

Quadrate in der Lucas-Folge

Unterlagen für Lehrende

Univ.-Prof. Dr. C. Fuchs

01.06.2023

Grundsätzlich: Die einzigen Quadratzahlen in der Lucas-Folge sind 1 und 4.

Technologieeinsatz mit Sage:

Link zu SageCell: <https://sagecell.sagemath.org/>

Einige nützliche Sage-Befehle: `BinaryRecurrenceSequence (period, pthpowers)`, `quadratic_residues`, `kronecker`

Programm in Stichworten:

Wiederholung (Fibonacci-Folge, Division mit Rest), Lucas-Folge, Eigenschaften und Zusammenhänge. Quadratische Reste: Motivation, Definition des Legendre- und Jacobi- (bzw. Kronecker-) Symbols, Eigenschaften. Bestimmung der Quadrate in der Lucas-Folge.

Dauer: 2 Unterrichtseinheiten, Voraussetzung: Fibonacci-Zahlen und Division mit Rest, Niveau: ★★★

Die Folge der Fibonacci-Zahlen ist definiert durch $F_0 = 0, F_1 = 1$ sowie $F_{n+2} = F_{n+1} + F_n$. Es gilt

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

Wir beginnen mit der Identität $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$. Sie gilt (unter Verwendung von $F_{-1} = 1$) für $m = 0$: $F_{m+n} = F_n = F_{-1}F_n + F_0F_{n+1} = F_{m-1}F_n + F_mF_{n+1}$. Sie gilt für $m = 1$: $F_{m+n} = F_{n+1} = F_0F_n + F_1F_{n+1} = F_{m-1}F_n + F_mF_{n+1}$. Wir zeigen nun den Induktionsschritt $m, m+1 \rightarrow m+2$: Nach Induktionsvoraussetzung gilt $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ und $F_{m+1+n} = F_{m+1-1}F_n + F_{m+1}F_{n+1}$. Addition der linken und rechten Seiten dieser Gleichungen liefert $F_{m+2+n} = F_{m+n} + F_{m+1+n} = F_{m-1}F_n + F_mF_{n+1} + F_{m+1-1}F_n + F_{m+1}F_{n+1} = (F_{m-1} + F_m)F_n + (F_m + F_{m+1})F_{n+1} = F_mF_n + F_{m+2}F_{n+1} = F_{m+2-1}F_n + F_{m+2}F_{n+1}$. Somit ist die Identität gezeigt.

Wir betrachten jetzt anstatt der Fibonacci-Zahlen die Folge der Lucas-Zahlen (benannt nach dem französischen Mathematiker Lucas): $L_0 = 2, L_1 = 1, L_{n+2} = L_{n+1} + L_n$. Führe die ersten vier [Arbeitsaufträge](#) durch. Ziel dieser Einheit ist, zu zeigen, dass wir bereits alle Quadrate in der Lucas-Folge gefunden haben. Analog zu oben (d.h. im Wesentlichen mit dem gleichen Induktionsbeweis) gilt die Identität $L_{m+n} = F_{m-1}L_n + F_mL_{n+1}$. (Führe den Induktionsbeweis aus!) Wie hängen Fibonacci- und Lucas-Zahlen zusammen; sie erfüllen ja dieselbe Rekursionsvorschrift. Dazu zeigen wir zunächst die Identität: $L_n = F_{n-1} + F_{n+1}$. Sie gilt für $n = 0$: $L_0 = 2 = 1 + 1 = F_{-1} + F_1$. Sie gilt auch für $n = 1$: $L_1 = 1 = 0 + 1 = F_0 + F_2$. Wir zeigen jetzt den Induktionsschritt $n, n+1 \rightarrow n+2$: $L_{n+2} = L_{n+1} + L_n = (F_n + F_{n+2}) + (F_{n-1} + F_{n+1}) = (F_n + F_{n-1}) + (F_{n+2} + F_{n+1}) = F_{n+1} + F_{n+3} = F_{n+2-1} + F_{n+2+1}$. Es folgt $F_{2n} = F_{n+n} = F_{n-1}F_n + F_nF_{n+1} = F_n(F_{n-1} + F_{n+1}) = F_nL_n$, also $F_{2n} = F_nL_n$. Umgekehrt gilt $L_{n-1} + L_{n+1} = 5F_n$ (führe den Induktionsbeweis dazu selbst als Übung aus). Mit Induktion zeigt man zudem

$$L_n = \left(\frac{1 + \sqrt{5}}{2} \right)^n + \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

(Überzeuge dich davon!) Aus dieser Formel folgt die Identität $L_n^2 - L_{2n} = 2(-1)^n$ (setze in die Formel ein und quadriere; verwende die binomische Formel).

Wir können damit zeigen, dass keine Lucas-Zahl mit einem geraden Indexwert eine Quadratzahl ist. Angenommen es wäre $L_{2n} = x^2$. Dann folgt aus der letzten Formel (nämlich aus $2(-1)^n = L_n^2 - L_{2n} = L_n^2 - x^2 = (L_n - x)(L_n + x)$, wobei wir die bekannte Zerlegungsformel verwendet haben), dass 2 eine Differenz von Quadraten ist. Das geht nicht, da 2 eine Primzahl ist und die einzige Zerlegung daher $2 = 2 \cdot 1 = 1 \cdot 2 = (-2) \cdot (-1) = (-1) \cdot (-2)$ lauten. Sieh dir noch einmal [Arbeitsauftrag 9](#) an. All diese Fälle sind nicht möglich, da L_n und x ganze (und nicht rationale) Zahlen sind.

Als nächstes sei an Division mit Rest erinnert. Sind a, b ganze Zahlen, so gibt es stets eindeutig bestimmte ganze Zahlen q, r mit $a = bq + r$ sowie $0 \leq r < |b|$. Wir setzen z.B. $b = 4$ und berechnen die Reste von L_n bei Division durch 4. Wir erhalten $2, 1, 3, 0, 3, 3, 2, 1, \dots$. Die Folge ist periodisch mit Periodenlänge 6; der nächste Wert ergibt sich zudem als der Rest bei Division durch 4 der Summe der beiden vorher berechneten Reste. Wählen wir $b = 2$ so erhalten wir $0, 1, 1, 0, 1, 1, 0, \dots$. Der Rest ist 0 bei jedem Indexwert, der ein Vielfaches von 3 ist (mit anderen Worten ist L_n genau dann gerade, wenn 3 ein Teiler von n ist). Wir haben [Arbeitsauftrag 5](#) erledigt. Führe als weitere Beispiele für Division mit Rest die [Arbeitsaufträge 6, 7 und 8](#) aus. Wir erkennen: *Nicht jeder mögliche Rest tritt als Rest einer Quadratzahl auf!* Zur systematischen Untersuchung definieren wir für eine positive ganze Zahl a und eine Primzahl p :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a, \\ 1 & \text{falls } a \text{ Rest bei Division durch } p \text{ einer Quadratzahl ist,} \\ -1 & \text{sonst.} \end{cases}$$

(man spricht “ a über p ” und nennt diese Funktion das Legendre-Symbol von a über p). Ist b eine positive ganze Zahl mit Primfaktorzerlegung $b = p_1 p_2 \cdots p_r$, dann definieren wir

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_r}\right).$$

Die Funktion “ a über b ” nennt man das Jacobi-Symbol. Es lässt sich auch für alle anderen ganzen Zahlen sinnvoll definieren (sodass es für positive ganze Zahlen mit der obigen Definition übereinstimmt); diese Funktion nennt man dann das Kronecker-Symbol. Führe jetzt mit Sage die [Arbeitsaufträge 11 und 12](#) aus; was fällt auf? Wir benötigen die folgenden Eigenschaften des Kronecker-Symbols:

- Haben a und a' denselben Rest bei Division durch b , so ist a über b gleich a' über b .
- Stets gilt a^2 über b ist gleich 1.
- $b - 1$ über b ist gleich $(-1)^{(b-1)/2}$.
- Das Kronecker-Symbol von aa' über b ist gleich dem Produkt der Kronecker-Symbole von a über p und a' über p .

Die letzten beiden Aussagen benötigen eine Begründung. Sie folgt aus [Arbeitsauftrag 10](#). Hier etwas Hintergrundmaterial, das bei Bedarf verwendet werden kann: Wir zeigen zuerst, dass

$$\left(\frac{p-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & p = 2 \text{ oder Rest von } p \text{ bei Division durch 4 ist 1,} \\ -1 & \text{sonst.} \end{cases}$$

Ist $p = 2$ so ist $p - 1 = 1 = 1^2$. Ist der Rest von p bei Division durch 4 gleich 1 so gilt

$$1 \cdot 2 \cdot \dots \cdot (p-1) = \left(1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}\right) \left(\left(p - \frac{p-1}{2}\right) \cdot \dots \cdot (p-2)(p-1)\right)$$

(beachte, dass wegen der Voraussetzung $p-1$ gerade ist). Somit lässt $(p-1)!$ denselben Rest bei Division durch p wie $((p-1)/2)!$. Der Rest von $(p-1)!$ bei Division durch p ist aber gleich -1 bzw. $p-1$. Das Kronecker-Symbol $p-1$ über p ist somit gleich 1. Nehmen wir an, dass der Rest von p bei Division durch 4 gleich 3 ist. Nehmen wir weiter an, dass ein ganzes x existiert, sodass der Rest von x^2 bei Division durch p gleich $p-1$ bzw. -1 ist. Dann sind aber die Rest bei Division durch p der folgenden Zahlen gleich: $x^{p-1}, x^{2(p-1)/2} = (x^2)^{(p-1)/2}, (-1)^{(p-1)/2} = -1$. Widerspruch zum zweiten Teil von [Arbeitsauftrag 10](#), da 1 und -1 nur für $p = 2$ denselben Rest bei Division durch p liefern. Die allgemeine Aussage folgt jetzt aus der Tatsache, dass für ungerade b, b' die Zahlen $(bb' - 1)/2$ und $(b - 1)/2 + (b' - 1)/2$ entweder beide gerade oder beide ungerade sind (betrachte dazu den Rest bei Division durch 2 von $(bb' - 1)/2 - (b - 1)/2 - (b' - 1)/2$ und $(b - 1)(b' - 1)/2$). Somit ergibt sich (führe den Induktionsbeweis selbst aus) für $b = p_1 \cdots p_r$:

$$(-1)^{(p_1-1)/2+\dots+(p_r-1)/2} = (-1)^{(b-1)/2}$$

und somit die gewünschte Eigenschaft. Der Nachweis der letzten Behauptung verwendet wieder [Arbeitsauftrag 10](#). Wir lassen ihn hier weg.

Wir kommen nun zur Behandlung der Lucas-Zahlen mit geradem Index. Wir zeigen zuerst noch eine letzte Identität: Sei k eine gerade, positive ganze Zahl, die nicht ein Vielfaches von 3 ist. Dann gilt $L_{m+2k} = F_{m-1}L_{2k} + F_mL_{2k+1} = L_{m+1+2k-1} = F_mL_{2k-1} + F_{m+1}L_{2k}$, woraus durch Addition $2L_{m+2k} = F_{m-1}L_{2k} + F_mL_{2k+1} + F_mL_{2k-1} + F_{m+1}L_{2k} = (F_{m-1} + F_{m+1})L_{2k} + F_m(L_{2k+1} + L_{2k-1}) = L_mL_{2k} + 5F_mF_{2k} = L_m(L_k^2 - 2) + 5F_mF_kL_k$ folgt. Somit ist der Rest von $2L_{m+2k}$ gleich dem Rest von $-2L_m$ bei Division durch L_k . Da L_k ungerade ist, können wir durch 2 kürzen (schreibe die entsprechende Gleichung hin und überzeuge dich davon!). Somit haben L_{m+2k} und $-L_m$ denselben Rest bei Division durch L_k . Wir unterscheiden jetzt zwei Fälle:

1. Fall: n hat Rest 1 bei Division durch 4 (z.B. $n = 1, 5, 9, \dots$). Für $n = 1$ haben wir das Quadrat $L_1 = 1 = 1^2$ gefunden. Sei $n \neq 1$. Wir schreiben $n = 1 + 2 \cdot 3^r \cdot k$ mit k positiv, gerade und kein Vielfaches von 3. Setze $b = L_k$. Dann hat L_n denselben Rest wie $b - 1$ bei Division durch b . Also ist

$$\left(\frac{L_n}{b}\right) = \left(\frac{b-1}{b}\right) = (-1)^{(b-1)/2} = -1.$$

Das kann aber nicht passieren, wenn $L_n = x^2$ für ein ganzes x wäre.

2. Fall: n hat Rest 3 bei Division durch 4 (z.B. $n = 3, 7, 11, \dots$). Für $n = 3$ haben wir das Quadrat $L_3 = 4 = 2^2$ gefunden. Sei $n \neq 3$. Wir schreiben $n = 3 + 2 \cdot 3^r \cdot k$ mit k positiv, gerade und kein Vielfaches von 3. Setze $b = L_k$. Dann hat L_n denselben Rest wie $-L_3 = -4$. Es gilt auch hier

$$\left(\frac{L_n}{b}\right) = \left(\frac{-4}{b}\right) = \left(\frac{4}{b}\right) \left(\frac{-1}{b}\right) = \left(\frac{b-1}{b}\right) = (-1)^{(b-1)/2} = -1.$$

Das kann aber wieder nicht passieren, wenn $L_n = x^2$ für ein ganzes x wäre.

Arbeitsaufträge:

1. Bestimme einige Elemente der Lucas-Folge (mit Hand oder per Computer).
2. Welche Werte sind Quadratzahlen (mit Hand oder per Computer).
3. Verifiziere die Identität $F_{2n} = F_nL_n$ für einige n 's.

4. Berechne $L_{2n} - L_n^2$ für $n = 1, 2, 3, \dots$. Was fällt auf?
5. Welche Reste lässt L_n bei Division durch 2 (bzw. durch 4)?
6. Sei m eine fest gewählte positive ganze Zahl. Bestimme den Rest von x^2 bei Division durch m für $x = 0, 1, \dots, m - 1$.
7. Wiederhole die letzte Aufgabe für $m = 2, 3, 4, 5, 6, 7, 8, 9, 10$.
8. Für welche m tritt $m - 1$ als quadratischer Rest auf?
9. Überlege, warum sich 2 nicht als Differenz zweier Quadrate (ganzer Zahlen) schreiben lässt.
10. Sei p eine fest gewählte ungerade Primzahl und a eine fest gewählte ganze Zahl, die zu p teilerfremd ist. Verifiziere, dass p ein Teiler von $(p - 1)! + 1$ sowie von $a^{p-1} - 1$ ist.
11. Finde ein m , sodass das Kronecker-Symbol von L_5, L_9, L_{13} gleich -1 ist.
12. Finde ein m , sodass das Kronecker-Symbol von L_7, L_{11}, L_{15} gleich -1 ist.

Literatur:

1. A. Dujella: Number Theory, Zagreb, 2021.
2. C. Fuchs: Zahlentheorie, Vorlesungsskript, PLUS, 2022
3. G. Bard: Sage for Undergraduates, AMS, 2022

Quadrate in der Lucas-Folge

Handout

Univ.-Prof. Dr. C. Fuchs
01.06.2023

Grundsätzlich: Die einzigen Quadratzahlen in der Lucas-Folge sind 1 und 4.

Technologieeinsatz mit Sage:

Link zu SageCell: <https://sagecell.sagemath.org/>

Einige nützliche Sage-Befehle: `BinaryRecurrenceSequence` (period, pthpowers), `quadratic_residues`, `kronecker`

Programm in Stichworten:

Wiederholung (Fibonacci-Folge, Division mit Rest), Lucas-Folge, Eigenschaften und Zusammenhänge. Quadratische Reste: Motivation, Definition des Legendre- und Jacobi- (bzw. Kronecker-) Symbols, Eigenschaften. Bestimmung der Quadrate in der Lucas-Folge.

Arbeitsaufträge:

1. Bestimme einige Elemente der Lucas-Folge (mit Hand oder per Computer).
2. Welche Werte sind Quadratzahlen (mit Hand oder per Computer).
3. Verifiziere die Identität $F_{2n} = F_n L_n$ für einige n 's.
4. Berechne $L_{2n} - L_n^2$ für $n = 1, 2, 3, \dots$. Was fällt auf?
5. Welche Reste lässt L_n bei Division durch 2 (bzw. durch 4)?
6. Sei m eine fest gewählte positive ganze Zahl. Bestimme den Rest von x^2 bei Division durch m für $x = 0, 1, \dots, m-1$.
7. Wiederhole die letzte Aufgabe für $m = 2, 3, 4, 5, 6, 7, 8, 9, 10$.
8. Für welche m tritt $m-1$ als quadratischer Rest auf?
9. Überlege, warum sich 2 nicht als Differenz zweier Quadrate (ganzer Zahlen) schreiben lässt.
10. Sei p eine fest gewählte ungerade Primzahl und a eine fest gewählte ganze Zahl, die zu p teilerfremd ist. Verifiziere, dass p ein Teiler von $(p-1)! + 1$ sowie von $a^{p-1} - 1$ ist.
11. Finde ein m , sodass das Kronecker-Symbol von L_5, L_9, L_{13} gleich -1 ist.
12. Finde ein m , sodass das Kronecker-Symbol von L_7, L_{11}, L_{15} gleich -1 ist.



Was ist die Lucas-Folge? Welche ihrer Elemente sind Quadratzahlen?

Was hast du heute sonst gelernt?

Das hat mir gefallen. Das hat mir nicht gefallen.