Georg Keller
Kantonsschule Schaffhausen, georg.keller@kanti.sh.ch

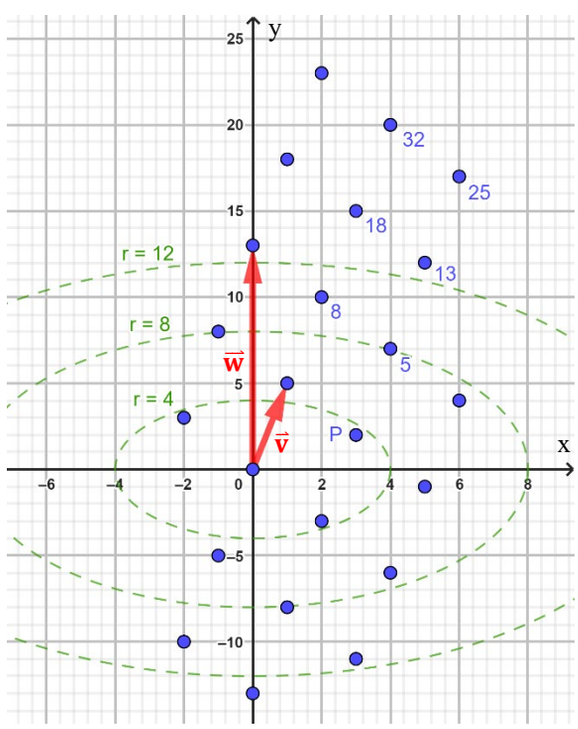
Eleganter Beweis des 2-Quadrate resp. 4-Quadrate-Satzes

Einleitung

Vor etwa einem Jahr begegnete ich auf den Seiten 6-9 des Buches „Combinatorial Geometry“ [1] einem mir unbekannten und m.E. erstaunlich kurzen, sehr eleganten Beweis des 2-Quadrate- resp. 4-Quadrate-Satzes. Weil diese Beweise manchen Mathematikern unbekannt zu sein scheinen und weil sie für einen Teil der Leserschaft des VSMP-Bulletins von Interesse sein könnten, werde ich diese Beweise gerne darlegen, wobei ich die Argumentation in [1] der hoffentlich besseren Verständlichkeit halber z.T. anpassen (z.B. mit Detailausführungen ergänzen) werde.

Statt jetzt aber sogleich mit den ersten Beweisschritten für den 2-Quadrate-Satz zu beginnen, wollen wir diese Einleitung noch einen Moment weiterführen. Denn als hoffentlich nützliche Orientierungshilfe möchten wir einen wenigstens groben Einblick in die dem Beweis des 2-Quadrate-Satzes zugrundeliegende Strategie geben, allerdings ohne jegliche Begründungen (welche später, d.h. in den nächsten drei Kapiteln, erfolgen werden). - Nun, der 2-Quadrate-Satz besagt ja, dass jede Primzahl der Form $p = 4n + 1$, $n \in \mathbb{N}$, als Summe der Quadrate zweier ganzer Zahlen geschrieben werden kann. Die kleinsten Primzahlen von dieser Form sind $p = 5, 13, 17, 29, 37, \ldots$; das zur Illustration gut geeignete Beispiel $p = 13$ betrachtend, kann die Beweisstrategie wie folgt umrissen werden:

- Man betrachtet das 2-dimensionale Gitter in $\mathbb{Z}^2$, welches durch die Vektoren $\vec{v} := \begin{pmatrix} 1 \\ 5 \end{pmatrix}$ und $\vec{w} := \begin{pmatrix} 0 \\ 13 \end{pmatrix}$ erzeugt wird (ein Ausschnitt dieses Gitters ist nebenstehend abgebildet, wobei die Gitterpunkte blau gefärbt sind; die Bedeutung der übrigen Teile der Abbildung wird im folgenden Text erläutert).



- Aufgrund der speziellen Wahl von $\vec{v}$ und $\vec{w}$ haben die Gitterpunkte (x, y) zwei bemerkenswerte und keineswegs offensichtliche Eigenschaften:

  1. $x^2 + y^2$ ist jeweils ein *ganzzahliges* Vielfaches von 13 ; so z.B. ist $4^2 + 20^2 = 32 \cdot 13$, weswegen beim Gitterpunkt $(4, 20)$ die blaue Zahl 32 steht. Zwecks Illustration sind in der Abbildung noch einige weitere dieser Multiplikatoren von 13 notiert.

  2. Es ist klar, dass mit kleiner werdendem Abstand $r := \sqrt{x^2 + y^2}$ der Gitterpunkte vom 0-Punkt der Wert von $x^2 + y^2$ ein immer kleineres Vielfaches von 13 wird (vgl. auch unsere Abbildung, wo als Lesehilfe Ellipsen(bögen) mit $r = 4, 8, 12$ abgebildet sind). Aber überhaupt nicht offensichtlich ist Folgendes: Für die am *nächsten* beim 0-Punkt liegenden Gitterpunkte ist $x^2 + y^2$ nicht das 2-fache oder 3-fache oder ... von 13 , sondern das *kleinstmögliche* (natürlich positive) Vielfache von 13 , d.h. das 1-fache von 13 . Angewandt auf den Gitterpunkt $P(3, 2)$, welcher einer der vier dem 0-Punkt am nächsten liegenden Gitterpunkte ist (zwei der übrigen drei nächstliegenden Gitterpunkte sind in der Abbildung ebenfalls gezeigt), heisst dies, dass $3^2 + 2^2 = 1 \cdot 13$ ist, d.h. $3^2 + 2^2 = 13$, womit die Richtigkeit des 2-Quadrate-Satzes für $p = 13$ nachgewiesen (und leicht verifizierbar) ist.

Dass das oben skizzierte Vorgehen nicht nur für $p = 13$ funktioniert, sondern für alle Primzahlen der Form $p = 4n + 1$, sofern $\vec{v}$ und $\vec{w}$ jeweils geeignet gewählt werden (z.B. für $p = 29$ wählt man $\vec{v} := \binom{1}{12}$ und $\vec{w} := \binom{0}{29}$), liegt überhaupt nicht auf der Hand, wird aber im Folgenden bewiesen werden.

Geometrische Vorbereitung

Gitterpunktsatz von Minkowski: Es sei $C \subseteq \mathbb{R}^d$ ein abgeschlossener, konvexer Körper, symmetrisch bezgl. des Nullpunkts des Koordinatensystems, und $\Lambda \subseteq \mathbb{R}^d$ sei ein d-dimensionales Gitter (wobei wir das Volumen einer Elementarzelle von Λ mit $\det(\Lambda)$ bezeichnen). Dann gilt: Falls $\mathrm{Vol}(C) \geq 2^d \cdot \det(\Lambda)$ ist, enthält C nebst dem Nullpunkt des Koordinatensystems mindestens noch einen weiteren Gitterpunkt von Λ.

Beweis:

- Wenn die Mengen $\frac{1}{2}C + u$, $u \in \Lambda$, paarweise disjunkt wären, dann müsste $\mathrm{Vol}\left(\frac{1}{2}C\right)$ kleiner als $\det(\Lambda)$ sein; wegen $\mathrm{Vol}\left(\frac{1}{2}C\right) = \frac{1}{2^d} \cdot \mathrm{Vol}(C)$ würde also gelten $\mathrm{Vol}(C) < 2^d \cdot \det(\Lambda)$. Weil aber vorausgesetzt wird, dass $\mathrm{Vol}(C) \geq 2^d \cdot \det(\Lambda)$ ist, gibt es mindestens zwei Mengen $\frac{1}{2}C + u_1$ und $\frac{1}{2}C + u_2$ mit $u_1 \neq u_2$, deren Durchschnitt nicht leer ist und z.B. den Punkt $v \in \mathbb{R}^d$ enthält.

- Es sei also $v \in \left(\frac{1}{2}C + u_1\right) \cap \left(\frac{1}{2}C + u_2\right)$. Daher ist $v - u_1 \in \frac{1}{2}C$ und $v - u_2 \in \frac{1}{2}C$; aus Punktsymmetriegründen gilt nebst Letzterem aber auch $u_2 - v \in \frac{1}{2}C$. Daher ist $0 \neq u_2 - u_1 = (u_2 - v) + (v - u_1) \in \frac{1}{2}C + \frac{1}{2}C$, was aus Konvexitätsgründen in C liegt. Also liegt nebst dem Nullpunkt des Koordinatensystems auch der Gitterpunkt $u_2 - u_1 \neq 0$ in C. ■

Algebraische Vorbereitung für den Beweis des 2-Quadrate-Satzes

Es sei p eine Primzahl; dann bezeichnen wir mit $\mathbb{Z}_p := \{0, 1, 2, \dots, (p-1)\}$ den Körper der Restklassen modulo p und mit $\mathbb{Z}_p^+ := \{1, 2, \dots, (p-1)\}$ die multiplikative, abelsche Gruppe der positiven Restklassen modulo p. Wir erinnern an die grundlegende (aber nur mit einem gewissen Aufwand beweisbare) Tatsache, dass $\mathbb{Z}_p^+$ eine zyklische Gruppe ist, d.h. dass es ein Element $a \in \mathbb{Z}_p^+$ gibt, sodass $\mathbb{Z}_p^+ = \{a, a^2 \bmod p, a^3 \bmod p, \dots, a^{p-1} \bmod p\}$ ist (wobei gemäss Kleinem Satz von Fermat $a^{p-1} \bmod p = 1$ ist); a wird erzeugendes Element von $\mathbb{Z}_p^+$ genannt. (Beispiele von Primzahlen p und kleinstem erzeugenden Element $a_{min} \in \mathbb{Z}_p^+$ sind $(p, a_{min}) = (2, 1), (3, 2), (5, 2), (7, 3), (11, 2), (13, 2), (17, 3), (19, 2)$.) Der Kürze halber werden wir statt $b \equiv c \pmod p$ nur $b =_p c$ schreiben. Mit dieser Notation gilt der folgende Satz.

Satz:

1. Es sei $w \in \mathbb{Z}_p^+$ gegeben. Dann hat für $x \in \mathbb{Z}_p$ die quadratische Gleichung $x^2 =_p w^2$ folgende Lösung: Für $p = 2$ ist $x = w$; für $p > 2$ aber gibt's die zwei unterschiedlichen Lösungen
$$x_1 = w \ , \ x_2 = p - w \ . \tag{1}$$

2. Wenn die Primzahl p von der Form $p = 4n + 1$, $n \in \mathbb{N}$, ist, existiert ein Element $j \in \mathbb{Z}_p^+$ mit
$$j^2 =_p -1 \ . \tag{2}$$

Beweis:

1. $x^2 =_p w^2 \Rightarrow (x - w)(x + w) =_p 0$; weil $\mathbb{Z}_p$ ein Körper ist, folgt, dass entweder $x - w =_p 0$ ist ($\Rightarrow x_1 = w$), oder dass $x + w =_p 0$ ist ($\Rightarrow x_2 + w = p$, weil $w > 0$ ist). Für $p = 2$ kann w nur gleich 1 sein, und daraus folgt $x_1 = x_2 = 1 \equiv w$; für $p > 2$ aber kann x_1 nicht gleich x_2 sein, denn sonst wäre p gerade.

2. Wegen $p = 4n + 1$, $n \in \mathbb{N}$, ist $\frac{p-1}{4} \in \mathbb{N}$. Sei a ein erzeugendes Element von $\mathbb{Z}_p^+$. Wir setzen $\jmath := a^{\frac{p-1}{4}} \bmod p \in \mathbb{Z}_p^+$, womit $(\jmath^2 \bmod p)^2 =_p a^{p-1} =_p 1$ ist. Wir sehen also, dass $\jmath^2 \bmod p \in \mathbb{Z}_p$ eine Lösung der quadratischen Gleichung $x^2 =_p 1$ ist; wegen $p > 2$ besagt (1), dass entweder $\jmath^2 \bmod p = 1$ oder $\jmath^2 \bmod p = p - 1$ ist. Weil a ein erzeugendes Element von $\mathbb{Z}_p^+$ ist und weil zur Berechnung von $\jmath^2$ der Exponent von a gleich $\frac{p-1}{2}$ und daher kleiner als $p - 1$ ist, kann $\jmath^2 \bmod p$ nicht gleich 1 sein; also gilt (2). ■

Anmerkung: Wegen (2) spielt $\jmath$ im Körper $\mathbb{Z}_p$ eine Rolle, welche an die imaginäre Einheit i erinnert; aus diesem Grund haben wir (im Unterschied zu [1]) für $\jmath$ einen i-ähnlichen Buchstaben gewählt.

2-Quadrate-Satz, Beweis

2-Quadrate-Satz: Jede Primzahl p der Form $p = 4n + 1$, $n \in \mathbb{N}$, kann als Summe der Quadrate zweier ganzer Zahlen geschrieben werden.

Beweis:

- Unter Verwendung der in (2) auftretenden Zahl $\jmath \in \mathbb{Z}_p^+$ betrachten wir dasjenige 2-dimensionale Gitter $\Lambda \subset \mathbb{Z}^2$, welches durch die Vektoren $\begin{pmatrix} 1 \\ \jmath \end{pmatrix}$ und $\begin{pmatrix} 0 \\ p \end{pmatrix}$ erzeugt wird. Offenbar ist $\det(\Lambda) = p$; und ein beliebiger Gitterpunkt $(x, y) \in \Lambda$ kann als $x = \alpha$ und $y = \alpha \cdot \jmath + \beta \cdot p$ mit irgendwelchen ganzen Zahlen α, β geschrieben werden, d.h. es gilt

$$y =_p x \cdot \jmath \quad . \tag{3}$$

- Als Nächstes betrachten wir die abgeschlossene Menge $C := \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq r^2 := 1.9\, p\}$. Offensichtlich ist C konvex und symmetrisch bezgl. des Nullpunkts des Koordinatensystems, und $\mathrm{Vol}(C) = \pi r^2 = \pi \cdot 1.9\, p \cong 5.97\, p$. Daher ist $\mathrm{Vol}(C) \cong 5.97\, p \geq 4\, p = 2^d \cdot \det(\Lambda)$, womit der Gitterpunktsatz von Minkowski besagt, dass C noch (mindestens) einen von 0 verschiedenen Gitterpunkt $(x', y') \in \Lambda$ ($\Rightarrow x'^2 + y'^2 > 0$) enthält, welcher gemäss (3) und (2) Folgendes erfüllt:

$$x'^2 + y'^2 \overset{(3)}{\underset{p}{=}} x'^2 + x'^2 \cdot \jmath^2 \overset{(2)}{\underset{p}{=}} 0 \tag{4}$$

(4) zeigt, dass für die zwei ganzen Zahlen x', y' die positive Zahl $x'^2 + y'^2$ ein (natürlich positives) Vielfaches von p ist, wobei gemäss Definition von C der Wert von $x'^2 + y'^2$ höchstens das 1.9-fache von p sein kann. Also ist $x'^2 + y'^2 = p$. ■

Anmerkung: Wir werden sehen, dass ein wesentlicher Teil des Beweises des 4-Quadrate-Satzes eng verwandt ist mit dem obigen Beweis. Daher wird es nicht sehr überraschen, dass wir als Nächstes eine auf den Beweis des 4-Quadrate-Satzes ausgerichtete und vom Kapitel „Algebraische Vorbereitung für den Beweis des 2-Quadrate-Satzes“ inspirierte Vorbereitung treffen.

Algebraische Vorbereitung für den Beweis des 4-Quadrate-Satzes

Satz: Wenn p eine Primzahl ist, dann existieren Elemente $\jmath_1, \jmath_2 \in \mathbb{Z}_p$ mit

$$\jmath_1^{\,2} + \jmath_2^{\,2} =_p -1 \quad . \tag{5}$$

Beweis:

- Für $p = 2$ kann (5) z.B. mit $\jmath_1 = 0$ und $\jmath_2 = 1$ erfüllt werden.

- Und für $p \geq 3$ ($\Rightarrow p$ ist ungerade) können wir wie folgt argumentieren:

- Z.B. anhand einer der binomischen Formeln sieht man sofort ein, dass $(p-1)^2 =_p 1^2$, $(p-2)^2 =_p 2^2$, $(p-3)^2 =_p 3^2$, ... ist. Daher, und weil $(p-1)$ gerade ist, gilt:

$$\begin{aligned}&|\{1^2 \bmod p\,, 2^2 \bmod p\,, \cdots, (p-2)^2 \bmod p\,, (p-1)^2 \bmod p\}| \\ &= \left|\{1^2 \bmod p\,, 2^2 \bmod p\,, \cdots, \left(\tfrac{p-1}{2}\right)^2 \bmod p\,\}\right| \le \tfrac{p-1}{2}\end{aligned}$$

  Die eben betrachteten Zahlen $i^2 \bmod p$, $1 \le i \le \frac{p-1}{2}$, sind ...

  - ➤ paarweise verschieden (denn sonst gäbe es ein Paar $1 \le i, j \le \frac{p-1}{2}$ mit $i \ne j$ und $i^2 =_p j^2$ $\overset{(1)}{\Rightarrow}$ entweder $i = j$ (offensichtlich unmöglich) oder $i = p - j$, was aber wegen $i + j < p$ ebenfalls unmöglich ist);
  - ➤ ungleich 0 (denn alle i sind in $\mathbb{Z}_p^+$).

  Also enthält die Menge $M_1 := \{0^2 \bmod p\,, 1^2 \bmod p\,, 2^2 \bmod p\,, \cdots, (p-2)^2 \bmod p\,, (p-1)^2 \bmod p\} \subset \mathbb{Z}_p$ genau $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ Elemente.

- Auf analoge Weise sieht man ein, dass auch die Menge $M_2 := \{(-0^2 - 1) \bmod p\,, (-1^2 - 1) \bmod p\,, (-2^2 - 1) \bmod p\,, \cdots, (-(p-2)^2 - 1) \bmod p\,, (-(p-1)^2 - 1) \bmod p\} \subset \mathbb{Z}_p$ genau $\frac{p+1}{2}$ Elemente enthält.

- Weil $\mathbb{Z}_p$ genau p Elemente enthält, ist es daher unmöglich, dass $M_1 \cap M_2 = \emptyset$ ist. Also gibt es ein Element $\jmath_1{}^2 \bmod p$ von M_1 und ein Element $\left(-\jmath_2{}^2 - 1\right) \bmod p$ von M_2 (mit $\jmath_1, \jmath_2 \in \mathbb{Z}_p$), welche übereinstimmen, d.h. mit $\jmath_1{}^2 =_p -\jmath_2{}^2 - 1$; und daraus folgt (5). ■

4-Quadrate-Satz, Beweis

4-Quadrate-Satz: Jede natürliche Zahl kann als Summe der Quadrate von vier ganzen Zahlen geschrieben werden.

Beweis: • Teil 1: Wir zeigen, dass jede Primzahl als Summe der Quadrate von vier ganzen Zahlen geschrieben werden kann. Nun, der Fall $p = 2$ ist rasch erledigt, denn $p = 1^2 + 1^2 + 0^2 + 0^2$; daher beschäftigen wir uns im Folgenden mit dem Fall $p \ge 3$:

- Unter Verwendung der in (5) auftretenden Zahlen $\jmath_1, \jmath_2 \in \mathbb{Z}_p$ betrachten wir das 4-dimensionale Gitter $\Lambda \subset \mathbb{Z}^4$, welches durch die Vektoren $\begin{pmatrix}1\\0\\\jmath_1\\\jmath_2\end{pmatrix}, \begin{pmatrix}0\\1\\\jmath_2\\-\jmath_1\end{pmatrix}, \begin{pmatrix}0\\0\\p\\0\end{pmatrix}$ und $\begin{pmatrix}0\\0\\0\\p\end{pmatrix}$ erzeugt wird. Es ist $\det(\Lambda) = p^2$; und ein beliebiger Gitterpunkt $(x, y, z, w) \in \Lambda$ hat die Form $x = \alpha$, $y = \beta$, $z = \alpha \cdot \jmath_1 + \beta \cdot \jmath_2 + \gamma \cdot p$ und $w = \alpha \cdot \jmath_2 - \beta \cdot \jmath_1 + \delta \cdot p$ für irgendwelche $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, d.h. es gilt

$$z =_p x \cdot \jmath_1 + y \cdot \jmath_2 \quad \text{und} \quad w =_p x \cdot \jmath_2 - y \cdot \jmath_1 \quad . \tag{6}$$

- Jetzt betrachten wir die abgeschlossene Menge $C := \{(x, y, z, w) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + w^2 \le r^2 := 1.9\, p\}$, welche konvex und symmetrisch bezgl. des Nullpunkts des Koordinatensystems ist; offenbar ist $\mathrm{Vol}(C) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 \cdot 1.9^2}{2} p^2 \cong 17.8\, p^2$.

- Also ist $\mathrm{Vol}(C) \cong 17.8\, p^2 \geq 16\, p^2 = 2^d \cdot \det(\Lambda)$, womit der Gitterpunktsatz von Minkowski besagt, dass C noch (mindestens) einen von 0 verschiedenen Gitterpunkt $(x', y', z', w') \in \Lambda$ $(\Rightarrow\ x'^2 + y'^2 + z'^2 + w'^2 > 0$) enthält, welcher gemäss (6) und (5) folgende Eigenschaft besitzt:

$$x'^2 + y'^2 + z'^2 + w'^2 \overset{(6)}{\underset{p}{\rightleftharpoons}} x'^2 + y'^2 + (x' \cdot \mathrm{i}_1 + y' \cdot \mathrm{i}_2)^2 + (x' \cdot \mathrm{i}_2 - y' \cdot \mathrm{i}_1)^2$$

$$= (x'^2 + y'^2) \cdot \left(1 + \mathrm{i}_1{}^2 + \mathrm{i}_2{}^2\right) \overset{(5)}{\underset{p}{\rightleftharpoons}} 0 \quad . \tag{7}$$

- Aufgrund von (7) ist für die vier ganzen Zahlen x', y', z', w' die positive Zahl $x'^2 + y'^2 + z'^2 + w'^2$ ein (sicherlich positives) Vielfaches von p ; gemäss Definition von C ist $x'^2 + y'^2 + z'^2 + w'^2$ aber höchstens das 1.9-fache von p , also ist $x'^2 + y'^2 + z'^2 + w'^2 = p$.

- Teil 2: Wir zeigen zuerst, dass wenn n_1 , n_2 natürliche Zahlen sind, welche je als Summe der Quadrate von vier ganzen Zahlen, d.h. als $a_i^2 + b_i^2 + c_i^2 + d_i^2$ mit $i \in \{1, 2\}$, geschrieben werden können, dies auch für ihr Produkt $n_1 \cdot n_2$ gilt. Beweis:

$$n_1 \cdot n_2 = (a_1^2 + b_1^2 + c_1^2 + d_1^2) \cdot (a_2^2 + b_2^2 + c_2^2 + d_2^2)$$

$$= \left(a_1\, a_2 - b_1\, b_2 - c_1\, c_2 - d_1\, d_2\right)^2 + \left(a_1\, b_2 + b_1\, a_2 + c_1\, d_2 - d_1\, c_2\right)^2$$

$$+ \left(a_1\, c_2 + c_1\, a_2 - b_1\, d_2 + d_1\, b_2\right)^2 + \left(a_1\, d_2 + d_1\, a_2 + b_1\, c_2 - c_1\, b_2\right)^2$$

Iterativ folgt daraus sofort: Wenn die natürlichen Zahlen n_i mit $i \in \{1, 2, \ldots, m\}$ je als Summe der Quadrate von vier ganzen Zahlen geschrieben werden können, dann gilt das auch für ihr Produkt $n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_m$.

- Teil 3: Die kleinste natürliche Zahl 1 kann offensichtlich als Summe der Quadrate von vier ganzen Zahlen geschrieben werden: $1 = 1^2 + 0^2 + 0^2 + 0^2$. Und jede natürliche Zahl $n \geq 2$ ist ...
  - entweder prim und kann, gemäss Teil 1 des Beweises, daher als Summe der Quadrate von vier ganzen Zahlen geschrieben werden;
  - oder sie ist das Produkt von mindestens zwei Primzahlen und kann damit (vgl. Teile 1, 2 des Beweises) ebenfalls als Summe der Quadrate von vier ganzen Zahlen geschrieben werden. ■

Referenz

[1] J. Pach, P.K. Agarwal: Combinatorial Geometry. Wiley-Interscience Series in Discrete Mathematics and Optimization (1995)