6. Summen von Quadraten.

Wir interessieren uns hier für die Frage, ob sich eine 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.

6.1. Zahlen, die sich als Summe zweier Quadrate schreiben lassen.

Vorbemerkung: Sei $n \in \mathbb{N}$. Untersucht wird, ob es ganze Zahlen x, y mit $x^2+y^2 = n$ gibt. Dabei können wir natürlich annehmen, dass x, y nicht-negativ sind. Wichtig ist aber, ob wir zulassen, dass eine der beiden Zahlen die Null ist. Denn 4 lässt sich als Summe zweier Quadratzahlen schreiben: $4 = 4 + 0$, nicht aber als Summe zweier Quadrate natürlicher Zahlen! (Nach Definition verstehen wir im Rahmen der Elementaren Zahlentheorie unter einer natürlichen Zahl eine ganze Zahl, die echt größer als Null ist.) Wir werden sehen, siehe Punkt (6), dass es für diese Fragestellung sinnvoll ist, nach Summen von Quadratzahlen, und nicht etwa nach Summen von Quadraten natürlicher Zahlen, zu fragen.

6.1.1. Satz. *Sei $n \in \mathbb{N}$. Genau dann gibt es ganze 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 (1601-1665) zugeschrieben. Der erste publizierte Beweis stammt von EULER (1754). Kern dieses Satzes ist der Spezialfall $n = p$ Primzahl.

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 $p \equiv 1 \mod 4$.*

Wir untersuchen zuerst den Fall $n = p$ Primzahl. Die Zahl $p = 2$ lässt sich eindeutig als Summe von Quadraten schreiben: $2 = 1 + 1$. Ist $p \equiv 3 \mod 4$, so kann man wegen (1) p nicht als Summe zweiter Quadrate schreiben. Es sind also die Primzahlen $p \equiv 1 \mod 4$ zu untersuchen.

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

Beweis: Dies ist ein Teil des Euler-Kriteriums 2.11.4: Ist p Primzahl mit $p \equiv 1 \mod 4$, so ist -1 quadratischer Rest modulo p, es gilt also ein s mit $s^2 \equiv -1 \mod p$. (Erinnerung: Ist -1 quadratischer Rest modulo p, so schreibt man $\left(\frac{-1}{p}\right) = 1$).

Sei nun n eine natürliche Zahl.

(3) *Sei $s \in \mathbb{Z}$ mit $s^2 \equiv -1 \mod n$. 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 $0 \le y < \sqrt{n}$. (Man beachte, dass wir für x die Ungleichung $x \le \sqrt{n}$, für y dagegen die echte Ungleichung $y < \sqrt{n}$ verlangen.)

Behauptung: *Die Anzahl dieser Paare $[x, y]$ ist größer als n.* Um dies zu zeigen, unterscheiden wir zwei Fälle. Erster Fall: Ist n keine Quadratzahl, so ist die Anzahl dieser Paare $(\lfloor\sqrt{n}\rfloor + 1)^2 > n$ (denn für jeden der beiden Faktoren ist die Anzahl der Möglichkeiten gleich $\lfloor\sqrt{n}\rfloor + 1 > \sqrt{n}$). Zweiter Fall: 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 $x^2 + y^2 = n$.

Damit ist der wesentliche Spezialfall gezeigt:

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

Zusatz: In 6.2 werden wir sehen, dass diese Darstellung sogar bis auf die Reihenfolge der Summanden eindeutig ist!

Beweis: In (2) haben wir daran erinnert, dass es s mit $s^2 \equiv -1 \mod p$ gibt. In (4) haben wir $x, y \in \mathbb{N}_0$ mit $x^2 + y^2 = p$ gefunden. Da p Primzahl ist, gilt $x \neq 0$, und $y \neq 0$.

(5) *Sei $x^2 + y^2 = n$ mit $(x, y) = 1$. Sei p ein Primteiler von n. Dann ist -1 quadratischer Rest modulo p, 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. Hier wird nun die zweite Teilaussage des Euler-Kriteriums 2.11.4 verwendet: Wäre $p \equiv 3 \mod 4$, so wäre -1 kein quadratischer Rest modulo p, Widerspruch. (Erinnerung: Ist -1 kein quadratischer Rest modulo p, so schreibt man $\left(\frac{-1}{p}\right) = -1$).

(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 Quadrat des Betrags der komplexen Zahl $a + bi \in \mathbb{C}$ und verwende die Produktregel für den Betrag einer komplexen Zahl an.
(Alle diese Beweise sind natürlich nur verschiedene Interpretationen der gleichen Rechnung.)

Die Aussage (6) ist ganz wesentlich: Sie zeigt, dass die Menge Q, die ja recht chaotisch wirkt:

$$Q = \{0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 19, 20, 25, \dots\}$$

eine schöne Struktur besitzt: bezüglich der Multiplikation ist dies eine Halbgruppe. Die Menge Q' der Summe zweier Quadrate natürlicher Zahlen ist dagegen nicht unter der Multiplikation abgeschlossen: $2 \in Q'$, aber $4 = 2 \cdot 2 \notin Q'$.

Die Aussage (6) war offensichtlich schon Leonardo von Pisa (= Fibonacci) bekannt ($\sim$1180-1241).

Es ist durchaus sinnvoll, die Menge der Paare $[a, b] \in \mathbb{Z}^2$ wirklich als Elemente der Zahlenebene, und damit als komplexe Zahlen aufzufassen. Beachte: Die Menge dieser Paare bildet einen Unterring von $\mathbb{C}$, man nennt diesen Ring den *Ring der ganzen Gauß'schen Zahlen,* siehe Abschnitt 6.2).

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 $1 \leq i \leq m$ eine Primzahl p mit $p = 2$ oder $p \equiv 1 \mod 4$. Natürlich ist $2 \in Q$. Wegen (2) und (4) wissen wir, dass auch jede Primzahl p mit $p \equiv 1 \mod 4$ zu Q gehört, also ist jedes n_i in Q. 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 (5) 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.

Vorschau: Im nächsten Abschnitt wird folgender Satz (6.2.4) bewiesen werden:

Satz. *Für $n \in \mathbb{N}$ sei $\gamma(n)$ die Anzahl der Paare $[x, y] \in \mathbb{Z}^2$ mit $x^2 + y^2 = n$. Dann gilt für $n = 2^e \cdot p_1^{e_1} \cdots p_s^{e_s} \cdot q_1^{f_1} \cdots q_t^{f_t}$ mit Primzahlen $p_i \equiv 1 \mod 4$ und $q_j \equiv 3 \mod 4$*

$$\gamma(n) = \begin{cases} 4(e_1 + 1) \cdots (e_s + 1) & \text{falls alle } f_i \text{ gerade sind,} \\ 0 & \text{sonst.} \end{cases}$$

Insbesondere ist $\frac{1}{4}\gamma$ eine multiplikative Funktion; diese Funktion zählt die Paare $[x, y]$ mit $x > 0$ und $y \geq 0$, für die $x^2 + y^2 = n$ gilt. Festzuhalten ist auch:

Spezialfall. *Ist p eine Primzahl mit $p \equiv 1 \mod 4$, so ist $\gamma(p) = 8$, es gibt also im wesentlichen nur eine Darstellung $p = x^2 + y^2$ mit ganzen Zahlen x, y,* (neben $p = x^2 + y^2$ hat man auch die Darstellung $p = y^2 + x^2$, und man kann x durch $-x$ und y durch $-y$ ersetzen, dadurch kommt man auf 8 Paare $[x, y]$).

6.2. Die ganzen Gauß'schen Zahlen.

Wir interessieren uns dafür, wann $x^2 + y^2 = n$ mit $x, y \in \mathbb{Z}$ gilt. Dafür empfiehlt es sich, alle Paare $[x, y]$ mit $x, y \in \mathbb{Z}$ zu betrachten, also die Menge $\mathbb{Z}^2$. Diese Menge kann als die Grundmenge eines Rings angesehen werden, nämlich des Rings der ganzen Gauß'schen Zahlen. Die Abbildung $[x, y] \mapsto x^2 + y^2$, an der wir interessiert sind, wird die zugehörige Normabbildung genannt und mit N bezeichnet.

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen. Es ist $\mathbb{C} = \mathbb{R}^2$ mit komponentenweiser Addition und mit Multiplikation $[a_1, a_2][b_1, b_2] = [a_1b_1 - a_2b_2, a_1b_2 + a_2b_1]$. Dies ist bekanntlich ein Körper und man setzt $i = [0, 1]$ und schreibt dann $a_1 + a_2i$ statt $[a_1, a_2]$. (Es ist $i^2 = -1$, also schreibt man manchmal auch $i = \sqrt{-1}$.) Sind $a_1, a_2 \in \mathbb{R}$ und $a = a_1 + a_2i$, so nennt man $\overline{a} = a_1 - a_2i$ die zu a *konjugierte komplexe* Zahl. Die Zuordnung $a \mapsto \overline{a}$ ist ein Körper-Automorphismus von $\mathbb{C}$. Wir betrachten die folgenden Teilmengen:

$$\mathbb{Q}[i] = \{a \in \mathbb{C} \mid a = a_1 + a_2i, \text{ mit } a_1, a_2 \in \mathbb{Q}\},$$
$$\mathbb{Z}[i] = \{z \in \mathbb{C} \mid z = z_1 + z_2i, \text{ mit } z_1, z_2 \in \mathbb{Z}\}.$$

Man sieht sehr leicht: $\mathbb{Q}[i]$ ist ein Unterkörper von $\mathbb{C}$ und $\mathbb{Z}[i]$ ist ein Unterring von $\mathbb{Q}[i]$. Man nennt $\mathbb{Z}[i]$ den Ring der *ganzen Gauß'schen Zahlen.*

Betrachte die folgende Abbildung

$$N\colon \mathbb{Z}[i] \to \mathbb{N}_0 \quad \text{mit } N(z) = z\overline{z} \text{ für } z \in \mathbb{Z}[i],$$

man nennt $N(z)$ die *Norm* von z. Schreibt man $z = z_1 + z_2i$ mit $z_1, z_2 \in \mathbb{Z}$, so ist $N(z) = z_1^2 + z_2^2$ (es ist also $N(z) = |z|^2$, wobei $|z|$ der Betrag der komplexen Zahl z ist, also der Abstand des Punkts $[z_1, z_2] \in \mathbb{R}^2$ vom Ursprung). Natürlich gilt: *Genau dann ist* $N(z) = 0$, *wenn* $z = 0$. Und es ist

$$N(zz') = N(z)N(z') \quad \text{für alle } z, z' \in \mathbb{Z}[i]$$

(dies haben wir beim Beweisschritt (6) im Abschnitt 6.1 verwendet).

Wir betrachten im folgenden den Ring $\mathbb{Z}[i]$. Wenn also ring-theoretische Begriffe verwendet werden (wie "invertierbares" Element, "Prim-Element" usw, so ist gemeint: *invertierbar in* $\mathbb{Z}[i]$ bzw. *Prim-Element in* $\mathbb{Z}[i]$, usw. Da $Z[i]$ ein nullteilerfreier kommutativer Ring ist, hat man in $\mathbb{Z}[i]$ den Teilbarkeits-Begriff zur Verfügung ($z|z'$ genau dann, wenn es z'' mit $zz'' = z'$ gibt).

Wichtig: *Sind* $a, b \in \mathbb{Z}$ *und gilt* $a|b$ *in* $\mathbb{Z}[i]$, *so gilt* $a|b$ *in* $\mathbb{Z}$ (die Umkehrung gilt auch, ist aber trivial). Beweis: Sei $a|b$ in $\mathbb{Z}[i]$. Es gibt also $z \in \mathbb{Z}[i]$ mit $az = b$. Sei $z = z_1 + z_2i$ mit $z_1, z_2 \in \mathbb{Z}$. Dann ist $b = az = a(z_1 + z_2i) = az_1 + bz_2$, und demnach stimmen die Realteile b und az_1 überein: es gibt also $z_1 \in \mathbb{Z}$ mit $b = az_1$.

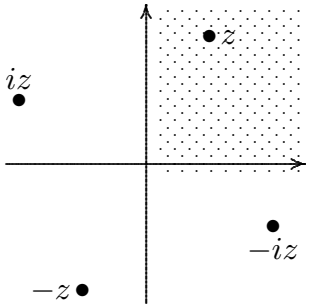
Ganz wichtig ist auch folgende Regel: *Aus* $z|z'$ *in* $\mathbb{Z}[i]$ *folgt die Teilbarkeitsbeziehung* $N(z)|N(z')$. Denn wenn $z|z'$ gilt, so gilt auch $\overline{z}|\overline{z'}$, also $N(z) = z\overline{z}|z'\overline{z'} = N(z')$.

6.2.1. Die invertierbaren Elemente in $\mathbb{Z}[i]$.

Lemma. *Es ist z in $\mathbb{Z}[i]$ genau dann invertierbar, wenn $N(z) = 1$. Es gibt genau vier invertierbare Elemente, nämlich $1, -1, i, -i$.*

Beweis: Sei $z \in \mathbb{Z}[i]$ invertierbar, also etwa $zz' = 1$ mit $z' \in \mathbb{Z}[i]$. Aus $zz' = 1$ folgt $1 = N(zz') = N(z)N(z')$. Da $N(z), N(z') \in \mathbb{N}_0$, folgt $N(z) = 1$. Ist $z = z_1 + z_2 i$ mit $z_1, z_2 \in \mathbb{Z}$ und gilt $1 = N(z) = z_1^2 + z_2^2$, so ist offensichtlich z eines der vier Elemente $1, -1, i, -i$. Und natürlich sind diese Elemente in $\mathbb{Z}[i]$ invertierbar.

Man nennt z, z' *assoziiert,* wenn gilt: $z|z'$ und $z'|z$. Genau dann sind z, z' assoziiert, wenn es ein invertierbares Element ϵ mit $z' = \epsilon z$ gibt. Ist $z \neq 0$, so gibt es genau vier zu z assoziierte Elemente, nämlich $z, iz, -z, -iz$ (hier haben wir die Elemente in der Reihenfolge notiert, wie sie in der reellen Ebene durch Drehung um 90^o um den Ursprung (= Multiplikation mit i) auseinander hervorgehen:



Assozierte Elemente haben natürlich die gleiche Norm, die Umkehrung gibt aber nicht!

6.2.2. Euklid'scher Algorithmus.

Satz. *Sind $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$, so gibt es $q, r \in \mathbb{Z}[i]$ mit*

$$a = qb + r \quad \text{und } N(r) < N(b).$$

(der Beweis zeigt, dass man sogar $N(r) \leq \frac{1}{2}N(b)$ verlangen darf).

Beweis: Da $\mathbb{Q}[i]$ ein Körper ist, gibt es $c = \frac{a}{b} \in \mathbb{Q}[i]$. Sei $c = c_1 + c_2 i$ mit $c_1, c_2 \in \mathbb{Q}$. Wir schreiben c_i in der Form $c_i = q_i + s_i$, dabei sei q_i eine ganze Zahl und es gelte $|s_i| \leq \frac{1}{2}$ (ist $c_i - \lfloor c_i \rfloor \leq \frac{1}{2}$, so nimm $c_i = \lfloor c_i \rfloor$, andernfalls nimm $c_i = \lfloor c_i \rfloor + 1$). Sei $q = q_1 + q_2 i$, $s = s_1 + s_2 i$ und $r = sb$. Es ist:

$$a = cb = (q + s)b = qb + sb = qb + r,$$

und

$$N(sb) = N(s)N(b) = (s_1^2 + s_2^2)N(b) \leq (\tfrac{1}{4} + \tfrac{1}{4})N(b) = \tfrac{1}{2}N(b).$$

Folgerung 1. Je zwei von Null verschiedene Elemente in $\mathbb{Z}[i]$ haben einen größten gemeinsamen Teiler (genauer: es gibt vier größte gemeinsame Teiler, nämlich eine Klasse assoziierter Elemente) (dabei nennt man c einen *größten gemeinsamen Teiler* von a, b, falls gilt: erstens, $c|a$ und $c|b$; zweitens: aus $d|a$ und $d|b$ folgt $d|c$).

Folgerung 2: Ist c größter gemeinsamer Teiler von a und b, so gibt es x, y mit $c = xa + yb$ (Bezout).

Folgerung 3. Irreduzible Elemente sind prime Elemente. (a heißt *irreduzible,* wenn a weder das Nullelement noch invertierbar ist, und wenn aus $a = bc$ folgt, dass b oder c invertierbar ist; a heißt *prim,* wenn aus $a|bc$ folgt $a|b$ oder $a|c$).

Folgerung 4. *Der Ring $\mathbb{Z}[i]$ ist ein Ring mit eindeutiger Primfaktorzerlegung (also ein "faktorieller" Ring):* Jedes Element, das weder Null noch invertierbar ist, lässt sich als Produkt von Primelementen schreiben — und diese Faktorisierung ist im wesentlichen eindeutig, denn für Produkte von Primelementen gilt: sind p_i, q_j Primelemente mit $1 \leq i \leq r$ und $1 \leq j \leq s$ und $p_1 \cdots p_r = q_j \cdots q_s$, so ist $r = s$ und es gibt eine Permutation σ der Menge $\{1, 2, \ldots, r\}$, sodass p_i und $q_{\sigma(i)}$ assoziert sind, für alle i.

Wählen wir für jedes Primelement den Repräsentanten $x = x_1 + ix_2$ mit $x_1 > 0$ und $x_2 \geq 0$ und nennen diese Menge $\mathcal{P}$, so gilt: *Die von Null verschiedenen ganzen Gauß'schen Zahlen entsprechen bijektiv den Paaren (ϵ, v) wobei ϵ eines der vier invertierbaren Elemente ist und $v\colon \mathcal{P} \to \mathbb{N}_0$ eine Abbildung mit endlichem Träger, und zwar wird dem Paar (ϵ, v) die Zahl $\epsilon \prod_{p\in\mathcal{P}} p^{v_p}$ zugeordnet.*

6.2.3. Die Prim-Elemente.

Vorbemerkung: Ist $N(z) = p$ eine Primzahl, so ist z Prim-Element. Denn aus $z = z'z''$ folgt $p = N(z) = N(z')N(z'')$, also muss eine der beiden Zahlen $N(z'), N(z'')$ gleich 1 sein, und demnach muss z' oder z'' invertierbar sein.

Beispiel 1: $N(1 + i) = 2$, also ist $1 + i$ Prim-Element. Die zu $1 + i$ assoziierten Elemente sind:

$$1 + i, \quad 1 - i = -i(1 + i), \quad -1 + i = i(1 + i), \quad -1 - i = -(1 + i).$$

Beispiel 2: Sei $p \equiv 1 \mod 4$. Dann gibt es x, y mit $x^2 + y^2 = p$, also $N(x+iy) = p$, und auch $N(x - iy) = p$, also sind die Elemente $x + iy, x - iy$ Primelemente. Die zu $x + iy$ assoziierten Elemente sind

$$x + iy, \quad y - ix = -i(x + iy), \quad -y + ix = i(x + iy), \quad -x - iy = -(x + iy).$$

Die zu $x - iy$ assoziierten Elemente sind

$$x - iy, \quad -y - ix = -i(x - iy), \quad y + ix = i(x - iy), \quad -x + iy = -(x - iy).$$

Sei $p \equiv 3 \mod 4$. Es ist $N(p) = p^2$. Sei $p = z'z''$ mit $z', z'' \in \mathbb{Z}[i]$. Es ist $N(p) = N(z')N(z'')$. Ist $N(z') = 1$, so ist z' invertierbar. Ist $N(z') = p^2$, so ist $N(z'') = 1$, also z'' invertierbar. Und $N(z') = p$ geht nicht, da sich p nicht als Summe zweier Quadrate schreiben lässt. In diesem Fall ist also p Prim-Element in $\mathbb{Z}[i]$.

Wir haben viele Prim-Elemente gefunden. Wir zeigen nun, dass es keine weiteren gibt:

Jedes Prim-Element z ist Teiler einer Primzahl. Beweis: Es ist $z\overline{z} = N(z) \in \mathbb{N}$. Schreibe $N(z)$ als Produkt $p_1 \cdots p_t$ von Primzahlen. Da z prim in $\mathbb{Z}[i]$ ist, ist z ein Teiler einer dieser Zahlen p_i.

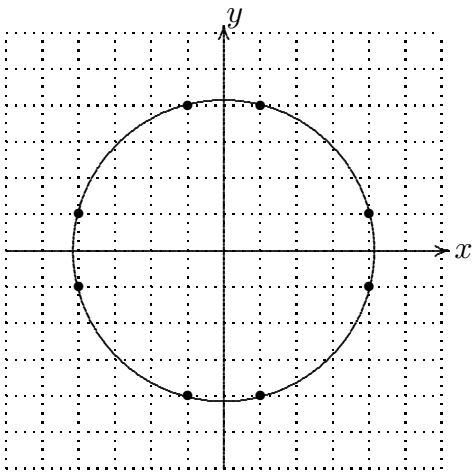
Sei also z Prim-Element in $\mathbb{Z}[i]$, sei p Primzahl mit $z|p$. Es ist dann $N(z)|N(p) = p^2$, also entweder $N(z) = p$ oder $N(z) = p^2$ (denn $N(z) = 1$ würde ja bedeuten, dass z invertierbar ist).

Wir unterscheiden drei Fälle für $z = z_1 + iz_2$.

Fall 1. $N(z) = 2$. Aus $z_1^2 + z_2^2 = 2$ folgt natürlich unmittelbar $z_1, z_2 \in \{1, -1\}$, und diese vier möglichen Elemente z sind alle assoziiert zu unserem Repräsentanten $1 + i$.

Fall 2. $N(z) = p$ ungerade Primzahl. Da p Summe zweier Quadratzahlen ist, ist $p \equiv 1 \mod 4$. Es ist $(z_1 + iz_2)(z_1 - iz_2) = z_1^2 + z_2^2 = p$. Die beiden Faktoren $z_1 + iz_2$, $z_1 - iz_2$ sind Primelemente, also ist dies die (eindeutige!) Primfaktorzerlegung von p: jeder Primteiler von p im Ring der ganzen Gauß'schen Zahlen ist assoziiert zu $z_1 + iz_2$ oder $z_1 - iz_2$.

Im folgenden Bild sieht man die Prim-Elemente z mit $N(z) = 17$.



Dass es genau 8 derartige Elemente gibt, folgt aus der eindeutigen Primfaktor-Zerlegung in $\mathbb{Z}[i]$: Zerlegt man $p = 17$ im Ring $\mathbb{Z}[i]$ in Primfaktoren, so gibt es nur zwei Faktoren (und jeder dieser Faktoren hat vier assoziierte Elemente).

Fall 3. $N(z) = p^2$. Aus $z\overline{z} = N(z) = p^2$ folgt, dass z ein Teiler von p^2 ist. Da wir voraussetzen, dass z ein Primelement ist, folgt: z ist ein Teiler von p. Da z und p die gleiche Norm haben, folgt: z ist assoziiert zu p, also ist z eine der Zahlen $p, -p, ip, -ip$. Wäre $p \equiv 1 \mod p$, so könnten wir p als Produkt zweier Faktoren mit Norm p schreiben, dann wäre aber z kein Primelement. Also folgt: $p \equiv 3 \mod 4$.

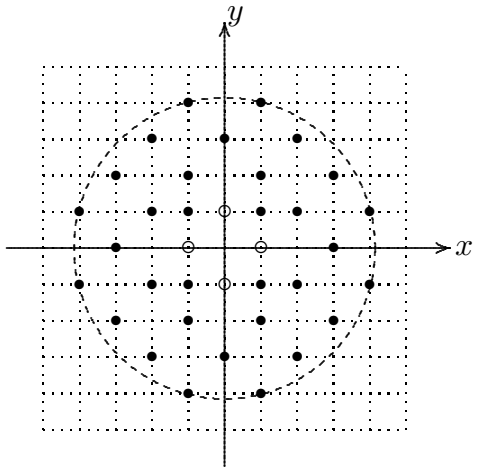
Wir haben also gezeigt:

Satz. *Die Menge $\mathcal{P}$ der Prim-Elemente $[x, y]$ von $\mathbb{Z}[i]$ mit $x > 0$ und $y \geq 0$ besteht aus*

- *dem Element $1 + i$,*
- *den Elementen $x + iy$ und $y + ix$ mit $x^2 + y^2 = p$, wobei $p \in \mathbb{N}$ eine Primzahl ist mit $p \equiv 1 \mod 4$,*
- *den Primzahlen $p \in \mathbb{N}$ mit $p \equiv 3 \mod 4$.*

Man erhält alle Prim-Elemente von $\mathbb{Z}[i]$, indem man alle Elemente in $\mathbb{Z}[i]$ bildet, die zu den Elementen in $\mathcal{P}$ assoziiert sind.

Im folgenden Koordinatensystem sind die Prim-Elemente z in $\mathbb{Z}[i]$ mit $N(z) \leq 17$ eingetragen (markiert durch $\bullet$); die Einheiten sind durch $\circ$ hervorgehoben).



6.2.4. Die Anzahl der ganzen Gauß'schen Zahlen mit fester Norm.

Für $n \in \mathbb{N}$ sei $\gamma(n)$ die Anzahl der ganzen Gauß'schen Zahlen mit Norm n, dies ist gerade die Menge der Paare $[x, y] \in \mathbb{Z}^2$ mit $x^2 + y^2 = n$ (in der Literatur wird diese Funktion oft mit τ statt mit γ bezeichnet).

Satz. *Sei $n = 2^e \cdot p_1^{e_1} \cdots p_s^{e_s} \cdot q_1^{f_1} \cdots q_t^{f_t}$ mit Primzahlen $p_i \equiv 1 \mod 4$ und $q_j \equiv 3 \mod 4$. Dann ist*

$$\gamma(n) = \begin{cases} 4(e_1 + 1) \cdots (e_s + 1) & \text{falls alle } f_j \text{ gerade sind} \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Dies folgt aus der Eindeutigkeit der Primfaktorzerlegung und unserer Kenntnis der Primelemente: Wir betrachten also Zahlen $z \in \mathbb{Z}[i]$ mit $N(z) = n$. Wir schreiben z als Produkt von Primelementen, genauer: als Produkt einer Einheit (dafür gibt es vier Möglichkeiten) und Repräsentanten unserer Primelemente. Sei also $z = \epsilon z_1 \cdots z_m$ mit einer Einheit ϵ und Repräsentanten $z_1, \ldots, z_m$.

Es ist $n = N(z) = N(z_1) \cdots N(z_m)$. Für jedes z_i ist $N(z_i) = p$ oder $N(z_i) = p^2$, jedem z_i ist also eine Primzahl zugeordnet.

Ist diese Primzahl $p \equiv 3 \mod 4$, so ist $N(z_i) = p^2$. In der Faktorisierung $n = 2^e \cdot p_1^{e_1} \cdots p_s^{e_s} \cdot q_1^{f_1} \cdots q_t^{f_t}$ handelt es sich also um eine der Primzahlen der Form q_j. Der

zugehörige Exponent f_j muss gerade sein, und $\frac{1}{2}f_j$ ist die Anzahl dieser Faktoren z_i. Hier gibt es keine Wahlmöglichkeit.

Für $p \equiv 1 \mod 4$ gibt es dagegen zwei mögliche Repräsentanten a, b mit Norm p. Wir haben demnach für vorgegebenes $e = e_i$ genau $e+1$ Möglichkeiten, um Produkte von a und b mit Norm p^e zu bilden, nämlich $a^e, a^{e-1}b, \ldots, ab^{e-1}, b^e$.

Beispiel. Gesucht seien alle Paare $[x, y] \in \mathbb{Z}^2$ mit $x^2+y^2 = 347\,633 = 11^2 \cdot 13^2 \cdot 17$ also alle Elemente $z = [x, y] \in \mathbb{Z}[i]$ mit Norm $N(z) = 347\,633$ (da $17 \equiv 1 \mod 4$, gibt es derartige Elemente z). Schreibe $z = \epsilon z_1 \cdot z_t$ mit einer Einheit ϵ und Repräsentanten z_i der Prim-Elemente. Offensichtlich ist $t = 4$ und wir können annehmen $N(z_1) = 11^2$, $N(z_2) = N(z_3) = 13$, und $N(z_4) = 17$. Demnach ist $z_1 = [11, 0]$. Für z_2 und z_3 gibt es die Möglichkeiten $[2, 3]$ und $[3, 2]$, für z_4 gibt es die Möglichkeiten $[1, 4]$ und $[4, 1]$. Insgesamt sehen wir also, dass $z_1 z_2 z_3 z_4$ eines der sechs Elemente

$$\begin{aligned}
&[11, 0][2, 3][2, 3][1, 4] = [-583, -88],\\
&[11, 0][2, 3][3, 2][1, 4] = [-572, 143],\\
&[11, 0][3, 2][3, 2][1, 4] = [-473, 352],\\
&[11, 0][2, 3][2, 3][4, 1] = [-352, 473],\\
&[11, 0][2, 3][3, 2][4, 1] = [-143, 572],\\
&[11, 0][3, 2][3, 2][4, 1] = [88, 583]
\end{aligned}$$

ist (die letzten drei Rechnungen hätten wir uns sparen können, hier handelt es sich nur um Ergebnisse, die durch Vertauschung von x und y aus den ersten drei Rechnungen gewonnen werden können). Also haben wir drei wesentlich verschiedene Darstellungen:

$$347\,633 = 88^2 + 583^2 = 143^2 + 572^2 = 352^2 + 473^2$$

(durch Vertauschung und durch Ersetzung von x und y durch $-x$ bzw. $-y$ erhält man insgesamt 24 derartige Darstellungen). Entsprechend liefert unsere Formel $\gamma(347\,633) = 4(e_1+1)(e_2+1) = 4 \cdot 3 \cdot 2 = 24$; hier ist e_1 der Exponent von 13 und e_2 der Exponent von 17.

Folgerung 1. *Die zahlentheoretische Funktion $\frac{1}{4}\gamma$ ist multiplikativ.*

Folgerung 2. *Ist p eine Primzahl mit $p \equiv 1 \mod 4$, so gibt es genau ein Paar natürlicher Zahlen $x < y$ mit $x^2 + y^2 = p$.*

Folgerung 3. *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:

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

6.2.5. Der Satz von Jacobi.

Satz (Jacobi). *Es ist* $\frac{1}{4}\gamma(n)$ *gleich der Differenz der Anzahl der Teiler* d *von* n *mit* $d \equiv 1 \mod 4$ *und der Anzahl der Teiler* d *von* n *mit* $d \equiv 3 \mod 4$

Beweis: Definiere eine Funktion $\alpha\colon \mathbb{N} \to \mathbb{Z}$ durch

$$\alpha(n) = \begin{cases} 0 & n \text{ gerade,} \\ 1 \quad \text{falls} & n \equiv 1 \mod 4, \\ -1 & n \equiv 3 \mod 4. \end{cases}$$

Diese Funktion ist multiplikativ (sogar stark multiplikativ) — wir kennen sie schon, es ist dies gerade der Restklassencharakter $\alpha = \chi_1^{(4)}$.

Also ist auch die summatorische Funktion $\delta = \alpha * U$ multiplikativ. Es ist

$$\delta(n) = \sum\nolimits_{d|n} \alpha(d),$$

dies ist also die Differenz der Anzahl der Teiler d mit $d \equiv 1 \mod 4$ und der Anzahl der Teiler d mit $d \equiv 3 \mod 4$.

Zu zeigen ist demnach:

$$\delta(n) = \begin{cases} (e_1+1)\cdots(e_s+1) & \text{falls alle } f_j \text{ gerade sind} \\ 0 & \text{sonst.} \end{cases}$$

Wegen der Multiplikativität von δ (und der Funktion, die rechts notiert ist), braucht man die Formel nur für Primzahlpotenzen $n = p^e$ zu beweisen. Sei also p eine Primzahl. Es ist

$$\delta(p^e) = \alpha(1) + \alpha(p) + \cdots + \alpha(p^e).$$

Für $p = 2$ steht hier $1+0+\cdots+0 = 1$. Für $p \equiv 1 \mod 4$ ist jeder Summand $\alpha(p^i) = 1$, also $\delta(p^e) = e+1$. Für $p \equiv 3 \mod 4$ ist $\alpha(1) + \alpha(p) + \cdots + \alpha(p^e) = 1 - 1 + 1 - \cdots$ mit insgesamt $e+1$ Summanden; also $\delta(p^e) = 1$ falls e gerade und $\delta(p^e) = 0$ falls e ungerade. Damit ist der Satz bewiesen.

6.3. Summen von vier 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*

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

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 $0 \leq x_i \leq \frac{p-1}{2}$ 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

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

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 $x_1^2 \equiv -x_2^2 - 1 \mod p$, 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

$$x_1^2 + x_2^2 + 1 \leq 2 \cdot (\tfrac{p-1}{2})^2 + 1 < p^2.$$

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 Repräsentanten, also wähle z_i mit $z_i \equiv x_i \mod a$ und $|z_i| \leq \frac{a}{2}$, für $i = 1, \ldots, 4$. Weil

a ungerade ist, gilt sogar $|z_i| < \frac{a}{2}$. Wären alle x_i 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 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

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

Die Multiplikativität der Summen von vier 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:

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

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:

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

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