Die Anzahl der Quadratsummendarstellungen

F.J. Király, L.H. Brewis

In diesem Abschnitt werden wir eine explizite Summe für die Anzahl der Quadratsummendarstellungen einer beliebigen ganzen Zahl herleiten.

0.1 Definition. Sei m eine ganze Zahl. Eine Quadratsummendarstellung von m ist eine Gleichung

$$a^2 + b^2 = m,$$

parametrisiert durch das geordnete Dupel $(a, b) \in \mathbb{Z}^2$. Dann bezeichnen wir mit $S^{\pm}(m)$ die Anzahl unterschiedlicher Quadratsummendarstellungen von m.

Die Darstellungen werden also durch $a, b \in \mathbb{Z}$ parametrisiert. Man sieht leicht, dass man oBdA die Quadratsummendarstellungen $a \geq b \geq 0$ betrachten kann:

0.2 Lemma. *Sei $S(m)$ die Anzahl Quadratsummendarstellungen*

$$a^2 + b^2 = m \text{ mit } a \geq b \geq 0.$$

Ist $\frac{m}{2}$ ganz und ein Quadrat, so ist $S^{\pm}(m) = 8S(m) - 4$. Ansonsten ist $S^{\pm}(m) = 8S(m)$.

Beweis: Man sieht, dass falls $a \neq \pm b$ eine Darstellung von m induziert, induzieren $\pm a$ und $\pm b$ sieben andere, paarweise verschiedene Darstellungen, die man erhält, indem man a und b vertauscht oder das Vorzeichen wechselt. Von den insgesamt acht so erhaltenen Darstellungen gilt offensichtlich für genau eine $a \geq b \geq 0$. Falls $a = \pm b$, so hat man nur vier verschiedene Darstellungen aus $\pm a$ und $\pm b$, von denen genau eine $a \geq b \geq 0$ erfüllt. □.

0.3 Beispiel. Beispielsweise ist $S(65) = 2$. Es gilt $8^2 + 1^2 = 7^2 + 4^2 = 65$, und durch Probieren sieht man, dass das die einzigen Quadratsummendarstellungen sind. Man kann nun vermuten, dass das irgendwie mit den Primfaktoren von 65 zusammenhängt.

Ein Satz aus der Vorlesung impliziert die folgende Aussage:

0.4 Lemma. *Falls p prim ist, so ist $S(p) = 0$, falls $p \equiv 3 \mod 4$ und $S(p) = 1$ sonst.*

Beweis: In der Vorlesung wurde bewiesen, dass p genau dann eine eindeutige Darstellung als Quadratsumme besitzt, falls $p \equiv 1 \mod 4$ ist oder $p = 2$. Daraus folgt die Behauptung. □

0.5 Bemerkung. Es wird sich als günstig erweisen, parallel zur klassischen Betrachtungsweise auch im Auge zu behalten, was im Ring der Gaußschen Zahlen passiert (also der komplexen Zahlen mit ganzen Koeffizienten). Viele Theoreme folgen wesentlich leichter aus der Tatsache, dass dieser Ring faktoriell ist, d.h. das die Primfaktorzerlegung in den Gaußschen Zahlen eindeutig ist (für beliebige Ringe muss das nicht gelten).

Das zentrale Lemma, dass man für weitere Betrachtungen braucht, ist folgendes:

0.6 Lemma. *Für Zahlen a, b, c, d gilt die Identität*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2.$$

Beweis: Durch elementares Nachrechnen. □.

0.7 Bemerkung. In den Gaußschen Zahlen hat dieses Lemma einen tieferen Sinn. Man kann zeigen, dass eine ganze Zahl m genau dann Summe zweier Quadrate ist, wenn es gaußsche Zahlen $z = x + yi$ und $\overline{z} = x - yi$ gibt mit

$$(x + yi)(x - yi) = z\overline{z} = m.$$

Das Lemma läuft dann nur auf eine Umordnung der Primfaktoren hinaus, sodass die Zahl dargestellt wird als Produkt zweier zueinander konjugierter Gaußscher Zahlen:

$$(a^2 + b^2)(c^2 + d^2) = (a + bi)(a - bi)(c + di)(c - di) = (a + bi)(c - di)(a - bi)(c + di)$$

$$= ((ac + bd) + (bc - ad)i)((ac + bd) - (bc - ad)i) = (ac + bd)^2 + (bc - ad)^2.$$

Man sieht außerdem, dass man im Lemma im Allgemeinen zwei voneinander verschiedene Möglichkeiten hat, die Zahlen zu verknüpfen. Sind a, c und b, d jeweils paarweise verschieden, so kann man a und b vertauschen und erhält eine andere Quadratsummendarstellung. Das spiegelt sich in der Faktorzerlegung bei den Gaußschen Zahlen wider.

Wir beweisen jetzt das folgende Lemma:

0.8 Lemma. *Sind p, q verschiedene Primzahlen mit $p \equiv q \equiv 1 \mod 4$, so ist $S(pq) = 2$. Allgemeiner ist für N paarweise verschiedene Primzahlen p_i*

$$S\left(\prod_{i=1}^{N} p_i\right) = 2^{N-1}.$$

Beweis: Durch wiederholte Anwendung der Identität in Lemma 0.6. Laut der vorhergehenden Bemerkung hat man mindestens zwei Möglichkeiten, eine Quadratsummendarstellung von $\prod_{i=1}^{n} p_i$ und eine von p_{n+1} zu einer Quadratsummendarstellung von $\prod_{i=1}^{n+1} p_i$ zu kombinieren. Dies sind tatsächlich auch höchstens und damit gemau zwei, da der Fermat-Abstieg nach dem Schubfachprinzip zwei verschiedene Summendarstellungen für ein p_i liefern würde, was nach Lemma 0.4 nicht sein kann. Also ist

$$S\left(\prod_{i=1}^{n+1} p_i\right) = 2S\left(\prod_{i=1}^{n} p_i\right)$$

und somit folgt per ganzzahliger Induktion die Behauptung. □
In den Gaußschen Zahlen entspricht dieser Satz dem Problem, das Produkt von Primfaktoren in zwei gleich große Mengen zu partitionieren, von denen die eine das Konjugat der Primfaktoren der anderen enthalten muss, um die Quadratsummenbedingung zu erfüllen. Da die Primfaktoren alle verschieden sein müssen (da die p_i verschieden sind und ein Primfaktor bereits die Primzahl, die er teilt, eindeutig bestimmt), ist das äquivalent zum Problem, aus N Säcken mit jeweils 2 voneinander unterscheidbaren Kugeln jeweils eine zu ziehen - eine Kugel entspricht dabei einem der Primfaktoren von p_i, der Sack entspricht der Nummer i. Dabei sollen Ergebnisse gleich sein, wenn die gezogenen Kugeln gleich sind oder die gezogenen Kugeln und die in den Säcken verbliebenen Kugeln gleich sind. Die Anzahl von Möglichkeiten ist aber genau 2^{N-1} - somit folgt die Behauptung direkt □.
Für Primzahlpotenzen muss man hingegen berücksichtigen, dass die Quadratsummendarstellungen alle gleich sind und somit die Zahlen in Lemma 0.6 ebenfalls.

0.9 Lemma. *Ist p eine Primzahl und e eine positive ganze Zahl. Sei $p(x) = 1$ für x gerade und $p(x) = 0$ für x ungerade. Dann ist*

$$S\left(p^e\right) = \left\lceil \frac{e+1}{2} \right\rceil,$$

falls $p \equiv 1 \mod 4$. Ansonsten ist $S\left(p^e\right) = p(e)$, falls $p \equiv 3 \mod 4$, und $S\left(2^e\right) = 1$.

Beweis: Für $p \not\equiv 1 \mod 4$ folgt das aus dem Lemma 0.4 aus der Vorlesung: Für gerade e erhält man einen Widerspruch, indem man durch eine gerade p-Potenz teilt. Dan hat man eine Darstellung für p, was einen Widerspruch zum Lemma führt. Für $p = 2$ sind die Koeffizienten in der Formel 0.6 immer 1 (aus $1^2 + 1^2 = 2$), also bekommt man immer nur entweder die Darstellung $2^e = 0^2 + \left(2^{\frac{e}{2}}\right)^2$ oder $2^e = \left(2^{\frac{e-1}{2}}\right)^2 + \left(2^{\frac{e-1}{2}}\right)^2$.
Der Rest folgt wieder durch Anwendung von Lemma 0.6. Man sieht, dass dadurch, dass die Zahlen a, c und c, d bei der ersten Anwendung paarweise gleich sind, eine zusätzliche Darstellung entsteht. Bei der zweiten Anwendung entsteht keine, da die Darstellungen aufgrund der Symmetrie des Problems gleich sind. Erst bei der dritten Anwendung erhält man wieder eine verschiedene Darstellung, und so weiter - bei jeder zweiten Anwendung bekommt man eine neue Darstellung. Daraus folgt die Behauptung. □
In den Gaußschen Zahlen entspricht das dem Problem, die $2e$ Primfaktoren, von denen es jetzt nur noch zwei Arten gibt, auf gleich große Mengen zu verteilen. Das entspricht dem kombinatorischen Problem, $2N$ Kugeln mit zwei verschiedenen Farben, z.B. schwarz und rot, die jeweils mit Mächtigkeit N vertreten sind, in zwei ununterscheidbare Mengen der Größe N aufzuteilen. Man überlegt sich, dass es genau $\left\lceil \frac{e+1}{2} \right\rceil$ Möglichkeiten gibt, das zu tun. Denn die Aufteilung wird genau durch die Anzahl schwarzer Kugeln in der Menge mit den meisten roten Kugeln bestimmt. □
Nun folgt der etwas schwierigere und nicht so leicht einzuesehende Satz für allgemeines m (eigentlich war die Aufgabe 47d) nur mit quadratfreiem m geplant - das wäre dann Lemma 0.8 gewesen. Dieser Satz enthält allerdings fast alle vorhergehende Lemmata als Korollar.

0.10 Theorem. *Sei m eine ganz Zahl mit der (über $\mathbb{Z}$) eindeutigen Primfaktorzerlegung*

$$m = \prod_{i=1}^{n} p_i^{e_i}.$$

Sei $N \subseteq \{1, \ldots, n\}$ die Teilmenge der Indizes, für die $p_i \equiv 1 \mod 4$. Sei $M \subseteq \{1, \ldots, n\}$ due Teilmenge der Indizes, für die $p_i \equiv 3 \mod 4$. Sei $p(x) = 1$ für x gerade und $p(x) = 0$ für x ungerade. Dann ist

$$S(m) = \prod_{i \in M} p(e_i) \sum_{I \subseteq N} \left\lceil 2^{\#N-1} \right\rceil \prod_{j \notin I} p(e_j) \prod_{j \in I} \left\lfloor \frac{e_j + 1}{2} \right\rfloor.$$

Beweis: Wir zeigen zunächst, dass man auf den Fall reduzieren kann, in dem alle $p_i \equiv 1 \mod 4$ sind. Man kann oBdA 2-er-Potenzen eliminieren, da sie aufgrund von Lemma 0.8 die Anzahl Darstellungen nicht ändern, d.h. $S(m) = S\left(\frac{m}{2}\right)$, falls m gerade ist. Falls in der Faktorisierung von m außerdem eine Primzahl $q \equiv 3 \mod 4$ auftritt, so existiert nach Lemma 0.8 mindestens eine Darstellung genau dann, falls ihr Exponent gerade ist. Ferner gilt in diesem Fall $S(m) = S\left(\frac{m}{q}\right)$, also kann man oBdA annehmen, dass m nur aus Faktoren mit $p_i \equiv 1 \mod 4$ besteht. In diesem Fall ist nur noch zu zeigen:

$$S(m) = \sum_{I \subseteq N} \left\lceil 2^{\#N-1} \right\rceil \prod_{j \notin I} p(e_j) \prod_{j \in I} \left\lfloor \frac{e_j + 1}{2} \right\rfloor.$$

Nach Lemma 0.9 ist $S(p^e) = \left\lceil \frac{e+1}{2} \right\rceil$ für Primzahlen p und ganze e. Wir verwenden Induktion mittels Lemma 0.6 über die teilerfremden Faktoren $p_i^{e_i}$. Die Frage ist: Wieviele Darstellungen hat man für die Produkte der $p_i^{e_i}$? Dazu muss man unterscheiden, ob die e_i gerade sind oder ungerade. Ist e_i ungerade, so erhält man aus der Formel in Lemma 0.9 für jede Darstellung von $p_i^{e_i}$ und von $p_j^{e_j}$ jeweils zwei Darstellungen für $p_i^{e_i} p_j^{e_j}$, da die Koeffizienten verschieden sind. Ist e_i gerade, so bekommt man für alle Darstellungen von $p_i^{e_i}$ bis auf eine zwei von $p_i^{e_i} p_j^{e_j}$, für eine ausgewählte Darstellung jedoch nur eine. Das ist genau die Darstellung, bei der man im Beweis von Lemma 0.9 bei der Anwendung der zentralen Formel aus Lemma 0.6 $\frac{e_i}{2}$-Mal positivies und $\frac{e_i}{2}$-mal negatives Vorzeichen gewählt hat; das entspricht in den Gaußschen Zahlen der Wahl genausovieler roter und schwarzer Kugeln in beiden Mengen (die ihrerseits daher genau gleich sind). Diese zusätzliche Symmetrie führt statt zwei also nur zu einer Darstellung des Produktes. Der Einfachheit halber nennen wir eine solche Darstellung von $p_i^{e_i}$ vom

Symmetrietyp.
Analog muss man unterscheiden, welche Symmetrien im N-fachen Produkt vorhanden sind. Wenn man bemerkt, dass eine Darstellung von m von Produkten von Darstellungen von $p_i^{e_i}$ kommt, so kann man schließen, dass die Anzahl Darstellungen von M, die man erhält, genau $\left\lceil 2^{N-1-n} \right\rceil$ ist, falls genau n der N Darstellungen von den $p_i^{e_i}, 1 = 1 \dots N$ vom Symmetrietyp sind. Damit erhält man die Formel

$$S(m) = \sum_{i=0}^{N} a_i \left\lceil 2^{i-1} \right\rceil \text{ mit } a_i = \sum_{\substack{I \subseteq N \\ \#I = i}} \prod_{j \notin I} p(e_i) \prod_{j \in I} \left\lfloor \frac{e_j + 1}{2} \right\rfloor .$$

In dieser Formel ist die Zweierpotenz die Anzahl generierter Darstellungen von m pro Kombination von Darstellungen der $p_i^{e_i}$, und a_i ist die Anzahl der Kombinationen mit $N - i$ Darstellungen vom Symmetrietyp. Die explizite Formel der a_i folgt daraus, dass es pro $p_i^{e_i}$ höchstens eine Darstellung vom Symmetrietyp gibt, abhängig von der Restklasse $p(e_i) = e_i + 1 \mod 2$ (also ob e_i gerade ist oder nicht). Denn $\left\lfloor \frac{e_i+1}{2} \right\rfloor$ ist gerade die Anzahl der Darstellungen von $p_i^{e_i}$, die nicht vom Symmetrietyp ist.
Nach einigen elementaren Umformungen bekommt man die Formel aus der Behauptung. □

0.11 Korollar. *Sei J die Teilmenge von N, die alle Indizes j enthält, für die e_j gerade ist. Dann gilt*

$$S(m) = 2^{\#J} \prod_{j \in J} \left\lfloor \frac{e_j + 1}{2} \right\rfloor \cdot S\left(\frac{m}{\prod_{j \in J} p_i^{e_i}} \right) .$$

Insbesondere gilt $S(m) \mid S(mr)$, falls r ein Quadrat ist.

0.12 Bemerkung. Man kann nun versuchen, diese Formel für Maple zu programmieren und mit der tatsächlichen Anzahl Quadratsummendarstellungen vergleichen. Nachdem man das Paket numtheory eingebunden hat, bekommt man die Anzahl der Darstellungen von m auf Brute-Force-Weise mittels nops(sum2sqr(m)).
Für den Fall $N = 2$ lautet die Formel aus dem vorhergehenden Satz

$$S(p^e q^f) = \left\lfloor \frac{e+1}{2} \right\rfloor \left\lfloor \frac{f+1}{2} \right\rfloor + \left\lceil \frac{e+1}{2} \right\rceil \left\lceil \frac{f+1}{2} \right\rceil ;$$

Man benutzt dazu einfach die Identität

$$\left\lfloor \frac{e_j + 1}{2} \right\rfloor + p(e_j) = \left\lceil \frac{e_j + 1}{2} \right\rceil .$$