Math Semesterber (2015) 62:7–15
DOI 10.1007/s00591-015-0144-x

Vom Kartenmischen zur Artinvermutung

Ehrhard Behrends

Eingegangen: 14. November 2014 / Angenommen: 12. Januar 2015 /
Online publiziert: 17. Februar 2015

In meinem Buch zum Thema „Mathematik und Zaubern“ spielt neben vielen anderen Verfahren auch das so genannte *Melkmischen* (englisch: “milk shuffle”) eine Rolle (vgl. [1], z. B. Abschn. 1.5). Darunter versteht man eine ganz besondere Methode, einen Kartenstapel durcheinanderzubringen. Es geht so:

- Man nehme den Stapel in die linke Hand und ziehe mit der rechten zwei Karten ab: eine von oben und eine von unten. Diese beiden Karten werden auf den Tisch gelegt.
- Zwei weitere werden abgezogen und auf die schon liegenden platziert.
- So geht das immer weiter, bis alle Karten auf dem Tisch liegen. (Ist die Kartenanzahl ungerade, wird die letzte Karte einfach auf die anderen gelegt.)

Aus nahe liegenden Gründen ist es für die Zauberei interessant zu wissen, welche Ordnung ein spezielles Mischverfahren hat, wie oft man es also anwenden muss, damit die ursprüngliche Kartenreihenfolge wieder erscheint. Für einige Beispiele ist das schon ausgerechnet worden. Zum Beispiel hat das perfekte Riffle Shuffle von 52 Karten die Ordnung 8. Mehr dazu findet man in [2], S. 99 und in [3]). Nachstehend wird die Ordnung des Melkmischens analysiert. (Für Untersuchungen zu einer damit verwandten Permutation vgl. [5]).

Formal gesehen ist einmaliges Melkmischen von n Karten eine Permutation Φ von n Elementen, also ein Element der symmetrischen Gruppe S_n, und gefragt wird nach der Ordnung von Φ in S_n. Hier ein Beispiel, wir betrachten 6 Karten, die wir von 0 bis 5 nummerieren. Die Ausgangskonfiguration ist dann 012345, durch Melkmischen wird daraus 231405. Im nächsten Schritt erhält man 143025, danach 304215, 420135 und schließlich 012345. Die Ordnung ist also im Fall $n = 6$ gleich 5. Mit Computerhilfe

E. Behrends (✉)
Fachbereich Mathematik und Informatik, Freie Universität Berlin,
Arnimallee 2–6, 14195 Berlin, Deutschland
E-Mail: behrends@mi.fu-berlin.de

Das Melkmischen

kann man entsprechende Rechnungen leicht bis zu einer beeindruckenden Größenordnung von n durchführen. Hier ist ein winziger Ausschnitt der entsprechenden Tabelle:

n	10	11	12	13	14	15	16	17	18	19	20	21	22
Ordnung	9	6	11	10	9	14	5	5	12	18	12	10	7
n	23	24	25	26	27	28	29	30	31	32	33	34	35
Ordnung	12	23	21	8	26	20	9	29	30	6	6	33	22

Trotz umfangreichen Datenmaterials war beim besten Willen kein allgemeines Bildungsgesetz zu erkennen. Lediglich zwei Regelmäßigkeiten fielen ins Auge:

- Die Ordnung im Fall von n Karten war immer durch $n-1$ beschränkt. Das ist überraschend, denn in der S_n sind ja viel größere Ordnungen möglich.
- In der berechneten Tabelle stand, für $s \in \mathbb{N}_0$, bei $n = 2^s$ und $n = 2^s + 1$ immer die Ordnung $s + 1$. (Vgl. die Werte für $n = 16, 17, 32$ und 33 im vorstehenden Ausschnitt.)

Weitere Rechnungen ergaben eine noch viel größere weitere Überraschung. Da die Ordung einer Permutation das kleinste gemeinsame Vielfache der Zykellängen ist, wurden auch diese systematisch bestimmt. Und dabei stellte sich heraus, dass alle Zykellängen Teiler einer speziellen Zykellänge sind. Damit wäre dann leicht zu erklären, dass die Ordnungen höchstens gleich $n-1$ sein können, es fehlte aber immer noch eine Formel für diese längste Zykellänge und eine Erklärung für dieses Teilbarkeitsphänomen.

Ziel der Arbeit ist eine vollständige Analyse des Problems. Das Hauptergebnis wird besagen, dass die gesuchte Ordnung mit der kleinsten Zahl s übereinstimmt, für die 2^s kongruent $+1$ oder -1 modulo $2n-1$ ist. Die offen bleibenden Fragen hängen mit seit Jahrzehnten ungelösten Problemen der Zahlentheorie zusammen (*Sophie-Germain-Primzahlen*, *Artin-Vermutung*).

1 Einige Bezeichnungsweisen

Wir fixieren für die ersten zwei Abschnitte ein $n \in \mathbb{N}$, die Kartenanzahl. Es wird günstig sein, ein spezielles Symbol für $n-1$ einzuführen: Wir definieren $m := n-1$. Um die zum Melkmischen von n Karten gehörige Permutation exakt beschreiben zu können, nummerieren wir die n Karten mit den Zahlen von 0 bis m. Das Melkmischen entspricht dann, wie leicht zu sehen ist, der Abbildung $\Phi : \{0, 1, \ldots, m\} \to \{0, 1, \ldots, m\}$, die folgendermaßen definiert ist: Für ein k mit $2k < m$ ist $\Phi(k) := m - 1 - 2k$, und für die k mit $2k \geq m$ wird $\Phi(k) := 2k - m$ gesetzt. Offensichtlich ist $\Phi(m) = m$, das entspricht der Tatsache, dass die unterste Karte beim Melkmischen unten bleibt. Uns interessiert die kleinste Zahl s, für die Φ^s die identische Abbildung ist.

Wir werden für die nachstehenden Untersuchungen einige Definitionen benötigen:

1. ψ_0 *und* ψ_1. Das sind diejenigen Abbildungen, die bei der Definition von Φ gebraucht wurden: ψ_0 und ψ_1 bilden $\mathbb{Z}$ nach $\mathbb{Z}$ ab, dabei ist ψ_0 durch $k \mapsto m - 1 - 2k$ und ψ_1 durch $k \mapsto 2k - m$ definiert.
2. *Die Abbildungen* ψ_σ. Es sei $s \in \mathbb{N}$, und $\sigma_1, \ldots, \sigma_s$ seien Elemente aus $\{0, 1\}$. Wir fassen das s-Tupel $\sigma_s \sigma_{s-1} \ldots \sigma_1 \in \{0, 1\}^s$ zum Symbol σ zusammen. (Achtung: Es wird von hinten nach vorne nummeriert.) $\psi_\sigma : \mathbb{Z} \to \mathbb{Z}$ ist dann durch

$$\psi_\sigma := \psi_{\sigma_s} \circ \psi_{\sigma_{s-1}} \circ \ldots \circ \psi_{\sigma_1}$$

   erklärt. So ist zum Beispiel $\psi_{110} = \psi_1 \circ \psi_1 \circ \psi_0$, d.h.

$$\psi_{110}(k) = 2(2(m - 1 - 2k) - m) - m = m - 4 - 8k.$$

3. *Die* $A_\sigma, B_\sigma, v_\sigma$. Aufgrund des Bildungsgesetzes der ψ_σ ist klar, dass $\psi_\sigma(k)$ stets mit geeigneten $A_\sigma, B_\sigma, v_\sigma$ als

$$\psi_\sigma(k) = A_\sigma m + B_\sigma + v_\sigma 2^s k$$

   geschrieben werden kann. Dabei ist $v_\sigma \in \{-1, +1\}$ das Vorzeichen von $2^s k$. Es ist leicht zu bestimmen: Jedes Mal, wenn ψ_0 angewendet wird, erhält k den Faktor -2, und im Fall von ψ_1 ist der Faktor $+2$. Damit ist $v_\sigma = (-1)^{N(\sigma)}$, wobei $N(\sigma)$ angibt, wie oft die 0 in σ auftritt.

2 Vorbereitungen

Für die $A_\sigma, B_\sigma, v_\sigma$ gibt es einfache Rekursionsformeln:

Lemma 2.1

(i) $A_0 = 1$, $A_1 = -1$, $B_0 = -1$, $B_1 = 0$, $v_0 = -1$, $v_1 = 0$.
(ii) $A_{0\sigma} = 1 - 2A_\sigma$, $A_{1\sigma} = 2A_\sigma - 1$.
(iii) $B_{0\sigma} = -1 - 2B_\sigma$, $B_{1\sigma} = 2B_\sigma$.
(iv) $v_{0\sigma} = -v_\sigma$, $v_{1\sigma} = v_\sigma$.

Dabei bedeutet, z.B., 0σ *dasjenige Element aus* $\{0, 1\}^{1+s}$*, für das die ersten (von rechts gezählten) Komponenten diejenigen von* σ *sind und die letzte gleich* 0 *ist.*

Beweis (i) ergibt sich direkt aus den Formeln für ψ_0 und ψ_1. Die Formeln für $A_{0\sigma}, B_{0\sigma}, v_{0\sigma}$ erhält man wie folgt. Nach Definition gilt doch $\psi_\sigma(k) = A_\sigma m + B_\sigma + v_\sigma 2^s k$. Dann ist

$$\begin{aligned}\psi_{0\sigma}(k) &= \psi_0(\psi_\sigma(k)) \\ &= m - 1 - 2\psi_\sigma(k) \\ &= m - 1 - 2(A_\sigma m + B_\sigma + v_\sigma 2^s k) \\ &= (1 - 2A_\sigma)m - 2B_\sigma - 1 - v_\sigma 2^{s+1} k.\end{aligned}$$

Der Faktor vor dem m, also die Zahl $A_{0\sigma}$, ist folglich $1 - 2A_\sigma$, und das beweist den ersten Teil von (ii). Ganz analog ergeben sich die noch fehlenden Formeln. □

Wir führen noch eine weitere Definition ein: C_σ soll die Zahl $1 - v_\sigma 2^s$ bezeichnen. Offensichtlich ist genau dann $\psi_\sigma(k) = k$, wenn $C_\sigma k = A_\sigma m + B_\sigma$ gilt. Das wird gleich wichtig werden, wenn wir den von k erzeugten Zykel analysieren wollen. Dazu werden wir die folgenden Tatsachen benötigen:

Lemma 2.2 *Für alle $\sigma = \sigma_s \dots \sigma_1$ gilt:*

(i) $C_\sigma = A_\sigma - 2B_\sigma$.
(ii) $\psi_\sigma(k) = k$ *gilt genau dann, wenn* $C_\sigma(2k+1) = A_\sigma(2m+1)$ *ist.*
(iii) A_σ *und* C_σ *haben stets das gleiche Vorzeichen. Genauer gilt: Ist* $N(\sigma)$ *(die Anzahl der Nullen in* σ*) gerade, so sind beide Zahlen negativ, und andernfalls sind sie positiv.*
(iv) *Es sei* $\sigma_1 = 0$ *und* $s \geq 2$. *Dann ist* $|A_\sigma| \leq 2^{s-1} - 1$.
(v) *Im Fall* $\sigma_1 = 1$ *und* $s \geq 2$ *ist* $|A_\sigma| \geq 2^{s-1} + 1$.
(vi) *Durchläuft* σ *alle Elemente aus* $\{0,1\}^s$, *so durchläuft* A_σ *alle ungeraden Zahlen* l *zwischen* -2^s *und* 2^s. *Da die Anzahl dieser Zahlen gleich* 2^s *ist, gibt es zu jedem derartigen* l *genau ein* σ *mit* $A_\sigma = l$.

Beweis (i) Wir beweisen das durch Induktion nach der Länge s von σ. Die Aussage ist für $s = 1$ richtig, denn wegen 2.1 (i) ist $A_0 - 2B_0 = 3 = 1 + 2^1 = 1 - v_0 2^1 = C_0$ sowie $A_1 - 2B_1 = -1 = 1 - 2^1 = 1 - v_1 2^1 = C_1$.

Wir nehmen nun an, dass für σ der Länge s alles bewiesen ist. Wir zeigen, dass die Gleichung dann auch für 0σ und 1σ gilt. Das folgt aus 2.1 (ii)–(iv):

$$\begin{aligned}A_{0\sigma} - 2B_{0\sigma} &= (1 - 2A_\sigma) - 2(-1 - 2B_\sigma) \\ &= 3 - 2(A_\sigma - 2B_\sigma) \\ &= 3 - 2C_\sigma \\ &= 3 - 2(1 - v_\sigma 2^s) \\ &= 1 + v_\sigma 2^{s+1} \\ &= 1 - v_{0\sigma} 2^{s+1} \\ &= C_{0\sigma}.\end{aligned}$$

Der Beweis für $A_{1\sigma} - 2B_{1\sigma} = C_{1\sigma}$ ist analog.

(ii) Angenommen, es gilt $k = \psi_\sigma(k)$. Das bedeutet $k = A_\sigma m + B_\sigma + v_\sigma 2^s k$, d.h. $C_\sigma k = A_\sigma m + B_\sigma$. Nach Multiplikation dieser Gleichung mit 2 und Ersetzen von $2B_\sigma$ durch $A_\sigma - C_\sigma$ folgt $C_\sigma(2k+1) = A_\sigma(2m+1)$.

Alle diese Schritte lassen sich umkehren: $C_\sigma(2k+1) = A_\sigma(2m+1)$ bedeutet

$$2C_\sigma k = 2A_\sigma m + A_\sigma - C_\sigma = 2A_\sigma m + 2B_\sigma,$$

woraus nach Teilen durch 2 die Gleichung $C_\sigma k = A_\sigma m + B_\sigma$, d.h. $\psi_\sigma(k) = k$ folgt.

(iii) Allgemein gilt: Ist $A_\sigma > 0$, so ist $B_\sigma < 0$; und ist $A_\sigma < 0$, so ist $B_\sigma \geq 0$. Das folgt wieder durch Induktion unter Verwendung von Lemma 2.1. (Beachte: Alle A_σ sind ungerade und folglich von 0 verschieden.) Mit (i) folgt, dass A_σ und C_σ das gleiche Vorzeichen haben. Der Zusatz ergibt sich dadurch, dass v_σ genau dann positiv ist, wenn $N(\sigma)$ gerade ist.

(iv) Die Aussage stimmt für $s = 2$, da $A_{00} = -1$ und $A_{10} = 1$ gilt. Für größere s machen wir einen Induktionsschluss unter Verwendung von 2.1(ii). Wir nehmen an, dass $|A_\sigma| \leq 2^{s-1} - 1$, wobei $s \geq 2$ und $\sigma_1 = 0$. Dann ist für beliebige $\sigma_{s+1} \in \{0, 1\}$

$$|A_{\sigma_{s+1}\sigma}| = |2A_\sigma - 1| \leq 2|A_\sigma| + 1 \leq 2^s - 1.$$

(v) Für $s = 2$ folgt die Aussage aus $A_{01} = 3$ und $A_{11} = -3$. Diesmal geht der Induktionsschluss so:

$$|A_{\sigma_{s+1}\sigma}| = |2A_\sigma - 1| \geq |2A_\sigma| - 1 \geq 2^s + 1.$$

(vi) Es ist $A_0 = 1$ und $A_1 = -1$, die Aussage ist also für $s = 1$ richtig. Angenommen, sie stimmt für ein festes s. Wir zeigen, dass sie dann auch für $s + 1$ gilt. Sei dazu l eine ungerade Zahl zwischen -2^{s+1} und 2^{s+1}. Wir unterscheiden zwei Fälle:

Fall 1: $l = 1 \bmod 4$. Dann ist $l' := (l+1)/2$ ungerade, und l' liegt zwischen -2^s und 2^s. Nach Induktionsannahme gibt es ein σ der Länge s mit $A_\sigma = l'$. Dann ist (wegen 2.1(ii)) $l = 2l' - 1 = 2A_\sigma - 1 = A_{1\sigma}$.

Fall 2: $l = 3 \bmod 4$. Diesmal ist $l' := (l-1)/2$ ungerade, und $-2^s < l' < 2^s$. Wähle σ mit $A_\sigma = -l'$. Dann ist $l = 2l' + 1 = 1 - 2A_\sigma = A_{0\sigma}$. □

Es folgt die wichtigste Vorbereitung. Wir werden die Ordnung von Φ dadurch bestimmen, dass wir die zugehörigen Zykellängen ausrechnen. Dazu analysieren wir im folgenden Satz, wie man $\Phi^s(k) = k$ charakterisieren kann. Um $k = m$ brauchen wir uns nicht zu kümmern, denn wegen $\Phi(m) = m$ ist für diese Zahl alles klar.

Satz 2.3 *Es sei $k \in \{0, \ldots, m-1\}$. Die folgenden Aussagen sind äquivalent:*

(i) $\Phi^s(k) = k$.
(ii) Es gibt ein $\sigma \in \{0,1\}^s$ mit $C_\sigma(2k+1) = A_\sigma(2m+1)$.
(iii) Es gilt $2^s(2k+1) = (2k+1) \bmod (2m+1)$ oder $2^s(2k+1) = -(2k+1) \bmod (2m+1)$.

Beweis „(i) ⇒ (ii):“ Sei $\Phi^s(k) = k$. Bei der Berechnung von $\Phi(k)$, $\Phi^2(k)$, ... wird ψ_0 oder ψ_1 verwendet, und die konkrete Reihenfolge erzeugt ein Element aus $\{0,1\}^s$.

Etwas präziser sieht es so aus. Definiere $\sigma_1 := 0$, falls $2k < m$, und $\sigma_1 := 1$, falls $2k \geq m$. Betrachte dann $k_1 := \Phi(k)$ und setze $\sigma_2 := 0$, falls $2k_1 < m$ bzw. $\sigma_2 := 1$, falls $2k_1 \geq m$. Auf diese Weise erhält man $\sigma := \sigma_s \dots \sigma_1$, und wegen $\Phi^s(k) = k$ ist $\psi_\sigma(k) = k$. Wegen Lemma 2.2(ii) heißt das $C_\sigma(2k+1) = A_\sigma(2m+1)$.

„(ii) $\Rightarrow$ (i):“ Dieser Beweisteil ist der entscheidende Baustein zur Analyse der Ordnung von Φ. Er besagt, dass ein σ mit $C_\sigma(2k+1) = A_\sigma(2m+1)$ genau diejenigen σ_i enthält, die man bei der Berechnung von $\Phi^s(k)$ braucht.

Wir beginnen also mit einem σ, für das $C_\sigma(2k+1) = A_\sigma(2m+1)$ gilt.

Behauptung 1: $\Phi(k) = \psi_{\sigma_1}(k)$. Anders ausgedrückt: Die erste (ganz rechts stehende) Komponente von σ ist die, die auch für die Berechnung von $\Phi(k)$ verwendet wird. Wir müssen also zeigen: Ist $\sigma_1 = 0$, so ist $2k < m$, und im Fall $\sigma_1 = 1$ gilt $2k \geq m$. Wir konzentrieren uns zunächst auf den Fall $s \geq 2$, um Lemma 2.2(iv)(v) verwenden zu können.

Angenommen, es ist $\sigma_1 = 0$. Dann ist wegen 2.2(iv) $|A_\sigma| \leq 2^{s-1} - 1$, und folglich gilt

$$\frac{2k+1}{2m+1} = \Big|\frac{A_\sigma}{C_\sigma}\Big| \leq \frac{2^{s-1}-1}{2^s - 1} < \frac{1}{2}.$$

Das impliziert $2k < m$.

Im Fall $\sigma_1 = 1$ wissen wir, dass $|A_\sigma| \geq 2^{s-1} + 1$ gilt. Es folgt

$$\frac{2k+1}{2m+1} = \Big|\frac{A_\sigma}{C_\sigma}\Big| \geq \frac{2^{s-1}+1}{2^s + 1} > \frac{1}{2},$$

und daraus kann man $2k \geq m$ schließen.

Es fehlt noch eine Diskussion des Falls $s = 1$. Die Gleichung $\psi_0(k) = k$ bedeutet $k = m - 1 - 2k$, d. h. $3k = m - 1$. Und für solche k ist wirklich $2k < m$. Ist dagegen $\psi_1(k) = 2k - m = k$, so folgt $k = m$, und insbesondere ist $2k \geq m$.

Behauptung 2: Für alle $t = 1, \dots, s$ *ist* $\Phi^t(k) = \psi_{\sigma_t \sigma_{t-1} \dots \sigma_1}$. Der Fall $t = 1$ entspricht gerade der vorstehenden Behauptung 1. Wir erläutern die Idee für die weiteren t am Fall $t = 2$. Wir setzen (ii) voraus, wegen Lemma 2.2(ii) heißt das $\psi_\sigma(k) = k$. Oder ausgeschrieben: $\psi_{\sigma_s} \circ \dots \circ \psi_{\sigma_1}(k) = k$. Wir wenden auf beide Seiten dieser Gleichung ψ_{σ_1} an und erhalten

$$\psi_{\sigma_1} \circ \psi_{\sigma_s} \circ \dots \circ \psi_{\sigma_2}(\psi_{\sigma_1}(k)) = \psi_{\sigma_1}(k).$$

Zur Abkürzung setzen wir $\tilde{\sigma} := \sigma_1 \sigma_s \dots \sigma_2$ und $k' := \psi_{\sigma_1}(k)$. Wegen Behauptung 1 liegt k' in $\{0, \dots, m\}$, und es gilt $\psi_{\tilde{\sigma}}(k') = k'$. Nun wenden wir noch einmal Behauptung 1 an, diesmal für $\tilde{\sigma}$ und k'. Damit ist $\psi_{\sigma_2}(k') = \Phi(k')$, und das bedeutet $\psi_{\sigma_2 \sigma_1}(k) = \Phi^2(k)$. Ganz analog werden die Fälle $t = 2, 3, \dots, s$ behandelt.

„(ii)$\Rightarrow$(iii):“ Wähle σ gemäß Voraussetzung. Angenommen, es ist $C_\sigma = 1 - 2^s$. Dann folgt $(1 - 2^s)(2k+1) = A_\sigma(2m+1)$, und insbesondere ist $(1 - 2^s)(2k+1) = 0 \bmod (2m+1)$. Dann ist aber auch $2^s(2k+1) = (2k+1) \bmod (2m+1)$. Es könnte aber auch $C_\sigma = 1 + 2^s$ gelten, dann würde $(1 + 2^s)(2k+1) = A_\sigma(2m+1)$ die Gleichung $2^s(2k+1) = -(2k+1) \bmod (2m+1)$ implizieren.

„(iii)⇒(ii):“ Wir nehmen einmal an, dass $2^s(2k+1) = (2k+1) \bmod (2m+1)$ gilt. Es gibt also ein Zahl l mit $(2^s-1)(2k+1) = l(2m+1)$. Notwendig ist l ungerade, und es gilt $0 < l < 2^s$. Wähle ein $\sigma \in \{0,1\}^s$ mit $-l = A_\sigma$ (Lemma 2.2.(vi)). Mit A_σ ist auch C_σ negativ (Lemma 2.2(iii)), es ist also $C_\sigma = 1 - 2^s$ und folglich $C_\sigma(2k+1) = A_\sigma(2m+1)$.

Falls $2^s(2k+1) = -(2k+1) \bmod (2m+1)$ gilt, schreiben wir $(1+2^s)(2k+1)$ als $l(2m+1)$ mit einem ungeraden l, das echt zwischen 0 und 2^s liegt. Diesmal wählen wir ein $\sigma \in \{0,1\}^s$ mit $l = A_\sigma$. Da A_σ positiv ist, gilt $C_\sigma = 1 + 2^s$, d.h. wir erhalten $C_\sigma(2k+1) = A_\sigma(2m+1)$. □

3 Die Hauptergebnisse

Die vorstehenden Vorbereitungen führen zu

Theorem 3.1 *Sei $n \in \mathbb{N}$ und Φ diejenige Permutation von $\{0,\ldots,n-1\}$, die dem Melkmischen entspricht. (Ab jetzt ersetzen wir m wieder durch $n-1$.)*

- *(i) Bezeichne für $k \in \{0,\ldots,n-1\}$ mit $\lambda_n(k)$ die Länge des zugehörigen Zykels, also das kleinste s, für das $\Phi^s(k) = k$ gilt. Dann ist $\lambda_n(k)$ das kleinste $s \in \mathbb{N}$, für das $2^s(2k+1) = (2k+1) \bmod (2n-1)$ oder $2^s(2k+1) = -(2k+1) \bmod (2n-1)$ ist.*
- *(ii) Für alle $k \in \{0,\ldots,n-1\}$ ist $\lambda_n(k)$ ein Teiler von $\lambda_n(0)$.*
- *(iii) Ist $2k+1$ teilerfremd zu $2n-1$, so ist $\lambda_n(k) = \lambda_n(0)$.*
- *(iv) Die Ordnung von Φ, also das kleinste s, für das Φ^s die Identität ist, stimmt mit $\lambda_n(0)$, also dem kleinsten $s \in \mathbb{N}$ mit $2^s = \pm 1 \bmod (2n-1)$, überein*[1].
- *(v) Die Ordnung von Φ ist ein Teiler von $\varphi(2n-1)/2$, wobei φ die Eulersche φ-Funktion bezeichnet.*

Beweis (i) Das folgt sofort aus Satz 2.3(iii).

(ii) Es sei Δ_k die Menge aller $s \in \mathbb{Z}$, für die $2^s(2k+1) = (2k+1) \bmod (2n-1)$ oder $2^s(2k+1) = -(2k+1) \bmod (2n-1)$ gilt; da 2 im Restklassenring $\mathbb{Z}_{2n-1}$ invertierbar ist, sind auch negative s zugelassen. Es ist leicht zu sehen, dass Δ_k eine additive Untergruppe von $\mathbb{Z}$ ist, sie stimmt offensichtlich mit $\lambda_n(k)\mathbb{Z}$ überein. Man beachte nun, dass sicher $\Delta_0 \subset \Delta_k$ gilt, denn aus $2^s = \pm 1 \bmod (2n-1)$ folgt $2^s(2k+1) = \pm(2k+1) \bmod (2n-1)$. Als Untergruppe von Δ_k muss Δ_0 die Form $c\Delta_k$ für ein geeignetes $c \in \mathbb{N}$ haben, und damit ist alles gezeigt.

(iii) In diesem Fall ist $2k+1$ im Ring $\mathbb{Z}_{2n-1}$ invertierbar, und deswegen ist $\Delta_k = \Delta_0$.

(vi) Das folgt sofort aus (ii), denn die Ordnung einer Permutation ist das kleinste gemeinsame Vielfache der Zykellängen.

(v) Die multiplikative Gruppe $\mathbb{Z}_{2n-1}^*$ der invertierbaren Elemente von $\mathbb{Z}_{2n-1}$ hat $\varphi(2n-1)$ Elemente, und sie enthält die 2. Das kleinste s mit $2^s = \pm 1$ ist doch die

[1] Für das Melkmischen besagt das: Sobald die am Anfang oberste Karte wieder oben liegt, ist die Originalreihenfolge wiederhergestellt.

Ordnung der zur 2 gehörigen Nebenklasse in der Quotientengruppe $\mathbb{Z}_{2n-1}^*/\{-1,+1\}$. Das beweist die Behauptung. □

Abschließend wenden wir uns der Frage zu, welche maximalen und welche minimalen Ordnungen auftreten können. Die kleinsten Werte werden bei Zahlen der Form 2^{s_0} und $2^{s_0}+1$ erreicht:

Satz 3.2 *Bezeichne mit* $\log_2 n$ *den Zweierlogarithmus von n. Stets ist die Ordnung von* Φ *größer oder gleich* $\lfloor \log_2 n \rfloor + 1$*; dabei steht, für* $x \in \mathbb{R}$, $\lfloor x \rfloor$ *für die größte ganze Zahl k mit* $k \le x$.

Genauer gilt: Ist n von der Form 2^{s_0} *oder* $2^{s_0}+1$ *für ein* $s_0 \in \mathbb{N}$*, so ist die Ordnung gleich* $s_0 + 1 = \lfloor \log_2 n \rfloor + 1$*, und andernfalls ist sie mindestens gleich* $\lfloor \log_2 n \rfloor + 3$.

Beweis Im Fall $n = 2^{s_0}$ ist $2n - 1 = 2^{s_0+1} - 1$. Damit ist $s_0 + 1$ das kleinste s, für das $2^s = \pm 1$ in $\mathbb{Z}_{2n-1}$ gilt. Ganz analog wird der Fall $n = 2^{s_0} + 1$ behandelt.

Ist n nicht von dieser Form, so liegt n echt zwischen $2^{s_0} + 1$ und 2^{s_0+1}, wobei $s_0 = \lfloor \log_2 n \rfloor$. Damit ist $2^{s_0+1} + 1 < 2n - 1 < 2^{s_0+2} - 1$. Deswegen ist keine der Zahlen $2^1, 2^2, \ldots, 2^{s_0+1}, 2^{s_0+2}$ kongruent $+1$ oder -1 modulo $2n-1$, und das beweist die Behauptung. (Es ist möglich, dass die Ordnung gleich $s_0 + 3$ ist. So gehört zu $n = 11$ etwa die Ordnung 6, und im Fall $n = 22$ hat Φ die Ordnung 7.) □

Die Frage nach den n mit maximaler Ordnung ist weit schwieriger zu beantworten. Wir beginnen mit einer Charakterisierung:

Satz 3.3 *Die folgenden Aussagen sind äquivalent:*

(i) Die Ordnung von Φ *ist maximal, also gleich* $n - 1$.
(ii) $2n - 1$ *ist eine Primzahl, und* $s = n - 1$ *ist die kleinste natürliche Zahl, für die* $2^s = 1$ *oder* $2^s = -1$ *im Körper* $\mathbb{Z}_{2n-1}$ *gilt.*

Beweis Wir setzen zunächst (i) voraus. Wäre $2n-1$ *keine* Primzahl, so wäre $\varphi(2n-1) < 2n-2$. Da die Ordnung von Φ ein Teiler von $\varphi(2n-1)/2$ ist, wäre sie im Widerspruch zur Voraussetzung kleiner als $n-1$. Dass $2^s = \pm 1$ erst für $s = n-1$ gelten kann, folgt aus Theorem 3.1(iv). Mit diesem Teil des Theorems ist auch klar, dass (i) aus (ii) folgt. □

Wenn man die Ordnungen mit dem Computer ausrechnen lässt, so zeigt sich, dass bis zur Größenordnung einiger Millionen etwa 7 % der Zahlen maximale Ordnung haben. Man kann sich fragen, ob das unendlich oft vorkommt. Die Antwort ist offen, wir können nur das folgende Teilergebnis präsentieren:

Satz 3.4

(i) Es sei p eine Sophie-Germain-Primzahl, d.h. p und $2p + 1$ *sind Primzahlen. Dann hat* Φ *für* $n = p + 1$ *maximale Ordnung.*
(ii) Die ungerade Primzahl p sei als $p = 2n - 1$ *geschrieben, und die Zahl* 2 *sei Primitivwurzel für p (d. h. die von* 2 *erzeugte multiplikative zyklische Gruppe stimmt mit* $\mathbb{Z}_p^*$ *überein). Dann hat* Φ *für dieses n maximale Ordnung.*

Beweis (i) Sei p eine derartige Primzahl und $n := p + 1$. Dann ist $\mathbb{Z}_{2n-1} = \mathbb{Z}_{2p+1}$ ein Körper, und $\phi(2n-1)/2 = p$. Die Ordnung von Φ ist ein Teiler von p und sicherlich nicht gleich 1. Sie ist also gleich $p = n - 1$ und folglich maximal.

(ii) Angenommen, es gäbe ein $s < (p-1)/2$ mit $2^s = 1$ oder gleich -1 in $\mathbb{Z}_p$. Dann wäre $2^{(p-1)/2} = 1$ im Widerspruch zur Voraussetzung, dass 2 Primitivwurzel bzgl. p ist. □

Bemerkung: Zur Illustration von (i) blättere man zu den Ordnungen für $n = 12, 24, 30$ in der obigen Tabelle zurück. Beispiele, bei denen 2 Primitivwurzel für die Primzahl $2n - 1$ ist, sind $n = 6, 7, 10, 15, 19, 27, \ldots$.

Es ist unbekannt, ob es unendlich viele Sophie-Germain-Primzahlen gibt, und man weiß auch nicht, ob es unendlich viele p gibt, für die 2 Primitivwurzel ist. Das ist ein Spezialfall der berühmten Artin-Vermutung. Für die hier betrachtete Frage würde es sogar reichen, dass 2 so etwas wie eine „halbe Primitivwurzel" ist: Die von 2 erzeugte zyklische Gruppe muss wenigstens $(p-1)/2$ Elemente enthalten. (Das ist – neben den Fällen, bei denn 2 wirklich eine Primitivwurzel ist – für $n = 12, 24, 36, 52, 84, \ldots$ der Fall.) Aber auch für diese abgeschwächte Form der Artin-Vermutung scheint es ein offenes Problem zu sein, ob unendlich viele p diese Eigenschaft haben.

Danksagung: Ich möchte meinem Kollegen Martin Aigner ganz herzlich für viele anregende Diskussionen zu den hier behandelten Fragen danken.

In [2], S. 95, wird darauf hingewiesen, dass das Melkmischen invers zum Mongemischen ist. Im Internet findet man zum Monge-Mischen die Quelle [2], S. 227, doch die ist auch nicht wirklich hilfreich. Es wird zwar eine Formel für die Ordnung beim Monge-Mischen angegeben, die als Spezialfall der vorstehenden Ergebnisse aufgefasst werden kann, es fehlt aber eine Quellenangabe, wo man die Details nachlesen könnte: "There exists a theorem ...".

In diesem Zusammenhang ist auch die Arbeit [5] zu erwähnen (die möglicherweise in [2] gemeint war). Sie enthält eine Ausarbeitung von Lévys Ergebnissen, die in den Jahren davor in den Comptes Rendus erschienen waren. Lévy untersucht die Permutation Ψ, die für die $k \in \{0, \ldots, n-1\}$ durch $k \mapsto 2k$ (für $2k \leq n-1$) bzw. $k \mapsto 2n - 1 - 2k$ (für $2k > n-1$) definiert ist. Es gilt $\Phi = I \circ \Psi \circ I$, wobei I das Invertieren der Reihenfolge bedeutet. Φ und Ψ sind also konjugiert in der Gruppe S_n und haben deswegen die gleiche Ordnung. Die Beweismethoden sind allerdings völlig verschieden, und ein Zusammenhang zu Mischverfahren wird auch nicht hergestellt.

Literatur

1. Behrends, E.: Der mathematische Zauberstab. Erscheint 2015 im Rowohlt-Verlag, etwa 220 Seiten.
2. Diaconis, P., Graham, R.: Magical Mathematics. Princeton University Press (2012)
3. Diaconis, P., Graham, R., Kantor, W.: The Mathematics of Perfect Shuffles. Adv. Appl. Math. **4**, 175–196 (1983)
4. Epstein, R.A.: The Theory of Gambling and Statistical Logic. Elsevier Inc. (2009)
5. Lévy, P.: Sur quelques classes de permutations. Compositio Math. **8**, 1–48 (1951)