Martin Aigner

Zahlentheorie

Eine Einführung mit Übungen, Hinweisen und Lösungen

STUDIUM

BACHELORKURS

Skripte

VIEWEG+
TEUBNER

Martin Aigner

Zahlentheorie

Bachelorkurs Mathematik

Herausgegeben von:
Prof. Dr. Martin Aigner,
Prof. Dr. Heike Faßbender,
Prof. Dr. Jürg Kramer,
Prof. Dr. Peter Gritzmann,
Prof. Dr. Volker Mehrmann,
Prof. Dr. Gisbert Wüstholz

Die Reihe ist zugeschnitten auf den Bachelor für mathematische Studiengänge.
Sie bietet Studierenden einen schnellen Zugang zu den wichtigsten mathematischen Teilgebieten. Die Auswahl der Themen entspricht gängigen Modulen, die in einsemestrigen Lehrveranstaltungen abgehandelt werden können.
Die Lehrbücher geben eine Einführung in ein mathematisches Teilgebiet. Sie sind im Vorlesungsstil geschrieben und benutzerfreundlich gegliedert. Die Reihe enthält Hochschultexte und kurz gefasste Skripte und soll durch Übungsbücher ergänzt werden.

Lars Grüne / Oliver Junge
Gewöhnliche Differentialgleichungen

Wolfgang Fischer / Ingo Lieb
Einführung in die Komplexe Analysis

Jörg Liesen / Volker Mehrmann
Lineare Algebra

Martin Aigner
Zahlentheorie

www.viewegteubner.de

Martin Aigner

Zahlentheorie

Eine Einführung mit Übungen, Hinweisen und Lösungen

STUDIUM

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Prof. Dr. Martin Aigner
Freie Universität Berlin
Institut für Mathematik
Arnimallee 3
14195 Berlin

aigner@math.fu-berlin.de

1. Auflage 2012

Lektorat: Schmickler-Hirzebruch | Barbara Gerlach

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: AZ Druck und Datentechnik, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8348-1805-8

Inhalt

Vorwort **vii**

1 Zum Aufwärmen **1**
1.1 Fibonacci Zahlen 1
1.2 Das Pascalsche Dreieck 7
1.3 e, π und andere Zahlen 12

2 Primzahlen **21**
2.1 Elementare Tatsachen 21
2.2 Kongruenzrechnung 24
2.3 Die prime Restklassengruppe $\mathbb{Z}_n^*$ 28
2.4 Quadratische Reste 32
2.5 Pseudoprimzahlen und der Miller-Rabin Test 41
2.6 Wo liegen die Primzahlen? 49
2.7 Wie erzeugt man Primzahlen? 52

3 Irrationale Zahlen **55**
3.1 Approximation durch Brüche 56
3.2 Kettenbrüche 58
3.3 Irrationalzahlen und unendliche Kettenbrüche 60
3.4 Approximation mittels Kettenbrüchen 64
3.5 Die Kettenbruchentwicklung von $\boldsymbol{e}$ 67
3.6 Die Pellsche Gleichung 70

4 Algebraische Zahlen **77**
4.1 Pythagoreische Tripel 77
4.2 Einiges über elliptische Kurven 79
4.3 Summe von Quadraten 85
4.4 Quadratische Formen 90
4.5 Quadratische Zahlringe 104
4.6 Das Polynom von Euler zur Primzahlerzeugung 114
4.7 Lucas-Lehmer Test 118

5 Transzendente Zahlen **121**
5.1 Gibt es transzendente Zahlen? 121
5.2 Ordnung der Approximierbarkeit 122
5.3 Konstruktion transzendenter Zahlen 124
5.4 Die Transzendenz von e und π 127

Anhang **137**
A. Hauptsatz der Arithmetik 137
B. Teilerlehre 137
C. Euklidischer Algorithmus 138
D. Algebraische Strukturen 139
E. Kongruenzrechnung 140

Lösungen der Übungen **143**

Literatur **155**

Index **159**

Vorwort

Die Zahlentheorie, neben Geometrie wohl das älteste Gebiet der Mathematik, hat im Lauf der Zeit nichts von ihrem Reiz eingebüßt – ganz im Gegenteil: Die Faszination zeitloser Probleme wie der Existenz von unendlich vielen Primzahlzwillingen oder der Fermatschen Vermutung genau so wie aktuelle Anwendungen in Kryptographie und Algorithmen lassen sie lebendiger denn je erscheinen. Trotzdem hat die Zahlentheorie nicht überall in der Bachelorausbildung ihren Platz. Das ist schade, zumal Vorlesungen über Zahlentheorie nach meiner Erfahrung als Grundlagen- und Anwendungsgebiet besonders geschätzt werden.

Das vorliegende Buch ist als Beitrag dazu gedacht, die Zahlentheorie in den Bachelor Lehrplan einzubauen. Es ist als Skript in mehreren Vorlesungen an der Freien Universität Berlin verwendet worden und ist das erste in der Bachelorreihe *Skripte* des Vieweg+Teubner Verlages. Es richtet sich an Bachelor Studenten der Mathematik des 3. – 5. Semesters und insbesondere auch an Lehramtsstudenten, die sich in Zahlentheorie vertiefen wollen. Es ist kein umfassendes Lehrbuch, sondern will den Stoff einer einsemestrigen Vorlesung vermitteln, der für einen ersten Überblick nötig ist. Für alle, die weitermachen wollen, hält die Literaturliste einige empfehlenswerte Bücher bereit.

Inhalt und Stil sind nach der Intention der Buchreihe eng an das tatsächliche Vorlesungsskript angelehnt, inklusive Zeitaufwand einer 4+2-stündigen Veranstaltung von 14 Wochen. Der Text umfasst dementsprechend etwa 140 Seiten, pro Woche gibt es 10 Übungen, die direkt in den Stoff einfließen (in der Vorlesung mussten jeweils 5 davon gelöst werden). Im einzelnen sieht der Zeitplan etwa so aus:

Kapitel 1:	Zum Aufwärmen	2 Wochen
Kapitel 2:	Primzahlen	4 Wochen
Kapitel 3:	Irrationale Zahlen	2½ Wochen
Kapitel 4:	Algebraische Zahlen	4 Wochen
Kapitel 5:	Transzendente Zahlen	1½ Wochen.

Die Übungen sind wie immer ein ganz wichtiger Teil. Es gibt einige reine Rechenaufgaben, andere haben einen Knobelcharakter, bei den meisten muss etwas bewiesen werden. Für viele Übungen gibt es Hinweise, und am Schluss des Buches findet man kurze Lösungen. Das Literaturverzeichnis enthält einige Klassiker, aber

auch neueste Bücher, die mir bei der Vorbereitung nützlich waren (oder die ich besonders schön finde). Es ist nach Kapiteln gegliedert und mit kurzen Kommentaren versehen.

Was wird vorausgesetzt? Zunächst natürlich eine Vertrautheit mit den mathematischen Grundbegriffen, wie sie in den Vorlesungen über Lineare Algebra und Analysis in den beiden ersten Semestern erworben wird. Empfehlenswert ist ferner eine Einführung in die Algebra/Zahlentheorie. Insbesondere von den folgenden Themen sollte man schon gehört haben:

- Hauptsatz der Arithmetik
- Größter gemeinsamer Teiler
- Euklidischer Algorithmus
- Grundbegriffe algebraischer Strukturen wie Gruppen und Ringe
- Kongruenzrechnung

Für alle, die sich hierbei nicht ganz sicher fühlen: Im Anhang werden die benötigten Begriffe bereit gestellt (und sie werden größtenteils im Text nochmals erläutert).

Mein Dank geht an Margrit Barrett vom Mathematischen Institut der Freien Universität Berlin für die makellose Abfassung des Manuskriptes, an Christoph Eyrich für die Endredaktion, und an Ulrike Schmickler-Hirzebruch vom Vieweg+Teubner Verlag für die wie immer angenehme Zusammenarbeit.

Zahlentheorie hat mich schon als Student begeistert, und die Faszination ist über die Jahre geblieben. Ein Skriptum kann natürlich niemals die Inspiration und Dramatik einer erstklassigen Vorlesung mit all ihren rhetorischen Höhenflügen erreichen. Es würde mich aber freuen, wenn dieses kurze „Skripte“-Buch einiges von der Schönheit und Eleganz dieses wunderbaren Gebietes vermitteln kann.

Berlin, Juli 2011 Martin Aigner

1 Zum Aufwärmen

Wir wollen am Beginn einige der bekanntesten Zahlen bzw. Zahlenfolgen betrachten und dabei typische Fragestellungen der Zahlentheorie kennenlernen, die ihrerseits wieder auf überraschende Zusammenhänge führen.

1.1 Fibonacci Zahlen

Jeder kennt die Fibonacci Zahlen. Sie sind bekanntlich definiert durch $F_0 = 0$, $F_1 = 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n \geq 2$. Hier ist eine Liste der ersten Zahlen:

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

Wir stellen uns folgende Fragen:

1) Gibt es eine geschlossene Formel für F_n?

2) Wie schnell wächst die Folge (F_n)?

3) Wann gilt, dass F_m ein Teiler von F_n ist?

4) Sei p Primzahl; gibt es ein n mit $p|F_n$?

Frage 1 lässt sich mit der allgemeinen Methode für Rekursionen beantworten. Hier ist der schnellste Weg. Es seien τ und ρ die Wurzeln der Gleichung $x^2 = x + 1$, also $\tau = \frac{1+\sqrt{5}}{2}$, $\rho = \frac{1-\sqrt{5}}{2}$; $\tau = 1{,}618$ heißt der *goldene Schnitt*. Es gilt $\tau > 1$, $-1 < \rho < 0$.

Behauptung. Für $z \in \{\rho, \tau\}$ gilt $z^n = F_n z + F_{n-1}$ $(n \geq 2)$.

Für $n = 2$ haben wir $z^2 = z + 1 = F_2 z + F_1$. Zum Induktionsschritt sehen wir

$$\begin{aligned} z^{n+1} &= zz^n = z(F_n z + F_{n-1}) = F_n z^2 + F_{n-1} z \\ &= F_n(z+1) + F_{n-1} z = F_{n+1} z + F_n. \end{aligned}$$

M. Aigner, *Zahlentheorie,* DOI 10.1007/978-3-8348-8344-5_1,

Somit ist

$$\tau^n = F_n\tau + F_{n-1}$$
$$\rho^n = F_n\rho + F_{n-1}.$$

Subtraktion ergibt

$$\tau^n - \rho^n = F_n(\tau - \rho)$$

und mit $\tau - \rho = \sqrt{5}$ erhalten wir

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\tfrac{1+\sqrt{5}}{2}\right)^n - \left(\tfrac{1-\sqrt{5}}{2}\right)^n\right]. \tag{1}$$

Übung 1. *Zeige* $F_n = \frac{1}{2^{n-1}}\sum_{i\geq 0}\binom{n}{2i+1}5^i$.
Hinweis: Binomialsatz in (1).

Aus (1) sehen wir

$$\frac{F_n}{\tau^n} = \frac{1}{\sqrt{5}}\left[1 - (\tfrac{\rho}{\tau})^n\right],$$

und wegen $|\frac{\rho}{\tau}| < 1$ folgt $\lim\limits_{n\to\infty}\frac{F_n}{\tau^n} = \frac{1}{\sqrt{5}}$, womit wir auch die Frage 2 beantwortet haben: F_n wächst wie $\frac{\tau^n}{\sqrt{5}}$, genauer ist F_n die nächste ganze Zahl an $\frac{\tau^n}{\sqrt{5}}$.
Ferner haben wir

$$\frac{F_{n+1}}{F_n} = \frac{\tau^{n+1} - \rho^{n+1}}{\tau^n - \rho^n} = \frac{\tau}{1 - (\frac{\rho}{\tau})^n} + \frac{\rho}{1 - (\frac{\tau}{\rho})^n} \underset{n\to\infty}{\longrightarrow} \tau. \tag{2}$$

Wir wollen uns nun die Folge der Brüche $\frac{F_{n+1}}{F_n}$ näher ansehen und (2) nochmals beweisen.

Sei $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

Behauptung. $A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$.

Dies stimmt für $n = 1$, und mit Induktion erhalten wir

$$A^{n+1} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}.$$

Wenden wir den Produktsatz für Determinanten an: $\det A^n = (\det A)^n$, so erhalten wir

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

und somit

$$\frac{F_{n+1}}{F_n} - \frac{F_n}{F_{n-1}} = \frac{(-1)^n}{F_nF_{n-1}}. \tag{3}$$

Dies wiederum ergibt

$$\frac{F_{2k}}{F_{2k-1}} < \frac{F_{2k-1}}{F_{2k-2}}, \frac{F_{2k+1}}{F_{2k}} \qquad (k \geq 1).$$

Die ersten Glieder sind

$$\frac{F_2}{F_1} = \frac{1}{1} < \frac{F_3}{F_2} = \frac{2}{1} > \frac{F_4}{F_3} = \frac{3}{2} < \frac{F_5}{F_4} = \frac{5}{3} > \dots$$

Nun betrachten wir die Teilfolgen $\left(\frac{F_{2k}}{F_{2k-1}}\right)$ und $\left(\frac{F_{2k+1}}{F_{2k}}\right)$ einzeln.

Übung 2. *Zeige*

$$1 = \frac{F_2}{F_1} < \frac{F_4}{F_3} < \frac{F_6}{F_4} < \dots \text{ bzw. } \dots < \frac{F_7}{F_6} < \frac{F_5}{F_4} < \frac{F_3}{F_2} = 2.$$

Ferner ist

$$\frac{F_{2k}}{F_{2k-1}} < \frac{F_{2j+1}}{F_{2j}} \text{ für alle } k, j \geq 1$$

wegen

$$\frac{F_{2k}}{F_{2k-1}} < \frac{F_{2k+2j+2}}{F_{2k+2j+1}} < \frac{F_{2k+2j+1}}{F_{2k+2j}} < \frac{F_{2j+1}}{F_{2j}}.$$

Also konvergieren $\left(\frac{F_{2k}}{F_{2k-1}}\right) \to \alpha$ und $\left(\frac{F_{2k+1}}{F_{2k}}\right) \to \beta$, und wegen (3) ist $\alpha = \beta$.

Somit existiert $\lim \frac{F_{n+1}}{F_n} = \alpha$. Und was ist α? Aus der definierenden Gleichung $F_{n+1} = F_n + F_{n-1}$ erhalten wir

$$\begin{array}{rcl} \frac{F_{n+1}}{F_n} & = & 1 + \frac{F_{n-1}}{F_n} \\ {\scriptstyle n\to\infty}\big\downarrow & & \\ \alpha & = & 1 + \frac{1}{\alpha}, \end{array}$$

das heißt $\alpha^2 = \alpha + 1$ und somit $\alpha = \tau$, da $\frac{F_{n+1}}{F_n}$ positiv ist.

In Kapitel 3 werden wir sehen, dass $\left(\frac{F_{n+1}}{F_n}\right)$ die „beste“ approximierende Folge von rationalen Zahlen zum goldenen Schnitt $\tau = \frac{1+\sqrt{5}}{2}$ ist.

Übung 3. *Zeige $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ und beweise umgekehrt, dass aus $|m^2 - mk - k^2| = 1$ für $m, k \in \mathbb{Z}$ folgt $\{m,k\} = \{\pm F_{n+1}, \pm F_n\}$ für ein n.*

Hinweis: Mit $\{m,k\}$ ist auch $\{k, m-k\}$ ein mögliches Paar.

Nun zur Frage 3 der Teilbarkeit. Zunächst haben wir aus der Rekursion und Induktion

$$\mathrm{ggT}(F_n, F_{n+1}) = \mathrm{ggT}(F_n, F_{n+2}) = 1 \qquad (n \geq 1).$$

Aus der Liste der ersten Zahlen sehen wir zum Beispiel, dass $F_3 = 2$ die Zahlen $F_6 = 8, F_9 = 34, F_{12} = 144, F_{15} = 610$ teilt und $F_4 = 3$ die Zahlen $F_8 = 21, F_{12} = 144$. Dies sollte den folgenden Satz nahelegen, dem wir eine Übung vorausschicken.

Übung 4. *Für alle $m, k \geq 1$ gilt $F_{m+k} = F_{k+1}F_m + F_kF_{m-1}$.* (4)

Hinweis: Induktion.

Satz 1.1. *Es gilt $F_m \big| F_n \iff m \big| n$ $(m, n \geq 3)$.*

Beweis. Sei $n = km$. Dann haben wir nach (4)

$$F_{km} = F_{(k-1)m+1}F_m + F_{(k-1)m}F_{m-1}.$$

Mit Induktion gilt $F_m \big| F_{(k-1)m}$ und somit $F_m \big| F_{km}$. Nun sei umgekehrt $F_m \big| F_n$. Wegen $m, n \geq 3$ haben wir $2 \leq F_m \leq F_n$, $m \leq n$; es sei $n = qm + r$, $0 \leq r < m$. Nach (4) gilt

$$F_n = F_{n-m+1}F_m + F_{n-m}F_{m-1} \tag{5}$$

und somit $F_m \big| F_{n-m}$, da F_m, F_{m-1} teilerfremd sind. Im nächsten Schritt sehen wir $F_m \big| F_{n-2m}$, und schließlich

$$F_m \big| F_{n-qm} = F_r.$$

Da aber $F_r < F_m$ ist, muß $F_r = 0$ sein, das heißt $r = 0$ und dies bedeutet $m \big| n$. □

Übung 5. *Zeige $\mathrm{ggT}(F_m, F_n) = F_{\mathrm{ggT}(m,n)}$.*

Hinweis. Euklidischer Algorithmus.

Wir kommen zur letzten und interessantesten Frage. Gibt es zu einer Primzahl p stets eine Fibonacci Zahl F_n, die ein Vielfaches von p ist? Wenn die Primzahl p in der Fibonacciliste auftaucht, dann liefert unser Satz eine vollständige Antwort:

Sei $p = F_m$, dann gilt $p \mid F_n \iff m \mid n$. Zum Beispiel haben wir

$$\begin{aligned} 2 \mid F_n &\iff 3 \mid n \\ 3 \mid F_n &\iff 4 \mid n \\ 5 \mid F_n &\iff 5 \mid n. \end{aligned}$$

Aber was ist mit Primzahlen, zum Beispiel 7 oder 11, die nicht in der Liste erscheinen? Wir sehen, dass 7 ein Teiler von $F_8 = 21$ ist und 11 ein Teiler von $F_{10} = 55$, und für 17 erhält man $17 \mid F_{18} = 2584$. Die Primzahl p scheint also mit dem Index n von F_n zusammen zu hängen, er ist $p+1$ für $p = 7, 17$ und $p-1$ für $p = 11$. Und dies gilt tatsächlich immer.

Satz 1.2. *Sei $p > 5$ Primzahl. Dann gilt*

$$\begin{aligned} p \mid F_{p-1} \quad &\text{falls } p \equiv 1,4 \pmod 5 \\ p \mid F_{p+1} \quad &\text{falls } p \equiv 2,3 \pmod 5. \end{aligned}$$

Beweis. Wir verwenden die Formel aus Übung 1:

$$F_n = \frac{1}{2^{n-1}} \sum_{i \geq 0} \binom{n}{2i+1} 5^i.$$

Für $n = p-1$ erhalten wir

$$2^{p-2} F_{p-1} = \tbinom{p-1}{1} + \tbinom{p-1}{3} 5 + \cdots + \tbinom{p-1}{p-2} 5^{\frac{p-3}{2}}.$$

Jeder Binomialkoeffizient $\binom{p-1}{k}$ ist kongruent $\frac{(-1)(-2)\cdots(-k)}{1 \cdot 2 \cdots k} \equiv (-1)^k \pmod p$, somit $\binom{p-1}{2i+1} \equiv (-1)^{2i+1} \equiv -1 \pmod p$. Für die rechte Seite gilt somit

$$\sum_{i \geq 0} \binom{p-1}{2i+1} 5^i \equiv -(5^0 + 5^1 + \cdots + 5^{\frac{p-3}{2}}) = -\frac{5^{\frac{p-1}{2}} - 1}{4} \pmod p,$$

also

$$-2^p F_{p-1} \equiv 5^{\frac{p-1}{2}} - 1 \pmod p. \tag{6}$$

Für $n = p+1$ erhalten wir analog

$$2^p F_{p+1} = \tbinom{p+1}{1} + \tbinom{p+1}{3} 5 + \cdots + \tbinom{p+1}{p} 5^{\frac{p-1}{2}}.$$

Hier ist jeder Binomialkoeffizient $\binom{p+1}{2i+1} \equiv 0 \pmod p$ für $1 \le i \le \frac{p-3}{2}$ (da p im Zähler des Binomialkoeffizienten vorkommt, aber nicht im Nenner), und wir erhalten

$$2^p F_{p+1} \equiv (p+1) + (p+1)5^{\frac{p-1}{2}} \equiv 5^{\frac{p-1}{2}} + 1 \pmod p. \tag{7}$$

Nun verwenden wir den Satz von Fermat, den wir im nächsten Kapitel beweisen werden: Für alle a teilerfremd zu p gilt

$$a^{p-1} - 1 \equiv 0 \pmod p.$$

Die linke Seite faktorisieren wir

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p.$$

Also gilt immer

$$a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p \quad \text{oder} \quad a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p,$$

das heißt

$$p \Big| a^{\frac{p-1}{2}} - 1 \quad \text{oder} \quad p \Big| a^{\frac{p+1}{2}} - 1.$$

Setzen wir $a = 5$ und sehen uns (6) und (7) an, so erkennen wir, dass stets $p \Big| F_{p-1}$ oder $p \Big| F_{p+1}$ gilt, da p zu 2 teilerfremd ist. Aber wann gilt welcher Fall? Dies werden wir im nächsten Kapitel beantworten, wenn wir das berühmte quadratische Rezipozitätsgesetz von Gauß besprechen. Die Antwort wird sein:

$$5^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p \Longleftrightarrow p \equiv 1, 4 \pmod 5$$
$$5^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p \Longleftrightarrow p \equiv 2, 3 \pmod 5,$$

und damit wird der Satz bewiesen sein. □

Bemerkung. Allgemeine Rekursionsfolgen mit $L_0 = a$, $L_1 = b$ und $L_n = P \cdot L_{n-1} + Q \cdot L_{n-2}$ $(n \ge 2)$ heißen *Lucas Folgen*. Sie können mit ähnlichen Methoden behandelt werden.

Übung 6. *Das Fibonacci Zahlensystem. Zeige, dass jede Zahl n eindeutig als Summe $n = F_{k_1} + F_{k_2} + \cdots + F_{k_t}$ mit $k_i \ge k_{i+1} + 2$, $k_t \ge 2$ dargestellt werden kann. Beispiel:* $30 = 21 + 8 + 1$.

Übung 7. *Die Lucas Zahl ist $L_n = F_{n-1} + F_{n+1}$. Zeige $F_{2n} = F_n L_n$ und drücke L_n durch $\tau = \frac{1+\sqrt{5}}{2}$ und $\rho = \frac{1-\sqrt{5}}{2}$ aus.*