Summen von Quadraten

1. Physikalische Motivation

Eine schwingende Saite hat eine Grundfrequenz F, die von Länge, Dicke, Beschaffenheit der Saite und so fort abhängt. Neben dieser Grundfrequenz gibt es auch noch Obertöne mit der doppelten, dreifachen, vierfachen usw. Frequenz:

$$F_n := n \cdot F.$$

Das Klangspektrum der Saite setzt sich aus diesen Obertönen zusammen, und wie stark die einzelnen Obertöne gewichtet sind, hängt vom Instrument ab und entscheidet über dessen Klang.

Wenn man anstelle der Saite eine quadratische Membran nimmt, in einen festen Rahmen spannt und zum Schwingen bringt, so setzt auch dieser Klang sich aus vielen Einzelfrequenzen zusammen. Hier haben wir Schwingungen in zwei Richtungen zu berücksichtigen, die sich überlagern. Dabei addieren sich die Energien derselben, die jeweils zum Quadrat der Frequenz proportional ist, und das ergibt für die Energie eine Einzelschwingung etwa von der Form

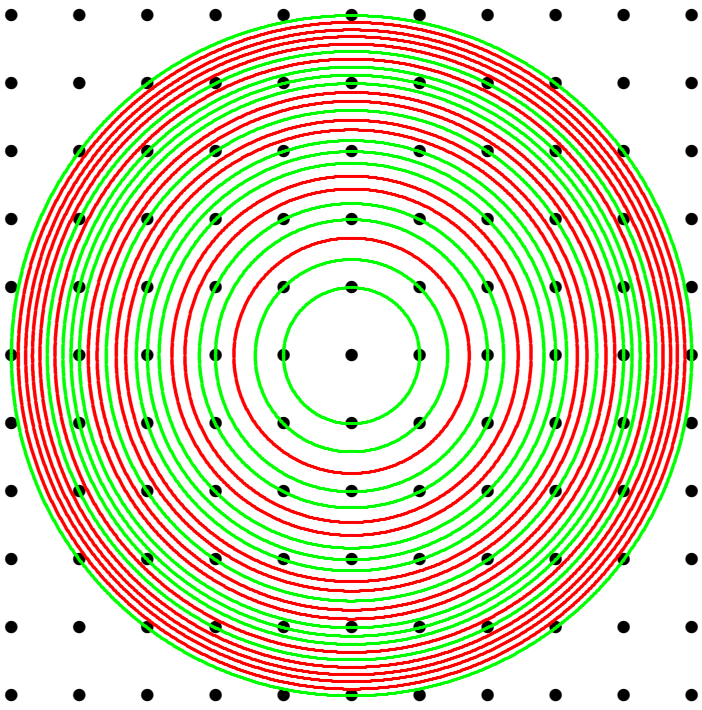
$$E \cdot (n^2 + m^2), \quad m, n \in \mathbb{N}_0.$$

Dabei ist E wieder eine Größe, in der der Grad der Anregung steckt.

Die grundlegenden Bausteine der Schwingung einer quadratischen Membran hängen also von Paaren ganzer Zahlen ab, das ist ein analytisches Phänomen, es gehört zur Fourier-Analysis. Dieses Faktum legt es nahe, die folgende Frage zu stellen:

Frage: Gegeben sei eine natürliche Zahl $k \in \mathbb{N}$. Wie lässt sich entscheiden, ob k eine Summe zweier Quadratzahlen ist?

Anders gefragt: Für welche k geht der Kreis um den Nullpunkt mit Radius $\sqrt{k}$ durch einen Punkt mit ganzzahligen Koordinaten? Im folgenden Bild sind das die grünen Kreise:



Eine kurze Tabelle soll uns erste Einsichten erleichtern. Der Strich heißt, dass es eine solche Darstellung nicht gibt.

1	=	1^2+0^2	9	=	3^2+0^2	17	=	4^2+1^2	25	=	5^2+0^2	33		–	
2	=	1^2+1^2	10	=	3^2+1^2	18	=	3^2+3^2	26	=	5^2+1^2	34		–	
3		–	11		–	19		–	27		–	35		–	
4	=	2^2+0^2	12		–	20	=	4^2+2^2	28		–	36	=	6^2+0^2	
5	=	2^2+1^2	13	=	3^2+2^2	21		–	29	=	5^2+2^2	37	=	6^2+1^2	
6		–	14		–	22		–	30		–	38		–	
7		–	15		–	23		–	31		–	39		–	
8	=	2^2+2^2	16	=	4^2+4^2	24		–	32	=	4^2+4^2	40	=	6^2+2^2	

2. Eine erste Einschränkung

Wir sehen an der Tabelle, dass eine Summe zweier Quadratzahlen scheinbar niemals bei Division durch 4 Rest 3 lässt. Woran könnte das liegen?

Das Quadrat einer ganzen Zahl m ist immer entweder durch 4 teilbar oder lässt bei Division durch 4 Rest 1.

Denn: Entweder ist m gerade, also $m = 2a$ und $m^2 = 4a^2$ ein Vielfaches von 4, oder m ist ungerade: $m = 2a + 1$, und dann lässt

$$m^2 = 4(a^2 + a) + 1$$

Rest 1 bei Division durch 4.

Fazit: eine Zahl, die bei Division durch 4 Rest 3 lässt, kann niemals eine Summe zweier Quadrate sein.

Das kann noch nicht alles erklären, denn auch 6, 12, 14, 21, 22, 24 (und noch ein paar mehr) sind keine Summen von Quadratzahlen. .

Es muss noch weitere Einschränkungen geben.

Zum Beispiel zeigt uns ein ähnliches Argument wie das eben vorgeführte[1], dass eine Summe von zwei Quadratzahlen bei Division durch 8 immer Rest 0,1,2,4 oder 5 lässt, aber niemals Rest 3,6 oder 7. Dass Rest 6 hier ausgeschlossen ist, ist für uns eine neue Einsicht.

Auch das erklärt noch nicht alles.

3. Multiplikativität

Wenn wir zwei Zahlen $k = m^2 + n^2$, $l = p^2 + q^2$, als Summe zweier Quadrate schreiben können, dann gilt auch

$$(mp - nq)^2 + (mq + np)^2 = m^2p^2 + n^2q^2 + m^2q^2 + n^2p^2 = (m^2 + n^2) \cdot (p^2 + q^2) = kl.$$

Es ist also auch das Produkt dieser Zahlen eine Summe zweier Quadrate.

Da die Primzahlen die multiplikative Struktur der natürlichen Zahlen beherrschen, erscheint es daher sinnvoll, sich zu fragen, wann eine Primzahl sich als Summe zweier Quadrate schreiben lässt.

[1] $4(a^2 + a) + 1$ lässt bei Division durch 8 Rest 1, denn a^2 und a haben dieselbe Parität, ihre Summe ist also gerade.

Also sehen wir uns die Primzahlen doch einmal an.

Die 2 spielt hier eine gewisse Sonderrolle, aber jedenfalls ist sie eine Summe zweier Quadrate.

Bei allen anderen Primzahlen muss man unterscheiden, ob sie bei Division durch 4 Rest 1 oder 3 lassen. Die letzteren sind nicht Summe zweier Quadrate. Das sind die Primzahlen

$$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, \ldots$$

Hiervon gibt es unendlich viele, denn für $N \geq 4$ hat die (riesige) Zahl $M := N! - 1$ nur solche Primteiler, die größer sind als N. Ließen aber alle bei Division durch 4 Rest 1, so wäre der Rest von M bei Division durch 4 auch 1[2], was nicht der Fall ist.

Also gibt es unendlich viele Primzahlen, die sich nicht als Summen zweier Quadrate schreiben lassen.

Die verbliebenen Primzahlen sind die Primzahlen

$$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \ldots$$

Bei diesen Beispielen sieht man schnell, dass sie Summen zweier Quadrate sind. $5,\ 13,\ 17, 29$ und 37 haben wir schon gesehen, und die anderen sind

$$41 = 5^2 + 4^2,\ 53 = 7^2 + 2^2,\ 61 = 6^2 + 5^2,\ 73 = 8^2 + 3^2,\ 89 = 8^2 + 5^2,\ 97 = 9^2 + 4^2, \ldots$$

Hier tun sich zwei Fragen auf, deren Antworten eng miteinander verknüpft sind:

- Gibt es unendlich viele Primzahlen, die bei Division durch 4 Rest 1 lassen?
- Ist jede dieser Primzahlen eine Summe zweier Quadrate?

4. Eine Wurzel aus -1

In diesem Abschnitt sei $p \geq 3$ eine Primzahl.

Wir sagen, -1 sei ein Quadrat *modulo* p, wenn es ganze Zahlen a, b gibt, sodass

$$-1 = a^2 + bp.$$

Für welche Primzahlen trifft das zu?

Dazu müssen wir einen kleinen Umweg machen.

Erster Umweg: Die Binomischen Formeln. Die Binomialkoeffizienten sind hoffentlich bekannt, es sind die Zahlen

$$\binom{m}{i} = \frac{m!}{(m-i)! \cdot i!},$$

die sagen, wieviel i-elementige Teilmengen eine Menge mit m Elementen hat.

Wenn man nun zwei Zahlen x, y nimmt und $(x+y)^m$ ausrechnen will, so muss man m Faktoren mit je zwei Summanden ausmultiplizieren. Das tut man auf die übliche Art. Es gibt beim Ausmultiplizieren genau $\binom{m}{i}$ Möglichkeiten, i Faktoren auszuwählen, bei

[2]Denn: $(4x+1)(4y+1) = 4 \cdot (4xy + x + y) + 1$

denen man das x benutzt, und bei allen anderen Faktoren das y zu nehmen. Das muss man für alle i zusammenfassen und erhält die schöne Formel

$$(x+y)^m = \sum_{i=0}^{m} \binom{m}{i} x^i y^{m-i}.$$

Sie heißt die Binomische Formel und verallgemeinert die übliche Binomische Formel

$$(x+y)^2 = x^2 + 2xy + y^2,\ (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3, \ldots$$

Zweiter Umweg: Kleiner Satz von Fermat Es sei p eine Primzahl. Für jede ganze Zahl c ist $c^p - c$ ein Vielfaches von p.

Es langt, dies für natürliche Zahlen zu beweisen. Wäre es hier falsch, so gäbe es eine kleinste natürliche Zahl, für die es falsch ist. Wir schreiben diese als $c+1$ und benutzen, dass $c^p - c$ durch p teilbar ist. Die Binomischen Formeln zeigen, dass

$$(c+1)^p - (c+1) = c^p - c + \sum_{i=1}^{p-1} \binom{p}{i} c^i,$$

wobei in der letzten Summe jeder Summand von p geteilt wird (denn dies gilt für die Binomialkoeffizienten) und $c^p - c$ dies auch erfüllt. Daher ist auch $(c+1)^p - (c+1)$ ein Vielfaches von p im Widerspruch zu unserer Annahme, der kleine Satz von Fermat sei falsch.

Nun gehen wir zurück zu unserer Zahl a, die $a^2 = -1 - pb$ für eine ganze Zahl b erfüllt. Natürlich wird dann a nicht von p geteilt und auch nicht $a^2 - 1$, denn p ist größer als 2. Da andererseits wegen Fermat p ein Teiler von $a^p - a = a(a^{p-1} - 1)$ ist, muss p ein Teiler von $a^{p-1} - 1$ sein. Nun schreiben wir $p-1$ als

$$p - 1 = 4l + m,\ m \in \{0; 2\}.$$

Dann ist p ein Teiler von

$$a^{p-1} - 1 - (a^4 - 1)(1 + a^4 + a^{2\cdot 4} + \cdots + a^{(l-1)\cdot 4}) = a^{p-1} - a^{4l} = a^{4l} \cdot (a^m - 1).$$

Also teilt es $a^m - 1$. Da aber p kein Teiler von $a^2 - 1$ ist, ist $m = 0$.

Fazit: Wenn -1 ein Quadrat modulo p ist, dann lässt p bei Division durch 4 Rest 1.

Die Umkehrung hiervon gilt auch, denn wenn $p-1$ durch 4 teilbar ist, dann kann man nachweisen, dass für $a = (\frac{p-1}{2})!$ tatsächlich p ein Teiler von $a^2 + 1$ ist.

Folgerung: Es gibt unendlich viele Primzahlen, die bei Division durch 4 Rest 1 lassen.

Denn: Wenn $N \geq 2$ ist, so setzen wir $M := (N!)^2 + 1$. Jeder Primteiler p dieser Zahl ist größer als N, und -1 ist ein Quadrat modulo p (benutze $a = N!$ in der Definition). Also gibt es Primzahlen $> N$, die bei Division durch 4 Rest 1 lassen. Da N beliebig ist, gibt es unendlich viele solcher Primzahlen.

Beispiele:

$$(2!)^2 + 1 = 5,\ (3!)^2 + 1 = 37,\ (4!)^2 + 1 = 577,\ (5!)^2 + 1 = 14401$$

sind allesamt Primzahlen. Der Eindruck, der sich hier aufdrängen könnte, ist falsch:

$$(6!)^2 + 1 = 13 \cdot 39877$$

ist keine Primzahl. Aber beide Primfaktoren sind 1 modulo 4.

5. Noch eine Quadratsumme

Nun sei p eine Primzahl, die bei Division durch 4 Rest 1 lässt. Weiter sei a eine Zahl, sodass p ein Teiler von a^2+1 ist.

Nun schauen wir uns alle ganzzahligen Punkte $(m|n)$ in der Ebene an, die die Bedingung erfüllen, dass $n-am$ ein Vielfaches von p ist. Diese zerlegen die Ebene in kongruente Parallelogramme des Flächeninhalts p. Man kann mit einem geometrischen Argument[3] zeigen, dass sich im Kreis mit Radius $2\sqrt{\frac{p}{\pi}}$ ein von $(0|0)$ verschiedener solcher Punkt $(m|n)$ befindet. Für diesen Punkt ist aber das Längenquadrat $\neq 0$, ein Vielfaches von p :

$$m^2+n^2 = m^2+(am+pl)^2 = (1+a^2)m^2+p\cdot(2aml+pl^2) = p\cdot\text{irgendwas}$$

und kleiner als $4\frac{p}{\pi} < 2p$.

Daher ist das Längenquadrat p selbst, und $p=m^2+n^2$ ist eine Summe zweier Quadrate.

6. Resümee

Alles in allem wissen wir jetzt über die Primzahlen bescheid. Eine Primzahl ist genau dann eine Summe zweier Quadrate, wenn sie 2 ist oder bei Division durch 4 Rest 1 lässt.

Man kann dies dann nutzen, um ein Kriterium anzugeben, wann eine beliebige natürliche Zahl k Summe zweier Quadratzahlen ist:

Satz: *Die natürliche Zahl k ist genau dann eine Summe zweier Quadratzahlen, wenn in der Primfaktorzerlegung von k alle Primfaktoren, die bei Division durch 4 Rest 3 lassen, mit einem geraden Exponenten auftauchen.*

Dass es für diese Zahlen geht folgt aus der Multiplikativität der Fragestellung. Dass es keine anderen gibt, bedarf noch eines Arguments, das hier noch skizziert sei:

Ist p ein Primteiler einer Summe zweier Quadrate $k=a^2+b^2$, und teilt p a nicht, dann teilt es auch b nicht, denn sonst wäre es ja doch ein Teiler von $a^2=k-b^2$. Da p kein Teiler von a ist, gibt es eine natürliche Zahl f, sodass p $fa-1$ teilt. Also teilt es auch $f^2a^2-1=(fa-1)(fa+1)$. Wir multiplizieren $k=a^2+b^2$ mit f^2 und erhalten

$$p \text{ teilt } f^2k = f^2a^2+f^2b^2 = 1+f^2b^2+p\cdot\text{irgendwas}.$$

Also ist -1 ein Quadrat modulo p, und p ist 2 oder lässt bei Division durch 4 Rest 1.

Das zeigt: Wenn p bei Division durch 4 Rest 3 lässt, dann muss p bereits ein Teiler von a und von b sein, also können wir die Gleichung $k=a^2+b^2$ durch p^2 teilen und somit nach und nach sehen, dass der Exponent von p in k gerade ist.

7. Ausblick

Wir wissen jetzt, wann eine natürliche Zahl eine Summe zweier Quadratzahlen ist. Dies können wir testen, ohne diese Quadratzahlen zu finden. Es handelt sich um eine reine Existenzaussage. Allerdings ist as auch sehr schwer, die Primzerlegung einer natürlichen Zahl zu finden. Interessanter Weise kann man hierzu gelegentlich ausnutzen, dass jede ungerade Zahl sich als **Differenz** zweier Quadratzahlen schreiben lässt, z.B. $2a+1=$

[3] Das ist der Gitterpunktsatz von Minkowski

$(a+1)^2-a^2$. Wenn man hier eine interessantere Variante findet, so folgt aus $x=m^2-n^2$, dass $(m+n)$ und $(m-n)$ Faktoren von x sind.

Erstaunlicher Weise hat die Frage nach Summen von drei Quadraten keine so glatte Antwort wie die hier behandelte. Das liegt daran, dass die multiplikative Struktur, die wir ja benutzt haben, dann nicht mehr gegeben ist. Für vier Quadrate haben wir eine solche wieder, und das kann man benutzen, um zu zeigen, dass jede natürliche Zahl eine Summe von vier Quadratzahlen ist. Das ist der Vier-Quadrate-Satz von Lagrange.

Wenn eine natürliche Zahl n gegeben ist kann man sich fragen, welche Primzahlen sich als x^2+ny^2 schreiben lassen. Das ist je nach Wahl von n schon eine sehr subtile Frage, zu deren Beantwortung man schon mehr an mathematischer Maschinerie einsetzen muss und auch dann noch keine leicht verständliche Antwort erhält.

Ein ganz anderer Aspekt unserer Überlegungen lässt sich in Dirichlets Primzahlsatz verallgemeinern: Wenn $a<b$ zwei teilerfremde Zahlen sind, dann gibt es unendlich viele Primzahlen, die bei Division durch b Rest a lassen. Das haben wir für $a=1, b=4$ und $a=3, b=4$ gesehen, mit ähnlichen Argumenten ließe sich auch der Fall $a=1$ oder 2 und $b=3$ behandeln. Aber danach fängt es an, komplizierter zu werden.