Quadratisch, praktisch, gut: Aus der Zahlentheorie

Christian Bernert, 28. Oktober 2021

Einleitung

In diesem Brief beschäftigen wir uns mit verschiedenen Wegen, quadratische Gleichungen in der Zahlentheorie zu lösen. Ziel ist es, einerseits diese verschiedenen Methoden kennenzulernen und zu verstehen, wann die eine und wann die andere vielver-sprechend ist, um eine Aufgabe zu lösen.

Andererseits soll aber auch hervorgehoben werden, dass die verschiedenen Methoden oft mehr oder weniger äquivalent zueinander sind und nur verschiedene Blickwinkel auf die gleiche Tatsache liefern. Daher werden wir einigen Beispiel-Aufgaben in diesem Brief mehrfach begegnen.

1 Eine geometrische Methode

Wir beginnen mit einer sehr einfachen und sehr bekannten quadratischen Gleichung, nämlich

$$x^2 + y^2 = z^2. \tag{1}$$

Nach dem Satz des Pythagoras treten Lösungen dieser Gleichung als Seitenlängen rechtwinkliger Dreiecke aus. Ganzzahlige (positive) Lösungstripel (x, y, z) von (1) werden daher auch als *Pythagoräische Zahlentripel* bezeichnet. Ein bekanntes Beispiel ist $(3, 4, 5)$. Nun lassen sich daraus sofort unendlich viele Lösungen konstruieren, nämlich $(3n, 4n, 5n)$ für eine beliebige natürliche Zahl n. Wir nennen ein pythagoräisches Zahlentripel *primitiv*, wenn die Zahlen x, y, z keinen gemeinsamen Teiler größer als 1 haben. Das Tripel $(3, 4, 5)$ ist also primitiv, $(3n, 4n, 5n)$ für $n > 1$ jedoch nicht. Gibt es unendlich viele primitive pythagoräische Zahlentripel? Auch dies ist nicht schwer zu beantworten, denn wann immer $2n + 1$ eine Quadratzahl ist (und dies ist sicherlich unendlich oft der Fall), können wir das (primitive) Tripel $(n, \sqrt{2n+1}, n + 1)$ wählen.

Was aber, wenn *alle* (primitiven) pythagoräischen Zahlentripel gesucht sind?
Um uns dieser Frage geometrisch zu nähern, bemerken wir zunächst, dass die Gleichung (1) äquivalent ist zu

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1,$$

mit $X = \frac{x}{z}$ und $Y = \frac{y}{z}$ also zu $X^2 + Y^2 = 1$, was genau die Gleichung des Einheitskreises im kartesischen Koordinatensystem ist.
Aus einem (primitiven) pythagoräischen Zahlentripel lässt sich also ein *rationaler Punkt* auf dem Einheitskreis konstruieren und umgekehrt (indem mit dem kleinsten gemeinsamen Nenner multipliziert wird). Aus dem Zahlentripel $(3, 4, 5)$ wird auf diese Weise etwa der Punkt $\left(\frac{3}{5}, \frac{4}{5}\right)$ auf dem Einheitskreis.

Um nun die rationalen Punkte auf dem Einheitskreis zu untersuchen, stellen wir folgende Überlegung an: Zunächst wählen wir *einen* festen rationalen Punkt, etwa $P = (-1, 0)$. (Wir könnten auch $\left(\frac{3}{5}, \frac{4}{5}\right)$ oder jeden beliebigen anderen Punkt wählen, die Rechnungen werden dann etwas umständlicher, das Prinzip bliebe aber das gleiche.)

Zu jedem weiteren rationalen Punkt Q auf dem Einheitskreis können wir nun die Gerade durch P und Q betrachten, diese hat sicherlich eine rationale Steigung $m \in \mathbb{Q}$. Die entscheidende Beobachtung ist, dass sich diese Überlegung umkehren lässt: Wählen wir eine beliebige rationale Steigung m und betrachten die Gerade durch P mit Steigung m, so schneidet diese den Kreis in einem zweiten Punkt und dieser hat, wie wir gleich direkt nachrechnen werden, wiederum rationale Koordinaten!

Konkret erhalten wir bei der Wahl von $P = (-1, 0)$ die Geradengleichung $y = m(x + 1)$. Den zweiten Schnittpunkt mit dem Kreis $x^2 + y^2 = 1$ erhalten wir durch Einsetzen:

$$0 = x^2 + (m(x + 1))^2 - 1 = (m^2 + 1)x^2 + 2m^2x + (m^2 - 1).$$

Dies ist eine quadratische Gleichung in x, von der bereits eine Lösung, $x = -1$, bekannt ist (diese entspricht dem ersten Schnittpunkt P). Wir können also $x + 1$ ausklammern und erhalten

$$0 = (x + 1)((m^2 + 1)x + (m^2 - 1)),$$

der zweite Schnittpunkt liegt also bei $x = \frac{1-m^2}{1+m^2}$ und $y = m(x + 1) = \frac{2m}{1+m^2}$.

Wir haben also gezeigt: Für jede rationale Zahl m ist $\left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$ ein rationaler Punkt auf dem Einheitskreis (dieser Teil ließe sich natürlich auch direkte Rechnung überprüfen) und umgekehrt sind alle rationalen Punkte außer $(-1, 0)$ von dieser Form. Schreiben wir nun $m = \frac{v}{u}$ mit teilerfremden Zahlen u und v, so erhalten wir die Punkte $\left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right)$. Damit ist bereits eine Parametrisierung aller rationalen Punkte auf dem Einheitskreis gefunden und mit einer kleinen Zusatzüberlegung erhalten wir schließlich auch die Parametrisierung aller primitiven pythagoräischen Zahlentripel:

Satz: Alle primitiven pythagoräischen Zahlentripel sind bis auf die Reihenfolge der ersten beiden Variablen von der Form

$$(u^2 - v^2, 2uv, u^2 + v^2)$$

mit teilerfremden natürlichen Zahlen u, v mit $u > v$.

Beweis: Es ist schon fast alles passiert. Ist (x, y, z) ein primitives pythagoräisches Zahlentripel, so zeigt eine Betrachtung der Gleichung modulo 4, dass x und y unterschiedliche Parität haben. Durch Vertauschen von x und y wenn nötig dürfen wir also annehmen, dass y gerade und x ungerade ist. Nach unseren Vorüberlegungen gibt es teilerfremde Zahlen u und v mit $\frac{x}{z} = \frac{u^2-v^2}{u^2+v^2}$ und $\frac{y}{z} = \frac{2uv}{u^2+v^2}$. Hier können sicherlich nicht u und v beide ungerade sein, sonst wäre in $y(u^2 + v^2) = 2uvz$ die rechte Seite nicht durch 4 teilbar, die linke jedoch schon. Haben u und v aber unterschiedliche Parität, so sind $2uv, u^2 - v^2$ und $u^2 + v^2$ paarweise teilerfremd (warum?) und es folgt $x = u^2 - v^2, y = 2uv, z = u^2 + v^2$. □

Mit der gleichen Methode wie in diesem Abschnitt lassen sich die rationalen Punkte auf beliebigen Kurven bestimmen, die durch quadratische Gleichungen beschrieben werden, also Kreise, Ellipsen, Hyperbeln und Parabeln (diese werden allgemein auch Kegelschnitte genannt). Um alle ganzzahligen Lösungen einer solchen Gleichung zu finden, ist eine solche Parametrisierung allerdings manchmal nur bedingt hilfreich, wie wir im kommenden Abschnitt noch an einem anderen Beispiel sehen werden.

Die Idee, Lösungsmengen von Polynomgleichungen mit geometrischen Methoden zu untersuchen, führt auf direktem Wege in das wichtige mathematische Gebiet der *Algebraischen Geometrie*.

Das Grundprinzip der hier beschriebenen Methode ist auf quadratische Gleichungen beschränkt. Allerdings lässt es sich in gewisser Weise auf bestimmte Kurven von Grad 3 erweitern (so genannte *Elliptische Kurven*, auch wenn diese nur über einige historische Umwege etwas mit Ellipsen zu tun haben) und spielt dort eine wichtige Rolle in der Zahlentheorie, z.B. ist es Grund-prinzip vieler moderner kryptographischen Verfahren.
Haben wir einen Punkt und betrachten eine Gerade mit rationaler Steigung durch diesen Punkt, so schneidet diese die Kurve von Grad 3 im Allgemeinen in zwei weiteren Punkten und diese haben keinen Grund, beide wieder rationale Koordinaten zu haben.
Haben wir allerdings *zwei* Punkte mit rationalen Koordinaten, so können wir die Gerade durch diese beiden Punkte betrachten. Der dritte Schnittpunkt dieser Gerade mit der Kurve hat dann auch wieder rationale Koordinaten (warum?). Mit einer leichten Modifikation dieser Konstruktion kann man auf der Menge der rationalen Punkte auf der Kurve eine *Gruppenstruktur* konstruieren, also eine Vorschrift, wie je zwei Punkte zu einem neuen Punkt „addiert“ werden können.
Diese Gruppenstruktur genau zu verstehen, ist ein sehr schwieriges Problem und hat viele Mathematiker im 20. und auch noch im 21. Jahrhundert beschäftigt. Die auf dieser simplen geometrischen Beobachtung aufbauende Theorie hat unter anderem vor einigen Jahren zum Beweis des Großen Fermatschen Satzes durch Andrew Wiles geführt.

2 Vieta-Sprünge

Im letzten Abschnitt haben wir den Schnittpunkt von Gerade und Kreis als Lösung einer quadratischen Gleichung bestimmt. Im Allgemeinen muss eine solche natürlich keine rationale Lösung haben. Hier war die Situation aber speziell: Uns war bereits eine Lösung der Gleichung bekannt. Sind nun alle Koeffizienten der quadratischen Gleichung rational und hat sie mindestens eine rationale Lösung, so ist auch die zweite Lösung rational. Dies folgt allgemein sofort aus dem wichtigen, aber trivialen

Satz von Vieta: Sind x_1, x_2 die Lösungen der quadratischen Gleichung $x^2 - ax + b = 0$, so gilt $x_1 + x_2 = a$ und $x_1 x_2 = b$.

Beweis: Es muss $x^2 + ax + b = (x - x_1)(x - x_2)$ gelten und die Behauptung folgt nach Vergleich der Koeffizienten. □

Ist also eine Lösung x_1 bekannt, so erhalten wir die zweite als $x_2 = a - x_1 = \frac{b}{x_1}$. Speziell die erste dieser Identitäten zeigt sogar mehr: Sind a und die erste Lösung x_1 ganzzahlig, so erhalten wir eine weitere ganzzahlige Lösung x_2.
Wir können also von einer Lösung zu einer weiteren „springen“. Dieses einfache Prinzip der *Vieta-Sprünge* erlaubt in vielen Fällen bereits, unendlich viele Lösungen einer Gleichung zu konstruieren, wie das folgende Beispiel zeigt:

Aufgabe: Zeige, dass es unendlich viele Paare (x, y) natürlicher Zahlen gibt mit

$$x^2 + y^2 + 1 = 3xy.$$

Lösung: Sicherlich ist $(1, 1)$ eine Lösung. Haben wir eine Lösung (x_0, y_0) gefunden, so ist eine Lösung $x = x_0$ der quadratischen Gleichung $x^2 - 3y_0 x + (y_0^2 + 1) = 0$ bekannt. Wir erhalten also eine weitere Lösung $x = 3y_0 - x_0 = \frac{y_0^2+1}{x_0}$. Aus der ersten Identität sehen wir, dass diese neue Lösung wieder ganzzahlig ist, aus der zweiten, dass sie positiv ist.

Wir können also mit einem Vieta-Sprung von einer Lösung (x, y) zur Lösung $(3y - x, y)$ gelangen. Da die Gleichung symmetrisch ist, können wir dieses Prinzip abwechselnd auf die beiden Variablen anwenden und erhalten auf diese Weise ausgehend von der Startlösung $(1, 1)$ die Folge von Lösungen $(2, 1), (2, 5), (13, 5), (13, 34), \ldots$. Es ist nun leicht zu zeigen, dass auf diese Weise in der Tat immer größere Lösungen entstehen und wir damit unendlich viele verschiedene Lösungen erhalten. (Tatsächlich zeigt scharfes Hinsehen, dass wir es hier mit Paaren der Form (F_{2n-1}, F_{2n+1}) zu tun haben, wobei (F_n) die Fibonaccifolge bezeichnet. Der Leser möge sich einen Beweis dieser Tatsache überlegen.) □

Bei dieser Aufgabe hatten wir zu jedem Zeitpunkt zwei Möglichkeiten, einen Vieta-Sprung auszuführen, da wir jeweils eine der beiden Variablen als fest wählen konnten. Um unendlich viele Lösungen zu erhalten, war es natürlich von Vorteil, immer „nach oben“ zu springen. Auch die Sprünge „nach unten“ können sich aber als nützlich erweisen. Auf diese Weise lassen sich Vieta-Sprünge nämlich auch als Methode verwenden, um *alle* Lösungen einer Gleichung zu finden bzw. um zu zeigen, dass es überhaupt keine Lösungen gibt.

Aufgabe: Seien x und y natürliche Zahlen mit $xy \mid x^2 + y^2 + 1$. Zeige: $\frac{x^2+y^2+1}{xy} = 3$.

Lösung: Um aus der Teilbarkeit eine Gleichung zu machen, führen wir zunächst eine neue Variable ein und schreiben $x^2 + y^2 + 1 = kxy$. Wir wollen $k = 3$ zeigen.
Für festes k können wir nun einen Vieta-Sprung von einer Lösung (x, y) zu $(ky - x, y)$ machen, wobei $ky - x = \frac{y^2+1}{x}$ wie in der vorigen Aufgabe wieder eine natürliche Zahl ist. Angenommen, für ein k gäbe es nun eine Lösung. Die Idee ist, zu versuchen, mit einem Vieta-Sprung „nach unten“ immer kleinere Lösungen zu konstruieren, was natürlich ein Widerspruch wäre. Um dies sauber aufzuschreiben, ist es am einfachsten, mit der *kleinsten* Lösung zu beginnen. Damit meinen wir für unser festes k eine Lösung (x_0, y_0), bei der $x_0 + y_0$ minimal wird. Dabei dürfen wir aufgrund der Symmetrie ohne Einschränkung $x_0 \geq y_0$ annehmen. Wir wissen nun, dass auch (x_1, y_0) mit $x_1 = kx_0 - y_0 = \frac{y_0^2+1}{x_0}$ eine Lösung ist. Nach unserer Annahme muss also $x_1 \geq x_0$ sein, denn sonst wären wir zu einer kleineren Lösung gesprungen. Also folgt $x_1 = \frac{y_0^2+1}{x_0} \geq x_0$ und damit $y_0^2 + 1 \geq x_0^2$. Wir hatten aber $x_0 \geq y_0$ angenommen, also folgt sofort $x_0 = y_0$. Einsetzen in unsere Ausgangsgleichung zeigt jetzt aber $(k - 2)x_0^2 = 1$, also muss $k = 3$ gelten. Das war zu zeigen. □

Übung: Zeige, dass es für $k = 3$ keine weiteren Lösungen gibt.

Zum Ende dieses Abschnitts noch einige allgemeine Bemerkungen zu Aufgaben, die man mithilfe von Vieta-Sprüngen lösen möchte: Der Grundaufbau ist immer der gleiche und erfordert lediglich etwas Routine, aber keinerlei Gehirnschmalz. Die Schwierigkeit (und das ist der Grund, warum es immer noch IMO-Aufgaben gibt, die sich damit lösen lassen, jedoch auch bei Kenntnis dieser Methode nicht trivial sind) liegt oft einerseits darin, eine Aufgabe zunächst auf ein Problem zu reduzieren, indem die Methode anwendbar ist, etwa indem ein ursprünglich komplizierterer Ausdruck auf eine quadratische Gleichung reduziert wird (dies kann durchaus sehr viel Scharfsinn erfordern!), und andererseits in der konkreten Ausführung des „Endspiels“, also wie aus der Annahme einer minimalen Lösung im Einzelfall ein Widerspruch gefolgert werden kann. Dies kann durchaus zu einer ganz neuen Aufgabe führen, deren Schwierigkeitsgrad irgendwo zwischen „trivial“ und „viel schwieriger als die ursprüngliche Aufgabe“ liegen kann.

Übung: Finde (z.B. mithilfe des ersten Abschnitts) alle Paare (x, y) *rationaler* Zahlen mit $x^2 + y^2 + 1 = 3xy$. Lassen sich auf diese Weise auch alle ganzzahligen Punkte bestimmen?

3 Pellsche Gleichungen

Wir betrachten ein weiteres Mal die Gleichung $x^2 + y^2 + 1 = 3xy$. Ein natürlicher Ansatz ist eine Variablensubstitution, bei der der gemischte Term $3xy$ verschwindet. Dazu sollten wir x durch $x - \frac{3}{2}y$ ersetzen, oder – da wir im ganzzahligen Bereich bleiben wollen, durch $t = 2x - 3y$. Die Gleichung wird nun zu

$$t^2 - 5y^2 = -4. \tag{2}$$

Dies sieht eigentlich einfacher aus, doch wie können wir die Lösungen einer solchen Gleichung bestimmen? Nun, unsere Variablensubstitution ist umkehrbar, wir können x auch wieder durch t ausdrücken mittels $x = \frac{t+3y}{2}$ (beachte, dass t und y sicherlich die gleiche Parität haben, diese Zahl x also wieder ganz ist). Wie „übersetzen“ sich die Vieta-Sprünge $(x, y) \mapsto (3y - x, y)$ und $(x, y) \mapsto (x, 3x - y)$ in diese neuen Variablen?
Eine kurze Rechnung zeigt, dass beim ersten Sprung eine Lösung (t, y) von (2) auf $(-t, y)$ abgebildet wird. Dass dies wieder eine Lösung von (2) ist, ist offensichtlich und scheint nicht besonders hilfreich zu sein. Der andere Sprung ist interessanter: Hier wird (t, y) auf $\left(\frac{3t+5y}{2}, \frac{t+3y}{2}\right)$ abgebildet (beachte wieder, dass dies tatsächlich ganze Zahlen sind). Dass dies wiederum eine Lösung ist, lässt sich natürlich auch leicht überprüfen, denn man einfach nachrechnen, dass für beliebige Zahlen t und y die Identität

$$\left(\frac{3t + 5y}{2}\right)^2 - 5\left(\frac{t + 3y}{2}\right)^2 = t^2 - 5y^2$$

gilt. Und natürlich lassen sich mithilfe dieses Sprungs nun auch wieder unendlich viele Lösungen von (2) konstruieren und in der Tat sogar alle. Die spannenderen Fragen sind nun aber: Wie erklärt sich, dass es solch einen Sprung gibt? Wie ließe sich dieser ohne den Umweg über den vorigen Abschnitt direkt finden? Und lassen sich auf diese Weise stets alle Lösungen einer Gleichung vom Typ (2) finden?

Glücklicherweise existieren zu diesen Fragen größtenteils sehr zufriedenstellende Antworten. Auf der Suche nach diesen Antworten gelangt man in ein faszinierendes Gebiet der Mathematik, die *Algebraische Zahlentheorie*. Natürlich umfasst diese wesentlich mehr, als wir auf diesen wenigen Seiten andeuten können.
Wir betrachten zunächst noch einmal die Gleichung (2). Mit der 3. Binomischen Formel lässt sich diese faktorisieren zu

$$(t + \sqrt{5}y)(t - \sqrt{5}y) = -4.$$

Allgemeiner definieren wir zu einer reellen Zahl der Form $\xi = a + b\sqrt{5}$ mit $a, b \in \mathbb{Z}$ (oder allgemeiner $a, b \in \mathbb{Q}$) die *konjugierte Zahl* $\overline{\xi} = a - b\sqrt{5}$ sowie die *Norm* $N(\xi) = \xi \cdot \overline{\xi} = a^2 - 5b^2$.[1]
(Wer bereits komplexe Zahlen kennt, sieht vielleicht die Ähnlichkeit dieser Konstruktion zur komplexen Konjugation.)
Entscheidend ist nun, dass sich die Konjugation gut mit der Addition und vor allem mit der Multiplikation von zwei solchen Zahlen verträgt: Es gilt nämlich $\overline{\xi_1 + \xi_2} = \overline{\xi_1} + \overline{\xi_2}$ und $\overline{\xi_1 \cdot \xi_2} = \overline{\xi_1} \cdot \overline{\xi_2}$. Beide Identitäten lassen sich unmittelbar nachrechnen.

[1] Hier benutzen wir durchgehend, dass $\sqrt{5}$ irrational ist, sodass die Darstellung von $\xi = a + b\sqrt{5}$ eindeutig ist und somit $\overline{\xi}$ und $N(\xi)$ wirklich nur von ξ abhängen und nicht etwa von einer Wahl von a und b.

Daraus folgt nun auch sofort die entscheidende Eigenschaft der Norm, sie ist *multiplikativ*. Es gilt nämlich

$$N(\xi_1\xi_2) = \xi_1\xi_2 \cdot \overline{\xi_1\xi_2} = \xi_1\xi_2 \cdot \overline{\xi_1} \cdot \overline{\xi_2} = (\xi_1 \cdot \overline{\xi_1}) \cdot (\xi_2 \cdot \overline{\xi_2}) = N(\xi_1)N(\xi_2).$$

Was hat dies nun mit unserer Gleichung zu tun? In unserer neuen Sprache sagt diese schlicht $N(\xi) = -4$, wobei $\xi = t + \sqrt{5}y$ ist.
Spannend ist aber, was mit unserem Vieta-Sprung $(t, y) \mapsto \left(\frac{3t+5y}{2}, \frac{t+3y}{2}\right)$ passiert: Schreiben wir $\xi = t + \sqrt{5}y$ und $\xi' = \frac{3t+5y}{2} + \sqrt{5} \cdot \frac{t+3y}{2}$, so zeigt scharfes Hinsehen, dass $\xi' = \frac{3+\sqrt{5}}{2} \cdot \xi$ gilt.
Die entscheidende Eigenschaft der Zahl $\xi_0 = \frac{3+\sqrt{5}}{2}$ ist nun $N(\xi_0) = 1$.
Unsere Strategie lässt sich also wie folgt übersetzen: Um unendlich viele Lösungen von $N(\xi) = -4$ zu finden, müssen wir zunächst *eine* Lösung ξ_1 von $N(\xi_1) = -4$ finden und außerdem *eine* Lösung ξ_0 von $N(\xi_0) = 1$. Dann folgt

$$N(\xi_1\xi_0^n) = N(\xi_1)N(\xi_0)^n = -4$$

für alle n aus der Multiplikativität und mit etwas Glück finden wir auf diese Weise unendlich viele Lösungen. Genauer gesagt müssen wir nur $\xi_0 \neq \pm 1$ voraussetzen, um sicherzugehen, dass die Zahlen $\xi_1\xi_0^n$ allesamt verschieden sind und wir tatsächlich unendlich viele Lösungen erhalten.[2]

Der aufmerksame Leser kann sich nun sicherlich vorstellen, dass der grundsätzliche Erfolg dieser Methode nicht von der Zahl 5 bzw. $\sqrt{5}$ abhängt. Ungeklärt bleibt aber bisher die Frage, wie in einem konkreten Fall sichergestellt werden kann, dass *alle* Lösungen einer Gleichung von diesem Typ gefunden wurden.
Um diese Frage zu untersuchen, betrachten wir zunächst die allgemeine Gleichung

$$x^2 - Dy^2 = 1,$$

die sogenannte *Pell-Gleichung*, wobei D eine feste natürliche Zahl ist, die keine Quadratzahl ist (sodass $\sqrt{D}$ irrational ist), etwa $D = 5$.

Übung: Welche Paare (x, y) ganzer Zahlen lösen die Pell-Gleichung $x^2 - Dy^2 = 1$, wenn D eine Quadratzahl ist?

Wie im Spezialfall $D = 5$ können wir nun zu einer Zahl $\xi = x + \sqrt{D}y$ mit $x, y \in \mathbb{Z}$ (oder allgemeiner $x, y \in \mathbb{Q}$) die *konjugierte Zahl* $\overline{\xi} = x - \sqrt{D}y$ sowie die *Norm* $N(\xi) = \xi \cdot \overline{\xi} = x^2 - Dy^2$ betrachten. Wie zuvor ist diese multiplikativ. Ganzzahlige Lösungen (x, y) der Pell-Gleichung korrespondieren also zu Lösungen $\xi = x + \sqrt{D}y$ von $N(\xi) = 1$.

Aus den Vorüberlegungen ergibt sich nun sofort: Haben wir *eine* Lösung $\xi_1 > 1$ mit $N(\xi_1) = 1$ gefunden, so erhalten wir sofort unendlich viele mittels $N(\xi_1^n) = N(\xi_1)^n = 1$. Können wir auf diese Weise *alle* Lösungen finden? Wählen wir ξ_1 als eine beliebige Lösung, so können wir dies sicherlich nicht erwarten. Denn hätten wir etwa ξ_1^2 statt ξ_1 gewählt, so erhielten wir nur höchstens jede zweite Lösung. Um überhaupt eine Chance zu haben, auf diese Weise alle Lösungen zu generieren, sollten wir also sicherlich $\xi_1 > 1$ als die *kleinste Lösung* mit dieser Eigenschaft wählen. Aber reicht das aus? Und kann es auch passieren, dass es überhaupt keine Lösung gibt? Die Antworten liefert der folgende fundamentale

[2] Eine kleine Subtilität liegt hier noch vor, denn ξ_0 selbst hatte keine ganzzahligen „Koordinaten“. Dennoch liefern alle Zahlen $\xi_1\xi_0^n$ eine ganzzahlige Lösung aufgrund der bereits mehrfach erwähnten Tatsache, dass die Koordinaten von ξ_1 die gleiche Parität haben.

Satz: Sei D eine beliebige natürliche Zahl, die keine Quadratzahl ist. Dann gilt:
1) Es gibt mindestens eine Lösung der Pell-Gleichung $x^2 - Dy^2 = 1$ mit natürlichen Zahlen $x, y > 0$.
2) Ist (x_1, y_1) die kleinste solche Lösung (die sogenannte *Fundamentallösung*), dann sind alle Lösungen (x, y) der Pell-Gleichung mit $x, y > 0$ von der Form $x + y\sqrt{D} = (x_1 + y_1\sqrt{D})^n$ für ein $n \in \mathbb{N}$.
3) Diese Lösungen lassen sich auch schreiben als

$$x_n = \frac{(x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n}{2}$$

und

$$y_n = \frac{(x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n}{2\sqrt{D}}.$$

Beide Folgen (x_n) und (y_n) erfüllen die Rekursion $x_{n+2} = 2x_1x_{n+1} - x_n$.

Beweis: Wir gehen rückwärts vor. Dazu nehmen wir zunächst an, dass 1) und 2) bereits gezeigt wurden und zeigen 3), was keine großen Schwierigkeiten bereitet. Schreiben wir $\xi_1 = x_1 + \sqrt{D}y_1$ und $\xi_n = x_n + \sqrt{D}y_n = \xi_1^n$, so folgt $x_n = \frac{\xi_n + \overline{\xi_n}}{2} = \frac{\xi_1^n + \overline{\xi_1}^n}{2}$, was exakt die behauptete Formel ist. Die Formel für y_n folgt analog. Schließlich erfüllen die Folgen $(\xi_n) = (\xi_1^n)$ und $(\overline{\xi_n}) = (\overline{\xi_1}^n)$ die Rekursion und damit auch (x_n) und (y_n).

Nun arbeiten wir uns zu Teil 2) vor, wobei wir weiterhin annehmen, dass Teil 1) bereits gezeigt wurde, dass es also überhaupt eine Lösung gibt. Wir haben bereits festgestellt, dass alle $\xi_n = \xi_1^n$ zu Lösungen führen. Zu zeigen bleibt, dass es keine weiteren gibt. Angenommen, $\xi > 1$ wäre die kleinste Lösung, die nicht von dieser Form ist. Dann gibt es ein $n \geq 0$ mit $\xi_1^n < \xi < \xi_1^{n+1}$. Es kann nicht $n = 0$ gelten, denn das wäre ein Widerspruch zur Minimalität von ξ_1. Gilt aber $n \geq 1$, so folgt $\xi_1^{n-1} < \xi \cdot \overline{\xi_1} < \xi_1^n$. Nun ist aber $\xi \cdot \overline{\xi_1} < \xi$ auch eine Lösung, die nicht von der bekannten Form ist, ein Widerspruch zur Minimalität von ξ.

Schließlich bleibt der Beweis von Teil 1). Der Plan ist dabei in zwei Schritten vorzugehen. Zunächst zeigen wir die Existenz unendlich vieler Zahlen ξ mit relativ kleiner Norm und folgern daraus dann im zweiten Schritt die Existenz eines ξ mit $N(\xi) = 1$.
Für den ersten Schritt beobachten wir, dass eine Zahl $\xi = x + \sqrt{D}y$ mit kleiner Norm eine ziemlich gute Approximation $\frac{x}{y} \approx \sqrt{D}$ liefert. Umgekehrt wird nun ein Schuh daraus: Können wir gute rationale Approximationen an $\sqrt{D}$ finden, so korrespondieren diese zu Elementen mit kleiner Norm.
Die Existenz guter rationaler Approximationen folgt aus dem sehr wichtigen
Dirichletschen Approximationssatz: Ist α irrational, so gibt es unendlich viele Paare (a, q) mit

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

Beweis des Dirichletschen Approximationssatzes: Schubfachprinzip![3] Sei Q eine beliebige natürliche Zahl. Nach dem Schubfachprinzip müssen zwei der Zahlen $0, \alpha, 2\alpha, \ldots, Q\alpha$ Nachkommaanteile haben, die sich um weniger als $\frac{1}{Q}$ unterscheiden. Ihre Differenz ist dann von der Form $q\alpha$, welches Abstand weniger als $\frac{1}{Q}$ zur nächsten ganzen Zahl hat, die wir

[3] Tatsächlich hat Dirichlet in diesem Beweis historisch gewissermaßen das Schubfachprinzip erfunden!

a nennen. Es gilt also $|q\alpha - a| \leq \frac{1}{Q} \leq \frac{1}{q}$, was zu zeigen war. Indem wir Q immer größer wählen, stellen wir sicher, dass wir immer neue Paare erhalten (nur hier benutzen wir, dass α irrational ist!). □

Wenden wir diesen Satz auf $\alpha = \sqrt{D}$ an, erhalten wir unendlich viele Paare (a, q) mit $|a - q\sqrt{D}| \leq \frac{1}{q}$, also

$$|a^2 - Dq^2| \leq \frac{a + q\sqrt{D}}{q}.$$

Nun folgt aus $|a - q\sqrt{D}| \leq \frac{1}{q}$ sicherlich insbesondere $a \leq q\sqrt{D} + \frac{1}{q}$, also erhalten wir

$$|a^2 - Dq^2| \leq \frac{2q\sqrt{D} + \frac{1}{q}}{q} \leq 2\sqrt{D} + 1.$$

Wir haben also tatsächlich unendlich viele Zahlen $\xi = a + \sqrt{D}q$ mit relativ kleiner Norm $|N(\xi)| \leq 2\sqrt{D} + 1$ gefunden (entscheidend ist hier nur irgendeine feste obere Schranke). Insbesondere gibt es also zwei Zahlen ξ_1 und ξ_2 mit $N(\xi_1) = N(\xi_2) = m$ und $|m| \leq 2\sqrt{D}+1$. Um eine Zahl mit Norm 1 zu produzieren, könnten wir nun $\xi = \frac{\xi_1}{\xi_2} = \frac{\xi_1\overline{\xi_2}}{m}$ setzen und erhielten $N(\xi) = 1$.
Der Haken ist nur, dass wir dabei durch m teilen mussten und die „Koordinaten“ von ξ daher nicht notwendigerweise ganzzahlig sein werden.
Ein Griff in die Trickkiste löst allerdings auch dieses Problem: Da wir unendlich viele Zahlen ξ mit $|N(\xi)| \leq 2\sqrt{D}+1$ gefunden haben, finden wir sicherlich für ein m mit $|m| \leq 2\sqrt{D}+1$ auch unendlich viele (nicht zur zwei) ξ mit $N(\xi) = m$. Unter diesen muss es dann nach einer erneuten Anwendung des Schubfachprinzips zwei Lösungen $\xi_1 = x_1 + \sqrt{D}y_1$ und $\xi_2 = x_2 + \sqrt{D}y_2$ geben, für die $x_1 \equiv y_1 \mod m$ und $x_2 \equiv y_2 \mod m$ gilt. Dann folgt

$$\xi = \frac{\xi_1}{\xi_2} = \frac{(x_1 + \sqrt{D}y_1)(x_2 - \sqrt{D}y_2)}{m} = \frac{x_1x_2 - Dy_1y_2}{m} + \sqrt{D} \cdot \frac{x_2y_1 - x_1y_2}{m}$$

und nach Konstruktion ist diese Zahl ξ nun von der Form $\xi = x + \sqrt{D}y$ mit $x, y \in \mathbb{Z}$. Das war zu zeigen! □

Nach diesem langen Beweis noch einige Bemerkungen:

1) In der Praxis muss Teil 1) eigentlich nie zitiert werden: Soll eine konkrete Gleichung gelöst werden, kann die Minimallösung natürlich einfach geraten werden. Es ist aber als Meta-Prinzip gut zu wissen, dass es immer eine Lösung gibt.

2) Im Beweis haben wir bereits gesehen, dass Lösungen der Pell-Gleichung zu sehr guten rationalen Approximationen von $\sqrt{D}$ gehören. Tatsächlich kann man zeigen, dass dies in einem präzisen Sinne die besten rationalen Approximationen sind. Dies erklärt sich auch über den Zusammenhang der Lösungen der Pell-Gleichung zur Kettenbruchentwicklung von $\sqrt{D}$, über die hier leider aus Platzgründen nichts weiter berichtet werden kann. Wer mehr wissen will, findet zu dem Thema aber viel Material im Internet.

3) Tatsächlich kann die Fundamentallösung in einigen Fällen überraschend groß sein. Für $D = 61$ ist diese etwa

$$1766319049 + \sqrt{61} \cdot 226153980.$$

Übung: Finde alle Paare (x, y) *rationaler* Lösungen von $x^2 - Dy^2 = 1$.

Schließlich wollen wir noch ein Beispiel sehen, wie die eben entwickelte Theorie in der Lösung einer Olympiade-Aufgabe zur Anwendung kommt, die zunächst nicht offensichtlich etwas mit Pell-Gleichungen zu tun hat.

Aufgabe (Bundesrunde 2021): Man untersuche, ob es unendlich viele Tripel (u, v, w) positiver ganzer Zahlen u, v und w gibt, für die u, v und w eine arithmetische Folge bilden und für die $uv + 1, vw + 1$ und $wu + 1$ Quadratzahlen sind.

Lösung: Natürlich liegt eine Grundschwierigkeit dieser Aufgabe darin, dass nicht verraten wird, in welche Richtung (Konstruktion unendlich vieler Lösungen oder Endlichkeitsbeweis?) gearbeitet werden muss. Versuchen wir aber die Existenz unendlich vieler Lösungen nachzuweisen, so dürfen wir auf dem Weg dorthin beliebige Ansätze verwenden – wir müssen ja nicht *alle* Lösungen finden.

Wir schreiben zunächst die Bedingung der arithmetischen Progression um zu $u = v - d, w = v + d$ und erhalten das System

$$\begin{aligned} v^2 - vd + 1 &= a^2 \\ v^2 + vd + 1 &= b^2 \\ v^2 - d^2 + 1 &= c^2. \end{aligned}$$

Addieren der ersten beiden Gleichungen und Vergleich mit der dritten liefert

$$a^2 + b^2 = 2v^2 + 2 = 2(c^2 + d^2) = (c + d)^2 + (c - d)^2.$$

Ein Ansatz, wie dies zu erfüllen ist, ist $a = d - c, b = d + c$. Mit diesem Ansatz wird unser Gleichungssystem zu

$$\begin{aligned} v^2 - vd + 1 &= (d - c)^2 \\ v^2 - d^2 + 1 &= c^2. \end{aligned}$$

Abziehen der beiden Gleichungen zeigt dann $v = 2c$, unser Gleichungssystem ist also genau dann erfüllt, wenn $d^2 - 3c^2 = 1$ gilt.

Jetzt wissen wir, was zu tun ist: Nach der soeben entwickelten Theorie gibt es unendlich viele Paare (c, d) natürlicher Zahlen, die die Pell-Gleichung $d^2 - 3c^2 = 1$ lösen (die Fundamentallösung ist hier durch $d = 2, c = 1$ gegeben). Nach Rücksubstitution ist dann $(u, v, w) = (2c - d, 2c, 2c + d)$ eine Lösung der Aufgabe.

Wir müssen lediglich noch überprüfen, ob diese auch aus natürlichen Zahlen besteht, ob also $2c > d$ gilt. Es ist aber $d^2 = 3c^2 + 1 < 4c^2$ für alle Lösungen außer der Fundamentallösung $d = 2, c = 1$. Damit sind tatsächlich unendlich viele Lösungen konstruiert und die Aufgabe ist gelöst. □

Obwohl wir wissen, dass aus der Fundamentallösung *alle* Lösungen der Pell-Gleichung konstruiert werden können, war dies bei unserer Aufgabe weder nötig noch hilfreich: Es war nicht nötig, da gar nicht nach allen Lösungen gefragt war. Es wäre aber auch für diesen Zweck nicht hilfreich gewesen, denn wir haben ja zuvor einen Ansatz gewählt, um die Aufgabe auf die Pell-Gleichung zu reduzieren. Es ist damit also durchaus nicht ausgeschlossen, dass es zur ursprünglichen Aufgabe mehr Lösungen als nur die von der Pell-Gleichung kommenden gibt. Tatsächlich gibt es solche Lösungen aber nicht. Wie man das zeigen kann, erfahren wir am Ende dieses Briefes, wenn wir noch einmal auf diese Aufgabe zurückkommen.

4 Diskriminanten und Quadratschachtelungen

Bisher haben wir uns mit ganzzahligen (oder rationalen) Lösungen von quadratischen Gleichungen in *mehreren* Variablen beschäftigt. Sehr einfach ist dagegen der Fall von Gleichungen in nur *einer* Variable. Es gilt nämlich der

Hilfssatz: Sind a, b, c ganze Zahlen, so hat die Gleichung $ax^2 + bx + c = 0$ genau dann eine rationale Lösung x, wenn $b^2 - 4ac$ eine Quadratzahl ist.

Beweis des Hilfssatzes: Quadratische Vervollständigung zeigt, dass die Gleichung äquivalent ist zu $(2ax + b)^2 = b^2 - 4ac$ und die Behauptung folgt sofort. □

Die Zahl $b^2 - 4ac$ wird auch *Diskriminante* der quadratischen Gleichung genannt. Auch (und gerade) für Probleme mit mehreren Variablen ist sie aber nützlich, wie das folgende Beispiel illustriert.

Aufgabe: Finde alle Paare (x, y) ganzer Zahlen mit

$$xy^2 + xy + x^2 - 2y - 1 = 0. \tag{3}$$

Lösung: Dies ist keine quadratische Gleichung im eigentlichen Sinn, denn der Term xy^2 hat Grad 3. Wir können sie aber als quadratische Gleichung in x betrachten, deren Koeffizienten von y abhängen, also

$$x^2 + (y^2 + y)x - (2y + 1) = 0.$$

Soll nun (x, y) eine ganzzahlige Lösung sein, so muss nach unserem Hilfssatz die Diskriminante $D = (y^2 + y)^2 + 4(2y + 1)$ eine Quadratzahl sein. Nun kommt die entscheidende zweite Idee dieses Abschnitts ins Spiel, die der *Quadratschachtelung*. Die Beobachtung ist, dass für betragsmäßig große y die Zahl D sehr nahe bei $(y^2 + y)^2$ (eine Quadratzahl!) ist, jedoch verschieden von dieser ist. Dies sollte also zu einem Widerspruch führen.
Präzise können wir wie folgt argumentieren: Gilt

$$(y^2 + y - 2)^2 < D < (y^2 + y + 2)^2,$$

so kann D keine Quadratzahl sein, denn D ist gerade und die einzige gerade Quadratzahl zwischen $(y^2 + y - 2)^2$ und $(y^2 + y + 2)^2$ ist $(y^2 + y)^2$, allerdings ist diese verschieden von D.
Wir überprüfen nun, für welche Werte von y die Ungleichung gilt. Diese ist äquivalent zu

$$-4y^2 - 4y + 4 < 4(2y + 1) < 4y^2 + 4y + 4.$$

Die rechte Ungleichung ist hier äquivalent zu $y^2 > y$, ist also für $y > 1$ und $y < 0$ erfüllt. Die linke Ungleichung ist äquivalent zu $y^2 + 3y > 0$, ist also für $y > 0$ und $y < -3$ erfüllt. Für alle $y < -3$ und alle $y > 1$ sind also beide Ungleichungen erfüllt und D kann keine Quadratzahl sein. Wir müssen nun nur noch die Fälle $y \in \{-3, -2, -1, 0, 1\}$ ausprobieren. Tatsächlich ist nur für $y = -3, y = 0$ und $y = 1$ die Zahl D eine Quadratzahl. In diesen drei Fällen können wir die resultierende quadratische Gleichung für x lösen und erhalten die sechs Lösungspaare $(-5, -3), (-1, -3), (-1, 0), (1, 0), (-3, 1), (1, 1)$. □

Übung: Wir können die Gleichung (3) auch als quadratische Gleichung in y auffassen. Lässt sich die Aufgabe auch auf diese Weise mithilfe der Diskriminante lösen?

Die Idee der Quadratschachtelung lässt sich auch in anderen Situationen verwenden, um den Lösungsbereich einer Gleichung einzugrenzen. Es ist ein typisches Merkmal dieser Methode, dass sie uns wie in der letzten Aufgabe lediglich gewisse Schranken für den Lösungsbereich liefert und sich eine Fallunterscheidung oft nicht komplett vermeiden lässt. Zum Abschluss betrachten wir allerdings wie versprochen noch eine elegante Anwendung auf die oben besprochene Bundesrunden-Aufgabe, die zeigt, dass wir durch unseren Ansatz dort bereits *alle* Lösungen gefunden haben (dies war in der Aufgabe gar nicht gefragt und war dem Aufgabenausschuss zuvor auch nicht bekannt, wurde aber in einer Schülerlösung gezeigt).

Neben der unbestreitbaren Tatsache, dass es aus ästhetischen Gründen sicherlich sehr zufriedenstellend ist, eine solche Lösung zu finden, hat ein solcher Lösungsansatz auch einen ganz praktischen Vorteil: Auch wenn in der Aufgabe nicht gefordert war, alle Lösungen zu finden, erspart uns der gleich beschriebene Ansatz eine Entscheidung, welche der beiden möglichen Antworten die richtige ist. Wir können also *ergebnisoffen* die Lösungsmenge der Aufgabe untersuchen und dürfen optimistisch sein, in jedem Fall zu einer Lösung der Aufgabe zu gelangen, sei es indem wir am Ende unendlich viele Tripel erhalten, oder indem wir einen Endlichkeitsbeweis erhalten. Nun aber genug der Vorrede.

Aufgabe: Zeige, dass wir bereits alle Lösungen (u, v, w) gefunden haben, für die $uv + 1, uw + 1$ und $vw + 1$ gleichzeitig Quadratzahlen sind.

Lösung (nach einer Idee von Matti Schoss):
Wir erinnern uns, dass wir die Aufgabe darauf reduziert hatten, nach Zahlen v und d mit $v > d$ zu suchen, für die $v^2 - vd + 1, v^2 + vd + 1$ und $v^2 - d^2 + 1$ sämtlich Quadratzahlen sind.

Als Vorüberlegung zeigen wir noch schnell, dass v gerade sein muss. Wäre nämlich v ungerade, so folgte aus einer Betrachtung von $v^2 - d^2 + 1$ modulo 4 leicht, dass auch d ungerade ist, dann lassen aber die ungeraden Quadratzahlen $v^2 - vd + 1$ und $v^2 + vd + 1$ unterschiedliche Reste modulo 4, Widerspruch!

Nach dieser Vorüberlegung kommt nun die erste entscheidende, aber sehr simple Idee, nämlich, dass auch das Produkt

$$N := (v^2 - vd + 1)(v^2 + vd + 1)(v^2 - d^2 + 1)$$

eine Quadratzahl sein muss. Tatsächlich reicht das für alle weiteren Überlegungen schon aus.

Um die Idee der Quadratschachtelung zu verwenden, müssen wir nun eine Quadratzahl finden, die möglichst nahe an N liegt. Dazu sortieren wir nach Potenzen von v und finden nach einer kurzen Rechnung (hier kommt es auch darauf an, sich nicht zu verrechnen!)

$$N = \left(v^3 + \left(\frac{3}{2} - d^2\right) \cdot v\right)^2 + \frac{3v^2}{4} + (1 - d^2) =: s^2 + \frac{3v^2}{4} + (1 - d^2)$$

mit $s = v^3 + \left(\frac{3}{2} - d^2\right) \cdot v$ und beachten, dass wegen $v > d$ sicherlich $s > 0$ gilt und wegen $2 \mid v$ weiterhin s eine ganze Zahl ist. Nun ist

$$(s + 1)^2 = s^2 + 2s + 1 > N$$

wegen

$$2s = 2v^3 + 3v - 2d^2v > \frac{3v^2}{4} - d^2,$$

was äquivalent zu

$$d^2(2v-1) < 2v^3 - \frac{3v^2}{4} + 3v$$

ist und leicht aus

$$d^2(2v-1) < v^2(2v-1) = 2v^3 - v^2 < RHS$$

folgt. Analog ist

$$(s-1)^2 = s^2 - 2s + 1 < N$$

wegen

$$2s = 2v^3 + 3v - 2d^2v > d^2 - \frac{3v^2}{4},$$

was äquivalent zu

$$2v^3 + \frac{3v^2}{4} + 3v > d^2(2v+1)$$

ist und leicht aus

$$d^2(2v+1) \leq (v-1)^2(2v+1) = 2v^3 - 3v^2 + 1 < LHS$$

folgt. Damit haben wir $(s-1)^2 < N < (s+1)^2$ gezeigt und es folgt $N = s^2$, also

$$\frac{3v^2}{4} + (1 - d^2) = 0$$

und damit $d^2 = 3\left(\frac{v}{2}\right)^2 + 1$, was genau die Pell-Gleichung ist. □