Quadratische Reste

Martin Welk, Leipzig

Bei der Lösung einer ganzen Reihe zahlentheoretischer Probleme ist von Nutzen, dass eine ungerade Quadratzahl bei Division durch 4 nur den Rest 1 lassen kann. Eine Verschärfung dieser wohl allgemein bekannten Aussage ist, dass eine ungerade Quadratzahl sogar bei Division durch 8 nur den Rest 1 lassen kann. Wenn wir die Beschränkung auf ungerade Zahlen fallen lassen, kann eine Quadratzahl bei Division durch 8 also nur den Rest 0, 1 oder 4 lassen.

Wir wollen uns hier eine allgemeinere Frage stellen:

> **Wie kann man bei einem gegebenen Divisor m und gegebenen Rest r bestimmen, ob es eine Quadratzahl gibt, die bei Division durch m den Rest r lässt?**

Für ungerade Primzahlen als Divisoren gilt der folgende Satz, dessen Beweis dem Leser bzw. der Leserin überlassen sei. (Weiter unten folgt noch ein Hinweis dazu.)

Satz 1 *Ist p eine ungerade Primzahl, so gibt es genau $\frac{p-1}{2}$ Reste, die als Reste von zu p teilerfremden Quadratzahlen bei Division durch p auftreten.*

Beispielsweise sind dies die Reste[1] 1 modulo 3; 1 und 4 modulo 5; 1, 2 und 4 modulo 7.

Solche Reste bezeichnet man als quadratische Reste.

Selbstverständlich gibt es auch durch p teilbare Quadratzahlen; wir wollen daher auch 0 als quadratischen Rest modulo p bezeichnen (in manchen Büchern wird ein anderer Sprachgebrauch gewählt und 0 nicht als quadratischer Rest angesehen). Im allgemeinen ist es schwer, einem Rest modulo p „anzusehen", ob es sich um einen quadratischen Rest handelt. Auf jeden Fall kann man aber alle quadratischen Reste modulo p auflisten, indem man 0^2, 1^2, ..., $\left(\frac{p-1}{2}\right)^2$ modulo p berechnet *(warum?)*.

Hinweis zum Beweis von Satz 1: Man zeige, dass für zwei ganze Zahlen a und b die Reste von a^2 und b^2 bei Division durch p dann und nur dann übereinstimmen, wenn $a+b$ oder $a-b$ durch p teilbar ist.

Für die Gesamtmenge der quadratischen Reste bei Division durch eine ungerade Primzahl können wir noch eine weitere Aussage machen, deren Beweis (mit Hilfe des Satzes von Wilson) die Leserin oder der Leser ebenfalls selbst finden kann.

Satz 2 *Ist p eine ungerade Primzahl und r ein von 0 verschiedener quadratischer Rest modulo p, so ist $-r$ dann und nur dann ebenfalls quadratischer Rest, wenn p bei Division durch 4 den Rest 1 lässt.*

---

[0] Beitrag für das Heft zum Landesseminar Sachsen, März 1999

[1] Die Bezeichnung „Rest k modulo m" ist nur ein kürzerer Ausdruck für „Rest k bei Division durch m". Wir legen uns hier nicht auf bestimmte Repräsentanten für Reste modulo m, etwa $0, \dots, m-1$, fest, sondern lassen zu, dass eine Restklasse durch eine beliebige ihr angehörende Zahl bezeichnet wird. Mit „dem Rest 7 modulo 3" ist also dieselbe Restklasse wie mit „dem Rest 1 modulo 3" gemeint.

Wir wenden uns nun dem nächst allgemeineren Fall zu, nämlich quadratischen Resten modulo p^k, wobei p wieder eine ungerade Primzahl und $k \geq 1$ eine natürliche Zahl ist.

Damit r ein quadratischer Rest modulo p^k sein kann, d. h. damit es eine Quadratzahl gibt, die bei Division durch p^k den Rest r lässt, muss r sicher auch quadratischer Rest modulo p sein. Ein verblüffendes Ergebnis ist, dass diese notwendige Bedingung auch schon hinreichend ist, sofern r nicht durch p teilbar ist.

Satz 3 *Ist p eine ungerade Primzahl, $k \geq 1$ eine natürliche Zahl und r ein nicht durch p teilbarer Rest modulo p^k, so ist r quadratischer Rest modulo p^k dann und nur dann, wenn r quadratischer Rest modulo p ist.*

BEWEIS : Die Notwendigkeit der Bedingung ist unmittelbar einzusehen. Die Hinlänglichkeit der Bedingung zeigen wir durch vollständige Induktion. Der Induktionsanfang ($k = 1$) ist klar, denn hier ist $p^k = p$.

Es sei nun $k \geq 1$ und r ein nicht durch p teilbarer Rest modulo p^{k+1}, der quadratischer Rest modulo p^k ist. Zur Ausführung des Induktionsschritts ist nun zu zeigen, dass r auch quadratischer Rest modulo p^{k+1} ist. Nach Induktionsvoraussetzung gibt es eine ganze Zahl a_k, für die

$$a_k^2 = r + b \cdot p^k \tag{1}$$

mit einer weiteren ganzen Zahl b gilt. Eine der Zahlen b und $b+p$ ist gerade; wir setzen daher $c := \dfrac{b}{2}$ bzw. $c := \dfrac{b+p}{2}$ je nachdem, welche dieser Zahlen ganz ist. Dann haben $b \cdot p^k$ und $2c \cdot p^k$ denselben Rest bei Division durch p^{k+1}, also gilt

$$a_k^2 = 2c \cdot p^k + r + s \cdot p^{k+1}$$

und mit der quadratischen Ergänzung $(c \cdot p^k)^2 = c^2 p^{k-1} \cdot p^{k+1}$

$$(a_k - c \cdot p^k)^2 = r + (s + c^2 p^{k-1}) \cdot p^{k+1}.$$

Aus der letzten Gleichung ergibt sich unmittelbar, dass das Quadrat der ganzen Zahl $a_{k+1} := a_k - c \cdot p^k$ bei Division durch p^{k+1} den Rest r lässt. Dieser ist damit quadratischer Rest modulo p^{k+1}, womit die Induktionsbehauptung gezeigt ist. QED

Wir haben hier die durch p teilbaren Reste modulo p^k zunächst von der Betrachtung ausgeschlossen. Es bereitet aber keine Schwierigkeiten, auch für diesen Fall eine geeignete Bedingung anzugeben. Wir machen dabei davon Gebrauch, dass sich jede durch p^l teilbare ganze Zahl, die nicht durch p^{l+1} teilbar ist, als $a \cdot p^l$ mit einer nicht durch p teilbaren ganzen Zahl a schreiben lässt; dabei bestimmt der Rest von $a \cdot p^l$ modulo p^k ($k > l$) eindeutig den Rest von a modulo p^{k-l} und umgekehrt.

In diesem Satz ist die Bedingung, dass p ungerade sein soll, nicht erforderlich.

Satz 4 *Es sei p eine Primzahl, k und l natürliche Zahlen mit $k > l \geq 1$ sowie $r \cdot p^l$ ein durch p^l, nicht aber durch p^{l+1} teilbarer Rest modulo p^k. Dann ist $r \cdot p^l$ quadratischer Rest modulo p^k dann und nur dann, wenn l gerade und r quadratischer Rest modulo p^{k-l} ist.*

BEWEIS : Ist a eine ganze Zahl mit $a^2 = r \cdot p^l + s \cdot p^k = (r + s \cdot p^{k-l}) \cdot p^l$, so muss a selbst durch p teilbar sein, d. h. es ist $a = a' \cdot p^t$ mit einer nicht durch p teilbaren ganzen Zahl a' und einer natürlichen Zahl $t \geq 1$. Damit ist $a^2 = {a'}^2 \cdot p^{2t}$ und ${a'}^2$ wiederum nicht durch p

teilbar. Da $r + s \cdot p^{k-l}$ zu p teilerfremd ist, ist $p^l = p^{2t}$ sowie $a'^2 = r + s \cdot p^{k-l}$. Aus der ersten Gleichung folgt, dass l gerade ist, aus der zweiten, dass a'^2 modulo p^{k-l} den Rest r besitzen muss, der damit quadratischer Rest sein muss.

Ist umgekehrt r quadratischer Rest modulo p^{k-l} und l gerade, so gibt es ganze Zahlen a', s mit $a'^2 = r + s \cdot p^{k-l}$. Mit der natürlichen Zahl $t := \frac{l}{2}$ gilt dann $(a' \cdot p^t)^2 = p^l \cdot (r + s \cdot p^{k-l}) = r \cdot p^l + s \cdot p^k$, also ist $r \cdot p^l$ quadratischer Rest modulo p^k. QED

Damit kann die eingangs aufgeworfene Frage für alle diejenigen Divisoren beantwortet werden, die Potenzen von Primzahlen sind – außer für die Potenzen der 2.

Der Rest 1 bei Division durch 2 ist offensichtlich quadratischer Rest; 3 besitzt bei Division durch 2 denselben Rest. Trotzdem ist zwar 1, nicht aber 3 quadratischer Rest modulo 4. Und wiederum ist von den beiden Resten 1 und 5 modulo 8, denen beiden derselbe Rest, 1, bei Division durch 4 entspricht, nur 1 quadratischer Rest modulo 8. Es hat danach den Anschein, dass sich die Eigenschaft eines Restes, quadratischer Rest zu sein, nicht so einfach vom Divisor 2^k auf 2^{k+1} „vererbt“ wie von p^k auf p^{k+1} für ungerade Primzahlen p.

Es stellt sich aber heraus, dass der Induktionsschritt aus dem Beweis von Satz 3 für $k \geq 3$ wieder funktioniert, so dass wir auch für Zweierpotenzen als Divisoren eine allgemeine Aussage beweisen können.

Satz 5 *Ist $k \geq 3$ eine natürliche Zahl und r ein ungerader Rest modulo 2^k, so ist r quadratischer Rest modulo 2^k dann und nur dann, wenn r den Rest 1 bei Division durch 8 besitzt.*

Beweis : Dass r nur dann quadratischer Rest sein kann, wenn sein Rest modulo 8 der Rest 1 ist, ist offensichtlich. Dass dies hinreichend ist, wird wieder durch vollständige Induktion gezeigt, wobei für den Induktionsanfang mit $k = 3$ wegen $2^3 = 8$ ebenfalls nichts zu beweisen ist.

Für den Induktionsschritt sei $k \geq 3$, r ungerade und r quadratischer Rest modulo 2^k. Wir wollen zeigen, dass r auch quadratischer Rest modulo 2^{k+1} ist.

Nach Induktionsvoraussetzung gibt es ganze Zahlen a und b mit

$$a^2 = r + b \cdot 2^k. \tag{2}$$

Wir stellen b in der Form $b = 2t + c$ mit einer ganzen Zahl t und $c = 0$ oder $c = 1$ dar; dann ist

$$a^2 = r + 2c \cdot 2^{k-1} + t \cdot 2^{k+1}$$

und unter Benutzung der quadratischen Ergänzung $\left(c \cdot 2^{k-1}\right)^2 = c^2 2^{k-3} \cdot 2^{k+1}$

$$(a - c \cdot 2^{k-1}) = r + (t + c^2 2^{k-3}) \cdot 2^{k+1}.$$

In der letzten Gleichung sehen wir, warum der Schluss erst für $k \geq 3$ funktioniert: denn nur wenn 2^{k-3} eine ganze Zahl ist, folgt daraus, dass r quadratischer Rest modulo 2^{k+1} ist. Damit ist aber die Induktionsbehauptung gezeigt. QED

Nun kann die Frage, ob ein gegebener Rest r quadratischer Rest bei Division durch einen gegebenen Divisor m ist, allgemein beantwortet werden. Dazu benötigen wir neben der Primfaktorzerlegung von m lediglich den sogenannten Chinesischen Restklassensatz, den wir ohne Beweis zitieren wollen.

Satz 6 (Chinesischer Restklassensatz) *Es seien $m_1, m_2, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen. Zu jeder dieser Zahlen m_i sei eine Restklasse r_i gegeben. Dann bestimmen die Reste r_i modulo m_i eindeutig eine Restklasse r modulo $m := m_1 \cdot m_2 \cdot \ldots \cdot m_n$, für die gilt: Alle ganzen Zahlen, die den Rest r modulo m lassen, und nur diese, lassen bei Division durch jedes einzelne m_i den zugehörigen Rest r_i.*

Unmittelbar einleuchtend ist, dass r höchstens dann quadratischer Rest modulo m sein kann, wenn r quadratischer Rest bezüglich jeder in der Primfaktorzerlegung von m auftretenden Primzahlpotenz ist. Diese Bedingung kann mit den Sätzen 3, 4 und 5 überprüft werden. Dass dies bereits eine ausreichende Bedingung darstellt, geht aus dem folgenden Satz hervor, den der Leser oder die Leserin mit Hilfe des Chinesischen Restklassensatzes beweisen kann.

Satz 7 *Es sei m eine natürliche Zahl und r ein gegebener Rest modulo m. Dann ist r dann und nur dann quadratischer Rest modulo m, wenn r quadratischer Rest modulo jeder in der Primfaktorzerlegung von m auftretenden Primzahlpotenz ist.*

Aufgaben:

1. Man zeige, dass es nicht möglich ist, in eine Tabelle aus $n \times n$ Feldern ungerade Quadratzahlen derart einzutragen, dass ihre Summe 1999 beträgt.
2. Man überprüfe durch direkte Berechnung der quadratischen Reste modulo 25 und modulo 27 die Behauptungen der Sätze 3 und 4 für diesen Fall.
3. Man zeige, dass 19 quadratischer Rest modulo 243 ist, und finde eine ganze Zahl, deren Quadrat den Rest 19 bei Division durch 243 lässt.
4. Welches ist die kleinste natürliche Zahl, die durch 37 und 3 teilbar ist und bei Division durch 19 den Rest 3 lässt?
5. Man zeige, dass 1999 quadratischer Rest modulo 12321 ist.
6. Für welche ganzen Zahlen z ist $z^2 - 4z + 3$ durch 11 teilbar?

   Für welche ganzen Zahlen z ist $z^2 - 4z + 3$ durch 120 teilbar?