Summen von Quadraten
Skript zur ETH Vorlesung HS21

Raphael S. Steiner

Department of Mathematics, ETH Zürich, 8092 Zürich, CH
raphael.steiner@math.ethz.ch

24. September 2021

Inhaltsverzeichnis

1 Motivation und Übersicht

Summen von Quadraten können sich an vielen Orten verstecken. Um dies zu illustrieren, beginnen wir mit einer informalen Besprechung eines Problems. Das Problem ist wiefolgt.

Problem. *Ob und wie kann man ein Quadrat in fünf gleich grosse Teilquadrate zerschneiden mit geraden Schnitten?*

Auf den ersten Blick bemerkt man sofort, dass man das Quadrat in $1, 4, 9, 16, \ldots, n^2, \ldots$ kleinere gleich grosse Quadrate zerschneiden kann und diese scheinen wirklich die einzigen Möglichkeiten zu sein. Dies ist tatsächlich der Fall, denn hätte man N gleich grosse Teilquadrate wäre die Seitenlänge $1/\sqrt{N} \in \mathbb{Q} \Leftrightarrow N = n^2$. Was passiert nun, wenn wir die Bedingung 'gleich gross' weglassen. In diesem Falle kann man beliebiges Teilquadrat nehmen und es in 4 Quadrate zerschneiden. Dies zeigt, dass wenn man ein Quadrat in N kleinere Quadrate zerschneiden kann, so kann man es auch in $N+3$ Quadrate zerschneiden. Nach weiterem überlegen findet man einen Weg ein Quadrat in 6,8,10,... , Teilquadrate zu zerlegen, indem man ein grosses Quadrat mit kleineren Quadraten von zwei Seiten umhüllt. Hier ist eine solche Anordnung für acht Teilquadrate zu sehen (Abbildung 1).

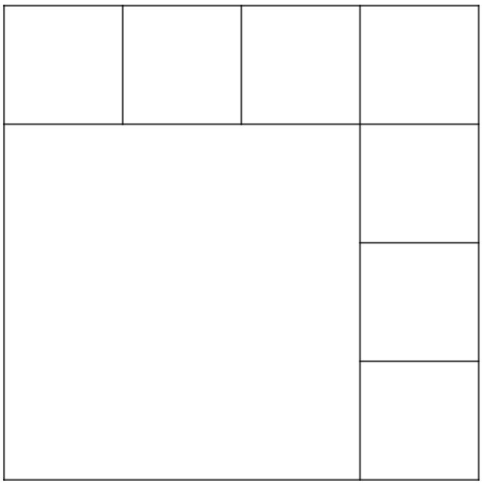

Abbildung 1: Acht Teilquadrate

Insgesamt findet man Wege ein Quadrat in N Teilquadrate zu zerlegen ausser für $N = 2, 3, 5$. Um fünf gleich grosse Quadrate zu erhalten müssen wir also etwas kreativer werden. Versuchen wir uns zuerst mal an zwei gleich grosse Teilquadrate. Durch herum probieren oder motiviert durch die Seitenlänge $1/\sqrt{2}$ und Pythagoras kommt man auf die Diagonalen (Abbildung 2). Hier kann man das linke und rechte Dreieck zu einem Quadrat zusammen kleben und ebenso das obere und untere Dreieck.

Das heisst, erlauben wir (Verschiebungen und) Kleben, so ist das zerschneiden in zwei gleich grosse Quadrate möglich. Wie sieht es aber nun mit fünf aus? Dies ist auch möglich. Dazu schneidet man von einer Ecke zu einer zur einem gegenüberliegenden Mittelpunkt und wiederholt dies für jede Ecke, wie in Abbildung 3, so erhält man fünf gleich grosse Quadrate.

Dass dies, wirklich der Fall ist könnte man nachrechnen, indem man Seitenlängen und Winkel berechnet. Wir möchten aber eine Intuitive Begründung. Der Name der Vorlesung gibt dabei einen kleinen Hinweis. Zwei und Fünf sind Summen von zwei Quadraten: $2 = 1^2 + 1^2$ und $5 = 2^2 + 1^2$. Betrachten wir unsere Schnitte etwas genauer, so sehen wir,

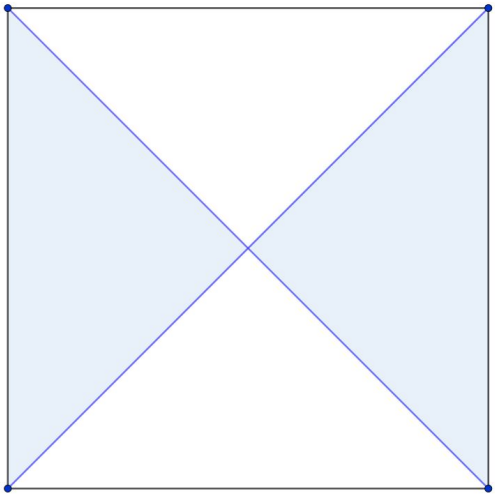

Abbildung 2: Zwei gleich grosse Teilquadrate

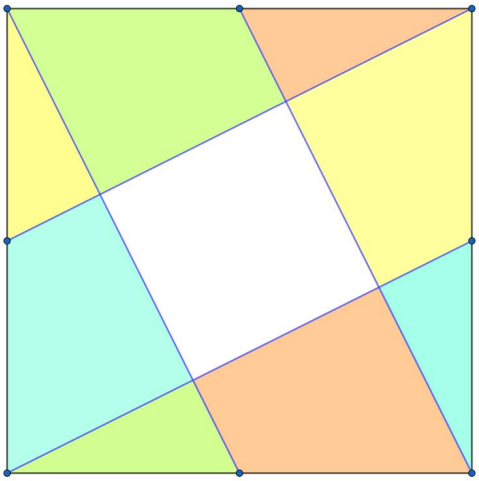

Abbildung 3: Fünf gleich grosse Teilquadrate

dass sie die Hypothenuse eines rechtwinkligen Dreiecks sind mit Kathetenverhältnis $1:1$, respektive $2:1$. Dies scheint kein Zufall zu sein. Tatsächlich ist dies kein Zufall, wie wir jetzt erklären werden.

Betrachte die ganzen Gitterpunkte $\mathbb{Z}^2 \subset \mathbb{R}^2$ in der Ebene. Ferner markiere man alle Punkte rot, welche man vom Ursprung $(0,0)$ durch das Addieren von beliebig vielen Vektoren der Form $(1,2)$, $(2,-1)$, $(-1,-2)$, oder $(-2,1)$ erreichen kann. Zeichnet man nun das quadratische Mesh, welches durch die ganzen Gitterpunkte $\mathbb{Z}^2$ gegeben ist, und ebenso für die rot markierten Punkte[a] so erkennen wir die Abbildung 3 wieder als eines der roten Quadrate (siehe Abbildung 4).

Färbt man nun die kleineren Quadrate so ein wie bei Abbildung 3, so sieht man, dass der Grund warum man fünf Teilquadrate erhält ist, dass es fünf verschiedene Verschiebungen des roten Gitters gibt, dessen gesamthafte Gitterpunkte gerade das Gitter $\mathbb{Z}^2$ ergibt. Letzteres können wir mit etwas Zahlentheorie erklären. Dazu identifizieren wir die

[a] Man überzeuge sich selbst, dass dies wirklich ein quadratisches Mesh darstellt.

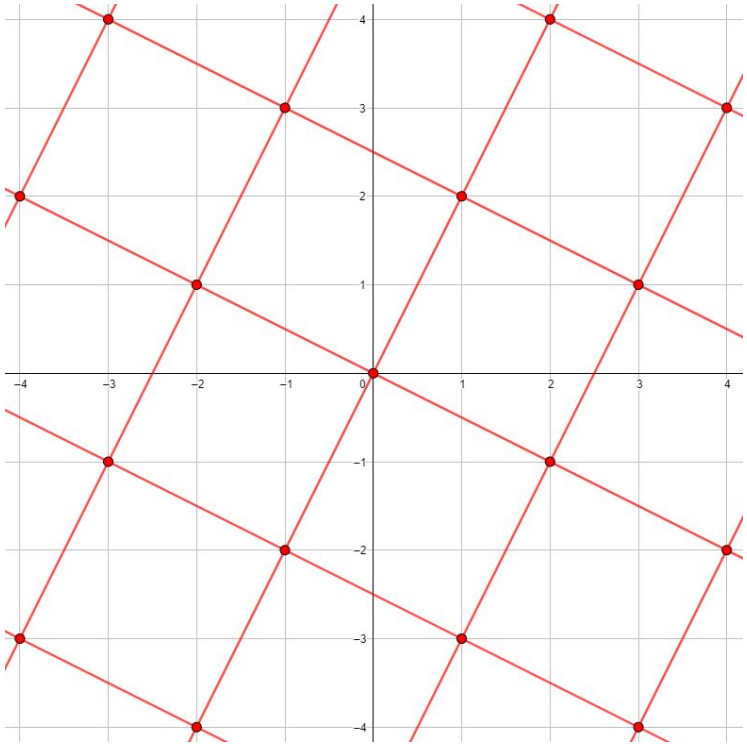

Abbildung 4: Gitter und Mesh in der Ebene

Ebene mit den komplexen Zahlen $\mathbb{C}$ und die ganzen Gitterpunkte mit den Gauss'schen Zahlen $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$. Es stellt sich nun heraus, dass die rot markierten Punkte gerade diejenigen Gauss'schen Zahlen sind, welche durch $2 - i$ teilbar sind. So ist zum Beispiel $1 + 2i = i(2 - i)$. In den Gauss'schen Zahlen gilt nun, dass die Division durch $2 - i$ mit Rest genau $|2 - i|^2_{\mathbb{C}} = 2^2 + 1^2 = 5$ verschiede Restklassen besitzt. Jene Restklassen stellen nun genau die verschiedenen Verschiebungen der roten Gitterpunkte dar.

Man kann nun mit dieser Konstruktion etwas Spass haben. Hier ist zum Beispiel, wie man ein Quadrat in $13 = 3^2 + 2^2$ gleich grosse Teilquadrate zerschneiden kann (Abbildung 5).

Wir haben nun motiviert, dass Summen von zwei Quadraten im Zusammenhang mit den Gauss'schen Zahlen $\mathbb{Z}[i]$ stehen. Jene sind ein Analog von den ganzen Zahlen in den komplexen Zahlen $\mathbb{C}$. Nun besitzt $\mathbb{C}$ eine Erweiterung, die Quaternionen $\mathbb{H}$. Sowie die Norm auf $\mathbb{C}$ im Zusammenhang mit Summen von zwei Quadraten steht, so steht die Norm der Quaternionen im Zusammenhang mit Summen von vier Quadraten. Wir werden in der Vorlesung sehen, wie man die Quaternionen konstruiert und dass man auch ein Analog der ganzen Zahlen finden kann. Wir werden jene benutzen, um den vier Quadrate Satz von Lagrange zu beweisen.

Satz (Lagrange)**.** *Jede natürliche Zahl lässt sich als Summe von vier Quadraten ganzer Zahlen schreiben.*

Man stellt sich nun die Frage, wie sieht es mit drei Quadraten aus? Die Theorie für Summen von drei Quadraten ist um einiges komplizierter. Der Grund dafür ist, dass es für Summen von drei Quadraten keine zugrundeliegende multiplikative Struktur gibt wie es im Fall von zwei Quadraten (die komplexen Zahlen) oder vier Quadraten (die Quaternionen) ist. Im Verlaufe der Vorlesung werden wir dies genauer präzisieren und zeigen, dass solche

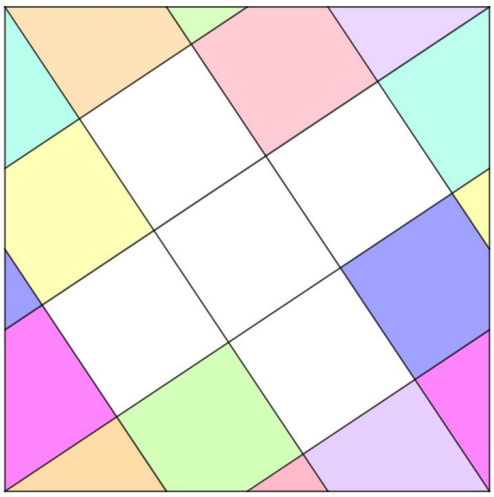

Abbildung 5: 13 gleich grosse Teilquadrate

multiplikativen Strukturen für Summen von N Quadraten gibt genau dann wenn $N = 1, 2, 4, 8$.

Zum Schluss werden wir Quadrate etwas verallgemeinern, nämlich zu positiv definiten binären quadratische Formen, und zeigen, dass man jene auch multiplizieren kann[b]. So hat man zum Beispiel

$$(2r^2 + 2rs + 3s^2)(2u^2 + 2uv + 3v^2) = x^2 + 5y^2,$$

wobei

$$x = 2ru + rv + su + 3sv, \quad y = rv - su.$$

2 Die ganzen Zahlen und ihre Quotienten

Die Theorie in diesem Kapitel lässt sich in den meisten Bücher über algebraische Zahlentheorie oder Algebra auffinden, so zum Beispiel [2], [3] oder [1].

2.1 Teiler und Faktorisierungen

Wir beginnen die Lektion mit einer Repetition der gängigen Eigenschaften der ganzen Zahlen. Wir werden jene Eigenschaften, wie z.B. die eindeutige Primfaktorzerlegung, in einer Art und Weise herleiten, sodass eine Verallgemeinerung auf andere Zahlsystem wie die Gauss'schen Zahlen sofort per Analogie folgt. Dabei erwähnen und verwenden wir die korrekten algebraischen Begriffe. Jedoch sind letztere für uns nicht von grösster Bedeutung, da wir immer mit konkreten algebraischen Strukturen arbeiten.

Zur Auffrischung errinnern wir uns an die Rechenregeln der ganzen Zahlen:

- Die Addition ist kommutativ: $\forall a, b \in \mathbb{Z} : a + b = b + a$.
- Die Addition ist assoziativ: $\forall a, b, c \in \mathbb{Z} : a + (b + c) = (a + b) + c$.
- Die Addition besitzt ein neutrales Element (Null): $\exists 0 \in \mathbb{Z} : \forall a \in \mathbb{Z} : a+0 = 0+a = a$.

[b] Sofern beide Formen dieselbe Diskriminante besitzen

- Es existieren inverse Elemente bezüglich der Addition: $\forall a \in \mathbb{Z} : a+(-a) = (-a)+a = 0$.
- Die Multiplikation ist kommutativ: $\forall a, b \in \mathbb{Z} : a \cdot b = b \cdot a$.
- Die Multiplikation ist assoziativ: $\forall a, b, c \in \mathbb{Z} : a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Die Multiplikation besitzt ein neutrales Element (Eins): $\exists 1 \in \mathbb{Z} : \forall a \in \mathbb{Z} : a \cdot 1 = 1 \cdot a = a$.
- Die Multiplikation ist links distributiv über die Addition: $\forall a, b, c \in \mathbb{Z} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- Die Multiplikation ist rechts distributiv über die Addition: $\forall a, b, c \in \mathbb{Z} : (b + c) \cdot a = (b \cdot a) + (c \cdot a)$.
- Keine von Null verschiedenen Nullteiler: $\forall a, b \in \mathbb{Z} : a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$.

Bemerkung. Eine solche algebraische Struktur nennt sich *Integritätsbereich*, falls $0 \neq 1$. Nebst $\mathbb{Z}$ sind auch $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \mathbb{Z}[X], \ldots$ Beispiele eines Intergritätsbereiches.

Definition. *Wir sagen eine Zahl $a \in \mathbb{Z}$* teilt *eine Zahl $b \in \mathbb{Z}$, schreibe $a \mid b$, genau dann wenn eine Zahl $c \in \mathbb{Z}$ existiert, sodass $ac = b$ gilt. Sofern jene Zahl c eindeutig ist, schreiben wir $\frac{b}{a} = c$.*

Bemerkung. Falls $0 \neq a \in \mathbb{Z}$ ein Teiler von $b \in \mathbb{Z}$, so ist c mit $ac = b$ eindeutig bestimmt. Denn für die ganzen Zahlen gilt folgende Eigenschaft $xy = 0$ mit $x, y \in \mathbb{Z}$, so folgt $x = 0$ oder $y = 0$. Wäre also $c' \in \mathbb{Z}$ ein anderes Element mit $ac' = b$ so folgt $a(c - c') = b - b = 0$ also $c - c' = 0 \Leftrightarrow c = c'$, da $a \neq 0$.

Die folgenden Teilereigenschaften sind einfach nachzuweisen.

Lemma 2.1. *Für ganzen Zahlen $a, b, c \in \mathbb{Z}$ gelten folgende Aussagen:*

1. *Falls $a \mid b$ und $b \mid c$, so gilt $a \mid c$,*
2. *Falls $a \mid b$ und $a \mid c$, so gilt $a \mid xb + yc$ für alle $x, y \in \mathbb{Z}$.*

Beweis. Für 1. finden wir $d, e \in \mathbb{Z}$, sodass $b = ad$ und $c = be$. Es folgt $c = be = a(de)$, also a teilt c. Für 2. finden wir $d, e \in \mathbb{Z}$, sodass $b = da$ und $c = ea$. Dann gilt für beliebige $x, y \in \mathbb{Z}$, dass $xb + yc = (xd + ye)a$. Es folgt, dass $a \mid xb + yc$. □

Definition. *Eine ganze Zahl $a \in \mathbb{Z}$ heisst* Einheit *genau dann, wenn es $b \in \mathbb{Z}$ gibt, sodass $ab = 1$. Die Menge der Einheiten von $\mathbb{Z}$ wird mit $\mathbb{Z}^\times$ bezeichnet.*

Bemerkung. Ist a eine Einheit, so ist auch $\frac{1}{a}$ eine Einheit. Anstatten von $\frac{1}{a}$ schreiben wir gängigerweise auch a^{-1}.

Für die ganzen Zahlen $\mathbb{Z}$ bestehen die Einheiten genau aus den Zahlen ± 1.

Definition. *Eine Zahl $c \in \mathbb{Z}$ heisst* grösster gemeinsamer Teiler *von $a, b \in \mathbb{Z}$, schreibe $c = \mathrm{ggT}(a, b)$, falls*

1. *$c \mid a$ und $c \mid b$,*
2. *für alle $d \in \mathbb{Z}$, sodass $d \mid a$ und $d \mid b$, gilt $d \mid c$.*

Der grösste gemeinsame Teiler zweier Zahlen (falls existent), ist bis auf Multiplikation einer Einheit eindeutig bestimmt, (d.h. bis auf Vorzeichen).

Letzteres ist der Fall, denn falls c, d grösste gemeinsame Teiler von $a, b \in \mathbb{Z}$ sind, so gilt nach der zweiten Eigenschaft, dass $c \mid d$ und $d \mid c$. Das heisst es existieren $e, f \in \mathbb{Z}$, sodass $d = ec$ und $c = fd$. Es folgt $d = ec = efd \Rightarrow d(ef - 1) = 0$. Wir unterscheiden zwei Fälle. Falls $d = 0$, so ist auch $c = 0 = d = d \cdot 1$ und wir sind fertig. Falls $d \neq 0$, so gilt $ef = 1$. Also sind e, f Einheiten und es gilt $c = fd$, $d = ec$.

Definition. *Zwei ganzen Zahlen, welche sich nur durch Multiplikation einer Einheit unterscheiden, heissen zueinander* assoziiert. *Dies ist eine Äquivalenzrelation.*

Lesende mögen ein positives Vorzeichen bei der Definition des grössten gemeinsamen Teilers bevorzugen, jedoch ist im Skript von einer beliebigen Wahl auszugehen, d.h. genau genommen müsste man von einer Äquivalenzklasse von Zahlen reden, welche durch Assoziiertheit definiert sind. Da es aber immer einfach ist mit einer Einheit zu multiplizieren, respektive durch eine Einheit zu dividieren, erlauben wir uns diese Ambiguität.

Literatur

[1] Siegfried Bosch. *Algebra.* Berlin: Springer Spektrum, 2020.

[2] Stefan Müller-Stach and Jens Piontkowski. *Elementare und algebraische Zahlentheorie. Ein moderner Zugang zu klassischen Themen.* Wiesbaden: Vieweg+Teubner, 2011.

[3] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie.* Berlin: Springer, 2007.