und wie wir ebenfalls aus Kapitel III wissen, ist

$$\det M = p_{n-2}q_{n-1} - q_{n-2}p_{n-1} = (-1)^{n-1} .$$

Somit sind die Vektoren $\binom{\alpha}{1}$ und $M\binom{\alpha_n}{1}$ proportional zueinander.

Als quadratische Irrationalität genügt α einer quadratischen Gleichung $A\alpha^2 + B\alpha + C = 0$; der Vektor $\binom{\alpha}{1}$ wird also von der quadratischen Form $Ax^2 + Bxy + Cy^2$ annulliert. Da mit $\binom{x}{y}$ auch alle Vielfachen dieses Vektors dieselbe Gleichung erfüllen, gilt dasselbe für den dazu proportionalen Vektor $M\binom{\alpha_n}{1}$.

Die Matrix zu dieser quadratischen Form sei Q. Wie wir aus dem vorigen Paragraphen wissen, erfüllen die Komponenten von $M\binom{\alpha_m}{1}$ dann die quadratische Gleichung zur Form mit Matrix ${}^tMQM$, die zu der mit Q äquivalent ist und somit dieselbe Diskriminante hat. Also haben alle α_n dieselbe Diskriminante wie α, denn da Multiplikation mit M einen Isomorphismus $\mathbb{Z}^2 \to \mathbb{Z}^2$ definiert, sind die Einträge von Q genau dann ganzzahlig und teilerfremd, wenn es die von ${}^tMQM$ sind.

Dies ist ein wesentlicher Schritt für den Beweis des folgenden Satzes:

Satz (LAGRANGE ∼1766): Die Kettenbruchentwicklung einer irrationalen Zahl α ist genau dann periodisch, wenn α eine quadratische Irrationalzahl ist.

Beweis: Angenommen, α hat eine periodische Kettenbruchentwicklung. Dann gibt es ein n und ein $k > 0$, so daß $\alpha_{n+k} = \alpha_n$ ist. Nach der Formel am Ende von §2 von Kapitel III ist daher

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}} = \frac{\alpha_{n+k} p_{n+k-2} + p_{n+k-1}}{\alpha_{n+k} q_{n+k-2} + q_{n+k-1}} = \frac{\alpha_n p_{n+k-2} + p_{n+k-1}}{\alpha_n q_{n+k-2} + q_{n+k-1}} .$$

Daraus folgt die Gleichheit von $(\alpha_n p_{n-2} + p_{n-1})(\alpha_n q_{n+k-2} + q_{n+k-1})$ und $(\alpha_n q_{n-2} + q_{n-1})(\alpha_n p_{n+k-2} + p_{n+k-1})$, und ausmultipliziert wird dies zu einer quadratischen Gleichung für α_n. Der Koeffizient von α_n^2 ist $p_{n-2}q_{n+k-2} + q_{n-2}p_{n+k-2}$, was als Summe positiver Zahlen nicht null sein kann; wir haben also eine echte quadratische Gleichung. Somit läßt sich α_n in der Form $\alpha = r + s\sqrt{D}$ schreiben, und damit auch

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}} .$$

Umgekehrt sei $\alpha = r + s\sqrt{D}$ mit quadratfreiem D eine quadratische Irrationalität, die der Gleichung $A_0\alpha^2 + B_0\alpha + C_0 = 0$ genüge. Dann zeigt die Konstruktionsvorschrift für die α_n, daß auch diese Zahlen sowie ihre Inversen in entsprechender Form geschrieben werden können und damit Gleichungen der Form

$$A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$$

genügen. Diese Gleichung können wir uns explizit verschaffen, indem wir

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}}$$

in die Gleichung $f(\alpha) = A_0\alpha^2 + B_0\alpha + C_0 = 0$ einsetzen und mit dem Nenner multiplizieren. Zumindest für die Koeffizienten A_n und C_n ergeben sich einigermaßen erträgliche Formeln:

$$A_n = A_0 p_{n-1}^2 + B_0 p_{n-1}q_{n-1} + C_0 q_{n-1}^2 = q_{n-1}^2 f\left(\frac{p_{n-1}}{q_{n-1}}\right)$$

und

$$C_n = A_0 p_{n-2}^2 + B_0 p_{n-2}q_{n-2} + C_0 q_{n-2}^2 = q_{n-2}^2 f\left(\frac{p_{n-2}}{q_{n-2}}\right) .$$

Da f eine quadratische Funktion ist, führt die TAYLOR-Entwicklung um α auf die Formel

$$f\left(\frac{p_{n-1}}{q_{n-1}}\right) = f(\alpha) + f'(\alpha)\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right) + \frac{f''(\alpha)}{2}\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)^2 .$$

Hierbei ist $f(\alpha) = 0$, und $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < 1/q_{n-1}^2 \le 1$. Somit ist

$$|A_n| \le |f'(\alpha)| + |f''(\alpha)| .$$

Genauso zeigt man die Ungleichung $|C_n| \le |f'(\alpha)| + |f''(\alpha)|$. Somit sind die Beträge der Koeffizienten A_n und C_n beschränkt durch eine von n unabhängige Konstante.

Wie wir oben gesehen haben, hat α_n dieselbe Diskriminante wie α; die Diskriminante $\Delta = B_n^2 - 4A_nC_n$ hängt also nicht ab von n. Daher folgen aus der obigen Schranken für A_n und C_n auch Schranken für $B_n^2 = \Delta + 4A_nC_n$, so daß auch der Betrag von B_n beschränkt ist.

Somit gibt es nur endlich viele Tripel (A_n, B_n, C_n), also auch nur endlich viele verschiedene Werte für α_n. Es muß daher zwei Zahlen n, k mit $k \geq 1$ geben derart, daß $\alpha_n = \alpha_{n+k}$ ist, und die Kettenbruchentwicklung wird spätestens ab der n-ten Stelle periodisch.

■

Der gerade bewiesene Satz charakterisiert Zahlen, deren Kettenbruchentwicklung periodisch *wird;* er besagt nicht, daß die Kettenbruchentwicklung einer quadratischen Irrationalität von Anfang an periodisch ist, und in der Tat kennen wir ja Beispiele wie

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}}}}}$$

oder

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \dots}}}},$$

bei denen das nicht der Fall ist. Für eine rein periodische Kettenbruchentwicklung brauchen wir also noch zusätzliche Bedingungen:

Satz: Die Kettenbruchentwicklung von α ist genau dann rein periodisch, wenn $\alpha > 1$ ist und sein konjugiertes Element $\overline{\alpha}$ zwischen -1 und 0 liegt.

Beweis: Sei zunächst $\alpha > 1$ und $-1 < \overline{\alpha} < 0$. Der Trick zum Beweis der reinen Periodizität der Folge der c_i besteht darin, die $c_i = [1/\alpha_i]$ durch die konjugierten Elemente $\overline{\alpha}_i$ auszudrücken.

Die Gleichung $\alpha = c_0 + \alpha_1$ wird, da c_0 eine rationale Zahl ist, durch Konjugation zu $\overline{\alpha} = c_0 + \overline{\alpha}_1$. Da $\overline{\alpha}$ nach Voraussetzung zwischen -1 und 0 liegt, ist somit

$$0 < -\overline{\alpha}_1 - c_0 < 1 \quad \text{und} \quad c_0 = [-\overline{\alpha}_1]\,.$$

Wegen $c_0 = [\alpha] \geq 1$ folgt außerdem $-1 < \dfrac{1}{\overline{\alpha}_1} < 0$.

Wir wollen induktiv zeigen, daß auch für alle $i > 0$ gilt

$$c_i = [-\overline{\alpha}_{i+1}] \quad \text{und} \quad -1 < \frac{1}{\overline{\alpha}_{i+1}} < 0\,.$$

Dazu nehmen wir an, dies gelte für $i - 1$. Aus

$$\frac{1}{\alpha_i} = c_i + \alpha_{i+1} \quad \text{und} \quad -1 < \frac{1}{\overline{\alpha}_i} < 0$$

folgt wie im Fall $i = 0$, daß $c_i = [-\alpha_{i+1}]$ ist, und da die Koeffizienten c_i für $i > 0$ bei jeder Kettenbruchentwicklung mindestens gleich eins sind, folgt auch die Ungleichung für $1/\overline{\alpha}_{i+1}$ genau wie dort.

Daraus folgt nun leicht die Periodizität der Kettenbruchentwicklung von α: Wir wissen bereits, daß sie periodisch *wird;* es gibt also irgendeinen Index $m \geq 0$ und eine Periode k, so daß $\alpha_{n+k} = \alpha_n$ für alle $n \geq m$. Wir betrachten das minimale m mit dieser Eigenschaft. Die Kettenbruchentwicklung von α ist genau dann rein periodisch, wenn $m = 0$ ist. Für $m \geq 1$ können wir aber aus $\alpha_{m+k} = \alpha_m$ und $c_{m+k} = c_m$ folgern, daß auch

$$c_{m+k-1} = [-\overline{\alpha}_{m+k}] = [-\overline{\alpha}_m] = c_{m-1}$$

ist. Aus den Gleichungen

$$\frac{1}{\alpha_{m+k-1}} = c_{m+k-1} + \alpha_{m+k} \quad \text{und} \quad \frac{1}{\alpha_{m-1}} = c_{m-1} + \alpha_m$$

folgt dann aber, daß auch $\alpha_{m-1+k} = \alpha_{m-1}$ ist, im Widerspruch zur Minimalität von m. Somit ist $m = 0$, die Kettenbruchentwicklung von α also rein periodisch.

Umgekehrt habe α eine rein periodische Kettenbruchentwicklung der Periode k mit Koeffizienten $c_0, c_1, \dots$. Wegen $c_k = c_0$ ist dabei auch c_0 positiv, denn alle c_n mit $n > 0$ müssen ja positiv sein. Somit ist insbesondere $\alpha > 1$.

Um zu sehen, daß $\overline{\alpha}$ zwischen -1 und 0 liegt, beachten wir, daß $\overline{\alpha}$ dieselbe quadratische Gleichung erfüllt wie α. Da diese Gleichung genau

zwei Nullstellen hat und α größer als eins ist, genügt es, wenn wir zeigen, daß diese Gleichung im Intervall $(-1,\ 0)$ eine Nullstelle hat. Das wiederum folgt aus dem Zwischenwertsatz, wenn wir zeigen können, daß die quadratische Funktion auf der linken Seite an den Stellen 0 und -1 Werte mit entgegengesetzten Vorzeichen annimmt.

Für $k = 1$ ist

$$\alpha = a_0 + \alpha_1 = c_0 + \frac{1}{\alpha} \Longrightarrow \alpha^2 - c_0\alpha - 1 = 0\,.$$

Die quadratische Funktion $x^2 - c_0x - 1$ nimmt an der Stelle 0 den Wert -1 an, und bei $x = 1$ den Wert $c_0 > 0$; somit gibt es eine Nullstelle zwischen diesen beiden Punkten.

Für $k \geq 2$ verwenden wir die bereits im vorigen Satz benutzte Formel aus Kapitel III, §2, und beachten, daß $\alpha_k = 1/\alpha$ ist. Dies führt auf die Gleichung

$$\alpha = \frac{\alpha_k p_{k-2} + p_{k-1}}{\alpha_k q_{k-2} + q_{k-1}} = \frac{p_{k-2} + p_{k-1}\alpha}{q_{k-2} + q_{k-1}\alpha}\,.$$

Überkreuzmultiplikation macht daraus die quadratische Gleichung

$$q_{k-1}\alpha^2 + (q_{k-2} - p_{k-2}\alpha - p_{k-1} = 0\,.$$

Hier nimmt die quadratische Funktion bei 0 den Wert $-p_{k-2} < 0$ an, und an der Stelle -1 den Wert

$$q_{k-1} - q_{k-2} + p_{k-2} - p_{k-1} = (q_{k-1} - q_{k-2}) + (p_{k-2} - p_{k-1})\,.$$

Dieser ist positiv, da sowohl die Folge der Zähler als auch die der Nenner der Konvergenten von α monoton steigt.

Damit ist der Satz vollständig bewiesen. ∎

§6: Die Pellsche Gleichung

Im letzten Kapitel hatten wir gesehen, daß eine Einheit $x+y\sqrt{D}$ von $\mathcal{O}_D$ die Gleichung $x^2 - Dy^2 = \pm 1$ erfüllen muß. Hauptziel dieses Paragraphen ist die Lösung der PELLschen Gleichung

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

für $(x, y) \in \mathbb{Z}^2$ oder –da es auf das Vorzeichen von x und y nicht ankommt– $(x, y) \in \mathbb{N}^2$.

Faktorisierung der linken Seite der PELLschen Gleichung führt auf

$$(x + y\sqrt{D})(x - y\sqrt{D}) = 1\,,$$

und damit ist

$$x - y\sqrt{D} = \frac{1}{x + y\sqrt{D}} \Longrightarrow \frac{x}{y} - \sqrt{D} = \frac{1}{y^2\left(\frac{x}{y} + \sqrt{D}\right)}\,.$$

Wegen der Positivität der rechten Seite ist $\frac{x}{y} > \sqrt{D}$, also folgt

$$\left|x - y\sqrt{D}\right| = x - y\sqrt{D} = \frac{1}{y^2\left(\frac{x}{y} + \sqrt{D}\right)} < \frac{1}{2y^2\sqrt{D}} < \frac{1}{2y^2}\,.$$

Nach dem Satz aus Kapitel III, §3 muß $\frac{x}{y}$ somit eine Konvergente der Kettenbruchentwicklung von $\sqrt{D}$ sein.

Umgekehrt liefert aber nicht jede Konvergente der Kettenbruchentwicklung von $\sqrt{D}$ eine Lösung der PELLschen Gleichung: Beispielsweise hat

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cdots}}}}}\,,$$

die Brüche

$$\frac{4}{1},\quad \frac{7}{2},\quad \frac{11}{3},\quad \frac{18}{5},\quad \frac{119}{33}$$

als seine ersten Konvergenten, aber

$$4^2 - 13 = 3,\quad 7^2 - 13\cdot 2^2 = -3,\quad 11^2 - 13\cdot 3^2 = 4$$
$$18^2 - 13\cdot 5^2 = -1 \quad \text{und} \quad 119^2 - 13\cdot 33^2 = 4\,.$$

Zumindest *a priori* ist nicht klar, ob es überhaupt eine Konvergente gibt, die auf eine Lösung der PELLschen Gleichung führt.

Um hier mehr zu erfahren, müssen wir uns die Kettenbruchentwicklung von $\sqrt{D}$ genauer ansehen. Dabei sei D im folgenden stets eine quadratfreie natürliche Zahl.

Das konjugierte Element zu $\sqrt{D}$ ist $-\sqrt{D}$ und somit kleiner als -1; die Kettenbruchentwicklung von $\sqrt{D}$ ist also nicht rein periodisch. Betrachten wir aber $\alpha = \lfloor\sqrt{D}\rfloor + \sqrt{D}$, so ist natürlich $\alpha > 1$. und $\overline{\alpha} = \lfloor\sqrt{D}\rfloor - \sqrt{D}$ liegt zwischen -1 und 0. Somit hat α eine rein periodische Kettenbruchentwicklung. Die Periode sei k und die Koeffizienten seien $c_0, c_1, \ldots$.

Die Kettenbruchentwicklung von $\sqrt{D} = \alpha - \lfloor\sqrt{D}\rfloor$ unterscheidet sich von der von α nur im ganzzahligen Anteil. Dieser ist im Falle von α gleich $2\lfloor\sqrt{D}\rfloor$, im Falle von $\sqrt{D}$ nur $\lfloor\sqrt{D}\rfloor$. Danach folgen in beiden Fällen die c_i mit $i \geq 1$. Wegen $c_k = c_0 = 2\lfloor\sqrt{D}\rfloor$ gilt daher

Satz: Ist D eine quadratfreie natürliche Zahl, so ist die Folge $c_0, c_1, \ldots$ der Koeffizienten der Kettenbruchentwicklung von $\sqrt{D}$ ab c_1 periodisch. Bezeichnet k die Periode, so ist $c_k = 2c_0 = 2\lfloor\sqrt{D}\rfloor$. ∎

Bezeichnet p_n/q_n wieder die n-te Konvergente dieser Kettenbruchentwicklung, so ist nach der schon oft benutzten Formel

$$\sqrt{D} = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}} .$$

Ist speziell $n = rk$ ein Vielfaches einer Periode, hat $1/\alpha_n$ eine Kettenbruchentwicklung mit Koeffizienten $c_{rk}, c_{rk+1}, c_{rk+2}, \ldots$; nach dem gerade bewiesenen Satz stimmt das überein mit der Folge $2c_0, c_1, c_2, \ldots$, d.h.

$$\frac{1}{\alpha_{rk}} = c_0 + \sqrt{D} = \lfloor\sqrt{D}\rfloor + \sqrt{D} .$$

Einsetzen in die obige Formel führt auf

$$\sqrt{D} = \frac{\alpha_{rk} p_{rk-2} + p_{rk-1}}{\alpha_{rk} q_{rk-2} + q_{rk-1}} = \frac{p_{rk-2} + p_{rk-1}\left(c_0 + \sqrt{D}\right)}{q_{rk-2} + q_{rk-1}\left(c_0 + \sqrt{D}\right)}$$

oder

$$(q_{rk-2} + q_{rk-1}c_0)\sqrt{D} + q_{rk-1}D = (p_{rk-2} + p_{rk-1}c_0) + p_{rk-1}\sqrt{D} .$$

Durch Koeffizientenvergleich folgt:

$$p_{rk-2} = q_{rk-1}D - p_{rk-1}c_0 \quad \text{und} \quad q_{rk-2} = p_{rk-1} - q_{rk-1}c_0 .$$

Setzen wir dies ein in die aus Kapitel III, §2, bekannte Formel

$$p_m q_{m-1} - q_m p_{m-1} = (-1)^{m-1}$$

mit $m = rk - 1$, erhalten wir die Gleichung

$$\begin{aligned} &p_{rk-1}^2 - p_{rk-1}q_{rk-1}c_0 - q_{rk-1}^2 D + q_{rk-1}p_{rk-1}c_0 \\ &\quad = p_{rk-1}^2 - Dq_{rk-1}^2 = (-1)^{rk-2} . \end{aligned}$$

Im Falle einer geraden Periode k ist somit (p_{kr-1}, q_{kr-1}) für jedes $r \in \mathbb{N}$ eine Lösung der PELLschen Gleichung ; für ungerade Perioden liefern nur die geradzahligen Vielfachen von k Lösungen, während die ungeradzahligen zu Lösungen der Gleichung $x^2 - Dy^2 = -1$ führen.

Im Eingangsbeispiel $D = 13$ zeigt eine genauere Rechnung, daß sich die Koeffizienten $1, 1, 1, 1, 6$ periodisch wiederholen, wir haben also die ungerade Periode fünf. Damit liefern die vierte, vierzehnte, vierundzwanzigste Konvergente der Kettenbruchentwicklung Lösungen der Gleichung $x^2 - Dy^2 = -1$, was wir für die vierte bereits nachgerechnet haben. Lösungen der PELLschen Gleichung liefern die neunte, neunzehnte *usw.* Konvergente. Die neunte Konvergente ist

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}}} = \frac{649}{180} ,$$

und in der Tat ist

$$649^2 - 13 \cdot 180^2 = 421\,201 - 13 \cdot 32\,400 = 421\,201 - 421\,200 = 1 .$$

Allgemein haben wir gezeigt, daß die PELLsche Gleichung für jedes quadratfreie D eine Lösung hat; zusammen mit dem Satz aus Kapitel IV, §6 folgt, daß die Einheitengruppe eines jeden reellquadratischen

Zahlkörpers unendlich ist und daß es speziell für die Gruppe der Einheiten mit Norm eins (der sogenannten Einseinheiten) ein Element $\alpha \in \mathcal{O}_D$ gibt, so daß jede Einseinheit in der Form $\pm\alpha^r$ mit einem $r \in \mathbb{Z}$ geschrieben werden kann. α ist die kleinste Einseinheit größer eins.

Natürlich kann auch α in der Form $p_n + q_n\sqrt{D}$ geschrieben werden, wobei p_n/q_n eine Konvergente der Kettenbruchentwicklung von $\sqrt{D}$ ist. Da Zähler und Nenner der Konvergenten strikt monoton ansteigen mit n, handelt es sich hier um die *erste* Konvergente p_n/q_n, für die $p_n^2 - Dq_n^2 = 1$ ist.

Mit Rechnungen, die sehr ähnlich zu den obigen sind, kann man zeigen, daß die oben gefundenen Indizes m mit $p_m^2 - Dq_m^2 = \pm 1$ tatsächlich die einzigen sind mit dieser Eigenschaft. Da wir schon viel mit Kettenbrüchen gerechnet haben und es noch viele andere interessante Teilgebiete der Zahlentheorie zu entdecken gilt, möchte ich auf diese Rechnungen verzichten.

Wer sich für diese Rechnungen interessiert, findet sie zum Beispiel in

WINFRIED SCHARLAU, HANS OPOLKA: Von Fermat bis Minkowski – Eine Vorlesung über Zahlentheorie und ihre Entwicklung, *Springer*, 1980

im Kapitel über LAGRANGE im (nur im Inhaltsverzeichnis benannten) Paragraphen *Lösung der Fermatschen (Pellschen) Gleichung* ab Seite 64. Es gibt zwar Rückverweise, aber wer den obigen Beweis verstanden hat, muß nur einem wirklich folgen. Zu beachten sind die unterschiedlichen Bezeichnungen: Was hier α heißt, ist dort θ, aber das dortige θ_n ist hier $1/\alpha_n$. Die hießigen c_n werden dort mit a_n bezeichnet.

Wenn wir dieses Ergebnis akzeptieren, können wir die Einheitengruppe eines jeden reellquadratischen Zahlkörpers $\mathbb{Q}[\sqrt{D}]$ explizit berechnen, zumindest für $D \not\equiv 1 \bmod 4$: Dann ist $\mathcal{O}_D = \mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$, so daß die Einheiten genau den ganzzahligen Lösungen der beiden Gleichungen $x^2 - Dy^2 = \pm 1$ entsprechen. Ist k die Periode der Kettenbruchentwicklung von $\sqrt{D}$ und p/q die $(k-1)$-te Konvergente, so ist $\alpha = p + q\sqrt{D}$ die Grundeinheit, und jede andere Einheit läßt als $\pm\alpha^r$ mit einem $r \in \mathbb{Z}$ schreiben. Für gerades k sind dies alles Einseinheiten, für ungerades k bekommen wir für gerade r Einseinheiten und sonst Einheiten der Norm -1.

Bleibt die Frage, für welche D die Periode k gerade *bzw.* ungerade ist.

Diese Frage muß nicht nur in dieser Vorlesung unbeantwortet bleiben: Es handelt sich hier um eines der vielen zahlentheoretischen Probleme, die trotz jahrhundertelanger Bemühungen auch heute noch offen sind.

Die zweite Frage ist: Was passiert für $D \equiv 1 \bmod 4$? Wie wir wissen, sind dann auch die Zahlen $\frac{1}{2}(x + y\sqrt{D})$ für ungerade ganze Zahlen x, y ganz, es kann also auch Einheiten dieser Form geben. In der Tat haben wir beim Eingangsbeispiel $D = 13$ bereits solche Fälle kennengelernt: Für die dritte Konvergente $11/4$ ist $11^2 - 13 \cdot 3^2 = 4$, d.h.

$$\mathrm{N}\left(\tfrac{1}{2}(11 + 3\sqrt{13})\right) = 1\,.$$

Wie eine genauere Untersuchung zeigt, ist dies genau dann möglich, wenn $D \equiv 5 \bmod 8$, jedoch nicht für alle solche D. Wenn es eine Grundeinheit dieser Form gibt, liegt ihre dritte Potenz in $\mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$, der Kettenbruchalgorithmus gibt dann also nur die dritte Potenz der Grundeinheit. Einzelheiten findet man beispielsweise in §16, 5D des Buchs

HELMUT HASSE: Vorlesungen über Zahlentheorie, *Springer*, ^{2}1964.

Kapitel 6
Quadratische Reste

§1: Das Legendre-Symbol

Definition: Für eine Primzahl p und eine nicht durch p teilbare natürliche Zahl a ist das LEGENDRE-Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls es ein } x \in \mathbb{N} \text{ gibt mit } x^2 \equiv a \bmod p \\ -1 & \text{sonst} \end{cases}$$

Im ersten Fall bezeichnen wir a als *quadratischen Rest* modulo p, andernfalls als quadratischen Nichtrest. Für eine durch p teilbare Zahl a setzen wir $\left(\frac{a}{p}\right) = 0$.

Sind a, b zwei modulo p kongruente natürliche Zahlen, so ist offensichtlich $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Wir haben daher auch für $a \in \mathbb{F}_p^\times$ ein wohldefiniertes LEGENDRE-Symbol $\left(\frac{a}{p}\right)$, das durch die Vorschrift $\left(\frac{0}{p}\right) = 0$ auf ganz $\mathbb{F}_p$ fortgesetzt wird.

ADRIEN-MARIE LEGENDRE (1752–1833) wurde in Toulouse oder Paris geboren; jedenfalls ging er in Paris zur Schule und studierte Mathematik und Physik am dortigen Collège Mazarin. Ab 1775 lehrte er an der Ecole Militaire und gewann einen Preis der Berliner Akademie für eine Arbeit über die Bahn von Kanonenkugeln. Andere Arbeiten befaßten sich mit der Anziehung von Ellipsoiden und der Himmelsmechanik. Ab etwa 1785 publizierte er auch Arbeiten über Zahlentheorie, in denen er z.B. das quadratische Reziprozitätsgesetz bewies sowie die Irratinalität von π und π^2.

Lemma: Das LEGENDRE-Symbol definiert einen Gruppenhomomorphismus

$$\left(\frac{\cdot}{p}\right) : \begin{cases} \mathbb{F}_p^\times \to \{+1, -1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{cases} .$$

Für $p = 2$ ist dies der triviale Homomorphismus, für ungerade p ist er surjektiv. Insbesondere gibt es dann jeweils $\frac{p-1}{2}$ quadratische Reste und Nichtreste.

Beweis: Für $p = 2$ ist $\mathbb{F}_2^\times = \{1\}$, und $1 = 1^2$ ist ein quadratischer Rest.

Sei nun p ungerade. Der Homomorphismus

$$\begin{cases} \mathbb{F}_p^\times \to \mathbb{F}_p^\times \\ x \mapsto x^2 \end{cases}$$

hat den Kern $\{+1, -1\}$, also besteht das Bild aus $\frac{p-1}{2}$ Elementen, den quadratischen Resten.

Trivialerweise ist das Produkt zweier quadratischer Reste wieder ein quadratischer Rest. Ist $a = x^2$ ein quadratischer Rest und b ein Nichtrest, so ist auch ab ein quadratischer Nichtrest, denn wäre $ab = y^2$, wäre $b = (yx^{-1})^2$ ein quadratischer Rest. Da Multiplikation mit b injektiv ist, folgt, daß sich jeder quadratische Nichtrest in der Form bc darstellen läßt, wobei c ein quadratischer Rest ist. Damit folgt, daß das Produkt zweier quadratischer Nichtreste ein quadratischer Rest ist, denn $bc \cdot bd = b^2cd$, wobei c und d Quadrate in $\mathbb{F}_p^\times$ sind.

■

Lemma(EULER): Für ungerades p ist und $a \in \mathbb{F}_p^\times$ ist $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Beweis: g sei ein erzeugendes Element von $\mathbb{F}_p^\times$. Dann ist offensichtlich jede Potenz g^r mit geradem r ein quadratischer Rest, und da es genau $\frac{p-1}{2}$ verschiedene solcher Potenzen gibt, sind das auch *alle* quadratischen Reste. Somit ist g^r genau dann ein quadratischer Rest, wenn r gerade ist.

Da g ein erzeugendes Element ist, kann $g^{(p-1)/2}$ nicht gleich eins sein; da nach dem kleinen Satz von FERMAT aber sein Quadrat $g^{p-1} = 1$ ist, folgt $g^{(p-1)/2} = -1$. Für $a = g^r$ ist somit

$$a^{\frac{p-1}{2}} = (g^r)^{\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}}\right)^r = (-1)^r$$

genau dann gleich eins, wenn a ein quadratischer Rest ist, und -1 sonst. ∎

Korollar: Für ungerades p ist

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}.$$

∎

§2: Das quadratische Reziprozitätsgesetz

Quadratisches Reziprozitätsgesetz: Für zwei verschiedene ungerade Primzahlen p, q ist

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Zum *Beweis* betrachten wir ein zum Nullpunkt symmetrisches Vertretersystem von $\mathbb{F}_p^\times$ in $\mathbb{Z}$, nämlich

$$R = \{-h, \ldots, -1, 1, \ldots, h\} \quad \text{mit} \quad h = \frac{p-1}{2}.$$

Weiter sei $S = \{q, 2q, \ldots, hq\}$. Da p und q teilerfremd sind, haben zwei verschiedene Elemente von S verschiedene Restklassen modulo p.

1. Schritt (GAUSS): q sei eine beliebige Primzahl und $p \neq q$ eine ungerade Primzahl. Dann ist $\left(\frac{q}{p}\right) = (-1)^m$, wobei m die Anzahl jener Elemente von S bezeichnet, die modulo p kongruent sind zu einem negativen Element von R.

Beweis: $a_1, \ldots, a_m$ seien die negativen Elemente von R, die zu Elementen aus S kongruent sind, $b_1, \ldots, b_n$ die positiven. Dann ist

$$a_1 \cdots a_m b_1 \cdots b_n \equiv \prod_{i=1}^{h} (iq) = h! q^h \bmod p.$$

Natürlich sind a_i und a_j für $i \neq j$ zwei verschiedene Zahlen, genauso auch b_i und b_j. Außerdem kann auch nie $|a_i| = |b_j|$ sein, denn sonst wäre einerseits $a_i + b_j = 0$, andererseits gäbe es aber Zahlen $1 \leq k, \ell \leq h$, so daß $a_i \equiv kq$ und $b_j \equiv \ell q \bmod p$. Also wäre $(k + \ell)q$ durch p teilbar, was nicht möglich ist, denn $k + \ell \leq 2h = p - 1$. Damit sind die Beträge der a_i und der b_j genau die Zahlen von 1 bis h, d.h.

$$a_1 \cdots a_m b_1 \cdots b_n = (-1)^m h!.$$

Vergleich mit der obigen Konguenz zeigt, daß dann $q^h \equiv (-1)^m \bmod p$ ist, also nach dem vorigen Lemma $\left(\frac{q}{p}\right) = (-1)^m$. ∎

2. Schritt (GAUSS): Für zwei ungerade Primzahlen $p \neq q$ ist

$$\left(\frac{q}{p}\right) = (-1)^M \quad \text{mit} \quad M = \sum_{i=1}^{h} \left[\frac{iq}{p}\right] \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Im *Beweis* sei zunächst auch noch der Fall $q = 2$ zugelassen. Für $i \leq h$ sei $\frac{r_i = iq - p \cdot \left[\frac{iq}{p}\right]}{}$; dann ist $0 \leq r_i < p$ und $\frac{iq = p \cdot \left[\frac{iq}{p}\right] + r_i}{}$. Falls iq modulo p kongruent ist zu einem negativen Element $a_j \in R$, ist also $r_i = p + a_j$; falls $r_i \equiv b_j > 0$ ist dagegen $r_i = b_j$. Somit ist

$$\sum_{i=1}^{h} iq = p \sum_{i=1}^{h} \left[\frac{iq}{p}\right] + \sum_{i=1}^{m} (a_i + p) + \sum_{i=1}^{n} b_i = pM + mp + \sum_{i=1}^{m} a_i + \sum_{i=1}^{n} b_i.$$

Andererseits ist

$$\sum_{i=1}^{h} iq = \frac{h(h+1)}{2} \cdot q = \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot q = \frac{p^2-1}{8} \cdot q.$$

Außerdem wissen wir aus dem ersten Schritt, daß

$$\{-a_1, \ldots, -a_m, b_1, \ldots, b_n\} = \{1, \ldots, h\}$$

ist, d.h.

$$-\sum_{i=1}^{m} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{h} i = \frac{h(h+1)}{2} = \frac{p^2-1}{8}$$