Über Fibonacci-Folgen

Thorsten Reinecke*

(2003-01-30, aktualisiert 2004-06-06)

Zusammenfassung

In dieser Ausarbeitung werden einige grundlegende und altbekannte Erkenntnisse und Eigenschaften über Fibonacci-Folgen hergeleitet sowie die Lucasfolge motiviert.

Vorbemerkungen und Erläuterungen

Die Bezeichnungen »grundlegend« und »altbekannt« sind so zu verstehen, daß einem Experten hier nichts (grundlegend) neues geboten wird. Viele weitere Themen (Lucasfunktionen U/V, Primzahltheorie, etc.) sind nicht behandelt, sie gehören aber vermutlich auch nicht mehr zu den Grundlagen, sondern bilden ein erweitertes Theoriegebäude.

Zum Inhalt: Die Story mit den Bienen (1.2) stammt aus [DoOl95] und kann anhand von [MiEn02] geprüft werden. Das Grundlagenkapitel beinhaltet eigentlich nur Trivialitäten; Restklassenbetrachtungen durchzuführen, war meine eigene Idee, sie erwiesen sich als nützlich für spätere Beweise. Das Kapitel 3 leitet die Lucaszahlen her und war die Motivation für diese Ausarbeitung: Ursprünglich wollte ich nur eine Formel für die schnelle Berechnung großer Werte allgemeiner Fibonaccifolgen herleiten. Ich habe erst später entdeckt, daß mein Ansatz auf die Lucasfolge führt, als auch in der GNU Multiple Precision Library die Fibonaccifolgen unterstützt wurden. Als ich darauf stieß, war der Rest einfach: Man kann auch einen langen Weg zu Fuß gehen, wenn man weiß, daß dieser zum Ziel führt! Kapitel 4 enthält eigentlich nur sture Rechnerei mit einigen Beispielen. Das Kapitel 5 über Teilbarkeiten ist durch mein generelles Interesse an der Faktorisierung von Zahlen begründet und ausgehend von der Eigenschaft 5.1, die in [DoOl95] ohne Beweis angegeben ist, vollständig selbst entwickelt. Kapitel 6 schließlich dürfte für Studierende interessant sein; es ist durch die Erinnerung an die Lektüre von [WoWa90] inspiriert. Die Thematik wurde aber auch in Passauer Vorlesungen über Diskrete Strukturen behandelt; sie kann auch in [ChJo65] gefunden werden. Man sollte sich generell merken: Viele Rekursionen lassen sich in eine geschlossene Form bringen! Auf einen Sprung hinüber zu den Potenzreihenringen habe ich verzichtet. Der Goldene Schnitt (Kapitel 7) darf bei einer Betrachtung der Fibonaccifolgen nicht fehlen; wenn man weiß, was man zeigen muß, geht es auch straight forward... Das Kapitel 8 ist zufällig entstanden, als mir die »tiefere Bedeutung« der Eigenschaften von λ^n bewußt wurde. Der entwickelte Algorithmus ergibt sich dann als Erleuchtung. 9 schließlich ist durch Formeln aus [DoOl95] inspiriert, die ich z.T. verallgemeinert habe und die einem Beweis meinerseits etwas stärkeren Widerstand entgegensetzten. Kapitel 10 zeigt, wie sich sogar die Fibonaccifolge zum Faktorisieren von natürlichen Zahlen mißbrauchen läßt. – Zahlentheoretische Grundlagen finden sich beispielsweise in [FrIs92], fortgeschrittene Anwendungen in [PLMo87] (wo auch eine kurze definitorische Zusammenfassung steht, an der ich mich orientiert habe).

Da die Beweise nicht direkt im Texteditor, sondern zuvor handschriftlich entwickelt wurden, sind Übertragungs- und Flüchtigkeitsfehler nicht auszuschließen. Errata werden jeweils bei der nächsten Aktualisierung berücksichtigt. Für Anregungen, Hinweise oder Korrekturen können Sie mich per e-mail unter *reinecke@thorstenreinecke.de* erreichen.

1 Einführung

1.1 Motivation und Definition

Viele Phänomene in der Natur lassen sich mathematisch über die Fibonacci-Folge oder abgewandelte Folgen erklären. Diese Folgen bilden sozusagen einen natürlichen Gegenpol zu den *Zweierpotenzen*, die in binärer Schreibweise das heutige Informationszeitalter beherrschen.

In Binärdarstellung repräsentiert das jeweils nächsthöhere Bit bekanntlich den doppelten Wert des Vorgängerwertes, wobei das niedrigste Bit den Wert 1 repräsentiert. Die Wertigkeiten dieser Bits lassen sich somit als Folge notieren: $b_0 := 1$ und $b_{n+1} := 2 \cdot b_n = b_n + b_n$ oder in direkter Form durch $b_n := 2^n$.

Wandelt man diesen Ansatz auf zwei abhängige Folgenglieder ab, so erhält man rekursiv definierte Folgen der Form $f_n := f_{n-1} + f_{n-2}$. Für den Spezialfall $f_0 := 0$ und $f_1 := 1$ bezeichnet f_n die *Fibonacci-Folge* F_n. Diese Folge wollen wir im folgenden näher betrachten.

*e-mail: reinecke@thorstenreinecke.de

Wenn nachfolgend nichts weiter über die Glieder f_0 sowie f_1 ausgesagt wird, so gelten die betrachteten Eigenschaften für alle Folgen dieser Form, deren Startwerte definiert sind. Ein zweiter Spezialfall ergibt sich für die Belegung $f_0 := 2$, $f_1 := 1$; die hierdurch definierte Folge nennen wir *Lucasfolge* L_n.

Doch stellen wir zunächst eine kleine Tabelle mit einigen Fibonacci- und Lucaszahlen auf (Tabelle 1):

Tabelle 1: Werte der Fibonacci- und Lucasfolge

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610
L_n	2	1	3	4	7	11	18	29	47	76	123	199	322	521	843	1364

Wir sehen deutlich, wie sich (mit Ausnahme der ersten beiden Folgenglieder) jedes Folgenglied aus der Summe der beiden vorherigen Glieder errechnet. Dies ist die grundlegende Eigenschaft aller Folgen, die wir hier betrachten wollen.

1.2 Vom Geschlechtsleben der Bienen

Wer seine Kinder aufklärt, sollte nicht mit den Bienen anfangen, es sei denn, er will über Fibonacci-Folgen referieren. Da ich letzteres beabsichtige, komme ich um das Geschlechtsleben der Bienen nicht herum.

In jedem Bienenstamm gibt es (unter anderem) eine Königin und auch ein paar Männchen. Diejenigen Eier der Königin, die in den Genuß kamen, von Männchen befruchtet zu werden, reifen später zu Weibchen heran, wohingegen die unbefruchteten Eier zu Männchen heranreifen. Weibchen haben also biologisch gesehen einen Vater und eine Mutter; Männchen hingegen nur eine Mutter und sind somit vaterlose Geschöpfe!

Betrachten wir nun die Anzahl der Individuen, die genetisch in der jeweiligen Generation Einfluß auf die Erbanlagen des Bienenmännchens Willy und seines menschlichen Namensvetterns genommen haben:

Die Bienendrohne Willy hat nur eine Mutter, diese wiederum hat zwei Eltern; der Großvater Willy´s hat nur eine eine Mutter, Willy´s Großmutter wiederum zwei Eltern, usw. Auch hier begegnet uns die Fibonacci-Folge[1]. Den Menschen liegt das Binärsystem hingegen schon in den Genen verankert.

Tabelle 3: Willy´s Vorfahren

	Willy	Eltern	Großeltern	Urgroßeltern	Urgroßeltern	Ururur...	Urururur...
Bienen	1	1	2	3	5	8	13
Menschen	1	2	4	8	16	32	64

2 Grundlegendes

2.1 Formale Definitionen

Wenn wir im folgenden die allgemeine Fibonaccifolge $(f_n)_{n\in\mathbb{N}}$ betrachten, so schreiben wir einfach exemplarisch und ein wenig unsauber f_n (je nach Kontext kann f_n natürlich auch den Folgenwert selbst bezeichnen!) oder manchmal in Funktionsschreibweise f (für $f : \mathbb{N} \to \mathbb{N}, n \mapsto f_n$). Wir setzen dabei voraus, daß zwei nicht näher spezifizierte Folgenglieder $f_0 \in \mathbb{N}$ und $f_1 \in \mathbb{N} \setminus \{0\}$ sowie die Rekursionsgleichung $f_n := f_{n-1} + f_{n-2}$ diese Folge definieren. Der Fall $f_1 = f_0 = 0$ ergibt trivialerweise die konstante Folge $f_n = 0$, die wir in der folgenden Betrachtung ausklammern.

[1] Sie sollten sich den Stammbaum aufzeichnen und die Rekursionsformel über eine nach Geschlechtern getrennte Betrachtung herleiten.

Für die Spezialfälle $f_0 := 0$, $f_1 := 1$ definieren die Folgenglieder f_n die spezielle bzw. eigentliche Fibonaccifolge, die wir mit $(F_n)_{n\in\mathbb{N}}$ oder kurz F_n, manchmal sogar in Funktionsschreibweise mit F bezeichnen wollen. Analog sei die Lucasfolge L_n für $L_0 := 2$ und $L_1 := 1$ definiert.

2.2 Einige Eigenschaften

In diesem Abschnitt folgen einige einfach zu beweisende Eigenschaften.

2.2.1 Gemeinsame Teiler

Haben zwei aufeinanderfolgende Glieder f_n sowie f_{n+1} einen gemeinsamen Teiler, so gilt dies für alle Folgenglieder und insbesondere für f_0 und f_1. Dies leitet sich unmittelbar aus einem grundlegenden Satz der Zahlentheorie ab, da mit $a \equiv 0 \pmod t$ und $b \equiv 0 \pmod t$ auch $a + b \equiv a - b \equiv 0 \pmod t$ folgt (vgl. euklidischer Algorithmus zur Bestimmung des ggT). Im übrigen sei bemerkt, daß die natürliche Zahl 0 durch alle übrigen natürlichen Zahlen (mit Ausnahme der 0) ohne Rest teilbar ist.

2.2.2 Periodizität in Restklassen

Allgemeine Betrachtung Betrachten wir $f_n \bmod m$: Da die Folgenwerte jeweils nur von der Summe ihrer beiden Vorgängerwerte abhängen und da $f_n \bmod m$ lediglich m verschiedene Werte annehmen kann, müssen sich diese Werte periodisch wiederholen. Eine Periode ist gefunden, wenn wir zwei Wertepaare (f_r, f_{r+1}) und (f_s, f_{s+1}) mit $r \neq s$ gefunden haben, deren Reste modulo m gleich sind.

Da es höchstens m^2 viele paarweise verschiedene Wertepaare geben kann, garantiert uns diese grobe Abschätzung die Existenz einer Periode innerhalb des Intervalls $\left[0, m^2 + 1\right]$, da dieses Intervall $m^2 + 1$ viele Wertepaare enthält.

Beispiel Betrachten wir die F_n sowie L_n modulo 8:

Tabelle 5: Werte der Fibonacci- und Lucasfolge modulo 8

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n	0	1	1	2	3	5	0	5	5	2	7	1	0	1
L_n	2	1	3	4	7	3	2	5	7	4	3	7	2	1

Wir können erkennen, daß sich die Folgenwerte in beiden Fällen periodisch wiederholen müssen, da beide Folgenwerte jeweils nur von der Summe ihrer beiden Vorgängerwerte abhängen. Wenn zwei aufeinander folgende Werte mit zwei bereits vorher auftauchenden aufeinander folgenden Werten identisch sind, so haben wir eine Periode gefunden. Dies ist bei F_n für $(F_{12}, F_{13}) \equiv (F_0, F_1) \pmod 8$ und bei L_n für $(L_{12}, L_{13}) \equiv (L_0, L_1) \pmod 8$ der Fall. Das Angenehme bei Restklassenbetrachtungen ist, daß man prinzipiell nur endlich viele Fälle betrachten muß, um eine Eigenschaft zu beweisen.

Wir halten beispielhaft folgende Eigenschaften fest:

1. $F_{12n+\Delta} \equiv F_\Delta \pmod 8$
2. $L_{12n+\Delta} \equiv L_\Delta \pmod 8$
3. $F_n \equiv 0 \pmod 4 \Rightarrow F_n \equiv 0 \pmod 8$ und $n \equiv 0 \pmod 6$
4. $L_n \neq 0 \pmod 8$

Die letzte Dezimalstelle Als weiteres Beispiel können wir F_n bzw. L_n modulo 10 betrachten. Die Periode beträgt 60. Damit gilt:

1. $F_n \equiv F_{n \bmod 60} (\mathrm{mod} 10)$
2. $L_n \equiv L_{n \bmod 60} \ (\mathrm{mod} 10)$

Durch die Betrachtung der relevanten Restklassen kann man vergleichsweise einfach auch Endziffern astronomisch großer Folgenwerte berechnen. Doch wer interessiert sich schon wirklich für die letzte Dezimalziffer von $F_{L_{1000}}$ (=3) oder $L_{9^{9^9}}$ (=6)?

2.3 Negative Indices

Die allgemeine Fibonaccifolge läßt sich auf die ganzen Zahlen ausdehnen, indem wir überall die Gültigkeit der Gleichung $f_n = f_{n-1} + f_{n-2}$ fordern. Damit gilt dann auch $f_{-n-1} + f_{-n} = f_{-n+1}$ bzw. die äquivalente Form $f_{-(n+1)} = f_{-(n-1)} - f_{-n}$, die durch die induktive Definition $f_{-(n+1)} := f_{-(n-1)} - f_{-n}$ in Verbindung mit den »herkömmlichen« Startwerten f_0 und f_1 der Ursprungsfolge erfüllt wird.

Diese Erweiterung erlaubt es uns jedoch nicht, ungeprüft (und unbewiesen) alle Ergebnisse und Eigenschaften der Fibonaccifolge, die auf den natürlichen Zahlen definiert ist, auf die negativen Indices auszuweiten. Insbesondere treten nun negative Folgenwerte auf!

Tabelle 7: Werte der erweiterten Fibonacci- und Lucasfolge

n	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
F_n	34	-21	13	-8	5	-3	2	-1	1	0	1	1	2	3	5	8	13	21	34
L_n	-76	47	-29	18	-11	7	-4	3	-1	2	1	3	4	7	11	18	29	47	76

Die nachfolgend bewiesenen Eigenschaften sind jedoch so nützlich, daß sie erwähnt werden.

2.3.1 F_{-n}

$$F_{-n} = (-1)^{n+1} \cdot F_n$$

Beweis: Die Richtigkeit der für den Induktionsanker erforderlichen Fälle n=0 sowie n=1 kann anhand der Tabelle geprüft werden. Gelte nun nach Induktionsannahme die oben genannte Beziehung. Zu zeigen bleibt die Richtigkeit für (n+1):

$$F_{-(n+1)} = F_{-(n-1)} - F_{-n} = (-1)^{(n-1)+1} \cdot F_{n-1} - (-1)^{n+1} \cdot F_n = (-1)^n F_{n-1} + (-1)^n F_n$$

$$= (-1)^n (F_{n-1} + F_n) = (-1)^n F_{n+1} = (-1)^{(n+1)+1} F_{n+1}$$

2.3.2 L_{-n}

$$L_{-n} = (-1)^n \cdot L_n$$

Beweis: Die Richtigkeit der für den Induktionsanker erforderlichen Fälle n=0 sowie n=1 kann anhand der Tabelle geprüft werden. Gelte nun nach Induktionsannahme die oben genannte Beziehung. Zu zeigen bleibt die Richtigkeit für (n+1):

$$L_{-(n+1)} = L_{-(n-1)} - L_{-n} = (-1)^{(n-1)} \cdot L_{n-1} - (-1)^n \cdot L_n = (-1)^{n-1} L_{n-1} + (-1)^{n-1} L_n$$

$$= (-1)^{n-1} (L_{n-1} + L_n) = (-1)^{n-1} L_{n+1} = (-1)^{n+1} L_{n+1}$$

3 Summen von Folgenwerten

Wir betrachten nun den Fall $f_{n+k} + f_{n-k}$ für $k := 2^j$ und $n \geq k$.

3.1 k=2

$$f_{n+2} + f_{n-2} = (f_{n+1} + f_n) + f_{n-2} = ((f_n + f_{n-1}) + f_n) + f_{n-2} = 2f_n + (f_{n-1} + f_{n-2}) = 3f_n$$

3.2 k=4

$$f_{n+4} + f_{n-4} = f_{n+4} + f_{n-4} + 2f_n - 2f_n = f_{n+2+2} + f_{n+2-2} + f_{n-2+2} + f_{n-2-2} - 2f_n$$

hier haben wir eine »Nullsumme« ergänzt, um nun den Fall k=2 anzuwenden!

$$= 3f_{n+2} + 3f_{n-2} - 2f_n = 3(f_{n+2} + f_{n-2}) - 2f_n$$

und erneute Anwendung ergibt

$$= 3(3f_n) - 2f_n = 7f_n$$

3.3 $k = 2^j$

Wir definieren nun die Koeffizienten $c_2 := 3$, $c_4 := 7$. Doch wie sehen die Koeffizienten für höhere Zweierpotenzen aus? – Nun, diese lassen sich induktiv bestimmen:

$$f_{n+2^{j+1}} + f_{n-2^{j+1}} = f_{n+2^{j+1}} + f_{n-2^{j+1}} + 2f_n - 2f_n$$

$$= f_{n+2^j+2^j} + f_n + f_n + f_{n-2^j-2^j} - 2f_n$$

$$= (f_{n+2^j+2^j} + f_{n+2^j-2^j}) + (f_{n-2^j+2^j} + f_{n-2^j-2^j}) - 2f_n$$

$$= c_{2^j} \cdot f_{n+2^j} + c_{2^j} \cdot f_{n-2^j} - 2f_n$$

(mit c_{2^j} sei bereits bekannter Koeffizient)

$$= c_{2^j} \cdot (f_{n+2^j} + f_{n-2^j}) - 2f_n$$

$$= c_{2^j} \cdot (c_{2^j} \cdot f_n) - 2f_n$$

$$= (c_{2^j}^2 - 2) \cdot f_n$$

(hier steht der nunmehr ermittelte Koeffizient)

$$= c_{2^{j+1}} f_n$$

Wir halten also fest:

- $f_{n+2^j} + f_{n-2^j} = c_{2^j} \cdot f_n$ für $j \geq 1$
- $c_2 := 3$ sowie $c_{2^j} := c_{2^{j-1}}^2 - 2$ für $j > 1$

3.4 Umstellungen

Stellt man das vorige Ergebnis um, so erhalten wir $f_n = c_{2^j} f_{n-2^j} - f_{n-2\cdot 2^j} = c_{2^j} f_{n-2^j} - f_{n-2^{j+1}}$; hiermit lassen sich rekursiv bereits die Folgenwerte von Zweierpotenzen effizient ermitteln.

Für andere Werte als Zweierpotenzen mag es angebracht sein, den Term erneut aufzulösen, um das Auftreten negativer Indices zu vermeiden. Zur Vereinfachung der Schreibweise wählen wir für ein gegebenes n ein eindeutig bestimmtes k mit der Eigenschaft $\frac{n}{8} < k := 2^j \leq \frac{n}{4}$. Dann gilt:

$$f_n = c_k f_{n-k} - f_{n-2k} = c_k \cdot (c_k f_{n-k-k} - f_{n-k-2k}) - f_{n-2k}$$

$$= c_k \cdot (c_k f_{n-2k} - f_{n-3k}) - f_{n-2k}$$

$$= (c_k^2 - 1) f_{n-2k} - c_k f_{n-3k}$$

3.5 k=1

Bisher haben wir den Wert $k = 1$ bei den obigen Betrachtungen ausgeklammert. Er scheint auch zunächst nicht sonderlich hilfreich zu sein. Bei der Berechnung von f_n können wir ja vorzeitig abbrechen und mit der »normalen« Rekursion $f_n := f_{n-1} + f_{n-2}$ fortfahren, lange bevor der Fall $k = 1$ relevant werden würde.

3.5.1 $k = 1$ im allgemeinen

Trotzdem sei der Fall der Vollständigkeit halber erwähnt:

$$f_{n+1} + f_{n-1} = (f_n + f_{n-1}) + f_{n-1} = f_n + 2f_{n-1}$$

3.5.2 $k = 1$ im besonderen: die Lucasfolge

Eine im Augenblick noch nicht direkt anwendbare, aber interessante Eigenschaft tritt zutage, wenn wir die Fibonaccifolge betrachten: $F_{n+1} + F_{n-1} = L_n$. Sie haben richtig gelesen, dies ergibt die Lucasfolge![2] Und diese Behauptung gilt es zu beweisen. Das geschieht in zwei Schritten:

Zunächst betrachten wir, ob die Startwerte übereinstimmen:

$L_0 = 2$, $F_{0+1} + F_{0-1} = F_1 + F_{-1} = 1 + 1 = 2$

$L_1 = 1$, $F_{1+1} + F_{1-1} = F_2 + F_0 = 1 + 0 = 1$

Die Startwerte stimmen also überein. Der Wert von F_{-1} kann nämlich folgerichtig anhand der Rekursionsgleichung $F_n = F_{n-1} + F_{n-2}$ für $n = 1$ ermittelt werden: $F_1 = F_0 + F_{-1}$, also $F_{-1} = F_1 - F_0 = 1 - 0 = 1$.

Im zweiten Schritt sollte noch gezeigt werden, daß die Folge $F_{n+1} + F_{n-1}$ auch tatsächlich der Rekursionsgleichung $L_n = L_{n-1} + L_{n-2}$ genügt:

$$L_n = L_{n-1} + L_{n-2} = (F_{n-1+1} + F_{n-1-1}) + (F_{n-2+1} + F_{n-2-1})$$

$$= F_n + F_{n-2} + F_{n-1} + F_{n-3} = (F_n + F_{n-1}) + (F_{n-2} + F_{n-3}) = F_{n+1} + F_{n-1}$$

q.e.d.

[2] Der erste Mensch, der diese Eigenschaft »entdeckt« hat, wird natürlich $L_n := F_{n+1} + F_{n-1}$ gesetzt und anschließend die zugehörigen Startwerte ermittelt haben.

3.5.3 wundersame Koeffizienten

Wenn wir die Koeffizienten aus 3.3 betrachten und ihnen die zugehörigen Lucasfolgenwerte gegenüberstellen, so kommen wir auf die Vermutung, daß diese für $j \geq 1$ gleich sind.

$c_{2^1} = c_2 = 3$ sowie $L_{2^1} = L_2 = L_1 + L_0 = 1 + 2 = 3$

$c_{2^2} = c_4 = 7$ sowie $L_{2^2} = L_4 = L_3 + L_2 = L_2 + L_1 + L_2 = 3 + 1 + 3 = 7$

Unter Anwendung von der Gleichung aus 3.4 bestätigt sich diese Vermutung:

Mit $c_{2^{j+1}} := c_{2^j}^2 - 2$ für $j \geq 1$ einerseits, und $L_{2^{j+1}} = c_{2^j} L_{2^{j+1}-2^j} - L_{2^{j+1}-2\cdot 2^j} = c_{2^j} L_{2^j} - L_0 = c_{2^j} L_{2^j} - 2$ anderseits folgt mit der Induktionsannahme $L_{2^j} = c_{2^j}$ auch $L_{2^{j+1}} = c_{2^j} L_{2^j} - 2 = c_{2^j} c_{2^j} - 2 = c_{2^j}^2 - 2 = c_{2^{j+1}}$ für alle folgenden Zweierpotenzen.

Wir halten also fest:

$L_{2^{j+1}} = c_{2^{j+1}} = L_{2^j}^2 - 2$ für $j \geq 1$

3.6 k verallgemeinert

Lösen wir uns jetzt von den Zweierpotenzen, so daß k nun beliebige Werte annehmen kann. Betrachten wir zunächst zwei weitere Beispiele, wobei wir das Vorzeichen variieren.

3.6.1 $k = 1$

$$f_{n+1} - f_{n-1} = (f_n + f_{n-1}) - f_{n-1} = f_n$$

3.6.2 $k = 3$

$$f_{n+3} - f_{n-3} = f_{n+2} + f_{n+1} - f_{n-3} = 2f_{n+1} + f_n - f_{n-3}$$

$$= 3f_n + 2f_{n-1} - f_{n-3} = 3f_n + f_{n-1} + f_{n-2} + f_{n-3} - f_{n-3} = 4f_n$$

3.6.3 eine allgemeine Formel

Wenn man die Koeffizienten mit den Werten der Lucasfolge vergleicht, kommt man nach einigem hin- und her vielleicht auf die Idee: L_k ist für gerade k bei der Summe und für ungerade k bei der Differenz der zugehörige Koeffizient.

Mithin vermutet man: $f_{n+k} + (-1)^k f_{n-k} = L_k \cdot f_n$

Diese Vermutung gilt es nun zu beweisen. Dies geschieht per Induktion über k.[3]

$k = 0$**:** $f_{n+0} + 1 \cdot f_{n-0} = 2f_n = L_0 \cdot f_n$ **(wahr)**

$k = 1$**:** $f_{n+1} + (-1) \cdot f_{n-1} = f_n + f_{n-1} - f_{n-1} = 1 \cdot f_n = L_1 \cdot f_n$ **(wahr)**

$k + 1$**:**

Induktionsannahme: Für $k > 0$ sei sowohl für $k - 1$ als auch für k die Behauptung erfüllt. Zu zeigen bleibt, daß sie dann auch für $k + 1$ erfüllt ist, und somit induktiv aufsteigend für alle $k + i$ durch den beliebig oft wiederholbaren Übergang von k auf $k + 1$ (vollständiges Induktionsprinzip).

$$L_{k+1} \cdot f_n = (L_k + L_{k-1}) \cdot f_n = L_k \cdot f_n + L_{k-1} \cdot f_n$$

$$= (f_{n+k} + (-1)^k \cdot f_{n-k}) + (f_{n+(k-1)} + (-1)^{k-1} \cdot f_{n-(k-1)})$$

(nach Induktionsannahme)

$$= f_{n+k} + f_{n+(k-1)} + (-1)^k f_{n-k} + (-1)^{k-1} f_{n-(k-1)}$$

[3] Es sei ausdrücklich erwähnt, daß die Induktion auf k basiert und damit auch für negative Werte von n gültig ist!

$$= f_{n+(k+1)} + (-1)^k f_{n-k} + (-1)^{k-1}(f_{n-k} + f_{n-(k+1)})$$

$$= f_{n+(k+1)} + (-1)^k f_{n-k} + (-1)^{k-1} f_{n-k} + (-1)^{k-1} f_{n-(k+1)}$$

$$= f_{n+(k+1)} + (-1)^{k-1} f_{n-(k+1)}$$

$$= f_{n+(k+1)} + (-1)^{k+1} f_{n-(k+1)}$$

q.e.d.

3.6.4 negative Indices erneut betrachtet

Für $n = 0$ erhalten wir mit obigem Satz

$$f_k + (-1)^k \cdot f_{-k} = L_k \cdot f_0$$

$$\Longleftrightarrow f_{-k} = (L_k \cdot f_0 - f_k) \cdot (-1)^k$$

3.6.5 Spezialisierung für L_{n+k}

Die Anwendung des obigen Satzes auf $f := L$ ergibt $L_{n+k} + (-1)^k \cdot L_{n-k} = L_n \cdot L_k$, somit ergibt sich $L_{n+k} = L_n L_k - (-1)^k L_{n-k}$.

3.6.6 Spezialisierung für L_{2n}

Setzen wir nun noch $k := n$, so erhalten wir $L_{n+n} = L_n \cdot L_n - (-1)^k L_{n-n} = L_n^2 - (-1)^n L_0$, also $L_{2n} = L_n^2 - (-1)^n \cdot 2$. Dies ist eine Verallgemeinerung des in 3.5.3 ermittelten Resultats.

3.6.7 L_{3n}

Wir wenden zunächst 3.6.5 für L_{2n+n} und später 3.6.6 an:

$$L_{3n} = L_{2n+n} = L_{2n} L_n - (-1)^n \cdot L_{2n-n} = L_{2n} L_n - (-1)^n L_n$$

$$= (L_{2n} - (-1)^n) L_n = (L_n^2 - (-1)^n \cdot 3) \cdot L_n$$

3.6.8 F_{n+k}

Die nachfolgende Herleitung ist typisch für die Mathematik. Natürlich hätten wir die Formel auch vom Himmel fallen lassen und anschließend beweisen können. Aber durch einen gezielt gewählten Umweg stößt man häufig auf die gewünschte Abkürzung. So findet das Schiff den Weg in die Flasche:

Wir betrachten $f := F$ sowie die Fälle f_{n+k} und f_{k+n} und erhalten hieraus $F_{n+k} = L_k F_n - (-1)^k F_{n-k}$ sowie $F_{k+n} = L_n F_k - (-1)^n F_{k-n}$.

Summation ergibt:

$$2 \cdot F_{n+k} = F_{n+k} + F_{k+n} = L_k F_n + L_n F_k - (-1)^k F_{n-k} - (-1)^n F_{k-n}$$

Unter Berücksichtigung der Eigenschaft $F_{k-n} = F_{-(n-k)} = (-1)^{(n-k)+1} F_{n-k}$ erhalten wir

$$(-1)^k F_{n-k} + (-1)^n F_{k-n} = (-1)^k F_{n-k} + (-1)^n (-1)^{n-k+1} F_{n-k} = F_{n-k} \cdot ((-1)^k + (-1)^{2n-k+1})$$

$$= F_{n-k} \cdot ((-1)^k + (-1)^{1-k}) = F_{n-k} \cdot 0 = 0$$

Also

$$F_{n+k} = \frac{F_n L_k + F_k L_n}{2}$$

Spezialfall $n = k$ Diesen Fall betrachten wir später noch einmal, trotzdem springt er uns hier schon ins Auge:

$$F_{2n} = F_{n+n} = \frac{F_n L_n + F_n L_n}{2} = F_n L_n$$

3.6.9 F_{n-k}

Mit 3.6.3 erhalten wir $F_{n-k} = (-1)^k \cdot (L_k F_n - F_{n+k})$. Also

$$F_{n-k} = (-1)^k \cdot (L_k F_n - \frac{F_n L_k + F_k L_n}{2}) = \frac{2L_k F_n - F_n L_k - F_k L_n}{2 \cdot (-1)^k} = \frac{F_n L_k - F_k L_n}{2 \cdot (-1)^k}$$

(Alternativ hätten wir auch $F_{n-k} = F_{n+(-k)} = \frac{F_n L_{-k} + F_{-k} L_n}{2}$ mit anschließender Anwendung von 2.3.1 sowie 2.3.2 ausrechnen können.)

3.7 Resümee

Manchmal fallen Formeln vom Himmel und sind dann zu beweisen. Dann steht man zunächst ohne jede Idee da und staunt (oder ärgert sich). Wenn man sich jedoch die Zeit nimmt, die fallenden Regentropfen zu betrachten, die schließlich als Schneeflocken auf die Erde fallen und den Boden mit einem weißen Mantel überdecken, dann bekommt man eine Ahnung davon, daß auch diese wunderbare Schönheit »nur« eine andere Form des Wassers ist...

4 Folgenwerte von Summen

4.1 f_{k+j}

$$f_{k+j} = f_{k+j-1} + f_{k+j-2} = 2f_{k+j-2} + f_{k+j-3} = 3f_{k+j-3} + 2f_{k+j-4}$$

Wenn wir uns die Koeffizienten näher betrachten, sehen wir, daß es Fibonacci-Zahlen sind; also notieren wir sie auch als solche...

$$= F_4 \cdot f_{k+j-3} + F_3 \cdot f_{k+j-4} = (F_4 + F_3) \cdot f_{k+j-4} + F_4 \cdot f_{k+j-5}$$
$$= F_5 \cdot f_{k+j-4} + F_4 \cdot f_{k+j-5} = ... =$$
$$= F_{i+1} \cdot f_{k+j-i} + F_i \cdot f_{k+j-(i+1)}$$

4.1.1 Spezialisierung 1

Nun spezialisieren wir für $i = j$:

$$f_{k+j} = F_{j+1} \cdot f_{k+j-j} + F_j \cdot f_{k+j-j-1} = F_{j+1} f_k + F_j f_{k-1}$$

Wir halten dieses Ergebnis für den allgemeinen Fall dieser zweistufigen Rekursionsfolgen fest!

4.1.2 Spezialisierung 2

Eine nicht minder interessante Spezialisierung erhalten wir für $i = k + j - 1$:

$$f_{k+j} = F_{(k+j-1)+1} \cdot f_{k+j-(k+j-1)} + F_{k+j-1} \cdot f_{k+j-((k+j-1)+1)} = F_{k+j} f_1 + F_{k+j-1} f_0$$

Wenn wir nun noch $n := k + j$ substituieren, erhalten wir $f_n = F_n f_1 + F_{n-1} f_0$, und das ist fürwahr ein gelungenes Ergebnis!

4.2 f_{2n}

$f_{2n} = f_{n+n} = F_{n+1} \cdot f_n + F_n \cdot f_{n-1}$ (mit 4.1.1)
Alternativ erhalten wir unter Anwendung von 3.6.3 $f_{n+n} = L_n \cdot f_n - (-1)^n f_{n-n}$, also $f_{2n} = L_n \cdot f_n - (-1)^n \cdot f_0$.

4.3 F_{2n}

Nun spezialisieren wir die obigen Fälle auf die Fibonacci-Folge, setzen also $f := F$.
$F_{2n} = F_{n+1} F_n + F_n \cdot F_{n-1}$
$= F_n \cdot (F_{n+1} + F_{n-1}) = F_n \cdot L_n$ (mit 3.5.2)
Dies halten wir als Ergebnis fest, rechnen aber trotzdem weiter:
$= (F_{n+1} - F_{n-1})(F_{n+1} + F_{n-1})$
$= F_{n+1}^2 - F_{n-1}^2$
Somit erhalten wir den Satz:

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2 = F_n \cdot L_n$$

4.4 L_{2n}

Mit 4.2 sowie 3.6.6 erhalten wir:

$$L_{2n} = F_{n+1} L_n + F_n L_{n-1} = L_n^2 - (-1)^n \cdot 2$$

4.5 F_{2n-1}

Rechnen wir mit obigem Ergebnis weiter:

$$L_{2n} = F_{n+1} L_n + F_n L_{n-1} = (F_n + F_{n-1}) L_n + F_n L_{n-1}$$

$$= F_n L_n + F_{n-1} L_n + F_n L_{n-1}$$

und unter Anwendung von 4.3

$$= F_{2n} + F_{n-1} L_n + F_n L_{n-1}$$

somit:

$$L_{2n} - F_{2n} = F_{n-1} L_n + F_n L_{n-1}$$

Außerdem ergibt sich wegen $L_n = F_{n+1} + F_{n-1}$ interessantes:

$$L_{2n} - F_{2n} = (F_{2n+1} + F_{2n-1}) - F_{2n}$$

$$= F_{2n} + F_{2n-1} + F_{2n-1} - F_{2n} = 2F_{2n-1}$$

also (und dies gilt es festzuhalten!):

$$F_{2n-1} = \frac{L_{2n} - F_{2n}}{2} = \frac{F_{n-1} L_n + F_n L_{n-1}}{2}$$

(Dasselbe Ergebnis hätten wir auch unter Verwendung von 3.6.8 für F_{-1+2n} sowie $F_{(n-1)+n}$ erhalten.)

4.6 L_{2n-1}

$$L_{2n-1} = F_{(2n-1)+1} + F_{(2n-1)-1} = F_{2n} + F_{2(n-1)} = F_n L_n + F_{n-1} L_{n-1}$$

4.7 F_{3n}

Unter Anwendung von 3.6.3 erhalten wir

$$F_{2n+n} + (-1)^n \cdot F_{2n-n} = L_n \cdot F_{2n}$$
$$\iff F_{3n} + (-1)^n F_n = L_n(L_n F_n) = L_n^2 F_n$$
$$\iff F_{3n} = F_n L_n^2 - F_n(-1)^n = F_n \cdot (L_n^2 - (-1)^n)$$

5 Teilbarkeiten

5.1 $F_{k \cdot n}$ und Primzahlen

Das folgende Resultat ist zwar nicht ganz befriedigend, weil keine allgemeingültige Formel zur Berechnung von $F_{k \cdot n}$ hergeleitet wird; trotzdem verblüfft es durch seine Einfachheit.

Zunächst halten wir fest, daß $F_{1 \cdot n} = F_n \equiv 0 \pmod{F_n}$ immer erfüllt ist. Nun zeigen wir per Induktion über k, daß $F_{kn} \equiv 0 \pmod{F_n}$ gilt[4]:

$F_{(k+1)n} = F_{kn+n} = F_{n+1}F_{kn} + F_n F_{kn-1}$ (nach 4.1.1)

Da $F_{n+1}F_{kn} \equiv 0 \pmod{F_n}$ wegen F_{kn} als Faktor (der nach Induktionsannahme durch F_n teilbar ist) und $F_n F_{kn-1} \equiv 0 \pmod{F_n}$ wegen F_n als Faktor gilt, folgt damit auch $F_{(k+1)n} \equiv 0 \pmod{F_n}$, womit der Induktionsbeweis bereits abgeschlossen ist.

Wenn wir berücksichtigen, daß $F_2 = 1$ keine Primzahl ist, können wir das Resultat sogar noch (scheinbar) allgemeiner fassen.

Folgerung:

Sei $n > 4$ eine zusammengesetzte Zahl, dann ist auch F_n zusammengesetzt.

Umkehrschluß:

Wenn F_n eine Primzahl ist, dann ist auch n eine Primzahl oder $n \leq 4$.

5.2 $L_{(2k+1)n}$

Für die Lucasfolge ergibt sich bei Betrachtung der ungeraden Faktoren im Index ein ähnliches Resultat. Die Induktion über k verhält sich ansonsten analog zum vorherigen Beweis:

$k = 0 : L_{(2k+1)n} = L_n \equiv 0 \pmod{L_n}$

Sei nun nach Induktionsannahme $L_{(2k+1)n} \equiv 0 \pmod{L_n}$. Mit 4.1.1 erhalten wir für $k+1$:

$$L_{(2(k+1)+1)n} = L_{(2k+3)n} = L_{(2k+1)n+2n}$$

$$= F_{2n+1}L_{(2k+1)n} + F_{2n}L_{(2k+1)n-1}$$

$$= F_{2n+1}L_{(2k+1)n} + F_n L_n L_{(2k+1)n-1}$$

Der erste Summand ist nach Induktionsannahme, der zweite wegen L_n als enthaltenem Faktor durch L_n ohne Rest teilbar. Die Teilbarkeit geht damit auf die Summe über.

5.3 Natürliche Zahlen als Teiler

Alle positiven natürlichen Zahlen kommen in der speziellen Fibonaccifolge unendlich oft als Teiler vor. Sei t eine beliebige positive natürliche Zahl, dann existiert eine Periode P_t mit der Maximallänge t^2, für die gilt: $F_{k \cdot P_t} \equiv 0 \pmod{t}$

[4] Das ist übrigens eine sehr interessante Eigenschaft, wenn man F_N für zusammengesetzte N faktorisieren möchte!

Beweis: Die Existenz einer Periode P_t wird durch 2.2.2 gesichert. Zu zeigen bleibt, daß diese auch den Nullwert enthält.

Nehmen wir an, es gäbe eine Konstante $c > 0$, so daß die Periodizität erst ab diesem c erfüllt wäre und insbesondere gilt: $F_{c-1} \neq F_{c-1+P_t} \pmod t$. (Wenn diese Konstante c nicht existiert, dann gilt $F_{k \cdot P_t} \equiv F_{0 \cdot P_t} \equiv F_0 \equiv 0 \pmod t$ und unsere Behauptung wäre bewiesen.)

Nach Definition der Fibonaccifolge gilt $F_{c-1} + F_c = F_{c+1}$ und $F_{c-1+P_t} + F_{c+P_t} = F_{c+1+P_t}$, somit wegen der Periodizität auch $F_{c+1} - F_c \equiv F_{c+1+P_t} - F_{c+P_t} \pmod t$. Das ist aber äquivalent zu $F_{c-1} \equiv F_{c-1+P_t} \pmod t$, was unserer Annahme widerspricht. □

5.4 Fünf Kostbarkeiten

5.4.1 Primfaktoren an Primstellen

Jeder an einer Primstelle p auftauchende Primfaktor von F_p taucht dort das erste Mal auf.

Beweis: Dies folgt beinahe unmittelbar aus 5.4.2: $\prod_{i=1}^{p-1} \gcd(i,p) = 1 \implies \prod_{i=1}^{p-1} \gcd(F_i, F_p) = 1$.

5.4.2 Teilerfremde Indices

Sind zwei Indices teilerfremd, so auch deren Fibonaccizahlen: $\gcd(r,s) = 1 \Longrightarrow \gcd(F_r, F_s) = 1$.

Beweis: Sei $\gcd(r,s) = 1$ mit $r, s > 1$. Wegen Teilerfremdheit von r und s existieren m_1, m_2, so daß $r \cdot m_1 + 1 = s \cdot m_2 =: h$ erfüllt wird (vgl. Chinesischer Restsatz, z.B. [FrIs92]; setze beispielsweise $m_2 := s^{-1} \bmod r$ und $m_1 := \frac{s \cdot m_2 - 1}{r}$).

Mit 5.1 folgt daraus $F_{h-1} = F_{r \cdot m_1} \equiv 0 \pmod{F_r}$ sowie $F_h = F_{s \cdot m_2} \equiv 0 \pmod{F_s}$. Für $t := \gcd(F_r, F_s)$ gilt somit $F_{h-1} \equiv F_h \equiv 0 \pmod t$. Mit 2.2.1 folgt die Teilbarkeit aller Fibonacciwerte durch t, insbesondere auch für $F_1 = 1$. Aus $0 \equiv 1 \pmod t$ folgt $t = 1$, womit der Beweis abgeschlossen wäre.

5.4.3 Fibonaccizahlen mit gemeinsamen Teiler

Haben zwei Fibonaccizahlen einen nichttrivialen gemeinsamen Teiler, so haben auch ihre Indices einen nichttrivialen gemeinsamen Teiler.

Beweis: Dies folgt im Umkehrschluß aus dem vorigen Satz: $a \Rightarrow b \models \neg b \Rightarrow \neg a$.

5.4.4 Indices mit gemeinsamen Teiler

Haben zwei Indices einen gemeinsamen Teiler größer als zwei, so haben die zugehörigen Fibonaccizahlen einen gemeinsamen Teiler größer als eins: $\gcd(r,s) > 2 \implies \gcd(F_r, F_s) > 1$.

Beweis: Für $t := \gcd(r,s) > 2$ gilt $F_t > F_2 = 1$. Mit 5.1 folgt $F_r \equiv 0 \pmod{F_t}$ und $F_s \equiv 0 \pmod{F_t}$, mithin $\gcd(F_r, F_s) \geq F_t > 1$. □

5.4.5 Teilerfremde Fibonaccizahlen

Sind zwei Fibonaccizahlen teilerfremd, so beträgt der größte gemeinsame Teiler der zugehörigen Indices höchstens zwei.

Beweis: Dies folgt im Umkehrschluß aus dem vorigen Satz: $a \Rightarrow b \models \neg b \Rightarrow \neg a$.

6 Geschlossene Form

Wie in 1.1 bereits erwähnt, bilden Fibonacci-Folgen gewissermaßen einen Gegenpol zu den Zweierpotenzen.

Die Zweierpotenzen lassen sich durch $b_0 := 1$; $b_n := b_{n-1} + b_{n-1} = 2b_{n-1}$ definieren und bilden als geschlossene Form den Term $b_n = 2^n$. Ist es auf ähnliche Weise möglich, die Fibonacci-Folge in eine geschlossene Form zu pressen? – Nun ja, manche Erkenntnis fällt vom Himmel, und manchmal muß man dazu etwas nachhelfen. Schießen wir also etwas Silberjodid in die Wolken und warten ab, was herunterkommt...

Der Ansatz lautet, $f_n = x^n$ zu setzen, und wir erhalten damit aus der Rekursionsgleichung $f_n = f_{n-1} + f_{n-2}$ die Gleichung $x^n = x^{n-1} + x^{n-2}$, die (für $x \neq 0$) zu $x^2 = x + 1$ äquivalent ist. Diese wiederum entspricht $x^2 - x - 1 = 0$, dem sogenannten »charakteristischen Polynom« der zugehörigen Rekursion. Wir ermitteln nun dessen Nullstellen, in dem wir eine quadratische Ergänzung auf beiden Seiten addieren:

(Die quadratische Ergänzung wird bestimmt durch den Ansatz $(x+y)^2 = x^2 + 2xy + y^2$, wobei hier $2xy = -x$ gewünscht wird. Also $y = -\frac{1}{2}$.)

$$x^2 - x - 1 + (-\frac{1}{2})^2 = (-\frac{1}{2})^2$$

$\Leftrightarrow$

$$(x - \frac{1}{2})^2 - 1 = \frac{1}{4}$$

// $\sqrt{()}$

$\Leftrightarrow$

$$x - \frac{1}{2} = \pm\sqrt{\frac{5}{4}}$$

$\Leftrightarrow$

$$x = \frac{1}{2} \pm \frac{\sqrt{5}}{2}$$

$\Leftrightarrow$

$$x = \frac{1 \pm \sqrt{5}}{2}$$

Wie man es bei quadratischen Gleichungen nicht anders erwarten kann, erhalten wir zwei Lösungen. Nun ja, wir haben ja auch zwei Startwerte f_0 und f_1, die wir bisher noch nicht ins Spiel gebracht haben. Versuchen wir eine Linearkombination der beiden Lösungen, um eine von den Startwerten abhängige geschlossene Form zu erhalten[5]:

$$f_n = a \cdot (\frac{1+\sqrt{5}}{2})^n + b \cdot (\frac{1-\sqrt{5}}{2})^n$$

Für f_0, also $n = 0$ erhalten wir daraus $f_0 = a \cdot (\frac{1+\sqrt{5}}{2})^0 + b \cdot (\frac{1-\sqrt{5}}{2})^0 = a + b$. Für f_1 ergibt sich $f_1 = a \cdot (\frac{1+\sqrt{5}}{2}) + b \cdot (\frac{1-\sqrt{5}}{2})$. Das ist ein lineares Gleichungssystem mit zwei Gleichungen und zwei Unbekannten und sollte sich daher lösen lassen:

[5] Wir lassen hierfür auch reelle Zahlen als Folgenwerte zu und treffen zusätzlich folgende Feststellungen:
Für alle Fibonaccifolgen f und g sowie jedem reellen Skalar α gilt:

$$(f \oplus g)_n := f_n + g_n = f_{n-1} + f_{n-2} + g_{n-1} + g_{n-2} = (f \oplus g)_{n-1} + (f \oplus g)_{n-2}$$

$$(\alpha \bullet f)_n := \alpha \cdot f_n = \alpha \cdot (f_{n-1} + f_{n-2}) = \alpha \cdot f_{n-1} + \alpha \cdot f_{n-2} = (\alpha \bullet f)_{n-1} + (\alpha \bullet f)_{n-2}$$

Jede Linearkombination zweier gegebener Fibonaccifolgen ist somit ebenfalls eine Fibonaccifolge. Die beiden Funktionsterme $(\frac{1+\sqrt{5}}{2})^n$ sowie $(\frac{1-\sqrt{5}}{2})^n$ sind geschlossene Ausdrücke für zwei verschiedene Fibonaccifolgen. Die nachfolgend aufgestellte Linearkombination ist also die geschlossene Form einer Fibonaccifolge.

Etwas abstrakter betrachtet bilden die Fibonaccifolgen somit einen zweidimensionalen Unterraum des (unendlichdimensionalen) Vektorraums aller Folgen. Die beiden ausgewählten Funktionsterme bilden zusammen ein Erzeugendensystem dieses zweidimensionalen Vektorraums.

Mit $b = f_0 - a$ (aus der ersten Gleichung) ergibt sich eingesetzt in die zweite

$$f_1 = a\frac{1+\sqrt{5}}{2} + (f_0 - a)\frac{1-\sqrt{5}}{2}$$

$$\Leftrightarrow$$

$$f_1 = a\frac{1+\sqrt{5}}{2} + f_0\frac{1-\sqrt{5}}{2} - a\frac{1-\sqrt{5}}{2}$$

$$\Leftrightarrow$$

$$f_1 = a\frac{(1+\sqrt{5}) - (1-\sqrt{5})}{2} + f_0\frac{1-\sqrt{5}}{2}$$

$$\Leftrightarrow$$

$$f_1 = a\sqrt{5} + f_0\frac{1-\sqrt{5}}{2}$$

$$\Leftrightarrow$$

$$a\sqrt{5} = f_1 - f_0\frac{1-\sqrt{5}}{2}$$

$$\Leftrightarrow$$

$$a = \frac{f_1 - f_0\frac{1-\sqrt{5}}{2}}{\sqrt{5}}$$

.

Für die Fibonacci-Folge F_n mit $F_0 = 0$ und $F_1 = 1$ ergibt dies $a = \frac{1}{\sqrt{5}}$ und $b = 0 - a = -\frac{1}{\sqrt{5}}$, also $F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n = \frac{(1+\sqrt{5})^n}{\sqrt{5}\cdot 2^n} - \frac{(1-\sqrt{5})^n}{\sqrt{5}\cdot 2^n} = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{\sqrt{5}\cdot 2^n}$.

Unter Berücksichtigung der Tatsache, daß $(1+\sqrt{5}) - (1-\sqrt{5}) = 2\cdot\sqrt{5}$ ist, ergibt sich $F_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{(1+\sqrt{5}) - (1-\sqrt{5})} \cdot (\frac{1}{2})^{n-1} = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}$ die sogenannte »binetsche Darstellung« der Fibonacci-Folge, die, wenn wir $\lambda := \frac{1+\sqrt{5}}{2}$ und $\mu := \frac{1-\sqrt{5}}{2}$ setzen, in der Form $F_n = \frac{\lambda^n - \mu^n}{\lambda - \mu}$ besonders einprägsam ist.

Unter Anwendung von 4.1.2 erhalten wir beinahe unmittelbar auch deren allgemeine geschlossene Darstellung geschenkt:

$$f_n = F_n f_1 + F_{n-1} f_0 = f_1\frac{\lambda^n - \mu^n}{\lambda - \mu} + f_0\frac{\lambda^{n-1} - \mu^{n-1}}{\lambda - \mu} = \frac{f_1\lambda^n - f_1\mu^n + f_0\lambda^{n-1} - f_0\mu^{n-1}}{\lambda - \mu}$$

$$= \frac{(f_1\lambda^n + f_0\lambda^{n-1}) - (f_1\mu^n + f_0\mu^{n-1})}{\lambda - \mu} = \frac{(f_1 + \frac{f_0}{\lambda})\lambda^n - (f_1 + \frac{f_0}{\mu})\mu^n}{\lambda - \mu}$$

7 Goldener Schnitt

Der goldene Schnitt wird allgemein als äußerst harmonisches Verhältnis zweier Seitenlängen zueinander angesehen. Zwei Zahlen stehen im goldenen Schnitt zueinander, wenn sich die Summe beider Zahlen zur größeren Zahl wie die größere Zahl zur kleineren Zahl verhält. Das Verhältnis zweier aufeinanderfolgender Fibonaccizahlen nähert sich dem goldenen Schnitt an.

7.1 Berechnung

Berechnen wir zunächst das Verhältnis zweier aufeinanderfolgender Glieder der allgemeinen Fibonaccifolge anhand der geschlossenen Form:

$$\frac{f_{n+1}}{f_n} = \frac{\frac{c_1\lambda^{n+1} - c_2\mu^{n+1}}{\lambda - \mu}}{\frac{c_1\lambda^n - c_2\mu^n}{\lambda - \mu}} = \frac{c_1\lambda^{n+1} - c_2\mu^{n+1}}{c_1\lambda^n - c_2\mu^n} = \frac{\frac{c_1\lambda^{n+1} - c_2\mu^{n+1}}{\lambda^n}}{\frac{c_1\lambda^n - c_2\mu^n}{\lambda^n}} = \frac{c_1\lambda(\frac{\lambda}{\lambda})^n - c_2\mu(\frac{\mu}{\lambda})^n}{c_1(\frac{\lambda}{\lambda})^n - c_2(\frac{\mu}{\lambda})^n} = \frac{c_1\lambda - c_2\mu(\frac{\mu}{\lambda})^n}{c_1 - c_2(\frac{\mu}{\lambda})^n}$$

mit $c_1 := (f_1 + \frac{f_0}{\lambda})$ und $c_2 := (f_1 + \frac{f_0}{\mu})$

Dieser Quotient strebt gegen einen Grenzwert, da $\left|\frac{\mu}{\lambda}\right| = \left|\frac{1-\sqrt{5}}{1+\sqrt{5}}\right| = \frac{\sqrt{5}-1}{\sqrt{5}+1} < 1$ und daher $\lim_{n\to\infty}(\frac{\mu}{\lambda})^n = 0$ gilt:

$$\lim_{n\to\infty}\frac{f_{n+1}}{f_n} = \lim_{n\to\infty}\frac{c_1\lambda - c_2\mu(\frac{\mu}{\lambda})^n}{c_1 - c_2(\frac{\mu}{\lambda})^n} = \frac{c_1\lambda - c_2\mu\lim_{n\to\infty}(\frac{\mu}{\lambda})^n}{c_1 - c_2\lim_{n\to\infty}(\frac{\mu}{\lambda})^n} = \frac{c_1\lambda - 0}{c_1 - 0} = \lambda = \frac{1+\sqrt{5}}{2}$$

7.2 Eigenschaften

λ hat einige interessante Eigenschaften, es gilt z.B.:

(i) $\lambda^2 = (\frac{1+\sqrt{5}}{2})^2 = \frac{1^2+2\cdot\sqrt{5}+5}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = \lambda + 1$

(ii) Mit Eigenschaft (i) im Zähler gilt $\frac{\lambda+1}{\lambda} = \frac{\lambda^2}{\lambda} = \frac{\lambda}{1} = \lambda$; damit erfüllt λ genau die oben geschilderte Definition des goldenen Schnitts. Andererseits ist $\frac{\lambda+1}{\lambda} = 1 + \frac{1}{\lambda}$. Folglich gilt $1 + \frac{1}{\lambda} = \lambda$ und das ist äquivalent zu $\frac{1}{\lambda} = \lambda - 1$.

Diese Eigenschaften folgen auch schon daraus, daß λ und μ die Nullstellen des charakteristischen Polynoms $x^2 - x - 1$ sind.

(iii) Ferner gilt $\lambda \cdot \mu = \frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = \frac{1^2-5}{4} = \frac{-4}{4} = -1$, also $\lambda = -\mu^{-1}$ sowie $\mu = -\lambda^{-1}$.

7.3 Eine andere Sicht

Lassen wir die Fibonaccifolgen für einen Augenblick ruhen und schreiben die Definition des Goldenen Schnitts nieder, wobei a und b (mit $a > b$) unsere zwei Zahlen seien, die im Verhältnis des Goldenen Schnitts stehen: $\frac{a+b}{a} = \frac{a}{b}$. Wir können diese Gleichung normieren, indem wir verlangen, daß die kleinere Zahl 1 ist: $\frac{\frac{a}{b}+1}{\frac{a}{b}} = \frac{\frac{a}{b}}{1}$. Setzen wir nun $x := \frac{a}{b}$, dann erhalten wir daraus die Gleichung $\frac{x+1}{x} = x$, die (für $x \neq 0$) zu $x + 1 = x^2$ bzw. $x^2 - x - 1 = 0$ äquivalent ist. Diese Gleichung haben wir aber bereits in Abschnitt 6 gelöst. Die einzigen Belegungen für x, die diese Gleichung erfüllen, sind $x = \frac{1+\sqrt{5}}{2}$ und $x = \frac{1-\sqrt{5}}{2}$.

Für $x = \frac{1+\sqrt{5}}{2} > 0$ können wir folgern: a und b haben das gleiche Vorzeichen; für $x = \frac{1-\sqrt{5}}{2} < 0$ gilt analog: a und b müssen verschiedene Vorzeichen besitzen. Da keine weiteren Lösungen existieren, steht zu jeder positiven Zahl a stets genau die positive Zahl $b := \frac{2a}{1+\sqrt{5}}$ im Verhältnis des Goldenen Schnitts $\frac{a}{b} = \frac{a}{\frac{2a}{1+\sqrt{5}}} = a \cdot \frac{1+\sqrt{5}}{2a} = \frac{1+\sqrt{5}}{2}$.

Dieses Verhältnis ist eine irrationale Zahl ($\frac{a}{b} =: x \in \mathbb{R} \setminus \mathbb{Q}$), woraus folgt: Rationale Zahlen stehen niemals zueinander im Verhältnis des Goldenen Schnitts. Diese Eigenschaft gilt dann erst recht für beliebige Teilmengen der rationalen Zahlen, also insbesondere für die natürlichen Zahlen.

8 Noch eine Berechnungsmethode für Fibonaccizahlen

Auf die folgende Berechnungsmethode bin ich gestoßen, als ich die Eigenschaften von λ näher untersucht habe. Dabei dürfte ich wohl ein mir bisher unbekanntes Verfahren »wiederentdeckt« haben.[6] Vielleicht ist die Herleitung aber interessant:

Betrachten wir das charakteristische Polynom $x^2 - x - 1$. Nullsetzen ergibt $x^2 = x + 1$. Die Nullstellen sind λ und μ. Für diese gilt $x^2 = x + 1$.

Für x^3 erhalten wir daraus $x^3 = x^2 \cdot x = (x+1) \cdot x = x^2 + x = (x+1) + x = 2x + 1 = F_3 \cdot x + F_2$; analog ergibt sich induktiv

$$x^n = x^{n-1} \cdot x = (F_{n-1} \cdot x + F_{n-2}) \cdot x = F_{n-1} \cdot x^2 + F_{n-2} \cdot x = F_{n-1} \cdot (x+1) + F_{n-2} \cdot x$$

[6] Und tatsächlich wird ein derartiges Verfahren auch vom Matheprogramm MAPLE verwendet, um Fibonaccifolgenwerte zu bestimmen.

$$= F_{n-1} \cdot x + F_{n-1} + F_{n-2} \cdot x = (F_{n-1} + F_{n-2}) \cdot x + F_{n-1} = F_n \cdot x + F_{n-1}$$

Mit diesem Wissen können wir die geschlossene Form auch einfach ausrechnen:

$$\frac{\lambda^n - \mu^n}{\lambda - \mu} = \frac{(F_n \cdot \lambda + F_{n-1}) - (F_n \cdot \mu + F_{n-1})}{\lambda - \mu} = \frac{F_n \cdot (\lambda - \mu)}{\lambda - \mu} = F_n$$

ebenso:

$$\lambda^n + \mu^n = (F_n\lambda + F_{n-1}) + (F_n\mu + F_{n-1}) = F_n \cdot (\lambda + \mu) + 2F_{n-1} = F_n \cdot (\frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2}) + 2F_{n-1}$$

$$= F_n + 2F_{n-1} = F_n + F_{n-1} + F_{n-1} = F_{n+1} + F_{n-1} = L_n$$

Eine neue Struktur Kennen Sie komplexe Zahlen? Ähnlich, wie man diese konstruiert, können wir auch hier vorgehen: Definiere $a := (a_1, a_2) := a_1 \cdot \lambda + a_2$; analog sei $b := (b_1, b_2) := b_1 \cdot \lambda + b_2$.

Die Definition eines solchen Zahlenpaares ist in dem Sinne eindeutig, dass es eine reelle Zahl darstellt, welche nicht durch ein anderes Paar aus rationalen (und daher erst recht nicht natürlichen) Zahlen gebildet werden kann. Denn sei z.B. $a = b$, also $a_1 \cdot \lambda + a_2 = b_1 \cdot \lambda + b_2$, dann folgt $(a_1 - b_1) \cdot \lambda = b_2 - a_2$, womit die rechte Seite der Gleichung entweder null oder ebenfalls irrational sein muß.

Mit obiger Definition gelten folgende Rechenregeln:

$$a + b = (a_1, a_2) + (b_1, b_2) = (a_1\lambda + a_2) + (b_1\lambda + b_2) = (a_1 + b_1)\lambda + (a_2 + b_2) = (a_1 + b_1, a_2 + b_2)$$

$$a \cdot b = (a_1, a_2) \cdot (b_1, b_2) = (a_1\lambda + a_2)(b_1\lambda + b_2) = a_1\lambda b_1\lambda + a_1\lambda b_2 + a_2 b_1\lambda + a_2 b_2$$

$$= a_1 b_1 \lambda^2 + (a_1 b_2 + a_2 b_1)\lambda + a_2 b_2 = a_1 b_1(\lambda + 1) + (a_1 b_2 + a_2 b_1)\lambda + a_2 b_2$$

$$= a_1 b_1 \lambda + a_1 b_1 + (a_1 b_2 + a_2 b_1)\lambda + a_2 b_2 = (a_1 b_1 + a_1 b_2 + a_2 b_1)\lambda + a_1 b_1 + a_2 b_2$$

$$= (a_1 b_1 + a_1 b_2 + a_2 b_1, a_1 b_1 + a_2 b_2)$$

In dieser Struktur kann man also »addieren« und »multiplizieren«. Wir stellen fest, daß $\lambda^0 = 1 = (0, 1)$, $\lambda^1 = \lambda = (1, 0)$, $\lambda^2 = \lambda + 1 = (1, 1)$ und allgemein gilt: $\lambda^n = F_n \cdot \lambda + F_{n-1} = (F_n, F_{n-1})$. Dies liefert uns ein Verfahren, um (F_n, F_{n-1}) durch schnelle Exponentiation (durch fortgesetztes Quadrieren mit anschließendem Zusammenmultiplizieren der zu den Zweierpotenzen gehörigen Quadrate) zu bestimmen. Die Lösung für allgemeine Fibonaccifolgen ergibt sich dann mittels 4.1.2.

Algorithmus Der Algorithmus 1 auf der nächsten Seite erwartet ein Fibonaccizahlenpaar $x := (f_1, f_0)$ mit den Startwerten der Fibonaccifolge sowie den Index n und liefert dann das Paar (f_n, f_{n-1}) als Ergebnis zurück.

Bemerkungen:

1. Der Ausdruck *(n and i)* steht für den komponentenweisen and-Operator: Genau diejenigen Bits, die sowohl in n als auch in i gesetzt sind, sind auch im Ergebnis gesetzt. Der Ausdruck ist genau dann als wahr zu interpretieren, wenn mindestens ein Bit im Ergebnis gesetzt ist.

2. Für $r \cdot q$ kommt man mit drei skalaren Multiplikationen aus, wenn man $h1 := (r1 + r2)(q1 + q2) = r1 \cdot q1 + r1 \cdot q2 + r2 \cdot q1 + r2 \cdot q2$; $h2 := r1 \cdot q1$; $h3 := r2 \cdot q2$ setzt. Es ergibt sich $(r1 \cdot q1 + r1 \cdot q2 + r2 \cdot q1, r1 \cdot q1 + r2 \cdot q2) = (h1 - h3, h2 + h3)$.

Algorithm 1 Fibonaccizahlen durch schnelle Exponentiation

```
function fibonacci(FIBPAIR x, NAT n) : FIBPAIR
begin
 FIBPAIR r,q;
 NAT i;
 r:=(0,1); q:=(1,0);
 i:=1;
 while i≤n do
  if (n and i) then
   r:=r*q; // (r1,r2):=(r1*q1+r1*q2+r2*q1,r1*q1+r2*q2)
  fi;
  q:=q*q; // (q1,q2):=(q1*q1+2*q1*q2,q1*q1+q2*q2)
  i:=i*2;
 od;
 return (r1*x1+r2*x2,r2*x1+(r1-r2)*x2);
end;
```

3. Die Anzahl der erforderlichen Multiplikationen für $q \cdot q$ kann man auf zwei reduzieren, in dem man die Lucasfolge verwendet: $h1 := q1 + 2 \cdot q2 = F_i + 2F_{i-1} = L_i$; $h2 := h1 \cdot h1 - (-1)^i \cdot 2 = L_i^2 - (-1)^i \cdot 2 = L_{2i}$; $h3 := q1 \cdot h1$. Es ergibt sich $(q1 \cdot q1 + 2 \cdot q1 \cdot q2, q1 \cdot q1 + q2 \cdot q2) = (F_{2i}, F_{2i-1}) = (F_i \cdot L_i, \frac{L_{2i}-F_{2i}}{2}) = (h3, \frac{h2-h3}{2})$.

4. Wird die Funktion häufig und mit vielen verschiedenen Werten aufgerufen[7], so kann man die Quadrate vorab berechnen und in einem Array speichern.

Ausblick: Es geht noch schneller, wenn man die binäre Exponentiation ein wenig umgestaltet und vom höchstwertigen Bit abwärts verlaufen läßt; abhängig vom jeweiligen Bit ist dann entweder (F_{2i}, F_{2i-1}) oder (F_{2i+1}, F_{2i}) zu bestimmen. Dabei kommt man mit reinen Quadrierungsschritten aus und kann die Multiplikationen einsparen. Für jeden Schritt sind dann nur noch zwei skalare Quadrierungen sowie einige billige Operationen (Addition, Subtraktion, Shiften) erforderlich. Erläuterungen hierzu und eine Implementierung finden sich beispielsweise in [GNU MP]. – Solche »Exponentiationsalgorithmen« kann man auch allgemein betrachten und weiteren Optimierungen unterziehen (wobei sich wiederum ein Bezug zu den Fibonaccizahlen ergibt); siehe [PLMo92] für eine solche Untersuchung.

9 Weitere Formeln

9.1 $F_{2n} = \sum_{i=0}^{n} \binom{n}{i} F_i$

Wir verwenden die Eigenschaft aus Abschnitt 8, dann erhalten wir einerseits

$$\lambda^{2n} = F_{2n}\lambda + F_{2n-1}$$

und andererseits unter Verwendung des Binomischen Satzes[8]

$$\lambda^{2n} = (\lambda^2)^n = (\lambda+1)^n = \sum_{i=0}^{n} \binom{n}{i} \lambda^i = \sum_{i=0}^{n} \binom{n}{i} (F_i\lambda + F_{i-1}) = \left(\sum_{i=0}^{n} \binom{n}{i} F_i\right) \cdot \lambda + \left(\sum_{i=0}^{n} \binom{n}{i} F_{i-1}\right)$$

Da aber für λ^{2n} keine andere Zerlegung als $F_{2n}\lambda + F_{2n-1}$ existieren kann, muß folglich gelten:

[7] Wenn in Restklassen gerechnet wird, dürfen sich diese nicht ändern.

[8] $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i \cdot b^{n-i}$ mit Binomialkoeffizient $\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}$, bekannt aus dem Pascalschen Dreieck

$$F_{2n} = \sum_{i=0}^{n} \binom{n}{i} F_i$$

und außerdem auch

$$F_{2n-1} = \sum_{i=0}^{n} \binom{n}{i} F_{i-1}$$

Dies ist übrigens auch leicht einzusehen, wenn man alternativ $\mu^{2n} = F_{2n}\mu + F_{2n-1}$ sowie $(\mu^2)^n = (\mu+1)^n = \left(\sum_{i=0}^{n} \binom{n}{i} F_i\right) \cdot \mu + \left(\sum_{i=0}^{n} \binom{n}{i} F_{i-1}\right)$ ausrechnet und die Terme in die Binetsche Formel einsetzt.

Abschließend für die Betrachtung des Terms λ^{2n} sei der Vollständigkeit halber noch auf eine dritte Umformungsvariante hingewiesen:

$$\lambda^{2n} = (\lambda^n)^2 = (F_n\lambda + F_{n-1})^2 = F_n^2 \underbrace{\lambda^2}_{\lambda+1} + 2F_n\lambda F_{n-1} + F_{2-1}^2 = (F_n^2 + 2F_nF_{n-1})\lambda + F_n^2 + F_{n-1}^2$$

Daraus ergibt sich $F_{2n} = F_n^2 + 2F_nF_{n-1}$ sowie $F_{2n-1} = F_n^2 + F_{n-1}^2$. Addiert man zur ersteren Gleichung auf beiden Seiten F_{n-1}^2, so erhält man $F_{2n} + F_{n-1}^2 = F_n^2 + 2F_nF_{n-1} + F_{n-1}^2 = (F_n + F_{n-1})^2 = F_{n+1}^2$, und dies ist äquivalent zu $F_{2n} = F_{n+1}^2 - F_{n-1}^2 = \underbrace{(F_{n+1} + F_{n-1})}_{L_n} \cdot \underbrace{(F_{n+1} - F_{n-1})}_{F_n}$, doch diese Formel kennen wir mit anderer Herleitung bereits aus Abschnitt 4.3.

9.2 $F_{k\cdot n} = \sum_{i=0}^{n} \binom{n}{i} F_i \cdot F_k^i \cdot F_{k-1}^{n-i}$

Auch auf die Gefahr hin, nun vollkommen zu langweilen, wenden wir das obige Prinzip aus 9.1 erneut an, diesmal um eine Formel für $F_{k\cdot n}$ zu bestimmen:

$$\lambda^{k\cdot n} = (\lambda^k)^n = (F_k \cdot \lambda + F_{k-1})^n = \sum_{i=0}^{n} \binom{n}{i} F_k^i \cdot \lambda^i \cdot F_{k-1}^{n-i} = \sum_{i=0}^{n} \binom{n}{i} F_k^i \cdot (F_i \cdot \lambda + F_{i-1}) \cdot F_{k-1}^{n-i}$$

$$= \sum_{i=0}^{n} \binom{n}{i} F_k^i \cdot F_i \cdot F_{k-1}^{n-i} \cdot \lambda + F_k^i \cdot F_{i-1} \cdot F_{k-1}^{n-i} = \left(\sum_{i=0}^{n} \binom{n}{i} F_i \cdot F_k^i \cdot F_{k-1}^{n-i}\right) \cdot \lambda + \left(\sum_{i=0}^{n} \binom{n}{i} F_{i-1} \cdot F_k^i \cdot F_{k-1}^{n-i}\right)$$

Daraus folgt dann analog zu oben:

$$F_{k\cdot n} = \sum_{i=0}^{n} \binom{n}{i} F_i \cdot F_k^i \cdot F_{k-1}^{n-i}$$

sowie

$$F_{k\cdot n-1} = \sum_{i=0}^{n} \binom{n}{i} F_{i-1} \cdot F_k^i \cdot F_{k-1}^{n-i}$$

Die beiden Formeln sind übrigens auch für $k = 1$ korrekt, wenn wir $0^0 := 1$ verlangen, da in beiden Formeln der Teilfaktor $F_{k-1}^{n-i} = F_0^{n-i} = 0^{n-i}$ dann alle Summanden bis auf den Term $\binom{n}{n} F_n \cdot F_1^n \cdot F_0^{n-n} = F_n$ (bzw. für $F_{k\cdot n-1}$ bis auf den Term $\binom{n}{n} F_{n-1} \cdot F_1^n \cdot F_0^{n-n} = F_{n-1}$) auf null setzt. ($n$ sollte aber in allen Fällen eine positive natürliche Zahl sein.)

Als möglicherweise noch recht interessantes Beispiel der Anwendung obiger Formel können wir F_{3n} betrachten. Es ergibt sich zum einen

$$F_{3n} = \sum_{i=0}^{n} \binom{n}{i} F_i \cdot F_3^i \cdot F_2^{n-i} = \sum_{i=0}^{n} \binom{n}{i} F_i \cdot 2^i$$

und da wir wegen der Kommutativität der Multiplikation auch noch k und n vertauschen dürfen, auch:

$$F_{3n} = F_{n\cdot 3} = \sum_{i=0}^{3} \binom{3}{i} F_i \cdot F_n^i \cdot F_{n-1}^{3-i} = 0 + 3F_1 \cdot F_n^1 \cdot F_{n-1}^2 + 3 \cdot F_2 \cdot F_n^2 \cdot F_{n-1}^1 + 1 \cdot F_3 \cdot F_n^3 \cdot F_{n-1}^0$$

$$= 3F_n F_{n-1}^2 + 3F_n^2 F_{n-1} + 2F_n^3 = F_n \cdot (3F_{n-1}^2 + 3F_n F_{n-1} + 2F_n^2)$$

9.3 $F_{n-\Delta} \cdot F_{n+\Delta}$

$$F_n^2 - (-1)^{n+\Delta} \cdot F_\Delta^2 = F_{n-\Delta} \cdot F_{n+\Delta} = \frac{F_n^2 L_\Delta^2 - F_\Delta^2 L_n^2}{4 \cdot (-1)^\Delta}$$

Beweis: Wir verwenden die geschlossene Form. Somit ergibt sich einerseits

$$F_n^2 - (-1)^{n+\Delta} \cdot F_\Delta^2 = (\frac{\lambda^n - \mu^n}{\lambda - \mu})^2 - (-1)^{n+\Delta} \cdot (\frac{\lambda^\Delta - \mu^\Delta}{\lambda - \mu})^2$$

$$= \frac{(\lambda^{2n} - 2(\lambda\mu)^n + \mu^{2n}) - (-1)^{n+\Delta} \cdot (\lambda^{2\Delta} - 2(\lambda\mu)^\Delta + \mu^{2\Delta})}{(\lambda - \mu)^2} = *$$

(Hinweis: $\lambda \cdot \mu = \frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = \frac{1^2-5}{2^2} = \frac{-4}{4} = -1$)

$$* = \frac{(\lambda^{2n} - 2 \cdot (-1)^n + \mu^{2n}) - (-1)^{n+\Delta}(\lambda^{2\Delta} - 2 \cdot (-1)^\Delta + \mu^{2\Delta})}{(\lambda - \mu)^2}$$

$$= \frac{\lambda^{2n} + \mu^{2n} - 2 \cdot (-1)^n + 2 \cdot (-1)^{n+\Delta+\Delta} - (-1)^{n+\Delta}(\lambda\mu)^\Delta((\frac{\lambda}{\mu})^\Delta + (\frac{\mu}{\lambda})^\Delta)}{(\lambda - \mu)^2}$$

$$= \frac{\lambda^{2n} + \mu^{2n} + 2 \cdot 0 - (-1)^{n+2\Delta}((\frac{\lambda}{\mu})^\Delta + (\frac{\mu}{\lambda})^\Delta)}{(\lambda - \mu)^2} = \frac{\lambda^{2n} + \mu^{2n} - (-1)^n((\frac{\lambda}{\mu})^\Delta + (\frac{\mu}{\lambda})^\Delta)}{(\lambda - \mu)^2} =: h$$

und andererseits

$$F_{n-\Delta} \cdot F_{n+\Delta} = \frac{\lambda^{n-\Delta} - \mu^{n-\Delta}}{\lambda - \mu} \cdot \frac{\lambda^{n+\Delta} - \mu^{n+\Delta}}{\lambda - \mu} = \frac{\lambda^{2n} - \lambda^{n-\Delta}\mu^{n+\Delta} - \lambda^{n+\Delta}\mu^{n-\Delta} + \mu^{2n}}{(\lambda - \mu)^2}$$

$$= \frac{\lambda^{2n} + \mu^{2n} - (\lambda\mu)^n((\frac{\mu}{\lambda})^\Delta + (\frac{\lambda}{\mu})^\Delta)}{(\lambda - \mu)^2} = \frac{\lambda^{2n} + \mu^{2n} - (-1)^n((\frac{\lambda}{\mu})^\Delta + (\frac{\mu}{\lambda})^\Delta)}{(\lambda - \mu)^2} = h$$

Da beide Terme gleich sind, ist der erste Teil der Formel korrekt. Für den letzten Teil ergibt sich mit 3.6.8 und 3.6.9:

$$F_{n+\Delta} \cdot F_{n-\Delta} = \frac{F_n L_\Delta + F_\Delta L_n}{2} \cdot \frac{F_n L_\Delta - F_\Delta L_n}{2 \cdot (-1)^\Delta} = \frac{F_n^2 L_\Delta^2 - F_\Delta^2 L_n^2}{4 \cdot (-1)^\Delta}$$

□

9.4 $F_{n-\Delta} \cdot F_{n-1+\Delta}$

Bevor wir die eigentliche Formel vorstellen und mit dem Induktionsbeweis beginnen, folgt zunächst ein kleiner Hilfssatz.

9.4.1 Lemma

$$F_{n-1-\Delta}F_{n+\Delta} + F_{n-\Delta}F_{n-1+\Delta} = 2F_nF_{n-1} + (-1)^{n+\Delta}F_\Delta^2$$

Beweis

(i) aus $(\lambda^n)^2 = (F_n^2 + 2F_nF_{n-1})\lambda + F_n^2 + F_{n-1}^2$ folgt $F_{2n} = F_n^2 + 2F_nF_{n-1}$

(ii) aus $\lambda^{2n} = \lambda^{n-\Delta} \cdot \lambda^{n+\Delta}$ folgt $F_{2n} = F_{n-\Delta}F_{n+\Delta} + F_{n-\Delta}F_{n-1+\Delta} + F_{n-1-\Delta}F_{n+\Delta}$

Aus (i) und (ii) in Verbindung mit Formel 9.3 folgt

$$F_n^2 + 2F_nF_{n-1} = F_n^2 - (-1)^{n+\Delta}F_\Delta^2 + F_{n-\Delta}F_{n-1+\Delta} + F_{n-1-\Delta}F_{n+\Delta}$$

und daraus folgt die obige Gleichung.

9.4.2 Formel und zugehöriger Induktionsbeweis

Nach dieser Vorarbeit kommen wir nun zu unserer Formel

$$F_nF_{n-1} = F_{n-\Delta}F_{n-1+\Delta} + (-1)^{n+\Delta}F_\Delta F_{\Delta-1}$$

die wir per Induktion über Δ beweisen wollen.

Der Induktionsanker $\Delta = 0$ ergibt $F_nF_{n-1} = F_nF_{n-1} + (-1)^n \cdot 0$ und ist daher erfüllt. Sei nun die Behauptung für Δ wahr. Zu zeigen bleibt die Korrektheit der Behauptung für $\Delta + 1$:

$$\begin{aligned}
&F_{n-(\Delta+1)}F_{n-1+(\Delta+1)} + (-1)^{n+(\Delta+1)}F_{\Delta+1}F_{(\Delta+1)-1} \\
&\quad = F_{n-1-\Delta}F_{n+\Delta} + (-1)^{n+\Delta+1}\underbrace{F_{\Delta+1}}_{F_\Delta+F_{\Delta-1}}F_\Delta \\
&= F_{n-1-\Delta}F_{n+\Delta} - \underbrace{(-1)^{n+\Delta}F_{\Delta-1}F_\Delta}_{F_nF_{n-1}-F_{n-\Delta}F_{n-1+\Delta} \text{ nach Induktionsannahme}} - (-1)^{n+\Delta}F_\Delta^2 \\
&= \underbrace{F_{n-1-\Delta}F_{n+\Delta} + F_{n-\Delta}F_{n-1+\Delta}}_{\text{Lemma!}} - F_nF_{n-1} - (-1)^{n+\Delta}F_\Delta^2 \\
&= 2F_nF_{n-1} + (-1)^{n+\Delta}F_\Delta^2 - F_nF_{n-1} - (-1)^{n+\Delta}F_\Delta^2 \\
&= F_nF_{n-1}
\end{aligned}$$

q.e.d.

9.5 Nochmalige Betrachtung von Periodizität und Teilbarkeit

Erinnern wir uns einerseits noch einmal an die Binetsche Formel $F_n = \frac{\lambda^n - \mu^n}{\lambda - \mu}$ aus Abschnitt 6. Dabei wurde $\lambda := \frac{1+\sqrt{5}}{2}$ und $\mu := \frac{1-\sqrt{5}}{2}$ gesetzt. Erinnern wir uns andererseits daran, daß es für Periodizitätsbetrachtungen häufig sinnvoll ist, in Restklassen zu rechnen. – Nun können wir die berechtigte Frage stellen: Ist es möglich, die geschlossene Form innerhalb einer Restklassenbetrachtung zu verwenden?

Diese Frage führt uns unmittelbar zu dem Problem, ob der Ausdruck $\sqrt{5}$ in den Restklassen, die wir betrachten wollen, auf sinnvolle Weise definiert werden kann.

Für die nachfolgende Betrachtung benötigen wir Wissen aus der Zahlentheorie, das z.B. bei [FrIs92] nachgeschlagen werden kann. Zum einen benötigen wir den sogenannten kleinen Fermatschen Satz, der für Primzahlen p und teilerfremde Basen a die Folgerung $a^{p-1} \equiv 1 \pmod p$ aufstellt. Zum anderen benötigen wir einige zentrale Eigenschaften über quadratische Reste.

9.5.1 Die Fälle $(\frac{5}{p}) = 1$

Betrachten wir Primzahlen $p > 5$ und die Primkörper $\mathbb{F}_p$, d.h. die Körper, die bei den Restklassenbetrachtungen modulo Primzahlen p entstehen. Die unter Abschnitt 6 hergeleitete geschlossene Form bleibt in solchen Primkörpern gültig, wenn 5 ein quadratischer Rest modulo p ist, mit Hilfe des Legendresymbols ausgedrückt also $(\frac{5}{p}) = 1$ gilt; nur dann ist Kongruenz $x^2 \equiv 5 \pmod p$ in $\mathbb{F}_p$ erfüllbar und wir können für unsere Betrachtung z.B. $\sqrt{5}$ als die »größere« und $-\sqrt{5}$ als die »kleinere« Lösung dieser Kongruenz definieren.

Für Primzahlen p mit $(\frac{5}{p}) = 1$ gilt somit aufgrund des kleinen Fermatschen Satzes

$$F_{p-1} = \frac{\lambda^{p-1} - \mu^{p-1}}{\lambda - \mu} \equiv \frac{1-1}{\sqrt{5}} \equiv 0 \pmod p$$

sowie

$$F_p = \frac{\lambda^p - \mu^p}{\lambda - \mu} \equiv \frac{\lambda - \mu}{\lambda - \mu} \equiv \frac{\sqrt{5}}{\sqrt{5}} \equiv 1 \pmod p$$

Damit gilt $(F_{p-1}, F_p) \equiv (0, 1) \equiv (F_0, F_1)$, mithin gilt die Periodizität $F_{k\cdot(p-1)+\Delta} \equiv F_\Delta \pmod p$ für Primzahlen der obengenannten Form.

Insbesondere sind für diese Primzahlen die Fibonacciwerte F_{p-1} sowie die Terme $F_{p-2} - 1$, $F_p - 1$ und $F_{p+1} - 1$ durch p teilbar.

Wegen des quadratischen Reziprozitätsgesetzes gilt für ungerade p

$$(\frac{p}{5}) = (\frac{5}{p}) \cdot (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} = (\frac{5}{p}) \cdot 1 = (\frac{5}{p})$$

Anstatt alle Fälle für $(\frac{5}{p}) = 1$ zu untersuchen, können wir uns also auf die Fälle $(\frac{p}{5}) = 1$ beschränken. Eine Restklassenbetrachtung auf $\mathbb{F}_5$ (vgl. Tabelle 9) zeigt uns, daß nur Zahlen der Form $5n$, $5n + 1$ und $5n + 4$ (bzw. $5n - 1$) quadratische Reste modulo 5 sind. Da Primzahlen größer als 5 weder durch 5 noch durch 2 teilbar sind, können wir folgern: Primzahlen mit der Eigenschaft $(\frac{5}{p}) = 1$ und $p > 5$ haben die Form $p = 10 \cdot n \pm 1$. (Diese Form enthält diejenigen quadratischen Reste modulo 10, die zu 10 teilerfremd sind.)

Tabelle 9: Quadratische Reste modulo 5 bzw. 10

x	0	1	2	3	4
$x^2 \bmod 5$	0	1	4	4	1

x	0	1	2	3	4	5	6	7	8	9
$x^2 \bmod 10$	0	1	4	9	6	5	6	9	4	1

Zusammenfassung dieser Ergebnisse Für Primzahlen der Form $p = 10 \cdot n \pm 1$ sind die Terme $F_{p-2} - 1$, F_{p-1}, $F_p - 1$ und $F_{p+1} - 1$ durch p ohne Rest teilbar.

Beispiel: $F_{909} - 1 \equiv F_{910} \equiv F_{911} - 1 \equiv F_{912} - 1 \equiv 0 \pmod{911}$

9.5.2 Die Fälle $(\frac{5}{p}) = -1$

Die nicht-quadratischen Reste modulo 10, die zu 10 teilerfremd sind, haben die Form $10 \cdot n \pm 3$. Für Primzahlen dieser Form gilt: Die Periode P_p (für $F_{k\cdot P_p+\Delta} \equiv F_\Delta \pmod p$) ist ein Vielfaches von $p + 1$ und es gilt $F_{p+1} \equiv 0 \pmod p$.

Beweis: Ich habe leider keinen Beweis gefunden, der ohne fortgeschrittene Konzepte aus der Zahlentheorie auskommt. Für die erforderlichen zahlentheoretischen Grundlagen sei daher auf [HaRi94], Appendix 4 (The Arithmetic of Quadratic Fields) verwiesen, ohne die der nachfolgende Beweis unverständlich sein dürfte.

Wir betrachten den Körper $\mathbb{Q}(\sqrt{5})$ und setzen $a := 2 \cdot \lambda = 1 + \sqrt{5}$, dann gilt $\bar{a} = 1 - \sqrt{5} = 2 \cdot \mu$. Wegen $a^2 - 2a - 4 = (1^2 + 2 \cdot \sqrt{5} + 5) - (2 + 2 \cdot \sqrt{5}) - 4 = 6 - 2 - 4 = 0$ sind sowohl a als auch $\bar{a}$ Elemente dieses Körpers.

Mit der Erweiterung des kleinen Fermatschen Satzes auf solche Körper gilt $a^p \equiv \bar{a} \pmod{p}$ für $(\frac{5}{p}) = -1$. Somit folgt

$$F_{p+1} = \frac{\lambda^{p+1} - \mu^{p+1}}{\lambda - \mu} = \frac{(a^{p+1} - \bar{a}^{p+1}) \cdot 2^{-p-1}}{(a - \bar{a}) \cdot 2^{-1}} = \frac{a \cdot a^p - \bar{a} \cdot \bar{a}^p}{a - \bar{a}} \cdot 2^{-p}$$

$$\equiv \frac{a\bar{a} - \bar{a}a}{a - \bar{a}} \cdot 2^{-1} = \frac{a\bar{a} - a\bar{a}}{(a - \bar{a}) \cdot 2} = \frac{0}{(a - \bar{a}) \cdot 2} = 0 \pmod{p}$$

□

10 Ein »einfacher« Faktorisierungsalgorithmus

Ich möchte hier nur kurz skizzieren, wie sich lineare Rekursionen prinzipiell anwenden lassen, um natürliche Zahlen zu faktorisieren.[9]

Wenn eine zusammengesetzte Zahl $N = p \cdot Q$ (mit p Primzahl und Q möglicherweise noch weiter zerlegbar) gegeben ist und $K := p - 1$ (für $(\frac{5}{p}) = 1$) bzw. $K := p + 1$ (für $(\frac{5}{p}) = -1$) in viele kleine Teiler zerfällt[10], so haben wir eine Chance, den Primfaktor p über die Fibonaccifolge zu ermitteln: Wir konstruieren eine hochgradig in kleine Primzahlen[11] zerlegbare »riesengroße« Zahl h und hoffen darauf, daß diese durch K teilbar ist. Wenn wir Erfolg haben, ist dies der Fall. Dann aber gilt $F_h \equiv F_K \equiv 0 \pmod{p}$ und damit auch $\gcd(F_h, p) = p$ und wegen $\gcd(p, N) = p$ ist $\gcd(F_h, N) \geq p$. Mit einiger Wahrscheinlichkeit haben wir dann auch $\gcd(F_h, N) = p$ gefunden. Der Leser möge sich davon überzeugen, daß es ausreicht, $F_h \bmod N$ zu berechnen; dies vermeidet eine explosionsartige Vergrößerung der Folgenwerte.

Der Algorithmus 2 bewerkstelligt das oben ausgeführte. Die »riesengroße« Zahl h wird dabei als Produkt kleinerer Zahlen h_i sukzessive aufgebaut; dies ermöglicht es, $F_{\prod h_i} \bmod N$ bereits in den Schleifendurchläufen zu ermitteln und die Schleife abzubrechen, wenn ein Faktor gefunden wird. Sobald ein Teiler von N gefunden ist, liefert ***fibfactor*** diesen als Ergebnis zurück; der gefundene Faktor ist nicht notwendigerweise eine Primzahl, in seltenen Fällen kann er sogar N selbst sein (z.B. für $N := F_q$ mit q prim und F_q zusammengesetzt (vgl. 5.4.1)). Auch ist nicht jeder gefundene Primfaktor notwendigerweise ± 1 in kleine Teiler zerlegbar.[12]

10.0.3 Beispiel

Wählen wir $p := 12347 = 2^2 \cdot 3^2 \cdot 7^3 - 1$ und $Q := 100000127 = 2^7 \cdot 3 \cdot 260417 - 1$; beides sind Primzahlen. Wir setzen $N := p \cdot Q = 1234701568069$. Nun »vergessen« wir die gewählten Faktoren und setzen den Algorithmus auf diese Zahl an. Wir wählen $h := 2^3 \cdot 3^3 \cdot 5^3 \cdot 7^3 = 9261000$. Nun berechnen wir $F_h \bmod N = 194310245762$. Wir berechnen den größten gemeinsamen Teiler dieser Zahl mit N; es ergibt sich $\gcd(194310245762, N) = 12347$. Nun prüfen wir (z.B. durch Probedivision), daß es sich bei

[9] Der explizite Ansatz, Fibonaccifolgen zu verwenden, ist eine Eigenkonstruktion und in gewisser Weise eine Spezialisierung des in der Literatur bereits hinlänglich bekannten (p+1)-Algorithmus.

Hier geht es weniger um ausgefeilte Effizienz als um die Grundidee! Der interessierte Leser möge für Optimierungsansätze z.B. [PLMo87] zu Rate ziehen.

[10] oder (ganz allgemein) $F_K \equiv 0 \pmod{p}$ erfüllt ist (denn wegen $F_{2n} = F_n L_n$ können sich auch Teiler der L_n dazugesellen, die nicht die obige Struktur aufweisen)

[11] Da kleine Primzahlen die gesuchte Zahl K möglicherweise mehrfach teilen, mag es nicht nur erlaubt, sondern sogar erwünscht sein, wenn sie auch in h mehrfach auftreten.

[12] Denn der Primfaktor kann auch Teiler einer in F_K enthaltenen Lucaszahl sein! Beispiel: $p := 197473779574608014956 7$; es ist $p + 1 = 2^6 \cdot 3^3 \cdot 7 \cdot 47 \cdot 515894844583 \cdot 6733$, aber es gilt trotzdem $\gcd(F_{2^6 \cdot 3^2 \cdot 7}, p) = p$, weil $\gcd(L_{2^5 \cdot 3^2 \cdot 7}, p) = p$ ist...

$p = 12347$ um eine Primzahl handelt und stellen ferner fest: $p + 1 = 2^2 \cdot 3^2 \cdot 7^3$. Wir dividieren den gefundenen Teiler ab und erhalten $Q = \frac{N}{p} = 100000127$.

Algorithm 2 Faktorisierung mit Fibonaccizahlen

```
function fibpow(FIBPAIR firstsquare, NAT n, NAT m) : FIBPAIR
begin
 FIBPAIR r,q;
 NAT i;
 r:=(0,1); q:=firstsquare;
 i:=1;
 while i≤n do
  if (n and i) then
   r:=r*q mod m; // (r1,r2):=(r1*q1+r1*q2+r2*q1 mod m,r1*q1+r2*q2 mod m)
  fi;
  q:=q*q mod m; // (q1,q2):=(q1*q1+2*q1*q2 mod m,q1*q1+q2*q2 mod m)
  i:=i*2;
 od;
 return r;
end;

function fibfactor(NAT N) : NAT
begin
 FIBPAIR fib:=(1,0);
 NAT hi;
 repeat
  hi:=»choose a multiplier«;
  fib:=fibpow(fib,hi,N);
 until gcd(fib1,N)≠1; // fib1 is first component of fib
 return gcd(fib1,N);
end;
```

10.0.4 Bemerkungen:

Der angegebene Algorithmus 2 kann als Template aufgefaßt werden, um strukturverwandte Faktorisierungsalgorithmen zu implementieren.

- Wenn man statt FIBPAIR den Datentyp NAT wählt und statt dem Startpaar fib=(1,0)=(F_1, F_0) eine Basis a wählt, so ergibt dies den klassischen $p-1$-Algorithmus. (Es ist dann allerdings $\gcd(a-1, N)$ anstelle von $\gcd(fib1, N)$ zu bilden.)

- Wenn man sich eine andere geeignete Multiplikation für FIBPAIR definiert, so erhält man andere Varianten des $(p \pm 1)$-Algorithmus: Wählen Sie einfach eine andere lineare Rekursion der Form $f_n := c_1 \cdot f_{n-1} + c_2 \cdot f_{n-2}$. Wenn wir das charakteristische Polynom $p_{ch}(x) := x^2 - c_1 \cdot x - c_2$ betrachten und die Nullstellen berechnen, so erhalten wir $x = \frac{c_1 \pm \sqrt{c_1^2+4c_2}}{2}$. Eine »Multiplikation« läßt sich dann durch $x^2 = c_1 x + c_2$ konstruieren (vgl. Abschnitt 8). Für $r := c_1^2 + 4c_2$ können wir dann die Fälle $(\frac{r}{p}) = 1$ bzw. $(\frac{r}{p}) = -1$ untersuchen. Dies wäre eine eher »experimentelle« Herleitung des $(p+1)$-Algorithmus...

- Prinzipiell könnte man auch Folgen der Form $f_n := \sum_{i=1}^{k} c_i \cdot f_{n-i}$ verwenden. Auch diese sind periodisch bezüglich Restklassenrechnung.[13]

[13] Die Ermittlung der Multiplikationsformel und die Untersuchung der Struktureigenschaften des charakteristischen Polynoms sollten Sie dann allerdings einem Computeralgebrasystem überlassen.

- Wenn Sie statt FIBPAIR eine Datenstruktur für elliptische Kurven verwenden, so erhalten Sie ein Grundgerüst für den Faktorisierungsalgorithmus mit elliptischen Kurven, welches nur noch unwesentlicher Modifikation bedarf.[14]

10.0.5 Zusätzliche Hinweise und Ausblicke

In einer effizienten Implementierung wäre der oben angegebene Algorithmus nur die erste Phase eines komplexeren Algorithmus.

Man würde die Phase 1 nach einiger Zeit abbrechen, um nach einem einzelnen verbliebenen Restfaktor in der Zerlegung von K zu suchen. Der simple Ansatz führt auf die sogenannte »standard continuation«, dieser läßt sich zur »improved standard continuation« verbessern. Letzterer wiederum läßt sich mittels »Pairing« von zwei Zahlen in seiner Geschwindigkeit verdoppeln. Bei Fibonaccizahlen kann man hierzu Formel 9.3 benutzen. Eine weitere Effizienzsteigerung läßt sich erreichen, in dem man die einzelnen Faktoren (oder Faktorpaare) zusammenmultipliziert, bevor man den größten gemeinsamen Teiler berechnet. Dann lassen sich diese aber bei geeigneter Strukturierung als Nullstellen eines Polynoms (sehr hohen Grades) betrachten. Solche Polynome wiederum können unter Zuhilfenahme der diskreten Variante der schnellen Fouriertransformation ausgewertet werden (fft-continuation).

Alle diese Stufen habe ich für die (p-1)-Methode, für elliptische Kurven und nun auch für die Fibonacci-Methode implementiert. Sie sind Bestandteil eines Faktorisierungsprogramms, das ich auf meiner Homepage zum Download bereitgestellt habe.

Literatur

[DoOl95] Dominic Olivastro: Das Chinesische Dreieck, München, 1995

[ChJo65] Charles Jordan: Calculus Of Finite Differences, (Budapest 1939), New York, 1965

[WoWa90] Wolfgang Walter: Analysis I, Springer Verlag, Berlin; Heidelberg, 1985, 1990

[FrIs92] Friedrich Ischebeck: Einladung zur Zahlentheorie, BI-Wiss.Verl., Mannheim; Leipzig; Wien; Zürich, 1992

[MiEn02] Microsoft Encarta 2002

[PLMo87] Peter L. Montgomery: Speeding the Pollard and Elliptic Curve Methods of Factorization, Mathematics Of Computation, 1987, Vol. 48, Number 177, p. 243-264

[HaRi94] Hans Riesel: Prime numbers and computer methods for factorization, 2nd Edition, Birkhäuser; Boston, 1994

[GNU MP] The GNU Multiple Precision Arithmetic Library, Edition 4.1.2; 2002; http://www.swox.com/gmp

[PLMo92] Peter L. Montgomery: Evaluating recurrences of form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains, 1983,1992; ftp://ftp.cwi.nl/pub/pmontgom/

[14] Dies dürfte auch der Grund dafür gewesen sein, warum Lenstra den genialen Einfall hatte, elliptische Kurven zu verwenden: Er hat die Template-Eigenschaft des (p-1)-Algorithmus erkannt und ihre Verwendbarkeit für elliptische Kurven gesehen!