der Arbeit: Over de Vergelijking van Pell, von D. Schepel, Nieuw Archief voor Wiskunde (1935), erlauben alsdann, zunächst die Menge $\mathfrak{M}(D, A)$ aller ganzzahligen Lösungen X, Y der Gleichung

$$X^2 - DY^2 = A$$

auf einfache Weise zu charakterisieren.

Wegen $A \neq 1$ hat diese Gleichung gewiss kein Lösungspaar X, Y mit $Y = 0$, und wegen $A \neq -D$ auch keins mit $X = 0$. Falls $\mathfrak{M}(D, A)$ nicht überhaupt leer ist, in welchem Fall erst recht $\mathfrak{N}(D, A)$ ohne Elemente sein würde, muss demnach jedes Element X, Y von $\mathfrak{M}(D, A)$ den Ungleichungen $X \neq 0$, $Y \neq 0$ genügen, und es existiert daher das Fundamentalpaar u, v von $\mathfrak{M}(D, A)$, das natürlich auf Grund seiner Definition eindeutig bestimmt ist.

Weil nach Voraussetzung A quadratfrei und ein Teiler von $2D$ ist, sind die aus diesem Fundamentalpaar u, v gebildeten Zahlen

$$\xi = \left| \frac{2u^2 - A}{A} \right| , \qquad \eta = \left| \frac{2uv}{A} \right|$$

beide ganz rational, und wie leicht einzusehen, sogar positiv; nach der erwähnten Arbeit von Schepel stellen ξ, η das Fundamentalpaar von $\mathfrak{M}(D, 1)$ dar, also die Lösung der Pellschen Gleichung

$$\xi^2 - D\eta^2 = 1$$

in natürlichen Zahlen mit kleinstem η.

Für jede natürliche Zahl $m + 1$ definieren wir zwei positive ganze rationale Zahlen X_m und Y_m vermöge der Gleichungen

$$X_m + Y_m\sqrt{D} = (u + v\sqrt{D})(\xi + \eta\sqrt{D})^m, \quad X_m - Y_m\sqrt{D} = (u - v\sqrt{D})(\xi - \eta\sqrt{D})^m$$

auf eindeutige Weise. Das Hauptergebnis von Schepel, das wir benutzen müssen, lautet alsdann:

«Falls $A \neq 1$ und $A \neq -D$ und $\mathfrak{M}(D, A)$ nicht leer ist, und falls ferner u, v das Fundamentalpaar dieser Menge darstellt, so besteht die Menge $\mathfrak{M}(D, A)$ aus den unendlichvielen Paaren

$$X = \pm X_m , \quad Y = \pm Y_m \qquad (m = 0, 1, 2, \ldots)$$

und aus keinen anderen.»

Dieser Satz lässt sich auf eine noch etwas elegantere Form bringen. Wegen $A \mid 2u$, d. h. $2u^2 \geq A = u^2 - Dv^2$, und also

$$\xi \pm \eta\sqrt{D} = \frac{2u^2 - (u^2 - Dv^2)}{|A|} \pm \frac{2uv}{|A|}\sqrt{D} = \frac{1}{|A|}(u \pm v\sqrt{D})^2$$

ist nämlich offenbar

$$X_m + Y_m\sqrt{D} = \frac{(u + v\sqrt{D})^{2m+1}}{|A|^m} , \qquad X_m - Y_m\sqrt{D} = \frac{(u - v\sqrt{D})^{2m+1}}{|A|^m} ,$$

so dass sich, wenn wir diese Gleichungen noch nach X_m und Y_n auflösen, der folgende Satz ergibt:

«*Sei* $A \neq 1$ *und* $A \neq -D$ *und* $\mathfrak{M}(D, A)$ *nicht leer, ferner* u, v *das Fundamentalpaar dieser Menge; dann besteht* $\mathfrak{M}(D, A)$ *aus den unendlichvielen Paaren*

$$X = \pm X_m, \quad Y = \pm Y_m \qquad (m = 0, 1, 2, \ldots)$$

und keinen weiteren, wobei

$$X_m = \frac{1}{2|A|^m}\left((u + v\sqrt{D})^{2m+1} + (u - v\sqrt{D})^{2m+1}\right),$$

$$Y_m = \frac{1}{2|A|^m\sqrt{D}}\left((u + v\sqrt{D})^{2m+1} - (u - v\sqrt{D})^{2m+1}\right)$$

ist».

3) Die Frage nach den Elementen von $\mathfrak{N}(D, A)$ kommt demnach zurück auf die nach denjenigen ungeraden Zahlen

$$n = 2m + 1,$$

für die der Ausdruck

$$Y_m = \frac{1}{2|A|^{\frac{n-1}{2}}\sqrt{D}}\left((u + v\sqrt{D})^n - (u - v\sqrt{D})^n\right)$$

allein durch solche Primteiler dividiert werden kann, die auch in D aufgehen. Für jede solche ungerade Zahl n gehören dann die Paare

$$X = \pm X_m, \quad Y = \pm Y_m$$

zu $\mathfrak{N}(D, A)$, und diese Menge kann als Untermenge von $\mathfrak{M}(D, A)$ auch keine anderen Elemente besitzen.

Statt X_m, Y_m schreiben wir zweckmässigerweise x_n, y_n, so dass also

$$x_n = \frac{1}{2|A|^{\frac{n-1}{2}}}\left((u + v\sqrt{D})^n + (u - v\sqrt{D})^n\right),$$

$$y_n = \frac{1}{2|A|^{\frac{n-1}{2}}\sqrt{D}}\left((u + v\sqrt{D})^n - (u - v\sqrt{D})^n\right)$$

ist; beide Ausdrücke stellen selbstverständlich gemäss ihrer Konstruktion natürliche Zahlen dar. Die so definierte Zahl y_n hat

eine besonders einfach ausdrückbare Eigenschaft. Sei nämlich ν eine zweite ungerade natürliche Zahl und zwar ein Teiler von n. Dann ist

$$\frac{y_n}{y_\nu} = z_{n,\nu}$$

eine rationale Zahl, die sich auch schreiben lässt in der Form

$$z_{n,\nu} = \frac{\left(\frac{u+v\sqrt{D}}{\sqrt{|A|}}\right)^n - \left(\frac{u-v\sqrt{D}}{\sqrt{|A|}}\right)^n}{\left(\frac{u+v\sqrt{D}}{\sqrt{|A|}}\right)^\nu - \left(\frac{u-v\sqrt{D}}{\sqrt{|A|}}\right)^\nu}$$

oder

$$z_{n,\nu} = \sum_{h=0}^{\frac{n}{\nu}-1} \left(\frac{u+v\sqrt{D}}{\sqrt{|A|}}\right)^{h\nu} \left(\frac{u-v\sqrt{D}}{\sqrt{|A|}}\right)^{\left(\frac{n}{\nu}-h-1\right)\nu}.$$

Die Quadrate

$$\left(\frac{u+v\sqrt{D}}{\sqrt{|A|}}\right)^2 = \xi + \eta\sqrt{D} \quad \text{und} \quad \left(\frac{u-v\sqrt{D}}{\sqrt{|A|}}\right)^2 = \xi - \eta\sqrt{D}$$

der einzelnen Faktoren in den Termen auf der rechten Seite sind aber gewiss ganze Zahlen des durch $\sqrt{D}$ erzeugten quadratischen Zahlkörpers, so dass $z_{n,\nu}$ selbst auch eine ganze algebraische und daher sogar ganze rationale Zahl darstellt. Es folgt also:

«Ist die ungerade natürliche Zahl ν ein Teiler der ungeraden natürlichen Zahl n, so ist auch y_ν ein Teiler von y_n.»

Verstehen wir unter

$$\mathfrak{n}(D, A)$$

die Menge derjenigen ungeraden natürlichen Zahlen n, für die die Paare

$$X = \pm x_n, \quad Y = \pm y_n$$

zu $\mathfrak{N}(D, A)$ gehören, so folgt also insbesondere,

«dass mit einer ungeraden natürlichen Zahl n auch jeder ungerade Teiler ν derselben, insbesondere also die Zahl 1 zu $\mathfrak{n}(D, A)$ gehört.»

Ist $\mathfrak{N}(D, A)$ nicht leer, so muss somit speziell $y_1 = v$ allein solche Primfaktoren enthalten, die auch Teiler von D sind.

4) Aus der Gleichung

$$y_n = \frac{1}{2|A|^{\frac{n-1}{2}}\sqrt{D}}\left((u + v\sqrt{D})^n - (u - v\sqrt{D})^n\right)$$

folgt die Reihenentwicklung

$$y_n^* = |A|^{\frac{n-1}{2}} y_n = v\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} u^{n-2k-1}(Dv^2)^k .$$

Sei n ein beliebiges Element von $\mathfrak{n}(D, A)$. Dann sind zwei Fälle zu unterscheiden:

Fall a: *A ist ein Teiler von D.*

Alsdann ist evident, dass y_n^* allein durch solche Primzahlen teilbar ist, die auch in D aufgehen.

Fall b: *A geht wohl in 2D, nicht aber in D auf.*

Nunmehr muss D ungerade sein, und A ist wohl durch 2, nicht aber durch 4 teilbar. Da das Paar x_n, y_n zu $\mathfrak{M}(D, A)$ gehört, so ist

$$x_n^2 - Dy_n^2 = A ,$$

also y_n zu x_n teilerfremd und folglich ungerade. Demnach ist

$$y_n^* = 2^{\frac{n-1}{2}}\left(\frac{|A|}{2}\right)^{\frac{n-1}{2}} y_n$$

genau durch die Potenz

$$2^{\frac{n-1}{2}}$$

von 2 teilbar, und also

$$2^{-\frac{n-1}{2}} y_n^*$$

ganz rational und nur durch solche Primzahlen teilbar, die auch in D aufgehen.

Um die Menge $\mathfrak{N}(D, A)$ zu bestimmen, ist es also in beiden Fällen erlaubt, statt y_n den einfacheren Ausdruck y_n^* zu betrachten.

5) Von jetzt ab werde ohne Einschränkung der Allgemeinheit angenommen, dass die Menge $\mathfrak{N}(D, A)$ *nicht leer* ist. Alsdann gehen nach § 3 in v und folglich auch in

$$D^* = Dv^2$$

allein solche Primzahlen auf, die auch Teiler von D sind.

Bedeute für zwei beliebige ganze rationale Zahlen a und b, die nicht zugleich Null sind, das Zeichen (a, b) die grösste *natürliche* Zahl, die gleichzeitig in a und b aufgeht.

Der Gleichung

$$u^2 - Dv^2 = u^2 - D^* = A$$

entnimmt man die Relationen

$$(u, v) = 1, \quad (A, v) = 1, \quad (D, A) = (D^*, A),$$

da A quadratfrei ist. Die Zahl

$$D_1 = (D, A) = (D^*, A)$$

ist als Teiler von A auch quadratfrei; sie geht in u^2 und folglich sogar in u selbst auf. Demnach gibt es drei ganze rationale Zahlen D_0, A_0 und u_0 mit

$$D = D_0 D_1, \quad A = A_0 D_1, \quad u = u_0 D_1.$$

Zwischen diesen neuen Grössen bestehen die Beziehungen

$$(D_0 v^2, D_1) = 1$$

und

$$(D_0 v^2, u_0) = 1.$$

Denn wäre die erste dieser Gleichungen falsch, so gäbe es eine Primzahl p mit

$$p | D_0 v^2, \quad p | D_1, \quad \text{also} \quad p^2 | D^*, \quad p^2 | u^2 \quad \text{und folglich} \quad p^2 | A,$$

was falsch ist. Wäre ferner die zweite Gleichung unrichtig, so ginge eine gewisse Primzahl p in $(D_0 v^2, u_0)$ und daher in (D_0, u_0) auf; wegen

$$D_1 u_0^2 - D_0 v^2 = A_0$$

wäre sie ein Teiler von A_0, so dass auf Grund der gerade bewiesenen Gleichung $(D_0, D_1) = 1$ nicht nur D_1, sondern sogar $D_1 p$ ein gemeinsamer Teiler von D und A wäre, was unserer Voraussetzung widerspricht.

6) In der Reihendarstellung

$$y_n^* = v \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} u^{n-2k-1} (Dv^2)^k$$

$$y_n^{*} = vD_1^{\frac{n-1}{2}} \eta_n ,$$

und zwar ist dabei

$$\eta_n = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} (D_1 u_0^2)^{\frac{n-1}{2}-k} (D_0 v^2)^k .$$

Liegt nun der Fall a nach § 4 vor, so ist nach dieser Definition von η_n klar, dass in η_n allein solche Primzahlen aufgehen, die auch Teiler von D, d. h. von D_0 oder D_1 sind. Liegt dagegen Fall b vor, so ist v und D, also auch D_0 und D_1 ungerade; in diesem Fall wird demnach

$$2^{-\frac{n-1}{2}} \eta_n$$

eine ungerade ganze rationale Zahl, in der allein Primzahlen aufgehen, die auch Teiler von D_0 oder D_1 sind. Der Reihenentwicklung von η_n entnimmt man jedoch die Kongruenz

$$\eta_n \equiv (D_0 v^2)^{\frac{n-1}{2}} \pmod{D_1},$$

und da nach dem vorigen Paragraphen

$$(D_0 v^2 , D_1) = 1$$

ist, so ist η_n gewiss zu D_1 teilerfremd.

Damit ergibt sich, dass der Index n dann und nur dann zu $\mathfrak{n}(D, A)$ gehört, wenn in Fall a die Zahl η_n und in Fall b die Zahl $2^{-\frac{n-1}{2}} \eta_n$ allein durch solche Primzahlen teilbar sind, die auch in D_0 aufgehen; im letzteren Fall ist also die Primzahl 2 als Teiler ausgeschlossen.

7) Aus der Reihe für η_n folgt noch die zweite Kongruenz

$$\eta_n \equiv n(D_1 u_0^2)^{\frac{n-1}{2}} \pmod{D_0}.$$

Nach § 5 ist aber

$$(D_0 , D_1) = (D_0 , u_0) = 1 .$$

Eine Primzahl p, die in η_n aufgeht und in Fall b von 2 verschieden sei, und die nach dem vorigen Paragraphen auch in D_0 aufgeht und also zu der Zahl $(D_1 u_0^2)^{\frac{n-1}{2}}$ teilerfremd ist, *muss demnach den Index n teilen und also auch im Fall a von 2 verschieden sein.*

Wir wollen zeigen, dass *die Elemente n aus* $\mathfrak{n}(D, A)$ durch keine Primzahl $p \geq 5$ teilbar und folglich *reine Potenzen von 3 sind.* Nach § 3 gehört mit einem n auch jeder Teiler hiervon zu $\mathfrak{n}(D, A)$; der Beweis ist also erbracht, wenn wir zeigen können, dass keine Primzahl $p \geq 5$ zu der Menge $\mathfrak{n}(D, A)$ gehört.

Sei $p \geq 5$ eine Primzahl. Nach Voraussetzung ist D_0 durch p teilbar und demnach

$$D_0 = D_0^* \, p$$

mit einer natürlichen Zahl D_0^*. Man hat folglich:

$$\eta_p = \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} p^k (D_1 u_0^2)^{\frac{p-1}{2}-k} (D_0^* \, v^2)^k .$$

In dieser Reihenentwicklung sind die beiden ersten Binomialkoeffizienten

$$\binom{p}{1} = p \qquad \text{und} \qquad \binom{p}{3} = \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3}$$

genau durch die erste Potenz von p teilbar und die übrigen auch ganz rational; von den Summanden

$$\binom{p}{2k+1} p^k (D_1 u_0^2)^{\frac{p-1}{2}-k} (D_0^* \, v^2)^k \qquad \left(k = 0, 1, \ldots, \tfrac{p-1}{2}\right)$$

von η_p sind demnach alle bis auf den ersten Multipla von p^2, und also besteht die Kongruenz

$$\eta_p \equiv p (D_1 u_0^2)^{\frac{p-1}{2}} \pmod{p^2},$$

aus der wegen

$$(p, D_1 u_0^2) = 1$$

folgt, dass η_p wohl durch p, nicht aber durch p^2 teilbar ist. Da im Fall a in η_p und im Fall b in $2^{-\frac{p-1}{2}} \eta_p$ auch keine andere Primzahl als p aufgehen kann, so muss demnach im Fall a

$$\eta_p = p$$

und im Fall b

$$\eta_p = 2^{\frac{p-1}{2}} p$$

sein. In der Reihenentwicklung von η_p sind nun jedoch alle Summanden positiv und treten mindestens drei Summanden auf;

berücksichtigen wir nur den letzten davon, so ist also insbesondere

$$\eta_p > p^{\frac{p-1}{2}} (D_0^* v^2)^{\frac{p-1}{2}} \geq p^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} p \cdot \frac{\left(\frac{p}{2}\right)^{\frac{p-3}{2}}}{2}$$

und folglich wegen $p \geq 5$

$$\eta_p > 2^{\frac{p-1}{2}} p,$$

so dass in beiden Fällen a und b die Zahl η_p nicht von der verlangten Form ist, und somit p wirklich nicht zu $\mathfrak{n}(D, A)$ gehört.

8) Wir betrachten weiter die Primzahl $p = 3$ und wollen zunächst annehmen, dass D_0 nicht nur durch 3, sondern sogar durch 9 teilbar ist; sei demnach

$$D_0 = 9D_0^{**}$$

mit einer natürlichen Zahl D_0^{**}. Man hat alsdann

$$\eta_3 = 3D_1 u_0^2 + 9D_0^{**} v^2,$$

also

$$\eta_3 \equiv 3D_1 u_0^2 \pmod 9,$$

so dass wegen

$$(3, D_1 u_0^2) = 1$$

die Zahl η_3 durch 3 und nicht durch 9 teilbar ist. Entsprechend wie im vorigen Paragraphen folgt somit, dass η_3 im Fall a gleich 3 und im Fall b gleich $2 \cdot 3$ sein muss; der vorigen expliziten Formel für η_3 entnimmt man aber unmittelbar, dass η_3 grösser als jeder dieser beiden Werte ist und somit unter der Annahme $9 \mid D_0$ die Primzahl $p = 3$ ebenfalls nicht in der Menge $\mathfrak{n}(D, A)$ vorkommt.

9) Sei endlich, wie im vorigen Paragraphen, $p = 3$ und D nur durch 3, nicht aber durch 9 teilbar. Wie wir zeigen wollen,

«gehört in diesem Fall vielleicht $n = 3$, jedenfalls aber nicht $n = 9$ und erst recht keine höhere Potenz von 3 zu $\mathfrak{n}(D, A)$.»

Vorab werde bemerkt, dass wegen der Definitionsformeln

$$A \mid 2D, \quad D_1 = (D, A), \quad A = A_0 D_1$$

offenbar Fall a dann und nur dann vorliegt, wenn

$$A_0 = \mp 1,$$

und Fall b dann und nur dann, wenn

$$A_0 = \mp 2$$

ist; andere Werte kann A_0 natürlich nicht annehmen. Somit gehört $n = 3$ dann und nur dann zu $\mathfrak{n}(D, A)$, wenn η_3 die Form

$$\eta_3 = |A_0| \cdot 3^l$$

mit einem Exponenten l, der eine natürliche Zahl ist, besitzt.

Von jetzt ab werde vorausgesetzt, dass $n = 3$ zu $\mathfrak{n}(D, A)$ gehört, so dass also die beiden Gleichungen

$$D_1 u_0^2 - D_0 v^2 = A_0,$$

$$3D_1 u_0^2 + D_0 v^2 = |A_0| \cdot 3^l$$

bestehen, aus denen umgekehrt

$$D_1 u_0^2 = \frac{|A_0| \cdot 3^l + A_0}{4}, \qquad D_0 v^2 = \frac{|A_0| \cdot 3^l - 3A_0}{4}$$

folgt. Setzt man diese Ausdrücke in

$$\eta_9 = \binom{9}{1}(D_1 u_0^2)^4 + \binom{9}{3}(D_1 u_0^2)^3 (D_0 v^2)^1 + \binom{9}{5}(D_1 u_0^2)^2 (D_0 v^2)^2 + \\ + \binom{9}{7}(D_1 u_0^2)^1 (D_0 v^2)^3 + (D_0 v^2)^4$$

ein, so ergibt sich nach einiger Rechnung die Formel

$$|A_0|^{-4} \eta_9 = 3^{l+1}(3^{3l-1} - \varepsilon \cdot 3^{2l} + \varepsilon), \qquad \varepsilon = \frac{A_0}{|A_0|} = \operatorname{sgn} A_0,$$

und, falls auch $n = 9$ zu $\mathfrak{n}(D, A)$ gehörte, müsste die rechte Seite dieser Gleichung eine reine Potenz von 3 sein. Offenbar ist das aber allein möglich für $\varepsilon = +1$, $l = 1$, also in den beiden Fällen

$A_0 = +1$, $D_1 u_0^2 = 1$, $D_0 v^2 = 0$ und $A_0 = +2$, $D_1 u_1^2 = 2$, $D_0 v^2 = 0$,

und diese sind evidenterweise sinnlos und auszuschliessen. Damit ist die obige Behauptung bewiesen.

10) Die Ergebnisse der drei letzten Paragraphen führen zu der vollständigen Lösung der Frage, alle Elemente von $\mathfrak{M}(D, A)$ zu bestimmen. Denn die zugehörigen Indizes n aus $\mathfrak{n}(D, A)$ sind ungerade, nach § 7 durch keine Primzahl $p \geq 5$ und nach dem

letzten Paragraphen auch nicht durch 9 teilbar. Also sind nur folgende drei Möglichkeiten vorhanden:

I: Die Menge $\mathfrak{n}(D, A)$ ist leer.
II: Die Menge $\mathfrak{n}(D, A)$ enthält nur das Element $n = 1$.
III: Die Menge $\mathfrak{n}(D, A)$ enthält nur die beiden Elemente $n = 1$ und $n = 3$, aber keine weiteren.

Indem man die Bedeutung von $\mathfrak{n}(D, A)$ berücksichtigt, lässt sich also auch die folgende Aussage machen:

Satz 1: Ist $A \neq 1$ und $A \neq -D$, so ist die Menge $\mathfrak{N}(D, A)$ entweder leer, oder sie besteht aus den vier Paaren

$$(\pm u, \quad \mp v),$$

oder sie besteht aus den acht Paaren

$$(\pm u, \mp v), \quad \left(\pm \frac{u^3 + 3uv^2D}{|A|}, \mp \frac{3u^2v + v^3D}{|A|}\right).$$

Dabei bezeichnet u, v das Fundamentalpaar.

Zusammen mit den ergänzenden Sätzen des § 1 für die ausgeschlossenen Fälle $A = 1$ und $A = -D$ ist damit $\mathfrak{N}(D, A)$ in allen Fällen ermittelt. Dabei ist es in jedem numerischen Fall, d. h. für gegebene Zahlwerte von D und A, immer möglich, alle Elemente von $\mathfrak{N}(D, A)$ explizit *in endlichvielen Schritten* auszurechnen. Dies ist in der Tat für $A = -D$ trivial und folgt für $A = 1$ aus den klassischen Sätzen über die Fundamentallösung der Pellschen Gleichung. Sei ferner $A \neq 1$ und $A \neq -D$ und u, v das Fundamentalpaar von $\mathfrak{M}(D, A)$. Nach dem in § 2 zitierten Satz von Schepel stellen die natürlichen Zahlen

$$\xi = \left|\frac{2u^2 - A}{A}\right|, \qquad \eta = \left|\frac{2uv}{A}\right|$$

alsdann die Fundamentallösung der Pellschen Gleichung

$$\xi^2 - D\eta^2 = 1$$

dar und können somit, wie schon erwähnt, in endlichvielen Schritten gefunden werden; aus ihren Werten folgen aber alsdann die von u und v auf triviale Art, wenn überhaupt ein Fundamentalpaar u, v von $\mathfrak{M}(D, A)$ existiert. Ist dieses Paar aber erst einmal bekannt, so lässt sich sofort feststellen, welcher der drei in Satz 1 genannten Fälle vorliegt, und gibt es kein Paar u, v, so ist erst recht $\mathfrak{N}(D, A)$ leer.

11) Besonders interessant sind diejenigen Zahlpaare D, A, für die $\mathfrak{n}(D, A)$ aus den beiden Zahlen $n=1$ und $n=3$ besteht; wir wollen sie *singulär* und alle anderen *regulär* nennen. Vermöge der Formeln in § 9 gelingt es, alle singulären D, A zu bestimmen.

Ist D, A singulär, stellt u, v das Fundamentalpaar von $\mathfrak{M}(D, A)$, das natürlich existiert, dar, und sind die abgeleiteten Zahlen D_0, D_1, A_0 und u_0 nach § 5 ermittelt, so muss nach § 9 mit einer geeigneten natürlichen Zahl l

$$D_1 u_0^2 = \frac{|A_0| \cdot 3^l + A_0}{4}, \quad D_0 v^2 = \frac{|A_0| \cdot 3^l - 3A_0}{4}$$

sein; beide Brüche müssen also speziell positive ganze rationale Zahlen darstellen und ferner im Fall b, d. h. für $A_0 = \mp 2$ ungerade sein. Darin liegt eine Einschränkung für l, die, wie man leicht erkennt, sich nur mit den folgenden Werten für A_0 und l erfüllen lässt:

$$A_0=+1,\ l=2\lambda+1,\ D_1 u_0^2=\frac{3^{2\lambda+1}+1}{4},\ D_0 v^2=\frac{3^{2\lambda+1}-3}{4} \qquad (\lambda=1,2,3,\ldots);$$

$$A_0=-1,\ l=2\lambda,\ D_1 u_0^2=\frac{3^{2\lambda}-1}{4},\ D_0 v^2=\frac{3^{2\lambda}+3}{4} \qquad (\lambda=1,2,3,\ldots);$$

$$A_0=+2,\ l=2\lambda,\ D_1 u_0^2=\frac{3^{2\lambda}+1}{2},\ D_0 v^2=\frac{3^{2\lambda}-3}{2} \qquad (\lambda=1,2,3,\ldots);$$

$$A_0=-2,\ l=2\lambda+1,\ D_1 u_0^2=\frac{3^{2\lambda+1}-1}{2},\ D_0 v^2=\frac{3^{2\lambda+1}+3}{2} \qquad (\lambda=0,1,2,\ldots).$$

Diese Formeln bestimmen zu gegebenem λ und A_0 noch nicht unmittelbar die Zahlen D_0, D_1, u_0, v sondern zunächst nur $D_1 u_0^2$ und $D_0 v^2$. Die Werte von D_1 und u_0 können aus ihnen aber leicht gewonnen werden, denn es ist ja $(D_1, u_0)=1$ und D_1 ist als Teiler von A quadratfrei; der Ausdruck für $D_1 u_0^2$ muss demnach eine Primzahlzerlegung besitzen, in der die Exponenten der einzelnen Primzahlen entweder gleich Eins oder gleich einer geraden Zahl sind, und alsdann ist D_1 das Produkt der Primzahlpotenzen mit Exponent Eins und u_0^2 das Produkt der übrigen Primzahlpotenzen. (Solche λ, für die der Bruch $\frac{3^{2\lambda+1}+1}{4}$, bzw. $\frac{3^{2\lambda}-1}{4}$, bzw. $\frac{3^{2\lambda}+1}{2}$, bzw. $\frac{3^{2\lambda+1}-1}{2}$

nicht eine Primzahlzerlegung der verlangten Art besitzt, sind dabei von der Betrachtung auszuschliessen.) Aus dem Wert von $D_0 v^2$ lässt sich dagegen D_0 und v nicht unbedingt eindeutig erschliessen, sondern es ist erlaubt, quadratische Faktoren von D_0 auf v^2 und umgekehrt zu übernehmen.

Seien nach diesen Vorschriften zu gegebenem A_0 und λ die Zahlen

$$D_0,\ D_1,\ u_0,\ v$$

ermittelt worden; dieselben genügen dann nach Konstruktion und wegen

$$D_1 u_0^2 - D_0 v^2 = A_0$$

den Relationen

$$(D_1, u_0) = 1, \quad (D_0 v^2,\ D_1 u_0^2) = 1,$$

und sind ferner im Fall b, d. h. für $|A_0| = 2$ alle vier ungerade. *Setzt man*

$$D = D_0 D_1, \quad A = A_0 D_1, \quad u = u_0 D_1,$$

so stellen u, v das Fundamentalpaar von $\mathfrak{M}(D, A)$ dar. Denn beide Zahlen sind so konstruiert, dass in v und in $3D_1 u_0^2 + D_0 v^2$ und daher auch in $\dfrac{3u^2 v + v^3 D}{|A|}$ nur solche Primzahlen aufgehen, die auch Teiler von D sind; wegen

$$u^2 - D v^2 = A \quad \text{und} \quad \left(\frac{u^3 + 3uv^2 D}{|A|}\right)^2 - D\left(\frac{3u^2 v + v^3 D}{|A|}\right)^2 = A$$

gehören daher die acht Paare

$$(\pm u,\ \pm v) \quad \text{und} \quad \left(\pm\frac{u^3 + 3uv^2 D}{|A|},\ \pm\frac{3u^2 v + v^3 D}{|A|}\right)$$

mit $v < \dfrac{3u^2 v + v^3 D}{|A|}$ zu $\mathfrak{N}(D, A)$, und das ist nach Satz 1 nur möglich, wenn das Fundamentalpaar von $\mathfrak{N}(D, A)$ durch u, v gegeben wird.

12) Indem man in die Formeln des letzten Paragraphen für $D_1 u_0^2$ und $D_0 v^2$ für λ der Reihe nach die Zahlen $1, 2, 3, \ldots$ bzw. $0, 1, 2, \ldots$ einsetzt, kommt man zu beliebig vielen singulären Paaren D, A und den Fundamentalpaaren der zugehörigen Mengen $\mathfrak{M}(D, A)$; man vergleiche hierzu die Tabelle, wo die niedersten

Fälle und zwar jeweils mit den Primzahlzerlegungen von D, A, u und v zusammengestellt sind. Man beachte, dass für alle diese singulären Paare D immer durch 3, nicht aber durch 9 teilbar ist, wie es ja auch sein muss.

Aus den Formeln aus § 11 lassen sich allgemeine Aussagen darüber gewinnen, wann Paare D, A singulär sind. Sei etwa $A = -1$, also

$$D_1 = 1, \quad D_0 = D, \quad A_0 = -1, \quad u_0 = u.$$

Da die Gleichung

$$u_0^2 = \frac{3^{2\lambda} - 1}{4}$$

gewiss keine Lösungen in natürlichen Zahlen u_0 und λ besitzt, *so ist jedes Paar $D, -1$ regulär und also die Menge $\mathfrak{N}(D, -1)$ für jede natürliche Zahl D, die kein Quadrat ist, entweder leer, oder sie besteht nur aus den vier Paaren*

$$(\pm u, \pm v).$$

Diese Verschärfung von Satz 1 ist identisch mit dem in § 1 erwähnten zweiten Satz von C. Störmer.

Ist ferner $A = +2$, also

$$D_1 = 1, \ D_0 = D, \ A_0 = +2, \ u_0 = u, \text{ bzw. } D_1 = 2, D_0 = \frac{D}{2}, \ A_0 = +1, \ u_0 = \frac{u}{2},$$

so ist $D, +2$ höchstens dann singulär, wenn die Gleichung

$$2u_0^2 = 3^{2\lambda} + 1, \qquad \text{bzw.} \qquad 8u_0^2 = 3^{2\lambda+1} + 1$$

sich in natürlichen Zahlen u_0, λ befriedigen lässt; beide sind aber unlösbar, da es nichtmals eine ganze rationale Zahl a mit

$$2a^2 \equiv 1 \pmod 9$$

gibt. *Folglich ist jedes Paar $D, +2$ regulär, so dass $\mathfrak{N}(D, +2)$ entweder gar keine Elemente besitzt oder nur die vier Paare $(\pm u, \pm v)$.*

Drittens sei $A = -2$, also

$$D_1 = 1, \ D_0 = D, \ A_0 = -2, \ u_0 = u, \text{ bzw. } D_1 = 2, D_0 = \frac{D}{2}, \ A_0 = -1, \ u_0 = \frac{u}{2}.$$

Damit $D, -2$ singulär ist, muss die Gleichung

$$(2u_0)^2 - 6(3^\lambda)^2 = -2, \quad \text{bzw.} \quad (4u_0)^2 - 18(3^{\lambda-1})^2 = -2$$

eine Lösung in natürlichen u_0 und einer ganzen Zahl $\lambda \geq 0$, bzw. $\lambda \geq 1$ besitzen. Beidemal kommt man damit auf eine

Frage von der in dieser Arbeit behandelten Art, und man kann Satz 1 anwenden, um alle Lösungen zu finden. Das Ergebnis, zu dem man auf diese Weise gelangt, lautet:

«*Es gibt genau drei singuläre Paare* $D, -2$, *nämlich* $3, -2$ *und* $6, -2$ *und* $123, -2$; *zu ihnen gehören die Mengen*

$\mathfrak{N}(3, -2)$ *mit den Elementen* $(\mp 1, \mp 1), (\mp 5, \mp 3),$
$\mathfrak{N}(6, -2)$ *mit den Elementen* $(\mp 2, \mp 1), (\mp 22, \mp 9),$
$\mathfrak{N}(123, -2)$ *mit den Elementen* $(\mp 11, \mp 1), (\mp 2695, \mp 243).$

Für jedes andere D *ist die Menge* $\mathfrak{N}(D, -2)$ *entweder leer, oder sie enthält allein die Elemente* $(\mp u, \mp v)$.»

13) Andere Werte von A lassen sich auf ähnliche Art behandeln; dabei reduziert sich die Bestimmung aller D, so dass D, A singulär ist, jedesmal auf die Bestimmung aller ganzzahligen Lösungen endlichvieler Diophantischer Gleichungen für u_0 und λ:

Für $2 \mid A$, $A > 0$ ist
entweder

$$A_0 = +1,\ D_1 = A,\ D_1 u_0^2 = \frac{3^{2\lambda+1}+1}{4},\quad D_0 v^2 = \frac{3^{2\lambda+1}-3}{4},\quad D = D_0 D_1,\ u = u_0 D_1,$$

oder

$$A_0 = +2,\ D_1 = \frac{A}{2},\ D_1 u_0^2 = \frac{3^{2\lambda}+1}{2},\quad D_0 v^2 = \frac{3^{2\lambda}-3}{2},\quad D = D_0 D_1,\ u = u_0 D_1.$$

Für $2 \mid A$, $A < 0$ ist
entweder

$$A_0 = -1,\ D_1 = |A|,\ D_1 u_0^2 = \frac{3^{2\lambda}-1}{4},\quad D_0 v^2 = \frac{3^{2\lambda}+3}{4},\quad D = D_0 D_1,\ u = u_0 D_1,$$

oder

$$A_0 = -2,\ D_1 = \frac{|A|}{2},\ D_1 u_0^2 = \frac{3^{2\lambda+1}-1}{2},\quad D_0 v^2 = \frac{3^{2\lambda+1}+3}{2},\quad D = D_0 D_1,\ u = u_0 D_1.$$

Für $2 \nmid A$, $A > 0$ ist

$$A_0 = +1,\ D_1 = A,\ D_1 u_0^2 = \frac{3^{2\lambda+1}+1}{4},\quad D_0 v^2 = \frac{3^{2\lambda+1}-3}{4},\quad D = D_0 D_1,\ u = u_0 D_1.$$

Für $2 \nmid A$, $A < 0$ ist

$$A_0 = -1,\ D_1 = |A|,\ D_1 u_0^2 = \frac{3^{2\lambda}-1}{4},\quad D_0 v^2 = \frac{3^{2\lambda}+3}{4},\quad D = D_0 D_1,\ u = u_0 D_1.$$

Jedesmal ist vermöge dieser Formeln jede Lösung λ zu bestimmen, für die u_0 teilerfremd zu D_1 wird; vermöge dieses λ

sind dann D_0 und v bis auf höchstens endlichviele Möglichkeiten bestimmt, so dass jedem λ insbesondere höchstens endlichviele D zugehören, für die D, A singulär ist. Andrerseits besitzt eine jede einzelne der vorigen Gleichungen für u_0 und λ höchstens endlichviele Lösungssysteme. Diese Behauptung ergibt sich sogleich aus dem bekannten Satz von Pólya, wonach die grösste Primzahl, die in dem Ausdruck at^2+bt+c mit ganzen rationalen Koeffizienten a, b, c mit $b^2-4ac \neq 0$ aufgeht, über alle Grenzen wächst, falls t durch alle natürlichen Zahlen läuft; insbesondere kann das Polynom daher nur für höchstens endlichviele t eine reine Potenz von 3 sein.

Also erhalten wir:

Satz 2: Zu jeder quadratfreien Zahl A gibt es höchstens endlichviele natürliche Zahlen D mit $A \mid 2D$, die kein Quadrat sind, so dass D, A singulär ist; folglich ist für alle genügend grosse D die Menge $\mathfrak{N}(D, A)$ entweder leer, oder sie enthält nur die Paare $(\pm u, \pm v)$.

TABELLE SINGULÄRER PAARE D, A UND DER ZUGEHÖRIGEN u, v:

$A_0 = +1$:	$D = 2.3.7$	$A = 7$	$u = 7$	$v = 1$
	$3.5.61$	61	61	2
	$2.3.7.13.547$	547	547	1
	$2.3.5.7.19.37.41$	$7.19.37$	$7.19.37$	2
$A_0 = -1$:	$D = 2.3$	$A = -2$	$u = 2$	$v = 1$
	$3.5.7$	-5	2.5	1
	$2.3.7.13.61$	$-2.7.13$	$2.7.13$	1
	$2.3.7.19.37.61$	-2.61	$2.11.61$	1
$A_0 = +2$:	$D = 3.5$	$A = 2.5$	$u = 5$	$v = 1$
	$3.13.41$	2.41	41	1
	$3.5.73$	$2.5.73$	5.73	11
	$3.17.193.1093$	$2.17.193$	17.193	1
	$3.13.757.1181$	2.1181	5.1181	1
$A_0 = -2$:	$D = 3$	$A = -2$	$u = 1$	$v = 1$
	$3.5.13$	-2.13	13	1
	3.41	-2	11	1
	$3.5.73.1093$	-2.1093	1093	1
	$3.13.17.193.757$	$-2.13.757$	13.757	1

II.

Bezeichnungen: Der Kürze halber bezeichnet im Folgenden:

A_0 eine feste unter den vier Zahlen $+1$, -1, $+2$ und -2,

D_1 eine feste zu A_0 teilerfremde quadratfreie natürliche Zahl,

z eine veränderliche und genügend grosse positive Zahl,

$M(z)$ die Menge aller natürlichen Zahlen x_0 mit $(x_0, A_0)=1$, für die

$$D_1 x_0^2 - A_0$$

positiv und allein durch Primzahlen $p \leq z$ teilbar ist,

$m(z)$ das grösste Element x_0 von $M(z)$.

Wir stellen uns das Ziel:

«*Ein Verfahren anzugeben, durch das sich zu gegebenen Werten von* A_0, D_1 *und* z *alle Elemente* x_0 *der Menge* $M(z)$ *bestimmen lassen, und eine obere Schranke für* $m(z)$ *herzuleiten.*»

14) Auf Grund der beiden Voraussetzungen

$$(A_0, D_1) = 1, \qquad (A_0, x_0) = 1$$

ist $D_1 x_0^2 - A_0$ für jede Zahl x_0 zu der offenbar quadratfreien Zahl

$$A = D_1 A_0$$

teilerfremd. Wir wollen mit

$$\pi = \pi(z \mid A)$$

die Anzahl aller verschiedenen nicht in A aufgehenden Primzahlen $p \leq z$ und mit

$$p_1, p_2, \ldots, p_\pi$$

diese Primzahlen selbst, nach steigender Grösse geordnet, bezeichnen; dabei möge z so gross angenommen werden, dass $\pi \geq 1$ ist. Da allein solche x_0 betrachtet werden, für die $D_1 x_0^2 - A_0$ positiv ist, so gehört jedes x_0 mit $(x_0, A_0) = 1$ dann und nur dann zu $M(z)$, wenn es hierzu π nichtnegative ganze rationale Zahlen $h_1, h_2, \ldots, h_\pi$ gibt, so dass

$$D_1 x_0^2 - A_0 = p_1^{h_1} p_2^{h_2} \ldots p_\pi^{h_\pi}$$

ist. Setzt man

$$k_\tau = \begin{cases} 0 \text{ für } h_\tau = 0, \\ 1 \text{ für } h_\tau \equiv 1 \pmod 2, \\ 2 \text{ für } h_\tau \equiv 0 \pmod 2,\ h_\tau > 0 \end{cases} \qquad (\tau = 1, 2, \ldots, \pi)$$

und

$$D_0 = p_1^{k_1} p_2^{k_2} \dots p_\pi^{k_\pi}, \quad y = p_1^{\frac{h_1 - k_1}{2}} p_2^{\frac{h_2 - k_2}{2}} \dots p_\pi^{\frac{h_\pi - k_\pi}{2}},$$

so geht diese Gleichung über in

$$D_1 x_0^2 - A_0 = D_0 y^2,$$

also in

$$x^2 - Dy^2 = A,$$

wenn die Bezeichnungen

$$D = D_0 D_1, \quad A = A_0 D_1, \quad x = x_0 D_1$$

benutzt werden. Dabei hat

$$D = D_0 D_1 = D_1 p_1^{k_1} p_2^{k_2} \dots p_\pi^{k_\pi}$$

höchstens 3^π verschiedene Möglichkeiten, da die Exponenten $k_1, k_2, \dots, k_\pi$ einzeln nur der Werte 0, 1, 2 fähig sind. Weiter ist y eine natürliche Zahl, in der allein solche Primzahlen aufgehen, die auch D_0 und daher erst recht D teilen. Die Zahl A ist, wie schon erwähnt, quadratfrei; x und y sind offenbar teilerfremd, und endlich noch ist

$$A \mid 2D, \quad (D_0, D_1) = 1, \quad (A, D) = D_1.$$

Da nach Voraussetzung D_1 quadratfrei ist, so wird D dann und nur dann ein Quadrat, wenn $D_1 = 1$ und jeder Exponent $k_1, k_2, \dots, k_\pi$ gleich Null oder Zwei ist. Da die alsdann entstehenden Gleichungen

$$x^2 - d^2 y^2 = A,$$

wo d die natürliche Zahl $\sqrt{D}$ und A eine der vier Zahlen $+1$, -1, $+2$ oder -2 bezeichnet, aber offenbar keine Lösungen in natürlichen Zahlen besitzen, so brauchen diese Werte von D nicht berücksichtigt zu werden.

Weiter ist dann und nur dann $A = -D$, wenn gleichzeitig $A_0 = -1$, also $A = -D_1$, und $D_0 = 1$, also $D = D_1$ ist; die alsdann entstehende Gleichung

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

hat aber nach § 1 keine Lösung in natürlichen Zahlen x, y, derart dass in y nur solche Primzahlen aufgehen, die auch D_1 teilen, und somit braucht in diesem Fall der Wert $D = D_1$ nicht beachtet zu werden.

15) Aus Satz 1, bzw. dem Störmerschen Satz in § 1 für den Ausnahmefall $A = 1$ (d. h. $A_0 = D_1 = 1$) ergibt sich damit folgendes Verfahren zur Bestimmung aller Elemente x der Menge $M(z)$:

Zum gegebenen z bestimmt man alle zu $A = A_0 D_1$ teilerfremden Primzahlen

$$p_1, p_2, \ldots, p_\pi,$$

die nicht grösser als z sind, und alsdann alle Zahlen der Form

$$D = D_1 p_1^{k_1} p_2^{k_2} \ldots p_\pi^{k_\pi},$$

deren Exponenten $k_1, k_2, \ldots, k_\pi$ gleich 0, 1 oder 2 sind, wobei aber für $D_1 = 1$ jede Quadratzahl D und für $A_0 = -1$ die Zahl $D = D_1$ fortzulassen ist. Seien

$$D^{(1)}, D^{(2)}, \ldots, D^{(t)}$$

die so erhaltenen verschiedenen Werte von D; die Anzahl t dieser Zahlen ist höchstens gleich 3^π. Zu jedem einzelnen Wert $D^{(\tau)}$ von D sucht man dann das Fundamentalpaar $u_\tau = u(D^{(\tau)})$, $v_\tau = v(D^{(\tau)})$ der Menge $\mathfrak{M}(D^{(\tau)}, A)$, falls ein solches überhaupt existiert; dies sei etwa für die Indizes

$$\tau = \tau_1, \tau_2, \ldots, \tau_s \qquad (0 \leq s \leq t)$$

und für keine anderen aus der Folge 1, 2, ..., t der Fall. Es gehört jetzt

$$x_0^{(\sigma)} = \frac{u_{\tau_\sigma}}{D_1}$$

dann und nur dann zu $M(z)$, wenn nur solche Primzahlen in v_{τ_σ} aufgehen, die auch Teiler von $D^{(\tau_\sigma)}$ sind. Ist ferner $D^{(\tau_\sigma)}$, A singulär, so gehören sogar beide Zahlen

$$x_0^{(\sigma)} = \frac{u_{\tau_\sigma}}{D_1} \quad \text{und} \quad x_0^{(\sigma)*} = \frac{u_{\tau_\sigma}^3 + 3u_{\tau_\sigma} v_{\tau_\sigma}^2 D^{(\tau_\sigma)}}{|A| D_1}$$

zu $M(z)$; unabhängig von dem Wert von z kann dies aber nach Satz 2 jedenfalls nur höchstens für eine beschränkte Anzahl von Zahlen $D^{(\tau_\sigma)}$ der Fall sein.

Also folgt speziell, dass für über alle Grenzen wachsendes z die Menge $M(z)$ höchstens

$$3^{\pi(z|A)} + O(1)$$

Elemente besitzt.

16) Nachdem so gezeigt worden ist, wie sich alle Elemente von $M(z)$ finden lassen, soll nunmehr eine obere Schranke für das Maximum $m(z)$ der Elemente x_0 dieser Menge hergeleitet werden.

Da nur endlichviele D existieren, für die D, A singulär ist, so wird $m(z)$ für alle hinreichend grossen z einen Wert

$$m(z) = x_0^{(\sigma)} = \frac{u_{\tau_\sigma}}{D_1}$$

haben, wo u_{τ_σ}, v_{τ_σ} das zu einem regulären Paar $D^{(\tau_\sigma)}, A$ gehörige Fundamentalpaar bezeichnet. Es genügt also, für die Zahlen u_{τ_σ}, v_{τ_σ} obere Abschätzungen zu bestimmen.

Im Ausnahmefall $A = 1$, also $A_0 = D_1 = 1$, ist u_{τ_σ}, v_{τ_σ} die Fundamentallösung der Pellschen Gleichung

$$\xi^2 - D^{(\tau_\sigma)} \eta^2 = 1$$

und also

$$u_{\tau_\sigma} + v_{\tau_\sigma} \sqrt{D^{(\tau_\sigma)}} \leq (8D^{(\tau_\sigma)})^{2\sqrt{D^{(\tau_\sigma)}}}$$

(wegen des Beweises dieser Ungleichung siehe meine Note «Über den grössten Primteiler der Polynome $x^2 + 1$, Satz 1), und folglich erst recht

(A): $$x_0^{(\sigma)} = \frac{u_{\tau_\sigma}}{1} \leq (8D^{(\tau_\sigma)})^{2\sqrt{D^{(\tau_\sigma)}}}$$

Sei dagegen $A \neq 1$. Da auch $A \neq -D^{(\tau_\sigma)}$ und $D^{(\tau_\sigma)}$ kein Quadrat ist, so wird alsdann nach § 2

$$(u_{\tau_\sigma} + v_{\tau_\sigma} \sqrt{D^{(\tau_\sigma)}})^2 = |A| (\xi + \eta \sqrt{D^{(\tau_\sigma)}}),$$

wo ξ, η die Fundamentallösung der Pellschen Gleichung

$$\xi^2 - D^{(\tau_\sigma)} \eta^2 = 1$$

bezeichnet und daher der schon soeben benutzten Ungleichung

$$\xi + \eta \sqrt{D^{(\tau_\sigma)}} \leq (8D^{(\tau_\sigma)})^{2\sqrt{D^{(\tau_\sigma)}}}$$

genügt. Somit wird in diesem Fall

$$u_{\tau_\sigma} + v_{\tau_\sigma} \sqrt{D^{(\tau_\sigma)}} \leq (A_0 D_1)^{1/2} (8D^{(\tau_\sigma)})^{\sqrt{D^{(\tau_\sigma)}}}$$

und erst recht

$$\text{(B):} \qquad x_0^{(\sigma)} = \frac{u_{\tau_\sigma}}{D_1} \leq \sqrt{\frac{A_0}{D_1}}\,(8D^{(\tau_\sigma)})^{\sqrt{D^{(\tau_\sigma)}}}.$$

In beiden Ungleichungen (A) und (B) ist $D^{(\tau_\sigma)}$ von der Form

$$D^{(\tau_\sigma)} = D_1 p_1^{k_1} p_2^{k_2} \cdots p_\pi^{k_\pi} \leq D_1 (p_1 p_2 \cdots p_\pi)^2,$$

und da $x_0^{(\sigma)}$ für geeignet gewähltes σ gleich $m(z)$ ist, so ergibt sich das folgende Paar von Ungleichungen:

Für $A = 1$:

$$m(z) \leq (8(p_1 p_2 \cdots p_\pi)^2)^{2p_1 p_2 \cdots p_\pi};$$

für $A \neq 1$:

$$m(z) \leq \sqrt{\frac{A_0}{D_1}}\,(8D_1 (p_1 p_2 \cdots p_\pi)^2)^{\sqrt{D_1}\, p_1 p_2 \cdots p_\pi}.$$

In denselben bezeichnet

$$p_1 p_2 \cdots p_\pi$$

das Produkt aller zu A teilerfremden Primzahlen, die nicht grösser als z sind, ist also nicht grösser als das Produkt aller Primzahlen $p \leq z$. Bedeutet ε eine beliebige positive Konstante und ist z grösser als eine von ε abhängige Schranke, so gilt folglich nach dem Primzahlsatz:

$$p_1 p_2 \cdots p_\pi \leq e^{\left(1+\frac{\varepsilon}{2}\right)z},$$

und demnach ist für $A = 1$

$$m(z) \leq (8e^{(2+\varepsilon)z})^{2e^{\left(1+\frac{\varepsilon}{2}\right)z}}$$

und für $A \neq 1$

$$m(z) \leq \sqrt{\frac{A_0}{D_1}}\,(8D_1 e^{(2+\varepsilon)z})^{\sqrt{D_1} e^{\left(1+\frac{\varepsilon}{2}\right)z}}.$$

In beiden Ungleichungen sind aber die rechten Seiten für genügend grosses z höchstens gleich

$$e^{e^{(1+\varepsilon)z}},$$

und da $D_1 x_0^2 - A_0$ für alle $x_0 \geq 3$ positiv ist, so lässt sich folgender Satz aussprechen:

Satz 3: Sei A_0 eine der vier Zahlen $+1, -1, +2$ oder -2, D_1 eine zu A_0 teilerfremde quadratfreie natürliche Zahl, ε eine positive Konstante und z eine positive Zahl, die grösser als eine von ε abhängige Schranke ist. Ist dann die natürliche Zahl x_0 zu A_0 teilerfremd und

$$x_0 > e^{e^{(1+\varepsilon)z}}$$

so geht in $D_1 x_0^2 - A_0$ eine Primzahl $p > z$ auf.

Man erkennt übrigens leicht, dass dieser Satz auch dann noch bestehen bleibt, wenn die Voraussetzungen, D_1 sei quadratfrei und zu A_0 teilerfremd und x sei zu A_0 teilerfremd, fallen gelassen werden.

Juli 1935.