5. Summen von Quadraten.

Wir interessieren uns hier für die Frage, ob sich eine (natürlich positive) Zahl n als Summe von sagen wir t Quadraten ganzer Zahlen schreiben lässt, oder auch, genauer, für die Anzahl der Möglichkeiten, n als Summe von t Quadraten zu schreiben.

5.1. Summen von zwei Quadratzahlen.

5.1.1. Satz. *Sei $n \in \mathbb{N}$. Genau dann gibt es natürliche Zahlen x, y mit $x^2+y^2 = n$, wenn jeder Primteiler p von n mit $p \equiv 3 \mod 4$ mit geradem Exponenten auftritt,* das heißt: Ist $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen p_i, und ist $p_i \equiv 3 \mod 4$, so ist $e_i \equiv 0 \mod 2$.

Dieser Satz wird meist A. GIRARD (1595-1632) oder FERMAT (1601-1605) zugeschrieben. Der erste publizierte Beweis stammt von EULER (1754). Kern dieses Satzes ist die folgende Aussage:

5.1.2. *Ist p eine Primzahl mit $p \equiv 1 \mod 4$, so gibt es $x, y \in \mathbb{N}$ mit $x^2+y^2 = p$.*

In 5.1.5 werden wir sehen, dass diese Darstellung sogar bis auf die Reihenfolge der Summanden eindeutig ist!

Der Beweis erfolgt in mehreren Schritten. Zuerst zeigen wir:

(1) *Ist $x^2+y^2 = n$, so ist $n \not\equiv 3 \mod 4$.*

Beweis. Für jede natürliche Zahl x gilt $x^2 \equiv 0$ or $\equiv 1 \mod 4$ (denn $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{0}$, $\overline{3}^2 = \overline{1}$).

(1′) *Ist also $x^2+y^2 = p$ eine Primzahl, so ist $p = 2$ oder $p \equiv 1 \mod 4$.*

(2) *Sei p eine Primzahl. Ist $p = 2$ oder $p \equiv 1 \mod 4$, so gibt es $s^2 \equiv -1 \mod p$.*

Beweis: Ist $p = 2$, so wähle $s = 1$. Es ist $s^2 = 1 \equiv -1 \mod 2$. Ist p Primzahl mit $p \equiv 1 \mod 4$, so ist $\left(\frac{-1}{p}\right) = 1$ (siehe Teil 4), also gibt es s mit $s^2 \equiv -1 \mod p$.

Sei nun n eine natürliche Zahl.

(3) *Sei $s^2 \equiv -1 \mod n$. Sind $x, y \in \mathbb{Z}$ mit $y \equiv sx \mod n$, so gilt $x^2+y^2 \equiv 0 \mod n$.*

Beweis: Aus $y \equiv sx \mod n$ folgt

$$x^2 + y^2 \equiv x^2 + (sx)^2 = (1+s^2)x^2 \equiv 0 \mod n.$$

(4) *Sei $s^2 \equiv -1 \mod n$. Es gibt $x, y \in \mathbb{N}_0$ mit $x^2+y^2 = n$ und $y \equiv sx \mod n$.*

Beweis: Betrachte die Paare $[x, y]$ ganzer Zahlen mit $0 \le x \le \sqrt{n}$ und $0 \le y < \sqrt{n}$. *Die Anzahl dieser Paare $[x, y]$ ist größer als n.* Um dies zu zeigen, unterscheiden

wir zwei Fälle: Ist n keine Quadratzahl, so ist die Anzahl dieser Paare $(\lfloor\sqrt{n}\rfloor+1)^2 > n$ (denn jeder der beiden Faktoren ist $\lfloor\sqrt{n}\rfloor+1 > \sqrt{n}$). Ist n Quadratzahl, so hat man $\sqrt{n}+1$ Möglichkeiten für x und $\sqrt{n}$ Möglichkeiten für y, also insgesamt $(\sqrt{n}+1)\sqrt{n} > n$ Möglichkeiten.

Zu jedem Paar $[x,y]$ betrachte die Zahl $y-sx$, oder besser ihre Restklasse modulo n. Es gibt mehr als n Paare, aber nur n Restklassen: Also sind zwei der Zahlen $y-sx$ modulo n äquivalent (**Dirichlet'sches Schubfachprinzip**), etwa

$$y' - sx' \equiv y'' - sx'' \mod n.$$

Sei $y = y' - y''$, und $x = x' - x''$. Es ist

$$y = y' - y'' \equiv sx' - sx'' = s(x' - x'') = sx \mod n.$$

Da die beiden Zahlen x', x'' zwischen 0 und $\sqrt{n}$ liegen, sehen wir, dass für ihre Differenz $x = x' - x''$ gilt $|x| \le \sqrt{n}$. Wäre $x = 0$, so wäre $y \equiv 0 \mod n$, also hätten wir sowohl $x' = x''$, also auch $y' \equiv y'' \mod n$, also $y' = y''$, im Widerspruch zur Wahl der Paare (x', y') und (x'', y''). Also

$$0 < |x| \le \sqrt{n}.$$

Wegen $0 \le y' < \sqrt{n}$ und $0 \le y'' < \sqrt{n}$ folgt für die Differenz $y = y' - y''$, dass gilt

$$0 \le |y| < \sqrt{n}.$$

Insgesamt erhalten wir

$$0 < x^2 + y^2 < 2n.$$

Aus $y \equiv sx \mod n$ folgt nach (3), dass $x^2 + y^2$ ein Vielfaches von n ist. Also ist $x^2 + y^2 = n$.

(5) *Sei $x^2 + y^2 = n$ mit $(x,y) = 1$. Sei p ein Teiler von n. Dann ist $\left(\frac{-1}{p}\right) = 1$,* also $p = 2$ oder $p \equiv 1 \mod 4$.

Beweis: Wegen $(x,y) = 1$ ist p kein Teiler von x (denn sonst wäre p Teiler von x und n, also auch von y). Also gibt es t mit $tx \equiv 1 \mod p$. Es ist $y^2 \equiv -x^2 \mod p$, also

$$(ty)^2 = t^2y^2 \equiv -t^2x^2 \equiv -1 \mod p,$$

wie behauptet.

(6) *Die Menge $Q = \{n \in \mathbb{N} \mid$ es gibt $x, y \in \mathbb{N}_0$ mit $n = x^2 + y^2\ \}$ ist abgeschlossen unter Multiplikation.*

Genauer: Es gilt

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

Beweis 1: Nachrechnen.

Beweis 2: Interpretiere a^2+b^2 als $\det \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ und verwende den Produktsatz für Determinanten von Matrizen.

Beweis 3: Interpretiere a^2+b^2 als Norm $N(a+bi)=|a+bi|^2$ der komplexen Zahl $a+bi \in \mathbb{C}$ und verwende die Produktregel für den Betrag einer komplexen Zahl.
(Alle diese Beweise sind natürlich nur verschiedene Interpretationen der gleichen Rechnung.)

Beweis des Satzes. Sei $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen p_i, gegeben, und es gelte: ist $p_i \equiv 3 \mod 4$, so ist $e_i \equiv 0 \mod 2$. Dann können wir n in der Form $n = d^2 n_1 \cdots n_m$ schreiben, wobei also d eine Quadratzahl und jedes n_i mit $1 \le i \le m$ eine Primzahl p mit $p=2$ oder $p \equiv 1 \mod 4$. Wegen $(1')$ und (4) wissen wir, dass jedes n_i zu Q gehört, natürlich gehört auch d^2 zu Q. Also gehört nach (6) auch n zu Q.

Umgekehrt setzen wir nun voraus, dass es x, y gibt mit $x^2+y^2=n$. Sei $d=(x,y)$ und $x_0 = \frac{x}{d}$, $y_0 = \frac{y}{d}$ und $n_0 = \frac{n}{d^2}$. Dann ist $x_0^2 + y_0^2 = n_0$, und $(x_0, y_0) = 1$. Nach (4) besitzt n_0 nur Primteiler p mit $p=2$ oder $p \equiv 1 \mod 4$. Wegen $n = d^2 n_0$ sehen wir, dass jeder Primteiler p von n mit $p \equiv 3 \mod 4$ in n mit geradem Exponenten auftreten muss.

Zweiter Beweis von 5.1.2. Hier ist ein zweiter Beweis für die Existenzaussage in 5.1.2.

Sei also $p=2$ oder $p \equiv 1 \mod 4$. Es gibt s mit $s^2 \equiv -1 \mod p$ (siehe (2), dabei können wir $0 < s < p$ voraussetzen. Sei $x=1$, und $y = s = s \cdot 1$. Dann gilt nach (3) $x^2+y^2 \equiv 0 \mod p$, also $x^2+y^2 = ap$ für ein a. Natürlich ist $a > 0$. Wegen $s < p$, ist $1+s^2 < p^2$, also ist $a < p$. Wir sehen also: *Es gibt* x_1, x_2 *mit*

$$x_1^2 + x_2^2 = ap, \quad \text{mit } 0 < a < p.$$

Wir zeigen: Ist $a \neq 1$, so findet man y_1, y_2 mit $y_1^2 + y_2^2 = a'p$ und $0 < a' < a$. (Mit diesem **Abstiegsalgorithmus** kann man also nach endlich vielen Schritten erreichen, dass $a=1$ gilt.)

Sei $a > 1$. Wir betrachten Restklassen modulo a, und zwar wählen wir jeweils betragsmäßig kleinste Representanten, also wähle z_i mit $z_i \equiv x_i \mod a$ und $|z_i| \le \frac{a}{2}$, für $i = 1, 2$. Wären x_1, x_2 beide durch a teilbar, so wäre $ap = x_1^2 + x_2^2$ durch a^2 teilbar, also $a|p$. Aber p ist eine Primzahl und $1 < a < p$. Dies zeigt, dass mindestens eine der beiden Zahlen x_1, x_2 nicht durch a teilbar ist, also ist mindestens eine der Zahlen z_1, z_2 von Null verschieden. Wir erhalten

$$0 < z_1^2 + z_2^2 \ \le \ 2\frac{a^2}{4} = \tfrac{1}{2}a^2 < a^2.$$

Andererseits ist

$$z_1^2 + z_2^2 \equiv x_1^2 + x_2^2 = ap \equiv 0 \mod a,$$

und damit ist

$$z_1^2 + z_2^2 = a'a \quad \text{mit } 1 \le a' < a.$$

Die Multiplikativität der Summen von Paaren von Quadraten liefert:

$$ap \cdot a'a = (x_1^2 + x_2^2)(z_2^2 + z_1^2) = (x_1z_2 - x_2z_1)^2 + (x_1z_1 + x_2z_2)^2.$$

Beiden Zahlen, die rechts quadriert werden, sind durch a teilbar, denn

$$\begin{aligned} x_1z_2 - x_2z_1 &\equiv x_1x_2 - x_2x_1 = 0 \mod a, \\ x_1z_1 + x_2z_2 &\equiv x_1x_1 + x_2x_2 = ap \equiv 0 \mod a. \end{aligned}$$

Schreiben wir also $x_1z_2 - x_2z_1 = ay_1$ und $x_1z_1 + x_2z_2 = ay_2$, so erhalten wir

$$ap \cdot a'a = (x_1z_2 - x_2z_1)^2 + (x_1z_1 + x_2z_2)^2 = (ay_1)^2 + (ay_2)^2 = a^2(y_1^2 + y_2^2).$$

Wir teilen durch a^2 und erhalten

$$a'p = y_1^2 + y_2^2.$$

Zusatz. Will man den Algorithmus wirklich durchführen, so kann man für a gerade folgendermaßen vorgehen: Weil a gerade ist, sind x_1 und x_2 entweder beide gerade oder beide ungerade, also sind die Zahlen $x_1 + x_2$ und $x_1 - x_2$ beide gerade. Setze

$$y_1 = \tfrac{1}{2}(x_1 + x_2), \quad y_2 = \tfrac{1}{2}(x_1 - x_2).$$

Es ist

$$y_1^2 + y_2^2 = \tfrac{1}{4}(x_1 + x_2)^2 + \tfrac{1}{4}(x_1 - x_2)^2 = \tfrac{1}{2}(x_1^2 + x_2^2) = \tfrac{1}{2}ap = a'p$$

mit $a' = \frac{1}{2}a$.

Wir betrachten noch einmal die Behauptung (2) und geben eine explizite Formel für s an. Zunächst (als Nachtrag zu Teil 3 der Vorlesung) der Satz von Wilson:

5.1.3. Satz von Wilson. *Für jede Primzahl p gilt* $(p-1)! \equiv -1 \mod p$.

Beweis: Für $p = 2$ ist $(p-1)! = 1! = 1$ und es ist $1 \equiv -1 \mod 2$. Sei nun p eine ungerade Primzahl. Die Gruppe $G = (\mathbb{Z}/p)^*$ ist zyklisch (3.4.2) und hat gerade Ordnung, die linke Seite der behaupteten Kongruenz ist gerade das Produkt über alle Element von G. In einer zyklischen Gruppe gerader Ordnung gibt es genau ein Element der Ordnung 2. Sei also $g_0 \in G$ das Element der Ordnung 2 (es ist dies die Restklasse $\overline{-1}$). Wir nennen g, h in G äquivalent, falls $g = h$ oder $g = h^{-1}$. Es gibt zwei Äquivalenzklassen, die jeweils nur aus einem Element bestehen, nämlich die Äquivalenzklassen zu 1 und zu g_0. Bilden wir das Produkt über alle Elemente von G, und zwar, indem wir jeweils diese Äquivalenzklassen betrachten, so ist das Produkt für jede zweielementige Äquivalenzklasse gleich 1. Die beiden einelementigen

Äquivalenzklassen liefern zusätzlich einen Faktor 1 und einen Faktor g_0. Insgesamt ist das Produkt also gleich g_0.

5.1.4. *Ist p Primzahl mit $p \equiv 1 \mod 4$, so gilt*

$$\left(\tfrac{p-1}{2}!\right)^2 \equiv -1 \mod p.$$

Beweis: Wegen $p \equiv 1 \mod 4$ ist $\frac{p-1}{2}$ gerade, demnach gilt für $s = \frac{p-1}{2}!$

$$\begin{aligned} s = 1 \cdot 2 \cdot \cdots \cdot \tfrac{p-1}{2} &= (-1) \cdot (-2) \cdot \cdots \cdot (-\tfrac{p-1}{2}) \\ &\equiv (p-1)(p-2) \cdots (p - \tfrac{p-1}{2}) \\ &= \tfrac{p+1}{2}(\tfrac{p+1}{2}+1) \cdots (p-2)(p-1) \mod p \end{aligned}$$

Es ist also $s^2 = (p-1)!$ und der Satz von Wilson liefert die Behauptung.

Zusatz. Für $p \equiv 3 \mod 4$ sieht man entsprechend: $\left(\frac{p-1}{2}!\right)^2 \equiv 1 \mod p$.

Dritter Beweis von 5.1.2 (Heath-Brown, 1971).

Betrachte die Menge

$$S = \{[x,y,z] \mid x > 0,\ y > 0, \quad 4xy + z^2 = p\}.$$

Es gilt:

(0) *S ist eine endliche Menge.*
Beweis: Offensichtlich ist $x \le \frac{1}{4}p$, $y \le \frac{1}{4}p$ und $|z| \le \sqrt{p}$.

(1) *Ist $[x,y,z] \in S$, so ist $z \neq 0$ und $z \neq y - x$.*
Beweis: Aus $z = 0$ folgt $p = 4xy$, aber p ist Primzahl, unmöglich. Und $z = y - x$ liefert $p = 4xy + z^2 = 4xy + (y-x)^2 = (y+x)^2$, ebenfalls ein Widerspruch.
Betrachte die Teilmengen T, T', U, U' von S mit

$$\begin{aligned} T &= \{[x,y,z] \in S \mid z > 0\}, \\ T' &= \{[x,y,z] \in S \mid z < 0\}, \\ U &= \{[x,y,z] \in S \mid z > y - x\}, \\ U' &= \{[x,y,z] \in S \mid z < y - x\}, \end{aligned}$$

(1′) *S ist die disjunkte Vereinigung von T und T', aber auch von U und U'.*

(2) *Es ist $|S| = 2 \cdot |T| = 2 \cdot |U|$.*
Beweis: Auf S definieren wir eine Involution f durch $f[x,y,z] = [y,x,-z]$ (Vertauschung von x und y, Multiplikation von z mit -1). Dies ist offensichtlich eine Abbildung, die eine Bijektion zwischen T und T' liefert. Also haben T und T' die gleiche Kardinalität, wegen (1′) ist dann $|S| = 2 \cdot |T|$
Die gleiche Involution f liefert auch eine Bijektion zwischen U und U', daher gilt auch $|S| = 2 \cdot |U|$.

(3) *Die Kardinalität von U ist ungerade.*

Beweis: Betrachte die Abbildung $g\colon U \to U$ mit $g[x,y,z] = [z+x-y, y, 2y-z]$. Wegen $z > y - x$ ist $z + x - y > 0$ und es ist

$$4(z+x-y)y + (2y-z)^2 = 4zy + 4xy - 4y^2 + 4y^2 - 4yz + z^2 = 4xy + z^2 = p.$$

Demnach gehört $g[x,y,z]$ zu S. Wegen $0 > -x$ ist auch $2y - z > y - (z+x-y)$, also ist $[x,y,z]$ in U. Die Abbildung g ist eine Involution, denn wenden wir g auf $[z+x-y, y, 2y-z]$ an, so erhalten wir

$$[2y - z + (z+x-y) - y, y, 2y - (2y-z)] = [x,y,z].$$

Und es gibt genau einen Fixpunkt, nämlich $[\frac{1}{4}(p-1), 1, 1]$ (unter g wird dieser Punkt auf $[1 + \frac{1}{4}(p-1) - 1, 1, 2-1] = [\frac{1}{4}(p-1), 1, 1]$ abgebildet) — natürlich ist vorher festzustellen, dass dies wirklich ein Element von U ist (aber $4\frac{1}{4}(p-1)\cdot 1 + 1 = p$ und $1 > 1 - \frac{1}{4}(p-1)$). Natürlich brauchen wir auch, dass $\frac{1}{4}(p-1)$ eine ganze Zahl ist. Hier wird also die Voraussetzung $p \equiv 1 \mod 4$ verwendet.

Sei umgekehrt $g[x,y,z] = [x,y,z]$, also $z + x - y = x$ und $2y - z = z$. Jede der Gleichungen liefert $y = z$, daraus folgt dann $p = 4xy + z^2 = 4xy + y^2 = (4x+y)y$, dann ist aber y ein natürlicher Teiler von p mit $y < \frac{p}{y}$ und demnach $y = 1$, und $4x + 1 = p$.

Offensichtlich gilt ganz allgemein: Besitzt eine endliche Menge M eine Involution mit genau einem Fixpunkt, so ist $|M|$ ungerade. Dies liefert die Behauptung.

(4) Die Kardinalität der Menge $|T|$ ist ungerade.

Folgt direkt aus (2) und (3).

Ende des Beweises: Auch auf T definieren wir nun eine Involution h, nämlich $h[x,y,z] = [y,x,z]$. Wegen (4) hat sie einen Fixpunkt: es gibt also einen Punkt der Form $[x,x,z] \in T$, und nach Definition von S gilt also $4x^2 + z^2 = p$.

5.1.5. Wir bestimmen die Anzahl der Darstellungen von n als Summe zweier Quadrate (insbesondere zeigen wir damit, dass wir für eine Primzahl $n = p$ (bis auf Reihenfolge) eine eindeutige Darstellung erhalten).

Sei $\mathcal{P}(n)$ die Menge der Paare $[x,y] \in \mathbb{N}_0^2$ mit $(x,y) = 1$ und $x^2 + y^2 = n$. und

Es gilt: *Die Anzahl der Paare $[x,y] \in \mathbb{N}_0^2$ mit $x^2 + y^2 = n$ ist* $\sum_{d^2|n} P(\frac{n}{d^2})$.

Beweis: Ordne jedem Paar $[x,y]$ mit $x^2 + y^2 = n$ das Paar $[x_0, y_0]$ zu, dabei sei $d = (x,y)$ und $x_0 = \frac{x}{d}$, $y_0 = \frac{y}{d}$.

Neben der Menge $\mathcal{P}(n)$ betrachten wir die Menge $\mathcal{R}(n)$ der Restklassen $\overline{s}$ modulo n aller Zahlen s mit $s^2 \equiv -1 \mod n$.

Satz. *Die zahlentheoretische Funktion $|\mathcal{R}(n)|$ ist mutiplikativ und es gilt:*

$$|\mathcal{P}(1)| = 2, \quad |\mathcal{R}(1)| = 1 \qquad \text{und}$$
$$|\mathcal{P}(n)| = |\mathcal{R}(n)| \qquad \text{für} \qquad n \geq 2,$$

Beweis: Dass die Funktion $|\mathcal{R}(n)|$ multiplikativ ist, folgt unmittelbar aus den chinesischen Restsatz, oder besser aus dem kanonischen Ring-Isomorphismus

$$\eta\colon \mathbb{Z}/nm \longrightarrow (\mathbb{Z}/n) \times (\mathbb{Z}/m)$$

für natürliche teilerfremde Zahlen n, m. Denn unter diesem Isomorpmorphismus wird die Restklasse $\overline{-1}$ auf das Paar von $(\overline{-1}, \overline{-1})$ abgebildet, und die Menge $\mathcal{R}(nm)$ auf $(\mathcal{R}(n)) \times (\mathcal{R}(m))$, also liefert η eine Bijektion $\mathcal{R}(nm) \longrightarrow (\mathcal{R}(n)) \times (\mathcal{R}(m))$.

Es ist $\mathcal{P}(1) = \{[1,0],[0,1]\}$, also ist dies eine zwei-elementige Menge, während $\mathcal{R}(1) = \mathbb{Z}/1$ einelementig ist.

Sei nun $n \geq 2$. Nach Definition ist $\mathcal{P}(n)$ die Menge der Paare $[x,y] \in \mathbb{N}_0^2$ mit $(x,y) = 1$ und $x^2 + y^2 = n$. Wegen $n \geq 2$ und $(x,y) = 1$ sieht man, dass $x \geq 1$ gilt. Und es gilt auch $(x,n) = 1$, denn ein gemeinsamer Primteiler von x und n wäre auch ein Teiler von y. Es gibt also t mit $tx \equiv 1 \mod n$. Sei $s = ty$. Dann ist

$$s^2 = (ty)^2 = t^2y^2 \equiv -t^2x^2 \equiv -1 \mod n.$$

Aus $s = ty$ folgt $sx = tyx \equiv y \mod n$. Wir haben also jedem Element $[x,y]$ in M eine Restklasse $\overline{s}$ zugeordnet mit $s^2 \equiv -1 \mod n$ und $y \equiv sx \mod n$, es ist also $s \in \mathcal{R}(n)$.

Diese Zuordnung ist injektiv: Sei nämlich auch $[u,v]$ in $\mathcal{P}(n)$ mit $v \equiv su \mod n$. Aus $v \equiv su$ und $y \equiv sx$ folgt $xv \equiv xsu \equiv yu \mod n$. Nun ist $1 \leq x < \sqrt{n}$ und $1 \leq v < \sqrt{n}$, also $1 \leq xv < n$ und entsprechend $1 \leq yu < n$. Da xv und yu die gleiche Restklasse module n liefern, muss $xv = yu$ gelten. Aus $(x,y) = 1$ folgt $x|u$, aus $(u,v) = 1$ folgt $u|x$, also ist $x = u$ und damit auch $y = v$.

Für die Surjektivität der Zuordnung brauchen wir (4): Sei $s^2 \equiv -1 \mod n$, so gibt es x, y mit $x^2 + y^2 = n$ und $y \equiv sx \mod n$.

Insbesondere gilt: *Ist p eine Primzahl mit $p \equiv 1 \mod 4$, so gibt es genau ein Paar von Zahlen $0 < x < y$ mit $x^2 + y^2 = p$* (denn es gibt zwei Restklassen $\overline{s}$ mit $s^2 \equiv -1 \mod n$, und natürlich gibt es neben dem Paar x, y noch das zweite Paar y, x.)

Hier eine kleine Tabelle:

p	=	5	13	17	29	37	41	53	61	73	89	97
x	=	1	2	1	2	1	4	2	5	3	5	4
y	=	2	3	4	5	6	5	7	6	8	8	9
s	=	2	8	4	17	6	32	30	50	27	55	75

Wir sehen auch: *Besitzt n mindestens zwei verschiedene Primteiler p_1, p_2 mit $p_i \equiv -1 \mod 4$, und kann n als Summe zweier Quadratzahlen geschrieben werden, so gibt es mehrere Möglichkeiten!*

Beispiel:

$$n = 65 = 5 \cdot 13 = 1^2 + 8^2 = 4^2 + 7^2.$$

Beachte: Unter dem Isomorphismus $\eta\colon (\mathbb{Z}/65)^* \to (\mathbb{Z}/5)^* \times (\mathbb{Z}/13)^*$ entspricht die Restklasse $-\overline{1}$ dem Paar $(-\overline{1}, -\overline{1})$. In $\mathbb{Z}/5$ liefern die Restklassen von $s = 2, 3$ Elemente mit $s^2 \equiv -1$, in $\mathbb{Z}/13$ sind dies die Restklassen von 5 und 8. Es ist

$$(\overline{2}, \overline{5}) = \eta(\overline{57}) \quad (\overline{2}, \overline{8}) = \eta(\overline{47}) \quad (\overline{3}, \overline{5}) = \eta(\overline{18}) \quad (\overline{3}, \overline{8}) = \eta(\overline{8}),$$

und es gilt (alle Kongruenzen modulo 65):

$$1 \cdot 8 = 8, \quad 8 \cdot 57 = 456 \equiv 1, \quad 4 \cdot 18 = 72 \equiv 7, \quad 7 \cdot 47 = 329 \equiv 4,$$

5.1.6. Für $n \in \mathbb{N}$, sei $\tau(n)$ die Anzahl der Paare $[x, y] \in \mathbb{Z}^2$ mit $x^2 + y^2 = n$. Sei $T(n) = \sum_{a=1}^{n} \tau(a)$. Offensichtlich ist $I(n)$ die Anzahl der Paare $[x, y] \in \mathbb{Z}^2$ mit $0 < x^2 + y^2 \leq n$.

Hier eine kleine Tabelle:

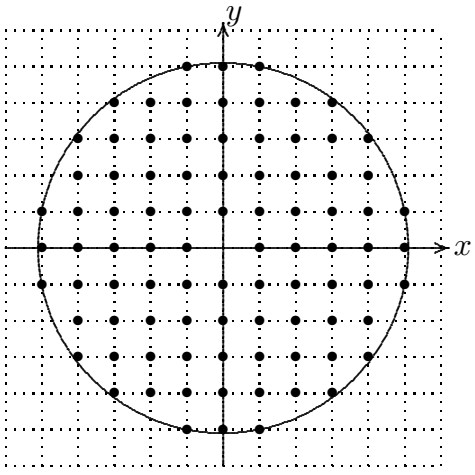
a	$=$	1	2	3	4	5	6	7	8	9	10	11
$\tau(a)$	$=$	4	4	0	4	8	0	0	4	4	8	0
$\frac{1}{n}T(n)$	$\approx$	4,00	4,00	2,67	3,00	4,00	3,33	2,86	3,00	3,11	3,60	3,27

Satz. *Es gilt*

$$\lim_{n\to\infty} \tfrac{1}{n} \sum_{a=1}^{n} \tau(a) = \pi.$$

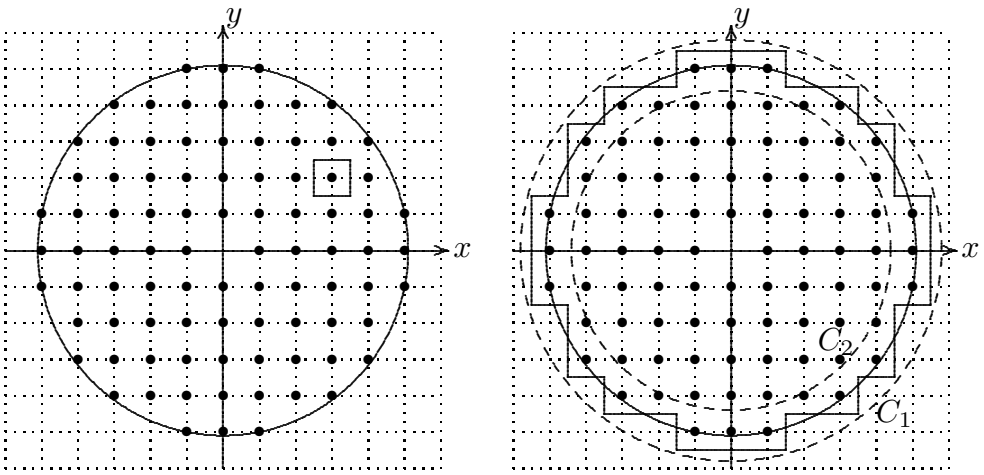
Dies besagt: *Der Mittelwert der Funktion $\tau(a)$ für $1 \leq a \leq n$ und n groß liegt nahe bei π und konvergiert gegen π.*

Beweis: Abzuzählen sind die Paare $[x, y] \in \mathbb{Z}^2$ mit $0 < x^2 + y^2 \leq n$.



Um jeden Gitterpunkt $[x, y]$ innerhalb des Usprungskreises mit Radius $\sqrt{n}$ legen wir ein achsen-paralleles Quadrat mit Mittelpunkt $[x, y]$ und Flächeninhalt 1.

Die Gesamtfläche F die wir auf diese Weise erhalten ist $T(n)+1$ (da wir neben den uns interessierenden Gitterpunkten auch den Ursprung betrachten). Links ist ein solches Quadrat eingezeichnet, rechts sieht man die Fläche F.



Sei C_1 der Ursprungskreis mit Radius $\sqrt{n}+\frac{1}{2}\sqrt{2}$ und C_2 der Ursprungskreis mit Radius $\sqrt{n}-\frac{1}{2}\sqrt{2}$. Unsere Fläche F liegt ganz innerhalb des Kreises C_1, während die Kreisscheibe mit Rand C_2 ganz in F enthalten ist. (Beweis: Jeder Punkt P in F hat Abstand höchstens $\frac{1}{2}\sqrt{2}$ zu einem Gitterpunkt $[x,y]$ mit $x^2+y^2 \le n$. Die Dreiecksungleichung besagt, dass der Abstand von P zum Usprung kleiner oder gleich $\sqrt{n}+\frac{1}{2}\sqrt{2}$ ist. Hat umgekehrt ein Punkt P' Abstand höchstens $\sqrt{n}-\frac{1}{2}\sqrt{2}$ vom Ursprung, und wählt man einen Gitterpunkt $[x,y]$ mit Abstand höchstens $\frac{1}{2}\sqrt{2}$ von P' (einen solchen Gitterpunkt gibt es immer), so hat $[x,y]$ vom Ursprung den Abstand höchstens $\sqrt{n}$. und P' liegt in F.) Dies zeigt:

$$\left(\sqrt{n}-\tfrac{1}{2}\sqrt{2}\right)^2\cdot\pi \;\le\; T(n)+1 \;\le\; \left(\sqrt{n}+\tfrac{1}{2}\sqrt{2}\right)^2\cdot\pi.$$

Es gilt ferner

$$\left(\sqrt{n}+\tfrac{1}{2}\sqrt{2}\right)^2\cdot\pi-1 = n\pi+\sqrt{n}\sqrt{2}\cdot\pi+\tfrac{1}{2}\pi-1 < n\cdot\pi+6\sqrt{n},$$

(denn $\sqrt{2}\cdot\pi \le 5$ und $\frac{1}{2}\pi-1<1\le\sqrt{n}$). Entsprechend gilt

$$\left(\sqrt{n}-\tfrac{1}{2}\sqrt{2}\right)^2\cdot\pi-1 = n\pi-\sqrt{n}\sqrt{2}\cdot\pi+\tfrac{1}{2}\pi-1 > n\cdot\pi-6\sqrt{n},$$

(denn $\sqrt{2}\cdot\pi-\frac{1}{2}\pi\le 5$ und wieder $1\le\sqrt{n}$). Insgesamt erhalten wir die Abschätzung

$$|T(n)-n\pi|<6\sqrt{n},$$

also

$$\left|\tfrac{T(n)}{n}-\pi\right|<\tfrac{6\sqrt{n}}{n},$$

und demnach $\lim_{n\to\infty}\frac{T(n)}{n}=\pi$.

5.2. Pythagoräische Tripel.

Man nennt ein Tripel $[x, y, z]$ natürlicher Zahlen ein *pythagoräisches Tripel,* falls gilt:

$$x^2 + y^2 = z^2.$$

Ist $[x, y, z]$ ein pythagoräisches Tripel, und $d \in \mathbb{N}$, so ist $[dx, dy, dz]$ ein pythagoräisches Tripel (und auch umgekehrt gilt: Ist $[x, y, z]$ ein Tripel natürlicher Zahlen, $d \in \mathbb{N}$ und ist $[dx, dy, dz]$ pythagoräisch, so ist auch $[x, y, z]$ pythagoräisch). Um die pythagoräischen Tripel zu klassifizieren (das wollen wir jetzt tun), reicht es also, die primitiven pythagoräischen Tripel zu finden, dabei heißt ein pythagoräisches Tripel $[x, y, z]$ *primitiv*, falls $(x, y) = 1$ gilt (äquivalent dazu ist $(x, z) = 1$ und auch $(y, z) = 1$).

Ist $[x, y, z]$ ein primitives pythagoräisches Tripel, so ist genau eine der beiden Zahlen x, y gerade.

Beweis: Da $(x, y) = 1$, können x, y nicht beide gerade sein. Wären beide Zahlen x, y ungerade, so wäre $x^2 \equiv 1$ und auch $y^2 \equiv 1$ modulo 4, also $z^2 \equiv 2 \mod 4$. Gerade Quadratzahlen sind aber durch 4 teilbar.

Satz. *Die Abbildung*

$$\{[a, b] \in \mathbb{N}^2 \mid a > b,\ (a, b) = 1,\ a \not\equiv b \mod 2\} \longrightarrow \{[x, y, z] \in \mathbb{N}^3 \mid x^2 + y^2 = z^2,\ (x, y) = 1,\ y \equiv 2 \mod 2\},$$

definiert durch

$$[a, b] \mapsto [a^2 - b^2, 2ab, a^2 + b^2]$$

ist eine Bijektion.

Insbesondere sehen wir: *Ist $x^2 + y^2 = z^2$, so ist z selbst die Summe zweier Quadratzahlen!*

Der Satz steht schon bei EUKLID (Elemente, IX, § 28, 29) und war möglicherweise schon den Babyloniern bekannt (1500 v.u.Z.), jedenfalls gibt es babylonische Listen von primitiven pythagoräischen Tripeln, die darauf hindeuten. Pythagoras kannte die Tripel, die man unter obiger Abbildung aus den Paaren $[a, b] = [n + 1, n]$ erhält: Offensichtlich erfüllen die Paare $[n+1, n]$ die drei Bedingungen $n+1 > n$, $(n+1, n) = 1$ und $n + 1 \not\equiv n \mod 2$; ihnen wird zugeordnet:

$$x = a^2 - b^2 = 2n + 1, \quad y = 2ab = 2n^2 + 2n, \quad z = a^2 + b^2 = 2n^2 + 2n + 1$$

(es sind dies gerade die pythagoräischen Tripel $[x, y, z]$ mit $z = y + 1$).

Hier die Liste pythagoräischer Tripel, die man erhält, wenn man die Paare $[a, b]$ mit $a > b$, $(a, b) = 1$, und $a \not\equiv b \mod 2$ betrachtet, für die $a \leq 9$ gilt:

a	=	2	3	4	4	5	5	6	6	7	7	7	8	8	8	8	9	9	9
b	=	1	2	1	3	2	4	1	5	2	4	6	1	3	5	7	2	4	8
x	=	3	5	15	7	21	9	35	11	45	33	13	63	55	39	15	77	65	17
y	=	4	12	8	24	20	40	12	60	28	56	84	16	48	80	112	36	72	144
z	=	5	13	17	25	29	41	37	61	53	65	85	65	73	89	113	85	97	145

Beweis des Satzes. Wir beginnen mit einem Paar $[a,b]$ natürlicher Zahlen, mit $a>b$, $(a,b)=1$, und $a \not\equiv b \mod 2$ und definieren x,y,z wie angegeben. Sei p ein Primteiler von $y=2ab$, es ist $p=2$ oder ein Teiler von a oder von b. Sei p auch Teiler von $x=a^2-b^2$. Wegen $a \not\equiv b \mod 2$ ist 2 kein Teiler von x. Ist p ein Teiler von a und von x, so auch von b^2, also von b. Aber dies widerspricht $(a,b)=1$. Entsprechend kann p kein Teiler von b sein. Also sehen wir $(x,y)=1$. Dass $y \equiv 0 \mod 2$ gilt, ist offensichtlich. Schließlich brauchen wir noch

$$x^2+y^2=(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2=z^2.$$

Die Zuordnung ist offensichtlich injektiv, denn $\frac{1}{2}(x+z)=a^2$ und $\frac{1}{2}(x-z)=b^2$.

Es bleibt zu zeigen, dass die Zuordnung surjektiv ist — dies ist auch die wirklich wichtige Aussage: gesucht ist ja ein Verfahren, um alle primitiven pythagoräischen Tripel zu erhalten. Sei also $[x,y,z]$ primitives pythagoräisches Tripel, mit y gerade. Wegen $(x,y)=1$ und $(y,z)=1$ sind x,z beide ungerade, es gibt also $u \in \mathbb{N}_0$ und $v,w \in \mathbb{N}$ mit

$$x=2u+1, \quad y=2v, \quad z=2w+1.$$

Setze $r=w+u+1$ und $s=w-u$. Es ist $(r,s)=1$, denn ist d ein Teiler von r und s, so auch von $r+s=2w+1=z$ und von $r-s=2u+1=x$, aber $(x,z)=1$.

Es ist

$$y^2=z^2-x^2=(z+x)(z-x)=(2w+2u+1)(2w-2u)=4rs.$$

Da r,s teilerfremd sind, sehen wir, dass beide Zahlen r,s Quadrate sind. Sei also $r=a^2, s=b^2$. Wegen $r=w+u+1>w \geq w-u=s$ ist $a>b$. Wegen $(r,s)=1$ ist $(a,b)=1$. Modulo 2 erhalten wir $r=w+u+1 \not\equiv w+u \equiv w-u=s \mod 2$, also ist auch $a \not\equiv b \mod 2$. Dies zeigt, dass $[a,b]$ alle geforderten Bedingungen erfüllt.

Zu zeigen bleibt, dass $[a,b]$ unter unserer Zuordnung auf $[x,y,z]$ abgebildet wird. Es ist $a^2-b^2=r-s=x$. Es ist $a^2+b^2=r+s=z$. Und schließlich ist $(2ab)^2=4a^2b^2=4rs=y^2$. Da $2ab$ und y positiv sind, folgt $2ab=y$. Damit ist der Satz bewiesen.

5.3. Summen von vier (oder fünf) Quadratzahlen.

Satz (Lagrange 1770). *Jede natürliche Zahl n lässt sich als Summe der Quadrate von vier ganzen Zahlen schreiben.*

Beweis. Kern des Beweises ist wieder der Spezialfall, dass $n=p$ eine Primzahl ist. Denn es gilt auch hier eine Multiplikativitäts-Aussage:

Lemma. *In jedem kommutativen Ring R gilt*

$$\begin{aligned}\Big(\sum_{i=1}^4 x_i^2\Big)\Big(\sum_{i=1}^4 y_i^2\Big) =& \Big(\sum_{i=1}^4 x_iy_i\Big)^2 \\ &+(-x_1y_2+x_2y_1-x_3y_4+x_4y_3)^2 \\ &+(-x_1y_3+x_3y_1-x_2y_4+x_4y_2)^2 \\ &+(-x_1y_4+x_4y_1-x_2y_3+x_3y_2)^2\end{aligned}$$

Beweis: Nachrechnen (für $R = \mathbb{R}$ handelt es sich um eine Regel für das Arbeiten mit Quaternionen).

Wir betrachten also den Fall, dass $n = p$ eine Primzahl ist. Wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ können wir annehmen, dass p ungerade ist. Als erstes zeigen wir:

Ist p ungerade Primzahl, so gibt es ganze Zahlen x_1, x_2 mit $0 \leq i \leq \frac{p-1}{2}$ und ein a mit $0 < a < p$, sodass gilt:

$$x_1^2 + x_2^2 + 1 = ap.$$

Beweis: Die Restklassen modulo p der Quadratzahlen

$$0^2,\ 1^2,\ \ldots,\ \left(\tfrac{p-1}{2}\right)^2$$

sind paarweise verschieden; multiplizieren wir diese Zahlen mit -1 und addieren jeweils -1, so erhalten wir

$$-0^2 - 1,\ -1^2 - 1,\ \ldots,\ -\left(\tfrac{p-1}{2}\right) - 1,$$

auch deren Restklassen modulo p sind paarweise verschieden. Wir haben hier jeweils $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ Elemente notiert, insgesamt bilden wir also $p+1$ Elemente in $\mathbb{Z}/p$. Es gibt aber nur p Restklassen modulo p.

Wir sehen, dass mindestens ein Element der ersten Reihe zu einem Element der zweiten Reihe kongruent sein muss, etwa $x_1^2 \equiv -x_2^2 - 1 \mod 4$, also $x_1^2 + x_2^2 + 1 \equiv 0 \mod p$.

Es gibt also $a \in \mathbb{Z}$ mit $x_1^2 + x_2^2 + 1 = ap$. Die linke Seite ist positiv, also ist $a \geq 1$. Wegen $0 \leq x_i \leq \frac{p-1}{2}$ für $i = 1, 2$ und auch $1 \leq \frac{p-1}{2}$, gilt $x_1^2 + x_2^2 + 1 \leq \frac{3}{4}(p-1) < p^2$. Also ist $0 < a < p$.

Beweis des Satzes von Lagrange für $n = p$ eine ungerade Primzahl. Wir haben gerade gesehen, dass es ganze Zahlen x_1, x_2, x_3, x_4 und $0 < a < p$ gibt mit

$$(*) \qquad x_1^2 + x_2^2 + x_3^2 + x_4^2 = ap.$$

Wir behaupten, dass $a = 1$ das kleinste derartige a ist. Wir zeigen nämlich: *Gilt die Gleichung $(*)$ für ein $1 < a < p$, so gibt es $1 \leq a' < a$ und ganze Zahlen y_i so dass gilt:*

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = a'p,$$

(es gibt also wieder einen **Abstiegs-Algorithmus**).

Beweis: Sei also $1 < a < p$ und $x_1^2 + x_2^2 + x_3^2 + x_4^2 = ap$.

Fall 1: a sei ungerade (hier imitieren wir den zweiten Beweis von 5.1.2.) Wir betrachten Restklassen modulo a, und zwar wählen wir jeweils betragsmäßig kleinste Representanten, also wähle z_i mit $z_i \equiv x_i \mod a$ und $|z_i| \leq \frac{a}{2}$, für $i = 1, 2$. Weil a ungerade ist, gilt sogar $|z_i| < \frac{a}{2}$. Wären alle x_i beide durch a teilbar, so wäre $ap = \sum x_i^2$ durch a^2 teilbar, also $a|p$. Aber p ist eine Primzahl und $1 < a < p$. Dies

zeigt, dass mindestens eine der beiden Zahlen x_i nicht durch a teilbar ist, also ist mindestens eine der Zahlen z_i von Null verschieden. Wir erhalten

$$0 < \sum_{i=1}^{4} z_i^2 < 4\frac{a^2}{4} = a^2.$$

Andererseits ist

$$\sum_{i=1}^{4} z_i^2 \equiv \sum_{i=1}^{4} x_i^2 = ap \equiv 0 \mod a,$$

und damit ist

$$\sum_{i=1}^{4} z_i^2 = a'a \quad \text{mit } 1 \le a' < a.$$

Die Multiplikativität der Summen von Paaren von Quadraten liefert:

$$\begin{aligned} ap \cdot a'a = \Big(\sum_{i=1}^{4} x_i^2\Big)\Big(\sum_{i=1}^{4} z_i^2\Big) = &\Big(\sum_{i=1}^{4} x_i z_i\Big)^2 \\ &+ (-x_1z_2 + x_2z_1 - x_3z_4 + x_4z_3)^2 \\ &+ (-x_1z_3 + x_3z_1 - x_2z_4 + x_4z_2)^2 \\ &+ (-x_1z_4 + x_4z_1 - x_2z_3 + x_3z_2)^2 \end{aligned}$$

Alle vier Zahlen, die rechts quadriert werden, sind, wie wir zeigen werden, durch a teilbar. Modulo a können wir jeweils z_i durch x_i ersetzen. Für das erste Element gilt:

$$\Big(\sum_{i=1}^{4} x_i z_i\Big)^2 \equiv \Big(\sum_{i=1}^{4} x_i x_i\Big)^2 = ap \equiv 0 \mod a$$

Für das zweite:

$$-x_1z_2 + x_2z_1 - x_3z_4 + x_4z_3 \equiv -x_1x_2 + x_2x_1 - x_3x_4 + x_4x_3 = 0 \mod a,$$

und entsprechend für das dritte und vierte. Schreiben wir also alle vier Elemente als Vielfache von a:

$$\begin{aligned} \Big(\sum_{i=1}^{4} x_i z_i\Big)^2 &= ay_1 \\ -x_1z_2 + x_2z_1 - x_3z_4 + x_4z_3 &= ay_2 \\ -x_1z_3 + x_3z_1 - x_2z_4 + x_4z_2 &= ay_3 \\ -x_1z_4 + x_4z_1 - x_2z_3 + x_3z_2 &= ay_4 \end{aligned}$$

so erhalten wir

$$ap \cdot a'a = (ay_1)^2 + (ay_2)^2 + (ay_3)^2 + (ay_4)^2 = a^2(y_1^2 + y_2^2 + y_3^2 + y_4^2).$$

Wir teilen durch a^2 und erhalten

$$a'p = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

Fall 2 (der einfachere Fall): a sei gerade. Weil a gerade ist, sind entweder 0, 2 oder 4 der Zahlen x_i gerade. Wir können daher annehmen dass gilt: x_1 und x_2 sind entweder beide gerade oder beide ungerade, und auch x_3 und x_4 sind entweder beide gerade oder beide ungerade. Also sind die Zahlen x_1+x_2, x_1-x_2 und x_3+x_4, x_3-x_4 gerade. Setze

$$y_1 = \tfrac{1}{2}(x_1 + x_2), \quad y_2 = \tfrac{1}{2}(x_1 - x_2), \quad y_3 = \tfrac{1}{2}(x_3 + x_4), \quad y_4 = \tfrac{1}{2}(x_3 - x_4).$$

Es ist

$$\begin{aligned} y_1^2 + y_2^2 + y_3^2 + y_4^2 &= \tfrac{1}{4}(x_1 + x_2)^2 + \tfrac{1}{4}(x_1 - x_2)^2 + \tfrac{1}{4}(x_3 + x_4)^2 + \tfrac{1}{4}(x_3 - x_4)^2 \\ &= \tfrac{1}{2}(x_1^2 + x_2^2 + x_3^2 + x_4^2) \\ &= \tfrac{1}{2}ap = a'p \end{aligned}$$

mit $a' = \frac{1}{2}a$.

Zusätze: (ohne Beweis)

Keine der Zahlen der Form $8 \cdot 4^n$ *lässt sich als Summe der Quadrate von vier natürlichen Zahlen schreiben* (es gibt noch weitere solche Zahlen).

Jede natürliche Zahl n *verschieden von* $1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33$ *kann als Summe der Quadrate von fünf natürlichen Zahlen geschrieben werden.*