ZUM q-ANALOGON DER KONGRUENZ VON LUCAS

Volker Strehl

Department of Computer Science (Informatik 8)
Friedrich-Alexander-Universität Erlangen-Nürnberg
D-91058 Erlangen, Germany

In seiner klassischen Untersuchung über die Kongruenzen für Euler–Zahlen verwendet LUCAS folgende, nach ihm benannte Kongruenz für die Binomialkoeffizienten:

$$\binom{ap+b}{cp+d} \equiv \binom{a}{b}\binom{b}{d} \mod p$$

für natürliche Zahlen a, b, c, d mit $0 \leq b, d < p$ und p prim.

In seiner Arbeit über sogenannte Kummersche Kongruenzen für die q-Analoga der Euler–Zahlen macht J. DÉSARMÉNIEN entscheidend Gebrauch von einem q-Analogon dieser LUCAS-Kongruenz:

$$\begin{bmatrix} ak+b \\ ck+d \end{bmatrix}_q \equiv \binom{a}{b} \begin{bmatrix} b \\ d \end{bmatrix}_q \mod \Phi_k(q) \ ,$$

wobei a, b, c, d, k natürliche Zehlen mit $0 \leq b, d < k$ sind, und wo $\Phi_k(q)$ das k-te Kreisteilungspolynom und $\left[\ \right]_q$ das q-Analogon der Binomialkoeffizienten bezeichnet. Der von Désarménien gegebene Beweis ist rein arithmetischer Natur, so daß sich angesichts der bekannten kombinatorischen Interpretationen der q-Binomialkoeffizienten (Inversionsstatistik beziehungsweise major-index von MacMahon, siehe zum Beispiel ANDREWS, FOATA, KNUTH) die Frage stellt, ob man diese Kongruenz mit (weitgehend) kombinatorischen Mitteln beweisen kann.

Die Kongruenz von LUCAS ist insofern etwas unbefriedigend, als man im Fall $b < d$ nur erfährt, daß ein Binomialkoeffizient $\equiv 0 \mod p$ ist; allgemeiner interessiert man sich jedoch für die Restklasse mod p^{e+1} eines Binomialkoeffizienten, wenn p^e die höchste Potenz von p ist, die diesen Binomialkoeffizienten teilt. Fragen dieser Art sind natürlich in der Literatur schon untersucht worden, zum Beispiel von SINGMASTER, und es liegt nahe, diese Art der Fragestellung auf den Fall der q-Kongruenzen auszudehnen. Die Verallgemeinerung für q-Multinomialkoeffizienten kann in einen solchen Ansatz natürlich gleich mit einbezogen werden.

Um nun das allgemeine Resultat der gesuchten Art vorzustellen, bedarf es einiger Notation:

A bezeichne ein endliches, totalgeordnetes Alphabet, etwa $A = \{1, 2, \ldots, m\}$ mit der üblichen Ordnung; A^+ sei das freie Abelsche Monoid über A, Elemente von A^+ werden geschrieben als Vektoren $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ mit $\alpha_i \in \mathbb{N}$, $\iota : A^+ \to \mathbb{N}$ bezeichne den natürlichen Morphismus, das heißt $\iota(\alpha_1, \alpha_2, \ldots, \alpha_m) = \alpha_1 + \alpha_2 + \cdots + \alpha_m$. A^* bezeichne, wie üblich, das freie Monoid über A, dessen Elemente als Wörter über A geschrieben werden. $\tau : A^* \to A^+$ bezeichne den natürlichen Morphismus, für $\boldsymbol{\alpha} \in A^+$ ist dann $[\boldsymbol{\alpha}] := \{\mathbf{a} \in A : \tau\mathbf{a} = \boldsymbol{\alpha}\}$ die Menge aller Wörter (Multipermutationen) vom Typ $\boldsymbol{\alpha}$. Für $\mathbf{a} = a_1 a_2 \ldots a_n \in A^*$ sei

$$\mathrm{inv}(\mathbf{a}) := \mathrm{card}\{(i, j) : 1 \leq i < j \leq n,\, a_i > a_j\}$$

die Anzahl der Inversionen von $\mathbf{a}$; für $\boldsymbol{\alpha} \in A^+$ stellt dann

$$[\boldsymbol{\alpha}]_q := \sum \left\{ q^{\mathrm{inv}(\mathbf{a})} : \mathbf{a} \in [\boldsymbol{\alpha}] \right\}$$

den zum Typ $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ gehörenden q-Multinomialkoeffizienten dar:

$$[\boldsymbol{\alpha}]_q = \begin{bmatrix} \iota\boldsymbol{\alpha} \\ \alpha_1, \alpha_2, \ldots, \alpha_m \end{bmatrix}_q .$$

Sei nun eine ganze Zahl $k \geq 1$ fixiert. Für beliebige $n \in \mathbb{N}$ seien $Qn \in \mathbb{N}$ und $Rn \in \{0, 1, \ldots, k-1\}$ mittels der üblichen Division mit Rest definiert: $n = k \cdot Qn + Rn$. Dies gibt Anlaß zur Definition von zwei Abbildungen $Q^+ : A^+ \to A^+$ und $R^+ : A^+ \to A^+$ mit:

$$\begin{aligned} Q^+(\alpha_1, \alpha_2, \ldots, \alpha_m) &:= (Q\alpha_1, Q\alpha_2, \ldots, Q\alpha_m) \qquad \text{und} \\ R^+(\alpha_1, \alpha_2, \ldots, \alpha_m) &:= (R\alpha_1, R\alpha_2, \ldots, R\alpha_m) . \end{aligned}$$

Offensichtlich gilt dann für $\boldsymbol{\alpha} \in A^+$

$$k \cdot (Q \cdot \iota - \iota \cdot Q^+)\boldsymbol{\alpha} = (\iota \cdot R^+ - R \cdot \iota)\boldsymbol{\alpha}$$

und

$$e\boldsymbol{\alpha} := (Q \cdot \iota - \iota \cdot Q^+)\boldsymbol{\alpha}$$

ist eine nichtnegative ganze Zahl. Mit diesen Begriffen kann nun das Resultat formuliert werden.

Theorem. *Für alle* $\boldsymbol{\alpha} \in A^+$ *gilt:*

$$[\boldsymbol{\alpha}]_q \equiv 0 \qquad \mod (\Phi_k(q))^{e\boldsymbol{\alpha}} , \tag{1}$$

$$[\boldsymbol{\alpha}]_q \equiv \binom{Q\iota\boldsymbol{\alpha}}{\iota Q^+\boldsymbol{\alpha}} [Q^+\boldsymbol{\alpha}]_1 \, [R^+\boldsymbol{\alpha}]_q \quad \mod (\Phi_k(q))^{1+e\boldsymbol{\alpha}} . \tag{2}$$

Insbesondere erweist sich $e\boldsymbol{\alpha}$ als der (exakte) Exponent von $\Phi_k(q)$ in $[\boldsymbol{\alpha}]_q$, so daß sich unter den Folgerungen, die aus diesem Theorem gezogen werden können, ganz präzise Informationen über die Zerlegung von $[\boldsymbol{\alpha}]_q$ in irreduzible Faktoren (in $\mathbb{Z}[q]$) befinden.

Für $m = 2$ beinhaltet (2) eine (im oben angedeuteten Sinne) verschärfte Version der q-LUCAS-Kongruenz von DÉSARMÉNIEN. Als weitere Folgerungen findet man beispielsweise Resultate von FRAY über die p-Bewertung von q-Binomialkoeffizienten für ganzzahliges q, sowie — natürlich — für $q = 1$ die klassischen Resultate über Primfaktorzerlegung und Kongruenzen für Binomial- und Multinomialkoeffizienten.

Abschließend sei betont, daß das Theorem, dessen arithmetische Konsequenzen natürlich keine großen Überraschungen beinhalten, und die man auch mit anderen Methoden herleiten kann, ein im Grunde rein kombinatorisches Resultat ist. Von arithmetischen Eigenschaften der Kreisteilungspolynome, die über die Definition und sich daran unmittelbar anschließende Folgerungen hinausgehen, wird kein Gebrauch gemacht.

Literatur

ANDREWS, *The Theory of partitions*, Addison–Wesley, 1976, Ch. 3.4.
DÉSARMÉNIEN, Europ. J. Combin. **3** (1982), 19–28.
FOATA, Proc. Amer. Math. Soc. **19** (1968), 236–240.
FRAY, Duke Math. J. **34** (1967), 469–480.
KNUTH, *The Art of Computer Programming*, vol. 3, Addison–Wesley, 1973, Ch. 5.1.
LUCAS, Bull. Soc. Math. France **6** (1878), 49–54.
SINGMASTER, J. London Math. Soc. (2) **8** (1974), 545–548.

Department of Computer Science (Informatik 8), Friedrich-Alexander-Universität Erlangen-Nürnberg, D-91058 Erlangen, Germany