Über die Teiler der Form $x^2 + Dy^2$

(O dzielnikach formy $x^2 + Dy^2$)

von

S. Lubelski

Diese Arbeit stellt die ersten 2 Teile der Abhandlung dar, welche von mir auf dem Kongress der slavischen Mathematiker in Warschau [1]) in den Hauptzügen besprochen wurde. Sie kann unter anderem auch als eine Einführung in die Theorie der binären quadratischen Formen, von einem neuen Standpunkte betrachtet, angesehen werden. Namentlich wird hier nur von der Form $x^2 + Dy^2$ und ihren Teilern gehandelt, dagegen werden die anderen binären quadratischen Formen derselben Diskriminante nicht in Betracht gezogen. Nichtsdestoweniger ergeben sich die wichtigsten Sätze der klassischen Theorie der binären quadratischen Formen aus dieser Terminologie; so ist z. B. der Hilfssatz II (Teil I) dem Lagrangeschen Satze über die Reduktion der binären quadratischen Formen aequivalent.

Der obige Standpunkt wird wohl auch unmittelbarer und auf kürzerem Wege zum Ziele führen. Größeres Interesse beansprucht aber die Tatsache, daß auch für die Verallgemeinerung der Theorie der binären quadratischen Formen auf algebraische Zahlkörper und rationale Funktionenkörper diese Methode von Bedeutung ist.

Bemerkung: Im folgenden wird angenommen:

1) In der Form $x^2 + Dy^2$ ist $D > 0$;
2) e. d. = eigentlich darstellbar;

[1]) s. d. Verfassers: Über die Teiler der Form $x^2 + Dy^2$. Comptes Rendus du 1-er Congrès des Mathématiciens des pays slaves (zurzeit unter der Presse).

3) e. D. = eingentliche Darstellung;
4) Q — der kleinste ungerade Teiler der Form x^2+Dy^2;
5) p/q — p ist ein Teiler von q (Bezeichnung von Prof. Landau);
6) $(p,q)=d$; d ist der größte gemeinschaftliche Teiler von p und q;
oder allgemeiner:
7) $(p,q)\gtreqless d$, — der größte gemeinschaftliche Teiler von p und q ist (entsprechend) größer, gleich oder kleiner als d.

ERSTER TEIL.

Einführung.

Schon Euler[1]) hat die Formen, deren Teiler durch dieselbe Form (eigentlich) darstellbar sind, behandelt. Er hat bewiesen, daß die Formen x^2+y^2, x^2+2y^2, x^2+3y^2 (eigentlich auch x^2+4y^2) diese Eigenschaft haben. Von Eichenberg[2]) wurde folgendes Kriterium für beliebige Formen angegeben: „ist der kleinste ungerade Teil $Q\,(Q>1)$ der Form $x^2+Dy^2\,(D>0)$ durch diese Form (eigentlich) darstellbar, so ist es auch jeder ungerade Teiler". — Es wird im folgenden bewiesen, daß diese Frage ganz einfach gelöst wird, indem:

„die Form $x+Dy^2$ $(D>0)$ (bzw. die Zahl Q) die genannte Eigen-
„schaft dann und nur dann hat, wenn $D=1, 2, 3, 4$ oder 7
„ist" (s. Satz I).

Obwohl dieses Kriterium eine derart beschränkte Anwendung hat, ist es jedenfalls Eichenbergs Verdienst, auf die Bedeutungs des kleinsten ungeraden Teilers hingewiesen zu haben. Es zeigt sich eben, daß:

„damit ein jeder ungerade Teiler L der Form x^2+Dy^2 $(D>0)$
„die Eigenschaft hat, daß entweder L oder 2^aL, wo a kon-
„stant und $a=0, 1, 2$ und für ungerade D auch $a=3$, durch die
„Form x^2+Dy^2 eigentlich darstellbar sein soll, genügt es, daß 2^aQ
„($Q=$ der kleinste ungerade Teiler der Form x^2+Dy^2) durch diese
„Form eigentlich darstellbar ist".

Um die Frage der Möglichkeit der Verallgemeinerung des Eichenberg-

[1]) Euler. Commentat. arith. collectae I 74, 210, 287.
[2]) S. Eichenberg. Über das quadratische Reziprozitätsgesetz und einige quadratische Zerfällungen der Primzahlen. Diss Göttingen 1886 S. 42; cf. Weber-Epstein. Enzyklop. der elementarmath. B. I 4-te Aufl. 1922 S. 266—271.

schen Satzes für beliebige a zu erledigen, wären noch die Fälle $a>3$ und $a=3$ bei geradem D, zu erwägen. Nun gilt der Satz:

„Ist jeder beliebige ungerade Teiler L der Form x^2+Dy^2 entweder
„selbst oder 2^aL, wo a konstant und $a\geqslant 3$ ist, eigentlich darstellbar,
„so ist

$$D=15, 23, 31, 2^a, 2^{a-1}, 2^{a-2}, 3, 2^{2b}, 7 \quad (b=\text{beliebig})$$

„und auch umgekehrt: für diese D existiert ein geeignetes a, wobei
„$a=3$ ist".

Satz I: „Ist jeder ungerade Teiler der Form x^2+Dy^2 durch
„diese Form darstellbar, so ist $D=1, 2, 3, 4$ oder 7".

Beweis. Infolge der Voraussetzung ist jeder ungerade Primteiler der Form x^2+Dy^2 e. d., also ist jeder ungerade Teiler der Form x^2+Dy^2 größer oder gleich D. Wenn demnach D ungerade ist, so hat die Zahl $1+D$ keinen ungeraden Teiler, die Zahl $1+D$ ist also eine Potenz der Zahl 2. Es sei $D>7$, also $16/(1+D)$.

Nun ist $9+D=8\left(\frac{1+D}{8}\right)$. Die Zahl N, wo

$$N=1+\frac{1+D}{8}=1+2\frac{1+D}{16}$$

ist ungerade und kleiner als D, was aber unmöglich ist, denn die Zahl N ist auch Teiler der Form x^2+Dy^2.

Es sei jetzt D gerade. Man erhält analog, daß die Zahlen D und 2^2+D Potenzen der Zahl 2 sind. Ist $D>4$, so ist $16/(2^2+D)$, folglich ist

$$4^2+D=4\left(3+\frac{2^2+D}{4}=4\left(3+2\frac{2^2+D}{8}\right)\right),$$

da $\left(3+2\frac{2^2+D}{8}\right)<D$, so kann kein Teiler dieser Zahl durch die Form x^2+Dy^2 e. d. sein. Also ist für gerades D: $D\leqslant 4$.

Daß für $D\leqslant 7$ die Formen x^2+y^2, x^2+2y^2, x^2+3y^2, x^2+4y^2, x^2+7y^2 diese und nur diese die Eigenschaft haben, daß jeder ihrer ungerade Teiler durch die entsprechende Form darstellbar und sogar e. d. ist, wird durch das Eichenbergsche Kriterium[1]) oder durch Satz III bewiesen.

Satz II: „Ist 2^aQ, wo a konstant und $a=0, 1, 2, 3$, durch die Form x^2+Dy^2 e. d., so ist:
für $a=0$: $Q=5, 3, 7$);

[1]) S. Eichenberg, l. c. S. 2.

für $a=1,2$: $Q=E\frac{1+D}{2^a}$ ($E=$ Entier);

für $a=3$, wenn nur $D=7,15,23,31$, so ist Q entsprechend gleich: $Q=7,3,3,5$ in allen anderen Fällen ist: $Q=\frac{1+\frac{D}{4}}{2}$ ^{a}.

Beweis. Es sei zuerst D Potenz der Zahl $2: D=2^b$. Ist b ungerade, so ist

$$\left(2^{\frac{b-1}{2}}\right)^2+D=2^{b-1}(1+2)\equiv 0. \pmod 3$$

Ist aber b gerade, so ist

$$\left(2^{\frac{b-2}{2}}\right)^2+D=2^{b-2}(1+4)\equiv 0, \pmod 5$$

demnach ist entweder $Q=3$ oder $Q=5$.

Ist $2^a/D$ und D keine Potenz der Zahl 2, so folgt, da D einen ungeraden Teiler hat, daß $Q\leqslant\frac{D}{2^a}$, es ist aber $2^a Q$ e. d., also $2^a Q\geqslant D$, demnach ist hier $Q=\frac{D}{2^a}$.

Wir betrachten jetzt den Fall: $(D,2)<2^a$.

Nun können wir $a>0$ annehmen, denn für $a=0$ ist der Satz schon bewiesen.

Ist $a=1,2$ und D ungerade, so folgt, da für gewisse r, s:

$$2^a Q=r^2+Ds^2 \quad (r,s)=1 \tag{1}$$

ist, und da $r^3\equiv s^2\equiv 1 \pmod 8$, also $2^a Q\equiv r^2+Ds^2\equiv 1+D \pmod 8$, daß $(1+D, 2^{a+1})=(2^a Q, 2^{a+1})=2^a$. Es muß also $Q\leqslant\frac{1+D}{2^a}$ (wo $a=1,2$) sein. Da aber $2^a Q$ e. d. ist, so ist (für $a=1,2$):

$$Q=\frac{1+D}{2^a}.$$

Es sei jetzt D gerade, aber nicht $2^a/D$ auch sei $a=1,2,3$. Es folgt, wie vorher, daß gleichzeitig D gerade und $(D,2^a)<2^a$, nur dann bestehen können, wenn $a=3$ ist. Demnach ist $4/D$ unp $2Q=\left(\frac{1}{2}r\right)^2+\frac{D}{4}s^2$, wo $\left(\frac{1}{2}r,s\right)=1$. Es ist also $2Q$ durch die Form $x^2+\frac{D}{4}y^2$ e. d., da $\frac{D}{4}$ ungerade ist, so er-

gibt sich infolge des vorigen Falles:

$$Q=\frac{1+\frac{D}{4}}{2}.$$

Wir betrachten jetzt den letzten Fall: $a=3$ und D ungerade.

Für die Formen x^2+7y^2 und x^2+15y^2 ist entsprechend $Q=7$ und $Q=3$. Wir können also $D>15$ annehmen, ist demnach $1+D$ Potenz der Zahl 2, so ist $32/(1+D)$ und es folgt

$$49+D=16\left(3+2\frac{1+D}{16}\right), \quad \text{also} \quad Q=\frac{49+D}{16}$$

mithin ergibt sich, da $8Q$ e. d. ist:

$$\frac{9+D}{8}\leqslant Q\leqslant\frac{49+D}{16}$$

was nur für $D\leqslant 31$ möglich ist.

Ist aber $1+D$ keine Potenz der Zahl 2, so ist $1+D=8Q$, also

$$9+D=8\left(1+\frac{1+D}{8}\right)=8(1+Q),$$

demnach ist $9+D$ Potenz der Zahl 2. Nun ist

$$25+D=16+9+D=16\left(1+2\frac{9+D}{8}\right),$$

also ist

$$\frac{1+D}{8}\leqslant Q\leqslant\frac{25+D}{16},$$

was nur für $D\leqslant 23$ möglich ist.

Aus den Relationen (1) ergibt sich, daß $D\equiv -1 \pmod 8$, also für $D>15$ sind nur die Zahlen $D=23,31$ möglich, und tatsächlich ist für die Formen x^2+23y, $x^2+31y^2: 3/(1+23)$, $5/(4+31)$, also ist entsprechend $Q=3$ oder $Q=5$.

Hilfssatz I: „Ist $M=U^2+DV^2$ und $M_1=U_1^2+DV_1^2$, so ist in „in der Darstellung

$$MM_1=(UU_1+eDVV_1)^2+(UV_1-eVU_1)^2, \quad (e=\pm 1),$$

„der größte gemeinsame Teiler der Zahlen

$$(UU_1+eDVV_1,\ UV_1-eVU) \qquad (e=\pm 1),$$

„Teiler des größten gemeinsamen Teilers der Zahlen (M, M_1).

Beweis. Es ist einleuchtend, daß wir $(U, V) = (U_1, V_1) = 1$ annehmen können.

Bezeichnen wir der Kürze halber

$$UU_1 + eDVV_1 = A; \qquad UV_1 - eVU_1 = A_1 \qquad (e = \pm 1),$$

so ist

$$U_1 = \frac{AU - eDA_1V}{U^2 + DV^2}, \qquad V_1 = \frac{UA_1 + AeV}{U^2 + DV^2}.$$

Haben die Zahlen A und A_1 einen gemeinsamen Teiler, welcher in der Zahl $U^2 + DV^2$ nicht aufgeht, so wird ein echter Teiler dieser Zahl in den Zahlen U_1, V_1 aufgehen — entgegen der Annahme, daß sie relativ prim zueinander sind.

Analog wird es folgen, daß jeder gemeinsame Teiler der Zahlen A und A_1 auch Teiler der Zahl M_1 sein wird, — somit ist dieser Hilfssatz bewiesen.

Bemerkung: Ist

$$\frac{U}{V} \equiv \pm \frac{U_1}{V_1} \pmod{P}, \tag{1}$$

wo $P/(M, M_1)$ ist, so ist die Zahl $\frac{MM_1}{P^2}$ durch die Form $x^2 + Dy^2$ darstellbar. Es ist einleuchtend, daß die Kongruenz (1) immer besteht, wenn nur P Potenz einer ungeraden Primzahl ist. Ist aber $P = 2^k$, so ist (wenn nur wieder $P/M, M_1$):

$$\frac{U}{V} \equiv \frac{U_1}{V_1} \pmod{2^{k-1}},$$

und dann ist die Zahl $\frac{MM_1}{(2^{k-1})^2}$ durch die Form $x^2 + Dy^2$ darstellbar [3]).

Hilfssatz II: „Für jeden Teiler L der Form $x^2 + Dy^2$, wo $L > 2\sqrt{\frac{D}{3}}$ „findet man immer eine Zahl l, für welche eine Darstellung „$Ll = U^2 + DV^2$ gilt, wobei $l < 2\sqrt{\frac{D}{3}}$ und $(U, V)/l$ ist.

Beweis. Es sei l das kleinste Element der Menge aller Zahlen l_s mit der Eigenschaft, daß für gewisse ganze Zahlen U_s, V_s: $Ll_s = U_s^2 + DV_s^2$ $(U_s, V_s)/l_s$ ist, dabei gleichzeitig die Kongruenz

$$r_s^2 + D \equiv 0 \pmod{l_s}, \quad \text{wo} \quad V_s r_s \equiv U_s \pmod{l_s}$$

gilt. Ersichtlich kann man $0 \leqslant r \leqslant \frac{l_s}{2}$ annehmen.

[3]) vgl. d. Verf.: Beweis und Verallgemeinerung eines Waring-Legendreschen Satzes. Math. Zeitschr. (zurzeit unter der Presse) — Hilfssatz I.

Multiplizieren wir die Darstellungen der Zahlen

$$Ll = U^2 + DV^2 \quad \text{und} \quad ll' = r^2 + D,$$

(l' eine gewisse Zahl), so erhalten wir, gemäß der Eulerschen Identität

$$Ll^2l' = (Ur + DV)^2 + D(U - Vr)^2.$$

Es ist also die Zahl Ll' durch die Form $x^2 + Dy^2$ darstellbar, und dabei ist infolge des Hilfssatzes I: $(Ur + DV, U - Vr)/ll'$ und auch

$$Ur + DV \equiv (U - Vr)r \pmod{ll'}.$$

Demnach ist entweder $L = l'$ oder l' ein Element der obigen Menge und es muß $l \leqslant l'$ sein. Nun folgt aus der Gleichung (1) im Falle $l \leqslant l'$

$$l^2 < r^2 + D < \tfrac{1}{4}l^2 + D, \quad \text{also} \quad l < 2\sqrt{\tfrac{1}{3}D}.$$

Ist aber $L = l'$ und $L < l$, so wird ersichtlich $0 \leqslant r \leqslant \frac{1}{2}L$ sein, also analog $L \leqslant 2\sqrt{\frac{1}{3}D}$, entgegen der Voraussetzung. w. z. b. w.

Satz III: „Damit ein jeder ungerade Teiler L der Form $x^2 + Dy^2$ „die Eigenschaft habe, daß entweder L oder 2^aL, wo a „konstant und $a = 0, 1, 2$ und für ungerade D auch $a = 3$ „ist, durch die Form $x^2 + Dy^2$ eigentlich darstellbar „sein soll, genügt es, daß 2^aQ e. d. ist.

Beweis. Ist L ein ungerader Teiler der Form $x^2 + Dy^2$, so folgt aus dem Hilfssatze II, daß es eine solche (komplementäre) Zahl l gibt, für welche $lL = U^2 + DV^2$ $(U, V)/l$ und $l < 2\sqrt{\frac{1}{3}D}$ ist.

Für $2^a = 4$ hat die Form $x^2 + Dy^2$ keine ungeraden Teiler, welche $> 2\sqrt{\frac{D}{3}}$ wären, und zwar ergibt sich dies folgendermaßen: für $D < 24$ ist dies unmittelbar ersichtlich, also sei $D \geqslant 24$. Da 2^aQ e. d., so wäre

$$\tfrac{1}{4}D \leqslant 2\sqrt{\tfrac{1}{3}D},$$

welches aber für $D \geqslant 24$ unmöglich ist. Die Zahl l kann also für $2^a = 4$ nur Potenz der Zahl 2 sein, demnach folgt

$$\text{für } 2^a = 2, \quad D \text{ — beliebig und für } 2^a = 2^2, \quad D \text{ — ungerade,}$$

daß entweder $l = 1$ oder $l = 2^a$.

Ist $2^a = 4$ und D gerade, so ist $4/D$, also ist Q durch die Form $x^2 + \frac{D}{4}$ e. d., demnach ist es auch jeder beliebige ungerade Teiler dieser Form. Somit ist auch jeder beliebige ungerade Teiler L der Form $x^2 + Dy^2$

entweder selbst oder $4L$ durch diese Form e. d., und zwar entspricht der erste Fall einem geraden, der zweite Fall einem ungeraden v der Gleichung $L = u^2 + \frac{D}{4}v^2$. Wir betrachten jetzt den letzten Fall, wo gleichzeitig $a = 3$ und D ungerade ist, daher infolge des Satzes II: $D = 7, 15, 23, 31$.

Dem Satze I gemäß, kann man für $D = 7$, $l = 1$ annehmen. Für $D = 15, 23$, da $l < 2\sqrt{\frac{D}{3}}$ (s. Hilfssatz II), kann es nur $l = 3$ sein, und für $D = 31$, — $l = 5$. Nun ist

$$24 = 8 \cdot 3 = 3^2 + 15 = 1 + 23\,; \qquad 40 = 8 \cdot 5 = 3^2 + 31.$$

Ist $l \neq 1$, so ist also entsprechend $l = 3$ oder $l = 5$. Wir multiplizieren jetzt die Darstellung der Zahl L mit der Darstellung der Zahl 24 oder 40. Nach der Eulerschen Identität und Hilfssatze I (s. auch Bemerkung) erhalten wir, daß $8L$ durch die Form $x^2 + Dy^2$ e. d. ist.

w. z. b. w.

Wir werden jetzt die Frage der Möglichkeit der weiteren Verallgemeinerung des Eichenbergschen Kriteriums behandeln.

Satz IV: Voraussetzung:

„Ist L ein beliebiger ungerader Teiler der Form $x^2 + Dy^2$,
„so ist entweder L oder $2^A L$, wo A konstant und $A \geqslant 3$
„ist, durch diese Form eigentlich darstellbar.

Behauptung:

„1) sind alle L eigentlich darstellbar, so ist $D = 1, 2, 3, 4$
„oder 7.

„2) Ist D gerade, so ist höchstens $D = 2^A$, $2^{2b} \cdot 7$, wo b eine
„beliebige ganze Zahl, welche $\leqslant \frac{1}{2}(A-3)$ ist. Außer-
„dem kann für gerade A, — D höchstens $D = 2^{A-2} \cdot 3$, für
„ungerade A, — $D = 2^{A-1}$ sein;

in allen andern Fällen

„3) kann $A = 3$ angenommen werden und D höchstens:

$$D = 7,\ 15,\ 23,\ 32$$

„sein.

Beweis. Für $D = 1, 2, 3, 4$ oder 7 ist dieser Satz mit dem Satze III identisch. Wir werden also $D \neq 1, 2, 3, 4, 7$ annehmen.

Nun berücksichtigen wir folgende Fälle:

1. Ist D ungerade, so kann $A = 3$ angenommen werden und

$$D = (1, 3, 7)\ 15, 23, 31.$$

2. Ist D gerade und $2^A \leqslant 2^B = (2^{B+1}, D)$, so ist D eine Potenz der Zahl 2 und $A = B$.

3. Ist D gerade und $2^A > 2^B = (2^{B+1}, D)$, so ist $D = 2^{2b} \cdot 7$, wo $b \leqslant \frac{1}{2}(A-3)$, wobei für ungerade A höchstens $D = 2^{A-1}$, für gerade A, — $D = 2^{A-2} \cdot 3$ ist.

Wir beweisen zuerst den Fall 1.

Da $D \neq 1, 2, 3, 4, 7$, so ergibt sich mindestens ein ungerader Teiler der Form $x^2 + Dy^2$, welcher selbst nicht e. d. ist, also ist $2^A L$ durch diese Form e. d. Somit ist $D \equiv -1 \pmod 8$ und auch, wenn a das kleinste aller möglichen A ist, welche der Voraussetzung des Satzes genügen, $a \geqslant 3$.

Wir betrachten jetzt die ungeraden Zahlen H_1, H_2, H_3, welche den Gleichungen

$$1 + D = 2^{a_1} H_1\,, \quad 9 + D = 2^{a_2} H_2\,, \quad 25 + D = 2^{a_3} H_3$$

genügen. Eine der Zahlen H_2, H_3 ist relativ prim zu D; denn ist $(D, H_2) \neq 1$ und gleichzeitig $(D, H_3) \neq 1$, so folgt $15/D$, — da aber $2^A \cdot 3$ und $2^A \cdot 5$ e. d. sind, so ergibt sich nach der Multiplikation ihrer Darstellungen miteinander (s. Bemerkung zum Hilfssatze I), daß $3 \cdot 5 = 15$ e. d. durch die Form $x^2 + Dy^2$ ist, also ist $D = 15$. Aber für dieses D ($D = 15$) ist schon alles durch die Sätze II und III bewiesen, und wir schließen diesen Fall aus.

Wir bezeichnen die Zahl H_2 oder H_3, für welche $(H_g, D) = 1$, wo $g = 1$ oder $= 2$ ist, mit H'. Es ist also

$$(H', D) = 1 \quad \text{und} \quad 2^{a'} H' = 9 + D \quad \text{oder} \quad = 25 + D,$$

wo a' entweder $= a_2$ oder $= a_3$ ist. Nun ist eine der Zahlen a_1, a' höchstens gleich 3; denn ist $a_1 > 3$, so folgt aus

$$9 + D = 8 + 1 + D = 8\left(1 + 2\frac{1+D}{16}\right); \quad 25 + D = 8\left(3 + 2\frac{1+D}{16}\right),$$

daß $a' = 3$ sein muß.

Die Zahlen H_1 und H' sind Primzahlpotenzen; denn ist $p_1 p_2 / H_1$ oder $p_1 p_2 / H'$, wo p_1, p_2 verschiedene ungerade Primzahlen sind, so sind, da $p_1 < D$ und $p_2 < D$, gleichzeitig $2^A p_1$ und $2^A p_2$ e. d., also ist infolge des Hilfssatzes I auch $p_1 p_2$ e. d. Demnach ist H_1 oder H' durch eine Zahl, welche e. d. ist, teilbar, — dies ist aber unmöglich, denn eine solche ist mindestens gleich $4 + D$.

Mit H bezeichnen wir die Zahl H_1 oder H', wenn nur entsprechend $a_1 = 3$ oder $a' = 3$ ist. Also ist $8H$ e. d. Wir multiplizieren jetzt die Darstellung der Zahl $2^a H$ mit der Darstellung der Zahl $8H$. Vermittels des Hilfssatzes I (s. auch Bemerkung) erhalten wir, wenn nur die Zahl a größer als 3 angenommen wird, daß entweder

$$2^{a+3-2} = 2^{a+1} \quad \text{oder} \quad 2^{a-3+2} = 2^{a-1}$$

e. d. ist. Ist $2^a L$, wo L ein beliebiger ungerader Teiler der Form $x^2 + Dy^2$ bedeutet, e. d., so ergibt sich aus der Multiplikation mit der Darstellung der Zahl 2^{a+1} (wenn nur diese e. d. ist), daß

$$2^{a+1+2-2(a-1)} L = 2^3 L$$

e. d. Denselben Schluß erhalten wir, wenn nicht die Zahl 2^{a+3-2}, sondern 2^{a-3+2} e. d. ist; denn es folgt analog, daß die Zahl

$$2^{a+a-1-2(a-2)} L = 2^3 L$$

e. d. ist. Da der ungerade Teiler L beliebig gewählt wird, erhalten wir, daß $a = 3$ sein muß; also ist $8Q$ durch die Form $x^2 + Dy^2$ e. d., demnach kann nur, wegen Satz II, höchstens $D = 7, 15, 23, 31$ sein.

Beweis des Falles 2.

Der Annahme entgegen, sei die Zahl D_1, wo $D_1 = \frac{D}{2^B} \neq 1$, ungerade. Wegen der Voraussetzung muß $2^A D_1$ e. d. sein, also $2^A D_1 = 2^B D_1$. Da hier $A \leqslant B$, so ist dies nur dann möglich, wenn $A = B$ ist.

Es sei zuerst die Zahl A gerade. Nun folgt aus $2^A Q = r^2 + 2^B D_1 s^2$, $(r, s) = 1$, daß $Q = r_1^2 + D_1 s^2$, wo $r_1 = \frac{r}{2^{\frac{1}{2}A}} = \frac{r}{2^{\frac{1}{2}B}}$; also ist die Zahl Q durch die Form $x^2 + D_1 y^2$ e. d. und demnach ist die ungerade Zahl D_1, wo $D_1 \neq 1$, gleich: 3 oder 7. Wir betrachten jetzt die Zahlen $13 = 1^2 + 3 \cdot 2^2$ und $29 = 1 + 7 \cdot 2^2$. Da sie prim sind, erhalten wir, daß

$$2^A 13 = (2^{\frac{1}{2}A})^2 + 2^A 3 \cdot 2^2; \quad 2^A \cdot 29 = (2^{\frac{1}{2}A})^2 + 2^A \cdot 7^2, \; —$$

ihre einzigen Darstellungen durch die entsprechende Form $x^2 + Dy^2$ ist. Diese Darstellungen sind aber nicht eigentlich und es kann also angenommen werden, daß A ungerade, mithin $2Q = r^2 + 2D_1 s^2$ ist. Nun ist die Zahl $(1 + 2D_1)$ Teiler der Eorm $x^2 + 2^A D_1 y^2$, denn

$$(2^{\frac{A-1}{2}})^2 + 2^A D_1 = 2^{A-1}(1 + 2D_1).$$

Da aber $1 + 2D_1 < 2^3 D_1 \leqslant 2^A D_1$, so ist die Zahl $(1 + 2D_1)$ durch die Form $x^2 + 2^A D_1 y^2$ nicht darstellbar. Also ist wegen der Voraussetzung $2^A(1 + 2D_1)$ e. d., mithin die Zahl $2(1 + 2D_1)$ durch die Form $x^2 + 2D_1 y^2$ e. d.. Nun ist aber die Zahl $1 + 2D_1$ prim, denn ist t ein echter Teiler der Zahl $1 + 2D_1$, so kann man unter anderm $t < \sqrt{1 + 2D_1}$ annehmen, was aber unmöglich ist, denn $t \geqslant Q = D_1$.

Wir betrachten jetzt die Form $x^2 + 2D_1 y^2$ und multiplizieren die Darstellungen der Zahlen $2(1 + 2D_1)$ und $(1 + 2D_1)$ miteinander. Zufolge des Hilfssatzes I erhält man (da $1 + 2D_1$ prim ist), daß die Zahl 2 durch die Form $x^2 + 2D_1 y^2$ e. d., also $D_1 = 1$ ist.

Ist aber $D = 2^B$, so ist, da $2^A Q$ durch die Form $x^2 + 2^B y^2$ e. d. ist

$$2^B = 2^A, \quad 2^{B-1} = 2^A \quad \text{oder} \quad 2^{B-2} = 2^A.$$

Nun sind aber die Fälle $2^{B-1} = 2^A$ oder $2^{B-2} = 2^A$ unmöglich: denn für die Form $x^2 + 2^B y^2$, wo $A < B$, A gerade ist, sind die Darstellungen

$$2^A g = (2^{\frac{1}{2}A})^2 + 2^{A+1} y^2, \quad 2^A 17 = (2^{\frac{1}{2}A})^2 + 2^{A+2} \cdot 2^2$$

wo g eine entsprechende beliebige ganze Zahl z. B. $g = 3$, die einzig möglichen für die entsprechenden Zahlen, folglich nicht eigentlich darstellbar.

Beweis des Falles 3:

Wir betrachten zuerst den Fall, wo $D \neq 2^B$, ist also

$$2^A Q = r^2 + 2^B D_1 s^2 \quad \text{wo} \quad (r, s) = 1,$$

so ist $2^B / r^2$. Es sei jetzt L ein beliebiger ungerader Teiler der Form $x^2 + 2^B D_1 y^2$. Ist L e. d., also ist

$$L = R^2 + 2^B D_1 S^2, \quad (R, S) = 1,$$

so muß

$$L = R^2 + D_1 (2^{\frac{B}{2}} S)^2, \quad (R, 2^{\frac{1}{2}B} S) = 1$$

sein. Ist aber $2^A L = R^2 + 2^B D_1 S^2$, so muß

$$2^{A-B} L = R_1^2 + D_1 S^2, \quad (R_1, S) = 1, \quad \text{wo} \quad R_1 = \frac{R}{2^{\frac{1}{2}B}},$$

sein. Da jeder ungerade Teiler L der Form $x^2 + Dy^2$ auch ungerader Teiler der Form $x^2 + D_1 y^2$ ist, ergibt sich, daß jeder ungerade Teiler L der Form $x^2 + D_1 y^2$ entweder selbst oder mit 2^{A-B} multipliziert, durch die Form $x^2 + D_1 y^2$ e. d. ist. Wir erhalten also, wegen des Falles 1, daß entweder $A - B = 1, 2$ oder gleichzeitig $A - B \geqslant 3$ und $D = 7, 15, 23, 31$ ist.

Ist $A - B = 1, 2$, so ist auf Grund des Satzes II, da D_1 ungerade ist, $Q = \frac{1 + D_1}{2^{A-B}}$; also kann D_1 keinen echten Teiler haben, denn dann wäre

$$\frac{1 + D_1}{2} \leqslant \sqrt{D_1}, \quad \text{also} \quad D_1^2 - 14 D_1 + 1 \leqslant 0,$$

was nur für $D_1 \leqslant 14$ möglich ist, wobei die entsprechenden Zahlen D_1, für welche $2^{A-B} Q = 2Q$ oder $= 4Q$ e. d. ist, die Werte 5, 11, 13 haben. Demnach

können wir annehmen, daß D_1 prim ist. Wegen der Voraussetzung ist für gewisse Zahlen g und h:

$$2^A D_1 = g^2 + 2^B D_1 h^2, \quad (g,h)=1, \quad \text{also} \quad 2^{A-B} D_1 = g_1^2 + D_1 h^2, \quad (g_1, h)=1,$$

und da die Zahl D_1 prim ist, ergibt sich

$$2^{A-B} = D_1 g_2^2 + h^2, \quad \text{wo} \quad g_2 = \frac{g_1}{D_1}.$$

Mithin (wenn nur $A-B=1,2$) folgt, daß entweder $D=2^B D_1$ Potenz der Zahl 2 ist, oder daß gleichzeitig $A-B=2$ und $D_1=3$. Wir erwägen jetzt den letzten Fall $A-B \geqslant 3$, also wegen 1 ist hier:

$$D_1 = 7, 15, 23, 31.$$

Der Fall $D_1=7$, ist mit der Behauptung des Satzes im Einklang, da $b=\frac{1}{2}B \leqslant \frac{1}{2}(A-3)$. Wir nehmen also an: $D_1=15,23,31$ und für diese D_1 definieren wir eine Zahl $P=P(D_1)$ folgendermaßen:

$$P(15)=2^2+15=19; \quad P(23)=6^2+23=59; \quad P(31)=4^2+31=37.$$

Nun nehmen wir an, daß das entsprechende D der Voraussetzung des Satzes genügt. Dann ist $2^A P$ durch die entsprechende Form e. d. und zwar:

$$2^A P = x^2 + Dy^2 = x^2 + 2^B D_1 y^2; \quad 2^{A-B} P = x_1^2 + D_1 y^2 \quad \text{wo} \quad x_1 = \frac{x}{2^{\frac{1}{2}B}}.$$

Da die Zahl P prim und selbst durch die Form $x^2+D_1y^2$ e. d. ist, so folgt aus der Multiplikation der Zahlen P und $2^{A-B}P$ miteinander, dem Hilfssatze 1 gemäß (s. auch Bemerkung zu diesem Hilfss.), daß 2^{A-B} durch die Form $x^2+D_1y^2$ e. d. ist.

Wir betrachten jetzt die Zahlen $K(D_1)=K$, welche für $D_1=15,23,31$ entsprechend gleich ist:

$$K(15)=17, \quad K(23)=3, \quad K(31)=5.$$

Diese Zahlen sind Primteiler der entsprechenden Form x^2+Dy^2, und zwar der Zahlen:

$$(2^{\frac{1}{2}B+1}\cdot 3)^2 + 2^B \cdot 15; \quad (2^{\frac{1}{2}B})^2 + 2^B \cdot 23; \quad (2^{\frac{1}{2}B})^2 + 2^B \cdot 31,$$

sie sind aber durch die (entsprechende) Form $x^2+2^BD_1y^2$ nicht darstellbar. Es ist demnach für gewisse ganze Zahlen W und T:

$$2^A K = W^2 + 2^B D_1 T^2; \quad 2^{A-B} K = W_1^2 + D_1 T^2, \quad \text{wo} \quad W_1 = \frac{W}{2^{\frac{1}{2}B}}.$$

Da 2^{A-B} e. d. ist, so erhält man nach der Multiplikation miteinander, dem

Hilfssatze I gemäß (s. auch Bemerkung), daß K durch die Form x^2+Dy^2 e. d. ist, was offenbar nicht stattfindet.

Es blieb noch zu beweisen, daß für $D=2^B$ höchstens $B=A-1$ ist. Dies ist aber klar, denn aus

$$2^A Q = r^2 + 2^B s^2 \quad \text{folgt} \quad 2^{A-B} Q = r_1^2 + s^2, \quad \text{wo} \quad r_1 = \frac{r}{2^{\frac{1}{2}B}}.$$

Da $A-B>0$, so ist $r_1^2 \equiv s^2 \equiv 1 \pmod 8$, also ist nur $A-B=1$ möglich und der Satz ist also vollständig bewiesen.

Satz V: (Umkehrungssatz):

„Ist L ein beliebiger ungerader Teiler der Form x^2+Dy^2,
„so ist:
„1) für $D=1,2,3,4$ und 7: L e. d. durch die Form x^2+Dy^2;
„2) für $D=2^A$;
für $D=2^{A-1}$, wenn nur A ungerade ist;
für $D=2^{A-2}\cdot 3$, wenn nur A gerade ist;
für $D=2^{2b}\cdot 7$, wo b eine beliebige natürliche Zahl, welche $\leqslant \frac{1}{2}(A-3)$ ist,
und „3) für $D=15,23,31$
„folgt stets, daß entweder 2^3L oder L e. d. durch die „Form x^2+Dy^2 ist.

Beweis. Der erste Fall ist im Satze I erledigt, der dritte im Satze III, — wir betrachten also den zweiten Fall. Es sei zuerst $D=2^{2b}\cdot 7$ und A eine beliebige Zahl, welche $\geqslant 2b+3$ ist. Nun ist die Zahl 2^{A-2b}, wo $A-2b \geqslant 3$ ist, durch die Form x^2+7y^2 e. d., und zwar folgt aus der e. D. der Zahl 2^n (n eine beliebige natürliche Zahl, welche $\geqslant 4$ ist) und $8=1+7$, nach ihrer Multiplikation (zufolge des Hilfssatzes I, s. auch Bemerkung) daß $2^{n+3-2}=2^{n+1}$ e. d. durch die Form x^2+Dy^2 ist. Multiplizieren wir mithin die Darstellung der Zahl L, erhalten wir, daß auch $2^{A-2b}\cdot L$ e. d. durch die Form x^2+7y^2 ist:

$$2^{A-2b} L = R^2 + 7S^2, \ (R,S)=1), \quad \text{also ist} \quad 2^A L = (2^b R) + 2^{2b}\cdot 7S^2,$$

wobei $(2^bR, S)=1$, denn R und S sind ungerade Zahlen.

Ist $D=2^A$, so ergibt sich für gerades A aus $L=R^2+S^2$:

$$2^A L = (2^{\frac{1}{2}A} R)^2 + 2^A S^2, \quad (2^{\frac{1}{2}A} R, S) = 1,$$

wenn nur R gerade ist. Ist A ungerade, so folgt aus $L=R^2+2S^2$ $(R,S)=1$:

$$2^A L = (2^{\frac{A+1}{2}} \cdot S)^2 + 2^A R^2, \quad (2^{\frac{A+1}{2}} \cdot S, R) = 1.$$

Für die Form $x^2+2^{A-2}3y^2$ folgt dieser Satz unmittelbar, denn der Vor-

aussetzung gemäß ist hier A gerade. Also ist jeder ungerade Teiler durch die Form x^2+3y^2 e. d.: $L=R^2+3S^2$, $(R,S)=1$, somit ist

$$4L=(R+S)^2+3(R-S)^2,\quad (R+S,\ R-S)=1;$$
$$2^AL=(2^{\frac{1}{2}(A-2)}(R+S))^2+3\cdot 2^{A-2}(R-S)^2.$$

Dabei sind die Zahlen $2^{\frac{1}{2}(A-2)}(R+S)$, $(R-S)$ zueinander relativ prim.

Aus diesen beiden Sätzen folgt unmittelbar:

Satz VI: „Ist jeder beliebige ungerade Teiler L der Form „x^2+Dy^2 entweder selbst oder 2^AL, wo A konstant und „$A\geqslant 3$ ist, e. d., so ist

$$D=15,23,31,2^A,\quad 2^{A-1},\quad 2^{A-2}3,\quad 2^{2b}\cdot 7\quad (b=\text{beliebig}).$$

„Und auch umgekehrt: Es existiert für diese D ein ge„eignetes A, wobei $A\geqslant 3$ ist.

Somit ist die Frage der Möglichkeit der Verallgemeinerung des Eichenbergschen Kriteriums für beliebige A gänzlich erledigt.

ZWEITER TEIL.

Einführung.

Um die Anwendungen der obigen Sätze hervorzuheben, weisen wir auf eine andere Bedeutung des kleinsten ungeraden Teilers hin. Es ergibt sich unmittelbar, daß jede ungerade, durch die beliebige primitive Form $AX^2+Bxy+Cy^2$ eigentlich darstellbare Zahl, eine Primzahl ist, wenn nur diese Zahl (absolut genommen) $<Q^2$ ist (Q — der kleinste ungerade Teiler dieser Form ist). Man erhält also quadratische Formen, welche viele Primzahlen darstellen, wenn nur Q möglich groß sein wird. Nun sind die drei höchstmöglichen Werte des kleinsten Q der Form x^2+Dy^2:

$$Q=D,\quad E\frac{1+D}{2},\quad E\frac{1+D}{4},\quad (E=\text{Entier})\ [4],$$

d. h. 2^aQ ist eigentlich darstellbar ($a=0,1,2$). Diese Tatsache ist der wesentliche Grund dafür, warum die bekannten Formen, auf welche Euler [5]

[4]) Es ist einleuchtend, daß um weitere Formen, welche Primzahlen darstellen, zu erhalten, die Formen x^2+Dy^2, für welche $8Q$ e. d. ist, beachtet werden müssen. Es soll aber bewiesen werden (s. Satz II), daß im allgemeinen diese Formen, von den obigen nicht wesentlich verschieden sind.

[5]) Euler: Memoires de l'Acad. de Berlin 1772, Histoire p. 36 — extrait d'un lettre a M. Bernoulli.

und andere Formen, auf welche Frobenius [6] hinwies, viele Primzahlen darstellen [7]). Mithin folgen auch viele verschiedene Verallgemeinerungen eines Frobeniusschen Satzes [8]), und zwar gilt unter anderem auch der Satz:

„Damit ein jeder ungerade Teiler L der Form x^2+Dy^2 die „Eigenschaft habe, daß entweder L oder 2^aL, wo a kon„stant und $a=1$ für $D\equiv 1,2\pmod 4$ und $a=2$ für $D\equiv 3\pmod 8$ „eigentlich darstellbar ist, es notwendig und hinreichend „ist, daß jedes Glied (resp. jedes gerade Glied) der Folge

$$(1)\qquad D,\quad A^2+D,\quad (2A)^2+D,\quad (3a)^2+D,\ldots(nA)^2+D$$

„wo A konstant, wobei
„für $D\equiv 1,2\pmod 4$: $A<\sqrt{D-2}$ und n alle natürlichen Zahlen „durchläuft, welche $n<\frac{1}{2}\sqrt{D}$ (resp. $A<\sqrt{\frac{D}{2}}$ und $n<\frac{1}{2}\sqrt{D}$),
„für $D\equiv 3\pmod 8$: $A<\sqrt{2(D-6)}$ und $n>\frac{1}{2}\sqrt{\frac{D}{3}}$ (resp. $A<\sqrt{D-1}$ „und $n<\frac{1}{2}\sqrt{\frac{D}{2}}$),
„entweder prim oder eine 2^a-faches einer Primzahl sei.

Den Fall, wo $a=2$, $A=1$ und die geraden Glieder der Folge (1) 4-fache von Primzahlen sind, hat Frobenius [6]) behandelt. Dasselbe gilt für den Fall, wo $A=a=1$ und die Glieder der Folge (1) entweder prim oder 2-fache einer Primzahl sind, aber Frobenius [9]) hat in diesem Falle vorausgesetzt, daß $n<\sqrt{\frac{D}{3}}$ und hier ist es $n<\sqrt{\frac{D}{4}}$.

[6]) G. Frobenius: Sitzungsb. d. k. preuss. Akad. d. Wissensch. Berlin 1921, S. 976.

[7]) Frobenius hat die Äquivalenz aller Klassen der entsprechenden Diskriminanten als „wesentliche Quelle" (s. 6) S. 966) für die Darstellbarkeit vieler Primzahlen angenommen, aber schon aus Verallgemeinerungsgründen, und zwar, um noch andere Formen (sogar von beliebigen Graden), welche viele Primzahlen darstellen, finden zu können, sieht man die Zweckmässigkeit unseres Standpunktes.

[8]) wenn er auch das Problem anders formulierte. Er stellt folgende Fragen:

1) wann wird jeder (ungerade) Teiler der Form $x^2+xy+Dy^2$ durch diese darstellbar. Dieses Problem läßt sich auf das obige zurückführen, denn $4(x^2+xy+Dy^2)=2(x+y)^2+Dy^2$, also $2^a=4$;

2) wann ist jeder Teiler der Form x^2+2py^2 durch dieselbe oder durch die Form $2x^2+py^2$ darstellbar; oder wann ist jeder Teiler der Form x^2+py^2 durch dieselbe oder durch die Form $2x^2+2xy+dy^2$. Diese Fälle entsprechen, dem Falle 2.

[9]) s. S. 973—6; vgl. L. Dickson: Theory of Numbers. Washington 1919 B. I Chap. VIII S. 4.

Werden wir nur die ungeraden Zahlen der Folge

$$D,\quad 1^2+D,\quad 2^2+D,\ldots,n^2+D \tag{2}$$

in Betracht nehmen, so wird sich Schluß des vorigen Satzes unter viel engeren Voraussetznngen ergeben

„damit, daß... (s. oben), daß jedes ungerade Glied der Folge „(2), wo für $D\equiv 1,2 \pmod 4$: $a=1$ und $n<\sqrt{\frac{5}{8}D}$; für $D\equiv 3$ „(mod 8): $a=2$ und $n<\sqrt{\frac{13}{48}D}$, prim sei.

Nun wollen wir auf die Möglichkeit der Anwendung obiger Sätze auf die Theorie des imaginär-quadratischen Körpers hinweisen. Unter anderem folgt eine Verallgemeinerung des Rabinowitsch-Nagellschen Kriteriums für die einklassigen imaginär-quadratischen Körper: und zwar entspricht dies dem Falle $A=1$, $a=2$, $n<\frac{1}{2}\sqrt{\frac{D}{3}}$.

Hilfssatz III: „Für eine beliebige bestimmte oder unbe- „stimmte Form $Ax^2+Bxy+Cy^2$ gilt:

„1) Jede ungerade Zahl, welche durch diese Form „e. d. und absolut genommen kleiner als Q^2, wo Q der „kleinste ungerade Teiler der Form $x^2+(4AC-B)y^2$ „ist, ist eine Primzahl.

„2) Ist B gerade und $AC-(\frac{1}{2}B)^2\equiv 1,2,3,5,6 \pmod 8$, so „ist jede gerade durch die Form $Ax^2+Bxy+Cy^2$ e. d. Zahl, „die absolut genommen kleiner als 2^aQ^2, wo $(L,8)=2^a$, „ein 2-faches einer Primzahl, wenn nur $a=1$ für „$AC-\frac{1}{4}B^2\equiv 1,2 \pmod 4$ und $a=2$ für $AC-\frac{1}{4}B^2\equiv 3 \pmod 8$.

Beweis I. Ist die ungerade Zahl $Ar^2+Brs+Cs^2$ wo $(r,s)=1$ absolut genommen kleiner als Q^2, so ist sie sicher prim, denn widrigenfalls hätte sie einen ungeraden Teiler t, welcher $\leqslant\sqrt{Ar^2+Brs+Cs^2}$, also $t<Q$ wäre — der Annahme entgegen.

II. Es sei jetzt B gerade: $B=2B_1$ und $AC-B_1^2\equiv 1,2,3,5,6 \pmod 8$ sind also unmöglich.

Ist die Zahl $L=Ar^2+2Brs+Cs^2$, wo $(r,s)=1$, gerade, so folgt, da eine der Zahlen A, C ungerade ist, — sei es z. B. A, daß:

$$AL=(Ar+B_1s)^2+(AC-B_1)s^2\equiv 0 \pmod{2^a},$$

wo $a=1$, für $AC-B_1^2\equiv 1,2 \pmod 4$ und $a=2$ für $AC-B_1^2\equiv 3 \pmod 8$.

Ist $L<2^aQ^2$, also $\frac{L}{2^a}<Q^2$, so folgt, da die Zahl $\frac{L}{2^a}$ ungerade ist, daß sie prim sein muß; denn widrigenfalls wird Q kein kleinster ungerader Teiler sein.

Es ist einleuchtend, daß der Beweis analog verlaufen wird, wenn wir annehmen, daß C ungerade ist.

Satz VII: „Sind die Zahlen (bzw. ungerade, bzw. gerade „Zahlen) der Folge

$$D,\quad A^2+D,\quad (2A)^2+D,\ldots(An)^2+D \tag{1}$$

„oder der Folge

$$1+DA^2,\quad 1+D(2A)^2,\ldots 1+D(nA)^2, \tag{2}$$

„wo $D=1,2,3,5,6 \pmod 8$ ist durch solche ungerade Prim- „zahlen teilbar, welche für $D\equiv 1,2 \pmod 4 \geqslant\sqrt{D}$ sind, wobei „n alle natürlichen Zahlen durchläuft, welche $<\frac{1}{2}\sqrt{D}$ „(bzw. $n<\sqrt{D}$) und für $D\equiv 3 \pmod 8$: $\geqslant\sqrt{\frac{D}{3}}$ sind, wobei „$n<\frac{1}{2}\sqrt{\frac{D}{3}}$ $\left(\text{bzw. } n<\sqrt{\frac{1}{3}D}\right)$, so ist für jeden ungeraden „Teiler L der Form x^2+Dy^2 entweder L oder 2^aL e. d., „dabei ist:

$$a=1 \text{ für } D\equiv 1,2 \pmod 4,$$
$$a=2 \text{ für } D\equiv 3 \pmod 8.$$

Beweis. Wir betrachten die Kongruenz

$$z^2+D\equiv 0 \pmod{2^aQ}$$

mit der kleinsten Lösung z. Also ist $z<Q$, denn eine der Zahlen

$$Z^2+D,\qquad (Q-Z)^2+D,$$

wo Z die kleinste Lösung der Kongruenz $Z^2+D\equiv 0 \pmod Q$ ist, d. h. $Z<\frac{1}{2}Q$, gerade ist. Es bezeichne die Zahl l den Bruch $l=\frac{Z^2+D}{2^aQ}$, also eine ungerade Zahl. Ist $l=1$ so ist 2^aQ e. d., somit ist, vermöge des Satzes III. alles bewiesen. Es sei $l>1$, demnach $l\geqslant Q$. Mithin erhalten wir die Relationen:

$$Q^2+D\geqslant Z^2+D=2^aQ\geqslant 2^aQ^2,$$

also ist $Q<\sqrt{\frac{D}{2^{a-1}}}$, was für $a=1$ ergibt: $Q<\sqrt{D}$ und für $a=2$, $Q<\sqrt{\frac{D}{3}}$.

Es ist also die Kongruenz

(3) $$A^2x^2 + D \equiv 0 \pmod{Q}$$

und die Kongruenz

(4) $$1 + DA^2x^2 \equiv 0 \pmod{Q}$$

für eine Zahl x, wo für $a=1$, $x<\frac{1}{2}\sqrt{D}$ und für $a=2$, $x<\frac{1}{2}\sqrt{\frac{D}{3}}$, lösbar. Demnach ist eine gewisse Zahl der Folge (1) oder der Folge (2) durch eine Zahl, welche, für $D\equiv 1,2 \pmod 4$, $-\leqslant\sqrt{D}$ und für $D\equiv 3 \pmod 8$ $\leqslant\sqrt{\frac{D}{3}}$, teilbar.

Beachten wir nur solche Lösungen der Kongruenz (3) oder (4), wo A^2x^2+D oder $1+DA^2x^2$ gerade (bzw. ungerade) sind, so findet man im Falle der Lösbarkeit der obigen Kongruenzen solche Lösungen x, für welche:

$$\text{für } D\equiv 1,2 \pmod 4,\ -\ x<\sqrt{D};$$

$$\text{für } D\equiv 3 \pmod 8,\ -\ x<\sqrt{\frac{D}{3}}.$$

Der Satz ist also bewiesen.

Folgerung I: „Damit ein jeder ungerade Teiler L der Form „x^2+Dy^2 die Eigenschaft habe, daß entweder L oder „2^aL, wo a konstant und $a=1$ für $D\equiv 1,2 \pmod 4$ und „$a=2$ für $D\equiv 3 \pmod 8$ (dabei nimmt D nur die Werte „$D\equiv 1, 2, 3, 5, 6 \pmod 8$ an) e. d. ist, — ist es notwendig „und hinreichend, daß jedes Glied (bzw. jedes gerade „Glied) der Folge

(1) $$D,\quad A^2+D,\quad (2A)^2+D,\quad (3A)^2+D,$$

„wo A konstant, wobei

„ für $D\equiv 1,2 \pmod 4$: $A<\sqrt{D-2}$ und n natürliche Zahlen durchläuft, welche $<\frac{1}{2}\sqrt{D}$; (bzw. $A<\sqrt{\frac{D}{2}}$ und „ $n<\sqrt{D}$);

„ für $D\equiv 3 \pmod 8$: $A<\frac{1}{2}\sqrt{3(D-6)}$ und $n<\frac{1}{2}\sqrt{\frac{D}{3}}$ (bzw. „ $A<\frac{1}{2}\sqrt{D-1}$ und $n<\sqrt{\frac{D}{3}}$),

„entweder prim oder ein 2^a-faches einer Primzahl sei.

Beweis. Die Notwendigkit folgt aus dem Hilfssatze II, denn für die angegebenen Werte von A und n ist jedes ungerade Glied der Folge (1) kleiner als Q^2 und jedes gerade Glied kleiner als 2^aQ^2. Dabei ist zu beachten, daß für $a=2$ die kleinste ungerade zusammengesetzte Zahl gleich $\left(\frac{1+D}{4}\right)\left(\frac{9+D}{4}\right)$ ist, und allgemein ist vermöge des Hilfssatzes: $Q=E\frac{1+D}{2^a}$. Daß diese Bedingung auch hinreichend ist, folgt unmittelbar aus dem vorigen Satze [10]).

Folgerung II: „Damit ein jeder ungerade Teiler L der Form „x^2+Dy^2, wo $D\equiv 1, 2, 3, 5, 6 \pmod 8$ wobei:

„ für $D\equiv 1,2 \pmod 4$, $a=1$;

„ für $D\equiv 3 \pmod 8$, $a=2$,

„e. d. ist, — ist es notwendig und hinreichend, daß jedes „des ungerade Glied der Folge

(5) $$D,\quad 1^2+D,\quad 2^2+D,\ldots,n^2+D,$$

„wo für $D\equiv 1,2 \pmod 4$ n alle natürlichen Zahlen durch„läuft, für welche $n<\sqrt{\frac{5}{8}D}$ und für $D\equiv 3 \pmod 8$ „$n<\sqrt{\frac{13}{48}D}$, prim ist.

Beweis. Daß diese Bedingung notwendig ist, folgt aus dem Satze II, wir werden also beweisen, daß sie auch hinreichend ist.

Wir betrachten zuerst alle Zahlen der Folge (1), wo n alle natürliche Zahlen durchläuft, für welche $n<\frac{1}{2}\sqrt{D}$, wenn nur $D\equiv 1,2 \pmod 4$ und $n<\frac{1}{2}\sqrt{\frac{D}{3}}$, — für $D\equiv 3 \pmod 8$. Wäre der Satz falsch, so wäre, vermöge der vorigen Folgerung, da alle ungeraden Zahlen prim sind, eine gerade Zahl dieser (letzten) Folge kein 2^a-faches einer Primzahl. Somit erhalten wir, daß die Form x^2+Dy^2 für $a=1$ einen ungeraden Teiler hat, welcher kleiner als $\sqrt{\frac{5}{8}D}$ und für $a=2$ einen ungeraden Teiler, welcher kleiner als $\sqrt{\frac{13}{48}D}$ ist. Denn für $a=1$ und $n<\frac{1}{2}\sqrt{D}$ ist $\frac{n^2+D}{2}<\frac{5}{8}D$; und für $a=2$, $n<\frac{1}{2}\sqrt{\frac{D}{3}}$ ist $\frac{n^2+D}{4}<\frac{13}{48}$.

[10]) Einen analogen Satz kann man auch für die Folge

$$1^2+DA,\quad 1+D(2A)^2,\ldots\quad 1+D(nA)^2$$

beweisen.

Anmerkung. Auf folgende Formen, welche viele Primzahlen darstellen, hat Euler [5]) hingewiesen:

$$x^2 - x + p, \quad \text{wo} \quad p = 3, 5, 11, 17, 41 \quad \text{und}$$
$$2x^2 + p, \quad \text{wo} \quad p = 3, 5\,11, 29;$$

demnach folgt für die Formen $x^2 + Dy^2$, wo

$$D = 11, 19, 43, 67, 163; \quad 6, 10, 22, 58,$$

daß für jeden ungeraden Teiler L dieser Formen entweder L oder $2^a L$ $(a = 1, 2)$ e. d. ist. Dasselbe gilt auch für die Formen, wo $D = 5, 13, 37$, auf welche Frobenius zuerst hinwies [6]).

Nun deuten wir auf die möglichen Anwendungen der obigen Sätze auf die Theorie der quadratischen Körper an, und zwar verläuft, die Theorie der quadratischen Formen der Theorie des quadratischen Körpers parallel. Jedenfalls kann man unmittelbar den folgenden (bekannten) Hilfssatz beweisen:

Hilfssatz IV: „Ist jede Zahl des imaginär-quadratischen „Körpers $K(w)$ in ein Produkt von Primzahlen dieses „Körpers eindeutig (bis auf Einheiten) zerlegbar, so „ist jeder Teiler der Form $N(u + vw)$ ($N(u + vw)$ = Norm „der Zahl $u + vw$) durch diese Form eigentlich dar„stellbar.

Beweis. Nach Satz III (s. auch Fußnote [8])) genügt es den Beweis nur für Primteiler (sogar nur für den kleinsten Primteiler) zu führen. Es sei

$$(u, v) = 1, \qquad N(u + vw) \equiv 0 \pmod{p},$$

wo u, v gewisse ganze Zahlen sind, $N(u + vw)$, — die Norm der Zahl $u + vw$ und p eine natürliche Primzahl. Da $(u, v) = 1$, so kann $N(u + vw)$, im Körper $K(w)$, nur dann eindeutig zerlegbar sein, wenn für gewisse 2 konjugierte Primteiler $u + vw$, $u + vw$ der Zahl $N(u + vw^*)$ (wenn nur der absolute Wert der Diskriminante > 4 ist)

$$p = (u + vw)(u + vw^*)$$

sein wird. Es folgt also, daß $p = x^2 + Dy^2$, wenn $w = \sqrt{-D}$, und $4p = x^2 + Dy^2$, wenn $w = \frac{1 + \sqrt{D}}{2}$ (s. [8])).

Zusatz: Diesem Hilfssatze gemäß, können wir, die Sätze, III, VII und die Folgerungen des Satzes VII, auf die imaginär-quadratischen einklassigen

Körper anwenden. Demnach folgt das Rabinowitsch [11])-Nagelsche [12]) Kriterium, und zwar entspringt dies aus dem Falle $A = 1$, $a = 2$, $n < \frac{1}{2}\sqrt{\frac{D}{3}}$ der Folgerung I des Satzes VII.

Streszczenie.

Celem niniejszej rozprawy jest podanie teorji form kwadratowych przy korzystaniu tylko z jednego pojęcia: dzielnika formy $x^2 + Dy^2$. Możliwości tkwiące w tem ujęciu widać już w twierdzeniu pomocniczem II, które stanowi uogólnienie twierdzenia o równoważności każdej formy z formą zredukowaną. Dalej są te możliwości widoczne w uogólnieniu i wyczerpaniu twierdzenia Eichenberga o roli najmniejszego dzielnika nieparzystego formy $x^2 + Dy^2$, zwłaszcza, że konieczność uogólnienia tego twierdzenia wyłania się z twierdzenia I, które wykazuje, że samo kryterjum Eichenberga zachodzi prawie że w próżni.

W II-giej części pracy, dzięki tej metodzie, otrzymuje się uogólnienie prac Frobeniusa, Rabinowitscha i Nagella.

---

[11]) G. Rabinowitsch: Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. Jour. für Math. B. 142, S. 153—164.

[12]) T. Nagell: Über die Klassanzahl imaginär-quadratischer Zahlkörper. Abhandl. aus dem math. Seminar, Hamburg B. 1, 1922, S. 145—150.