

Zum q-Analogon der Kongruenz von LUCAS

Volker Strehl

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

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

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

In seiner Arbeit über sogenannte Kummer'sche Kongruenzen für die q-Analoga der Euler-Zahlen macht J. DESARMENIEN entscheidend Gebrauch von einem q-Analogon dieser LUCAS-Kongruenz:

$$\left[\begin{matrix} ak+b \\ ck+d \end{matrix} \right]_q \equiv \binom{a}{c} \left[\begin{matrix} b \\ d \end{matrix} \right]_q \pmod{\phi_k(q)}$$

wobei a, b, c, d, k natürliche Zahlen mit $0 \leq b, d < k$ sind, und wo $\phi_k(q)$ das k-te Kreisteilungspolynom und $\left[\begin{matrix} \\ \end{matrix} \right]_q$ das q-Analogon der Binomialkoeffizienten bezeichnet. Der von Desarmenien gegebene Beweis ist rein arithmetischer Natur, so dass sich angesichts der bekannten kombinatorischen Interpretationen der q-Binomialkoeffizienten (Inversionsstatistik bzw. major-index von MacMahon, siehe z.B. 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 $\equiv 0 \pmod{p}$ ist; allgemeiner interessiert man sich jedoch für die Restklasse $\pmod{p^{e+1}}$ 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, z.B. 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 $A = \{1, 2, \dots, m\}$ mit der üblichen Ordnung; A^+ sei das freie abelsche Monoid über A, Elemente von A^+ werden geschrieben als Vektoren $\underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_m)$ mit $\alpha_i \in \mathbb{N}$, $l: A^+ \rightarrow \mathbb{N}$ bezeichne den natürlichen Morphismus, d.h. $l(\alpha_1, \alpha_2, \dots, \alpha_m) = \alpha_1 + \alpha_2 + \dots + \alpha_m$. A^* bezeichne, wie üblich, das freie Monoid über A, dessen Elemente als Wörter über A geschrieben werden. $\tau: A^* \rightarrow A^+$ bezeichne den natürlichen Morphismus, für $\underline{\alpha} \in A^+$ ist dann $[\underline{\alpha}] := \{\underline{a} \in A^* ; \tau \underline{a} = \underline{\alpha}\}$ die Menge aller Wörter (Multi-permutationen) vom Typ $\underline{\alpha}$. Für $\underline{a} = a_1 a_2 \dots a_n \in A^*$ sei

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

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

$$[\underline{\alpha}]_q := \sum \{ q^{\text{inv}(\underline{a})} ; \underline{a} \in [\underline{\alpha}] \}$$

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

$$[\underline{\alpha}]_q = \left[\alpha_1, \alpha_2, \dots, \alpha_m \right]_q^{\underline{l}\underline{\alpha}}$$

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

$$Q^+(\alpha_1, \alpha_2, \dots, \alpha_m) := (Q\alpha_1, Q\alpha_2, \dots, Q\alpha_m) \quad \text{und}$$

$$R^+(\alpha_1, \alpha_2, \dots, \alpha_m) := (R\alpha_1, R\alpha_2, \dots, R\alpha_m) \quad .$$

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

$$k \cdot (Q \circ l - l \circ Q^+) \underline{\alpha} = (l \circ R^+ - R \circ l) \underline{\alpha}$$

und
$$e_{\underline{\alpha}} := (Q \circ l - l \circ Q^+) \underline{\alpha}$$

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

Theorem: Für alle $\underline{\alpha} \in A^+$ gilt:

$$(1) \quad [\underline{\alpha}]_q \equiv 0 \pmod{(\phi_k(q))^{e_{\underline{\alpha}}}}$$

$$(2) \quad [\underline{\alpha}]_q \equiv \binom{Q \underline{l} \underline{\alpha}}{l Q^+ \underline{\alpha}} [Q^+ \underline{\alpha}]_1 [R^+ \underline{\alpha}]_q \pmod{(\phi_k(q))^{1+e_{\underline{\alpha}}}}$$

Insbesondere erweist sich $e_{\underline{a}}$ als der (exakte) Exponent von $\Phi_k(q)$ in $[\underline{a}]_q$, so dass sich unter den Folgerungen, die aus diesem Theorem gezogen werden können, ganz präzise Informationen über die Zerlegung von $[\underline{a}]_q$ 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 DESARMENIEN. 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
 DESARMENIEN erscheint in: J.Europ.Combinatoire
 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