# Der Zwei-Quadrate-Satz von Fermat

BEWEIS VON R. HEATH-BROWN UND D. ZAGIER

Uhlmann Rudolf

# Inhalt

# 1 Einleitung

Der Zwei-Quadrate-Satz von Pierre de Fermat (1607-1665) wurde von Albert Girard 1625 entdeckt und von Fermat 1640 weiter ausgebaut.

Der **Zwei-Quadrate-Satz** ist ein mathematischer Satz der Zahlentheorie:
Jede ungerade Primzahl $p$ kann genau dann als Summe zweier natürlicher Quadratzahlen

$$p = m^2 + n^2 \; ; \;\; n, m \in \mathbb{N}$$

dargestellt werden, wenn $p = 4k + 1$ mit $k \in \mathbb{N}$

Der Satz wurde von Fermat selbst nicht bewiesen. Der erste Beweis gelang 1755 Leonhard Euler (1707-1783), also etwa 100 Jahre später. Inzwischen gibt es mehrere alternative Beweise. Der Beweis in diesem Skriptum stammt von Roger Heath-Brown (1984) in der von Don Zagier überarbeiteten Form.

Der Zwei-Quadrate-Satz ist ein Abkömmling des Pythagoreischen Lehrsatzes

$$a^2 + b^2 = c^2$$

und der Frage, ob es ganzzahlige Lösungen dafür gibt. Solche ganzzahligen Lösungen nennt man „Pythagoreische Tripel“. Beispiele sind $3^2 + 4^2 = 5^2$ oder $12^2 + 5^2 = 13^2$ etc.

Beim Zwei-Quadrate-Satz stellt sich allerdings umgekehrt die Frage, welche Zahlen überhaupt für $c^2$ herauskommen können, wenn $a$ und $b$ ganzzahlig sind. Es genügt, sich auf natürliche Zahlen zu beschränken:

$$m^2 + n^2 = C \; ; \quad n, m, C \in \mathbb{N}$$

So ist $3^2 + 1^2 = 10$ und $3^2 + 2^2 = 13$, für die Zahlen $11$ und $12$ lässt sich allerdings so eine Darstellung nicht finden.

Die folgende Tabelle hebt unter den ersten Zahlen jene hervor, die als Summe zweier Quadratzahlen darstellbar sind. Z.B.: $\mathbf{0} = 0^2 + 0^2$ ; $\mathbf{1} = 0^2 + 1^2$ ; $\mathbf{2} = 1^2 + 1^2$ ; … ; $\mathbf{10} = 1^2 + 3^2$ ; …

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **0** | **1** | **2** | *3* | **4** | **5** | *6* | *7* | **8** | **9** |
| **10** | *11* | *12* | **13** | *14* | *15* | **16** | *17* | *18* | *19* |
| **20** | 21 | 22 | 23 | 24 | **25** | **26** | 27 | 28 | **29** |
| 30 | 31 | **32** | 33 | **34** | 35 | **36** | **37** | 38 | … |

*Tabelle 1*

Der Zwei-Quadrate-Satz bezieht sich nur auf Primzahlen. Es stellt sich nämlich heraus, dass letztlich die Primfaktorenzerlegung einer natürlichen Zahl bestimmt, ob diese als Summe zweier Quadratzahlen darstellbar ist oder nicht.

# 2 Definitionen und Bezeichnungen

**Quadratzahl:** Sofern nicht anders beschrieben, wird als „Quadratzahl“ immer eine natürliche Quadratzahl verstanden. $\{0, 1, 4, 9, 16, \dots\}$

Für die **Menge der natürlichen Zahlen** gibt es zwei Varianten:
$\mathbb{N}_0 = \{0,1,2,3,4,5, \dots\}$ und $\mathbb{N} = \{1,2,3,4,5, \dots\}$

Eine **Primzahl** $p$ ist eine natürliche Zahl, die nur durch $1$ und sich selbst teilbar ist.

**Restklasse und Modul:** Der Modul ist eine beliebige natürliche Zahl $M > 1$, deren Vielfache die Restklasse mit Rest $0$ definieren. Diejenigen Zahlen $n$, bei denen bezüglich der Vielfachen von $M$ derselbe Rest $r$ bleibt ( $n = M \cdot k + r$ ; $k \in \mathbb{N}_0$ ), bilden eine Restklasse.

Für $M = 7$ bildet $\{0,7,14,21,28, \dots\}$ die Restklasse $[0]_7$ mit Rest $0$.
$\{1,8,15,22,29, \dots\}$ die Restklasse $[1]_7$ mit Rest $1$.
$\{5,12,19,26,33, \dots\}$ die Restklasse $[5]_7$ mit Rest $5$.

Mit der Schreibweise $a \equiv_M b$ ($a$ kongruent $b$ bezüglich Modul $M$) wird dargelegt, dass $a$ und $b$ in der gleichen Restklasse sind. (z.B. $26 \equiv_7 5$ )

**Quadratsummenzahl:** Im Folgenden werden die natürlichen Zahlen, die sich als Summe zweier Quadratzahlen darstellen lassen, der Einfachheit halber als Quadratsummenzahlen bezeichnet.
So ist die Zahl $61$ wegen $61 = 5^2 + 6^2$ eine Quadratsummenzahl, die Zahl $62$ nicht, sie ist nicht als Summe zweier Quadratzahlen darstellbar.

**Pythagoreische Primzahl:** Eine Primzahl, die sich als Summe zweier Quadratzahlen darstellen lässt, wird in der Literatur auch als pythagoreische Primzahl bezeichnet.

# 3 Primzahlen und Restklassen

Erweitern wir Tabelle 1 und gliedern sie in Restklassen zum Modul 4.

In der blauen Spalte sind alle Vielfachen von $4$, also Zahlen der Form $4k + 0$ (Restklasse $[0]_4$) und rechts daneben in Spalten die Zahlen der Form $4k + 1$ (Restklasse $[1]_4$), $4k + 2$ (Restklasse $[2]_4$) und $4k + 3$ (Restklasse $[3]_4$), $k \in \mathbb{N}_0$.

Alle Zahlen, die sich als Summe zweier Quadratzahlen darstellen lassen, sind fett hervorgehoben. Zusätzlich sind Primzahlen grün hinterlegt. Den um die geht es ja im Zwei-Quadrate-Satz von Fermat. Diejenigen Primzahlen, die sich als Summe zweier Quadratzahlen darstellen lassen, sind dunkelgrün hinterlegt.

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | **1** | **2** | 3 | **4** | **5** | 6 | 7 | **8** | **9** | **10** | 11 | 12 | **13** | 14 | 15 | **16** | **17** | 18 | 19 |
| **20** | 21 | 22 | 23 | 24 | **25** | **26** | 27 | 28 | **29** | 30 | 31 | **32** | 33 | **34** | 35 | **36** | **37** | 38 | 39 |
| **40** | **41** | 42 | 43 | 44 | **45** | 46 | 47 | 48 | **49** | **50** | 51 | **52** | **53** | 54 | 55 | 56 | 57 | **58** | 59 |
| 60 | **61** | 62 | 63 | **64** | **65** | 66 | 67 | **68** | 69 | 70 | 71 | **72** | **73** | **74** | 75 | 76 | 77 | 78 | 79 |
| **80** | **81** | **82** | 83 | 84 | **85** | 86 | 87 | 88 | **89** | **90** | 91 | 92 | 93 | 94 | 95 | 96 | **97** | **98** | 99 |
| **100** | **101** | 102 | 103 | **104** | 105 | **106** | 107 | 108 | **109** | 110 | 111 | 112 | **113** | 114 | 115 | **116** | **117** | 118 | 119 |
| 120 | **121** | **122** | 123 | 124 | **125** | 126 | 127 | **128** | 129 | **130** | 131 | 132 | 133 | 134 | 135 | **136** | **137** | 138 | 139 |
| 140 | 141 | 142 | 143 | **144** | **145** | **146** | 147 | **148** | **149** | 150 | 151 | 152 | **153** | 154 | 155 | 156 | **157** | 158 | 159 |
| **160** | 161 | **162** | 163 | **164** | 165 | 166 | 167 | 168 | **169** | **170** | 171 | 172 | **173** | 174 | 175 | 176 | 177 | **178** | 179 |
| **180** | **181** | 182 | 183 | 184 | **185** | 186 | 187 | 188 | 189 | 190 | 191 | 192 | **193** | **194** | 195 | **196** | **197** | 198 | 199 |
| **200** | 201 | **202** | 203 | 204 | **205** | 206 | 207 | **208** | 209 | 210 | 211 | **212** | 213 | 214 | 215 | 216 | 217 | **218** | 219 |
| 220 | **221** | 222 | 223 | 224 | **225** | **226** | 227 | 228 | **229** | 230 | 231 | **232** | **233** | **234** | 235 | 236 | 237 | 238 | 239 |
| 240 | **241** | **242** | 243 | **244** | **245** | 246 | 247 | 248 | 249 | **250** | 251 | 252 | 253 | 254 | 255 | **256** | **257** | 258 | 259 |
| **260** | **261** | 262 | 263 | 264 | **265** | 266 | 267 | 268 | **269** | 270 | 271 | **272** | 273 | **274** | 275 | 276 | **277** | 278 | 279 |
| 280 | **281** | 282 | 283 | 284 | 285 | 286 | 287 | **288** | **289** | **290** | 291 | **292** | **293** | 294 | 295 | **296** | 297 | **298** | 299 |
| 300 | 301 | 302 | 303 | 304 | **305** | **306** | 307 | 308 | 309 | 310 | 311 | 312 | **313** | **314** | 315 | 316 | **317** | 318 | 319 |
| **320** | 321 | 322 | 323 | **324** | **325** | 326 | 327 | **328** | 329 | 330 | 331 | 332 | **333** | 334 | 335 | 336 | **337** | **338** | 339 |
| **340** | 341 | 342 | 343 | 344 | 345 | **346** | 347 | 348 | **349** | 350 | 351 | 352 | **353** | 354 | 355 | **356** | **357** | 358 | 359 |
| **360** | **361** | **362** | 363 | 364 | **365** | 366 | 367 | 368 | **369** | **370** | 371 | 372 | **373** | 374 | 375 | 376 | **377** | 378 | 379 |
| 380 | 381 | 382 | 383 | 384 | 385 | **386** | 387 | **388** | **389** | 390 | 391 | **392** | 393 | **394** | 395 | 396 | **397** | 398 | 399 |
| **$\equiv_4 0$** | **$\equiv_4 1$** | **$\equiv_4 2$** | **$\equiv_4 3$** | **$\equiv_4 0$** | **$\equiv_4 1$** | **$\equiv_4 2$** | **$\equiv_4 3$** | **$\equiv_4 0$** | **$\equiv_4 1$** | **$\equiv_4 2$** | **$\equiv_4 3$** | **$\equiv_4 0$** | **$\equiv_4 1$** | **$\equiv_4 2$** | **$\equiv_4 3$** | **$\equiv_4 0$** | **$\equiv_4 1$** | **$\equiv_4 2$** | **$\equiv_4 3$** |
| **4k+0** | **4k+1** | **4k+2** | **4k+3** | **4k+0** | **4k+1** | **4k+2** | **4k+3** | **4k+0** | **4k+1** | **4k+2** | **4k+3** | **4k+0** | **4k+1** | **4k+2** | **4k+3** | **4k+0** | **4k+1** | **4k+2** | **4k+3** |

*Tabelle 2*

Die Tabelle legt nahe, dass alle Primzahlen der Restklasse $[1]_4$, also der Form $p = 4k + 1$, als Summe zweier Quadratzahlen darstellbar sind.

Bevor wir uns dieser Restklasse widmen, überlegen wir, wie das bezüglich der anderen Restklassen aussieht.

## 3.1 Primzahlen aus den Restklassen $[0]_4$ und $[2]_4$

Die Restklasse $[0]_4$ sind die Vielfachen von $4$ und daher befindet sich darunter keine Primzahl. Die Restklasse $[2]_4$ besteht nur aus geraden Zahlen und beinhaltet somit nur die Primzahl $2$.
Der Zwei-Quadrate-Satz von Fermat bezieht sich nur auf ungerade Primzahlen und die befinden sich ausschließlich in $[1]_4$ und $[3]_4$.

## 3.2 Primzahlen der Restklasse $[3]_4$

Wir sehen, dass sich die Primzahlen in zwei Gruppen teilen. Nämlich in die der Restklasse $[1]_4$ und in die der Restklasse $[3]_4$. In der Restklasse $[3]_4$ gibt es offensichtlich überhaupt keine Quadratsummenzahlen.

**Satz 1** Zahlen der Restklasse $[3]_4$ sind keine Quadratsummenzahlen.

$$C \neq m^2 + n^2 \text{ ; für alle } m, n \in \mathbb{N}_0.$$

**Beweis:** Seien $m$ und $n$ Vielfache $(k)$ der Zahl 4 plus einem Rest $(r)$.

$$m = 4k_1 + r_1 \quad \text{und} \quad n = 4k_2 + r_2\,, \quad k_i, r_i \in \mathbb{N}_0,$$

dann gilt für die Quadrate

$$m^2 = 4 \cdot (\dots) + r_1^2 \quad \text{und} \quad n^2 = 4 \cdot (\dots) + r_2^2$$

Die Reste können bezüglich Modul $4$ die Werte $0, 1, 2$ und $3$ annehmen. Für Quadratzahlen kommen nur die Reste $0$ und $1$ in Betracht, da $0^2 \equiv_4 0$, $1^2 \equiv_4 1$, $2^2 \equiv_4 0$ und $3^2 \equiv_4 1$.

Für die Summe zweier Quadratzahlen

$$m^2 + n^2 = \dots = 4 \cdot (\dots) + r_1^2 + r_2^2$$

gibt es deshalb nur die Reste $0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 2$, aber nie $3$. □

## 3.3 Primzahlen aus der Restklasse $[1]_4$

In dieser Restklasse liegen angeblich alle ungeraden Primzahlen, die als Summe von Quadratzahlen darstellbar sind. Genau das besagt auch der Zwei-Quadrate-Satz von Fermat.

Nachdem wir schon bewiesen haben, dass die Restklassen $[0]_4$, $[2]_4$ und $[3]_4$ keine Primzahlen enthalten können, die als Quadratsumme darstellbar sind, wird das Gegenteil nun für Restklasse $[1]_4$ zu beweisen sein.

# 4 Der Zwei-Quadrate-Satz

**Satz 2** (**Zwei-Quadrate-Satz**)
Jede ungerade Primzahl $p$ kann genau dann als Summe zweier natürlicher Quadratzahlen

$$p = m^2 + n^2 \; ; \;\; n, m \in \mathbb{N}$$

dargestellt werden, wenn $p = 4k + 1$ mit $k \in \mathbb{N}$

Bemerkung: Da $p$ eine Primzahl, sind daher $m, n \neq 0$. Ansonsten wäre $p$ eine Quadratzahl, was eine Primzahl nicht sein kann.

## 4.1 Der Beweis

Im ersten Teil des Beweises wird **Satz 2** in einer alternativen Form neu formuliert.

Alle Primzahlen $p > 2$ sind ungerade. Damit die Quadratsumme $m^2 + n^2$ ungerade ist, muss einer der beiden Summanden ungerade und der andere gerade sein.
O.E.d.A. sei dies $m^2$. Wenn $m^2 \in \mathbb{N}_u$ und $n^2 \in \mathbb{N}_g$, dann auch $m \in \mathbb{N}_u$ und $n \in \mathbb{N}_g$. Für $n$ lässt sich dann $n = 2y \;\; (y \in \mathbb{N})$ schreiben. Somit bekommen wir

$$\begin{aligned} p &= m^2 + (2y)^2 = \\ &= m^2 + 4y^2 = \\ &= x^2 + 4y^2 \end{aligned}$$

Die Umbenennung von $m$ in $x$ dient dabei nur kosmetischen Gründen.

Die weitere Vorgangsweise ist von der Sorte „Trick 17“ 😉 !

### 4.1.1 „Trick 17“

Die Grundidee stammt von Roger Heath-Brown (1971), die heute bekannte Version stammt von Don Zagier.

Der Trick besteht darin, den **Ausdruck $p = x^2 + 4y^2$** als **Spezialfall** von $p = x^2 + 4yz$ mit $y = z$ zu verstehen. Sehr anschaulich wird das Ganze, wenn man das Problem **graphisch interpretiert**.

Es wird also für den zweiten Summanden keine Quadratzahl gesucht, sondern versucht, den allgemeineren Fall $p = x^2 + 4yz$ zu lösen und nebenbei auch auf eine Lösung mit $y = z$ zu stoßen.

DREI BEISPIELE:

| **73** | | | | |
|---|---|---|---|---|
| **x** | **$x^2$** | **+** | **4 ·** | **y · z** |
| 1 | 1 | + | 4 · | 18 |
| 3 | 9 | + | 4 · | 16 |
| 5 | 25 | + | 4 · | 12 |
| 7 | 49 | + | 4 · | 6 |

| **149** | | | | |
|---|---|---|---|---|
| **x** | **$x^2$** | **+** | **4 ·** | **y · z** |
| 1 | 1 | + | 4 · | 37 |
| 3 | 9 | + | 4 · | 35 |
| 5 | 25 | + | 4 · | 31 |
| 7 | 49 | + | 4 · | 25 |
| 9 | 81 | + | 4 · | 17 |
| 11 | 121 | + | 4 · | 7 |

| **271** | | | | |
|---|---|---|---|---|
| **x** | **$x^2$** | **+** | **4 ·** | **y · z** |
| 1 | 1 | + | 4 · | 68 |
| 3 | 9 | + | 4 · | 66 |
| 5 | 25 | + | 4 · | 62 |
| 7 | 49 | + | 4 · | 56 |
| 9 | 81 | + | 4 · | 48 |
| 11 | 121 | + | 4 · | 38 |
| 13 | 169 | + | 4 · | 26 |
| 15 | 225 | + | 4 · | 12 |

*Tabelle 3*

Für $p = 73$ findet man 21 Lösungen $(x, y, z)$. Sie sind in Tabelle 4 angeführt. Eine davon ist von der Form $y = z$. Somit kann 73 als Summe zweier Quadratzahlen dargestellt werden:

$$73 = 9 + 4 * 16 = 3^2 + 8^2.$$

| **73** | | | | |
|---|---|---|---|---|
| **x** | **$x^2$** | **+** | **4 ·** | **y · z** |
| 1 | 1 | + | 4 · | 18 |
| 3 | 9 | + | 4 · | 16 |
| 5 | 25 | + | 4 · | 12 |
| 7 | 49 | + | 4 · | 6 |

| LÖSUNGEN für $p = 73$ | | | | | |
|---|---|---|---|---|---|
| (1,1,18) | (1,18,1) | (1,3,6) | (1,6,3) | (1,9,2) | (1,2,9) |
| (3,1,16) | (3,16,1) | (3,2,8) | (3,8,2) | **(3, 4, 4)** | |
| (5,1,12) | (5,12,1) | (5,3,4) | (5,4,3) | (5,2,6) | (5,6,2) |
| (7,1,6) | (7,6,1) | (7,3,2) | (7,2,3) | | |

*Tabelle 4*

### 4.1.2 Die ersten Beweisschritte

① Die Gleichung $p = x^2 + 4yz$ hat nur endlich viele Lösungen.

Dies ist darin begründet, dass $x, y, z$ alle kleiner als $p$ sind und die Anzahl der Variationen dieser Zahlen den Wert $p^3$ nicht übersteigen kann.

② Die Gleichung $p = x^2 + 4yz$ hat mindestens zwei Lösungstripel.

Da $p = 4k + 1 = 1^2 + 4 \cdot 1 \cdot k$, sind dies die Lösung $(1,1,k)$ und $(1,k,1)$.
Für 73 also $(1,1,18)$ und $(1,18,1)$.

③ **Man beachte die Anzahl der Lösungen.** Sie ist fast immer gerade.

Der Grund dafür ist, dass das Vertauschen von $y$ und $z$ ja immer auch immer eine Lösung ist. Das heißt, die **Lösungen kommen paarweise vor**.

Es gibt eine **einzige Ausnahme**! Wenn $\boldsymbol{y = z}$ ist!!!

$$yz = 18 = \begin{matrix} 1 \cdot 18 & 18 \cdot 1 \\ 2 \cdot 9 & 9 \cdot 2 \\ 3 \cdot 6 & 6 \cdot 3 \end{matrix} \qquad yz = 16 = \begin{matrix} 1 \cdot 16 & 16 \cdot 1 \\ 2 \cdot 8 & 8 \cdot 2 \\ 4 \cdot 4 & \end{matrix}$$

④ **Folgerung** bezüglich der Anzahl der Lösungstripel $(x, y, z)$ der Gleichung $p = x^2 + 4yz$ für eine bestimmte Primzahl $p$.

**Ist die Anzahl der Lösungen ungerade, dann** liegt das an der Existenz einer Lösung $(x, y, y)$. In diesem Fall **kann die Primzahl $\boldsymbol{p}$ dann als**

$$p = x^2 + 4y^2 = x^2 + (2y)^2 = \\ = m^2 + n^2$$

**geschrieben werden!**

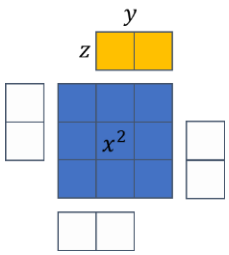
### 4.1.3 Die geometrische Interpretation

Hier kommt die geometrische Interpretation ins Spiel. Dabei wird die Gleichung $p = x^2 + 4yz$ als Summe eines Quadrats mit vier Rechtecken verstanden.

$x^2$ steht für den Flächeninhalt des Quadrats und $y$ für die Breite sowie $z$ für die Höhe der vier Rechtecke. Die Rechtecke sind so um das Quadrat gelegt, wie dargestellt. Damit ergibt sich eine geschlossene Fläche ohne Überschneidungen, in ihrer Form an Windmühlen erinnernd, deren Flächeninhalt die darzustellende Zahl $p$ beschreibt.

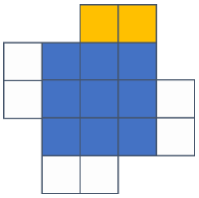
Einige Beispiele: (Zur Erinnerung, $x$ ist ungerade)

$17 = x^2 + 4yz$

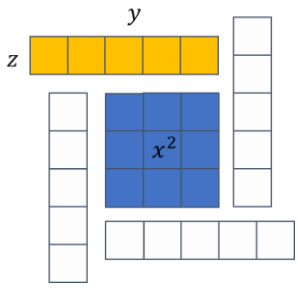



$17 = 3^2 + 4 \cdot 2 \cdot 1$

*Eine Lösung für* $p = 17$: $(3,2,1)$

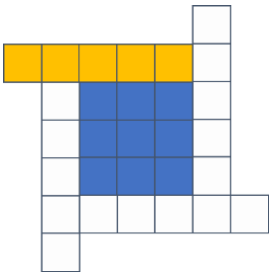


$29 = x^2 + 4yz$




$29 = 3^2 + 4 \cdot 5 \cdot 1$

*Eine Lösung für* $p = 29$: $(3,5,1)$

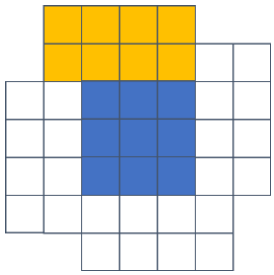


$41 = x^2 + 4yz$

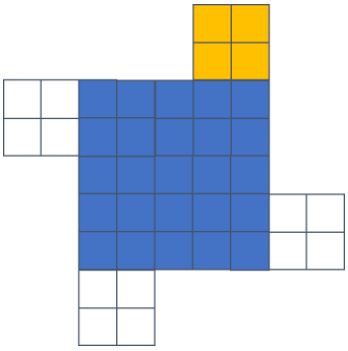
*Eine Lösung für* $p = 41$: $(3,4,2)$

*Die zweite Lösung zeigt, dass* $41$ *eine Quadratsummenzahl ist!*

$41 = 5^2 + 4 \cdot 2^2 =$
$= 5^2 + 4^2$



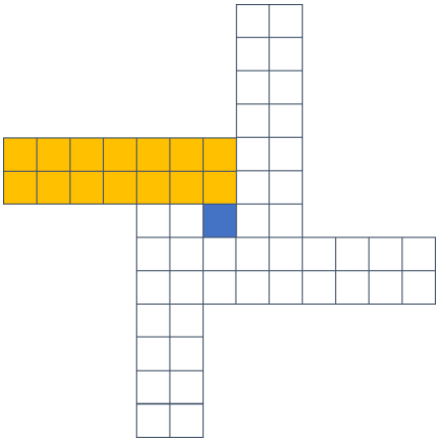
*Eine weitere Lösung*: $(5,2,2)$



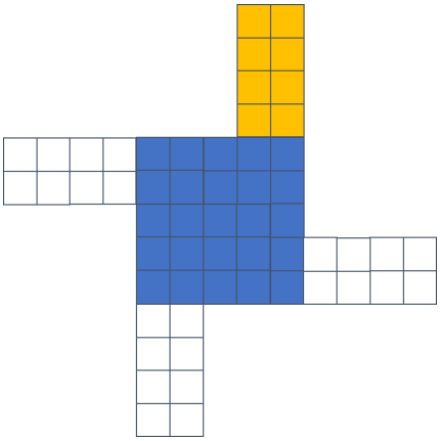
$57 = x^2 + 4yz$

*57 ist keine Primzahl, aber trotzdem von der Form $4k + 1$.*

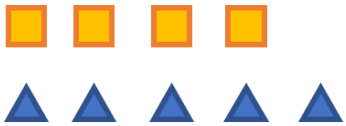
*Eine Lösung für* $57$: $(1,7,2)$



*Eine weitere Lösung*: $(5,2,4)$



Ob eine Anzahl gerade oder ungerade ist, kann man klären, indem man die Elemente in Paaren gruppiert. Wenn dabei eines übrig bleibt, ist die Anzahl ungerade.



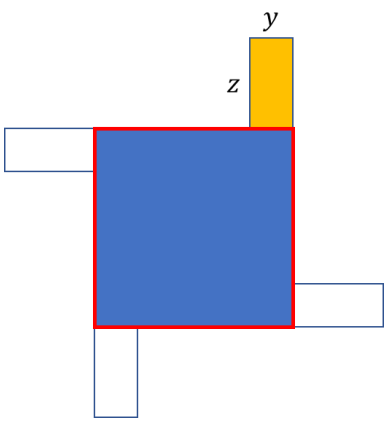
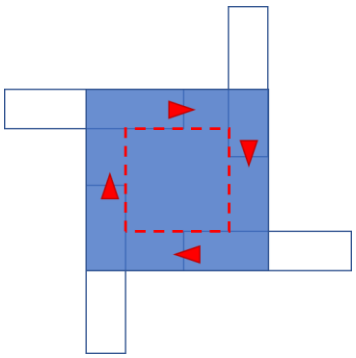
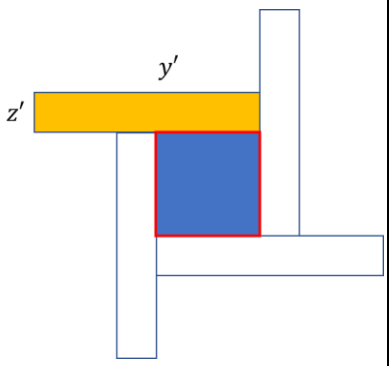
Für die Gruppierung der Lösungen von $p = x^2 + 4yz$ in Paaren haben Heath-Brown und Zagier eine geniale Methode gefunden.

| Zu jeder Lösung existiert nämlich genau eine zweite Lösung mit kongruenter Gesamtfläche. |
|---|

Inwiefern dem so ist und wie man diese „kongruente Lösung“ findet, wird im Folgenden beschrieben.

**FALL 1:** $y < x/2$

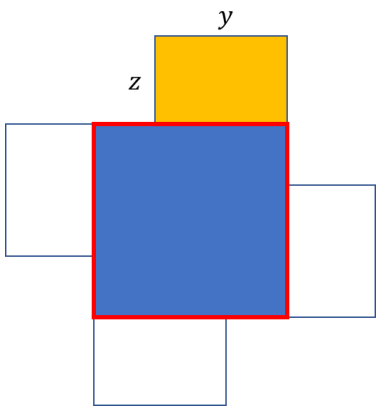
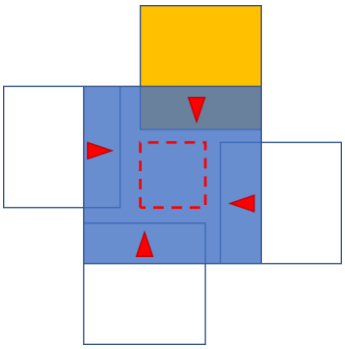
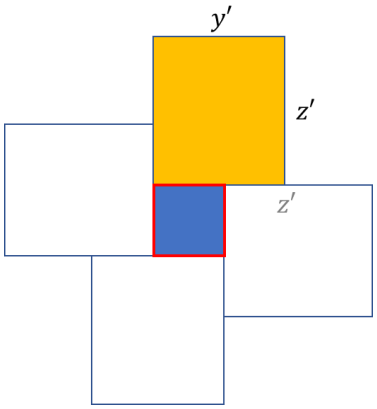
FORM

| Lösung | Transformation | Partnerlösung |
|---|---|---|
|   |  |   |

$z$ nach innen maximal vergrößern, so entsteht die zweite kongruente Lösung.

**FALL 2:** $\frac{x}{2} < y < x$

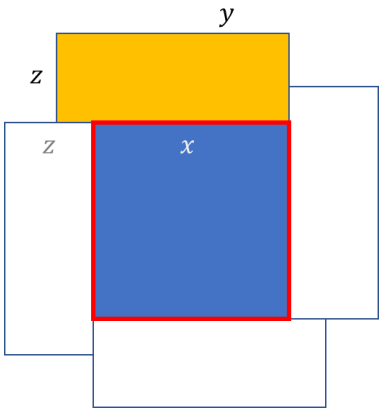
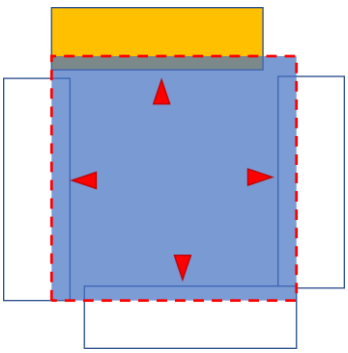
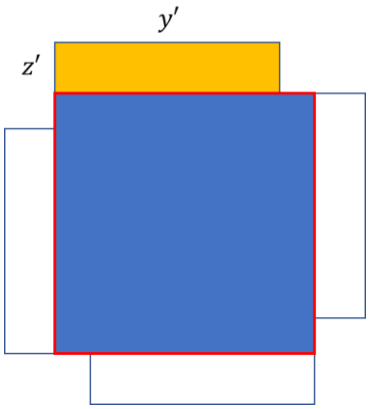
FORM

| Lösung | Transformation | Partnerlösung |
|---|---|---|
|  |  |  |

$z$ nach innen maximal vergrößern, so entsteht die zweite kongruente Lösung.

**FALL 3:** $x < y < x + z$

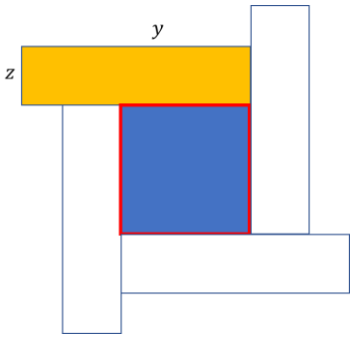
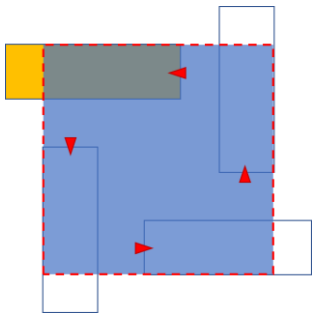
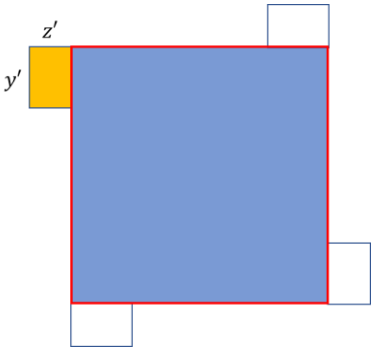
FORM

| Lösung | Transformation | Partnerlösung |
|---|---|---|
|  |  |  |

$z$ nach außen maximal verkleinern, so entsteht die zweite kongruente Lösung.

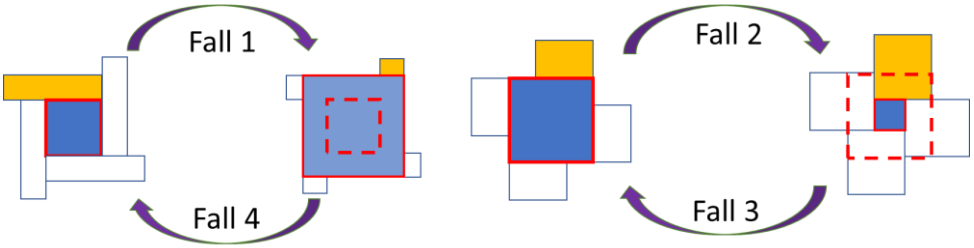
**FALL 4:** $y > x + z$

FORM 

| Lösung | Transformation | Partnerlösung |
|---|---|---|
|   |  |   |

$y$ nach außen maximal verkleinern, so entsteht die zweite kongruente Lösung.

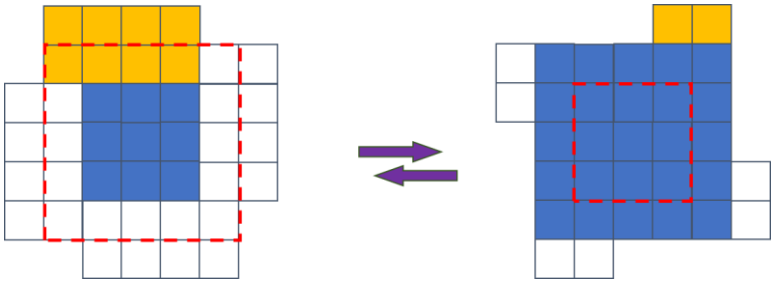
!!! **Durch diese Zuordnung werden die Lösungen paarweise zusammengeführt** !!!




Die Zuordnung als Funktion von $S \rightarrow S = \{(x, y, z) \in \mathbb{N}^3 : p = x^2 + 4yz\}$

$$(x,y,z) \mapsto \begin{cases} (x-2y, x-y+z, y) & \text{für } y < \frac{x}{2} \quad Fall\ 1 \\ (2y-x, y, x-y+z) & \text{für } \frac{x}{2} < y < x+z \quad Fall\ 2\&3 \\ (x+2z, z, y-z-x) & \text{für } y > x+z \quad Fall\ 4 \end{cases}$$

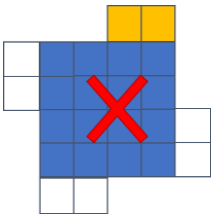
Beispiel (Fall 2&3):



$$(3,4,2) \mapsto (2 \cdot 4 - 3, 4, 3 - 4 + 2) = (5,4,1)$$
$$(5,4,1) \mapsto (2 \cdot 4 - 5, 4, 5 - 4 + 1) = (3,4,2)$$

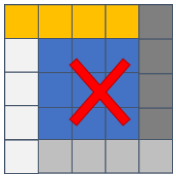
### 4.1.4 Die Spezialfälle

$y = \frac{x}{2}$



Da $x$ ungerade vorausgesetzt wird,
ist dies keine Lösung im Sinne des
Zwei-Quadrate-Satzes!

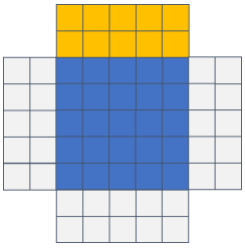
$y = x + z$



Dies Darstellung stellt keine Primzahl dar.
Da $p$ eine Primzahl ist, kann die Gesamtfläche
$p = x^2 + 4yz$ keine Quadratzahl sein.

**Die Kreuzlösung, der wesentliche Spezialfall !!!**

$y = x$



In diesem Fall ist die Zahl $x^2 + 4yz = x^2 + 4xz = x(x + 4z)$
durch $x$ teilbar.

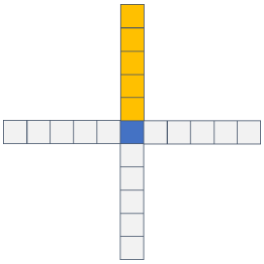
Diese Lösung ist der einzige Fixpunkt der Zuordnung. Sie wird auf sich selbst abgebildet und deshalb nur einmal gezählt.

Somit ist die Behauptung von weiter oben …
*„Zu jeder Lösung existiert genau eine zweite Lösung mit kongruenter Gesamtfläche.“*
nicht unbedingt richtig. Es gibt auch Lösungen ohne Partner.

### 4.1.5 Die Anzahl der Lösungen für $p = 4k + 1$ ist ungerade

Die Frage ist allerdings, ob eine Primzahl solche Fixpunktlösungen überhaupt hat. Das ist entscheidend. Gibt es sie und gibt es nur eine Fixpunktlösung, dann ist die Anzahl aller Lösungen ungerade, ansonsten gerade.

Da diese Lösung durch $x$ teilbar ist und wir Primzahlen betrachten, sind für $x$ nur die Werte $x = 1$ oder $x = p$ möglich.
Die Lösung mit $x = y = p \implies p = p^2 + 4pz \implies z < 0$ widerspricht den Voraussetzungen.
Die Lösung mit $x = y = 1 \implies p = 1^2 + 4 \cdot 1 \cdot z = 1 + 4z$ ist nicht für alle Primzahlen gültig, aber sehr wohl für alle Primzahlen der Form $p = 4k + 1 = 1 + 4 \cdot 1 \cdot k$.



Diese „Kreuzlösung“ gibt es für $p$ aus der Restklasse $[1]_4$ ja immer! Das $4k$ außen und die $1$ in der Mitte. Und klarerweise ist sie die einzige Fixpunktlösung. Jede andere Kreuzlösung würde eine Teilbarkeit von $p$ durch $x$ bedeuten!

| Damit ist die Anzahl der Lösungen der Gleichung $p = x^2 + 4xy$ für $p \in [1]_4$ immer ungerade. |
|---|

### 4.1.6 Letzter Beweisschritt

⑤ In der Gleichung $p = 1 + 4yz$ hat jede Primzahl der Form $p = 4k + 1$ eine ungerade Anzahl an Lösungen.

Aus geometrischer Sicht ist es die Kreuzlösung, die partnerlos ist. Aus algebraischer Sicht ist es die Lösung $(x, y, y)$. Wie diese im Detail aussieht, ist nicht wesentlich und auch meistens nicht bekannt, aber es gibt sie.

Daraus folgt für alle Primzahlen der Form $p = 4k + 1$, dass sie in der Form

$$\begin{aligned} p &= x^2 + 4yy \\ &= x^2 + 4y^2 = \\ &= x^2 + (2y)^2 = \\ &= m^2 + n^2 \end{aligned}$$

als Summe zweier Quadrate geschrieben werden können!

QUOD ERAT DEMONSTRANDUM □

# 5 Ausblick: Der allgemeine Zwei-Quadrate-Satz

Wann ist allgemein eine natürliche Zahl als Summe zweier Quadrate darstellbar? Hier noch einmal die Tabelle der ersten Zahlen.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **0** | **1** | **2** | *3* | **4** | **5** | *6* | *7* | **8** | **9** |
| **10** | *11* | *12* | **13** | *14* | *15* | **16** | *17* | *18* | *19* |
| **20** | 21 | 22 | 23 | 24 | **25** | **26** | 27 | 28 | **29** |
| 30 | 31 | **32** | 33 | **34** | 35 | **36** | **37** | 38 | … |
| 0 | 1 | **2** | 3 | **4** | 5 | **6** | **7** | 8 | 9 |
| 10 | 11 | **12** | 13 | **14** | 15 | **16** | **17** | 18 | 19 |
| 20 | 21 | **22** | 23 | **24** | 25 | **26** | **27** | 28 | 29 |
| 30 | 31 | **32** | 33 | **34** | 35 | **36** | **37** | 38 | … |

Jede natürliche Zahl $N \in \mathbb{N}$ hat eine eindeutige Primfaktorenzerlegung

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n \cdot \bar{p}_1 \cdot \bar{p}_2 \cdot \ldots \cdot \bar{p}_m \, .$$

Dabei seien die Primzahlen $p_i$ von der Form $p_i = 4k + 1$ oder $p_i = 2$ (das sind die „Guten“ 😊) und die Primzahlen $p_j$ von der Form $\bar{p}_j = 4k + 3$.

**Satz 3** Die Multiplikation zweier Quadratsummenzahlen ist wieder eine Quadratsummenzahl.

**Beweis:**
Seien $u = a^2 + b^2$ und $v = c^2 + d^2$ Quadratsummenzahlen.

$$\begin{aligned} u \cdot v &= (a^2 + b^2)(c^2 + d^2) = \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 = \\ &= (ac)^2 + 2acbd + (bd)^2 + (ad)^2 - 2adbc + (bc)^2 = \\ &= (ac + bd)^2 + (ad - bc)^2 \quad \square \end{aligned}$$

**Folgerung:**
Der erste Teil der Primfaktorenzerlegung

$$N = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) \cdot (\bar{p}_1 \cdot \bar{p}_2 \cdot \ldots \cdot \bar{p}_m)$$

bildet eine Quadratsummenzahl.

**Satz 4** Jede Quadratzahl ist eine Quadratsummenzahl.

**Beweis:**
$a^2 = a^2 + 0^2$ $\square$

**Folgerung:**
Auch die Primfaktorenpotenzen $\bar{p}_j{}^2$ und damit auch $\bar{p}_j{}^{2n}$ sind Quadratsummenzahlen.

**Satz 5 Allgemeiner Zwei-Quadrate-Satz**
Eine natürliche Zahl ist genau dann als Summe zweier Quadratzahlen darstellbar, wenn ihre Primfaktoren der Form $4n + 3$ alle in geraden Potenzen auftreten.

Beispiel:
$96040 = 2^3 \cdot 5 \cdot 7^4 = 294^2 + 98^2$

**Beweisskizze:** (Der Beweis kann hier nur teilweise wiedergegeben werden.)

„genau dann“ bedeutet „$\Leftrightarrow$“

„$\Rightarrow$“:
*„Die Primfaktoren einer natürlichen Zahl der Form $4n + 3$ treten alle in geraden Potenzen auf $\Rightarrow$ Die natürliche Zahl ist als Summe zweier Quadratzahlen darstellbar.“*

Dies geht aus 0 und der Folgerung von Satz 4 hervor.

„$\Leftarrow$“
*„Die natürliche Zahl ist als Summe zweier Quadratzahlen darstellbar $\Rightarrow$ Die Primfaktoren einer natürlichen Zahl der Form $4n + 3$ treten alle in geraden Potenzen auf“*

Der Beweis dieser Implikation erfordert noch mehr Wissen über Restklassenringe von Primzahlen und sprengt den hier gesteckten Rahmen. ☹

# 6 Literaturverzeichnis


Kreck, M. (18. 07 2016). The One Sentence Proof (in multiple sentences) - Numberphile. Von https://www.youtube.com/watch?v=yGsIw8LHXM8&t=454s abgerufen

*mathoverflow.net*. (2011). Von https://mathoverflow.net/questions/31113/zagiers-one-sentence-proof-of-a-theorem-of-fermat abgerufen

Polster, B. (25. 01 2020). Why was this visual proof missed for 400 years? (Fermat's two square theorem). Von https://www.youtube.com/watch?v=DjI1NICfjOk&t=1196s abgerufen

Weitz, E. (28. 01 2018). Der Zwei-Quadrate-Satz von Fermat. Von https://www.youtube.com/watch?v=6r3X7r-wUnQ abgerufen

*Welche natürlichen Zahlen lassen sich als Summe zweier Quadrate ganzer Zahlen schreiben?* (06. 03 2010). Von Matroids Matheplanet: https://matheplanet.de/default3.html?article=1324 abgerufen