1 Entdeckungen an goldenen Dreiecken

„Man muss auch verstehen was man weiß“

„Wer mehr weiß, als er verstehen kann, ist genauso ein Dummkopf wie der, der nichts weiß“

1.1 Bilder

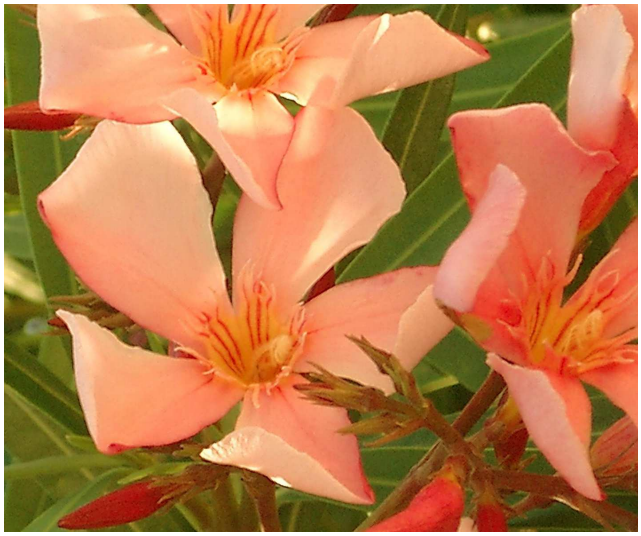


Fig. 1.1: Fünfecke

In der Natur kommen häufig reguläre Fünfecke vor. Gleichschenklige Dreiecke mit Basiswinkel 72° sind Lieblingskinder der Natur.

1.2 Goldene Dreiecke

1.2.1 Wechselwegnahme. Nicht alles ist Zahl.

Die Göttin Arithmetica war geschmeichelt als ihr Priester – von ihr und ihrer Schwester Musica erleuchtet – verkündete:

„Alles ist Zahl“

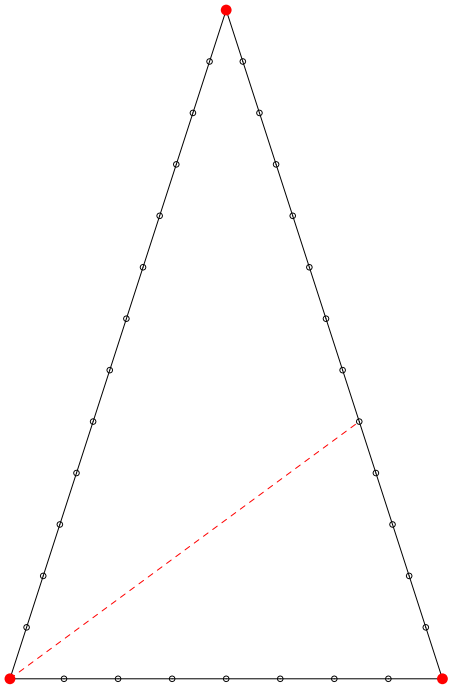


Fig. 1.2: goldene Dreiecke

Gern zählte sie an ihren fünf Fingern ab. So gefiel ihr auch besonders das Logo, welches sich ihr Jünger für seinen Geheimbund aussuchte. Das reguläre Fünfeck. Die Natur liebt dies Fünfecke. Unzählige Blüten, Meerestiere formen sich nach diesem Muster. Im regulären Fünfeck bilden die Diagonalen und die Seite ein gleichschenkliges Dreieck mit Basiswinkel 72°. Wir wollen ein solches Dreieck *goldenes Dreieck* nennen. Hippasos war ein junger Schüler des Meisters Pythagoras. Er wanderte zu seiner morgentlichen einsamen Meditation – die Ordensregel schrieb das vor– ans Meer. Er hatte sich vorgenommen über solche goldenen Dreiecke nachzudenken. Wir begleiten den Hippasos an den Strand und versuchen mit gleich großen Bausteinen solche Dreieck zu legen. Kann ich mit gleich großen kreisrunden Steinen die Seiten eines solchen Dreiecks auslegen? Wir können es mit Streichhölzern oder unsern Magnetbausteinen versuchen. Wir erhalten beispielsweise mit der Basis 8 und dem Schenkel 13 das Dreieck nebenan. Aber ist es wirklich ein goldenes Dreieck? Messen wir den Winkel mit dem Geodreieck, so ist die Antwort ja. Aber messen ist schwierig. Sicher ist nur, dass das Ergebnis nur ungefähr richtig, also vor der unerbittlichen Wahrheit falsch ist. Wie kann man mit Mitteln der 8ten Klasse – ohne Ähnlichkeitslehre – nachweisen, dass unser Dreieck kein goldenes ist? Sehr hilfreich ist die folgende Feststellung von Hippasos.

Satz 1. *Ist ein gleichschenkliges Dreieck mit der Basis x und den Schenkeln y ein goldenes Dreieck, so auch das Dreieck mit der Basis $y - x$ und den Schenkeln x.*

Es sei F der Schnittpunkt der Winkelhalbierenden von $\angle BAD$ mit BD. Dann ist $\angle BAF = 36° = \angle ADB$. Da der $\angle ABD = 72°$ ist ergibt die Winkelsumme im Dreieck, dass $\angle BFA$ auch $72°$ ist. Daher ist auch $\triangle BFA$ ein goldenes Dreieck, wegen dem Satz über die Gleichheit der Basiswinkel. Auch das $\triangle AFD$ ist gleichschenklig. Daher ist $\overline{DF} = x$. Es folgt: Das $\triangle BFA$ hat die Basis $y - x$ und den Schenkel x und ist ein goldenes Dreieck. □

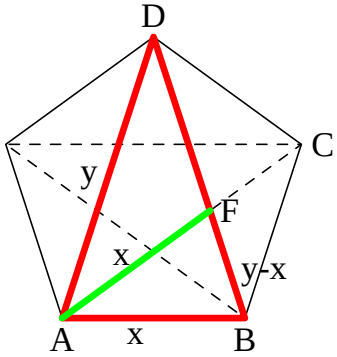


Fig. 1.3: Pentagramm

Diese Entdeckung des Hippasos wenden wir auf das Dreieck $\begin{pmatrix} 8 \\ 13 \end{pmatrix}$ an. In der ersten Komponente steht die Basislänge und in der zweiten Komponente steht die Schenkellänge. Angenommen $\begin{pmatrix} 8 \\ 13 \end{pmatrix}$ ist golden. Dann auch $\begin{pmatrix} 5 \\ 8 \end{pmatrix}$. Den Gedanken wiederholen wir und erhalten die folgende Kette

$$\begin{pmatrix} 8 \\ 13 \end{pmatrix} \to \begin{pmatrix} 5 \\ 8 \end{pmatrix} \to \begin{pmatrix} 3 \\ 5 \end{pmatrix} \to \begin{pmatrix} 2 \\ 3 \end{pmatrix} \to \begin{pmatrix} 1 \\ 2 \end{pmatrix} \to \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Ein Dreieck mit Basis 1 und Schenkellänge 1 ist aber gleichseitig und hat daher den Basiswinkel 60°. Also war auch das ursprüngliche Dreieck nicht golden.
Jetzt wollen wir es erzwingen. Wir zeichnen zuerst ein solches Dreieck etwa mit Basis 10 und messen den zugehörigen Schenkel. Wir messen ganz genau und erhalten etwa $16,18$ als Schenkellänge Aber!! Auch hier führt die wiederholte Wechselwegnahme zu unmöglichen Dreieck. Schön kann man dies mit einer Tabellenkalkulation rechnen lassen. Ich habe es mit einem einfachen `Lisp` Programm getan.
Computerecke:

1. ```
   (defun wechselweg(a)
     (list (- (nth 1 a) (nth 0 a))
           (nth 0 a))
   )
   ```

   Diese Funktion ist die Zuordnung: $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y-x \\ x \end{pmatrix}$. So ergibt `(wechselweg (list 8 13))==> (5 8)`

2. ```
   (defun wieoft(a)
    (let ((n 0 ))
      (loop while (> (nth 0 a) 0) do
            (setq a (wechselweg a) n (+ 1 n))
            )
   n
   )
   )
   ```

   Diese Funktion zählt wie oft ich vernünftigerweise im Wechsel wegnehmen darf. So ergibt `(wieoft (list 1 (/ (+ (sqrt 5) 1) 2)))==>40`

Jede physikalische Messung hat die folgende Eigenschaft. Wir haben eine Grundlänge als Längeneinheit und alle wirklichen Messungen führen zu Vielfachen dieser Grundeinheit. Diese Elementarlänge mag eventuell sehr klein sein, etwa die Wellenlänge einer bestimmten Spektrallinie. Unsere leidvolle Erfahrung beim Vermessen „goldener Dreiecke“ lässt uns mit Hippasos vermuten.

Satz 2. *Es gibt keine goldenen Dreiecke, deren Seitenlängen natürliche Zahlen entsprechen.*

Beim Beweis brauchen wir das folgendes einleuchtendes Axiom.

$\mathbb{N}$ *ist wohlgeordnet. Das heißt: Jede nichtleere Teilmenge von* $\mathbb{N}$ *hat ein kleinstes Element.*

Angenommen es gebe überhaupt ein goldenes Dreieck, dessen Seitenlängen natürliche Zahlen sind. Dann gibt es auch eins mit kleinsten Schenkel y. Die zugehörige Basis bezeichnen wir mit x. Dann ist $x < y$. Das Dreieck mit Basis $y - x$ und Schenkel x ist wieder ein solches Dreieck. Dies widerspricht der Annahme. □

Diese Entdeckung gehört zu den großen Leistungen der jungen griechischen Mathematik. Sie weist eine Unmöglichkeit auf. Meist nur widerwillig finden wir Menschen uns damit ab. Von Unmöglichem wenden wir uns mit Grausen. Der Zusammenhang zwischen Geometrie und Algebra ist nicht so eng, wie Pythagoras meinte.

Nicht alles ist Zahl.

1.2.2 Übersetzung in die Algebra

Betrachten wir noch einmal die Zeichnung 1. Die Dreiecke $\triangle BFA$ und $\triangle ABD$ sind ähnlich. Das heißt es gilt:

$$\frac{x}{y} = \frac{y-x}{x}$$
$$x^2 + xy - y^2 = 0 \tag{1.1}$$

Die Algebra hat gegenüber der Geometrie Nachteile. Dies wurde den Griechen nach der Entdeckung des Hippassos schmerzlich bewußt. In der Geometrie gibt es Strecken, die sich nicht wie natürliche Zahlen verhalten. Die Geometrie ist vielleicht reicher wie die Algebra. Zumindestens ist sie reicher als die Arithmetic. Es gibt Phänomene, die nicht zählbar sind. Auch spricht die Algebra wenig zu unserm Vorstellungsvermögen.
Aber ein großer Vorzug der Algebra ist: Bilder sind nicht mehr wirklich notwendig Algebra und Logik sind enger verwandt. Es ist meist klarer, welche Voraussetzung man benutzt. Daher können wir in der Algebra leichter abstrahieren
So wollen auch wir den geometrischen Ausgangspunkt vergessen und die Frage allgemeiner stellen. Wir untersuchen die Funktion:

$$N : \mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \mapsto N(x,y) = x^2 + xy - y^2 \in \mathbb{R} \tag{1.2}$$

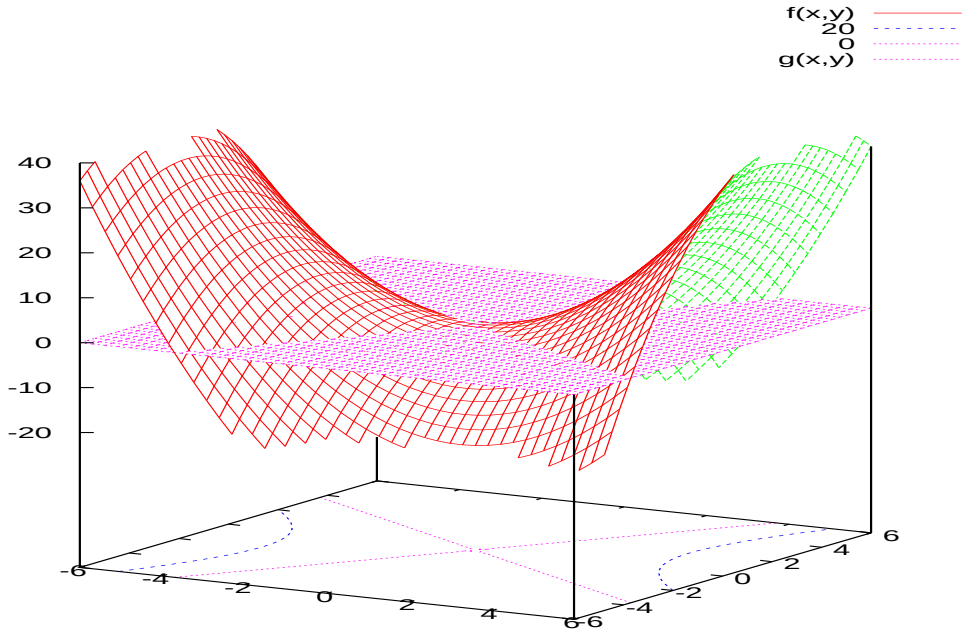


Fig. 1.4: Funktonsgebirge

Wir interessieren uns besonders für die Höhenlinien dieses Funktionsgebirges und die Gitterpunkte auf diesen Höhenlinien. Hippasos hat gezeigt: Keine Gitterpunkte sind Nullstellen dieser Funktion.
Man kann sich nun fragen: Welche Operationen, linearen Abbildungen der $x-y$- Ebene lassen den Wert der Form konstant. Wir fragen nach den Isometrien der Form N. Wir bezeichnen:

$$G : R^2 \ni \vec{x} = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y-x \\ x \end{pmatrix} \in R^2$$
$$F : R^2 \ni \vec{x} = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x+y \end{pmatrix} \in R^2$$
$$H : R^2 \ni \vec{x} = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ x-y \end{pmatrix} \in R^2$$

Dabei ist R irgend ein kommutativer Ring. Wer es nicht so allgemein haben will, denke bei R an $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ oder $\mathbb{Z}/m\mathbb{Z}$. Mit $N(\vec{x})$ sei $x^2 + xy - y^2$ bezeichnet.

Satz 3. *Es gilt:*

1. $F \circ G = G \circ F = Id_{R^2}$.

2. $F^2 - F - Id = 0$.

3. $N(\vec{x}) = -N(F(\vec{x}))$.

4. $N(\vec{x}) = -N(G(\vec{x}))$.

5. $N(H(\vec{x})) = N(\vec{x})$.

1. Wir haben $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y-x \\ x \end{pmatrix} \mapsto \begin{pmatrix} x \\ y-x+x \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$. Daraus ergibt sich die Behauptung.

2. Wir haben $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x+y \end{pmatrix} \mapsto \begin{pmatrix} x+y \\ x+2y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} y \\ x+y \end{pmatrix}$. Daraus ergibt sich die Behauptung.

3. Wir haben $N(F(\vec{x}) = y^2 + y(x+y) - (x+y)^2 = y^2 + yx + y^2 - x^2 - 2xy - y^2 = y^2 - yx - x^2 = -N(\vec{x})$.

4. Genauso.

Legen wir einen geordneten Ring zugrunde, so bedeutet die Aussage 3), 4) und 5): Die Transformation H lässt den Wert der Form konstant. Wendet man die Transformationen F oder G zweimal hintereinander an, so bleibt der Wert der Form konstant. Es sind H, $F \circ F$ und $G \circ G$ zu der Form N gehörende Isometrien. □

Diese Bemerkung, auf die uns Hippasos mit seiner Wechselwegnahme hingewiesen hat, erleichtert die Suche nach Lösungen. Ändern wir die goldene Gleichung 1.1 etwas ab.

$$x^2 + xy - y^2 = \pm 1 \tag{1.3}$$

so erhalten wir eine Kette von Lösungen:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \overset{F}{\to} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} 1 \\ 1 \end{pmatrix} \to \begin{pmatrix} 1 \\ 2 \end{pmatrix} \to \begin{pmatrix} 2 \\ 3 \end{pmatrix} \to \begin{pmatrix} 3 \\ 5 \end{pmatrix} \cdots$$

Satz 4. *Die Gleichung* $N(\vec{x}) = \pm 1$ *hat unendlich viele Lösungen in* $\mathbb{N}^2$.

Es sei $\mathbb{L} = \{\vec{x} | \vec{x} \in \mathbb{N}^2 \text{ mit } N(\vec{x}) = \pm 1\} \subset \mathbb{N}^2$ die Lösungsmenge der Gleichung 1.3. Ist $\vec{x} \in \mathbb{L}$, so besagt der Satz 3 Teil 3, dass auch $F(\vec{x}) \in \mathbb{L}$ ist. Daher kann F als Funktion $\mathbb{L} \to \mathbb{L}$ aufgefasst werden. Es ist $G \circ F = Id$. Dahe ist F injektiv. Außerdem ist $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \notin Bi(F)$. Daher ist F nicht surjektiv. Das heißt $F : \mathbb{L} \to \mathbb{L}$ ist eine injektive und nicht surjektive Funktion. Das bedeutet $\mathbb{L}$ ist unendlich. [1] □

[1] Dedekind hat geklärt: Eine Menge ist unendlich, wenn es eine injektiev aber nicht surjektive Funktion der Menge in sich gibt.

Aber erreichen wir mit unere Methode auch wirklich alle Lösungen? Nähern wir uns dem Problem von einer anderen Seite, ganz wie es der Titel der Veranstaltung anregt. Lösen wir die Gleichung 1.3, wie wir es gelernt haben, nach y auf:

$$\begin{aligned} x^2 + xy - y^2 &= 1 \\ y_1 &= \frac{x + \sqrt{5x^2 - 4}}{2} \\ y_2 &= \frac{x - \sqrt{5x^2 - 4}}{2} \end{aligned}$$

Es ist $y_2 < 0$ für $x > 1$. Wenn wir nur Lösungen aus $(\mathbb{R}^+)^2$ betrachten, so gibt die Funktion $f(x) = \frac{x+\sqrt{5x^2-4}}{2}$ zu jedem positiven x ein y an, welches die Gleichung 1.3 löst. Beachtet man noch die Gleichung:

$$x^2 + xy - y^2 = -1$$

so erhält man die Funktion $g(x) = \frac{x+\sqrt{5x^2+4}}{2}$. Durch welche Gitterpunkte gehen die Graphen dieser Funktionen?

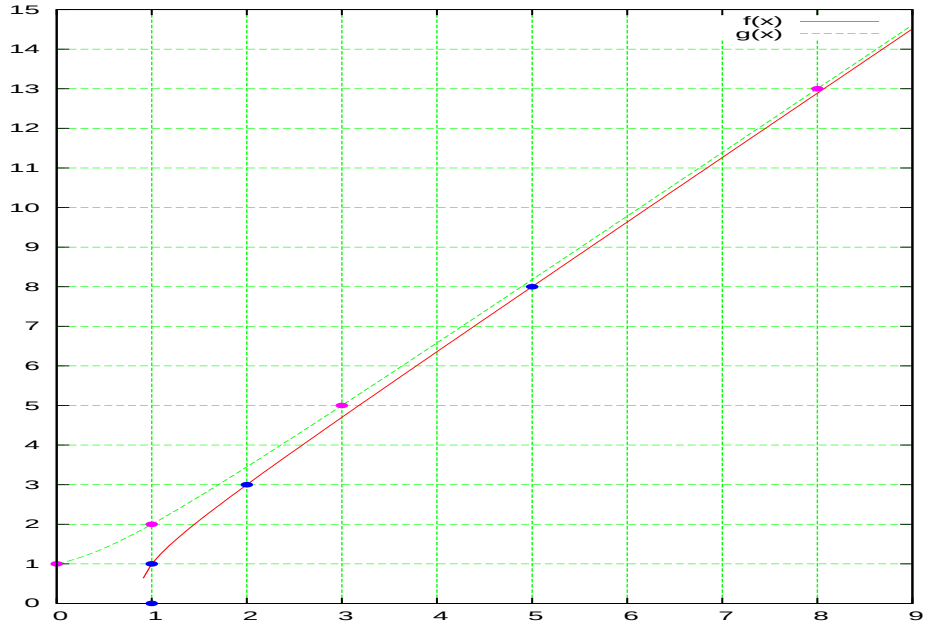


Fig. 1.5: Gitterpunkte

Der Graph legt nahe, dass es nur die Punkte der Folge:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 3 \end{pmatrix} \mapsto \begin{pmatrix} 3 \\ 5 \end{pmatrix} \dots$$

sind. Aber wie können wir sicher sein? Vielleicht suchen wir weiter? Man kann versuchen mit einer Tabellenkalkulation nach Lösungen zu suchen indem man ganzzahlige x einsetzt und nachschaut, wann das zugehörige $f(x)$ beziehungsweise $g(x)$ ganzzahlig ist. Leider rechnet eine Tabellenkalkulation nicht beliebig genau. Wir brauchen als wieder Lisp oder ein Computeralgebrasystem.
Computerecke:

3. Eine Funktion, welche angibt ob eine Zahl $n \in \mathbb{N}$ eine Quadratzahl ist.

```
(defun istquadrat(n)
  (= (* (isqrt n) (isqrt n) ) n)
  )
```

   Die Funktion `(isqrt n)` gibt die größte ganze Zahl $\leq \sqrt{n}$ an.

4. Den Wert von $5 \cdot x^2 - 4$. Dies ist die Diskriminante der Gleichung $x^2 + xy - y^2 = 1$:

```
(defun diskr-(x)
  (- (* 5 x x ) 4)
 )
```

5. Den Wert von $5 \cdot x^2 + 4$.

```
(defun diskr+(x)
  (+ (* 5 x x ) 4)
 )
```

6. Die nächste Funktion erstellt eine aller $x \leq y$, bei denen $5 \cdot x^2 + 4$ oder $5 \cdot x^2 - 4$ eine Quadratzahl ist.

```
(defun loesungen(y)
  (let (( x 1) (liste nil))
    (loop while (<= x y) do
    (if (or
        (istquadrat (diskr+ x)) (istquadrat (diskr- x)))
        (setq liste (append liste (list x))))
     (setq x (1+ x))
    )
 liste)
)
```

   So ergibt `(print (loesungen 1000))` die Liste `(1 2 3 5 8 13 21 34 55 89 144 233 377 610 987)` Also genau die Fibonaccizahlen.

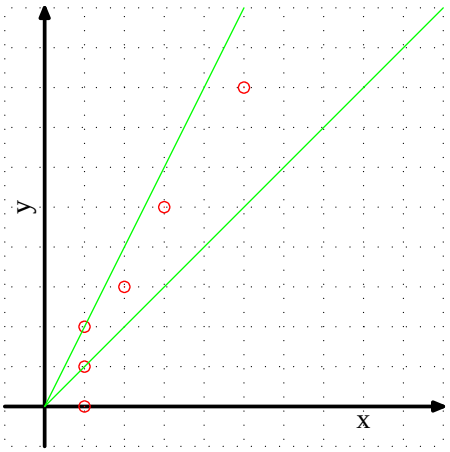


Fig. 1.6: Fast Goldene Gleichung

Spielt man eine Weile mit diesen Programmen, so wird man bestärkt: Es gibt keine weiteren Lösungen. In der Folge:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 2 \end{pmatrix} \dots$$

tauchen alle Lösungen aus $\mathbb{N}^2$ auf. Betrachtet man nochmal die Lösungsmenge so vermutet man zunächst: Alle Lösungspunkte mit Ausnahme von $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ liegen oberhalb der Winkelhalbierenden und unterhalb der Geraden $y = 2x$. Wir halten die erste Aussage fest.

Bemerkung. *Löst* $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{N}^2$ *die fast goldene Gleichung 1.3, so ist* $x < y$ *außer den beiden Fällen* $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *und* $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Zunächst betrachten wir:

$$\begin{aligned} x^2 + xy - y^2 &= -1 \\ x^2 + 1 &= y^2 - xy = y(y - x) \end{aligned}$$

Also ist $y - x > 0$, da auf der linken Seite der Gleichng eine positive Zahl steht.
Nun betrachten wir

$$\begin{aligned} x^2 + xy - y^2 &= 1 \\ x^2 - 1 &= y(y - x) \end{aligned}$$

Steht wieder links etwas positives ist man wieder fertig. Andernfalls ist $x^2 - 1 = 0 = y(y - x)$. Daher ist $x = 1$ und also muss $y = 0$ oder $y = 1$ sein. Wir erhalten die beiden Ausnahmen $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. □

Wenden wir die Abbildung F n– mal hintereinander an, so bezeichnen wir die entstehende Abbildung mit F^n.

Satz 5. *Ist* $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{N}^2$ *eine Lösung von 1.3, so gibt es eine natürliche Zahl* n *mit* $F^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$.

Angenommen es gebe eine Lösung von 1.3, die nicht von der Art $F^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ist. Dann gibt es auch eine mit kleinster erster Komponente etwa $\begin{pmatrix} x_m \\ y_m \end{pmatrix}$. Es ist $x_m > 1$. Es ist

$$\begin{aligned} x_m^2 \pm 1 &= y_m^2 - x_m y_m \\ x_m^2 \pm 1 &= y_m(y_m - x_m) \\ y_m &> x_m \end{aligned}$$

Also ist $\begin{pmatrix} y_m - x_m \\ x_m \end{pmatrix}$ auch eine Lösung. Ist $y_m - x_m = 1$, so ist $x_m = 1$ oder $x_m = 0$. In beiden Fällen ist $\begin{pmatrix} y_m - x_m \\ x_m \end{pmatrix}$ von der Form $F^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Andernfalls ist $\begin{pmatrix} y_m - x_m \\ x_m \end{pmatrix}$ eine Lösung mit kleinerer erster Komponente. Nach Voraussetzung gibt es ein $n \in \mathbb{N}$ mit $F^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} y_m - x_m \\ x_m \end{pmatrix}$. Dann ist aber

$$F^{n+1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = F \begin{pmatrix} y_m - x_m \\ x_m \end{pmatrix} = \begin{pmatrix} x_m \\ y_m \end{pmatrix}.$$

Dies widerspricht der Wahl von x_m. Also sind alle Lösungen von 1.3 ausgehend von $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ durch wiederholte Anwendung von F erreichbar. □

Wir können den Bereich, in dem wir nach Lösungen suchen müssen, stark einschränken und dadurch dieses Resultat verbessern.

Satz 6. *Es sei* $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{N}^2$ *eine Lösung der Gleichung* $x^2 + xy - y^2 = n (n \in \mathbb{N})$. *Dann gilt:*

1. $x < y \iff x^2 > n$.
2. $2x - y > 0$.
3. *Es gibt eine Lösung* $\begin{pmatrix} x \\ y \end{pmatrix}$ *mit* $\frac{4}{5}n < x^2 \leq n$.

1. Wir haben $x^2 - n = y \cdot (y - x)$. Aus dieser Gleichung ergibt sich die Behauptung.
2. Hier hilft die quadratische Ergänzung weiter: $x^2 + xy - y^2 = (x + \frac{1}{2}y)^2 - \frac{5}{4}y^2$. Ist $x^2 + xy - y^2 = n$, so folgt

$$\begin{aligned} (x + \frac{1}{2}y)^2 &= n + \frac{5}{4}y^2 \\ (2x + y)^2 > 4y^2 \quad &\iff \quad 2x - y > 0 \end{aligned}$$

3. Unter den Lösungen gibt es eine mit kleinstmöglichem y. Dann ist $y < x$. Denn sonst wäre $G^2 \begin{pmatrix} x \\ y \end{pmatrix}$ eine Lösung mit kleinerem y. Das geht nicht. Die Diskriminante der Gleichung $y^2 + xy + n - x^2 = 0$ ist $D = 5x^2 - 4 \cdot n$. Daraus ergibt sich die Behauptung. □

Beispiele:

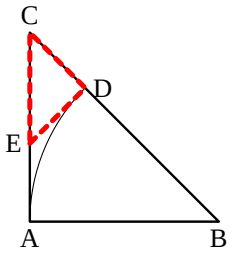
1. $n = 0$ (Fall des Hippasos): Wir brauchen nur zu betrachten: $\frac{4}{5} \cdot 0 \leq x^2 \leq 0$. Also kommt nur $x = 0$ in Frage. Dann muss aber $y = 0$ sein. Also gibt es keine Lösungen in positiven Zahlen. Wir haben wie in der Geometrie geschlossen. Und genau wie dort erhalten wir das „enttäuschende“ Ergebnis: Es gibt nicht mal eine einzige Lösung
2. $n = 2$. Es ist nur $x^2 = 1$ möglich. Da $y \leq x$ brauchen wir nur $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ testen. Dies ist keine Lösung.
3. $n = 3391$: Es ist $\lfloor \frac{4}{5} p \rfloor = 2713^2$. Wir brauchen für x nur Zahlen zwischen $53, \ldots, 59$ zu probieren. Bei 56 sind wir erfolgreich. Wir erhalten $y = 51$. Es ist $56^2 + 56 \cdot 51 - 51^2 = 3391$. Hier haben wir daher unendlich viele Lösungen

Aufgaben:

1. Ein Punkt $\vec{x}$ der Ebene $\mathbb{R}^2$ heißt rational, wenn seine Koordinaten rationale Zahlen sind.
   a) Liegen auf einer Geraden zwei verschiedene rationale Punkte, so liegen auf ihr unendlich viele rationale Punkte.
   b) Auf der Kurve mit der Gleichung $x^2 + xy - y^2 = 0$ ist der Nullpunkt der einzig rationale Punkt.
2. Ein Paar natürlicher Zahlen $\begin{pmatrix} x \\ y \end{pmatrix}$ erfülle die fast goldene Gleichung 1.3.
   a) Für welche $\begin{pmatrix} x \\ y \end{pmatrix}$ ist $3x < 2y$?
   b) Für welche $\begin{pmatrix} x \\ y \end{pmatrix}$ ist $3y < 5x$?
3. a) Die Gleichung $x^2 + xy - y^2 = 3$ hat in $\mathbb{N}^2$ keine Lösung.
   b) Die Gleichung $x^2 + xy - y^2 = 5$ hat in $\mathbb{N}^2$ unendlich viele Lösungen. Unendlich ist hier in folgendem Sinn gemeint. Es gibt ein Verfahren welches immer wieder eine neue Lösung erzeugt.
   c) Zeige allgemein: Die Gleichung $x^2 + xy - y^2 = d$ mit $d \in \mathbb{N}$ hat unendlich viele Lösungen oder gar keine. Wie erreicht man alle Lösungen?
4. a) Für welche reelle Zahlen ist $\frac{x}{2+\sqrt{5x^2-4}} 2 > x$?
   b) Für welche reellen Zahlen x ist $\frac{x-\sqrt{5x^2-4}}{2} > 0$?
   c) Für welche $x \in \mathbb{N}$ ist $5x^2 - 4$ eine Quadratzahl?
   d) Für welche $x \in \mathbb{N}$ ist $5x^2 + 4$ eine Quadratzahl?

[2] $\lfloor x \rfloor$ ist die größte ganze Zahl $\leq x$

5. Die Basis eines gleichschenkligen rechtwinkligen Dreiecks sei x und die Schenkellänge sei y.



   a) Zeige wie beim goldenen Dreieck: Es gibt keine natürlichen Zahlen, die diese Bedingungen erfüllen. Beachte dazu die Zeichnung nebenan.

   b) Entwickle ein Verfahren aus einer Lösung $\begin{pmatrix} x \\ y \end{pmatrix}$ der Gleichung $x^2 - 2y^2 = \pm 1$ eine weitere zu erhalten.

   c) Wieviel Lösungen aus $\mathbb{N}^2$ hat die Gleichung: $x^2 - 2y^2 = 2$?

   d) Zeige: Mit dem im Aufgabenteil 5b erhält man alle Lösungen der Gleichung $x^2 - 2y^2 = \pm 1$.

   e) Erhält man mit dem Verfahren aus 5b auch alle Lösungen von $x^2 - 2y^2 = 7$?

6. Gegeben ist der Term $H(x, y) = x^2 - 2 \cdot x \cdot y - y^2$.
   a) Zeige: Die Gleichung $H(x, y) = 1$ hat in $\mathbb{N}^2$ unendlich viele Lösungen, indem du ein Verfahren angibst aus einer Lösung eine neue zu erhalten.
   b) Zeige: Die Gleichung $H(x, y) = d$ mit $d \in \mathbb{N}$ hat keine oder unendlich viele Lösungen.
7. Zeige: die Gleichung $x^2 - axy - y^2 = 1$ hat unendlich viele Lösungen für $a \in \mathbb{N}$.
8. Wir betrachten die Gleichung 1.3 in $\mathbb{Z}/m\mathbb{Z}^2$.
   a) Wieviel Lösungen gibt es für $m = 3$?
   b) Wieviel Lösungen gibt es für $m = 5$?
   c) Wieviel Lösungen gibt es für $m = 7$?
9. Sei

$$f : \mathbb{R}^+ \cup \{\infty\} \ni x \mapsto \begin{cases} \frac{1}{x - [x]} \text{ falls } x \notin \mathbb{N} \cup \{\infty\} \\ \infty \text{ falls } x \in \mathbb{N} \cup \{\infty\} \end{cases} \in \mathbb{R}^+ \cup \{\infty\} \tag{1.4}$$

   a) Berechne den kleinsten positiven Fixpunkt der Funktion.
   b) Zeige: x ist genau dann rational, wenn es ein $n \in \mathbb{N}$ gibt mit $f^n(x) = \infty$.
   c) Zeichne den Graph von f.
   d) Zeige: Ist $\alpha \notin \mathbb{Q}$ Lösung einer quadratischen Gleichung $ax^2 + b \cdot x + c =$ mit $a, b, c \in \mathbb{Z}$, so ist auch $f(\alpha)$ Lösung einer solchen Gleichung mit gleicher Diskriminante.
   e) Kennzeichne alle Fixpunkte von f.
   f) Kennzeichne alle $x \in \mathbb{R}^+$ mit $f^2(x) = x$

1.3 Der Ring $\mathbb{Z}[\phi]$

1.3.1 Fibonacci-Zahlen

Wir sind göttlichen Geschlechtes und besitzen ohne jeden Zweifel schöpferische Kraft nicht bloß in materiellen Dingen (Eisenbahnen, Telegraphen), sondern ganz besonders in geistigen Dingen. (Richard Dedekind)

Eine natürliche Frage ist: Gegeben ist ein Zahlenpaar $\begin{pmatrix} a \\ b \end{pmatrix}$ mit positiven Zahlen $a, b \in \mathbb{R}$. Wie oft kann ich die Wechselwegnahme durchführen bis ich zum ersten mal auf eine Zahl ≤ 0 treffe?
Um dies zu untersuchen betrachten wir die zur Wechselwegnahme umgekehrte Transformation.

$$F : \mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x+y \end{pmatrix} \in \mathbb{R}^2$$

Dies führt zu der folgenden Kette.

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 3 \end{pmatrix} \mapsto \begin{pmatrix} 3 \\ 5 \end{pmatrix} \ldots \mapsto \begin{pmatrix} f(n+1) \\ f(n+2) \end{pmatrix} \ldots$$

Es ist also $f(0) = 0, f(1) = 1$ und $f(n+2) := f(n) + f(n+1)$ die rekursive Definition einer Zahlenfolge der Fibonacci Folge.
Um diese Zahlenfolge zu untersuchen setze ich ab jetzt die folgende Situation voraus: R ist ein kommutativer Ring mit 1. Wir haben einen unitären Ringhomomorphismus $\rho : R \to S$ In dem Ring S hat das Polynom $X^2 - X - 1$ Nullstellen. Wir wählen eine aus und nennen sie ϕ.
Beispiele:

4. $\mathbb{Q} \hookrightarrow \mathbb{Q}[\phi]$ ist der kleinste Unterring von $\mathbb{R}$, der $\mathbb{Q}$ und die Zahl $\phi = \frac{1+\sqrt{5}}{2}$ enthält.
5. $\mathbb{Z}[\phi]$.
6. Wählt man als S den 2×2 Matrizenring über $\mathbb{Z}$. Als ϕ die Matrix
$$\phi = F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$
7. In dem Ring $\mathbb{Z}/11\mathbb{Z} = \{0, 1, 2, \ldots, 10\}$ ist etwa $4^2 - 4 - 1 = 11 = 0 \bmod 11$. Also kann man $\phi = 4$ wählen.
8. In dem Ring $\mathbb{Z}/7\mathbb{Z}$ hat das Polynom keine Nullstelle. Dann kann man als S wieder den 2×2 Matrizenring wählen. Als ϕ wählt man wieder die Matrix $F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

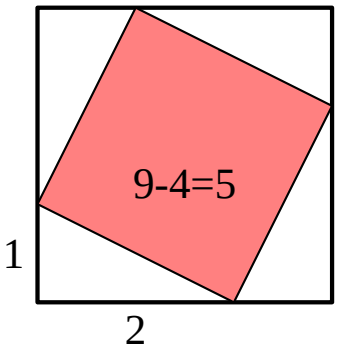


Fig. 1.7: 5=9-4

Die Voraussetzungen hören sich hohepriesterlich an. Aber unser Freund Max aus der 8ten Klasse kennt sicher den Fächeninhalt eines rechtwinkligen Dreiecks mit den Katheten a und b. Er ist $F = \frac{a \cdot b}{2}$. Besteht eine Figur aus mehreren Flächen, die sich nicht überlappen, so erhält man den Gesamtflächeninhalt durch Addition der Einzelflächen. Dann sieht er aber auch ein, dass der Flächeninhalt des schraffierten Quadrates nebenan 5 ist. Leicht kann er jetzt $\phi = \frac{1+\sqrt{5}}{2}$ konstruieren und nachweisen, dass $\phi^2 - \phi - 1 = 0$ gilt. Wir haben also eine Lösung der goldenen Gleichung. Max wird sich freuen.

Aufgaben:

10. a) Konstruiere ein Quadrat mit dem Flächeninhalt 68, indem Du die Gleichung benutzt $10^2 - 2 \cdot 8 \cdot 2 = 68$.

    b) Gib allgemein ein Verfahren an ein Quadrat vom Flächeninhalt $a^2 + b^2$ zu konstruieren, wenn a, b gegebene Zahlen sind. Es ist eine spannende Frage: Welche Zahlen sind Summe von zwei Quadratzahlen?

    c) Wir haben einfach so getan als ob ϕ eine Zahl sei. Wir sind schon so lange an reelle Zahlen gewohnt, dass dies sebstverständlich erscheint. Wir übernehmen also doch wieder den Standpunkt des Pythagoras. „Alles ist Zahl“. Wenn mal zuwnig Zahlen da sind, so machen wir uns welche. Denke darüber nach.

Satz 7. *1. $1 - \phi$ ist die zweite Nullstelle von $X^2 - X - 1$.*

2. ϕ ist invertierbar. Es ist $\phi^{-1} = \phi - 1$.

3. $\phi^n = f(n-1) + f(n)\phi$.

4. $(1-\phi)^n = f(n+1) - f(n)\phi$.

5. $\phi^{-n} = (-1)^n (f(n+1) - f(n))\phi$.

6. $f(n-1)f(n+1) - f(n)^2 = (-1)^n$.

1. $(1-\phi)^2 - (1-\phi) - 1 = 1 - 2\phi + \phi^2 - 1 + \phi - 1 = 1 - 2\phi + \phi + 1 - 1 + \phi - 1 = 0$.

2. $\phi(\phi - 1) = \phi^2 - \phi = \phi + 1 - \phi = 1$.

3. Es ist $\phi^0 = 1$ und $\phi^1 = f(0) + f(1)\phi$. Gelte die Behauptung für n. Wir erhalten:

$$\begin{aligned} \phi \cdot \phi^n &= \phi \cdot (f(n-1) + f(n)\phi) \\ &= f(n-1)\phi + f(n) + f(n)\phi \\ &= f(n) + f(n+1)\phi \end{aligned}$$

4. Da $(1-\phi)$ auch Lösung der goldenen Gleichung ist, ist $(1-\phi)^n = f(n-1) + f(n)(1-\phi) = f(n+1) - f(n)\phi$.

5. Dies liegt einfach daran, dass $\phi^{-1} = (\phi - 1) = (-1) \cdot (1 - \phi)$ ist.

6. Wir haben:

$$\begin{aligned}(-1)^n &= \phi^n(1-\phi)^n \\ &= (f(n-1) + f(n)\phi) \cdot (f(n+1) - f(n)\phi) \\ &= f(n-1)f(n+1) - f(n-1)f(n)\phi + f(n)f(n+1)\phi - f(n)\phi^2 \\ &= f(n-1)f(n+1) + f(n)(f(n+1) - f(n-1))\phi - f(n)^2 - f(n)^2\phi \\ &= f(n-1)f(n+1) - f(n)^2\end{aligned}$$

Die letzte Gleichung gilt, da $f(n+1) - f(n-1) = f(n)$ ist. □

Folgerung 8. *In $\mathbb{Q}$ gilt: Für alle $n \in \mathbb{N}$ gilt:*

$$\frac{f(2n+2)}{f(2n+1)} < \frac{f(2n+4)}{f(2n+1)} < \cdots < \frac{f(2n+3)}{f(2n+2)} < \frac{f(2n+1)}{f(2n)} \tag{1.5}$$

Dies kann man einfach nachrechnen.
Kehren wir nun noch einmal zur Wechselwegnahme vom Anfang zurück. Wir können sie folgendermaßen deuten: Ist $a + b\phi$ gegeben, so erhält man:

$$(a + b\phi)\phi^{-1} = (a + b\phi)(\phi - 1) = (b - a) + a\phi.$$

Dies entspricht genau der Wechselwegnahme.
Es ist

$$(a + b\phi)\phi^{-n} = (f(n+1)a - f(n)b + (-f(n)a + f(n-1)b)\phi) \cdot (-1)^n \tag{1.6}$$

Jetzt können wir die Frage am Anfang von Abschnitt 1.3.1 auf Seite 13 leicht beantworten. Dazu folgende Vereinbarung: Wir sagen die Wechselwegnahme bricht bei dem Paar $\begin{pmatrix} a \\ b \end{pmatrix}$ ab, wenn $a \leq 0$ ist. Wir fragen uns: Gegeben ist ein Zahlenpaar $\begin{pmatrix} a \\ b \end{pmatrix}$. Wann bricht die Wechselwegnahme ab? Unser Programm `wieoft(a)` liefert beispielsweise: `(wieoft (list 1 1.61803)) ===>15`. Bevor wir diese Frage genau beantworten lösen wir eine Aufgabe:
Aufgaben:

11. Kennzeichne in der Ebene die Punkte, bei denen die Wechselwegnahme genau 2 mal durchführbar ist.

12. Kennzeichne in der Ebene die Punkte, bei denen die Wechselwegnahme genau 3 mal durchführbar ist.

Wir bezeichnen mit $Fib(n)$ das Interval mit den Randpunkten $\frac{f(n)}{f(n-1)}$ und $\frac{f(n+1)}{f(n)}$ und nennen es $n$tes Fibonacciintervall.

Satz 9. *Sei $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$. Folgende Aussagen sind dann äquivalent.*

1. *In* $\begin{pmatrix} a_n \\ b_n \end{pmatrix} = G^n \begin{pmatrix} a \\ b \end{pmatrix}$ *sind beide Komponenten positiv.*
2. $\frac{b}{a}$ *liegt in dem Intervall mit den Randpunkten* $Fib(n)$*.*

Das heißt wir können auf ein Zahlenpaar die Wechselwegnahme genau dann n mal „sinnvoll“[3] durchführen, wenn $\frac{b}{a} \in Fib(n)$ liegt.

1. Sei n gerade. Wegen der Gleichung gilt:

$$(a + b\phi)\phi^{-n} = (f(n+1)a - f(n)b + (-f(n)a + f(n-1)b)\phi)$$

   Es ist

$$f(n+1)a - f(n)b > 0$$
$$\frac{f(n+1)}{f(n)} > \frac{b}{a}$$

   Und es ist:

$$f(n-1)b - f(n)a > 0$$
$$\frac{b}{a} > \frac{f(n)}{f(n-1)}$$

   Daraus folgt die Behauptung.

2. Ist n ungerade, so folgt die Behauptung entsprechend. □

Folgerung 10. *Für ein paar positiver Zahlen* $\begin{pmatrix} a \\ b \end{pmatrix}$ *sind äquivalent:*

1. *Die Wechselwegnahme kann unendlich oft durchgeführt werden.*
2. $\frac{b}{a} \in \bigcap_{n \in \mathbb{N}} Fib(n)$*.*

Folgerung 11. *Ist* $\begin{pmatrix} a \\ b \end{pmatrix}$ *ein paar positiver reeller Zahlen und* $\begin{pmatrix} a(n) \\ a(n+1) \end{pmatrix} = F^n \begin{pmatrix} a \\ b \end{pmatrix}$*, so ist* $\frac{a(n+1)}{a(n)} \in Fib()$

Es ist $(a(n) + a(n+1)\phi) \cdot \phi^{-n} = a + b\phi$. a, b sind positiv. Die Behauptung folgt. □

Wenn man nun noch zeigt, dass die Folge $(\frac{f(n+1)}{f(n)} | n \in \mathbb{N})$ konvergiert, so sieht man auch dass der Grenzwert der Folge $\phi = \frac{1+\sqrt{5}}{2}$ ist.

[3] Mit geometrischer Bedeutung

Bemerkung 1 Ist $\vec{a} = \begin{pmatrix} a \\ b \end{pmatrix}$ mit $b = a\phi$, so ist $F \begin{pmatrix} a \\ b \end{pmatrix} = \phi \begin{pmatrix} a \\ b \end{pmatrix}$. Es ist $\begin{pmatrix} a \\ b \end{pmatrix}$ ein Eigenvektor der Transformation F und ϕ der zugehörige Eigenwert. Außerdem gilt $F \begin{pmatrix} -\phi \\ 1 \end{pmatrix} = (1-\phi) \begin{pmatrix} -\phi \\ 1 \end{pmatrix}$. □

Dies rechnet man nach. □

Es gibt eine sehr schnelle Methode a^b zu berechnen. In dem Buch [Bartholomé et al., 2008, Seite 9] ist diese Methode `aepot(a,b)` genannt. Übertragen wir die Methode auf $\mathbb{Z}[\phi]$ so erhalten wir eine sehr schnelle Methode um die Fibonacci Zahlen zu berechnen. Die $n$te Fibonacci-Zahl erhalten wir ja mit ϕ^n als Dreingabe. Um ein beliebiges Element α aus $\mathbb{Z}[\phi]$ zu potenzieren gehen wir folgendermaßen vor:

1. Ist $n = 0$, so ist $\alpha^n = 1$.
2. Ist n gerade, so ist $\alpha^n = (\alpha^2)^{(n-1)/2}$.
3. Ist n ungerade, so ist $\alpha^n = \alpha \cdot \alpha^{n-1}$

Computerecke:

7. Um dieses Programm tatsächlich in `clisp` zu schreiben müssen wir zunächst Addition und Multiplikation in $\mathbb{Z}[\phi]$ programmieren. Also die Addition:

```
(defun +phi(x y)
 "addiert in Z[phi] zwei Zahlen"
  (list (+ (nth 0 x) (nth 0  y))
        (+ (nth 1 x) (nth 1 y)))
 )
```

8. Nun die Multiplikation. Es ist $(a + b\phi) \cdot (c + d\phi) = ac + bd + (ad + bc + bd)\phi$. Übersetzt man das in ein Lisp Programm, so ergibt sich:

```
(defun *phi(x y)
  (list (+ (* (nth 0 x) (nth 0 y))
           (* (nth 1 x) (nth 1 y)))
        (+ (* (nth 0 x) (nth 1 y))
           (* (nth 1 x) (nth 0 y))
           (* (nth 1 x) (nth 1 y))
        )
)
)
```

Setzt man:

```
 (setq a (list 0 1))
(setq a (*phi a a))
```

und ruft die zweite Zeile 4 mal auf, so erhält man ϕ^{16} und daher die 15te und 16te Fibonacci Zahl 987. Der nächste Aufruf ergibt schon (1346269 2178309) Also die 31te und 32te Fibonacci Zahl.

9. Jetzt aber zur versprochenen schnellen Potenzierungsmethode.

```
(defun phipow(a b)
  (if (= b 0) (list 1 0)
       (if (oddp b) (*phi (phipow a (- b 1)) a)
                    (phipow (*phi a a) (/ b 2))
       )))
```

Hiermit rechnen wir blitzschnell aus, was die 300. Fibonacci Zahl ist, nämlich

222323244629420445529739893461909967206666939096499764990979600

Unser nächstes Ziel ist es die invertierbaren Elemente in $\mathbb{Z}[\phi]$ genau zu bestimmen. Dazu als Vorbereitung:

Satz 12. *Es sei R ein kommutativer Ring.*

1. *Gibt es einen Homomorphismus der Ringe $\mathbb{Z}[\phi] \to R$, so gibt es ein $a \in R$ mit $a^2 - a - 1 = 0$.*

2. *Gibt es in R ein a mit $a^2 - a - 1 = 0$, so gibt es genau einen Ringhomomorphismus $\rho : \mathbb{Z}[\phi] \to R$ mit $\rho(\phi) = a$.*

1. In $\mathbb{Z}[\phi]$ ist $\phi^2 - \phi - 1 = 0$. Mit $a = \rho(\phi)$ folgt die Behauptung.

2. Wir erklären die Abbildung $\rho(x + y\phi) := x + y \cdot a \in R$. Damit ist ρ wohldefiniert und ein Homomorphismus abelscher Gruppen. Es ist $\rho(1) = 1$. Es bleibt zu zeigen, dass ρ ein Homomorphismus der Ringe ist. Sei dazu $x + y\phi$ und $x' + y'\phi$ zwei Zahlen aus $\mathbb{Z}[\phi]$. Dann ist $(x + y\phi) \cdot (x' + y'\phi) = (xx' + yy') + (xy' + yx' + yy') \cdot \phi$. Daher ist $\rho((x + y\phi) \cdot (x' + y'\phi)) = (xx' + yy') + (xy' + yx' + yy') \cdot a$. Andererseits ist, da $a^2 - a - 1 = 0$ in R gilt, $\rho(x + y\phi) \cdot \rho(x' + y'\phi) = (x + ya) \cdot (x' + y'a) = (xx' + yy') + (xy' + yx' + yy')a$. Daraus folgt die Behauptung. Leicht bestätigt man, dass es einen weiteren Homomorphismus mit dieser Eigenschaft nicht geben kann. □

Satz 13. *Hat ein Ring S die folgenden Eigenschaft:*

- *Es gibt ein $\alpha \in S$ mit $\alpha^2 - \alpha - 1 = 0$.*
- *Zu jedem Ring R und $a \in R$ mit $a^2 - a - 1 = 0$ gibt es genau einen Ringhomomorphismus $\rho : S \to R$ mit $\rho(\alpha) = a$,*

dann ist $S \cong \mathbb{Z}[\phi]$.

Sei S ein Ring und α wie in der Voraussetzung beschrieben. Dann gibt es genau einen Homomorphismus $\rho : \mathbb{Z}[\phi] \to S$ mit $\rho(\phi) = \alpha$. Genauso gibt es einen Homomorphismus $\mu : S \to \mathbb{Z}[\phi]$ mit $\mu(\alpha) = \phi$. Also ist $\mu(\rho(\phi)) = \phi$. Es ist aber die Identität der einzige Ringhomomorphismus $\mathbb{Z}[\phi] \to \mathbb{Z}[\phi]$ mit dieser Eigenschaft. Daher ist $\mu \circ \rho = Id_{\mathbb{Z}[\phi]}$. Die umgekehrte Verkettung ist die Identität auf S. Daher sind S und $\mathbb{Z}[\phi]$ isomorph. □

Folgerung 14. *In der Menge der reellen Zahlen hat die Gleichung $x^2 - x - 1 = 0$ eine Lösung nämlich $\frac{1+\sqrt{5}}{2}$. Der nach Satz 12 eindeutig bestimmte Homomorphismus ist ein Monomorphismus. Wir können $\mathbb{Z}[\phi]$ als Unterring von $\mathbb{R}$ auffassen und ϕ mit $\frac{1+\sqrt{5}}{2}$ identifizieren.*

Wir müssen nur zeigen, dass ρ eine injektive Abbildung ist. Es sei

$\rho(a + b\phi) = 0$ mit $a, b \in \mathbb{Z}$. Dann ist $a + b\frac{1+\sqrt{5}}{2} = 0$. Da $\frac{1+\sqrt{5}}{2}$ keine rationale Zahl ist, muss $a = b = 0$ sein. Daher ist ρ ein injektiver Gruppenhomomorphismus. Damit folgt die Behauptung □

Wir wollen in Zukunft $\mathbb{Z}[\phi]$ mit dem entsprechenden Unterring von $\mathbb{R}$ identifizieren. Insbesondere ist $\mathbb{Z}[\phi]$ ein Unterring von $\mathbb{Q}[\phi] = \{x + y\phi | x, y \in \mathbb{Q}\}$.

Jetzt endlich kann die Einheitengruppe von $\mathbb{Z}[\phi]$ ihre Geheimnisse nicht mehr vor uns verbergen. Wir definieren für $\alpha = a + b\phi \in \mathbb{Q}[\phi]$: $N(\alpha) := a^2 + ab - b^2$ und nennen es die Norm des Elementes α. Da $N(\alpha)$ nichts anders als die Determinante der Matrix $a + b\phi = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$ ist, gilt für $\alpha, \beta \in \mathbb{Z}[\phi]$: $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$. Man kann dies auch direkt nachrechnen. Es ist $N(\alpha) = (a + b\phi) \cdot (a + b(1 - \phi))$.

Satz 15. *$\alpha = a + b\phi \in \mathbb{Z}[\phi]$ ist eine Einheit genau dann, wenn $N(\alpha) = \pm 1$ ist.*

Ist $\alpha \in \mathbb{Z}[\phi]$ ein invertierbares Element, so gibt es ein $\beta \in \mathbb{Z}[\phi]$ mit $\alpha \cdot \beta = 1$. Daher ist $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) = 1$. Also ist $N(\alpha) = \pm 1$. Ist umgekehrt $N(\alpha) = \pm 1$, so ist $(a + b\phi) \cdot (a + b(1 - \phi)) = \pm 1$. Daher ist α invertierbar. □

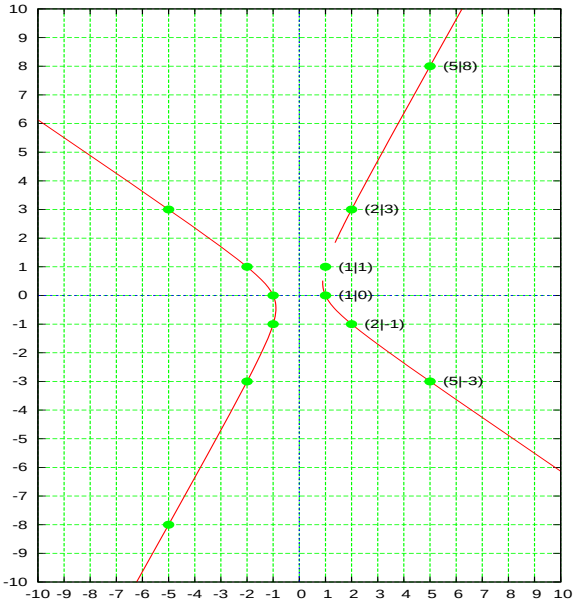


Fig. 1.8: Einheiten

Zeichnet man die Punkte mit $x^2 + xy - y^2 = 1$, so erhält man die Hyperbel im Bild nebenan. Die Gitterpunkte, die auf dem rechten Hyperbelarm liegen entsprechen den Einheiten der Form $\{\phi^z | z \in \mathbb{Z}\}$. Zum Beispiel entspricht dem Punkt $(1|1)$ die Zahl $1 + \phi$. Nicht in der Zeichnung sind die Punkte negativer Norm. Der nächste Satz kennzeichnet die Gruppe der Einheiten in $\mathbb{Z}[\phi]$ vollständig.

Satz 16. *Ist U die Gruppe der Einheiten in $\mathbb{Z}[\phi]$, so gilt:*

$$U = \{\pm 1\} \cdot \{\phi^z | z \in \mathbb{Z}\}.$$

Sei $\alpha = a + b\phi$ eine Einheit. Dann ist $N(\alpha) = \pm 1$. Wir betrachten verschiedene Fälle.

1. Es sind $a, b > 0$. $\phi = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ Nach den Überlegungen auf Seite 9 gibt es ein $n \in \mathbb{N}$ mit $\phi^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$. Daher ist $\phi^n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} = a + b\phi$. Also ist das invertierbare Element α von der Form ϕ^n.

2. $a, b < 0$. Dann ist $(-1) \cdot \alpha$ von der Form ϕ^n.

3. $a > 0$ und $b < 0$. Dann überlegt man sich, dass $a \geq |b|$ ist. Ist $a = |b|$, so ist $a = 1 = -b$. Es ist $1 - \phi = -\phi^{-1}$. Andernfalls ist $a > |b|$. Es folgt: $a + b(1 - \phi) = (a+b) + (-b)\phi = \phi^n$ für ein $n \in \mathbb{N}$. Daher ist $(a+b\phi) \cdot (a+b(1-\phi)) = (a+b\phi) \cdot \phi^n = \pm 1$. Damit ist $a + b\phi = \pm 1 \cdot \phi^{-n}$.

4. Den Fall $a < 0$ und $b > 0$ führt man durch Multiplikation mit -1 auf den eben betrachteten Fall zurück. □

Aufgaben:

13. Betrachte die Transformation, die sich aus der Aufgabe 5 ergibt:

$$W : \mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2y - x \\ x - y \end{pmatrix} \in \mathbb{R}^2$$
$$T : \mathbb{R}^2 \ni \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x + 2y \\ x + y \end{pmatrix} \in \mathbb{R}^2$$

    a) Die Abbildungen W und T sind invers zueinander.
    b) Wir definieren induktiv: $\begin{pmatrix} a(0) \\ b(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} a(n+1) \\ b(n+1) \end{pmatrix} = T \begin{pmatrix} a(n) \\ b(n) \end{pmatrix}$. Berechne $T^{10} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
    c) Wir bezeichnen $N(\vec{x}) = N(\begin{pmatrix} x \\ y \end{pmatrix}) = x^2 - 2y^2$. Zeige: $N(T(\vec{x})) = N(W(\vec{x})) = (-1)N(\vec{x})$.
    d) Zeige: Ist Sind $0 < x, 0 < y \in \mathbb{N}$ mit $x^2 - 2y^2 = 0$, so ist $x > y$ und $x < 2y$.
    e) Zeige mit dem Minimumprinzip, dass $x^2 - 2y^2 = 0$ in $\mathbb{N}^2$ keine Lösungen hat.
    f) Zeige: Ist $1 \leq x, 1 \leq y \in \mathbb{N}$ und $x^2 - 2y^2 = \pm 1$, so ist $x > y$ und $x < 2y$. Schraffiere das Gebiet in dem sich das Zahlenpaar $\begin{pmatrix} x \\ y \end{pmatrix}$ liegt.
    g) Zeige nun: Jede Lösung der Gleichung $x^2 - 2y^2 = \pm 1$ lässt sich durch wiederholte Anwendung von T erreichen, wenn man von $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ausgeht.

14. Wir wollen die gleichen Methoden wie in Satz 7 auf eine etwas andere Situation anwenden. Wir betrachten das Polynom $X^2 - 2X - 1$ und es sei α eine Nullstelle des Polynom. Wir definieren rekursiv. $a(0) = 1$, $a(1) = 0$ und $a(n+2) := a(n) + 2a(n+1)$ Zeige:

    a) Das Inverse von α ist $(2 - \alpha)$.
    b) $(2 - \alpha)$ ist die zweite Nullstelle des Polynoms.
    c) $\alpha^n = a(n-1) + a(n)\alpha$.

1.3.2 Der euklidische Ring $\mathbb{Z}[\phi]$

Unser Ziel ist es, die Zahlen n zu bestimmen für welche die Gleichung $x^2 + xy - y^2 = n$ in ganzen Zahlen lösbar sind. Das heißt: Welche natürlichen Zahlen tauchen als Norm einer Zahl aus $\mathbb{Z}[\phi]$ auf? Dazu gehören $\{1, 4, 5, 9, 11, \dots\}$. Unter den Primzahlen gehören dazu $\{5, 11, 19, 29, 31, \dots\}$. So ist beispielsweise $11 = 3^2 + 3 \cdot 2 - 2^2$. Aus diesem Zahlenmaterial kann man vermuten, dass es die Primzahlen der Form $p = 10n \pm 1$ sind. Um dies zu beweisen, müssen wir die Struktur des Ringes $\mathbb{Z}[\phi]$ tiefer verstehen.

Satz 17. *Zu jedem Paar rationaler Zahlen $x, y \in \mathbb{Q}$ gibt es ein Paar $(a, b) \in \mathbb{Z}^2$ mit:* $|(x-a)^2 + (x-a)(y-b) - (y-b)^2| < 1$

Zu x, y gibt es ein $a, b \in \mathbb{Z}$ mit $|x - a| \leq \frac{1}{2}, |y - b| \leq \frac{1}{2}$. Wir erhalten:

$$\begin{aligned} |(x-a)^2 + (x-a)(y-b) - (y-b)^2| &\leq |x-a|(|x-a| + |y-b|) + (y-b)^2 \\ &\leq \frac{1}{2} \cdot 1 + \frac{1}{4} < 1 \end{aligned}$$

Für $\alpha = a + b\phi \in \mathbb{Z}[\phi]$ bezeichnen wir mit $d(\alpha) := |N(\alpha)| = |a^2 + ab - b^2|$. Jetzt können wir in $\mathbb{Z}[\phi]$ analog wie in $\mathbb{Z}$ mit Rest teilen.

Satz 18 (Teilen mit Rest). *Zu je zwei Zahlen α, β mit $\beta \neq 0$ gibt es $q, r \in \mathbb{Z}[\phi]$ mit $\alpha = q \cdot \beta + r$ und $d(r) < d(\beta)$.*

Wir können den Nenner von $\frac{\alpha}{\beta}$ rational machen. Es ist daher $\frac{\alpha}{\beta} = x + y\phi$ mit $x, y \in \mathbb{Q}$. Es gibt ein $q = a + b\phi \in \mathbb{Z}[\phi]$ mit $d(\frac{\alpha}{\beta} - q) < 1$. Setzt man $r = \alpha - q\beta = (\frac{\alpha}{\beta} - q)\beta$, so folgt $d(r) = d(\frac{\alpha}{\beta} - q)d(\beta) < d(\beta)$. □

Einen kommutativen Ring nennen wir Integritätsring, wenn für alle $a, b \in R$ gilt: Ist $a \cdot b = 0$, so ist $a = 0$ oder $b = 0$.

Definition 1. Es sei R ein Integritätsring und $d : R^* := R \setminus \{0\} \to \mathbb{N} \setminus \{0\}$. Wir nennen d euklidische Normfunktion, wenn folgendes gilt:

1. Sind $a, b \in R^*$ dann gibt es $q, r \in R$ mit $a = q \cdot b + r$. Dabei ist $r = 0$ oder $d(r) < d(b)$.
2. Für alle $a, b \in R^*$ ist $d(a \cdot b) \geq d(a)$. Ein Ring mit euklidischer Normfunktion heißt euklidischer Ring.

Beispiele:

9. $\mathbb{Z}$ ist mit dem Absolutbetrag als Normfunktion ein euklidischer Ring.
10. Gerade haben wir gesehen, dass $\mathbb{Z}[\phi]$ mit der Norm $d(x + y\phi) := |x^2 + xy - y^2|$ ein euklidischer Ring ist. Er erfüllt die schärfere Bedingung $d(\alpha \cdot \beta) = d(\alpha) \cdot d(\beta)$ für alle $\alpha, \beta \in R^*$.
11. In den Übungen werden wir weitere Beispiele euklidischer Ringe kennenlernen.

In jedem euklidischen Ring funktioniert der euklidische Algorithmus, wie er in beispielsweise in [Bartholomé et al., 2008, Seite 36] erklärt ist. Wir erinnern an den Begriff des Ideals:

Definition 2. Eine Teilmenge $\mathfrak{a} \subset R$ heißt Ideal, wenn für alle $a, b \in \mathfrak{a}$ und alle $r \in R$ gilt $a + b \in \mathfrak{a}$ und $a \cdot r \in \mathfrak{a}$

Satz 19. *In einem euklidischen Ring ist jedes Ideal von einem Element erzeugt. Der Ring ist ein Hauptidealring.*

Sei $\mathfrak{b}$ ein Ideal in R nicht das Nullideal. Dann gibt es in dem Ideal $\mathfrak{b}$ ein b mit kleinstmöglichem $d(b) \neq 0$. Ist a aus dem Ideal, so ist $a = q \cdot b + r$ mit q, $r \in R$ und $d(r) < d(b)$.

1. Fall: $r = 0$. Dann ist $a \in b \cdot R$.
2. Fall: $r \neq 0$. Dann ist $d(r) < d(b)$. Dies kann nicht sein, da $r \in \mathfrak{b}$ ist, und b schon ein Element minimaler Norm aus diesem Ideal ist. □

Wir drücken jetzt den Begriff der Teilbarkeit durch Ideale aus.

Satz 20. *Sei R ein Integritätsring. Dann gilt: b teilt a genau dann, wenn $aR \subset bR$ ist.*

b teile a. Dann gibt es ein $x \in R$ mit $a = b \cdot x$. Das heißt $a \in bR$ und damit ist $aR \subset bR$. Sei umgekehrt $aR \subset bR$. Dann ist $a \in bR$. Es gibt daher ein $x \in R$ mit $a = bx$. Damit ist b ein Teiler von a. □

Jetz drücken wir mit von Idealen aus, wann ein Element $b \in R$ unzerlegbar ist.

Satz 21. *Für ein p in dem Integritätsring R sind äquivalent:*

1. *Ist $p = b \cdot x$, so ist x oder b eine Einheit.*
2. *Ist bR irgend ein Hauptideal $\neq R$, welches pR enthält, so ist $bR = pR$. Man sagt: In der Menge der echten Hauptideal ist pR maximal.*

1.$\Longrightarrow$2.: Es sei $pR \subset bR \neq R$. Dann gibt es ein $x \in R$ mit $p = b \cdot x$. Da b keine Einheit ist, sonst wäre $bR = R$, muss x eine Einheit sein. Daher ist $b = p \cdot x^{-1} \in pR$. Damit $pR = bR$.
2. $\Longrightarrow$1.: Sei pR maximal unter den echten Hauptidealen und $p = b \cdot x$. Es sei etwa b keine Einheit. Dann ist $p \in bR \neq R$. Also ist $pR \subset bR$ und damit $pR = bR$. Es gibt also ein y mit $b = p \cdot y$. Es folgt $b = py = bxy$ und damit $b(1 - xy) = 0$. Da R ein Integritätsring ist, ist $1 - xy = 0$. Das heißt $1 = xy$. Es ist also x eine Einheit. □

Definition 3. Ein Element p eines Integritätsringes R heißt unzerlegbar, wenn es die äquivalenten Eigenschaften des Satzes 21 erfüllt. Ein Element in dem Ring heißt prim, wenn für beliebige $a, b \in R$ gilt: Ist p ein Teiler des Produktes $a \cdot b$, so teilt p einen der Faktoren.

Satz 22. *Ist R ein Integritätsring dann gilt:*

1. *Ist p ein Primelement, so ist p unzerlegbar.*
2. *Ist R ein Hauptidealring, so ist jedes unzerlegbare Element auch prim.*

1. Dies ergibt sich sofort aus der Definition.
2. Das unzerlegbare Element p teile $a \cdot b$ aber nicht a. Dann ist $a \notin pR$. Also ist $pR \subsetneq pR + aR$. Da pR maximal unter den echten Hauptidealen ist muss $aR + pR = R$ sein. Es gibt daher ein x und ein $y \in R$ mit $ax + py = 1$. Daher ist $abx + pby = b$. Da $ab, p \in pR$ sind, ist auch $b \in pR$. Also ist p ein Teiler von b. □

Was sind Primelemente im goldnen Ring $\mathbb{Z}[\phi]$? Wir werden in Zukunft die Primzahlen in $\mathbb{Z}$ mit dem Namen „Primzahl“ bezeichnen. In anderen Ringen sagen wir „Primelement“.

Beispiele:

12. 2 ist in $\mathbb{Z}[\phi]$ ein Primelement. Dazu zeigen wir, dass 2 unzerlegbar in $\mathbb{Z}[\phi]$ ist. Angenommen es ist $2 = \alpha \cdot \beta$ mit $\alpha, \beta \in \mathbb{Z}[\phi]$. Dann ist $4 = d(2) = d(\alpha) \cdot d(\beta)$. Ist $d(\alpha) = 1$, dann ist α eine Einheit. Wäre $d(\alpha) = 2$, so gäbe es $x, y \in \mathbb{Z}$ mit $2 = x^2 + xy - y^2$. Dies ist unmöglich (Siehe Aufgabe 2) Also bleibt nur übrig, dass $d(\alpha) = 4$ ist. Dann ist aber β eine Einheit.
13. Genauso zeigt man, dass 3 ein Primelement ist $\mathbb{Z}[\phi]$ ist.
14. Ist $\alpha \in \mathbb{Z}[\phi]$ und $d(\alpha)$ eine Primzahl, dann ist α ein Primelement. Denn sei $d(\alpha) = p$ und p eine Primzahl. Angenommen es ist $\alpha = \beta \cdot \gamma$ mit $\beta, \gamma \in \mathbb{Z}[\phi]$. Dann ist $d(\alpha) = p = d(\beta) \cdot d(\gamma)$. Also ist β oder γ eine Einheit. Also ist beispielsweise $2 + \phi$ ein Primelement in $\mathbb{Z}[\phi]$. Die Umkehrung dieser Bemerkung gilt nicht, wie wir bei 2, oder auch 3 gerade gesehen haben.

Satz 23. *In einem euklidischen Ring R hat jede Nichteinheit $a \neq 0$ ein Primelement als Faktor.*

Sei $a \in R$ keine Einheit und $a \neq 0$. Dann gibt es unter den Faktoren von a einen α mit kleinstmöglicher euklidischer Norm.
Beh.: Dieses α ist unzerlegbar und damit prim.
Bew.: Angenommen es ist $\alpha = \beta \cdot \gamma$. mit $\beta, \gamma \in R$. Dann ist $d(\alpha) \geq d(\beta)$. Es gibt $q, r \in R$ mit $\beta = q \cdot \alpha + r$. Da β ein Teiler von α ist, teilt β auch r. Wäre $r \neq 0$, so wäre $d(\beta) \leq d(r) < d(\alpha)$. Dies geht nicht, da ja schon α ein Teiler mit kleinster Norm von a ist. Es folgt $r = 0$. Damit folgt $\beta = q \cdot \alpha = q \cdot \beta \cdot \gamma$. Daher ist γ eine Einheit. Damit ist α unzerlegbar und daher ein Primelement. □

Satz 24. *Ist $p > 2$ eine Primzahl, so dass 5 ein quadratischer Rest modulo p ist, so ist p in $\mathbb{Z}[\phi] = R$ zerlegbar und es ist p die Norm eines Elementes α. Dabei ist α ein Primelement in $\mathbb{Z}[\phi]$.*

Da 5 ein quadratischer Rest modulo p ist, gibt es in $\mathbb{Z}/p\mathbb{Z}$ ein a mit $a^2 - a - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Die Abbildung $\rho : \mathbb{Z}[\phi] \ni x + y\phi \mapsto x + ya \in \mathbb{Z}/p\mathbb{Z}$ ist daher ein Ringhomomorphismus. Wir haben $\rho(a - \phi) = a - a = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Daher ist $a - \phi \in \text{Kern}(\rho)$. Aber es ist $a - \phi \notin pR$. Es gibt ein $\alpha \in R$ mit $pR \subsetneq \text{Kern}(\rho) = \alpha R$. Daher ist α ein echter Teiler von p. Es gibt also ein $\beta \in R$ mit $p = \alpha \cdot \beta$. Daher ist $p^2 = d(p) = d(\alpha) \cdot d(\beta)$, wobei α, β keine Einheiten sind. Daher ist $d(\alpha) = p$. □

Satz 25. *Die Primzahl $p > 2$ ist in $\mathbb{Z}[\phi]$ genau dann unzerlegbar, wenn p nicht die Norm eines Elementes α ist.*

Angenommen es ist $p = N(\alpha) = x^2 + xy - y^2$. Dabei ist x nicht durch p teilbar. Denn sonst wäre auch y durch p teilbar und damit p durch p^2. Also können wir in $\mathbb{Z}/p\mathbb{Z}$ die Gleichung $x^2 + xy - y^2$ durch $-x^2$ teilen und erhalten

$$\left(\frac{y}{x}\right)^2 - \left(\frac{y}{x}\right) - 1 = 0$$

Also hat in $\mathbb{Z}/p\mathbb{Z}$ die Gleichung $x^2 - x - 1 = 0$ eine Lösung α. Damit ist $(2\alpha - 1)^2 = 4(\alpha^2 - \alpha - 1) + 5 = 5$. Damit ist 5 quadratischer Rest daher ist p zerlegbar. Dies widerspricht der Voraussetzung.

Zur Umkehrung. Seien α, β, so dass $p = \alpha \cdot \beta$ ist. Dann ist $p^2 = N(\alpha) \cdot N(\beta)$. Es kann $N(\alpha) = p$ nicht gelten nach Voraussetzung. Daher ist $N(\alpha) = 1$ oder es ist $N(\alpha) = p^2$. Im ersten Fall ist α eine Einheit, im zweiten Fall ist β Einheit. Das heißt p ist unzerlegbar.□

Jetzt können wir den Satz von der eindeutigen Primfaktorzerlegung im Hauptidealring beweisen.

Satz 26. *In jedem Hauptidealring ist jedes Element des Ringes bis auf Einheiten eindeutiges Produkt von Primelementen.*

Wir beweisen den Satz nur für euklidische Ringe. Dazu verwenden wir fast wörtlich den Beweis zum Hauptsatz der elementaren Zahlentheorie. Der Sinn unserer ganzen Mühe war es ja, genau die gleichen Argumente in einer allgemeineren Situation zu verwenden. Angenommen es gibt Ringelemente $a \neq 0$, die keine Einheiten sind und nicht eindeutiges Produkt von Primelementen sind. Unter diesen gibt es ein a mit kleinstmöglicher euklidischer Norm $d(a)$. Ist a selber ein Primelement ist man fertig. Andernfalls hat diese a einen Primfaktor π. Es ist also $a = \pi \cdot b$, für ein $b \in R$. Es ist $d(b) < d(a)$. Daher ist b eindeutiges Produkt von Primelementen. $b = \pi_1 \cdots \pi_n$. Es ergibt sich $a = \pi \cdot \pi_1 \cdots \pi_n$. Dass dieses Produkt eindeutig bis auf Einheiten ist zeigt man genauso, wie im Falle $\mathbb{N}$.□

Der Satz gilt in jedem Hauptidealring. Der Leser kann ihn zum Beispiel in dem Algebrabuch von Bosch [Bosch, 1993, Seite 45 ff] nachlesen. Er muss aber ein unkonstruktives Argument gelten lassen. Es wird dort belegt, dass jedes Element einen Primfaktor hat, aber keiner sagt uns, wie man diesen finden soll. In euklidischen Ringen ist dies möglich. Bis jetzt wissen wir welche Primzahlen als Norm vorkommen. Der Satz von der eindeutigen Primfaktorzerlegung in $\mathbb{Z}[\phi]$ ermöglicht es jetzt alle natürlichen Zahlen kennen zu lernen, die als Norm vorkommen. Noch eine kleine Bemerkung zu den Primelementen in $\mathbb{Z}[\phi]$

Satz 27. *$\alpha := a + b\phi \in \mathbb{Z}[\phi]$ ist genau dann Primelement in $\mathbb{Z}[\phi]$, wenn $\rho(\alpha) = a + b(1 - \phi)$ ein Primelement ist.*

Dies liebe Leserin ist ein geeignete Übungsaufgabe für dich. Noch eine weitere Bemerkung ist wichtig.

Satz 28. *Ist $\pi \in \mathbb{Z}[\phi]$ ein Primelement, so ist $N(\pi) = \pm 1 \cdot p$ oder $N(\pi) = \pm 1 \cdot p^2$ für eine Primzahl $p \in \mathbb{N}$.*

Es sei $N(\pi) = p \cdot a$ mit $a \in \mathbb{N}$. Da π ein Primelement ist, teilt π die Zahl p oder a.

1. Es ist $p = \pi \cdot \alpha$ mit $\alpha \in \mathbb{Z}[\phi]$. Damit ist $N(\pi) = \pi \cdot \rho(\pi) = \pi \cdot \alpha \cdot a$. Es ergibt sich $\rho(\pi) = \alpha \cdot a$. Da $\rho(\pi)$ ein Primelement in $\mathbb{Z}[\phi]$ ist, muss α oder a eine Einheit sein. Ist a eine Einheit, so ist $N(a) = a^2 = 1$ und daher $a = \pm 1$. Also ist $N(\pi) = \pm p$. Ist α eine Einheit in $\mathbb{Z}[\phi]$, so ist $p^2 = N(p) = N(\pi) \cdot N(\alpha) = \pm 1 \cdot N(\pi)$.

2. π ist ein Teiler von a. Dann ist $\pi \cdot \rho(\pi) = p \cdot \pi \cdot \alpha$ für ein $\alpha \in \mathbb{Z}[\phi]$. Wir erhalten $\rho(\pi) = p\alpha$. Dann ist α eine Einheit und es folgt: $N(\rho(\pi)) = N(\pi) = p^2 \cdot (\pm 1)$. □

Jetzt endlich erscheint die Antwort der Frage, welche natürlichen Zahlen sind die Norm einer Zahl aus $\mathbb{Z}[\phi]$ hell am Horizont.

Satz 29. *Die natürliche Zahl n ist die Norm eines Elementes $\alpha \in \mathbb{Z}[\phi]$ genau dann, wenn in der Primfaktorzerlegung in $\mathbb{N}$ alle in $\mathbb{Z}[\phi]$ unzerlegbaren Primzahlen nur mit geradem Exponenten vorkommen.*

In $\mathbb{Z}[\phi]$ sind genau die natürlichen Primzahlen p unzerlegbar, bei denen 5 kein quadratischer Rest modulo p ist. Später wird sich herausstellen, dass dies genau die Primzahlen der Form $5n \pm 2$ sind. Jetzt mit frischem Mut zum Beweis:

Für $n = \pm 1$ gilt die Behauptung sicher. Angenommen es gibt eine natürliche Zahl, für die Behauptung des Satzes nicht gilt. Dann gibt es auch eine kleinste dieser Sorte $n = N(\alpha)$. Wir zerlegen α in Primfaktoren in $\mathbb{Z}[\phi]$, $\alpha = N(\pi_1 \cdots \pi_k)$. Es sei $n = p \cdot a$ mit der Primzahl p und natürliche Zahl a. Man erhält

$$n = p \cdot a = N(\pi_1 \cdots \pi_k).$$

Ohne Einschränkung können wir annehmen, dass p die Zahl $N(\pi_1)$ teilt. Ist $p = N(\pi_1)$, dann ist auch a die Norm eines Elementes aus $\mathbb{Z}[\phi]$. Für die kleinere Zahl a trifft aber die Behauptung des Satzes zu. Im andern Fall ist $p^2 = N(\pi_1)$. Diesmal können wir die Gleichung durch p^2 teilen. Damit ist der Satz bewiesen. □

2 Was hat 5 mit großen Primzahlen zu tun?

Es gibt einen erstaunlichen Zusammenhang zwischen der Zahl 5 den Fibonacci Zahlen und den größten Primzahlen, die wir bis heute kennen. Den so genannten Mersennschen Primzahlen. Diesen Zusammenhang entdeckte Edouard Lucas im 19ten Jahrhundert. Sein Primzahltest wird noch heute mit Computern angewendet, wenn sie Zahlen $2^p - 1$ auf Primalität testen. Dabei ist p selber eine Primzahl. Um den Test von Lucas zu verstehen sind ein paar Vorbereitungen notwendig.

2.1 Fermat in anderen Ringen

Wir wollen den kleinen Satz von Fermat auf andere Ringe übertragen. Um etwas vor Augen zu haben betrachten wir Unterringe des 2×2 Matrizenringes über $\mathbb{Z}/n\mathbb{Z}$. Euler hat als erster den Satz von Fermat bewiesen und dabei die binomischen Formeln verwendet.

$$(a+b)^n = a^n + \binom{n}{1} \cdot a^{n-1} \cdot b + \binom{n}{2} \cdot a^{n-2} \cdot b + \ldots + b^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} \cdot b^i.$$

Er zeigte, dass $\binom{p}{k} = 0$ in $\mathbb{Z}/p\mathbb{Z}$ für alle Primzahlen p und alle $1 \leq k < p$ gilt. Es ist dann $(x+y)^p = x^p + y^p$ für alle $x, y \in \mathbb{Z}/p\mathbb{Z}$. Damit ist die Abbildung $\rho : \mathbb{Z}/\ni\mathbb{Z}x \mapsto x^p \in \mathbb{Z}/p\mathbb{Z}$ ein Ringhomomorphismus. Insbesondere ist $(1+x)^p = 1 + x^p$. Durch Induktion folgt dann: $x^p = x$ für alle $x \in \mathbb{Z}/p\mathbb{Z}$. Von diesen Gedanken wollen wir uns inspirieren lassen. Wir müssen dabei noch ein paar Hürden überwinden. Berechnen wir in einem allgemeinen Ring $(a+b)^2$ so erhalten wir $a^2 + ab + ba + b^2$. Nur dann dürfen wir dies durch $a^2 + 2ab + b^2$ ersetzen, wenn $ab = ba$. Wir sagen in diesem Fall $a, b \in R$ sind vertauschbar. Wir setzen am besten voraus, dass R kommutativ ist. In Ist $A \in R^{(2,2)}$ eine Matrix und R kommutativ, so ist $R[A]$ der kleinste Unterring von $R^{(2,2)}$, der A enthält, so $R[A]$ kommutativ. Nur für solche Ringe wollen wir den kleinen Satz von Fermat verallgemeinern. Zunächst berechnen wir die Binomialkoeffizienten indem wir nur addieren. Wir definieren rekursiv.

$$B(n,0) := B(n,n) := 1 \text{ für alle } n \in \mathbb{N}$$
$$B(n+1,k) := B(n,k-1) + B(n,k) \text{ für } 1 \leq k < n$$

1				
1	1			
1	2	1		
1	3	3	1	
1	4	6	4	1

Mit dieser Definition können wir das so genannte pascalsche Dreieck in jedem Ring berechnen. In $\mathbb{Z}$ ergibt sich das nebenstehende Beispiel.

Satz 30 (binomischer Lehrsatz). *Ist R ein Ring, in dem a, b vertauschbar sind, so gilt:* $(a+b)^n = \sum_{k=0}^{n} B(n,k) a^{n-k} b^k$.

Die Formel gilt sicherlich für $n = 0, 1, 2$. Sie gelte für $n+1$. Wir betrachten das Produkt $(a+b)^n \cdot (a+b)$. In der entstehenden Summe ist der Koeffizient von $a^{n-k}b^k$ gleich $B(n, k-1) + B(n,k) = B(n+1, k)$. Damit folgt die Behauptung. □

Der nächste Satz ist in $\mathbb{Z}$ schon bekannt. Aber wir wollen die bekannte Tatsache ohne Quotienten schreiben.

Satz 31. *Es gilt für alle $0 < k < n$: $k! \cdot B(n,k) = n \cdot (n-1) \cdots (n-k+1)$.*

Für $n = 0$ und $n = 1, 2$ ist die Behauptung klar. Die Behauptung gelte für $n \geq 2$. Wir betrachten $B(n+1, k)$ mit $1 \leq k \leq n$. Ist $k = n$, so ist $B(n+1, n) = B(n,n) + B(n-1) = n+1$. Man erhält: $n!(n+1) = (n+1) \cdot 22$. Für $k < n$ folgt: $k!B(n+1,k) = k!(B(n,k) + B(n,k-1)) = (n+1) \cdots (n+1-(k-1))$. Das war zu zeigen. □

Jetzt kommen wir zu der Folgerung, auf die es uns ganz besonders ankommt:

Folgerung 32. *Ist die Charakteristik eines Ringes R eine Primzahl p, so ist $B(p,k) = 0$ in R für alle $1 \leq k < p$.*

Da p eine Primzahl ist und kein Teiler von $k!$ ist muss p die Zahl $B(p,k)$ teilen. □

Satz 33. *Ist die Charakteristik eines Ringes eine Primzahl p, so ist die Abbildung $\rho : R \ni x \mapsto x^p$ ein Homomorphismus des Ringes in sich.*

Es ist sicher $(x \cdot y)^p = x^p \cdot y^p$ und $1^p = 1$. Außerdem ist $(x+y)^p = x^p + y^p$, da $B(n,k) = 0$ ist für alle $1 \leq k < p$. □

Als Folgerung aus diesem Satz ergibt sich, wie es Euler schon hergeleitet hat der kleine Satz von Fermat. Aber viel mehr. Ist α in dem Ring $\mathbb{Z}/p\mathbb{Z}^{(2,2)}$ eine Lösung einer Gleichung der Form $x^2 + p \cdot x + q$ und $R = \mathbb{Z}/p\mathbb{Z}[\alpha]$ wie gewöhnlich so können wir leicht für jedes Ringelement ausrechnen, was $(a + b \cdot \alpha)^p$. Wir brauchen ja nur α^p zu berechnen. Für unsere Lieblingsgleichung wollen wir dies durchführen. Dem Leser überlassen wir andere Fälle.

Satz 34. *In dem Ring R sei α Lösung der goldenen Gleichung $x^2 - x - 1$. Außerdem sei die Charakteristik des Ringes eine Primzahl $p > 2$. Dann gilt:*

1. *Ist $p = 5$, so ist $\alpha^p = 3$.*
2. *Ist 5 ein quadratischer Rest modulo p, so ist $\alpha^p = a$.*
3. *Ist 5 kein quadratischer Rest modulo p, dann ist $\alpha^p = 1 - \alpha$.*

Es ist $\alpha^2 - \alpha - 1 = 0$ in R. Dies ergibt $(2\alpha - 1)^2 = 4(\alpha^2 - \alpha - 1) + 5 = 5$. Es ist daher $(2\alpha-1)^{p-1} = ((2\alpha-1)^2)^{\frac{p-1}{2}}$. Also ist $(2\alpha-1)^p = 5^{\frac{p-1}{2}}(2\alpha-1) = 2^p\alpha^p - 1^p = 5^{\frac{p-1}{2}}(2\alpha-1)$. Wegen dem kleinen Satz von Fermat folgt: $2 \cdot \alpha^p = 1 + 5^{\frac{p-1}{2}}(2\alpha - 1)$.

1. $p = 5$. Dann ist $2\alpha^5 = 1$ und daher $\alpha^5 = 3$.
2. 5 ist quadratischer Rest modulo p. Dann ist $5^{\frac{p-1}{2}} = 1$ in R. Also ist $2 \cdot \alpha^p = 1 + 2\alpha - 1 = 2\alpha$. Daher ist $\alpha^p = a$.
3. 5 ist kein Quadrat. Dann ist $5^{\frac{p-1}{2}} = -1 \in R$. Also ist $2 \cdot \alpha^p = 1 - (2\alpha - 1) = 2 - 2\alpha$. Dann ist $\alpha^p = 1 - \alpha$. □

Folgerung 35. *Die Voraussetzung seien wie in dem Satz 34 und $\beta = a + b\alpha \in R, a, b \in \mathbb{Z}$. Dann gilt:*

1. *$p = 5$, so ist $\beta^5 = a + 3b$.*
2. *Ist 5 ein quadratischer Rest modulo p, so ist $\beta^p = \beta$.*
3. *Ist 5 kein quadratischer Rest modulo p, dann ist $\beta^p = a + b(1 - \alpha)$ und $\beta^{p^2} = \beta$.*

Dies rechnet man einfach.
Aufgaben:

15. Zeige: In jedem Ring R gilt:

    a) $2^n = \sum_{i=0}^{n} B(n, i)$.

    b) $\sum_{i=0}^{n} B(n, i)^2 = \binom{2n}{n}$.

    Viele weitere Aufgaben zu den Binomialkoeffizienten findet man in dem schönen Buch von Matoušek und Nešetřil [Matoušek and Nešetřil, 2002, Kapitel 2.3]. Dort geht es mehr um den Zusammenhang zur Kombinatorik.

16. Gib ein Beispiel für a, b in einem Ring R an, so dass $a^2 + 2ab + b^2 \neq (a + b)^2$ gilt.

17. a) Wir betrachten $B(n, k)$ in $\mathbb{Z}/2\mathbb{Z}$.
        i. Berechne bis $n = 16$ den Binomialkoeffizienten $B(n, k)$ in $\mathbb{Z}/2\mathbb{Z}$. Dies ergibt ein interessantes Muster.
        ii. Für welche n ist $B(n, 2) = 0$?
        iii. Für welche $n \in \mathbb{N}$ ist $B(n, k) = 0$?

    b) Führe dieselben Berechnungen wie in der Aufgabe vorher durch nur diesmal in $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$.

18. Es sei K ein Körper $(\mathbb{Q}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z})$, in dem die quadratische Gleichung $x^2 + ax + b = 0$ $(a, b \in K)$ keine Lösung hat. Weiter sei $R = K^{(2,2)}$ der 2×2 Matrizenring über K.

    a) Zeige: Die Matrix $\alpha = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$ ist in R eine Lösung der Gleichung.

b) α ist invertierbar in $K[\alpha]$.

c) Zeige:$\beta = b \cdot \alpha^2$ ist die zweite Lösung der Gleichung.

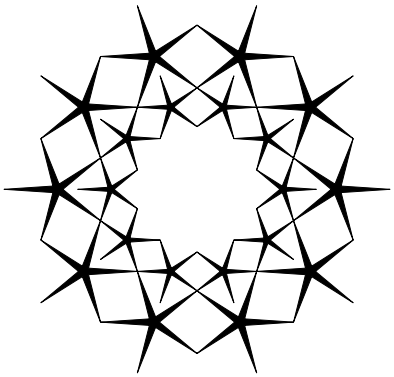
d) Die Abbildung $\rho : K[\alpha] \ni x + y\alpha \mapsto x + y\beta \in K[\alpha]$ ist ein Ringhomomorphismus, der sämtliche Elemente aus K festlässt. Der einzige weitere Homomorphismus dieser Art ist die Identität.

e) Die Abbildung $N : K[\alpha] \ni \gamma \mapsto \gamma \cdot \rho(\gamma)$ ist multiplikativ.

f) $K[\alpha]$ ist ein Körper. Das heißt jedes Element $\neq 0$ ist bezüglich der Multiplikation invertierbar in $K[\alpha]$.

g) Es sei nun $K = \mathbb{Z}/p\mathbb{Z}$. Berechne α^p ind $K[\alpha]$.

2.2 Der Lucas Test



Wir haben schon mehrfach von Mersennschen Primzahlen gesprochen. Das sind Primzahlen der Form 2^p-1, wobei p eine Primzahl ist. Von Zeit zu Zeit geht durch die Presse die Meldung, dass wieder eine solche gigantische Primzahl gefunden wurde. Die größte (bis August 2008) bekannte Mersenne-Primzahl ist $M_{43112609} = 2^{43112609} - 1$ (Curtis Cooper and Steven Boone/GIMPS). GIMPS ist ein Programm zur Suche großer Primzahlen.
Hat man einen Computer, der nachts nichts zu tun hat, kann man sich mit GIMPS an der Suche beteiligen ohne auch das Geringste von Primzahlen zu verstehen. Es fragt sich welchen Erkenntnisgewinn man davon hat. $M_{43112609}$ ist zugleich auch die größte bekannte Primzahl.Wir wollen Einsicht. Daher bemühen wir uns in diesem den Test zu verstehen, den das Programm GIMPS verwendet. Er ist lange vor der Computerzeit von Edouard Lucas entwickelt worden. Beim Verständnis dieses Testes hilft uns wieder der Ring der goldenen Zahlen.
Wir betrachten in dem Ring $\mathbb{Z}[\phi]$ die Folge:

$$r(n) := \phi^{2^n} + (1-\phi)^{2^n} \tag{2.1}$$

Es gilt:

$$\begin{aligned} r(1) = \phi^2 + (1-\phi)^2 = \phi^{2+1} - 2\phi + \phi^2 = 2(\phi^2 - \phi - 1) + 3 = 3. \\ \vdots = \vdots \\ (\phi^{2^m} + (1-\phi)^{2^m})^2 = \phi^{2^{m+1}} + 2(\phi(1-\phi))^{2^m} + (1-\phi)^{2^{m+1}} = r(m+1) + 2. \end{aligned}$$

Daher ist $r(m+1) = r(m)^2 - 2$. Das ergibt eine sehr schnell wachsende Folge natürlicher Zahlen: 3, 7, 47, 2207, 4870847, 23725150497407, ...
Alle $r(m)$ sind untereinander teilerfremd. Denn $r(m) = 0 \bmod p$. Daher ist $r(m+1) = -2 \bmod p$ und $r(m+2) = 2 \bmod p$. Also folgt die Behauptung.

Multiplizieren wir die Gleichung 2.1 mit ϕ^{2^n}, so erhalten wir:

$$\phi^{2^n} \cdot r(n) = \phi^{2^{n+1}} + (-1)^{2^n} = \phi^{2^{n+1}} + 1 \tag{2.2}$$

Hieraus ergibt sich die Entdeckung von Lucas:

Satz 36. *Ist p eine Primzahl der Form $4n+3$ und ist $M = 2^p - 1$ eine Primzahl, so ist $r(p-1)$ durch M teilbar.*

Es sei M eine Primzahl. Es ist

$$\begin{aligned} M &= 2^p - 1 = 2^{4n+3} - 1 \\ &= 8 \cdot 16^n - 1 = 8 - 1 \bmod 10 = 7 \bmod 10 \end{aligned}$$

Also ist 5 modulo M kein Quadrat. Wir betrachten den Ring $R = (\mathbb{Z}/M\mathbb{Z})[\phi]$. In diesem Ring ist wegen Satz 34: $\phi^M = (1 - \phi)$ und daher

$$\phi^{M+1} = \phi(1 - \phi) = -1 \bmod M.$$

Setzt man $p - 1$ für n in der Gleichung 2.2 ein so ergibt sich:

$$\phi^{2^{p-1}} \cdot r(p-1) = \phi^{M+1} + 1$$

Auf der rechten Seite der Gleichung steht 0 in R. Da ϕ in R eine Einheit ist, muss $r(p-1)$ durch M teilbar sein. □

Auch die Umkehrung des Satzes gilt. Auf dem Wege dahin zeigen wir zwei Teilergebnisse, die selber von Bedeutung sind.

Satz 37. *Sei q ein Primfaktor von $r(n)$. Dann gilt:*

1. *Ist 5 ein quadratischer Rest modulo q, so ist $q - 1$ ein Vielfaches von 2^{n+2}.*
2. *Ist 5 kein quadratischer Rest modulo q, so ist $q + 1$ ein Vielfaches von 2^{n+1}*

Wieder betrachten wir die Gleichung 2.2 in $\mathbb{Z}[\phi]$.

1. Da 5 ein quadratischer Rest modulo q ist, gibt es in $\mathbb{Z}/q\mathbb{Z}$ eine Lösung a der goldenen Gleichung $x^2 - x - 1 = 0$. Also gibt es genau einen unitären Ringhomomorphismus $\rho : \mathbb{Z}[\phi] \to \mathbb{Z}/q\mathbb{Z}$ mit $\rho(\phi) = a$. In $\mathbb{Z}/q\mathbb{Z}$ erhalten wir dann, da $r(n)$ durch q teilbar ist:

   $$0 = a^{2^n} \rho(r(n)) = a^{2^{n+1}} + 1 \iff a^{2^{n+1}} = -1$$

   Damit ist die Ordnung von a in $\mathbb{Z}/q\mathbb{Z}$ gleich 2^{n+2}. Daher ist $q - 1$ ein Vielfaches von 2^{n+2}.

2. Da es in $\mathbb{Z}/q\mathbb{Z}$ keine Lösung der goldenen Gleichung gibt, betrachten wir in dem 2×2 Matrizenring über $\mathbb{Z}/q\mathbb{Z}$ die Matrix $\phi = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ und den kleinsten Unterring $\mathbb{Z}/q\mathbb{Z}[\phi]$, der diese Matrix enthält. ϕ ist in diesem Ring Lösung der goldenen Gleichung. Daher ist die Ordnung von ϕ in diesem Ring wieder 2^{n+2}. Andererseits ist $\phi^q = 1 - \phi$ (wegen Satz 34). Daher ist $\phi^{2(q+1)} = 1$. Es ist also $2 \cdot (q+1)$ ein Vielfaches von 2^{n+2} und damit ist $q - 1$ ein Vielfaches von 2^{n+1}. □

Verdeutlichen wir uns dies nochmal an Zahlen.
Beispiele:

15. Es ist $r(1) = 3$, $r(2) = 7$, $r(3) = 47$, $r(4) = 2207$ und $r(5) = 4870847 = 1087 \cdot 4481$. Weiter ist 1374 eine Lösung der Gleichung $x^2 - x - 1 = 0$ in $\mathbb{Z}/4481\mathbb{Z}$. Die Ordnung von 1374 modulo 4481 ist gleich $2^7 = 2^{5+2}$ und $4480 = 35 \cdot 128$.

16. Wie wir sehen ist 1087 ein Primfaktor der Form $10n \pm 3$. Diesmal ist 1088 ein Vielfaches einer Potenz von 2. Es ist $1088 = 17 \cdot 64 = 17 \cdot 2^6$.

In der Folge $(r(n)|n \in \mathbb{N})$ treten also nur große Primfaktoren auf. Jetzt folgt die Umkehrung des Satzes 36

Satz 38. *Ist $M = 2^p - 1$ ein Teiler von $r(p-1)$, so ist M eine Primzahl.*

In der Folge $(r(n)|n \in \mathbb{N})$ treten nur Primfaktoren der Form $k \cdot 2^{n+2} + 1$ und $l \cdot 2^{n+1} - 1$ auf.

Es sei q ein Primfaktor von M dann ist q auch ein Primfaktor von $r(p-1)$.

1. q ist von der Form $k \cdot 2^{p+1} + 1$. Dies kann nicht sein, da $q \leq M$ ist.

2. Es ist q von der Form $l \cdot 2^p - 1$. Dann muss $l = 1$ gelten. Daher ist $q = M = 2^p - 1$ eine Primzahl. □

Im Grunde ist die Berechnung der Folge $r(n)$ nichts anders, als die Berechnung von $\phi^k + (1-\phi)^k$ nach dem ägyptischen Verfahren. Diese Überlegungen stammen im Wesentlichen von Edouard Lucas aus der Arbeit Lucas [1876]. Er wandte dies an um zu entscheiden wann eine Zahl der Form $2^n - 1$ Primzahl ist. Man muss ja nur $r(p-1)$ modulo $M = 2^p - 1$ berechnen. Auf diese Weise berechnete er, dass $2^{127} - 1$ eine Primzahl ist lange vor der Computerzeit. Wie man sieht ist doch das entscheidende der Gedanke nicht unbedingt die Maschine. Sie erleichtert nur manchmal unsere Arbeit. Die Methode von Lucas ist leicht zu programmieren.
Aufgaben:

19. Bestätige den Satz 37 noch einmal an $r(6)$.

20. Besorge dir Daten darüber, wie lange ein zeitgemäßer Computer für eine Probedivision braucht. Mit dem naiven Verfahren soll getestet werden, ob $M = 2^{127} - 1$ eine Primzahl ist. Naives Verfahren bedeutet: Probediviedieren bis der Probeteiler $\geq \sqrt{M}$ ist.

21. Es sei p eine Primzahl, so dass 5 quadratischer Rest modulo p ist und a eine Lösung der goldenen Gleichung in $\mathbb{Z}/p\mathbb{Z}$. Zeige: $a^p + (1-a)^p = 1$ in $\mathbb{Z}/p\mathbb{Z}$.

22. Ist $\frac{p-1}{2}$ ungerade, so ist $a^{\frac{p-1}{2}} + (1-a)^{\frac{p-1}{2}} = 0$ in $\mathbb{Z}/p\mathbb{Z}$.

23. Ist $\frac{p-1}{2}$ gerade, so ist $a^{\frac{p-1}{2}} + (1-a)^{\frac{p-1}{2}} = \pm 2$.

24. Man könnte auch die Folge: $s(n) = (3+5\phi)^{2^n} + (8-5\phi)^{2^n}$ betrachten. Gelten für diese Folge analoge Aussagen wie für die von uns betrachtete Folge?

25. Es sei allgemein α eine Einheit $\neq \pm 1 \in \mathbb{Z}[\phi]$. β die zu α konjugierte Zahl. Das heißt es ist $\beta = \rho(\alpha)$, wenn ρ der Ringhomomorphismus $\rho : \mathbb{Z}[\phi] \ni x + y\Phi \mapsto x + y(1-\phi) \in \mathbb{Z}[\phi]$ ist. Wir definieren $s(n) = \alpha^{2^n} + \beta^{2^n}$. Gelten analoge Aussagen für $s(n)$?

26. Unser Verfahren (das ursprüngliche von Lucas) liefert nur für die Primzahlen der Form $p = 4n+3$ ob $M = 2^p - 1$ eine Primzahl ist oder nicht. Es ist aber leicht so zu verbessern, dass es stets zum Erfolg führt. Man muss in der Folge mit $r(1) = 4$ starten. Ansonsten ändert sich beim Algorithmus nichts. Um die Gültigkeit zu beweisen rechnet man diesmal in $\mathbb{Z}[\sqrt{3}]$. Man definiert dann $r(m) := (2+\sqrt{3})^m + (2-\sqrt{3})^m$. Es ist jetzt eine Übungsaufgabe die Einzelheiten ähnlich wie im Text durchzuführen. Man kann auch im Buch von Forster [Forster, 1996, Seite 143] oder von Müller Piontkowski [2006] nachlesen.

Computerecke:

10. Die Methode von Lucas ist denkbar einfach zu programmieren. Wir verwenden die Folge $(r(n)|n \in \mathbb{N})$, die für alle p ergibt ob $M = 2^p - 1$ Primzahl ist oder nicht. Wir starten daher mit $r(1) = 4$. Die folgende Funktion berechnet dann $r(n)$ mod M. Ist $r(p-1) = 0$, so ist M eine Primzahl.

```
(defun rmod(n p)
  (let ((k (- n 1)) (h 4))
  (dotimes (i k)
     (setq h (- (mod (* h h) p) 2))
   )
  h)
)
```

11. Mit dieser Funktion `(rmod n p)` ergibt sich sofort eine Funktion, welche uns angibt ob eine bestimmt Zahl Mersenne Primzahl ist oder nicht.

```
(defun mersenne (n)
  "Ergibt T wenn 2^n-1 die nte
  Mersenne Primzahl ist"
 (let ((p (- (expt 2 n) 1)))
     (= (rmod (- n 1) p) 0)
))
```

Auf einem PC ergibt beispielsweise der Aufruf `(mersenne 11213)` nach einer halben Minute `T`.

Literaturverzeichnis

Andreas Bartholomé, Josef Rung, and Hans Kern. *Zahlentheorie für Einsteiger*. Vieweg, Braunschweig Wiesbaden, 6 edition, 2008.

Siegfried Bosch. *Algebra*. Springer, Berlin Heidelberg, 1993.

Otto Forster. *Algorithmische Zahlentheorie*. Vieweg, 1996.

G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford Universty Press, 5 edition, 1979.

Edouard Lucas. Sur la recherche des grandes premiers. *Séances Mathématik*, 1876.

J. Matoušek and J. Nešetřil. *Diskrete Mathematik*. Springer, Berlin Heidelberg, 2002.

Stefan Müller-Stach Jens Piontkowski. *Elementare und algebraische Zahlentheorie*. Vieweg, Wiesbaden, 2006.