Quadratsummen in Restklassenringen

Autor(en): **Wegmann, H.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **38 (1983)**

Heft 2

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-37182

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Quadratsummen in Restklassenringen

In der Arbeit [1] hat kürzlich Laugwitz das folgende Problem behandelt und im wesentlichen gelöst: Sei $\mathbf{Z}$ der Ring der ganzen Zahlen, sei $m \geqq 2$ eine ganze Zahl und $\mathbf{Z}_m$ der Restklassenring modulo m. Jedes Element $k \in \mathbf{Z}_m$ besitzt eine Darstellung

$$k \equiv x_1^2 + \cdots + x_s^2 (\mathrm{mod}\, m)$$

als Summe von Quadraten aus $\mathbf{Z}_m$. Bestimme die kleinste Zahl $s = s(k,m)$, mit der eine solche Darstellung möglich ist. Laugwitz [1] hat die Werte dieser Funktion $s(k,m)$ für fast alle Argumente k und m bestimmt. Er verwendete dabei die bekannten Sätze über die Darstellung ganzer Zahlen als Summe von Quadraten und den Satz von Dirichlet. Da es sich um ein Problem über Restklassenringe handelt, sollte es möglich sein, die Eigenschaften der Funktion $s(k,m)$ allein aus den Struktureigenschaften dieser endlichen Ringe zu erhalten. Ziel dieser Arbeit ist es, dies durchzuführen. Dabei lassen sich die wenigen in der Arbeit von Laugwitz offengebliebenen Fragen mit lösen.

1. Ergebnisse

Satz 1. $s(k,m) = \max\limits_{p^a \| m} s(k,p^a)$.

Satz 2. *Sei* $p > 2, 0 < k < p^a$ *und* $k = p^{2b} k'$ *mit* $p^2 \nmid k'$.

Dann ist

$$s(k,p^a) = \begin{cases} 1 & \text{falls } k' \text{ qu. Rest mod } p \\ 2 & \text{falls } k' \text{ qu. Nichtrest mod } p \\ 2 & \text{falls } p \mid k' \text{ und } p \equiv 1 \pmod 4 \\ 3 & \text{falls } p \mid k' \text{ und } p \equiv 3 \pmod 4 \end{cases}$$

Satz 3. *Sei* $0 < k < 2^a$ *und* $k = 4^b k'$ *mit* $4 \nmid k'$.

Dann ist $s(k,2) = 1, s(k,4) = k$ und

$$s(k,2^a) = \begin{cases} 1 \\ 2 \\ 3 \\ 4 \end{cases} \quad \text{für} \quad k' \equiv \begin{matrix} 1 \\ 2 \\ 3 \\ 7 \end{matrix} \quad \begin{matrix} \\ \text{oder} \\ \text{oder} \\ \\ \end{matrix} \quad \begin{matrix} \\ 5 \\ 6 \\ \\ \end{matrix} \quad (\mathrm{mod}\, 8)$$

2. Hilfsmittel aus der Zahlentheorie

A. Die Gruppe der primen Restklassen mod p ist zyklisch mit der Ordnung $p-1$. Die Quadrate bilden eine Untergruppe der Ordnung $(p-1)/2$.

B. Der Rest -1 ist qu. Rest mod p, falls $p \equiv 1 \pmod 4$ und qu. Nichtrest, falls $p \equiv 3 \pmod 4$.
C. Sei $p > 2$. Ist u mit $(u,p) = 1$ ein qu. Rest mod p, so auch mod p^a für alle $a \geq 1$.
D. Die Gruppe der primen Restklassen mod $2^a (a \geq 3)$ besteht aus den Resten $\pm 5^i, i = 1, \ldots, 2^{a-2}$. Die Quadrate sind die Reste $5^{2i}, i = 1, \ldots, 2^{a-3}$, also die Reste $\equiv 1 \pmod 8$.
E. Der Restklassenring mod $m = p_1^{a_1} \ldots p_r^{a_r}$ ist isomorph zum direkten Produkt der Restklassenringe mod $p_i^{a_i}$, $i = 1, \ldots, r$.

3. Beweise

Satz 1 ist eine Folgerung aus dem chinesischen Restklassensatz E.
Für Details verweisen wir auf den Hilfssatz von Laugwitz [1].
Die Beweise der Sätze 2 und 3 erfolgen in mehreren Schritten.

Hilfssatz 1

$$s(k,p^a) \geqq s(k,p^b) \quad \text{für} \quad a \geq b \tag{1}$$
$$s(p^2 k, p^a) \leq s(k, p^{a-2}) \quad \text{für} \quad a > 2. \tag{2}$$

Beweis trivial.

Hilfssatz 2

$$s(k,p) = \begin{cases} 1 \\ 2 \end{cases} \quad \text{falls} \quad k = \begin{matrix} 0 \text{ oder qu. Rest} \\ \text{qu. Nichtrest} \end{matrix} \tag{3}$$

$$s(k,8) = \begin{cases} 1 \\ 2 \\ 3 \\ 4 \end{cases} \quad \text{falls} \quad k \equiv \begin{matrix} 1 \\ 2 \quad \text{oder} \quad 5 \\ 3 \quad \text{oder} \quad 6 \\ 7 \end{matrix} \pmod 8 \tag{4}$$

Beweis von (3): Sei k qu. Nichtrest. Unter den $(p+1)/2$ verschiedenen Resten

$$k, k-1^2, k-2^2, \ldots, k-[(p-1)/2]^2$$

muss ein qu. Rest sein.
(4) lässt sich direkt nachrechnen.

Beweis von Satz 2 für $p^2 \nmid k$:
Wegen Hilfssatz 2 darf man $a \geq 2$ annehmen.
Ist k qu. Rest mod p, so folgt $s(k,p^a) = 1$ aus C.
Ist k qu. Nichtrest mod p, so ist $s(k,p^a) \geq 2$ wegen (1).
Sei $x_1^2 + x_2^2 \equiv k \pmod p$. Dann ist $k - x_2^2$ qu. Rest mod p, also ist auch $x_1^2 \equiv k - x_2^2 \pmod{p^a}$ lösbar (wegen C).

Ist $p \mid k$ aber $p^2 \nmid k$, so folgt aus

$$x_1^2 + x_2^2 \equiv k \pmod{p^a}, \tag{5}$$

dass die Reste x_1 und x_2 nicht durch p teilbar sind.
Im Falle $p \equiv 1 \pmod 4$ ist (wegen $k \equiv 0 \pmod p$)

$$x_2^2 \equiv k - 1^2 \pmod p$$

lösbar. Also ist $k-1$ auch qu. Rest mod p^a, und man erhält $s(k, p^a) = 2$.
Im Falle $p \equiv 3 \pmod 4$ ist

$$x_1^2 + x_2^2 \equiv 0 \pmod p$$

nicht lösbar mit $x_1 \not\equiv 0 \pmod p$ (wegen B) aber dafür wegen (3)

$$x_2^2 + x_3^2 \equiv k - 1^2 \pmod p.$$

Also ist $k - 1^2 - x_2^2$ ein qu. Rest mod p und damit auch mod p^a.

Beweis von Satz 3 für $4 \nmid k$: Sei $a \geq 3$.
Aus D folgt $s(k, 2^a) = 1$ für $k \equiv 1 \pmod 8$ und aus Hilfssatz 2 und (1) die Ungleichungen

$$s(k, 2^a) \geq 2, \geq 3, \geq 4 \quad \text{für} \quad k \equiv 2 \quad \text{oder} \quad 5, 3 \quad \text{oder} \quad 6, 7 \bmod 8.$$

Für $k \equiv 2$ oder 5 ist $k - 1^2$ bzw. $k - 2^2 \equiv 1 \pmod 8$ also ein Quadrat. Daraus folgt $s(k, 2^a) = 2$.
Für $k \equiv 3$ oder 6 ist $k - 1^2 - 1^2$ bzw. $k - 1^2 - 2^2 \equiv 1 \pmod 8$. Daraus folgt $s(k, 2^a) = 3$.
Schliesslich ist für $k \equiv 7 \pmod 8$ der Rest $k - 1^2 - 1^2 - 2^2 \equiv 1 \pmod 8$. Also ist $s(k, p^a) = 4$.

Beweis der Sätze 2 und 3 für $p^2 \mid k$
Die Behauptung folgt direkt aus (2) und

Hilfssatz 3. *Für $a > 2$ ist $s(p^2 k, p^a) \geq s(k, p^{a-2})$.*

Beweis: Aus (2) und dem bewiesenen Teil der Sätze 2 und 3 folgt

$$s(k, p^a) \leq \begin{cases} 2 & p \equiv 1 \pmod 4 \\ 3 \quad \text{für} & p \equiv 3 \pmod 4 \\ 4 & p \equiv 2 \end{cases}$$

Sei $s(k, p^{a-2}) = s$, $s(p^2 k, p^a) = t$ und

$$x_1^2 + \cdots + x_t^2 \equiv p^2 k \pmod{p^a}. \tag{6}$$

Dann ist

$$x_1^2+\cdots+x_t^2\equiv 0 \pmod{p^2}.$$

Ist $p\equiv 1 \pmod 4$ und $t=2$, so ist wegen $s\leq 2$ sicher $s\leq t$.
Ist aber $t=1$, so folgt $p\mid x_1$ und aus (6) $(x_1/p)^2\equiv k \pmod{p^{a-2}}$.
Ist $p\equiv 3 \pmod 4$, so ist nur im Falle $t\leq 2$ etwas zu beweisen.
Wegen B hat aber $x_1^2+x_2^2\equiv 0 \pmod p$ nur Lösungen x_1, x_2 mit $x_1, x_2\equiv 0 \pmod p$.
Also folgt aus (6)

$$(x_1/p)^2+(x_2/p)^2\equiv k \pmod{p^{a-2}}.$$

Ist $p=2$, so ist nur im Falle $t\leq 3$ etwas zu beweisen.
Die Kongruenz $x_1^2+x_2^2+x_3^2\equiv 0 \pmod 4$ hat nur Lösungen x_1, x_2, x_3 mit $x_1, x_2, x_3\equiv 0 \pmod 2$.
Also folgt aus (6)

$$(x_1/2)^2+\cdots+(x_t/2)^2\equiv k \pmod{2^{a-2}}$$

und daraus $s(k, 2^{a-2})\leq t$.

H. Wegmann, TH Darmstadt

LITERATURVERZEICHNIS

1 D. Laugwitz: Quadratsummen in Restklassenringen. El. Math. *35*, 73–79 (1980).

© 1983 Birkhäuser Verlag, Basel 0013-6018/83/020036-04$1.50+0.20/0

Sätze vom Holditch-Typ für ebene Kurven

Herrn Prof. Dr. H. R. Müller zum 70. Geburtstag gewidmet

Werden in der euklidischen Ebene die Endpunkte X und X^* einer Strecke s von *konstanter Länge* C entlang einer Eilinie k bewegt, so erzeugt ein *fester Punkt* $\bar{X}\in s$ eine i. a. nichtkonvexe Kurve $\bar{k}$. Der *Flächeninhalt* des Bereiches zwischen k und $\bar{k}$ hängt nach einem Satz von Holditch nicht von der Gestalt der Kurve k ab, sondern nur von der Lage des Punktes $\bar{X}$ auf s [8]. Ausführlichere Untersuchungen damit zusammenhängender Fragen und Präzisierungen der klassischen Formulierung sind bei A. Broman [3, 4] zu finden. Ein etwas allgemeineres Ergebnis erhalten wir, wenn sich die Endpunkte der Strecke s entlang zweier verschiedener Kurven k und k^* bewegen [2]. H. R. Müller hat diese Resultate u. a. auf ein in gewissem Sinne *«duales»* Gegenstück zur klassischen Holditch-Bewegung übertragen [9]. Er unter-