Kapitel 4. Additive Probleme und diophantische Gleichungen

In § 1 dieses Kapitels werden einige additive Fragen studiert. Dabei werden zwei weitere Beweise für das schon in 3.3.4 gezeigte Resultat über die Darstellbarkeit von Primzahlen als Summe zweier Quadrate gegeben. Interessant sind hierbei die Beweismittel: Einmal wird der erste Ergänzungssatz zum quadratischen Reziprozitätsgesetz mit einem DIRICHLETschen Schubfachschluß kombiniert, das andere Mal wird auf das Prinzip des kleinsten Elements zurückgegriffen. Überdies sind jeweils (wie übrigens häufig in diesem Kapitel) Kongruenzbetrachtungen anzustellen.

Im weiteren Verlauf des § 1 wird die Darstellbarkeit natürlicher Zahlen als Summe von zwei, drei oder vier Quadratzahlen untersucht, wobei ein Satz von LAGRANGE besagt, daß vier Quadrate zur Darstellung immer ausreichen. Wann man mit zwei bzw. drei Quadraten auskommt, kann genau charakterisiert werden. Auf die Anzahl der Darstellungen natürlicher Zahlen als Summe von zwei bzw. vier Quadraten wird ebenso eingegangen wie auf die Darstellbarkeit als Summe von k–ten Potenzen.

In den Paragraphen 2 und 3 geht es erneut um die in § 3 von Kap. 1 erstmals angeschnittene Thematik der diophantischen Gleichungen. § 2 beschäftigt sich mit rationalen Punkten auf algebraischen Kurven. Dabei wird mit dem von EUKLID völlig gelösten Problem der Bestimmung aller rechtwinkligen Dreiecke ganzzahliger Seitenlängen begonnen; hier ist $X^2 + Y^2 = 1$ die Gleichung der Kurve. Weiter wird die allgemeine Kurve zweiten Grades diskutiert ebenso wie die DIOPHANTsche Sekanten– bzw. Tangentenmethode zur Behandlung von Kurven dritten oder vierten Grades. Zum Schluß dieses Paragraphen wird auf die berühmte, inzwischen bewiesene FERMATsche Vermutung eingegangen.

Gegenstand von § 3 ist die PELLsche Gleichung $X^2 - dY^2 = 1$ bei natürlichem, nicht quadratischem d. Mit einem Satz über die Annäherung reeller irrationaler Zahlen durch rationale gelingt die völlige Klärung der Struktur der unendlich vielen ganzzahligen Lösungen dieser Gleichung. Die dabei entwickelten Methoden sind auch geeignet zur Untersuchung der Einheiten reell–quadratischer

Zahlkörper und der ganzzahligen Punkte auf der allgemeinen algebraischen Kurve zweiten Grades.

§ 1. Potenzsummen, insbesondere Quadratsummen

1. Primzahlen als Summe zweier Quadrate. In 3.3.4 wurde gezeigt, daß für jede Primzahl $p \equiv 1 \pmod 4$ die diophantische Gleichung

$$X^2 + Y^2 = p \tag{1}$$

ganzzahlig lösbar ist. Dort wurde für jedes solche p *eine* Lösung explizit angegeben; daß daraus sogar alle Lösungen von (1) konstruiert werden können, ist aus Proposition 1.6.10 bekannt, wird sich aber sogleich nochmals ergeben. Ist nämlich $(x, y) \in \mathbb{Z}^2$ eine Lösung von (1), so dürfen o.B.d.A. $x, y \in \mathbb{N}$ angenommen werden und es ist $x \neq y$. So sind (x, y), $(x, -y)$, $(-x, y)$ und $(-x, -y)$ (man faßt diese vier verschiedenen Paare bisweilen in der Kurzschreibweise $(\pm x, \pm y)$ zusammen) sowie die daraus durch Vertauschung von x und y entstehenden vier Paare insgesamt acht paarweise verschiedene Lösungen von (1). Es wird sogleich bewiesen, daß mit diesen acht bereits sämtliche Lösungen von (1) erschöpft sind.

Genau dann, wenn (1) lösbar ist, sagt man, *p sei als Summe zweier Quadratzahlen* (oder kürzer: zweier Quadrate) *darstellbar*. Die vier Lösungen $(\pm x, \pm y)$ von (1) entsprechen selbstverständlich *einer* Darstellung von p als Summe der beiden Quadrate x^2, y^2 in dieser Reihenfolge. Man hat nun folgenden

Satz. *Für Primzahlen p gilt folgende Äquivalenz:*

(i) *Es ist $p \not\equiv 3 \pmod 4$.*

(ii) *p ist als Summe zweier Quadrate darstellbar und die Darstellung ist, abgesehen von der Reihenfolge der Summanden, eindeutig.*

Beweis. Um den vorher diskutierten Fall $p \equiv 1 \pmod 4$ zu Ende zu führen, seien (x, y) und (u, v) Lösungen von (1) in natürlichen Zahlen. O.B.d.A. darf $x < y$ und $u < v$ vorausgesetzt werden und offenbar ist auch $x, y, u, v < \sqrt{p}$ sowie $p \not| xyuv$ klar. Wegen

$$x^2v^2 - y^2u^2 = (p - y^2)v^2 - y^2u^2 = p(v^2 - y^2)$$

folgt $p|(xv - yu)(xv + yu)$. Ist $p|(xv + yu)$, so ergibt sich aus $0 < xv + yu < 2(\sqrt{p})^2 = 2p$ die Gleichung $xv + yu = p$. Die leicht durch Ausmultiplikation einsichtige Formel

$$(x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2 \tag{2}$$

führt dann zu $p^2 = (xu - yv)^2 + p^2$, also $xu = yv$ entgegen $yv > xu$. Es muß also $p|(xv - yu)$ gelten und wegen $-p = -(\sqrt{p})^2 < xv - yu < (\sqrt{p})^2 = p$ heißt dies $xv = yu$. Die Teilerfremdheit von x und y impliziert $x|u$, etwa $u = dx$; dann muß auch $v = dy$ gelten und $p = u^2 + v^2 = d^2(x^2 + y^2) = d^2 p$ ergibt $d = 1$ und somit $u = x$, $v = y$.

Für $p = 2$ ist (1) ersichtlich lösbar mit genau den vier Lösungen $(\pm 1, \pm 1)$. Für $p \equiv 3 \pmod 4$ ist (1) jedoch unlösbar; denn das Quadrat einer ganzen Zahl ist kongruent 0 oder 1 modulo 4 und so ist für $x, y \in \mathbb{Z}$ stets $x^2 + y^2 \not\equiv 3 \pmod 4$. □

Bemerkungen. 1) Für reelle x, y, u, v folgt der "Zwei–Quadrate–Satz" (2) aus der Produktregel $|z|\,|w| = |zw|$ für die komplexen Zahlen $z = x + iy$, $w = u + iv$. Darüberhinaus läßt sich (2) wie oben durch Nachrechnen in jedem kommutativen Ring einsehen.

2) Der vorstehend bewiesene Satz wird FERMAT (1640) zugeschrieben, obwohl ihn A. GIRARD schon einige Jahre früher gekannt zu haben scheint. Während FERMAT in einem Brief an MERSENNE behauptete, er habe einen Beweis für die im Satz notierte Aussage (ohne den Zusatz über die Eindeutigkeit), scheint aber der erste publizierte Beweis auf EULER (1754) zurückzugehen.

2. Thues Lemma. Für den "nichttrivialen" Teil von Satz 1, nämlich die Lösbarkeit von 1(1) im Falle $p \equiv 1 \pmod 4$, soll hier ein zweiter Beweis angegeben werden; in 5 wird ein dritter hinzugefügt. Diese beiden Beweise sind viel einfacher, als wenn man sich auf das Resultat von E. JACOBSTHAL in 3.3.4 stützt.

Die wesentlichen Hilfsmittel beim zweiten Beweis sind einerseits der erste Ergänzungssatz zum quadratischen Reziprozitätsgesetz (vgl. 3.2.6) und andererseits das bereits früher formulierte und angewandte DIRICHLETsche Schubfachprinzip (vgl. 2.3.1). Mit letzterem beweist man leicht folgendes

Lemma von Thue. *Seien $\ell, m, u, v \in \mathbb{Z}$, $0 < u, v \leq m < uv$ und $(\ell, m) = 1$. Dann gibt es $x, y \in \mathbb{N}$ mit $x < u$ und $y < v$, so daß $\ell y \equiv x$ oder $\ell y \equiv -x \pmod m$ gilt.*

Beweis. Man sieht sich die uv ganzen Zahlen $\xi + \ell\eta$ mit $\xi \in \{0, \ldots, u-1\}$, $\eta \in \{0, \ldots, v-1\}$ an. Nach Voraussetzung sind dies mehr als m Stück und nach dem DIRICHLETschen Schubfachprinzip muß es mindestens eine Restklasse modulo m geben, in die mindestens zwei der $\xi + \ell\eta$, etwa $\xi_1 + \ell\eta_1$ und $\xi_2 + \ell\eta_2$, hineinfallen. Es ist also

$$\ell(\eta_2 - \eta_1) \equiv \xi_1 - \xi_2 \pmod m. \tag{1}$$

Nun würde $\eta_2 = \eta_1$ die Teilbarkeitsbedingung $m|(\xi_2 - \xi_1)$ implizieren und aus $|\xi_2 - \xi_1| < u \leq m$ würde sich auch $\xi_2 = \xi_1$ ergeben. O.B.d.A. darf die Numerierung also so angenommen werden, daß $y := \eta_2 - \eta_1 > 0$ ist; $y < v$ ist damit klar. Aus $x := |\xi_1 - \xi_2|$ und (1) folgt, daß eine der Kongruenzen im THUEschen Lemma gelten muß. Ebenfalls einsichtig ist $0 < x < u$, da aus $x = 0$ und (1) die Teilbarkeitsbeziehung $m|\ell y$ und also $m|y$ (damit $m \leq y$, entgegen $y < v \leq m$) folgen würde; man beachte $(\ell, m) = 1$. □

Zweiter Beweis für die Lösbarkeit von 1(1) bei $p \equiv 1 \pmod 4$. Nach dem ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz ist -1 quadratischer Rest modulo p und so gibt es ein $\ell \in \mathbb{Z}$ mit $\ell^2 \equiv -1 \pmod p$, insbesondere $p \nmid \ell$. Nun wendet man THUEes Lemma an mit $m = p$, $u = v = [\sqrt{p}] + 1$, welch letzteres wegen $p \geq 5$ tatsächlich p nicht übersteigt; weiter ist $uv > (\sqrt{p})^2 = m$ erfüllt. Nach dem Lemma gibt es $x, y \in \mathbb{N}$ mit $x, y \leq [\sqrt{p}]$, so daß $\ell y \equiv x$ oder $\ell y \equiv -x \pmod p$ gilt, also $-y^2 \equiv \ell^2 y^2 \equiv x^2 \pmod p$. Wegen $[\sqrt{p}] < \sqrt{p}$ kann sogar auf $x, y < \sqrt{p}$ geschlossen werden und daher ist die natürliche Zahl $x^2 + y^2$ einerseits durch p teilbar, andererseits kleiner als $2p$; daher löst (x, y) die Gleichung 1(1). □

3. Natürliche Zahlen als Summe zweier Quadrate. Bisher wurden *Primzahlen* bezüglich ihrer Darstellbarkeit als Summe zweier Quadrate untersucht; nun soll dieselbe Frage für *beliebige natürliche Zahlen* geklärt werden. Bei festem $n \in \mathbb{N}$ wird also nach der Lösbarkeit der diophantischen Gleichung

$$X^2 + Y^2 = n \tag{1}$$

gefragt. Sei (1) für ein gewisses n lösbar und (x, y) eine Lösung; diese heißt *primitiv* (oder *eigentlich*) bzw. *imprimitiv* (oder *uneigentlich*), wenn x und y teilerfremd bzw. nicht teilerfremd sind. Klar ist $d^2|n$, wenn d den größten gemeinsamen Teiler von x und y bezeichnet. Weiter ist einsichtig, daß (1) bei quadratfreiem n (speziell also für Primzahlen n) höchstens primitive Lösungen besitzen kann.

Als kleine Vorbereitung für den nächsten Satz benötigt man folgende

Proposition. *Hat $n \in \mathbb{N}$ eine primitive Darstellung als Summe zweier Quadrate, d.h. hat (1) eine primitive Lösung, so hat n keinen Primfaktor $\equiv 3 \pmod 4$.*

Beweis. Es möge $(x, y) \in \mathbb{Z}^2$ die Gleichung (1) lösen und x, y seien teilerfremd; p sei eine n teilende Primzahl. Aus $x^2 + y^2 \equiv 0 \pmod p$ folgt dann $p \nmid xy$; ist y_1 modulo p zu y invers, so gilt die Kongruenz $(xy_1)^2 + 1 \equiv 0 \pmod p$, d.h. -1 ist quadratischer Rest modulo p und so ist $p \not\equiv 3 \pmod 4$. □

Nun können leicht alle $n \in \mathbb{N}$ bestimmt werden, für die (1) lösbar ist.

Satz. *Für natürliche Zahlen n sind äquivalent:*

(i) *Gleichung (1) ist lösbar.*

(ii) *Für jede Primzahl $p \equiv 3 \pmod 4$ ist die Vielfachheit $\nu_p(n)$ gerade.*

Beweis. Ist $\nu_p(n)$ für alle Primzahlen $p \equiv 3 \pmod 4$ gerade, so ist

$$n_0 := \prod_{p \equiv 3\,(4)} p^{\nu_p(n)} = \Big(\prod_{p \equiv 3\,(4)} p^{\nu_p(n)/2} \Big)^2 + 0^2$$

und somit ist (1) für n_0 lösbar. Nach Satz 1 ist 1(1) auch für alle Primzahlen $p \not\equiv 3 \pmod 4$ lösbar und nun wendet man endlich oft folgende Regel an: Ist (1) für $n_1, n_2 \in \mathbb{N}$ lösbar, so auch für das Produkt $n_1 n_2$; denn $x^2 + y^2 = n_1$, $u^2 + v^2 = n_2$ und 1(2) implizieren $(xu - yv)^2 + (xv + yu)^2 = n_1 n_2$.

Sei nun umgekehrt (1) lösbar, (x, y) eine Lösung und d der größte gemeinsame Teiler von x und y. Dann sind $x_1 := x/d$ und $y_1 := y/d$ zueinander teilerfremd, es ist $d^2 | n$ und so besitzt (1) für $n_1 := n/d^2 \in \mathbb{N}$ die primitive Lösung (x_1, y_1). Nach der vorausgeschickten Proposition hat n/d^2 keinen Primfaktor $\equiv 3 \pmod 4$ und daher ist die Vielfachheit jeder solchen Primzahl in n gerade. □

Der hier gezeigte Satz beschreibt abschließend die Menge S der natürlichen Zahlen, die als Summe zweier Quadrate darstellbar sind. Offenbar ist S eine unendliche Menge, aber auch $\mathbb{N} \setminus S$, letzteres z.B. deswegen, weil es unendlich viele Primzahlen $\equiv 3 \pmod 4$ gibt (vgl. 3.2.10). Man weiß jedoch viel genauer, daß dieses Komplement von S bezüglich $\mathbb{N}$ in folgendem Sinne "die meisten" natürlichen Zahlen enthält: Ist $S(x) := \#\{n \in \mathbb{N} : \ n \le x, \ n \in S\}$ für reelles x gesetzt, so gilt nach Landau [12], § 183

$$S(x) \sim c \frac{x}{\sqrt{\log x}} \qquad \text{bei } x \to \infty$$

mit einer gewissen reellen Konstanten $c > 0$. Nach Definition von $\sim$ in 1.4.12 beinhaltet dies $\lim_{x \to \infty} \frac{S(x)}{x} = 0$, d.h. der Anteil der natürlichen Zahlen unterhalb x, die Summe zweier Quadrate sind, an allen natürlichen Zahlen unterhalb x konvergiert gegen Null. In diesem Sinne lassen sich also "die wenigsten" natürlichen Zahlen als Summe *zweier* Quadrate schreiben. Es ist klar, daß sich die Chancen verbessern werden, jede natürliche Zahl als Summe von Quadraten darstellen zu können, wenn man die Anzahl der zugelassenen Summanden erhöht. Dies Problem wird in 4 weiter verfolgt.

4. Natürliche Zahlen als Summe von vier Quadraten: Lagranges Satz. Am Ende von 3 wurde festgestellt, daß eine natürliche Zahl im allgemeinen nicht als Summe *zweier* Quadrate geschrieben werden kann. Wie das Beispiel $7 = 2^2 + 1^2 + 1^2 + 1^2$ zeigt, wird man auch mit *drei* Quadraten nicht immer auskommen. Jedoch hat 1770 LAGRANGE (Oeuvres III, 189–201) den ersten Beweis dafür publiziert, daß *vier* Quadrat–Summanden zur Darstellung jeder natürlichen Zahl ausreichend sind. Hauptziel dieses Abschnitts ist der Beweis eben dieses Ergebnisses:

Satz von Lagrange. *Jede natürliche Zahl ist als Summe von vier Quadraten darstellbar.*

Drei Jahre nach LAGRANGE hat EULER (Opera Omnia Ser. 1, III, 218–239) dessen Beweis deutlich vereinfacht. Hier wird im wesentlichen EULERs Weg nachvollzogen; dazu beginnt man mit folgendem

Lemma A. *Zu jeder Primzahl p gibt es ganze nichtnegative x, y mit $x, y \leq \frac{1}{2}p$ und $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Ist $p \not\equiv 3 \pmod 4$, so kann hier $y = 0$ gewählt werden.*

Beweis. Für $p = 2$ nehme man $x = 1$, $y = 0$. Für $p \equiv 1 \pmod 4$ ist $X^2 \equiv -1 \pmod p$ lösbar und man nehme x als die im absolut kleinsten Restsystem modulo p gelegene positive Lösung. Ist $p \equiv 3 \pmod 4$, so sei c die kleinste natürliche Zahl, die quadratischer Nichtrest modulo p ist; es ist $c \geq 2$ und die natürliche Zahl $c - 1$ ist quadratischer Rest modulo p. Daher und wegen $(\frac{-c}{p}) = (\frac{-1}{p})(\frac{c}{p}) = (-1)^2 = 1$ gibt es $x, y \in \mathbb{Z}$, die $x^2 \equiv c - 1$, $y^2 \equiv -c$ und also $x^2 + y^2 \equiv -1 \pmod p$ genügen; die x, y können wieder positiv und im absolut kleinsten Restsystem modulo p gewählt werden wegen $p \not| c(c-1)$, d.h. $p \not| xy$. □

Legt man auf dem Zusatz über $p \not\equiv 3 \pmod 4$ keinen Wert, so kann man den Schluß mit dem DIRICHLETschen Schubfachprinzip anstelle des quadratischen Restverhaltens ziehen: Für ungerade p betrachtet man die beiden Mengen

$$\{0, -1^2, \ldots, -(\frac{1}{2}(p-1))^2\} \quad \text{und} \quad \{1, 1+1^2, \ldots, 1+(\frac{1}{2}(p-1))^2\}$$

von jeweils $\frac{1}{2}(p+1)$ modulo p inkongruenten Zahlen. Insgesamt hat man $p+1$ ganze Zahlen, aber nur p Restklassen modulo p. Somit muß eine Zahl der ersten Menge zu einer gewissen Zahl der zweiten Menge modulo p kongruent sein und dies gibt die Behauptung, der man noch entnimmt:

Lemma B. *Zu jeder ungeraden Primzahl p gibt es $x_1, x_2, x_3, x_4 \in \{0, \ldots, \frac{1}{2}(p-1)\}$ und $h \in \{1, \ldots, p-1\}$, so daß gilt*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp.$$

Für $p \equiv 1 \pmod 4$ kann $x_3 = x_4 = 0$ gewählt werden.

Beweis. Mit den x, y aus Lemma A wählt man $x_1 = x$, $x_2 = 1$, $x_3 = y$, $x_4 = 0$ und hat $0 < x_1^2 + \ldots + x_4^2 < 4(\frac{1}{2}p)^2 = p^2$ sowie $p|(x_1^2 + \ldots + x_4^2)$, woraus sich die Behauptung ergibt. □

Der entscheidende Schritt zum Beweis des LAGRANGEschen Satzes ist enthalten in

Lemma C. *Für jede Primzahl p ist die diophantische Gleichung*

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 = p \tag{1}$$

lösbar.

Beweis. Für $p = 2$ ist dies klar. Sei nun $p \neq 2$ fest und $h_0 = h_0(p)$ die kleinste natürliche Zahl, zu der es $x_1, \ldots, x_4 \in \mathbb{Z}$ gibt, die

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = h_0 p \tag{2}$$

genügen. Die Existenz von h_0 sowie die Ungleichung $h_0 < p$ sind aus Lemma B zu entnehmen; es bleibt jetzt noch $h_0 = 1$ zu zeigen.

Wäre h_0 gerade, so wären alle, zwei oder keine der Zahlen x_i ungerade und ihre Numerierung darf o.B.d.A. so vorausgesetzt werden, daß $x_1 - x_2$ und $x_3 - x_4$ gerade sind. Dann sind auch $x_1 + x_2$, $x_3 + x_4$ gerade und man setzt $z_1 := \frac{1}{2}(x_1 + x_2)$, $z_2 := \frac{1}{2}(x_1 - x_2)$, $z_3 := \frac{1}{2}(x_3 + x_4)$, $z_4 := \frac{1}{2}(x_3 - x_4)$, was wegen (2) zu

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = h_0' p$$

mit natürlichem $h_0' := \frac{1}{2}h_0 < h_0$ führt. Dies seinerseits widerspricht der Minimaleigenschaft von h_0.

Nun werde angenommen, h_0 sei ungerade und mindestens gleich 3. Zu den x_i in (2) können y_i aus dem absolut kleinsten Restsystem modulo h_0 so gewählt werden, daß $y_i \equiv x_i \pmod{h_0}$ für $i = 1, \ldots, 4$ gilt. Nicht alle x_i können durch h_0 teilbar sein (sonst wäre $h_0|p$) und so sind nicht alle y_i Null, also $0 < y_1^2 + \ldots + y_4^2 < 4(\frac{1}{2}h_0)^2 = h_0^2$ und $y_1^2 + \ldots + y_4^2 \equiv x_1^2 + \ldots + x_4^2 \equiv 0 \pmod{h_0}$. Daher ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = h_1 h_0 \tag{3}$$

mit natürlichem $h_1 < h_0$. Nun hat man die zu 1(2) analoge, auf EULER (1748) zurückgehende Formel

$$\begin{aligned}(\sum_{i=1}^{4} x_i^2)(\sum_{i=1}^{4} y_i^2) = (\sum_{i=1}^{4} x_i y_i)^2 + (-x_1y_2 + x_2y_1 - x_3y_4 + x_4y_3)^2 \\ + (-x_1y_3 + x_3y_1 - x_4y_2 + x_2y_4)^2 \\ + (-x_1y_4 + x_4y_1 - x_2y_3 + x_3y_2)^2,\end{aligned} \tag{4}$$

die man wieder durch einfaches Ausrechnen bestätigen kann. Offenbar sind die drei letzten Klammern rechts in (4) jeweils durch h_0 teilbar und wegen

$$\sum_{i=1}^{4} x_i y_i \equiv \sum_{i=1}^{4} x_i^2 = h_0 p \equiv 0 \pmod{h_0}$$

trifft dies auch für die erste Klammer rechts in (4) zu. Schreibt man diese vier Klammern daher nacheinander als h_0u_1,h_0u_2, h_0u_3, h_0u_4 mit ganzen u_i, so ergibt sich aus (2), (3), (4)

$$h_1 h_0^2 p = h_0^2(u_1^2 + u_2^2 + u_3^2 + u_4^2).$$

Nach Kürzen durch h_0^2 erhält man hieraus einen Widerspruch zu der bei (2) formulierten Minimaleigenschaft von h_0; man beachte $h_1 < h_0$. □

Beweis des Satzes von LAGRANGE. (4) besagt, daß das Produkt zweier natürlicher Zahlen, die beide als Summe von vier Quadraten darstellbar sind, selbst ebenfalls in dieser Weise darstellbar ist. Da nach Lemma C jede Primzahl als Summe von vier Quadraten darstellbar ist, hat man den gewünschten Satz. □

Bemerkung. Für reelle $x_1, \ldots, x_4$, $y_1, \ldots, y_4$ ergibt sich der "Vier–Quadrate–Satz" (4) aus der Produktregel $|x|\,|y| = |xy|$ für die Quaternionen $x := x_1 + x_2i + x_3j + x_4k$, $y := y_1 + y_2i + y_3j + y_4k$, wenn man gemäß der Festsetzungen $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ multipliziert und noch die Definition $\bar{x} := x_1 - x_2i - x_3j - x_4k$ und $|x| := \sqrt{x\bar{x}}$ beachtet. Wie früher 1(2) bleibt auch (4) in jedem kommutativen Ring gültig.

5. Nochmals Primzahlen als Summe zweier Quadrate. Sei jetzt $p \equiv 1 \pmod 4$ und wie in 2 angekündigt soll für solche Primzahlen p hier ein dritter Beweis für die Lösbarkeit von 1(1) gegeben werden, der eng mit demjenigen verwandt ist, der zuletzt zur Lösbarkeit von 4(1) geführt hat:

Man definiert $g_0 = g_0(p)$ als kleinste natürliche Zahl, zu der es $x_1, x_2 \in \mathbb{Z}$ gibt, die $x_1^2 + x_2^2 = g_0 p$ genügen; die Existenz von g_0 und die Abschätzung $g_0 < p$ sind aus demselben Grund wie in 4 bei h_0 klar und es bleibt wieder $g_0 = 1$ einzusehen. Wäre g_0 gerade, so wären beide oder kein x_i ungerade, jedenfalls also sind $x_1 + x_2$ und $x_1 - x_2$ gerade und mit z_1, z_2 wie in 4 ist $z_1^2 + z_2^2 = g_0' p$ mit natürlichem $g_0' := \frac{1}{2} g_0 < g_0$ entgegen der Definition von g_0. Ist $g_0 \geq 3$ und ungerade, so definiere man y_1, y_2 analog wie in 4. Nicht beide x_i können durch g_0 teilbar sein, da sonst $g_0 | p$ gelten müßte, und so sind nicht alle y_i Null, also $0 < y_1^2 + y_2^2 < 2(\frac{1}{2} g_0)^2 < g_0^2$ und $y_1^2 + y_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{g_0}$, d.h. $y_1^2 + y_2^2 = g_1 g_0$ mit natürlichem $g_1 < g_0$. Nach 1(2) ist

$$g_1 g_0^2 p = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$$

und hier sind beide Klammern durch g_0 teilbar, die erste wegen $x_1 y_1 + x_2 y_2 \equiv x_1^2 + x_2^2 = g_0 p \equiv 0 \pmod{g_0}$. Wie in 4 findet man ganze u_1, u_2, die $u_1^2 + u_2^2 = g_1 p$ genügen, im Widerspruch zur Definition von g_0.

6. Summen dreier Quadrate. Bereits zu Anfang von 4 war zu erkennen, daß es gewisse natürliche Zahlen n gibt, für die die Gleichung

$$X_1^2 + X_2^2 + X_3^2 = n \tag{1}$$

unlösbar ist. Die n mit dieser Eigenschaft kann man wie folgt charakterisieren:

Satz. *Genau dann, wenn die natürliche Zahl n die Gestalt $4^a u$ mit $a, u \in \mathbb{N}_0$, $u \equiv 7 \pmod 8$ hat, ist (1) unlösbar.*

D.h. genau diese n sind nicht als Summe von drei Quadraten darstellbar; hier braucht man wirklich vier Summanden. Da Quadrate ganzer Zahlen $\equiv 0, 1$ oder $4 \pmod 8$ sind, ist die Summe dreier Quadrate $\not\equiv 7 \pmod 8$. Ist also $u \equiv 7 \pmod 8$, so ist

$$X_1^2 + X_2^2 + X_3^2 = 4^a u \tag{1_a}$$

bei $a = 0$ unlösbar. Sei nun $a \in \mathbb{N}$ und die Unlösbarkeit von (1_{a-1}) bereits bekannt. Ist dann (1_a) lösbar und $(x_1, x_2, x_3) \in \mathbb{Z}^3$ eine solche Lösung, so ist $x_1^2 + x_2^2 + x_3^2$ modulo 4 kongruent der Anzahl der ungeraden x_i, wegen (1_a) also kongruent Null. Alle x_i sind demnach gerade und $y_i := \frac{1}{2} x_i$ für $i = 1, 2, 3$ führt zu $y_1^2 + y_2^2 + y_3^2 = 4^{a-1} u$ im Widerspruch zur Unlösbarkeit von (1_{a-1}). Damit ist die leichtere Richtung des obigen Satzes bewiesen.

Die schwierigere wurde erstmals von LEGENDRE (1798) und GAUSS (1801) erledigt, soll hier jedoch nicht ausgeführt werden. Der interessierte Leser kann hierzu etwa LANDAU [13], Band I konsultieren.

7. Warings Problem und Hilberts Satz. In seinen *Meditationes Algebraicae* (1770, S. 203–204) schrieb WARING im selben Jahr, in dem LAGRANGE Satz 4 bewiesen hatte: "Omnis integer numerus vel est cubus; vel e duobus, tribus, 4, 5, 6, 7, 8, vel novem cubus compositus: est etiam quadratoquadratus; vel e duobus, tribus & c. usque ad novemdecim compositus & sic deinceps." In der Ausgabe von 1782 ist auf Seite 349 hinzugefügt: "... consimilia etiam affirmari possunt (exceptis excipiendis) de eodem numero quantitatum earundem dimensionum."

Offenbar behauptete WARING also, allerdings ohne Angabe irgendeines Beweises, jede natürliche Zahl sei Summe von höchstens neun Kuben, von höchstens neunzehn Biquadraten usw. Man hat diese Feststellung später so als WARINGsches Problem interpretiert: *Zu jedem ganzen $k \geq 2$ gibt es eine natürliche Zahl g derart, daß jedes $n \in \mathbb{N}$ als Summe von g ganzen nichtnegativen Zahlen darstellbar ist, die k–te Potenzen sind.*

Der LAGRANGEsche Satz in Verbindung mit Satz 6 lehrt, daß man für $k = 2$ mit $g = 4$, aber keinem kleineren g auskommt. Historisch das nächste Resultat dürfte von J. LIOUVILLE (1859) stammen, der für $k = 4$ beweisen konnte, daß jedenfalls $g = 53$ ausreicht.

Im Jahre 1909 gab es dann zwei bedeutende Fortschritte: A. WIEFERICH bewies, daß $g = 9$ (aber kein kleineres g) für $k = 3$ ausreicht und HILBERT gelang die volle Lösung des Problems von WARING, indem er dessen Vermutung bestätigen konnte.

Seither ist eine überaus umfangreiche Literatur, vor allem im Bereich der analytischen Zahlentheorie, entstanden, die sich mit dem WARING–HILBERTschen Ergebnis befaßt. Nachdem für jedes $k \geq 2$ die Existenz eines g mit den obigen Eigenschaften bewiesen war, war die nächste interessierende Frage, für jedes $k \geq 2$ das kleinste ausreichende g tatsächlich zu ermitteln; dieses werde hinfort wie üblich $g(k)$ genannt.

Es ist plausibel, daß $g(k)$ mit k anwachsen muß. Dies wird präzisiert in der folgenden

Proposition. *Für jedes ganze $k \geq 2$ ist*

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

Beweis. Man betrachte die natürlichen Zahlen

$$n_k := 2^k\big[(\frac{3}{2})^k\big] - 1,$$

die kleiner als 3^k sind. Für ihre Darstellung in der Form $x_1^k + \ldots + x_{g(k)}^k$ müssen offenbar alle x_i gleich 0, 1 oder 2 sein. Sind etwa a_k Stück gleich 0, b_k Stück gleich 1 und c_k Stück gleich 2, so ist $n_k = 2^k c_k + b_k$ und also

$$g(k) = a_k + b_k + c_k \geq b_k + c_k = n_k - c_k(2^k - 1) \geq n_k - \big(\big[(\frac{3}{2})^k\big] - 1\big)\big(2^k - 1\big)$$
$$= 2^k + \big[(\frac{3}{2})^k\big] - 2 =: g^*(k),$$

da $c_k < [(\frac{3}{2})^k]$ bleiben muß. □

Bei kleinen Werten von k hat man folgende Unterschranken $g^*(k)$ für $g(k)$ gemäß obiger Proposition:

k	2	3	4	5	6	7	8	9	10
$g^*(k)$	4	9	19	37	73	143	279	548	1079

Man vermutet, daß $g(k) = g^*(k)$ für $k = 2, 3, \ldots$ gilt. Für $k = 2$ bzw. 3 ist dies durch die Ergebnisse von LAGRANGE bzw. WIEFERICH bestätigt, für $k = 4$ durch R. BALASUBRAMANIAN, J.–M. DESHOUILLERS und F. DRESS (1985) und für $k = 5$ durch J.–R. CHEN (1964). Ebenfalls 1964 konnte die fragliche Gleichheit für alle k mit $400 < k \leq 200\,000$ von R.M. STEMMLER bewiesen werden, nachdem dies für den Bereich $6 \leq k \leq 400$ schon 1936 von L.E. DICKSON erledigt worden war. 1990 konnten J.M. KUBINA und M.C. WUNDERLICH die Gleichheit sogar bis 471 600 000 nachweisen.

Auch im Bereich $k > 471\,600\,000$ hat man fast vollständige Klarheit: Mit einer Verfeinerung des THUE–SIEGEL–ROTHschen Approximationssatzes 6.2.1 konnte MAHLER 1957 nachweisen, daß $g(k) > g^*(k)$ höchstens endlich oft möglich ist.

8. Anmerkungen über Darstellungsanzahlen. Für die Zwecke dieses Abschnitts werde

$$r_g(n) := \#\{(m_1, \ldots, m_g) \in \mathbb{Z}^g : m_1^2 + \ldots + m_g^2 = n\} \tag{1}$$

bei ganzen $g > 0$ und n gesetzt. In den Sätzen 3 bzw. 6 wurden die ganzen $n > 0$ mit $r_2(n) > 0$ bzw. $r_3(n) > 0$ charakterisiert, während LAGRANGEs Satz 4 nichts anderes als $r_4(n) > 0$ für alle natürlichen n besagt.

Hier soll noch ein möglicher analytischer Zugang zu expliziten Formeln für die Darstellungsanzahl $r_g(n)$ angedeutet werden. Zunächst ist aus (1) klar, daß die Gleichung

$$\Big(\sum_{m\in\mathbb{Z}} z^{m^2}\Big)^g = \sum_{n=0}^{\infty} r_g(n) z^n \tag{2}$$

für alle komplexen z mit $|z| < 1$ gilt. Setzt man für dieselben z

$$\Theta(z) := \sum_{m\in\mathbb{Z}} z^{m^2}, \tag{3}$$

so kann man hoffen, aus (2) durch Koeffizientenvergleich $r_g(n)$ zu ermitteln, falls eine geeignete Reihenentwicklung von $\Theta(z)^g$ gelingt.

Tatsächlich hat in dieser Richtung JACOBI die beiden Formeln

$$\Theta(z)^2 = 1 + 4\sum_{\ell=0}^{\infty} \frac{(-1)^\ell z^{2\ell+1}}{1 - z^{2\ell+1}} \tag{4}$$

bzw.

$$\Theta(z)^4 = 1 + 8\sum_{\ell=1}^{\infty} \frac{\ell z^\ell}{1 + (-z)^\ell} \tag{5}$$

entdeckt und in einem Brief vom 9. September 1828 LEGENDRE mitgeteilt. Beweise für beide Formeln finden sich in § 40 von JACOBIs berühmten *Fundamenta Nova Theoriae Functionum Ellipticarum* (= Gesammelte Werke I, 49–239) aus dem Jahre 1829.

Aus (4) folgt nun leicht mittels geometrischer Reihe in $|z| < 1$

$$\Theta(z)^2 = 1 + 4\sum_{\ell=0}^{\infty}\sum_{m=1}^{\infty} (-1)^\ell z^{(2\ell+1)m} = 1 + 4\sum_{n=1}^{\infty} \delta(n) z^n \tag{6}$$

mit

$$\delta(n) := \sum_{\substack{d|n \\ d \text{ ungerade}}} (-1)^{(d-1)/2} \tag{7}$$

für $n \in \mathbb{N}$. Für dieselben n ergibt sich aus (2), (3) und (6)

$$r_2(n) = 4\delta(n). \tag{8}$$

Die vollständige Berechnung von $r_2(n)$ mittels (8) wird vorbereitet durch folgendes

Lemma. *Die durch (7) definierte zahlentheoretische Funktion δ ist multiplikativ.*

Beweis. Seien $n_1, n_2 \in \mathbb{N}$ zueinander teilerfremd. Jedes ungerade $d \in \mathbb{N}$ mit $d | n_1 n_2$ läßt sich dann eindeutig in der Form $d = d_1 d_2$ mit $d_1 | n_1$, $d_2 | n_2$ und $2 \nmid d_1$, $2 \nmid d_2$ schreiben, was zu

$$\begin{aligned}\delta(n_1 n_2) &= \sum_{\substack{d_1 | n_1,\, d_2 | n_2 \\ d_1, d_2 \text{ ungerade}}} (-1)^{(d_1 d_2 - 1)/2} = \prod_{j=1}^{2} \sum_{\substack{d_j | n_j \\ d_j \text{ ungerade}}} (-1)^{(d_j - 1)/2} \\ &= \delta(n_1)\delta(n_2)\end{aligned}$$

führt; man beachte dabei, daß $0 \equiv (d_1 - 1)(d_2 - 1) = (d_1 d_2 - 1) - (d_1 + d_2 - 2)$ (mod 4) äquivalent ist mit $\frac{1}{2}(d_1 d_2 - 1) \equiv \frac{1}{2}(d_1 - 1) + \frac{1}{2}(d_2 - 1)$ (mod 2). □

Dies Lemma führt jetzt leicht zum

Satz von Gauss. *Für natürliche n gilt*

$$r_2(n) = \begin{cases} 0, & \text{falls } 2 \nmid \nu_p(n) \text{ für eine Primzahl } p \equiv 3 \pmod 4, \\ 4 \prod\limits_{p \equiv 1 \,(4)} (1 + \nu_p(n)) & \text{sonst.} \end{cases}$$

Beweis. Für ungerade Primzahlen p und $\nu \in \mathbb{N}_0$ ist nach (7)

$$\delta(p^\nu) = \sum_{\mu=0}^{\nu} (-1)^{(p^\mu - 1)/2} = \begin{cases} 1 + \nu, & \text{falls } p \equiv 1 \pmod 4, \\ 1, & \text{falls } p \equiv 3 \pmod 4 \text{ und } 2 | \nu, \\ 0, & \text{falls } p \equiv 3 \pmod 4 \text{ und } 2 \nmid \nu; \end{cases}$$

weiter gilt $\delta(2^\nu) = 1$ für alle $\nu \in \mathbb{N}_0$. Die Behauptung ergibt sich jetzt aus (8) mit Hilfe des Lemmas. □

Bemerkungen. 1) Die obige Formel für $r_2(n)$ findet sich wohl erstmals bei Gauss (*Disquisitiones Arithmeticae*, Art. 182), der an gleicher Stelle (Artt. 291, 292) für $r_3(n)$ einen geschlossenen Ausdruck angegeben hat.

2) Reihen des Typs $\sum_{n \geq 1} a_n z^n/(1 - z^n)$, wie sie rechts in (4) auftreten, heißen übrigens Lambertsche Reihen. Sie sind für die analytische Zahlentheorie von gewisser Bedeutung.

Um als nächstes für $r_4(n)$ eine Formel bequem aufschreiben zu können, ist die Einführung der folgenden, durch

$$\sigma_u(n) := \sum_{\substack{d|n \\ d \text{ ungerade}}} d$$

für alle ganzen $n > 0$ definierten (offenbar multiplikativen) zahlentheoretischen Funktion zweckmäßig. Damit gilt der

Satz von Jacobi. *Für jedes natürliche n gilt $r_4(n) = 8(2 + (-1)^n)\sigma_u(n)$.*

Beweis. Nach (2), (3) und (5) gilt in $|z| < 1$

$$\begin{aligned} \sum_{n=0}^{\infty} r_4(n) z^n &= 1 + 8 \sum_{\ell=1}^{\infty} \sum_{m=0}^{\infty} (-1)^{(\ell+1)m} \ell z^{\ell(m+1)} \\ &= 1 + 8 \sum_{\ell,m=1}^{\infty} (-1)^{(\ell+1)(m+1)} \ell z^{\ell m} \qquad (9) \\ &= 1 + 8 \sum_{n=1}^{\infty} \Delta(n) z^n \end{aligned}$$

mit

$$\Delta(n) := \sum_{\ell|n} (-1)^{(\ell+1)((n/\ell)+1)} \ell. \qquad (10)$$

Bei ungeradem n folgt hieraus $\Delta(n) = \sum_{\ell|n} \ell = \sigma(n) = \sigma_u(n)$ mit der in 1.1.7 eingeführten Teilersummenfunktion σ, also $r_4(n) = 8\Delta(n) = 8\sigma_u(n)$ wegen (9), was hier die Behauptung des Jacobischen Satzes beweist.

Ist $n > 0$ gerade, etwa $n = 2^i k$ mit $i, k \in \mathbb{N}$, $2 \not| k$, so läßt sich jeder Teiler ℓ von n rechts in (10) eindeutig in der Form $\ell = 2^\iota \kappa$ mit $\iota \in \{0, \ldots, i\}$, $\kappa \in \mathbb{N}$, $\kappa | k$ schreiben. Automatisch sind κ und $\frac{k}{\kappa}$ ungerade und (10) liefert

$$\begin{aligned} \Delta(n) &= \sum_{\iota=0}^{i} \sum_{\kappa|k} (-1)^{(2^\iota \kappa+1)(2^{i-\iota}(k/\kappa)+1)} 2^\iota \kappa \\ &= \Big(\sum_{\iota=0}^{i} (-1)^{(2^\iota+1)(2^{i-\iota}+1)} 2^\iota\Big) \Big(\sum_{\kappa|k} \kappa\Big). \end{aligned}$$

Für $0 < \iota < i$ ist hier der Exponent von -1 ungerade, während er für $\iota = 0$ und $\iota = i$ gerade ist. Dies führt zu

$$\Delta(n) = (2^i - 2^{i-1} - \ldots - 2 + 1)\sigma(k) = 3\sigma(k) = 3\sigma_u(n),$$

also wegen (9) zu $r_4(n) = 8\Delta(n) = 24\sigma_u(n)$, was auch in diesem Fall Jacobis Formel beweist. □

Bemerkung. 3) Zum Schluß sei darauf hingewiesen, daß die in 7 angesprochenen Ergebnisse ebenfalls quantitative Verfeinerungen folgender Art zulassen: Ist bei ganzem $k \geq 2$ die natürliche Zahl g (in Abhängigkeit von k) genügend groß, so kann man mit analytischen Hilfsmitteln für die Anzahl der Darstellungen aller "großen" natürlichen Zahlen als Summe von g natürlichen Zahlen, die ihrerseits k–te Potenzen sind, eine asymptotische Formel angeben. Der Leser sei diesbezüglich auf R.C. VAUGHAN [30] verwiesen.

§ 2. Polynomiale diophantische Gleichungen

1. Pythagoräische Tripel. Bei der Frage nach rechtwinkligen Dreiecken mit ganzzahligen Seitenlängen stößt man auf die diophantische Gleichung

$$X^2 + Y^2 = Z^2. \tag{1}$$

Mindestens bis in die babylonische Mathematik läßt sich dieses Problem zurückverfolgen. PYTHAGORAS soll bereits die unendlich vielen Lösungstripel

$$(2k+1, 2k^2+2k, 2k^2+2k+1), \qquad k = 1, 2, 3, \ldots, \tag{2}$$

von (1) in natürlichen Zahlen gekannt haben. Diese Folge beginnt mit $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, ...

Hauptziel des nächsten Abschnitts ist die Ermittlung aller Lösungen $(x, y, z) \in \mathbb{Z}^3$ von (1). Dazu ist es aber sinnvoll, zunächst einige leichte Reduktionen durchzuführen. Erst einmal darf o.B.d.A. $xyz \neq 0$ vorausgesetzt werden: Ist nämlich $z = 0$, so ist $(0, 0, 0)$ die einzige Lösung von (1); ist $z \neq 0$, aber $xy = 0$, so sind $(\pm z, 0, z)$ und $(0, \pm z, z)$ die einzigen Lösungen.

Sei im weiteren $xyz \neq 0$. Das Tripel (x, y, z) löst (1) genau dann, wenn die acht Tripel $(\pm x, \pm y, \pm z)$ die Gleichung (1) lösen. Genau eines dieser Tripel hat lauter positive Komponenten. So darf o.B.d.A. $x, y, z \in \mathbb{N}$ vorausgesetzt werden und jede Lösung $(x, y, z) \in \mathbb{N}^3$ von (1) heißt ein *pythagoräisches Tripel*. Ist (x, y, z) ein pythagoräisches Tripel und $d \in \mathbb{N}$, so ist offenbar auch (dx, dy, dz) ein pythagoräisches Tripel; hat man umgekehrt ein pythagoräisches Tripel (x', y', z') und ist d der größte gemeinsame Teiler der Komponenten x', y', z', so ist $(x'/d,\ y'/d,\ z'/d)$ ein pythagoräisches Tripel mit zueinander teilerfremden Komponenten. Lösungen (x, y, z) von (1) mit teilerfremden Komponenten nennt man *primitiv*. Es reicht also, alle primitiven pythagoräischen Tripel zu bestimmen, d.h. alle (1) lösenden $(x, y, z) \in \mathbb{N}^3$ mit paarweise teilerfremden Komponenten.

Die Teilerfremdheit schlechthin und die paarweise Teilerfremdheit sind hier wegen der speziellen Gestalt von (1) tatsächlich äquivalent: Offenbar folgt stets die

erstere aus der letzteren. Sind umgekehrt irgend zwei der Zahlen x, y, z nicht zueinander teilerfremd, so sei p eine beide teilende Primzahl; wegen (1) teilt p (sogar p^2) das Quadrat der dritten Zahl, also diese selbst und damit sind x, y, z nicht zueinander teilerfremd.

Sei nun (x, y, z) ein primitives pythagoräisches Tripel. *Von den x, y ist genau eines gerade (und künftig sei dies o.B.d.A. y)*: Wegen der paarweisen Teilerfremdheit können nicht beide gerade sein; wären sie jedoch beide ungerade, so hätte man $x^2 + y^2 \equiv 2 \pmod 4$, aber $z^2 \not\equiv 2 \pmod 4$.

2. Euklids Satz über pythagoräische Tripel. Nach den zuletzt vorgenommenen Reduktionen kann das abschließende Ergebnis formuliert werden, welches auf EUKLID (*Elemente* X, §§ 28, 29) zurückgeht:

Satz. *Alle primitiven pythagoräischen Tripel (x, y, z) mit geradem y sind durch folgende Parameterdarstellung gegeben*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2 \tag{1}$$

mit teilerfremden natürlichen a, b, so daß die Differenz $a-b$ positiv und ungerade ist.

Die eine Richtung des Beweises wird vorbereitet durch das noch öfter zu benützende

Lemma. *Gilt $j^n = gh$ mit $g, h, j, n \in \mathbb{N}$ und sind g, h teilerfremd, so existieren teilerfremde $g_1, h_1 \in \mathbb{N}$, so daß $g = g_1^n$, $h = h_1^n$ gilt.*

Beweis. Ist

$$j = \prod_{\kappa=1}^{k} p_\kappa^{a_\kappa} = \prod_{\substack{\kappa=1 \\ p_\kappa | g}}^{k} p_\kappa^{a_\kappa} \cdot \prod_{\substack{\kappa=1 \\ p_\kappa | h}}^{k} p_\kappa^{a_\kappa} =: g_1 \cdot h_1,$$

so hat man nach Voraussetzung $g_1^n h_1^n = gh$. Da g und h_1^n zueinander teilerfremd sind, ist $h_1^n | h$ nach Satz 1.2.6(i), also $h = dh_1^n$ und daher $g_1^n = dg$ mit $d \in \mathbb{N}$. Ist p eine d teilende Primzahl, so gilt $p|h$ und $p|g_1$, also $p|g$, was $d = 1$ impliziert. □

Beweis des EUKLIDschen *Satzes.* Hierzu überlegt man erst, daß die durch (1) gegebenen (x, y, z) primitive pythagoräische Tripel sind. Dabei ist die Primitivität folgendermaßen ersichtlich: Sei p eine x und z teilende Primzahl; dann ist $p \neq 2$ und $p|2a^2$, $p|2b^2$, also $p|a$ und $p|b$ entgegen der vorausgesetzten Teilerfremdheit von a, b.

Sei nun umgekehrt (x, y, z) ein primitives pythagoräisches Tripel mit geradem y. Da x und z beide ungerade sein müssen, sind $z+x$ und $z-x$ gerade. Man setzt $y_1 := \frac{1}{2}y$, $g := \frac{1}{2}(z+x)$, $h := \frac{1}{2}(z-x)$ und hat $y_1^2 = gh$ wegen 1(1). Wäre p ein gemeinsamer Primfaktor der natürlichen Zahlen g, h, so wäre $p|(g+h)$, $p|(g-h)$, also würden x und z von p geteilt entgegen ihrer vorausgesetzten Teilerfremdheit. Nach dem bereitgestellten Lemma ist mit teilerfremden $a, b \in \mathbb{N}$: $g = a^2$, $h = b^2$, woraus sich x und z bereits wie in (1) ergeben. Aus $y^2 = 4y_1^2 = (2ab)^2$ folgt $y = 2ab$, aus $x > 0$ folgt $a > b$ und aus $2 \nmid x$ ergibt sich $2 \nmid (a-b)$ wie behauptet. □

Bemerkung. Die Abbildung der Menge aller Paare (a, b) mit den in EUKLIDs Satz genannten Eigenschaften auf die Menge aller primitiven pythagoräischen Tripel (x, y, z) mit $2|y$, die durch (1) beschrieben wird, ist übrigens bijektiv: Aus $(a_1^2 - b_1^2, 2a_1b_1, a_1^2 + b_1^2) = (a_2^2 - b_2^2, 2a_2b_2, a_2^2 + b_2^2)$ mit a_i, b_i wie in EUKLIDs Satz folgt nämlich $a_1^2 + b_1^2 = a_2^2 + b_2^2$, $a_1^2 - b_1^2 = a_2^2 - b_2^2$, somit $a_1^2 = a_2^2$, $b_1^2 = b_2^2$ und daraus $a_1 = a_2$, $b_1 = b_2$ wegen $a_i, b_i \in \mathbb{N}$.

Übrigens entsprechen die von PYTHAGORAS angegebenen Lösungstripel 1(2) der Gleichung 1(1) genau den Paaren (a, b) mit $a = k+1$, $b = k$ $(k = 1, 2, \ldots)$ in EUKLIDs Satz.

3. Rationale Punkte auf Kurven zweiten Grades. Wie bereits erwähnt war die vollständige Lösung der diophantischen Gleichung 1(1) in natürlichen Zahlen schon EUKLID bekannt. Hier soll dieselbe Problemstellung zunächst in äquivalenter Weise umformuliert und anschließend verallgemeinert werden.

Hat man eine Lösung $(x, y, z) \in \mathbb{Z}^3$ mit $z \neq 0$ der Gleichung

$$1(1) \qquad X^2 + Y^2 - Z^2 = 0$$

und setzt man $u := \frac{x}{z}$, $v := \frac{y}{z}$, so ist $(u, v) \in \mathbb{Q}^2$ eine rationale Lösung der Gleichung

$$(1) \qquad U^2 + V^2 - 1 = 0.$$

Umgekehrt kann man selbstverständlich von jeder rationalen Lösung (u, v) von (1) zu einer Lösung (x, y, z) mit $z \neq 0$ von 1(1) in ganzen Zahlen übergehen.

Man betrachtet nun allgemeiner Polynome zweiten Grades in zwei Unbestimmten mit rationalen Koeffizienten

$$(2) \qquad f(U, V) := c_{00} + 2c_{01}U + 2c_{02}V + c_{11}U^2 + 2c_{12}UV + c_{22}V^2 \in \mathbb{Q}[U, V],$$

bei denen die symmetrische Matrix

$$\begin{pmatrix} c_{00} & c_{01} & c_{02} \\ c_{01} & c_{11} & c_{12} \\ c_{02} & c_{12} & c_{22} \end{pmatrix} \tag{3}$$

maximalen Rang haben möge. Daher verschwinden insbesondere nicht alle c_{11}, c_{12}, c_{22} und so ist f vom Gesamtgrad 2; ferner ist f über $\mathbb{Q}$ irreduzibel.

Geometrisch bestimmt die Menge der $(u, v) \in \mathbb{R}^2$ mit $f(u, v) = 0$ im $\mathbb{R}^2$ eine algebraische Kurve zweiten Grades, die nach den gemachten Voraussetzungen nicht zerfällt. Genauer kann gesagt werden: Haben alle Eigenwerte von (3) dasselbe Vorzeichen, so ist die Kurve ohne reellen Punkt; andernfalls stellt sie eine Hyperbel, Parabel bzw. Ellipse (d.h. einen nicht zerfallenden Kegelschnitt) dar je nachdem, ob $c_{12}^2 - c_{11}c_{22}$ größer, gleich bzw. kleiner als Null ist. Jedes $(u, v) \in \mathbb{Q}^2$ mit $f(u, v) = 0$ nennt man in der hier eingeführten geometrischen Sprechweise einen *rationalen Punkt* auf der vorgelegten algebraischen Kurve.

Bei der Behandlung mehrerer Probleme (z.B. 8, 9, 16, 17) des zweiten Buchs seiner *Arithmetika* hat DIOPHANT eine Methode vorgestellt, die es gestattet, aus einem einzigen rationalen Punkt der vorgegebenen Kurve sofort sämtliche zu gewinnnen. Mit seiner Methode läßt sich der folgende Satz beweisen.

Satz. *Sei f gemäß (2) vorgelegt, der Rang der Matrix (3) sei maximal und die diophantische Gleichung $f(U, V) = 0$ habe eine rationale Lösung (u_0, v_0). Dann hat sie bereits unendlich viele solche Lösungen und beide Komponenten sämtlicher rationaler Lösungen dieser Gleichung ergeben sich als Werte gewisser rationaler Funktionen einer Unbestimmten mit rationalen, nur von f, u_0, v_0 abhängigen Koeffizienten an rationalen Argumentstellen.*

Beweis. Die TAYLOR–Entwicklung von f um (u_0, v_0) erhält man unter Beachtung von $f(u_0, v_0) = 0$ rein algebraisch zu

$$\begin{aligned} f(U, V) = {} & 2d_1(U - u_0) + 2d_2(V - v_0) + c_{11}(U - u_0)^2 \\ & + 2c_{12}(U - u_0)(V - v_0) + c_{22}(V - v_0)^2 \end{aligned} \tag{4}$$

mit den Festsetzungen

$$d_1 := c_{01} + c_{11}u_0 + c_{12}v_0, \quad d_2 := c_{02} + c_{12}u_0 + c_{22}v_0. \tag{5}$$

Hier können d_1, d_2 nicht beide verschwinden; wegen $f(u_0, v_0) = 0$ wäre sonst auch noch $c_{00} + c_{01}u_0 + c_{02}v_0$ gleich Null im Gegensatz zur Rangvoraussetzung über die Matrix (3). Nun wählt man sich, DIOPHANT folgend, ein beliebiges

rationales k mit $c_{11}k^2 + 2c_{12}k + c_{22} \neq 0$ (hierdurch werden höchstens zwei k–Werte ausgeschlossen) und bestimmt dazu $t(k)$ gemäß

$$t(k) := \frac{-2(d_1k + d_2)}{c_{11}k^2 + 2c_{12}k + c_{22}}. \tag{6}$$

Aus (4) sieht man direkt, daß $f(u(k), v(k)) = 0$ wird für

$$u(k) := u_0 + kt(k) \quad v(k) := v_0 + t(k). \tag{7}$$

Wegen der Rationalität der c_{ij}, u_0, v_0 ist nach (5) und (6) auch $t(k)$ rational für jedes oben zugelassene rationale k. Nun ist $u(k) = u(k')$, $v(k) = v(k')$ gleichbedeutend mit $t(k) = t(k')$, $kt(k) = k't(k')$. Ist $t(k) \neq 0$, so folgt daraus schon $k = k'$; ist $t(k) = 0$, so auch $t(k') = 0$ und in diesem Fall muß $d_1 \neq 0$ sein wegen der Bemerkung nach (5) und aus $d_1k + d_2 = 0$, $d_1k' + d_2 = 0$ folgt erneut $k = k'$. Damit ist die erste Hälfte der Behauptung bewiesen.

Nimmt man im Falle $c_{11} = 0$ an, es sei auch $c_{01} + c_{12}v_0 = 0$, so würde sich $d_1 = 0$ aus (5) ergeben und damit aus (4)

$$f(U, V) = (V - v_0)(2d_2 + 2c_{12}(U - u_0) + c_{22}(V - v_0))$$

entgegen der Irreduzibilität von f über $\mathbb{Q}$. Für $c_{11} = 0$ ist also $d_1 \neq 0$, weshalb aus $f(u, v_0) = (u - u_0)(2d_1 + c_{11}(u - u_0)) = 0$ folgt $u = u_0$, falls $c_{11} = 0$, bzw. $u = u_0$ oder $u = u_0 - 2d_1/c_{11}$, falls $c_{11} \neq 0$. Jedenfalls hat man außer den in (7) erfaßten rationalen Lösungen $(u(k), v(k))$ der vorgelegten diophantischen Gleichung gegebenenfalls noch die eine weitere $(u_0 - 2d_1/c_{11}, v_0)$, falls $c_{11} \neq 0$.

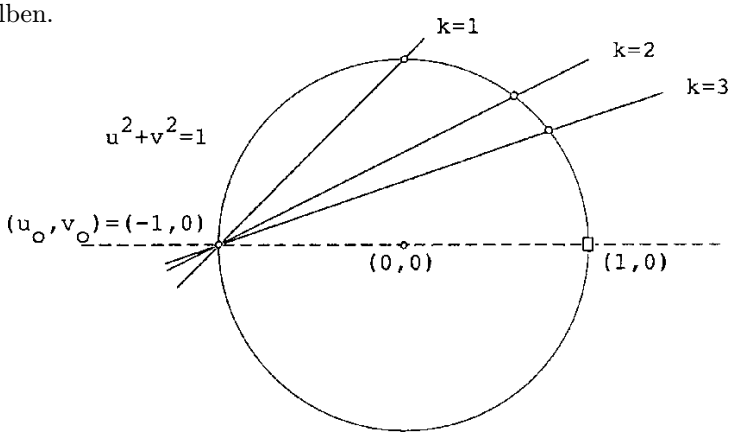
Sei jetzt umgekehrt (u, v) ein beliebiger rationaler Punkt der Kurve, o.B.d.A. mit $v \neq v_0$. Setzt man $t := v - v_0$ und dann $k := (u - u_0)/t$, so sind $t \neq 0$ und k rational und (4) in Verbindung mit $f(u, v) = 0$ besagt

$$2(d_1k + d_2) + (c_{11}k^2 + 2c_{12}k + c_{22})t = 0. \tag{8}$$

Wäre nun $c_{11}k^2 + 2c_{12}k + c_{22} = 0$, so auch $d_1k + d_2 = 0$ und (8) würde für jedes reelle t^* (statt t) gelten. Dies hieße aber, daß jeder Punkt (u^*, v^*) der Geraden $u^* - u_0 = kt^*$, $v^* - v_0 = t^*$ wegen (4) der Gleichung $f(u^*, v^*) = 0$ genügen müßte, was nicht geht. Aus (8) folgt daher $t = t(k)$ mit dem $t(k)$ aus (6). □

Bemerkungen. 1) Geometrisch bedeutet der in (7) zum Ausdruck kommende DIOPHANTsche Ansatz $u = u_0 + kt$, $v = v_0 + t$ offenbar, daß man den vorgelegten Kegelschnitt mit allen "rationalen" Geraden der Form $u - u_0 = k(v - v_0)$, $k \in \mathbb{Q}$, durch den bekannten rationalen Kurvenpunkt (u_0, v_0) zum Schnitt bringt; dabei bleibt dann die Gerade $v = v_0$ noch gesondert zu untersuchen. Die im

allgemeinen anfallenden, von (u_0, v_0) verschiedenen Schnittpunkte der jeweiligen Geraden durch (u_0, v_0) mit dem Kegelschnitt sind weitere rationale Punkte desselben.



2) Wendet man den Satz speziell auf Gleichung (1) an, so sind $-c_{00} = c_{11} = c_{22} = 1$, alle anderen $c_{ij} = 0$. Arbeitet man etwa mit $(u_0, v_0) = (-1, 0)$, so wird $d_1 = -1$, $d_2 = 0$ und (6), (7) führen zu

$$u(k) = \frac{k^2 - 1}{k^2 + 1} \qquad v(k) = \frac{2k}{k^2 + 1}\,. \tag{9}$$

Wegen $c_{11} \neq 0$ erhält man noch $(u_0 - 2d_1/c_{11}, v_0) = (1, 0)$ als weiteren Kurvenpunkt. Wählt man noch a, b wie in Satz 2 und setzt damit $k := a/b$, so wird der gemäß (9) gebildete Punkt gleich $((a^2 - b^2)/(a^2 + b^2),\ 2ab/(a^2 + b^2))$, also gleich $(x/z, y/z)$ wie in 2(1).

4. Rationale Punkte gewisser Kurven dritten Grades. Sei jetzt $f \in \mathbb{Q}[U, V]$ irreduzibel über $\mathbb{Q}$ und tatsächlich von beiden Unbestimmten abhängig; in 3(2) war dies wegen der Rangforderung an die Matrix 3(3) automatisch erfüllt. Im $\mathbb{R}^2$ wird dann durch die Gleichung $f(u, v) = 0$ eine *algebraische Kurve* definiert; unter deren *Grad* versteht man den Gesamtgrad von f, und der Begriff eines rationalen Punktes dieser Kurve wird wie in 3 gefaßt.

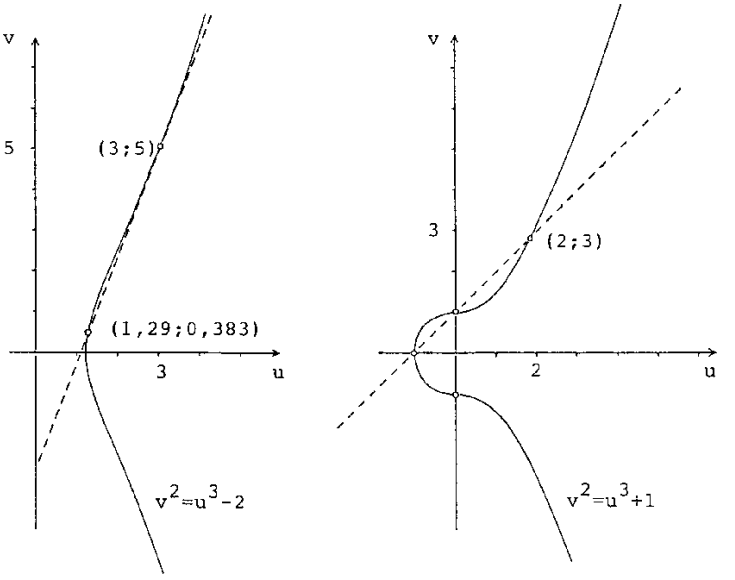
Während die Frage nach den rationalen Punkten einer algebraischen Kurve ersten bzw. zweiten Grades in 1.3.3 bzw. 3 abgehandelt wurde, *sollen hier zwei Methoden präsentiert werden, mit denen man aus einem oder zwei bekannten rationalen Punkten einer Kurve dritten Grades im allgemeinen einen neuen derartigen Punkt gewinnen kann.* Diese Methoden werden bisweilen C.G. BACHET (auch EULER oder CAUCHY) zugeschrieben, der sie 1621 erstmalig auf die Gleichung

$$V^2 = U^3 + k \tag{1}$$

im Falle $k = -2$ angewandt haben soll. In der Tat hat BACHET in jenem Jahr eine Neuausgabe von griechischem Original und lateinischer Übersetzung einschließlich einer ausführlichen Kommentierung der DIOPHANTschen *Arithmetika* besorgt, in deren viertem bzw. sechstem Buch bei einigen Problemen über Kurven dritten Grades (z.B. 24,26 bzw. 18,19) sich beide Methoden zumindest implizit finden. Um technische Komplikationen zu vermeiden, werden beide anhand der speziellen, durch (1) mit rationalem k festgelegten algebraischen Kurve erläutert, die eine sehr typische vom dritten Grade ist, vgl. 5.

Die Tangentenmethode. Ist $(u_0, v_0) \in \mathbb{Q}^2$ ein Punkt der durch (1) gegebenen Kurve, so ist $v - v_0 = \frac{3u_0^2}{2v_0}(u - u_0)$ für $v_0 \neq 0$ die Gleichung der Tangente in diesem Punkt an die Kurve. Schneidet man diese Tangente mit der Kurve, so muß jeder Schnittpunkt (u, v) außer der Tangentengleichung die Gleichung $v^2 - v_0^2 = u^3 - u_0^3$ erfüllen, was sich nach kurzer Rechnung als äquivalent mit $(u - u_0)^2(u - u_1) = 0$ erweist, wobei $u_1 := u_0(u_0^3 - 8k)/(4v_0^2)$ gesetzt ist. Für $u_1 \neq u_0$ hat man in (u_1, v_1) mit $v_1 := v_0 + 3u_0^2(u_1 - u_0)/(2v_0)$ einen neuen rationalen Kurvenpunkt gefunden. Dabei ist $u_1 \neq u_0$ gleichbedeutend mit $u_0^3 \neq -4k$, d.h. mit der Tatsache, daß (u_0, v_0) nicht Wendepunkt der Kurve ist.

Beispiel zur Tangentenmethode. Betrachtet man BACHETs Gleichung (1) mit $k = -2$, so ist offenbar $(3, 5)$ eine rationale Lösung, aus der sich mit der soeben beschriebenen Tangentenmethode $(\frac{129}{100}, \frac{383}{1000})$ als weitere rationale Lösung einstellt, die tatsächlich von BACHET angegeben wurde.



Die Sekantenmethode. Sind (u_0, v_0), $(u_1, v_1) \in \mathbb{Q}^2$ zwei Punkte der durch (1) gegebenen Kurve mit $u_0 \neq u_1$, so ist $v = pu + q$ mit

$$p := \frac{v_1 - v_0}{u_1 - u_0}, \quad q := \frac{u_1 v_0 - u_0 v_1}{u_1 - u_0}$$

die Gleichung der Sekante durch die beiden vorgegebenen Kurvenpunkte. Schneidet man diese Sekante mit der Kurve, so muß jeder Schnittpunkt (u, v) außer der Sekantengleichung die Gleichung $v^2 = u^3 + k$ erfüllen, was mit dem Bestehen von

$$u^3 - p^2 u^2 - 2pqu + k - q^2 = 0$$

äquivalent ist. Da aber u_0, u_1 dieser Gleichung genügen, hat sie eine weitere Wurzel u_2, die nach VIETAs Satz aus $u_0 + u_1 + u_2 = p^2$ gewonnen werden kann. Setzt man noch $v_2 := pu_2 + q$, so hat man in (u_2, v_2) einen rationalen Kurvenpunkt gefunden, der genau dann von den beiden Ausgangspunkten verschieden ist, wenn die Sekante nicht gleichzeitig Tangente in einem der Ausgangspunkte ist.

Beispiel zur Sekantenmethode. Gleichung (1) hat für $k = 1$ offenbar die drei rationalen Lösungen $(-1, 0)$, $(0, 1)$ und $(0, -1)$. Wendet man hier auf die ersten beiden die Sekantenmethode an, so erhält man $(2, 3)$ als neue Lösung; wegen der speziellen Form (1) ist damit auch $(2, -3)$ Lösung.

Bemerkungen. 1) Es erscheint ganz plausibel zu erwarten, daß man durch sukzessive Anwendung von Tangenten- und Sekantenmethode aus einer oder zwei rationalen Lösungen von (1) bei festem rationalem $k \neq 0$ im allgemeinen unendlich viele *verschiedene* rationale Lösungen gewinnen kann. Im Anschluß an BACHET behauptete FERMAT dies über Gleichung (1) bei $k = -2$, allerdings ohne Angabe eines Beweises. Erst 1930 konnte R. FUETER dies beweisen, der für ganzes $k \neq 0$, welches sich nach Division durch die größte darin als Faktor enthaltene sechste Potenz nicht auf 1 oder -432 reduziert, zeigte: Hat (1) eine rationale Lösung (u_0, v_0) mit $u_0 v_0 \neq 0$, so gibt es deren unendlich viele. Für $k = -432$ gibt es nur die beiden rationalen Lösungen $(12, \pm 36)$ und für $k = 1$ gibt es keine weiteren rationalen Lösungen als die fünf im Beispiel zur Sekantenmethode angegebenen. Übrigens wurde das soeben zitierte, den Fall $k = 1$ betreffende Resultat bereits 1738 von EULER mit Hilfe der in 6 zu besprechenden FERMATschen Deszendenzmethode bewiesen. Erwähnt sei noch, daß es auch gewisse k–Werte gibt (z.B. $k = 7$), für die (1) rational unlösbar ist.

2) Was die *ganzzahligen* Lösungen von (1) bei ganzem $k \neq 0$ betrifft, so hat A. THUE 1917 mit Hilfe seines in 6.2.1 angesprochenen Approximationssatzes die Endlichkeit der Lösungsanzahl sichern können. Eine explizite, alleine von k abhängige obere Schranke für $|u|$, $|v|$ hat A. BAKER 1968 gefunden, wenn

$(u, v) \in \mathbb{Z}^2$ Gleichung (1) löst. Sein diesbezügliches Ergebnis stützt sich auf seine in b) von 6.5.9 angedeuteten quantitativen Linearformensätze.

3) Für weitere Einzelheiten über Gleichung (1), die in der Theorie der diophantischen Gleichungen 350 Jahre lang immer wieder eine bedeutende Rolle gespielt hat, kann der interessierte Leser auf L.J. MORDELL [16], Kap. 26, verwiesen werden.

5. Resultate von Poincaré, Mordell und Faltings. Es fragt sich nun, unter welchen Bedingungen die in 3 bzw. 4 beschriebenen Verfahren geeignet sind, *alle* rationalen Punkte auf einer algebraischen Kurve, wie diese zu Anfang von 4 erklärt wurde, zu bestimmen. Um hier die entscheidenden Ergebnisse wenigstens formulieren zu können, muß man erst eine adäquate Einteilung der Kurven vornehmen; ihre Klassifikation nach dem Grad erweist sich jedenfalls als nicht ganz angemessen.

Hat man ein über $\mathbf{C}$ irreduzibles Polynom $f \in \mathbf{C}[U, V]$, welches o.B.d.A. von V tatsächlich abhängt, so wird durch die Gleichung $f(u, v) = 0$ implizit eine (komplexwertige) algebraische Funktion v der komplexen Variablen u definiert. In der Funktionentheorie führt man den Begriff der RIEMANNschen Fläche Φ_f dieser Funktion ein. Ist m_f der Grad von f bezüglich V, so ist m_f die Anzahl der Blätter von Φ_f. Sind $e_1, \ldots, e_{\ell_f}$ sämtliche paarweise verschiedenen Verzweigungspunkte von Φ_f in $\hat{\mathbf{C}} := \mathbf{C} \cup \{\infty\}$ und hängen für $\lambda = 1, \ldots, \ell_f$ in e_λ genau ε_λ Blätter zusammen, so kann man das *Geschlecht* g_f von Φ_f definieren durch

$$g_f := 1 - m_f + \frac{1}{2} \sum_{\lambda=1}^{\ell_f} (\varepsilon_\lambda - 1). \tag{1}$$

Stets erweist sich g_f als ganze nichtnegative Zahl.

Ist nun eine algebraische Kurve wie zu Anfang von 4 definiert, so versteht man unter ihrem Geschlecht die soeben eingeführte Zahl g_f. Ist $m_f = 1$, so $\ell_f = 0$ und $g_f = 0$. Ist $m_f = 2$, so ist $\ell_f = 2$ und $\varepsilon_\lambda = 2$ für $\lambda = 1, 2$, also erneut $g_f = 0$. Die durch 4(1) definierte algebraische Kurve ist vom Geschlecht 1, falls $k \neq 0$. Es ist nämlich $m_f = 2$ und also sind alle ε_λ gleich 2; weiter ist $\ell_f = 4$, ein e_λ ist ∞ und die übrigen drei sind die verschiedenen komplexen Nullstellen des Polynoms $U^3 + k$. (Im Fall $k = 0$ ergibt sich hier das Geschlecht 0.)

Während der Begriff des Geschlechts bereits um die Mitte des 19. Jahrhunderts von RIEMANN eingeführt wurde, hat erst H. POINCARE 1901 seine Bedeutung für die Frage nach den rationalen Punkten einer algebraischen Kurve voll erkannt. POINCARE hat damals (implizit) gezeigt, daß die DIOPHANTsche Methode aus 3 zur Bestimmung aller rationalen Punkte einer beliebigen algebraischen Kurve

vom Geschlecht Null führt, wenn man nur einen einzigen rationalen Kurvenpunkt kennt. Überdies hat man in diesem Fall eine rationale Parameterdarstellung für beide Komponenten sämtlicher rationaler Punkte, wie dies im Spezialfall von Satz 3 zum Ausdruck kam.

Um dieses POINCARÉsche Ergebnis verständlich zu machen, sei folgendes festgestellt: Hat man $f, g \in \mathbb{Q}(U, V)$, die jeweils von beiden Unbestimmten tatsächlich abhängen und gibt es $\varphi, \psi \in \mathbb{Q}(X, Y)$, so daß $g(X, Y) = f(\varphi(X, Y), \psi(X, Y))$ ist, so entsprechen den rationalen Punkten der durch $g(x, y) = 0$ definierten algebraischen Kurve rationale Punkte der durch $f(u, v) = 0$ gegebenen Kurve, wenn man einmal von höchstens endlich vielen Ausnahmepunkten absieht. Sind die obigen φ, ψ zusätzlich so beschaffen, daß es $\varphi_1, \psi_1 \in \mathbb{Q}(U, V)$ gibt mit $X = \varphi_1(\varphi(X, Y), \psi(X, Y))$, $Y = \psi_1(\varphi(X, Y), \psi(X, Y))$, so ist

$$f(U, V) = g(\varphi_1(U, V), \psi_1(U, V))$$

und den rationalen Punkten von $f(u, v) = 0$ entsprechen umgekehrt auch rationale Punkte von $g(x, y) = 0$.

Gibt es nun $\varphi, \psi, \varphi_1, \psi_1$ der beschriebenen Art, so nennt man die beiden in Frage stehenden algebraischen Kurven *birational äquivalent*. Es ist eine Tatsache, daß birational äquivalente algebraische Kurven gleiches Geschlecht haben. Dagegen gibt es durchaus birational nicht äquivalente Kurven gleichen Geschlechts.

POINCARÉ hatte seinerzeit bewiesen, daß jede algebraische Kurve vom Geschlecht Null und vom Grad $m \geq 3$ zu einer Kurve vom Grad $m - 2$ birational äquivalent ist. Dies erst macht POINCARÉs oben zitierte, das Geschlecht Null betreffende Resultate voll einsichtig, da sich hier alles auf Kurven vom Grad 1 oder 2 reduziert.

Ist das Geschlecht der algebraischen Kurve positiv, so geht die Eigenschaft ihrer rationalen Punkte, eine rationale Parameterdarstellung obiger Art zu besitzen, verloren. Immerhin konnte POINCARÉ noch zeigen, daß im Falle des Geschlechts Eins die in 4 besprochene DIOPHANTsche Tangenten– bzw. Sekantenmethode zur Bestimmung rationaler Kurvenpunkte aus "wenigen" vorgegebenen angewandt werden kann. Kurven des Geschlechts Eins mit mindestens einem rationalen Punkt erweisen sich nämlich als birational äquivalent zu einer Kurve dritten Grades, die durch eine Gleichung des Typs

$$V^2 = U^3 + aU + b \qquad \text{mit } a, b \in \mathbb{Q} \tag{2}$$

festgelegt wird, wobei das Polynom in U rechts ohne mehrfache Nullstelle ist. Daher war Gleichung 4(1) bei $k \neq 0$ ein sehr typisches Beispiel einer algebraischen Kurve vom Geschlecht Eins.

Die Punkte der durch (2) festgelegten Kurve lassen sich, wie bereits erwähnt, zwar nicht mehr rational parametrisieren; dafür ist jedoch eine Parameterdarstellung mit Hilfe meromorpher transzendenter Funktionen möglich, am einfachsten mittels der WEIERSTRASSschen elliptischen $\wp$–Funktion und deren Ableitung. Daher nennt man generell algebraische Kurven vom Geschlecht Eins *elliptisch*; bei Geschlecht größer als Eins haben sich Sonderbezeichnungen nicht eingebürgert, während man bei Geschlecht Null heute von *rationalen* Kurven spricht.

Über elliptische Kurven hatte POINCARE (indirekt) die Vermutung ausgesprochen, daß man ihre sämtlichen rationalen Punkte stets aus endlich vielen unter ihnen durch sukzessive Anwendung der Sekanten– und Tangentenmethode konstruieren kann. Diese Vermutung wurde von MORDELL 1922 mit der bereits in Bemerkung 1 zu 4 angesprochenen Deszendenzmethode bewiesen.

In derselben Arbeit sprach MORDELL seinerseits die Vermutung aus, daß jede algebraische, nicht rationale oder elliptische Kurve höchstens endlich viele rationale Punkte hat. Dies konnte 1983 von G. FALTINGS gezeigt werden, der für seine diesbezüglichen (wesentlich weitergehenden) Untersuchungen auf dem Internationalen Mathematiker–Kongreß in Berkeley 1986 eine FIELDS–Medaille erhielt.

Bemerkungen. 1) JACOBI hatte schon 1834 das EULERsche Additionstheorem für elliptische Integrale zur Definition einer "Addition" von Punkten einer elliptischen Kurve herangezogen. Aber erst POINCARE hat erkannt, daß der JACOBIsche analytische Ansatz aufs engste mit der geometrischen Sekanten–Tangenten–Methode des DIOPHANT zusammenhängt. Für genauere Details hierzu muß der interessierte Leser etwa auf S.LANG (*Elliptic Functions*, Addison-Wesley, Reading etc., 1973) verwiesen werden.

2) Daß jede algebraische, nicht rationale Kurve höchstens endlich viele *ganzzahlige* Punkte hat, wurde bereits 1929 von C.L. SIEGEL gezeigt.

6. Pythagoräische Dreiecke quadratischer Kathetenlängen. Hier wird ein Resultat über pythagoräische Dreiecke gewonnen, dessen Beweis methodisch etwas Neues bringen wird.

Proposition. *Es gibt keine pythagoräischen Dreiecke, deren beide Katheten Längen haben, die Quadratzahlen sind.*

Dies ist eine unmittelbare Folgerung aus dem nachstehenden, auf EULER (1738) zurückgehenden

Satz. *Die diophantische Gleichung*

$$X^4 + Y^4 = Z^2 \tag{1}$$

ist nichttrivial unlösbar.

Dies bedeutet, daß es kein (1) genügendes Tripel $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$ gibt. Als weitere Konsequenz dieses Satzes sei angeführt das

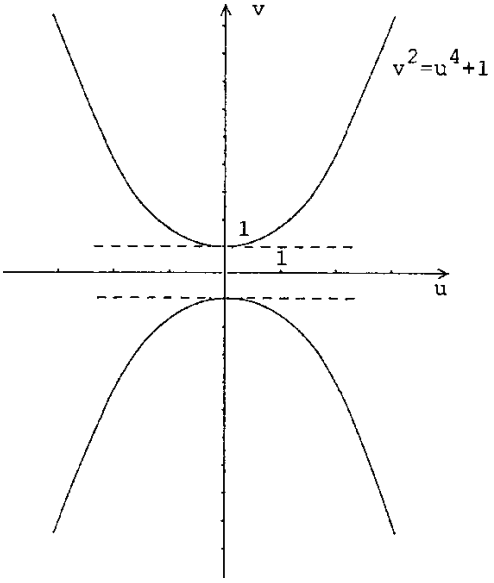
Korollar. *Die einzigen rationalen Punkte der elliptischen Kurve*

$$V^2 = U^4 + 1 \tag{2}$$

sind $(0, 1)$ *und* $(0, -1)$.

Beweis. Wäre nämlich $(u, v) \in \mathbb{Q}^2$ mit $u \neq 0$ ein Punkt auf der durch (2) definierten algebraischen Kurve vom Geschlecht Eins, so sei $y \in \mathbb{N}$ so gewählt, daß $x := uy$ und $z := vy$ ganz sind. Offenbar löst (x, y, z) dann (1) nichttrivial, denn $uv \neq 0$ impliziert $xyz \neq 0$. □

Bemerkung. Daß weder mittels Sekanten– noch Tangentenmethode aus den beiden rationalen Punkten $(0, 1)$, $(0, -1)$ von (2) neue rationale Punkte zu erhalten sind, lehrt ein Blick auf die nachstehende Skizze.



Beweis des Satzes. Es werde angenommen, Gleichung (1) sei nichttrivial lösbar und $(x_0, y_0, z_0) \in \mathbb{Z}^3$ sei eine ihrer Lösungen mit $x_0 y_0 z_0 \neq 0$. Da alle Exponenten in (1) gerade sind, sind gleichzeitig alle acht Tripel $(\pm x_0, \pm y_0, \pm z_0)$

nichttriviale Lösungen von (1) und genau eines dieser Tripel hat lauter positive Komponenten. O.B.d.A. darf $x_0, y_0, z_0 \in \mathbb{N}$ vorausgesetzt werden. Ziel ist nun die Konstruktion einer weiteren nichttrivialen Lösung (x_1, y_1, z_1) von (1) in natürlichen Zahlen mit $z_1 < z_0$.

Ist die Lösung (x_0, y_0, z_0) nicht primitiv, so sei p eine alle Komponenten teilende Primzahl. Mit $\hat{x}_0 := x_0/p$, $\hat{y}_0 := y_0/p$, $\hat{z}_0 := z_0/p$ erhält man $p^2(\hat{x}_0^4 + \hat{y}_0^4) = \hat{z}_0^2$, woraus man $p|\hat{z}_0$ sieht. Offenbar ist $(x_1, y_1, z_1) := (\hat{x}_0, \hat{y}_0, \hat{z}_0/p)$ eine nichttriviale Lösung von (1) in natürlichen Zahlen mit $z_1 = \hat{z}_0/p = z_0/p^2 < z_0$.

Ist die ursprüngliche Lösung (x_0, y_0, z_0) von (1) jedoch primitiv, so ist $(x_0^2, y_0^2, z_0) \in \mathbb{N}^3$ wegen (1) ein primitives pythagoräisches Tripel. Nach den Überlegungen am Ende von 1 ist genau eine der Zahlen x_0, y_0 gerade und o.B.d.A. sei dies y_0. Nach EUKLIDs Satz 2 gilt dann mit teilerfremden $a, b \in \mathbb{N}$, $a > b$ und ungerader Summe $a + b$

$$x_0^2 = a^2 - b^2, \qquad y_0^2 = 2ab, \qquad z_0 = a^2 + b^2.$$

Bei geradem a wäre b ungerade, also $x_0^2 \equiv 3 \pmod 4$, was nicht geht. So ist a ungerade und b gerade sowie $x_0^2 + b^2 = a^2$. Daher ist (x_0, b, a) ein primitives pythagoräisches Tripel mit gerader Mittelkomponente und erneut liefert EUKLIDs Satz

$$x_0 = c^2 - d^2, \qquad b = 2cd, \qquad a = c^2 + d^2$$

mit teilerfremden $c, d \in \mathbb{N}$, $c > d$, $2 \nmid (c + d)$. Da a und b teilerfremd sind, sind $c, d, c^2 + d^2$ sogar paarweise teilerfremd. Wegen $(\frac{1}{2} y_0)^2 = cd(c^2 + d^2)$ und Lemma 2 ergibt sich daraus

$$c = x_1^2, \qquad d = y_1^2, \qquad c^2 + d^2 = z_1^2$$

mit (paarweise teilerfremden) $x_1, y_1, z_1 \in \mathbb{N}$, die offenbar $x_1^4 + y_1^4 = z_1^2$ und wegen $z_1 \leq z_1^2 = c^2 + d^2 = a < a^2 < a^2 + b^2 = z_0$ auch $z_1 < z_0$ erfüllen. Damit ist in jedem Fall das oben gesteckte Ziel erreicht.

Die Annahme der Existenz einer nichttrivialen Lösung (x_0, y_0, z_0) von (1) in natürlichen Zahlen führt somit zur Konstruktion einer unendlichen Folge

$$((x_k, y_k, z_k))_{k=0,1,\ldots}$$

nichttrivialer Lösungen von (1) in natürlichen Zahlen, die überdies der Bedingung $z_0 > z_1 > \ldots > z_k > \ldots > 0$ genügen, welch letzteres unmöglich ist. □

7. Fermats Vermutung. In seinem Exemplar von BACHETs bereits in 4 erwähnter Übersetzung von DIOPHANTs *Arithmetika* fand man folgende Bemerkung von FERMAT aus der Zeit zwischen 1631 und 1637 als Randnotiz neben

Problem 8 ("Ein gegebenes Quadrat soll in eine Summe zweier Quadrate zerlegt werden") des zweiten Buches:

"Cubum in duos cubos aut quadrato-quadratum in duos quadrato-quadratos et generaliter nullam in infinitum, ultra quadratum, potestam in duas ejusdem nominis fas est dividere.

Cujus rei demonstrationem mirabilem sane detexi, hanc marginis exiguitas non caperet."

Diese FERMATsche Bemerkung läuft also darauf hinaus, daß die diophantische Gleichung

$$X^n + Y^n = Z^n \tag{1}$$

für kein natürliches $n \geq 3$ nichttrivial lösbar ist, d.h. daß es kein (1) genügendes Tripel $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$ gibt. Leider hinterließ FERMAT seiner Nachwelt den "fürwahr wunderbaren Beweis dieser Tatsache", den er "entdeckt hatte", nicht, da "der schmale Rand diesen nicht fassen würde".

FERMATs Randnotiz ging in die spätere Literatur als FERMAT*sche Vermutung* ein; manche Autoren sprechen auch vom *großen* FERMAT*schen Satz* (in der englisch–sprachigen Literatur praktisch ausschließlich FERMAT*'s last theorem*) in Abgrenzung zum "kleinen" FERMATschen Satz, der in 2.3.3 diskutiert wurde.

In einem Brief an P. DE CARCAVI (1659) hat FERMAT eine neue Methode ausführlich beschrieben, mit der er seine eigene Randnotiz neben Problem 20 im sechsten Buch von DIOPHANTs *Arithmetika* beweisen konnte, daß es nämlich kein pythagoräisches Dreieck geben würde, dessen Fläche eine Quadratzahl sei. Offenbar ist diese Behauptung mit der nichttrivialen Unlösbarkeit der Gleichung

$$X^4 - Y^4 = Z^2 \tag{2}$$

äquivalent. FERMAT vermerkt in seinem Brief: "Da die Methoden in der Literatur für den Beweis so schwieriger Sätze nicht ausreichen, fand ich schließlich einen ganz und gar einzigartigen Weg. Ich nannte diese Beweismethode *la descente infinie* ..."

Diese Schlußweise, mit der im vorigen Abschnitt die nichttriviale Unlösbarkeit von 6(1) gezeigt wurde, ist heute als FERMATsche *Deszendenzmethode* bekannt und für die Untersuchung zahlreicher Fragen über diophantische Gleichungen unersetzlich. Wie am Ende von 6 gesehen, beruht sie einfach auf dem in 1.1.1 erwähnten Prinzip des kleinsten Elements.

Sowohl aus dem FERMATschen Resultat über (2) wie aus dem EULERschen über 6(1) erhält man die folgende

Proposition A. *Die* FERMAT*–Gleichung (1) zum Exponenten $n > 0$ ist unlösbar, falls n Vielfaches von 4 ist.*

Bemerkung. "Lösbar" bzw. "unlösbar" bedeutet für den Rest dieses Paragraphen stets "nichttrivial lösbar" bzw. "nichttrivial unlösbar".

Beweis. Es sei $n = 4m$ mit einem $m \in \mathbb{N}$ und es werde angenommen, (1) habe für solche n eine nichttriviale Lösung (x, y, z). Ersichtlich wäre dann (x^m, y^m, z^{2m}) eine nichttriviale Lösung von 6(1) entgegen dem EULERschen Satz 6. □

Folgende leichte Reduktion der FERMAT–Vermutung kann noch vorgenommen werden:

Proposition B. *Zum Beweis der* FERMAT*schen Vermutung reicht es, die Unlösbarkeit der* FERMAT*–Gleichung (1) für jeden Exponenten zu zeigen, der eine ungerade Primzahl ist.*

Beweis. Sei $n \geq 3$ eine natürliche Zahl. Der Fall $4|n$ wurde bereits durch Proposition A erledigt. Ist n nicht Vielfaches von 4, so wird es von mindestens einer ungeraden Primzahl p geteilt und mit $m := n/p$ kann gesagt werden: Löst (x_0, y_0, z_0) die FERMAT–Gleichung (1) zum Exponenten n, so löst (x_0^m, y_0^m, z_0^m) die FERMAT–Gleichung zum Exponenten p. □

8. Weitere Entwicklung des Fermat–Problems (bis 1993). Die Unlösbarkeit der FERMAT-Gleichung

$$X^p + Y^p = Z^p \tag{1}$$

für die Primzahl $p = 3$ wurde zwischen 1753 und 1770 von EULER gezeigt und 1770 publiziert (vgl. *Vollständige Anleitung zur Algebra* = Opera Omnia, Ser. 1, I, 1–498, hier insbesondere 484–489). Eine kleine Lücke in seinem Beweis konnte LEGENDRE 1830 schließen. Den Exponenten $p = 5$ haben dann unabhängig voneinander zwischen 1825 und 1828 DIRICHLET und LEGENDRE erledigt.

Daß zunächst die beiden kleinsten ungeraden Primzahlen behandelt werden konnten, hat algebraisch–arithmetische Gründe: Der Satz über die eindeutige Primfaktorzerlegung (vgl. 1.1.5) im Unterring $\mathbb{Z}$ der ganzen Zahlen des Körpers $\mathbb{Q}$ spielte mehr oder weniger explizit (vgl. etwa Beweis von Lemma 2) bei der Behandlung der FERMAT–Gleichung zu den Exponenten 2 bzw. 4 (vgl. die Sätze 2 bzw. 6) eine entscheidende Rolle. Wie in 1.5.5–6 gesehen, hat man analog im Unterring der ganzen Zahlen der quadratischen Zahlkörper $\mathbb{Q}(\sqrt{-3})$

und $\mathbb{Q}(\sqrt{5})$ den Satz von der eindeutigen Zerlegbarkeit in Primelemente, da hier die genannten Unterringe euklidisch sind (vgl. Satz 1.6.9).

Um 1843 herum soll E.E. KUMMER eine Arbeit an DIRICHLET eingereicht haben, in der vermeintlich die Unlösbarkeit von (1) für jede Primzahl $p > 2$ und damit nach Proposition 7B die Richtigkeit der FERMATschen Vermutung bewiesen wurde. DIRICHLET fand aber bei der Durchsicht, daß KUMMER bei seinem "Beweis" den Satz von der eindeutigen Primelementzerlegung im Ring der ganzen Zahlen gewisser vom jeweils betrachteten p abhängigen algebraischen Zahlkörper als gültig hingenommen hatte. So jedenfalls soll diese Geschichte nach einer Erzählung von HENSEL (1910), der einzigen Quelle, abgelaufen sein; man vergleiche dazu H.M. EDWARDS [3], Kap.4.1. Fest steht jedenfalls, daß sich KUMMER seit jener Zeit intensiv dem Studium der Teilbarkeitsgesetze in speziellen algebraischen Zahlkörpern, den sogenannten Kreisteilungskörpern, widmete. Obwohl es KUMMER trotz aller Bemühungen nicht gelungen ist, die Unlösbarkeit von (1) für alle Primzahlen $p > 2$ zu beweisen, hat er überaus wichtige Ergebnisse zum FERMAT–Problem erzielt und der späteren Entwicklung entscheidende Impulse gegeben.

KUMMER selbst hat gegen 1850 beweisen können, daß (1) für alle sogenannten *regulären* Primzahlen p unlösbar ist. Seine ursprüngliche Regularitätsdefinition verlangt für eine Reproduktion an dieser Stelle zu viele algebraische Vorkenntnisse. Er zeigte aber, daß eine Primzahl $p > 2$ genau dann regulär ist, wenn p keinen Zähler der (rationalen) BERNOULLI–Zahlen $B_2, B_4, \ldots, B_{p-3}$ (in ihrer gekürzten Darstellung) teilt. Dabei sind die BERNOULLI–Zahlen über die im Kreis $|z| < 2\pi$ der komplexen Ebene konvergente TAYLOR–Entwicklung der Funktion $\frac{z}{e^z-1}$ gemäß

$$\frac{z}{e^z-1} = \sum_{k=0}^{\infty} B_k \frac{z^k}{k!}$$

definiert. Als k–te Ableitung von $\frac{z}{e^z-1}$ an der Stelle 0 ist B_k rational; insbesondere gilt $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$, $B_{14} = \frac{7}{6}$, $B_{16} = -\frac{3617}{510}$ und $B_k = 0$ für alle ungeraden $k \geq 3$.

Wendet man dieses KUMMERsche Kriterium an, so erkennt man die Regularität der Primzahlen 3, 5, 7, 11, 13, 17 und 19. Unterhalb 100 sind lediglich die Primzahlen 37, 59 und 67 nicht regulär (kurz: *irregulär*). Seit KUMMER vermutet man, daß es unendlich viele reguläre Primzahlen gibt, ein Problem, das bis heute offen ist. Dagegen weiß man seit K.L. JENSEN (1915), daß es unendlich viele irreguläre Primzahlen gibt.

Über das oben zitierte KUMMER–Kriterium via BERNOULLI–Zahlen hinaus sind heute zahlreiche Ergebnisse bekannt, die die Entscheidung, ob (1) für ein $p > 2$ lösbar ist, mit anderen, mehr oder weniger leicht nachprüfbaren Eigenschaften

von p in Zusammenhang bringen. Mit derartigen Kriterien ist es J. BUHLER, R. CRANDALL, R. ERNVALL und T. METSÄNKYLÄ (Math. Comp. *61*, 151–153 (1993)) gelungen, unter Computereinsatz zu zeigen, daß (1) für alle ungeraden Primzahlen $p < 4 \cdot 10^6$ unlösbar ist.

Bemerkungen. 1) Nach der anfangs von 3 beschriebenen Vorgehensweise ist klar, daß sich Lösungen $(x, y, z) \in \mathbb{Z}^3$ mit $z \neq 0$ der FERMAT–Gleichung 7(1) und rationale Punkte (u, v) der durch

$$V^n = 1 - U^n \tag{4}$$

definierten algebraischen Kurve gegenseitig entsprechen. Nach 5(1) ist die "FERMAT–Kurve" (4) vom Geschlecht $\frac{1}{2}(n-1)(n-2)$, also im Fall $n = 3$ elliptisch. Es ist nun ganz leicht nachzurechnen, daß (4) für $n = 3$ und 4(1) für $k = -432$, also $Y^2 = X^3 - 432$, in dem in 4 erklärten Sinne birational äquivalent sind. Dazu zeigt man, daß die Transformationen $U = (Y - 36)/(Y + 36)$, $V = 3X/(Y + 36)$ bzw. $X = 12V/(1-U)$, $Y = 36(1+U)/(1-U)$ die Übergänge von der einen zur anderen Gleichung vermitteln. Nun klärt sich auch auf, wieso Gleichung 4(1) für $k = -432$ lediglich zwei rationale Lösungen hat, vgl. Bemerkung 1 zu 4.

2) Da die FERMAT–Kurve (4) für $n \geq 4$ ein Geschlecht größer als Eins hat, liefert der Satz von FALTINGS am Schluß von 5 die Endlichkeit der Anzahl ihrer rationalen Punkte. Anders ausgedrückt: Für jedes $n \geq 4$ ist die Anzahl der primitiven Lösungen $(x, y, z) \in \mathbb{Z}^3$ der FERMAT–Gleichung 7(1) endlich.

3) Dem Leser, der sich über Entwicklung und Stand bis 1919 des FERMAT–Problems genauer informieren möchte, sei das Buch von P. BACHMANN (*Das Fermatproblem in seiner bisherigen Entwicklung* (Nachdruck), Springer, Berlin etc., 1976) genannt. Dieses enthält eine hervorragende Übersicht über alle wichtigen Resultate zur FERMAT–Vermutung, die bis zum Erscheinungsjahr 1919 der Originalausgabe gefunden wurden. Aus der neueren Literatur seien die beiden Werke von EDWARDS [3] und P. RIBENBOIM [23] besonders empfohlen.

9. Lösung des Fermat–Problems. Auf einer kleineren Spezialtagung über algebraische Zahlentheorie in Cambridge (England) hielt A. WILES am 21., 22. und 23. Juni 1993 drei zusammenhängende Vorträge über "Modular forms, elliptic curves and GALOIS representations". Nichts im Titel deutete auf Querverbindungen zum FERMAT–Problem hin. Am Ende seines dritten Vortrags schrieb WILES als Folgerung aus wesentlich allgemeineren Sätzen ein *quod erat demonstrandum* hinter den FERMATschen Satz. Stunden später verbreitete sich bereits die Nachricht von diesem Ereignis durch Faxe und Electronic Mails über die ganze mathematische Welt. Schon am 24. Juni berichtete "The New York Times" auf Seite 1 über diese Sensation. Was war geschehen?

Die Vorarbeiten, die schlußendlich zum Erfolg führten, begannen 1955, als Y. TANIYAMA eine (hier nicht wiederzugebende) Vermutung elliptische Kurven über $\mathbb{Q}$ betreffend formulierte, die wenige Jahre später durch Forschungen von G. SHIMURA und A. WEIL weiter präzisiert wurde. Aber fast drei Jahrzehnte lang ahnte niemand, daß diese Dinge irgendwie mit dem FERMAT–Problem zu tun haben könnten. Erst 1986 stellte G. FREY eine überraschende Beziehung zwischen diesem Problem und der SHIMURA–TANIYAMA–WEIL–Vermutung her und 1987 konnte K. RIBET beweisen, daß aus der Richtigkeit der SHIMURA–TANIYAMA–WEIL–Vermutung diejenige der FERMAT-Vermutung folgt. Seit Bekanntwerden dieses Zusammenhangs hat WILES an einem Beweis der SHIMURA–TANIYAMA–WEIL–Vermutung gearbeitet, wenigstens für elliptische Kurven speziellen Typs, die auch schon für die FERMAT–Vermutung ausreichen würden.

Nach der großen Sensation im Juni 1993 gab es bereits zwei Monate später erste Gerüchte und Spekulationen über Lücken im noch nicht publizierten Beweis von WILES: Nachdem sich sogar die Weltpresse (z.B. "Le Monde" vom 2. Dezember 1993:"Le théorème de FERMAT fait de la résistance") dieser Schwierigkeiten annahm, wandte sich WILES selbst am 4. Dezember 1993 mit einem e–mail an die mathematische Öffentlichkeit: "However the final calculation ... is not yet complete as it stands. I believe that I will be able to finish this in the near future using the ideas explained in my Cambridge lectures."

Während der ersten Hälfte des Jahres 1994 flossen die Neuigkeiten zum FERMAT–Problem dann relativ spärlich. Es war aber nur natürlich, daß WILES zu einem Hauptvortrag auf dem Züricher Internationalen Mathematiker–Kongreß im August desselben Jahres eingeladen wurde. Der Titel seines Vortrags, des letzten des gesamten Kongresses, ließ alle Möglichkeiten offen. Tatsächlich stellte er dort unmißverständlich klar, was er bis dato zeigen konnte, daß jedoch die hartnäckigste Lücke in seinem Beweis noch immer nicht geschlossen sei.

Nur wenige Wochen später, am 25. Oktober 1994, machte WILES dann zwei Manuskripte der Fachwelt zugänglich, in denen die oben angesprochene Lücke zwar nicht beseitigt, wohl aber unter Mithilfe seines Schülers R. TAYLOR unter Rückgriff auf einen früheren Ansatz umgangen wurde. Die beiden hier angesprochenen Arbeiten von WILES bzw. TAYLOR und WILES sind in Ann. Math. (2) *142*, 443–551 bzw. 553–572 (1995) publiziert. Zusammengenommen enthalten sie weit mehr als einen von den führenden Spezialisten inzwischen als stichhaltig akzeptierten Beweis der FERMAT–Vermutung, nämlich einen Beweis der SHIMURA–TANIYAMA–WEIL–Vermutung für sogenannte semistabile elliptische Kurven über $\mathbb{Q}$.

Nach Lösung des über 350 Jahre alten FERMAT–Problems, mit dem so viele Generationen hervorragender Zahlentheoretiker vergeblich gerungen haben, ist es verständlich, daß ein breiteres mathematisches Publikum den Wunsch hat,

sich die grundlegenden Ideen der Beweisführung nicht mühsam aus den 130 Seiten der beiden Originalarbeiten herausholen zu müssen, sondern sich in kurzen Übersichtsartikeln informieren zu können. Als solche seien z.B. die vorzüglichen Aufsätze von FALTINGS (DMV– Mitteilungen 2/1995, S. 6–8) und WILES (Proc. ICM Zürich 1994, Vol. 1, Birkhäuser, Basel–Boston–Berlin, 1995, pp. 243–245) genannt.

§ 3. Die Pellsche Gleichung und Verwandtes

1. Problemstellung. Als PELLsche Gleichung bezeichnet man die diophantische Gleichung in zwei Unbestimmten

$$X^2 - dY^2 = 1, \tag{1}$$

wobei $d \neq 0$ als fest vorgegebene ganze Zahl gedacht ist. Offenbar sind $(1, 0)$ und $(-1, 0)$ stets Lösungen von (1) – man bezeichnet sie als die *trivialen Lösungen* von (1) – und bei $d \leq -2$ gibt es auch keine weiteren. Bei $d = -1$ kommen zu den beiden trivialen noch die beiden Lösungen $(0, 1)$, $(0, -1)$ hinzu.

Recht uninteressant ist weiterhin der Fall eines quadratischen d: Ist nämlich $d = e^2$ mit ganzem $e \neq 0$, so löst $(x, y) \in \mathbb{Z}^2$ Gleichung (1) genau dann, wenn $(x + ey)(x - ey) = 1$ gilt, d.h. wenn gleichzeitig entweder $x + ey = 1$, $x - ey = 1$ oder $x + ey = -1$, $x - ey = -1$ gelten. Unschwer erkennt man hieraus, daß (1) im Falle eines quadratischen $d \neq 0$ alleine die beiden trivialen Lösungen hat.

Zurück bleibt somit das *Problem, die Lösbarkeit der* PELL*schen Gleichung* (1) *bei* $d \in \mathbb{N}$, d *kein Quadrat, zu untersuchen.* In dieser Allgemeinheit scheint das Problem von FERMAT gestellt worden zu sein, der 1657 in einem Brief an FRENICLE behauptete, (1) habe unter den soeben angegebenen Bedingungen an d stets unendlich viele ganzzahlige Lösungen (x, y). Nach einer Bemerkung EULERS ist diese Frage wohl zuerst von J. PELL im 17. Jahrhundert mit einigem Erfolg angegriffen worden. Es gibt jedoch auch Mathematikhistoriker, die einen wirklichen Beitrag PELLS zur Theorie der Gleichung (1) bezweifeln. Fest steht, daß erst LAGRANGE um 1766 die volle Lösung des Problems gelang, indem er zeigte, daß (1) unter den über d zuletzt gemachten Voraussetzungen unendlich viele Lösungen besitzt, und indem er überdies die Struktur dieser Lösungsgesamtheit vollständig aufklärte. Der Darstellung der genannten LAGRANGEschen Resultate sind die Abschnitte 3 und 4 gewidmet.

Schließlich sei noch angemerkt, daß historisch die Beschäftigung mit der Gleichung (1) für spezielle, kleine d etwa bis 400 v. Chr. zurückreicht. Um diese Zeit tauchten in Indien und Griechenland rationale Näherungen $\frac{x}{y}$ für $\sqrt{2}$ auf, deren Zähler und Nenner der Gleichung (1) für $d = 2$ genügen, etwa $\frac{17}{12}$ und $\frac{577}{408}$.

Bei EUKLID (*Elemente* II, § 10) findet sich im Prinzip – allerdings geometrisch eingekleidet – ein rekursives Verfahren zur Bestimmung sämtlicher Lösungen von (1) bei $d = 2$ in natürlichen Zahlen.

Die bedeutenden griechischen Mathematiker der alexandrinischen Zeit (ca. 300 – 200 v. Chr.) wagten sich gelegentlich auch für große d–Werte an Gleichung (1) heran. So soll ARCHIMEDES dem ERATOSTHENES das berühmte "Rinderproblem" gestellt haben, in dem unter einer ganzen Reihe von Nebenbedingungen Anzahlen verschiedenfarbiger Kühe und Stiere gesucht waren (vgl. DICKSON [*G* 2] II, S. 342ff.). Immerhin lief dieses Problem auf die Bestimmung nichttrivialer Lösungen von (1) für $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 = 4\,729\,494$ hinaus. Übrigens hat dieses Rinderproblem den Dichter G.E. LESSING (1773) zu einem griechischen Epigramm in 24 Versen angeregt.

2. Der Dirichletsche Approximationssatz. Wie in 1 erwähnt, wurden in der Antike Lösungen der PELLschen Gleichung 1(1) in natürlichen Zahlen zur Berechnung guter rationaler Annäherungen an gewisse quadratische Irrationalitäten wie $\sqrt{2}$ benutzt. Um die in 1 in Aussicht gestellten LAGRANGEschen Ergebnisse zu erhalten, stellt man heute meist umgekehrt ein Resultat über die Approximation von $\sqrt{d}$ durch rationale Zahlen an den Anfang und gewinnt hieraus dann sämtliche Lösungen der PELLschen Gleichung. Dieser Weg wird auch hier beschritten.

Die benötigte Approximationsaussage entnimmt man dabei dem

Dirichletschen Approximationssatz. *Sei $\alpha \in \mathbb{R}$, $\omega \in \mathbb{N}$, $\omega \geq 2$. Dann existieren $p, q \in \mathbb{Z}$ mit $1 \leq q < \omega$ und $|\alpha q - p| \leq \frac{1}{\omega}$. Ist α irrational, so existieren unendlich viele verschiedene teilerfremde $p, q \in \mathbb{Z}$, $q > 0$, für die $|\alpha q - p| < \frac{1}{q}$ gilt.*

Beweis. Für den ersten Teil des Satzes betrachte man die $\omega + 1$ im Einheitsintervall $[0, 1]$ gelegenen Zahlen 1 und*) $\{\alpha x\}$ mit $x \in \{0, \ldots, \omega - 1\}$ und die ω Teilintervalle $[\frac{j-1}{\omega}, \frac{j}{\omega}]$, $j = 1, \ldots, \omega$, von $[0, 1]$ der Länge $\frac{1}{\omega}$. Es existiert mindestens ein derartiges Teilintervall, in das wenigstens zwei der $\omega + 1$ oben genannten Zahlen fallen. Sind dies zwei Zahlen des Typs $\{\alpha x\}$, etwa $\{\alpha x_1\}$ und $\{\alpha x_2\}$, wobei o.B.d.A. $x_1 < x_2$ gelten möge, so setzt man $q := x_2 - x_1$, $p := [\alpha x_2] - [\alpha x_1]$ und hat damit alle Forderungen erfüllt. Fallen jedoch 1 und eine Zahl des Typs $\{\alpha x\}$ ins gleiche Teilintervall, so ist $x > 0$, da die Zahl 0

*) Für reelles z wird $\{z\} := z - [z]$ gesetzt; $\{z\}$ heißt der *gebrochene Teil* von z. Weiter bedeutet $\|z\| := \mathrm{Min}(\{z\}, 1 - \{z\})$ den Abstand von z zur nächstgelegenen ganzen Zahl.

wegen $\omega \geq 2$ nicht in diesem Teilintervall liegen kann. In diesem Fall setzt man $q := x$, $p := [\alpha x]+1$ und hat damit erneut alle Forderungen für die erste Aussage im Approximationssatz erfüllt.

Zu jedem $\omega = 2, 3, \ldots$ existiert also ein Paar $(p(\omega), q(\omega)) \in \mathbb{Z} \times \mathbb{N}$ mit

$$|\alpha q(\omega) - p(\omega)| \leq \frac{1}{\omega}, \qquad q(\omega) < \omega; \tag{1}$$

dabei dürfen $p(\omega)$, $q(\omega)$ offenbar als teilerfremd vorausgesetzt werden. Kämen nun unter den Paaren $(p(\omega), q(\omega))$, $\omega = 2, 3, \ldots$, nur endlich viele verschiedene vor, so gäbe es ein $(p_0, q_0) \in \mathbb{Z} \times \mathbb{N}$ mit $p(\omega) = p_0$, $q(\omega) = q_0$ für unendlich viele ω und für diese ω müßte $|\alpha q_0 - p_0| \leq \frac{1}{\omega}$ nach (1) gelten, woraus mit $\alpha = p_0/q_0$ die Rationalität von α folgen würde entgegen der Zusatzvoraussetzung für den zweiten Teil des Satzes. Aus (1) folgt $|\alpha q(\omega) - p(\omega)| < 1/q(\omega)$ für $\omega = 2, 3, \ldots$ und somit ist auch der zweite Teil bewiesen. □

Bemerkungen. 1) DIRICHLET (Werke I, 635–638) hat ursprünglich einen wesentlich allgemeineren, sich auf simultane Approximationen beziehenden Satz angegeben.

2) Der zweite Teil des DIRICHLETschen Approximationssatzes kann ergänzt werden zu einem notwendigen und hinreichenden

Irrationalitätskriterium. *Eine reelle Zahl α ist genau dann irrational, wenn die Ungleichung $|\alpha q - p| < 1/q$ unendlich viele verschiedene teilerfremde Lösungen $(p, q) \in \mathbb{Z} \times \mathbb{N}$ besitzt.*

Beweis. Ist α irrational, so ist bereits alles erledigt; diesen Teil erhält man übrigens auch mittels Kettenbruchtheorie, vgl. den Beginn von 5.3.6. Sei umgekehrt α rational, etwa $\alpha = a/b$ mit teilerfremden $a, b \in \mathbb{Z}$, $b > 0$. Die Ungleichung im Kriterium ist dann mit $|qa - pb| < b/q$ gleichbedeutend. Hier verschwindet die linke Seite für teilerfremde $p, q \in \mathbb{Z}$, $q > 0$ genau für $p = a$, $q = b$ und so folgt aus der letzten Ungleichung bei $(p, q) \neq (a, b)$ direkt $q < b$ und daraus $|p| < 1 + |a|$. Bei rationalem α hat die Ungleichung im Kriterium also nur endlich viele teilerfremde Lösungen (p, q). □

3) *Aus dem ersten Teil des* DIRICHLET*schen Approximationssatzes folgt* THUES *Lemma* (vgl. 1.2) *ohne nochmalige Verwendung des Schubfachprinzips:*

Man wendet den Approximationssatz nämlich an mit $\alpha := \ell/m$, $\omega := v$ (wegen $0 < u \leq m < uv$ ist $1 < v$); somit gibt es ganze p, q mit $1 \leq q < v$ und $|q\ell - pm| \leq m/v < u$. Sicher ist $q\ell \neq pm$, da sonst $m|q$ wegen $(\ell, m) = 1$ gelten müßte; dann wäre aber $m \leq q < v \leq m$, was nicht geht. Nun leisten $x := |q\ell - pm|$, $y := q$ das in THUES Lemma Gewünschte: Da $y\ell - pm$ entweder x oder $-x$ ist, ist auch $\pm x \equiv \ell y \pmod{m}$ klar. □

Diese Bemerkung macht verständlich, wieso gelegentlich (vgl. etwa HARDY–WRIGHT [6]) der DIRICHLETsche Approximationssatz zum Beweis von Satz 1.1 verwandt wird.

3. Unendlich viele Lösungen der Pell–Gleichung. Wie bereits in 1 in Aussicht gestellt, soll nun bewiesen werden der

Satz. *Ist $d \in \mathbb{N}$ kein Quadrat, so hat die* PELLsche *Gleichung*

$$X^2 - dY^2 = 1 \tag{1}$$

unendlich viele Lösungen.

Beweis. Man setzt $\alpha := \sqrt{d}$ und bemerkt zunächst, daß dies α nach Korollar 1.1.9 irrational ist. Nach dem zweiten Teil des DIRICHLETschen Approximationssatzes gibt es unendlich viele verschiedene $(x, y) \in \mathbb{Z} \times \mathbb{N}$ mit teilerfremden x, y und

$$|x - \alpha y| < \frac{1}{y}. \tag{2}$$

Übrigens sind hier auch die x positiv; denn bei $x \leq 0$ wäre (2) zu $(|x| + \alpha y)y < 1$ äquivalent und die letztere Ungleichung ist ersichtlich unmöglich. Offenbar gilt für diese (x, y) weiterhin

$$0 < |x^2 - dy^2| = |x - \alpha y|(x + \alpha y) < \frac{x}{y} + \alpha < 2\alpha + 1. \tag{3}$$

Denn aus (2) ist $\frac{x}{y} < \alpha + y^{-2} \leq \alpha + 1$ sofort klar und $x^2 = dy^2$ ist unmöglich. Wegen (3) gibt es ein ganzes k mit $0 < |k| < 2\alpha + 1$, so daß für unendlich viele verschiedene (x, y) wie oben die Gleichung

$$x^2 - dy^2 = k \tag{4}$$

erfüllt ist. Nach dem DIRICHLETschen Schubfachprinzip 2.3.1 gibt es $\xi, \eta \in \{0, \ldots, |k| - 1\}$, so daß gleichzeitig

$$x \equiv \xi, \quad y \equiv \eta \pmod{k} \tag{5}$$

für unendlich viele der (4) genügenden $(x, y) \in \mathbb{N}^2$ gilt. Seien (x_1, y_1), (x_2, y_2) zwei verschiedene solche Paare; damit gewinnt man

$$(x_1 - \alpha y_1)(x_2 + \alpha y_2) = (x_1 x_2 - d y_1 y_2) + \alpha(x_1 y_2 - x_2 y_1) \tag{6}$$

und wegen (4) und (5)

$$x_1x_2 - dy_1y_2 \equiv \xi^2 - d\eta^2 \equiv 0, \quad x_1y_2 - x_2y_1 \equiv 0 \pmod{k}.$$

Definiert man im Anschluß hieran $u, v \in \mathbb{Z}$ vermöge

$$ku := x_1x_2 - dy_1y_2, \quad kv := x_1y_2 - x_2y_1,$$

so wird (6) zu

$$(x_1 - \alpha y_1)(x_2 + \alpha y_2) = k(u + \alpha v) \tag{6'}$$

und analog gilt

$$(x_1 + \alpha y_1)(x_2 - \alpha y_2) = k(u - \alpha v). \tag{6''}$$

Da (x_1, y_1) und (x_2, y_2) beide (4) erfüllen, liefert Multiplikation von (6′) und (6″) und anschließende Division durch k^2 die Gleichung

$$u^2 - dv^2 = 1. \tag{7}$$

Sicher ist hier $uv \neq 0$; denn $v = 0$ hieße $x_1y_2 = x_2y_1$ und Positivität sowie Teilerfremdheit der x_i, y_i würde $x_2 = x_1$, $y_2 = y_1$ implizieren entgegen der vorausgesetzten Verschiedenheit von (x_1, y_1) und (x_2, y_2). Für genau eines der vier Paare $(\pm u, \pm v)$ sind beide Komponenten positiv und wegen (7) lösen alle vier Paare die Pellsche Gleichung (1) in nichttrivialer Weise. Man weiß also, daß die Menge

$$\mathbf{P} := \{(x, y) \in \mathbb{N}^2 : x^2 - dy^2 = 1\}$$

nicht leer ist. Für $(x, y) \in \mathbf{P}$ ist $x + \alpha y > 1$ und somit sind die Zahlen

$$\begin{aligned}(x + \alpha y)^n = &\sum_{0 \le \nu \le n/2} \binom{n}{2\nu} x^{n-2\nu} d^\nu y^{2\nu} \\ &+ \alpha \sum_{0 \le \nu < n/2} \binom{n}{2\nu+1} x^{n-2\nu-1} d^\nu y^{2\nu+1} \\ &=: x_n + \alpha y_n \qquad (n = 1, 2, \ldots)\end{aligned} \tag{8}$$

paarweise verschieden, also auch die Paare $(x_n, y_n) \in \mathbb{N}^2$. Wegen

$$(x - \alpha y)^n = x_n - \alpha y_n \qquad \text{für } n = 1, 2, \ldots, \tag{8'}$$

(8) und $(x, y) \in \mathbf{P}$ ist $x_n^2 - dy_n^2 = (x^2 - dy^2)^n = 1$, also sind alle (x_n, y_n) aus $\mathbf{P}$ und der Satz ist bewiesen. □

Eine in 7 benötigte Konsequenz des obigen Satzes ist folgendes

Korollar. *Ist $d \in \mathbb{N}$ kein Quadrat und $\rho \in \mathbb{Z}$, $\rho \neq 0$, so hat (1) unendlich viele Lösungen $(x, y) \in \mathbb{N}^2$ mit $x \equiv 1$, $y \equiv 0 \pmod{\rho}$.*

Beweis. Man wendet den obigen Satz an auf die PELL–Gleichung $X^2 - d'Y^2 = 1$ mit $d' := d\rho^2$, was positiv ganz, aber kein Quadrat ist: $(x', y') \in \mathbb{N}^2$ löst diese genau dann, wenn $(x', |\rho|y') \in \mathbb{N}^2$ Gleichung (1) löst. Daher hat (1) jedenfalls unendlich viele verschiedene Lösungen $(\hat{x}, \hat{y}) \in \mathbb{N}^2$ mit $\hat{y} \equiv 0 \pmod{\rho}$ und daher $\hat{x}^2 \equiv 1 \pmod{\rho}$ wegen (1). Löst $(\hat{x}, \hat{y}) \in \mathbb{N}^2$ Gleichung (1) und setzt man $x := \hat{x}^2 + d\hat{y}^2$, $y := 2\hat{x}\hat{y}$, so ist (x, y) aus $\mathbb{N}^2$ und löst wegen

$$x^2 - dy^2 = (\hat{x}^2 + d\hat{y}^2)^2 - 4d\hat{x}^2\hat{y}^2 = (\hat{x}^2 - d\hat{y}^2)^2 = 1$$

Gleichung (1); weiter entsprechen verschiedenen $(\hat{x}, \hat{y})$ auch verschiedene (x, y). Damit hat man unendlich viele verschiedene Lösungen $(x, y) \in \mathbb{N}^2$ von (1) mit

$$y = 2\hat{x}\hat{y} \equiv 0, \quad x = \hat{x}^2 + d\hat{y}^2 \equiv 1 \pmod{\rho}. \qquad \square$$

4. Lösungsstruktur der Pell–Gleichung. Unter Abänderung der Bezeichnungsweise aus 3 werde nun $y_1 \in \mathbb{N}$ *minimal* so gewählt, daß es dazu ein $x_1 \in \mathbb{N}$ gibt mit $(x_1, y_1) \in \mathbf{P}$. Für jedes $(x, y) \in \mathbf{P}$ ist dann $x_1^2 = 1 + dy_1^2 \leq 1 + dy^2 = x^2$, also auch $x_1 \leq x$ und (x_1, y_1) heißt die *Minimallösung* der PELLschen Gleichung. Klar ist: Alle (x_n, y_n), die analog zu 3(8) gemäß

$$x_n + \alpha y_n = (x_1 + \alpha y_1)^n, \qquad n = 1, 2, \dots, \tag{1}$$

gebildet werden, gehören zu $\mathbf{P}$. Der folgende Satz besagt, daß es andere $(x, y) \in \mathbf{P}$ als die soeben beschriebenen (x_n, y_n) nicht gibt.

Satz. *Sämtliche Lösungen der* PELL*–Gleichung 3(1) in natürlichen Zahlen sind gegeben durch*

$$x = \frac{1}{2}\big((x_1+\alpha y_1)^n + (x_1-\alpha y_1)^n\big), \quad y = \frac{1}{2\alpha}\big((x_1+\alpha y_1)^n - (x_1-\alpha y_1)^n\big), \quad n \in \mathbb{N};$$

hier bedeutet (x_1, y_1) die Minimallösung von 3(1) und $\alpha := \sqrt{d}$.

Beweis. Ist $(x, y) \in \mathbf{P}$, so ist $1 < x_1 + \alpha y_1 \leq x + \alpha y$ wegen $y_1 \leq y$ und dem vorhin daraus gefolgerten $x_1 \leq x$. Daher ist für genau ein $n \in \mathbb{N}$

$$(x_1 + \alpha y_1)^n \leq x + \alpha y < (x_1 + \alpha y_1)^{n+1},$$

was wegen $0 < x_1 - \alpha y_1$ zu

$$1 \le (x + \alpha y)(x_1 - \alpha y_1)^n < x_1 + \alpha y_1 \tag{2}$$

äquivalent ist. Wegen 3(8′) und (1) ist $(x_1 - \alpha y_1)^n = x_n - \alpha y_n$ und mit $u := xx_n - dyy_n$, $v := yx_n - xy_n$ folgt $1 \le u + \alpha v < x_1 + \alpha y_1$ aus (2). Wegen (x, y), $(x_n, y_n) \in \mathbf{P}$ ist

$$u^2 - dv^2 = (u + \alpha v)(u - \alpha v) = (x + \alpha y)(x_n - \alpha y_n)(x - \alpha y)(x_n + \alpha y_n) = 1$$

klar und ebenso $v \in \mathbb{N}_0$: Denn bei $v < 0$ müßte $1 \le u + \alpha v < u - \alpha v$ sein, was nicht geht. Die Ungleichung $v \ge 0$ bedeutet $x_n \ge xy_n/y$, was zu $u \ge (x^2 - dy^2)y_n/y = y_n/y > 0$ führt. Wäre nun $v \ge 1$, so müßte bereits $v \ge y_1$ (und damit $u \ge x_1$) nach Definition der Minimallösung gelten, also $u + \alpha v \ge x_1 + \alpha y_1$. Daher ist $v = 0$, d.h. $yx_n = xy_n$ und aus denselben Gründen wie nach 3(7) folgt daraus

$$x = x_n, \quad y = y_n; \tag{3}$$

denn jedes 3(1) genügende Paar ganzer Zahlen hat automatisch teilerfremde Komponenten. Aus (1) und $x_n - \alpha y_n = (x_1 - \alpha y_1)^n$ folgt mit (3) sofort die Behauptung. □

Nach den bisherigen Erläuterungen ist bei nicht quadratischem $d \in \mathbb{N}$ klar, daß *die* Pell*–Gleichung genau die folgenden Lösungen besitzt: Die beiden trivialen* $(\pm 1, 0)$ *und für jedes* $(x, y) \in \mathbf{P}$ *die vier Paare* $(\pm x, \pm y)$.

Offenbar reduziert obiger Satz das Problem der Lösung der Pell–Gleichung 3(1) unter den über d gemachten Voraussetzungen einzig und allein darauf, die zugehörige Minimallösung aufzufinden. Prinzipiell läßt sich diese stets wie folgt gewinnen: Man betrachte die Zahlen $1 + dy^2$ für $y = 1, 2, \ldots$; das kleinste y_1, für welches $1 + dy_1^2$ ein Quadrat wird, etwa x_1^2, führt zwangsläufig zur Minimallösung. Ist z.B. $d = 3$, so wird $y_1 = 1$, $x_1 = 2$ und $(2, 1)$ ist die Minimallösung von $X^2 - 3Y^2 = 1$.

Dieses Probierverfahren zur Gewinnung der Minimallösung kann, abhängig von d, ziemlich lange dauern; zum Beispiel lautet im Falle der Primzahl $d = 98597$ die Minimallösung $(197193, 628)$, vgl. 5.3.6. Einen stets gangbaren und systematischen Weg zur Auffindung der Minimallösung hat Euler mit Hilfe der Theorie der regelmäßigen Kettenbrüche aufgezeigt, worauf in 5.3.6 eingegangen wird.

5. Pythagoräische Dreiecke mit Kathetendifferenz Eins. Als Anwendung der Ergebnisse über die Pell–Gleichung sollen hier *alle pythagoräischen Dreiecke bestimmt werden, deren Kathetenlängen sich um Eins unterscheiden.*

Offenbar geht es um die Ermittlung aller $(x, y, z) \in \mathbb{N}^3$ mit $x^2 + y^2 = z^2$ und $|x - y| = 1$. Wegen der letzten Bedingung sind alle sich hier ergebenden pythagoräischen Tripel primitiv und es darf o.B.d.A. $x < y$ (hier also $y = x+1$) vorausgesetzt werden. Somit interessieren alle Paare $(x, z) \in \mathbb{N}^2$ mit $2x^2 + 2x + 1 = z^2$ oder äquivalent $(2x + 1)^2 - 2z^2 = -1$ und man hat die diophantische Gleichung

$$X^2 - 2Y^2 = -1 \tag{1}$$

zu studieren und alle ihre Lösungen in natürlichen Zahlen zu finden.

Dies wiederum soll sofort etwas allgemeiner durchgeführt werden, indem die Gleichung

$$X^2 - dY^2 = -1 \tag{2}$$

untersucht wird. Während jedoch die PELL–Gleichung 3(1) für nicht quadratisches $d \in \mathbb{N}$ nach Satz 3 stets unendlich viele Lösungen hat, kann (2) unter denselben Voraussetzungen unlösbar sein: Ist d etwa durch 4 oder durch eine Primzahl $\equiv 3 \pmod 4$ teilbar, so ist (2) unlösbar. Im ersten Fall folgt dies aus $x^2 \not\equiv 3 \pmod 4$ für alle ganzen x. Ist im zweiten Fall $p \equiv 3 \pmod 4$ eine in d aufgehende Primzahl, so gilt $x^2 \not\equiv -1 \pmod p$ nach dem ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz (vgl. 3.2.6) und also auch $x^2 - dy^2 \neq -1$ für alle ganzen x, y. Übrigens findet sich ein notwendiges und hinreichendes Lösbarkeitskriterium für (2) mittels Kettenbruchtheorie bei PERRON [19], § 26.

Über Gleichung (2) gibt Auskunft der folgende

Satz. *Sei $d \in \mathbb{N}$ kein Quadrat. Ist $(\xi, \eta) \in \mathbb{Z}^2$ eine feste Lösung von (2), so erhält man in der Form $(\xi x - d\eta y,\ \eta x - \xi y)$ jede Lösung von (2), wenn (x, y) alle Lösungen der zugehörigen* PELL*–Gleichung 3(1) durchläuft.*

Beweis. Man betrachtet die (von (ξ, η) abhängige) Abbildung

$$\varphi : (x, y) \mapsto (\xi x - d\eta y,\ \eta x - \xi y)$$

der Menge aller Lösungen von 3(1) in die Menge aller Lösungen von (2). Wie in 3(6) ist nämlich mit $\alpha := \sqrt{d}$

$$(x - \alpha y)(\xi + \alpha\eta) = (\xi x - d\eta y) + \alpha(\eta x - \xi y); \tag{3}$$

ersetzt man hierin α durch $-\alpha$ und multipliziert dann die neu entstandene Gleichung mit (3), so wird

$$1 \cdot (-1) = (x^2 - dy^2)(\xi^2 - d\eta^2) = (\xi x - d\eta y)^2 - d(\eta x - \xi y)^2.$$

Ist nun $(u, v) \in \mathbb{Z}^2$ vorgegeben, so kann man das lineare Gleichungssystem

$$\xi x - d\eta y = u, \qquad \eta x - \xi y = v$$

wegen $d\eta^2 - \xi^2 = 1$ nach x, y auflösen und erhält $x = -u\xi + d\eta v$, $y = -\eta u + \xi v \in \mathbb{Z}$. Löst (u, v) Gleichung (2), so löst (x, y) Gleichung 3(1). Somit ist φ surjektiv; die Injektivität von φ ist klar. □

Ersichtlich löst $(1,1)$ Gleichung (1), so daß sich nach dem soeben gezeigten Satz alle Lösungen von (1) in der Form $(x-2y, x-y)$ ergeben, wenn (x,y) alle Lösungen der zu (1) gehörigen PELL–Gleichung

$$X^2 - 2Y^2 = 1 \tag{4}$$

durchläuft. Da $(3,2)$ die Minimallösung von (4) ist, erhält man aus Satz 4, wenn man noch $\beta := 3+2\sqrt{2}$, $\gamma := 3-2\sqrt{2}$ setzt: Die (x_n, y_n) mit

$$x_n = \frac{1}{2}(\beta^n + \gamma^n), \quad y_n = \frac{1}{2\sqrt{2}}(\beta^n - \gamma^n) \quad (n = 0,1,\ldots) \tag{5}$$

sind genau die (4) genügenden Paare mit nichtnegativen Komponenten. Da β und γ die beiden Wurzeln des Polynoms $X^2 - 6X + 1$ sind, gilt

$$\beta^{n+2} - 6\beta^{n+1} + \beta^n = 0 \text{ und } \gamma^{n+2} - 6\gamma^{n+1} + \gamma^n = 0 \quad \text{für } n = 0,1,\ldots$$

und so genügen die x_n wegen (5) der Rekursion

$$x_{n+2} = 6x_{n+1} - x_n \qquad (n = 0,1,\ldots) \tag{6}$$

mit den Anfangswerten $x_0 = 1$, $x_1 = 3$. Derselben Rekursion gehorchen die y_n, allerdings mit den Anfangswerten $y_0 = 0$, $y_1 = 2$. Man hat also nachstehende kleine Tabelle für den Beginn dieser beiden Folgen:

n	0	1	2	3	4	5	6	7	8	9
x_n	1	3	17	99	577	3363	19601	114243	665857	3880899
y_n	0	2	12	70	408	2378	13860	80782	470832	2744210

Da

$$y_n < x_n < 2y_n \qquad \text{für } n = 1,2,\ldots \tag{7}$$

gilt, hat für alle diese n von den vier verschiedenen Paaren

$$(x_n + 2y_n, x_n + y_n), \quad (x_n - 2y_n, x_n - y_n),$$

$$(-x_n + 2y_n, -x_n + y_n), \quad (-x_n - 2y_n, -x_n - y_n)$$

jeweils genau das erste beide Komponenten positiv; für $n = 0$ sind die beiden ersten Paare gleich $(1,1)$, die beiden letzten $(-1,-1)$. Damit kann gesagt werden: Alle Lösungen von (1) in natürlichen Zahlen sind von der Form $(x_n+2y_n, x_n+y_n) =: (u_n, v_n)$ für $n = 0,1,\ldots$. Diese u_n, v_n kann man wiederum

rekursiv bestimmen: Da die x_n, y_n nämlich derselben linearen homogenen Rekursion (6) genügen, muß dies auch für die u_n, v_n zutreffen, d.h. man hat für $n = 0, 1, \ldots$

$$u_{n+2} = 6u_{n+1} - u_n \quad \text{bzw.} \quad v_{n+2} = 6v_{n+1} - v_n$$

mit den Anfangswerten $u_0 = 1$, $u_1 = 7$; $v_0 = 1$, $v_1 = 5$. Die ersten u_n bzw. v_n entnimmt man der zweiten bzw. fünften Zeile der nachfolgenden Tabelle; nach den Ausführungen vor (1) erscheinen in den drei letzten Zeilen der n–ten Spalte für $n = 1, 2, \ldots$ die Komponenten x, y, z der neun kleinsten pythagoräischen Tripel (x, y, z) mit $y = x + 1$.

n	0	1	2	3	4	5	6	7	8	9
u_n	1	7	41	239	1393	8119	47321	275807	1607521	9369319
$\frac{1}{2}(u_n - 1)$	0	3	20	119	696	4059	23660	137903	803760	4684659
$\frac{1}{2}(u_n + 1)$	1	4	21	120	697	4060	23661	137904	803761	4684660
v_n	1	5	29	169	985	5741	33461	195025	1136689	6625109

Bemerkungen. 1) Wegen $\beta > 1 > \gamma > 0$ entnimmt man (5) die Relation $\lim_{n\to\infty} x_n/y_n = \sqrt{2}$ und in der Tat weicht x_9/y_9 von $\sqrt{2}$ um weniger als $6 \cdot 10^{-14}$ ab. Die beiden Brüche x_2/y_2 und x_4/y_4 wurden, wie in 1 erwähnt, bereits vor etwa 2500 Jahren als Näherungen für $\sqrt{2}$ verwendet. In der Sprache von 5.3.2 sind die x_n/y_n nichts anderes als die oberhalb $\sqrt{2}$ gelegenen Näherungsbrüche des regelmäßigen Kettenbruchs von $\sqrt{2}$.

2) In (6) ist der Leser zweigliedrigen linearen homogenen Rekursionen begegnet. Das historich älteste Beispiel einer derartigen Rekursion ist wohl die durch

$$F_0 := 0 \quad F_1 := 1 \quad \text{und} \quad F_{n+2} := F_{n+1} + F_n \quad \text{für } n \geq 0$$

definierte FIBONACCI–Folge $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$. L. PISANO *), genannt FIBONACCI (kurz für *filius* BONACCI), hat in seinem *Liber Abaci* (1202) folgendes Problem gestellt. Jemand setzt ein neugeborenes Kaninchenpaar in einen Stall. Nach w Wochen ist es fortpflanzungsfähig und nach weiteren w Wochen wird ein junges Kaninchenpaar geworfen. Das Leben des jungen Paares

*) Seine Geburtsstadt Pisa ehrte FIBONACCI mit einer monumentalen Marmorskulptur, die sich unter denen zahlreicher weiterer Honoratioren im Camposanto auf der weltberühmten Piazza dei Miracoli findet, und zwar in der dem Eingang diagonal gegenüberliegenden Ecke.

verläuft genau wie das des älteren, welch letzteres wieder nach w Wochen ein drittes Kaninchenpaar hervorbringt usw. Man überlegt sich leicht, daß nach $n \cdot w$ Wochen F_n Kaninchenpaare im Stall sind (falls kein Kaninchen eingeht).

Die Bedeutung des *Liber Abaci* beruht allerdings weniger auf der Überlieferung dieser Aufgabe als vielmehr auf der Tatsache, daß dies eines der wenigen einflußreichen mittelalterlichen Mathematikbücher war, welches der indisch–arabischen Ziffernschreibweise (vgl. 5.1.12) in Europa zum Durchbruch verhalf.

6. Einheiten reell–quadratischer Zahlkörper. Wie bei quadratfreiem ganzem $d \neq 1$ der Ganzheitsring O_d des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ aussieht, wurde in Satz 1.6.7 ermittelt. Anschließend wurden in Satz 1.6.8A die Einheiten in O_d wie folgt charakterisiert: Bei $d \equiv 2, 3 \pmod 4$ ist $\varepsilon \in O_d$ genau dann Einheit, wenn das Paar $(x, y) \in \mathbb{Z}^2$ in $\varepsilon = x + y\sqrt{d}$ eine der beiden folgenden Gleichungen löst.

$$(1a, b) \qquad X^2 - dY^2 = 1, \quad X^2 - dY^2 = -1.$$

Ist dagegen $d \equiv 1 \pmod 4$, so ist $\varepsilon \in O_d$ genau dann Einheit, wenn (x, y) in $\varepsilon = \frac{1}{2}(x + y\sqrt{d})$ der Bedingung $2 | (x - y)$ genügt und eine der beiden Gleichungen

$$(2a, b) \qquad X^2 - dY^2 = 4, \quad X^2 - dY^2 = -4$$

löst. Hieraus ergibt sich unmittelbar folgender

Satz. *Bei quadratfreiem ganzem $d \geq 2$ führen die Lösungen (x, y) der* Pell*–Gleichung (1a) stets zu Einheiten $x + y\sqrt{d}$ des reell–quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$. Bei $d \equiv 1 \pmod 4$ oder $d \equiv 2 \pmod 8$ können zusätzlich die Lösungen (x, y) von (1b) zu weiteren Einheiten $x + y\sqrt{d}$ führen; ist schließlich $d \equiv 5 \pmod 8$, so können noch die Lösungen (x, y) mit $2 \nmid xy$ von (2a) oder (2b) Einheiten der Form $\frac{1}{2}(x + y\sqrt{d})$ liefern.*

Beweis. Daß (1b) für $d \equiv 3 \pmod 4$ unlösbar ist, wurde schon vor Satz 5 geklärt; denn dann muß d einen Primfaktor $\equiv 3 \pmod 4$ enthalten. Hätte man bei $d \equiv 6 \pmod 8$ eine Lösung (x, y) von (1b), so wäre x ungerade, also $dy^2 = x^2 + 1 \equiv 2 \pmod 8$, was $3y^2 \equiv 1 \pmod 4$ implizieren würde. Gibt es eine Lösung (x, y) mit $2 \nmid xy$ von (2a) oder (2b), so gilt $1 - d \equiv 4 \pmod 8$, also $d \equiv 5 \pmod 8$. □

Während Satz 1.6.8B gezeigt hat, daß imaginär–quadratische Zahlkörper stets endlich viele, im allgemeinen sogar nur die beiden trivialen Einheiten 1 und -1 besitzen, verhalten sich reell–quadratische Zahlkörper in dieser Hinsicht anders:

Korollar. *Jeder reell–quadratische Zahlkörper hat unendlich viele Einheiten.*

Bemerkung. Ist $d \in \mathbb{N}$ quadratfrei und $d \equiv 3$, 6 oder 7 (mod 8), so rühren nach obigem Satz die Einheiten des reell-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ alleine von den Lösungen der PELL–Gleichung (1a) her. In den Fällen $d \equiv 1, 2, 5 \pmod 8$ kann (1b) lösbar bzw. unlösbar sein; Beispiele dafür sind 17, 2, 5 bzw. 33, 42, 21. Im Fall $d \equiv 5 \pmod 8$ kann (2b) in ungeraden Zahlen lösbar (z.B. für $d = 13$) oder unlösbar (z.B. $d = 21$) sein; im gleichen Fall ist (2a) in ungeraden Zahlen lösbar z.B. für $d = 21$ und unlösbar für $d = 37$.

Dabei sieht man die Lösbarkeitsaussagen jeweils mit Hilfe eines leichten Beispiels; für die Unlösbarkeitsbehauptungen beachtet man $3|d$ (vgl. 5) außer für (2a) bei $d = 37$. Für die Unlösbarkeit von $X^2 - 37Y^2 = 4$ in ungeraden Zahlen konsultiere man PERRON [19], § 26 oder die Tabelle bei A. CAYLEY (Mathematical Papers IV, 40–42).

Nach obigem Satz können lediglich im Fall $d \in \mathbb{N}$, $d \equiv 5 \pmod 8$ und quadratfrei, Einheiten von $\mathbb{Q}(\sqrt{d})$ von ungeraden Lösungen der Gleichungen (2a) oder (2b) herrühren. Man kann sich fragen, ob für

$$X^2 - dY^2 = a, \qquad a \in \{4, -4\} \tag{2}$$

ein zu Satz 5 analoges Ergebnis gezeigt werden kann derart, daß man aus einer einzigen Lösung (ξ, η) von (2) in ungeraden Zahlen mit Hilfe aller Lösungen der zugehörigen PELL–Gleichung (1a) *sämtliche* ungeraden Lösungen von (2) gewinnen kann. Dies ist in folgendem Sinne "genau zur Hälfte" richtig:

Proposition. *Sei $d \in \mathbb{N}$, $d \equiv 5 \pmod 8$ und $(\xi, \eta) \in \mathbb{Z}^2$ eine feste Lösung von (2) mit $2 \nmid \xi\eta$. Dann hat jedes Paar aus*

$$\{(\xi x - d\eta y, \eta x - \xi y) : \ (x, y) \in \mathbb{Z}^2,\ x^2 - dy^2 = 1\} \tag{3}$$

ungerade Komponenten und löst (2). Ist umgekehrt $(\hat{x}, \hat{y})$ mit $2 \nmid \hat{x}\hat{y}$ irgendeine Lösung von (2), so kommt von den beiden Lösungen $(\hat{x}, \hat{y})$, $(\hat{x}, -\hat{y})$ (bzw. von $(\hat{x}, \hat{y})$, $(-\hat{x}, \hat{y})$) von (2) genau eine in der Menge (3) vor.

Der *Beweis* kann dem Leser zur Übung überlassen bleiben.

7. Ganze Punkte auf Kurven zweiten Grades. In den letzten vier Abschnitten wurden verschiedentlich Fragen der Art behandelt, wann es zu festen $a, d \in \mathbb{Z} \setminus \{0\}$ ganzzahlige (x, y) gibt, die das spezielle Polynom $X^2 - dY^2 - a$ in zwei Unbestimmten annullieren. Es ist naheliegend, dieselbe Frage allgemeiner für

$$f(X, Y) := c_{00} + 2c_{01}X + 2c_{02}Y + c_{11}X^2 + 2c_{12}XY + c_{22}Y^2 \in \mathbb{Z}[X, Y] \tag{1}$$

(vgl. 2.3(2)) zu untersuchen, wenn wieder die symmetrische Matrix 2.3(3)

$$\mathbf{C} := \begin{pmatrix} c_{00} & c_{01} & c_{02} \\ c_{01} & c_{11} & c_{12} \\ c_{02} & c_{12} & c_{22} \end{pmatrix}$$

maximalen Rang hat. Durch diese Rangforderung bleiben gewisse Ausartungsfälle beiseite, für die das Problem der Bestimmung aller ganzzahligen Lösungen von

$$f(X, Y) = 0 \tag{2}$$

prinzipiell bereits in 1.3.3–4 erledigt wurde.

Man definiert jetzt

$$\begin{aligned} d &:= c_{12}^2 - c_{11}c_{22}, & e &:= c_{01}^2 - c_{00}c_{11}, \\ \ell &:= c_{01}c_{22} - c_{12}c_{02}, & m &:= c_{02}c_{11} - c_{01}c_{12} \end{aligned} \tag{3}$$

und diskutiert vorab den Fall $d = 0$, in welchem $m \neq 0$ wegen der Rangforderung gelten muß. Sicher ist hier $(c_{11}, c_{22}) \neq (0, 0)$, da andernfalls wegen (3) auch $c_{12} = 0$, also Rang $\mathbf{C} < 3$ sein müßte. Ist etwa o.B.d.A. $c_{11} \neq 0$, so ist (2) ersichtlich gleichbedeutend mit $(c_{01} + c_{11}X + c_{12}Y)^2 = e - 2mY$. Ist die Kongruenz $Z^2 \equiv e \pmod{2m}$ unlösbar, so ist (2) unlösbar; ist diese Kongruenz jedoch lösbar, so führen genau diejenigen $(z, y) \in \mathbb{Z}^2$ mit $z^2 = e - 2my$, für die $c_{11} | (z - c_{01} - c_{12}y)$ gilt, zu einem (2) lösenden Paar $(x, y) \in \mathbb{Z}^2$.

Ab jetzt sei $d \neq 0$ und $\alpha := \ell/d$, $\beta := m/d$ gesetzt; diese rationalen Zahlen sind genau so gewählt, daß der Gradient von f im Punkt (α, β) verschwindet. Daher schreibt sich (1) jetzt als

$$f(X, Y) = f(\alpha, \beta) + c_{11}(X - \alpha)^2 + 2c_{12}(X - \alpha)(Y - \beta) + c_{22}(Y - \beta)^2. \tag{4}$$

Nach Wahl von α, β ist

$$f(\alpha, \beta) = c_{00} + c_{01}\alpha + c_{02}\beta = \frac{1}{d}(c_{00}d + c_{01}\ell + c_{02}m) = -\frac{1}{d}\det \mathbf{C};$$

dabei sieht man die letzte Gleichung leicht durch Laplace–Entwicklung von $\det \mathbf{C}$ nach erster Zeile oder Spalte. Somit ist (2) wegen (4) äquivalent zur diophantischen Gleichung

$$c_{11}(dX - \ell)^2 + 2c_{12}(dX - \ell)(dY - m) + c_{22}(dY - m)^2 = d \cdot \det \mathbf{C}, \tag{5}$$

wobei die rechte Seite nicht verschwindet.

Bei $c_{11} = 0$ hat (8) höchstens endlich viele Lösungen. Ist nämlich $(x, y) \in \mathbb{Z}^2$ eine solche, so gilt $dy - m = t$ und $2c_{12}(dx - \ell) + c_{22}t = d(\det \mathbf{C})/t$, wo $t \in \mathbb{Z} \setminus \{0\}$ einer der endlich vielen Teiler von $d \cdot \det \mathbf{C}$ sein muß; man beachte $c_{12} \neq 0$ wegen $d \neq 0$ und (3).

Für $c_{11} \neq 0$ sind (2) und (5) gleichbedeutend mit

$$(dY - m)^2 - d(c_{01} + c_{11}X + c_{12}Y)^2 = -c_{11} \det \mathbf{C}. \tag{6}$$

Ist jetzt d entweder negativ oder ein positives Quadrat, so hat (2) wieder höchstens endlich viele Lösungen. Mit dem nun noch ausstehenden interessantesten Fall beschäftigt sich folgender

Satz. *In (1) sei* $\det \mathbf{C} \neq 0$ *und* $c_{12}^2 - c_{11}c_{22}$ *sei positiv, aber kein Quadrat. Löst* $(\xi, \eta) \in \mathbb{Z}^2$ *Gleichung (2), so lassen sich daraus unendlich viele verschiedene ganzzahlige Lösungen von (1) konstruieren.*

Beweis. Man setzt

$$\xi_1 := d\eta - m, \ \eta_1 := c_{01} + c_{11}\xi + c_{12}\eta, \ b := -c_{11} \det \mathbf{C} \ \ (\neq 0) \tag{7}$$

und kann wegen $f(\xi, \eta) = 0$ und (6) sagen, daß $(\xi_1, \eta_1) \in \mathbb{Z}^2$ die diophantische Gleichung

$$U^2 - dV^2 = b \tag{8}$$

löst. Ist nun (u, v) eine beliebige Lösung der zu (8) gehörigen PELL–Gleichung, so lösen analog zu 5 und 6 auch alle paarweise verschiedenen

$$(\xi_1 u - d\eta_1 v, \eta_1 u - \xi_1 v)$$

die Gleichung (8). Nach Korollar 3 gelten für unendlich viele dieser (u, v) die simultanen Kongruenzen

$$u \equiv 1, \quad v \equiv 0 \pmod{c_{11}d}; \tag{9}$$

$c_{11} \neq 0$ trifft ja zu, da d andernfalls ein positives Quadrat wäre. Mit diesen (u, v) ist wegen (7) und (9) modulo $c_{11}d$

$$\xi_1 u - d\eta_1 v \equiv d\eta - m, \quad \eta_1 u - \xi_1 v \equiv \eta_1 = c_{01} + c_{11}\xi + c_{12}\eta.$$

Die erste dieser Kongruenzen bedeutet, daß es ein *ganzes* y mit

$$\xi_1 u - d\eta_1 v = dy - m \quad \text{und} \quad y \equiv \eta \pmod{c_{11}} \tag{10}$$

gibt. Die zweite Kongruenz besagt, daß man (zu diesem y) auch noch ein *ganzes* x finden kann, so daß folgende Gleichung besteht

$$\eta_1 u - \xi_1 v = c_{01} + c_{11}x + c_{12}y. \tag{11}$$

Verschiedenen (u, v) entsprechen offenbar verschiedene (x, y) und wegen (7), (8), (10), (11) lösen alle (x, y) die Gleichungen (6) und (2). □

Bemerkung. Die ab 3 untersuchten Gleichungen $X^2 - dY^2 = a$ waren stets von dem im Satz behandelten Typ.

8. Anmerkungen dazu. 1) Hat 7(2) unendlich viele Lösungen, so wird man diese im allgemeinen *nicht alle* auf dem Wege aus einer einzigen gewinnen können, der im Beweis von Satz 7 (und auch schon in 5) eingeschlagen wurde. Dies belegt z.B. Proposition 6. Man kann jedoch zeigen – und darauf deutet die genannte Proposition ebenfalls schon hin –, daß man unter den Voraussetzungen des letzten Satzes *endlich viele* verschiedene "Grundlösungen" (ξ_j, η_j) von 7(2) finden kann derart, daß man daraus auf dem oben angesprochenen Weg tatsächlich *alle* Lösungen von 7(2) erhält.

2) Schreibt man U, V statt $dX - \ell$, $dY - m$ in 7(5), so ist 7(5) äquivalent mit dem Problem der Darstellung der unter den Voraussetzungen des letzten Satzes von Null verschiedenen ganzen Zahl $d \det \mathbf{C}$ durch die nicht ausgeartete *indefinite binäre quadratische Form* $c_{11}U^2 + 2c_{12}UV + c_{22}V^2$. In dieser Auffassung wurde das Problem von Gauss (*Disquisitiones Arithmeticae*, insbesondere Artt. 299, 300) vollständig gelöst. Die sogenannte Reduktionstheorie liefert ein System von Grundlösungen, wie sie in der vorigen Bemerkung angesprochen wurden. Hier soll allerdings auf die Theorie der quadratischen Formen nicht näher eingegangen werden; der interessierte Leser sei in diesem Punkt z.B. verwiesen auf die elementare Einführung in Scholz/Schoeneberg (*Einführung in die Zahlentheorie*, 5. Aufl., de Gruyter, Berlin–New York, 1973).

3) In 1.3.3 hat man gesehen, daß die Komponenten der unendlich vielen Lösungen einer *linearen* diophantischen Gleichung $c_0 + c_1X + c_2Y = 0$ mit $(c_1, c_2) \neq (0, 0)$ gewissen *arithmetischen* Folgen angehören, wenn die Gleichung überhaupt lösbar ist. Nach den Sätzen 4 und 5 und nach Anmerkung 1 kann man sagen, daß die Komponenten der Lösungen der *quadratischen* Gleichung 7(2) bei $\det \mathbf{C} \neq 0$ und d positiv, aber kein Quadrat, gewissen verallgemeinerten *geometrischen* Folgen angehören, wenn 7(2) überhaupt lösbar ist; vgl. dazu die Formel für die Lösungen der Pell–Gleichung in Satz 4. Im quadratischen Fall sind die Lösungen, wenn überhaupt vorhanden, also wesentlich seltener als im linearen.

Dieser Trend setzt sich tatsächlich fort: In 6.2.3 wird sich zeigen, daß polynomiale diophantische Gleichungen mindestens dritten Grades in zwei Unbestimmten im allgemeinen höchstens noch endlich viele Lösungen haben.