Kleine Mitteilungen

Kleine Mitteilungen

Eine Bemerkung zu den zyklischen Gruppen

1. Einleitung

Eine endliche zyklische Gruppe G von der Ordnung $O(G) = n$ enthält genau $\varphi(n)$ [1*] sogenannte primitive Elemente ω derart, daß jedes $a \in G$ eine Darstellung

$$a = \omega^r \quad (r \leqq n) \tag{1}$$

besitzt. Aufgrund von (1) is jedes $a \in G$ daher auch in der Form

$$a = \omega_1 \omega_2 \dots \omega_s \quad (s \leqq n)$$

mit nicht notwendig verschiedenen primitiven Elementen $\omega_i \in G$ darstellbar.
Es stellt sich dazu die Frage nach dem kleinsten s [2*]. Für eine zyklische Gruppe G und $a \in G$ möge mit $\mu(a, G)$ die kleinste Anzahl der nicht notwendig verschiedenen primitiven Elemente $\omega_i \in G$ bezeichnet werden, für welche $a = \omega_1 \omega_2 \dots \omega_s$ gilt.
In der vorliegenden Note soll $\mu(a, G)$ als Funktion der Ordnungen $o(a)$, $O(G)$ genau bestimmt werden.

Theorem. *Sei G eine zyklische Gruppe mit $O(G) = n$ und $a \in G$ mit $o(a) = t$. Dann gilt*

$$\mu(a, G) = \begin{cases} 1, & \textit{wenn} \quad t = n \\ 2, & \textit{wenn} \quad t < n \qquad\qquad \textit{und} \quad n \equiv 1 \pmod 2 \\ 2, & \textit{wenn} \quad t < n,\ n \equiv 0 \pmod 2 \quad \textit{und} \quad n/t \equiv 0 \pmod 2 \\ 3, & \textit{wenn} \quad t < n,\ n \equiv 0 \pmod 2 \quad \textit{und} \quad n/t \equiv 1 \pmod 2 \end{cases}.$$

2. Die additive Restklassengruppe modulo *n*

2.1. Es sei G_n eine zyklische Gruppe von der Ordnung n. Dann ist G_n isomorph zur additiven Gruppe R_n^+ der Restklassen modulo n.

2.2. Für die Ordnung $o(\bar{a})$ eines $\bar{a} \in R_n^+$ gilt die Regel [3*]

$$o(\bar{a}) = n/(a, n) \quad \text{bei} \quad a \in \bar{a}. \tag{2}$$

2.3. Zur Bestimmung von $\mu_n(a) := \mu(\bar{a}, R_n^+)$ bei $\bar{a} \in R_n^+$ und $a \in \bar{a}$ hat man die bezüglich s kleinste zulässige Darstellung

$$a \equiv b_1 + \dots + b_s \pmod n \tag{3}$$

zu ermitteln. Dabei möge eine Darstellung (3) von $a \in \mathbb{Z}$ genau dann *zulässig* heißen, wenn $b_i \in \mathbb{Z}$ und $(b_i, n) = 1$ für $i = 1, \dots, s$.

3. Herleitung eines Lemmas

Zur Ermittlung von (3) benötigt man das folgende

Lemma. *Sei* $a \in \mathbb{Z}$ *und* $n_1, n_2 \in \mathbb{N}$ *mit* $(n_1, n_2) = 1$. *Besitzt* a *die zulässigen Darstellungen*

$$a \equiv x_1 + \ldots + x_s \pmod{n_1}$$
$$a \equiv y_1 + \ldots + y_s \pmod{n_2},$$

so ist a *auch in der Form*

$$a \equiv z_1 + \ldots + z_s \pmod{n_1 n_2}$$

zulässig darstellbar [4*].

Beweis. Wegen $(n_1, n_2) = 1$ gibt es ganze Zahlen ξ_1, ξ_2 mit $n_2 \xi_1 \equiv 1 \pmod{n_1}$ bzw. $n_1 \xi_2 \equiv 1 \pmod{n_2}$. Man bilde die Zahlen

$$z_i = x_i n_2 \xi_1 + y_i n_1 \xi_2 \quad (i = 1, \ldots, s).$$

Dann ist $z_i \equiv x_i \pmod{n_1}$ bzw. $z_i \equiv y_i \pmod{n_2}$, so daß $a \equiv z_1 + \ldots + z_s \pmod{n_1}$ bzw. $a \equiv z_1 + \ldots + z_s \pmod{n_2}$. Wegen $(n_1, n_2) = 1$ gilt damit $a \equiv z_1 + \ldots + z_s \pmod{n_1 n_2}$. Andererseits ist $(z_i, n_1) = 1$ bzw. $(z_i, n_2) = 1$ und folglich $(z_i, n_1 n_2) = 1$ für $i = 1, \ldots, s$. Damit ist das Lemma bewiesen.

4. Beweis des Theorems

Es sei $\bar{a} \in R_n^+$ mit $o(\bar{a}) = t$. Aufgrund von (2) ist $n/t = (a, n)$ bei $a \in \bar{a}$. Zur Bestimmung von $\mu_n(a)$ für ein $a \in \mathbb{Z}$ sollen jetzt die Fälle «$t \leqq n$, $n \equiv 0, 1 \pmod 2$, $(a, n) \equiv 0, 1 \pmod 2$» untersucht werden.

4.1. Sei $t = n$. Dann ist $(a, n) = 1$ und damit $\mu_n(a) = 1$.

4.2. Sei $t < n$ *und* $n \equiv 1 \pmod 2$. Wegen $t < n$ ist $\mu_n(a) \geqq 2$. Für Primzahlen $p > 2$ ist $a \not\equiv -1 \pmod p$ oder $a \not\equiv 1 \pmod p$ und folglich $a \equiv (a+1) - 1 \pmod{p^\alpha}$ oder $a \equiv (a-1) + 1 \pmod{p^\alpha}$ eine zulässige Darstellung von a. Wegen $n \equiv 1 \pmod 2$ enthält die Primzahlpotenzzerlegung von n nur Primzahlen $p > 2$. Durch wiederholte Anwendung des Lemmas gewinnt man damit eine zulässige Darstellung $a \equiv b_1 + b_2 \pmod n$ von a, so daß $\mu_n(a) \leqq 2$ und daher $\mu_n(a) = 2$.

4.3. Sei $t < n$, $n \equiv 0 \pmod 2$ *und* $(a, n) \equiv 0 \pmod 2$. Wegen $t < n$ ist $\mu_n(a) \geqq 2$. Für Primzahlen $p > 2$ ist $a \equiv (a+1) - 1 \pmod{p^\alpha}$ oder $a \equiv (a-1) + 1 \pmod{p^\alpha}$ eine zulässige Darstellung von a. Aus $(a, n) \equiv 0 \pmod 2$ folgt $a \equiv 0 \pmod 2$. Damit ist aber $a \equiv (a-1) + 1 \pmod{2^\beta}$ eine zulässige Darstellung von a. Unter Verwendung des Lemmas erhält man somit eine zulässige Darstellung $a \equiv b_1 + b_2 \pmod n$, so daß $\mu_n(a) \leqq 2$ und damit $\mu_n(a) = 2$.

4.4. Sei $t < n$, $n \equiv 0 \pmod 2$ *und* $(a, n) \equiv 1 \pmod 2$. Wegen $n \equiv 0 \pmod 2$ und $(a, n) \equiv 1 \pmod 2$ hat man $a \equiv 1 \pmod 2$. Für ein $b \in \mathbb{Z}$ folgt aus $(b, n) = 1$ ebenso $b \equiv 1 \pmod 2$. Eine mögliche zulässige Darstellung $a \equiv b_1 + b_2 \pmod n$ von a würde also auf den Widerspruch $1 \equiv 1 + 1 \pmod 2$ führen. Wegen $\mu_n(a) \geqq 2$ (da $t < n$) ist somit $\mu_n(a) \geqq 3$.
Für Primzahlen $p > 2$ ist $a \not\equiv -2 \pmod p$ oder $a \not\equiv 2 \pmod p$ und folglich $a \equiv (a + 2) - 1 - 1 \pmod{p^\alpha}$ oder $a \equiv (a - 2) + 1 + 1 \pmod{p^\alpha}$ eine zulässige Darstellung von a. Und wegen $a \equiv 1 \pmod 2$ ist $a \equiv (a - 2) + 1 + 1 \pmod{2^\beta}$ ein zulässige Darstellung von a. Unter Heranziehung des Lemmas erhält man somit eine zulässige Darstellung $a \equiv b_1 + b_2 + b_3 \pmod n$ von a, so daß $\mu_n(a) \leqq 3$ und folglich $\mu_n(a) = 3$.
Damit sind alle Fälle «$t \leqq n$, $n \equiv 0, 1 \pmod 2$, $(a, n) \equiv 0, 1 \pmod 2$» abgehandelt. Das Theorem ist bewiesen.

H. Bergmann, Hamburg

ANMERKUNGEN

[1*] Für $n \in \mathbb{N}$ ist $\varphi(n)$ die Eulersche Funktion.
[2*] Die Frage ist offensichtlich nur für endliche zyklische Gruppen interessant.
[3*] Dabei bedeutet $a \in \bar{a}$, daß $a \in \mathbb{Z}$ ein Repräsentant (Element) der Restklasse $\bar{a} \in R_n^+$ ist.
[4*] Eine Modifizierung des chinesischen Restklassensatzes.

 0013-6018/90/010019-03$1.50 + 0.20/0

Didaktik und Elementarmathematik

An integral recurrence for sums of powers

Every first year calculus student encounters formulas for the sums of powers of the integers. In this note, we present an elementary proof of the curious fact that the formula for the sum of the $(k + 1)$st powers can be obtained simply from the integral of the formula for the sum of the kth powers. This integral recurrence provides an easy means for computing these formulas.
We note first that if a function $F : [0, \infty) \to \mathbb{R}$ satisfies

$$\left.\begin{array}{ll} \text{(i)} & F(0) = 0 \quad \text{and} \\ \text{(ii)} & F(x + 1) = F(x) + (x + 1)^\alpha \end{array}\right\} \quad (*)$$

for some $\alpha \in \mathbb{R}$, then it follows at once that

$$F(n) = \sum_{j=1}^{n} j^\alpha$$

for every positive integer n.
We next prove the following