1. Einleitung

Das Kreisproblem von Gauss beschäftigt sich mit der Frage, wie groß die Anzahl $G(r)$ der Punkte mit ganzzahligen Koordinaten, den so genannten Gitterpunkten in einem Kreis (mit Rand) mit dem Mittelpunkt $(0, 0)$ und dem Radius r ist. Eine erste Abschätzung für $G(r)$ lieferte Gauss Anfang des 19. Jahrhunderts. In der folgenden Arbeit wird diese Abschätzung vorgestellt und zudem zwei exakte Formeln zur Bestimmung von $G(r)$ gegeben.

Im folgenden sei für $r \in \mathbb{R}_{\geq 0}$

$G(r) = \#\{(x, y) \in \mathbb{Z}^2 | x^2 + y^2 \leq r^2\}$
$\quad$ = die Anzahl der Gitterpunkte im Kreis vom Radius r

Dabei fassen wir G als Funktion von $\mathbb{R}_{\geq 0} \to \mathbb{N}$ auf, also $G : \mathbb{R}_{\geq 0} \to \mathbb{N}$.
Für die z. B. gilt $G(0) = 1$.

Außerdem bezeichnen wir mit $[r] := max\{n \in \mathbb{Z} | n \leq r\}$ mit $r \in \mathbb{R}$ die Gaussklammer.

2. Abschätzung von Gauss

Um $G(r)$ abzuschätzen, zeichnen wir einen Kreis mit Mittelpunkt $(0,0)$ und Radius r und ein flächengleiches Quadrat.
Abb.
Um jeden Gitterpunkt im Kreis zeichnen wir Einheitsquadrate, also Quadrate mit Kantenlänge 1 (s. Abb.) Dieser Abbildung kann man entnehmen, dass das große Quadrat und der Kreis flächengleich sind. Dies lässt uns zu der Vermutung kommen, dass der Kreis und das Quadrat ungefähr die gleiche Anzahl an Gitterpunkten beinhalten, also dass gilt

$$G(r) \approx \pi r^2$$

Genauer gilt:

Satz 1 (Gauss): $G(r) \sim \pi r$, d. h. der Limes $\frac{G(r)}{\pi r^2}$ für $r \longrightarrow \infty$ existiert und ist gleich 1:

$$\lim_{r\to\infty} \frac{G(r)}{\pi r^2} = 1$$

Beweis: Um diesen Satz zu beweisen, betrachten wir wieder den Kreis mit Mittelpunkt $(0,0)$ und Radius r. Wie zeichnen die weiteren Gitterpunkte ein und rahmen diese wieder in Einheitsquadrate (s. Abb.)
Abb.
Die schattierte Fläche und $G(r)$ sind gleich. Wir sehen mit Hilfe der Abb., dass einige schattierte Flächen außerhalb des Kreises sind und dass der Kreis nicht vollständig schattiert ist. Diese Beobachtung verpflichtet uns $G(r)$ von oben und unten abzuschätzen. Dazu müssen wir den größten Kreis finden, der komplett schattiert ist und den kleinsten Kreis, welcher außerhalb vollständig unschattiert ist. Da die Diagonale der Einheitsquadrate $\sqrt{2}$ beträgt, müssen alle schattierten Quadrate im Kreis mit Radius $r + \frac{1}{2}\sqrt{2}$ liegen.
Abb.
Denn jeder Punkt $P \in \mathbb{R}^2$ befindet sich in einem Einheitsquadrat, dessen Mittelpunkt ein Gitterpunkt Q ist. Wie oben erwähnt, ist die Diagonale der Einheitsquadrate $\sqrt{2}$ lang. Somit ist der Radius des Umkreises $\frac{1}{2}\sqrt{2}$ lang. Da

das Einheitsquadrat in seinem Umkreis enthalten ist und jeder Punkt P sich in einem Einheitsquadrat befindet, ist jeder Punkt P höchstens $\frac{1}{2}\sqrt{2}$ von einem Gitterpunkt entfernt. Analoges gilt für den Kreis mit Radius $r - \frac{1}{2}\sqrt{2}$. Wir wollen diese Erkenntnisse nun formal aufschreiben und beweisen.

Lemma 1: Ist Q ein Gitterpunkt, der im Kreis vom Radius r um 0 liegt, so ist das Einheitsquadrat mit Mittelpunkt Q vollständig im Kreis vom Radius $r + \frac{1}{2}\sqrt{2}$ um 0 enthalten.

Beweis: Sei P ein Punkt in diesem Einheitsquadrat. Wir verwenden die Dreiecksungleichung: $\|Q\| = \|Q - P + P\| \leq \|P\| + \|Q - P\| \leq r + \frac{1}{2}\sqrt{2}$

Lemma 2: Sei U die Fläche, die aus allen Einheitsquadraten besteht, deren Gitterpunkte im Kreis vom Radius r um 0 liegen. Dann enthält U den Kreis vom Radius $r - \frac{1}{2}\sqrt{2}$ um 0.

Beweis: Sei $\|P\| \leq r - \frac{1}{2}\sqrt{2}$, wähle Q einen Gitterpunkt, dessen Einheitsquadrat P enthält; wie oben gilt dann $\|P - Q\| \leq \frac{1}{2}\sqrt{2}$ und wieder mit der Dreiecksungleichung $\|Q\| \leq \|P - Q\| + \|P\| \leq r$, d. h. Q ist ein Gitterpunkt, der im Kreis von Radius r um 0 liegt. Per Definition ist das zugehörige Einheitsquadrat in U enthalten und damit auch P.

Sei U wie in Lemma 2.
Es gilt:

i) Flächeninhalt $(U) = G(r)$

ii) Flächeninhalt $(U) \leq \pi(r + \frac{1}{2}\sqrt{2})^2$ nach Lemma 1

$$= \pi r^2 + \pi r\sqrt{2} + \frac{\pi}{2}$$

iii) Flächeninhalt $(U) \geq \pi(r - \frac{1}{2}\sqrt{2})^2$ nach Lemma 2

$$= \pi r^2 - \pi r\sqrt{2} - \frac{\pi}{2}$$

$$\Rightarrow \pi r^2 - \pi r\sqrt{2} - \frac{\pi}{2} \leq G(r) \leq \pi r^2 + \pi r\sqrt{2} + \frac{\pi}{2} \qquad |: \pi$$

$$\Leftrightarrow r^2 - r\sqrt{2} - \frac{1}{2} \leq \frac{G(r)}{\pi} \leq r^2 + r\sqrt{2} + \frac{1}{2} \qquad |: r^2$$

$$\Leftrightarrow 1 - \frac{\sqrt{2}}{r} - \frac{1}{2r^2} \leq \frac{G(r)}{\pi r^2} \leq 1 + \frac{\sqrt{2}}{r} + \frac{1}{2r^2} \qquad | -1$$

$$\Leftrightarrow -(\frac{\sqrt{2}}{r} + \frac{1}{2r^2}) \leq \frac{G(r)}{\pi r^2} - 1 \leq +\frac{\sqrt{2}}{r} + \frac{1}{2r^2}$$

$$\Leftrightarrow |\frac{G(r)}{\pi r^2} - 1| \leq \frac{\sqrt{2}}{r} + \frac{1}{2r^2} \longrightarrow 0 \text{ für } r \longrightarrow \infty$$

Also gilt $\lim\limits_{r\to\infty} \frac{G(r)}{\pi r^2} = 1$

Bemerkung 1: Äquivalent zum Satz von Gauss gilt: $\lim\limits_{r\to\infty} \frac{G(r)}{r^2} = \pi$

Sei $E(r) := G(r) - \pi r^2$ die Fehlerfunktion. Das Verhalten von $E(r)$ ist bis heute nicht gänzlich geklärt. Es wird vermutet, dass gilt

$$\forall\, \varepsilon > 0 : E(r) = O(r^{1/2+\varepsilon})$$

Das Zeichen O wurde von dem Mathematiker Edmund Landau eingeführt. Er bezeichnete damit, dass eine Funktion bis auf einen konstanten Faktor nicht schneller wächst als eine andere Funktion. Für die genaue Definition und Bedeutung siehe **[5]**. Seit mehr als 100 Jahren versuchen Mathematiker diese Abschätzung zu verbessern. Erst 1906 gelang es Sierpinski eine bessere Abschätzung zu beweisen. Seitdem gab es immer wieder Verbesserungen. Die bisher beste Abschätzung gelang Martin Huxley 2003 mit $E(r) = O(r^{131/208})$.

2. Ansatz

Für $n \in \mathbb{Z}_{\geq 0}$ sei $H(n) := \sharp\{(x,y) \in \mathbb{Z}^2 \mid x^2+y^2 = n\}$
Dies ist die Anzahl der Möglichkeiten, n als Summe von zwei Quadraten in $\mathbb{Z}$ zu schreiben.
Bei diesem Ansatz gehen wir wie folgt vor:
Wir betrachten wieder unser zweidimensionales Koordinatensystem und zeichnen nun Kreislinien. Wir zählen die Gitterpunkte auf den einzelnen Kreislinien und summieren diese dann auf, damit erhalten wir die Anzahl der Gitterpunkte bis zur größten betrachteten Kreislinie.
(Abb.)
Jede Kreislinie auf dem ein Gitterpunkt liegt, hat $r^2 \in \mathbb{Z}_{\geqslant 0}$ und die Anzahl der Gitterpunkte auf einer Kreislinie mit $r^2 = n \in \mathbb{Z}_{\geqslant 0}$ ist $H(n)$, also erhalten wir

$$G(r) = \sum_{n=0}^{[r^2]} H(n)$$

Korollar: $G : \mathbb{R}_{\geqslant 0} \longrightarrow \mathbb{N}$ ist eine monoton wachsende Treppenfunktion. Die Sprungstellen sind genau die Werte $r = \sqrt{n}$ mit $n \in \mathbb{Z}_{\geqslant 0}$ und $H(n) \neq 0$.

Beweis:

Treppenfunktion: Bevor wir zeigen, dass G eine Treppenfunktion ist, wollen wir definieren, was wir darunter verstehen.
Definition (Treppenfunktion) Eine Funktion f: $\mathbb{R} \longrightarrow \mathbb{R}$ heißt Treppenfunktion, wenn sie geschrieben werden kann, als $f(x) = \sum_{i=0}^{n} \alpha_i \chi_{A_i}(x)$ für ein reelles $x, n \geq 0, \alpha_i \in \mathbb{R}, A_i$ Intervalle und χ_A ist die charakteristische Funktion von A, für die gilt:
$\chi_A(x) = \begin{cases} 1, wenn\ x \in A \\ 0, wenn\ x \notin A \end{cases}$
Hier gilt nun
$G(r) = \sum_{n=0}^{[r^2]} H(n) = \sum_{n=0}^{[r^2]} H(n)\, \chi_{A_n}(r) = \sum_{n=0}^{[r^2]} H(n)\, \chi_{[n,n+1)}(r)$
mit $H(n) = \alpha(n)$

Wenn $r \in [i, i+1)$ für ein $i \in \mathbb{Z}_{\geqslant 0}$, dann ist $G(r) = \sum_{n=0}^{[r^2]} H(n)\, \chi_{[n,n+1)}(r)$

mit $\chi_{[n,n+1)}(r) = \begin{cases} 1, wenn\ r \in [n, n+1) = A_n, also\ n = i \\ 0, sonst \end{cases}$

Monotonie: Sei $r_1 \geq r_2$

1. Fall: $[r_1^2] = [r_2^2]$

$$\Rightarrow G(r_1) = \sum_{n=0}^{[r_1^2]} H(n) \geq \sum_{n=0}^{[r_2^2]} H(n) = G(r_2)$$

2. Fall: $[r_1^2] > [r_2^2]$

$$\Rightarrow G(r_1) = \sum_{n=0}^{[r_1^2]} H(n) = \sum_{n=0}^{[r_2^2]} H(n) + \sum_{n=[r_2^2]+1}^{[r_1^2]} H(n) > G(r_2)$$

Sprungstellen: Sei $r_1 < \sqrt{n} \Rightarrow r_1^2 < n \Rightarrow [r_1^2] < [n] = n$

$\Rightarrow G(r_1) < G(n)$ für alle $r_1 < \sqrt{n}$

$\Rightarrow r_1 = \sqrt{n}$ ist Sprungstelle

Sei $\sqrt{n-1} < r_1 < r_2 < \sqrt{n}$

$\Rightarrow n - 1 < (r_1)^2 < (r_2)^2 < n$

$\Rightarrow [n-1] = [(r_1)^2] = [(r_2)^2] < n$

$\Rightarrow G(\sqrt{n-1}) = G(r_1) = G(r_2)$, denn

$$\sum_{k=0}^{[n-1]} H(k) \leq \sum_{k=0}^{[r_1^2]} H(k) \leq \sum_{k=0}^{[r_2^2]} H(k) < \sum_{k=0}^{[n]} H(k)$$

Wegen $G(r) = \sum_{n=0}^{[r]} H(n)$ genügt es zur expliziten Bestimmung von $G(r)$,

eine explizite Formel für $H(n)$ anzugeben, wenn $n \in \mathbb{N}$. Dazu verwenden wir die Gaußschen Zahlen $\mathbb{Z}[i]$, die wir mit den Gitterpunkten $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ identifizieren, d. h. $x + iy$ entspricht dem Punkt (x, y), wenn $x, y \in \mathbb{Z}$. Wir schauen uns nun einige Eigenschaften von $\mathbb{Z}[i]$ an, dazu richten wir uns nach **[6]**. Zunächst definieren wir die Begriffe Ring, Ideal und Integritätsring.

Definition (Ring) Ein Ring R ist eine Menge mit zwei assoziativen Verknüpfungen + und $\cdot$, so dass folgende Gesetze gelten:

1) $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.

2) $(R, \cdot)$ besitzt ein neutrales Element 1.

3) Für alle $a, b, c \in R$ gelten die Distributivgesetze $(a+b)c = ac+bc$ sowie $a(b+c) = ac+bc$.

Also ist ein Ring eine Menge mit zwei Operationen für die diese Axiome erfüllt sind.

Der Ring $(R, +, \cdot)$ heißt

* kommutativ, wenn $(R, \cdot)$ kommutativ ist, d.h. es gilt $ab = ba$ für alle $a, b \in R$.

* Ring mit 1, wenn er ein Einselement $1 \neq 0$ besitzt, d.h. $(R, \cdot)$ besitzt ein neutrales Element 1, das vom neutralen Element 0 von $(R, +)$ verschieden ist.

Bsp.: Die Menge $\mathbb{Z}$ bildet mit ihren Verknüpfungen + und $\cdot$ einen kommutativen Ring mit 1.

Definition (Integritätsring) Ein kommutativer Ring R heißt Integritätsring, wenn er außer der Null keine Nullteiler besitzt, d.h. wenn für alle $a, b \in R$ gilt: ist $ab = 0$, so ist bereits $a = 0$ oder $b = 0$.
Bsp.:

$\mathbb{Z}$ ist ein Integritätsring, denn aus $ab = 0$ folgt $a = 0$ oder $b = 0$

$\mathbb{Z}/6\mathbb{Z}$ ist kein Integritätsring, denn $2 \cdot 3 = 6 = 0$, aber $2 \neq 0 \neq 3$

Definition (Ideal) Sei R ein Ring, $I \subseteq R$. Man nennt I ein Ideal von R, falls gilt:

1) $0 \in I$

2) $\forall a, b \in I$ ist $a + b \in I$

3) $a \in I$ und $r \in R \Rightarrow r \cdot a \in I$, $a \cdot r \in I$

   Man spricht von einem Linksideal, falls statt 3) nur $r \cdot a \in I$ gilt und von einem Rechtsideal, falls nur $a \cdot r \in I$ gilt.

Definition (Teilbarkeit, Einheiten, Assoziiertheit) Sei R ein Integritätsring und $a, b \in R$.

1) a teilt b, falls $b = ac$ für ein $c \in R$. Dies schreibt man als $a \mid b$. Nicht-Teilbarkeit wird als $a \nmid b$ notiert.

2) Die Einheiten des Ringes sind die Teiler der Eins, $R^\times := \{u \in R : u \mid 1\}$

3) Die Elemente a, b heißen assoziiert, falls sie sich nur um eine Einheit unterscheiden, also $a = ub$ für ein $u \in R^x$.

Assoziiertheit in $\mathbb{Z}$
Seien $a, b \in \mathbb{Z}$. a und b heißen assoziiert, falls ein $e \in \mathbb{Z}^\times$ existiert für das gilt $a = eb$

$$\mathbb{Z}^\times = \{u \in \mathbb{Z} : u \mid 1\} = \{u \in \mathbb{Z} \; \exists \; \tilde{u} \in \mathbb{Z} \; mit \; 1 = \tilde{u}u\}$$

d.h. alle invertierbaren Elemente

$$= \{+1, -1\}$$

Also sind a, b assoziiert genau dann, wenn $a = \pm b$ gilt.

Lemma 3
Für Elemente in einem Integritätsring gilt:

1) $a \mid b \Rightarrow a \mid bc$

2) $a \mid b_1$ und $a \mid b_2 \Rightarrow a \mid c_1 b_1 + c_2 b_2$ für alle $c_1, c_2 \in R$

3) $a \mid b \Leftrightarrow ca \mid cb$, falls $c \neq 0$

4) $a \mid b$ und $b \mid c \Rightarrow a \mid c$

5) $a \mid b$ und $b \mid a \Leftrightarrow a = ub$ für ein $u \in R^\times$

Beweis:

1) $a \mid b$, d.h. nach Definition $b = af$ für ein $f \in R$. Wir multiplizieren c an $b = af$, also $b = af \Rightarrow bc = a \underbrace{fc}_{\in R} \Rightarrow a \mid bc$

2) $a \mid b_1$, d.h. $b_1 = t_1 a$ für ein $t_1 \in R$

   $b_2 = t_2 a$ für ein $t_2 \in R$

   Mit 1) gilt: $a \mid b_1 \Rightarrow a \mid b_1 c_1$ für alle $c_1 \in R$

   $a \mid b_2 \Rightarrow a \mid b_2 c_2$ für alle $c_2 \in R$

   $a \mid b_1 c_1$, d.h. $b_1 c_1 = a f_1$ für ein $f_1 \in R$

   $a \mid b_2 c_2$, d.h. $b_2 c_2 = a f_2$ für ein $f_2 \in R$

   Wir addieren beide Gleichungen und erhalten

   $b_1 c_1 + b_2 c_2 = a f_1 + a f_2 \Leftrightarrow b_1 c_1 + b_2 c_2 = a \underbrace{(f_1 + f_2)}_{:=f}$, also $b_1 c_1 + b_2 c_2 = af$

   und somit $a \mid c_1 b_1 + c_2 b_2$

3) " $\Rightarrow$ "

   $a \mid b$, d.h. $b = ta$ für ein $t \in R$

   zu zeigen: $\exists\ f \in R : cb = fca$

   Es gilt: $b = ta \Rightarrow cb = \underbrace{cta}_{R\ kommutativ} = tca$, wählen also $f = t$.

   " $\Leftarrow$ "

   $ca \mid cb$, d.h. $cb = tca$ für ein $t \in R$

   $cb = tca \Leftrightarrow 0 = cb - cta \Leftrightarrow 0 = c(b - ta)$, da $c \neq 0$ gilt und da R ein Integritätsring ist, folgt $b - ta = 0 \Leftrightarrow b = ta$, also $a \mid b$

4) $a \mid b$, d.h. $b = ad$ für ein $d \in R$

$b \mid c$, d.h. $c = be$ für ein $e \in R$.
Wir setzen $b = ad$ in $c = be$ ein, also $c = a \underbrace{de}_{\in R}$, also $c = af$ für ein $f \in R$

5) " $\Rightarrow$ "

$a \mid b$, d.h. $b = ad$ für ein $d \in R$

$b \mid a$, d.h. $a = bc$ für ein $c \in R$
Wir sehen: Ist $a = 0$ oder $b = 0$, so sind tatsächlich beide gleich 0 und daher assoziiert. Wir können daher ohne Einschränkung $a \neq 0$ und $b \neq 0$ annehmen.

Wir setzen beide Gleichungen ineinander, so dass wir folgendes erhalten

$b = bcd$ und $a = adc$

Wir können nun durch a und b kürzen, denn $a \neq 0$ und $b \neq 0$ und erhalten $cd = 1$ und somit $c \in R^\times$

" $\Leftarrow$ "

Sei $a = bc$ mit einem $c \in R^\times$.

Wir können dies dann auch als $b = ac^{-1}$ schreiben und erhalten $a \mid b$ und $b \mid a$

Euklidische Ringe

Ein Integritätsring R heißt euklidisch, falls eine Norm-Funktion

$$N : R \setminus \{0\} \to \mathbb{N}_0$$

existiert, so dass gilt:

Sind $a, b \in R$ mit $b \neq 0$, dann gibt es $q, r \in R$ mit $a = qb + r$, wobei entweder $r = 0$ oder $r \neq 0$ und $N(r) < N(b)$ gilt.

Bsp. 1: $R = \mathbb{Z}$ mit $N(z) = |z|$, $\mathbb{Z}$ ist laut letztem Vortrag euklidisch.

Bsp. 2: $K[X] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in R, n > 0, n \in \mathbb{N}\}$ Polynomring über einen Körper K. Die Normfunktion N ist hier durch die Gradabbildung gegeben. Wir nehmen uns zwei Polynome aus $K[X]$ und führen die übliche Division mit Rest durch.
Seien z.B. $a = x^2 + x - 1$ und $b = x - 5$
Nun gilt:

$$\begin{array}{r} \left(\quad x^2 \quad + x \quad - 1 \right) \div \left(x - 5 \right) = x + 6 + \dfrac{29}{x-5} \\ \underline{-\,x^2 + 5x} \\ \qquad\qquad 6x \quad - 1 \\ \qquad\quad \underline{-\,6x + 30} \\ \qquad\qquad\quad\; 29 \end{array}$$

Laut Definition gilt $a = qb + r$ mit $q = x + 6$ und $r = 29$, also
$(x^2 + x - 1) = (x + 6)(x - 5) + 29$ und $1 = grad(b) > grad(r) = 0$

Gaußsche Zahlen

Die Gaußschen Zahlen sind definiert als

$$\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$$

Sie sind abgeschlossen bzgl. der Addition und Multiplikation und bilden somit einen Ring.
Sie bilden einen Unterring der komplexen Zahlen, denn es gilt für $a, b, c, d \in \mathbb{Z}$

i) $a + ib - (c + id) = a - c + i(b - d)$

ii) $(a + ib)(c + id) = ac - bd + i(ad + bc)$

Wir können nun sehen, dass die Ergebnisse wieder Gaußsche Zahlen bilden, denn Summen, Differenzen und Produkte ganzer Zahlen sind wieder ganze Zahlen. Um zu zeigen, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist, definieren wir uns folgende Norm:

$$N : \mathbb{Z}[i] \to \mathbb{N}_0$$

$$z \mapsto |z|^2 = z\overline{z}$$

Wir zeigen die Wohldefiniertheit und folgern daraus die Existenz:
Sei $z \in \mathbb{Z}[i]$ mit $z := a + bi$ für $a, b \in \mathbb{Z}$ Es gilt $N(z) = |z|^2 = z\overline{z} = (a + ib)(a - ib) = a^2 + b^2$
Für a^2+b^2 gilt, dass sie $\in \mathbb{Z}$ und ≥ 0 und damit $\in \mathbb{N}_0$ sind. Damit ist N wohldefiniert, d.h. es existiert eine Norm-Funktion auf $\mathbb{Z}[i]$. Bevor wir nun zeigen, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist, schauen wir uns wichtige Eigenschaften von N an.

1) $N(z) = 0 \Leftrightarrow z = 0$

2) $N(wz) = N(w)N(z) \ \forall \ w, z \in \mathbb{Z}[i]$

Beweis:

1) $N(z) = 0 = |z^2| = z\overline{z} = a^2 + b^2 = 0 \Leftrightarrow a = 0$ und $b = 0$, da a^2 und $b^2 \in \mathbb{N}_0$

2) $N(w)N(z) = w\overline{w}z\overline{z} = (a^2 + b^2)(x^2 + y^2) = a^2x^2 + b^2x^2 + a^2y^2 + b^2y^2$ mit $w := a + ib$ und $z := x + iy$

   $N(wz) = wz\overline{wz} = (a+ib)(x+iy)(a-ib)(x-iy) = a^2x^2+b^2x^2+a^2y^2+b^2y^2$

   $\Rightarrow N(wz) = wz\overline{wz} = w\overline{w}z\overline{z} = N(w)N(z)$

Mit Hilfe dieser Eigenschaften berechnen wir die Einheiten von $\mathbb{Z}[i]$
$z \in \mathbb{Z}[i]^\times \Leftrightarrow z \mid \underbrace{1}_{1+0i}$, d.h. es existiert $\widehat{z}$ mit $1 = z\widehat{z}$
$\underbrace{N(1)}_{|1^2|} = N(z\widehat{z}) = N(z)N(\widehat{z}) = 1 \Rightarrow N(z) = 1$

und $N(\widehat{z}) = 1$, da $N(z)$ und $N(\widehat{z}) \in \mathbb{N}_0$

Es folgt $\mathbb{Z}[i]^x = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$
D.h. Einheiten haben die Eigenschaft, dass sie Norm 1 haben, also $N(z) = 1$ nach der Rechnung.
Wie sieht $\mathbb{Z}[i]^\times$ nun konkret aus?
$N(z) = N(a+ib) = a^2+b^2 = 1 \Rightarrow a = \pm 1$ und $b = 0$ oder $a = 0$ und $b = \pm 1$, d.h. $\pm 1 + 0i$ oder $0 \pm 1i$, d.h. $z \in \{\pm 1, \pm i\}$

Zurück zum Beweis: Wir wollen nun zeigen: Sind $a, b \in \mathbb{Z}[i], b \neq 0$, so gibt es $q, r \in \mathbb{Z}[i]$ mit

$$a = qb + r \begin{cases} r = 0 \; oder \\ r \neq 0 \; und \; N(r) < N(b) \end{cases}$$

Wir bezeichnen ihren Quotienten $\frac{a}{b}$ in $\mathbb{C}$ mit c. Es gilt $c = u+iv$ mit $u, v \in \mathbb{Q}$. Wir wählen $ú, ý \in \mathbb{Z}$ mit der Eigenschaft $|u - ú| \leq \frac{1}{2}$ und $|v - ý| \leq \frac{1}{2}$. Wir setzen $q := ú + iý \in \mathbb{Z}[i]$ und $r = a - bq$.
Dann gilt $|c - q|^2 = |u - ú|^2 + |v - ý|^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$

$$\Rightarrow N(r) = |r|^2 = |a - bq|^2 = |cb - qb|^2 \leq \tfrac{1}{2}|b|^2 = \tfrac{1}{2}N(b) < N(b)$$

Bsp.: Seien $a = 3 - 2i$ und $b = 1 - 2i$.

Wir erhalten als Quotienten

$\frac{3-2i}{1-2i} = \frac{(3-2i)(1+2i)}{(1-2i)(1+2i)} = \frac{3-2i+6i-4i^2}{1^2+2^2} = \frac{7}{5} + \frac{4i}{5}$, also c= $\frac{7}{5} + \frac{4i}{5}$.

Nun suchen wir uns $ú$ und $ý$, so dass gilt $|\frac{7}{5} - ú| \leq \frac{1}{2}$ und $|\frac{4}{5} - ý| \leq \frac{1}{2}$.
Wie wählen für $ú = 1$ und $ý = 1$ Somit erhalten wir für $q = 1+1i = 1+i$.
Damit erhalten wir für $r = (3 - 2i) - (1 - 2i)(1 + i) = 0 - i$
Daraus folgt $1 = N(r) < N(b) = 5$. Wir zeigen nun, dass $\mathbb{Z}[i]$ faktoriell ist.

Definition(Hauptidealring): Ein Integritätsring heißt Hauptidealring, falls jedes Ideal I in R ein Hauptideal ist, d. h. $I = (a) := Ra := ra | r \in R$ für ein $a \in R$

Satz 2: Jeder euklidische Ring ist ein Hauptidealring.

Beweis: Sei $I \neq 0$ ein Ideal. Wir wählen $a \in I \setminus 0$ mit minimaler Norm $N(a)$. Wir behaupten, dass gilt $I = (a)$. Sei $b \in I$ beliebig. Wir müssen zeigen, dass $b \in (a)$ gilt. Da wir einen euklidischen Ring vorausgesetzt haben, gibt es q, r mit $b = qa + r$ und $r = 0$ oder $N(a) < N(b)$. Da $r = b - qa \in I$ mit $a, b \in I$ folgt $r \in I$. Aus $N(a) < N(b)$ und der Wahl von $N(a)$, nämlich minimal, folgt $r = 0$. Damit gilt $r = 0$. Also erhalten wir $0 = b - qa \Leftrightarrow b = qa$, damit $b \in (a)$.

Definition (prim, irreduzibel, reduzibel): Sei R ein Integritätsring und

$0 \neq p \in R \setminus R^x$.

i) p heißt prim, falls für alle $r, s \in R$ aus $p \mid rs$ folgt, dass $p \mid r$ oder $p \mid s$

ii) p heißt irreduzibel, falls aus $p = rs$ für $r, s \in R$ folgt, dass p zu r oder s assoziiert ist. (Der andere Faktor ist damit eine Einheit)

iii) p heißt reduzibel, falls p nicht irreduzibel ist.

Bemerkung 2: Ein primes Element ist immer irreduzibel.

Beweis: Sei p primes Element mit $p = ab$. Wir müssen zeigen, dass $a \in R^x$ oder $b \in R^x$ gilt. Da p prim ist, gilt mit der Definition, dass $p \mid a$ oder $p \mid b$. O.B.d.A. gelte $p \mid a$. Mit der Teilbarkeitsdefintion gilt also $a = pr$ mit $r \in R$. Damit erhalten wir $p = ab = (pr)b = (rb)p$. Da R ein Integritätsring ist, gilt: $p = ab = prb = rbp$. Kürzen von p liefert $rb = 1$, also ist $b \in R^x$ und $a = pr$ assoziiert zu p.

Definition(faktorieller Ring): Ein faktorieller Ring ist ein Integritätsring, in dem jedes Element, das weder Null noch eine Einheit ist, in ein Produkt von Primelementen zerlegt werden kann. (Primfaktorzerlegung)

Lemma 4: In einem faktoriellen Ring ist ein irreduzibles Element prim.

Beweis: Da sich ein irreduzibles Element nicht weiter in Primfaktoren zerlegen lässt, muss es in einem faktoriellen Ring prim sein.

Satz 3: Für ein Integritätsring sind aquivalent:

1) R ist faktoriell.

2) Jedes Element, das weder Null noch eine Einheit ist, kann in ein Produkt von Primelementen zerlegt werden, wobei die Faktoren bis auf Assoziiertheit und Reihenfolge der Faktoren eindeutig sind.

3) Jedes Element, das weder Null noch eine Einheit ist, kann in ein Produkt von irrdeuziblen Elementen zerlegt werden, wobei die Faktoren bis auf Assoziiertheit und Reihenfolge der Faktoren eindeutig sind.

4) Jedes Element, das weder Null noch eine Einheit ist, kann in ein Produkt von irreduziblen Elementen zerlegt werden. Weiter ist jedes Element irreduzible Element prim.

Beweis: s. [**6**] S. 9

Satz 4: Jeder Hauptidealring ist faktoriell.

Beweis: s. [**6**] S. 9

Im folgenden möchten wir die **Primelemente** in $\mathbb{Z}[i]$ bestimmen:
Die Einheiten $\pm 1, \pm i$ in $\mathbb{Z}[i]$ haben die Norm 1. Sei $\pi \in \mathbb{Z}[i]$ prim. Wegen $N(\pi) = \pi\overline{\pi} \in \mathbb{Z}$, gilt $\pi \mid N(\pi)$ (Definition der Teilbarkeit). Da $N(\pi) \neq \pm 1$ teilt π auch eine Primzahl p. Da $p \mid \pi$ gilt, können wir schreiben $p = \pi z$ für ein $z \in \mathbb{Z}[i]$. Es folgt $N(\pi)N(z) = N(p) = p^2$. Also gilt entweder $N(\pi) = p$ oder π ist assoziiert zu p.

i) $N(\pi) = p$ ist prim, denn aus $\pi = ab$ folgt $p = N(\pi) = N(ab) = N(a)N(b)$, damit ist $N(a)$ oder $N(b)$ eins und a und b eine Einheit. Damit ist π irreduzibel, da $\mathbb{Z}[i]$ faktoriell ist, ist π damit prim.

ii) Wir betrachten eine Primzahl $p \in \mathbb{P}$. Wegen $2 = (1+i)(1-i)$ ist 2 nicht prim in $\mathbb{Z}[i]$. Sei $p \in \mathbb{P}$ eine ungerade Primzahl. Wir wollen zeigen, dass p genau dann prim in $\mathbb{Z}[i]$ ist, wenn p nicht die Summe der Quadrate zweier natrlicher Zahlen ist. Sei $p = x^2+y^2$ die Summe zweier Quadrate, dann ist p wegen $p = (x+iy)(x-iy)$ und $N(x \pm iy) = p \neq 1$ nicht prim. Andererseits sollte p nicht prim sein, so gibt es Nichteinheiten $a, b \in \mathbb{Z}[i]$ mit $p = ab$. Wegen $p^2 = N(p) = N(a)N(b)$ und $N(a), N(b) \neq 1$ folgt $N(a) = N(b) = p$. Falls $a = x + iy$ ist, ist $p = N(a) = x^2 + y^2$ die Summe zweier Quadrate.

Daraus folgt: Primelemente in $\mathbb{Z}[i]$ sind bis auf Assoziiertheit die Zahlen mit einer Norm, die eine Primzahl in $\mathbb{Z}$ sind und die Primzahlen in $\mathbb{Z}$ der Form $p = 4k+3$. Wie wir gleich sehen werden können Primzahlen dieser Form nicht als Summen der Quadrate zweier natrlicher Zahlen geschrieben werden.

Als nächstes schauen wir uns die **Quadratsätze** an.

Satz 5 (erster Qudratsatz): Eine Primzahl p ist genau dann als Summe zweier Quadrate darstellbar, wenn $p = 2$ oder wenn $p \equiv 1 \ (mod\ 4)$ ist.

Bevor wir diesen Satz beweisen, wollen wir ein Lemma beweisen, das wir gleich benötigen werden.

Lemma 5: Sei p eine Primzahl. Die Kongruenz $x^2 \equiv -1 \ (mod\ p)$ ist genau

dann lösbar, wenn $p \equiv 1 \ (mod\ 4)$ ist.

Für den Beweis schauen wir uns folgende Definition und Satz an.

Definition (Legendre-Symbol): Für eine Primzahl $p \in \mathbb{P}$ ist das Legendre-Symbol $(\frac{a}{p})$ definiert durch $(\frac{a}{p}) = \begin{cases} +1, falls\ x^2 \equiv a\ mod\ p\ lösbar\ ist\ und\ a \equiv 0\ mod\ p\ nicht\ gilt \\ -1, falls\ x^2 \equiv a\ mod\ p\ nicht\ lösbar\ ist \\ 0, falls\ a \equiv\ 0\ mod\ p \end{cases}$

Satz 6 (Euler): Sei p eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Dann gilt:
$\frac{a}{p} = a^{p-1/2} (mod\ p)$
Beweis: s. **[6]** S. 52-53

Beweis von Lemma 5: Sei $x^2 \equiv -1 \ (mod\ p)$ lösbar. Mit dem Legendre-Symbol erhalten wir hier für $a = -1$:

$$\frac{-1}{p} = 1$$

Mit dem Satz von Euler gilt:

$$\frac{-1}{p} = (-1)^{\frac{p-1}{2}} \ (mod\ p).$$

Wir setzen dies gleich und erhalten

$$1 = (-1)^{\frac{p-1}{2}}$$

Diese Gleichung gilt nur, wenn $\frac{p-1}{2}$ gerade ist, d. h. es gibt $k \in \mathbb{Z}$ mit $\frac{p-1}{2} = 2k$. Durch Umformung erhalten wir $p = 4k + 1 \Leftrightarrow p \equiv 1 \ (mod\ 4)$, denn $4 \mid p - 1$, d. h. es existiert k mit $(p - 1) = 4k \Leftrightarrow p = 4k + 1$.

Beweis des ersten Quadratsatzes

- Für $p = 2$ gilt $2 = 1^2 + 1^2$
- $p \equiv 1\ mod\ 4$
  Modulo 4 sind alle Quadrate $0, (\pm 1)^2 = 1, 2^2 = 0$. Aus diesem Grund

muss für $p \equiv 1 \ (mod\ 4)$ oder $p \equiv 0 \ (mod\ 2)$ gelten. Nach Lemma 5 existiert ein $a \in \mathbb{N}$ mit $a^2 \equiv -1 \ (mod\ p)$. Deshalb können wir ein $k \in \mathbb{N}$ mit $a^2 + 1 = kp$ finden. Wir betrachten diese Gleichung in dem Ring $\mathbb{Z}[i]$: $a^2 + 1 = (a + i)(a - i) = kp(*)$
Sei $x + iy = ggT(a + i, p)$
Behauptung: $p = N(x + iy) = x^2 + y^2$ gilt.
Die Aussage des Satzes wäre damit bewiesen.
Aus $x + iy \mid p$ folgt $N(x + iy) = N(p) = p^2$, denn $x + iy \mid p$ bedeutet $p = \alpha(x + iy)$ für geeignetes $\alpha \in \mathbb{Z}[i]$. Dies sehen wir so:
$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2$
$N(p) = p^2 = pp = \alpha(x + iy)\overline{\alpha(x + iy)} = \alpha(x + iy)\overline{\alpha}(x - iy) = \alpha\overline{\alpha}(x + iy)(x - iy) = \alpha\overline{\alpha}N(x + iy)$
$\Rightarrow N(x + iy) \mid N(p) = p^2$.
Wir schließen nun die Fälle $N(x + iy) = 1$ oder $N(x + iy) = p^2$ aus.
Angenommen $N(x + iy) = p^2$ gilt. Wegen $x + iy \mid p$ existiert $\beta \in \mathbb{Z}[i]$ mit $p = \beta(x + iy)$
Wir wenden die Normfunktion an: $p^2 = N(p) = N(x + iy)N(z) = p^2N(z) \Rightarrow N(z) = 1$ und damit $z \in \mathbb{Z}[i]^x = \pm 1, \pm i$
Es folgt $x = 0$ oder $y = 0$, was wegen $x + iy \mid a + i$ unmöglich ist, denn nehmen wir an, dass $y = 0$ ist, d. h. $x \mid a + i$, d. h. $a + i = x(c + id) = xc + xdi$ mit $c + id \in \mathbb{Z}[i]$.
Wir müssen beachten, dass $a, x, c, d \in \mathbb{Z}$ sind, damit erhalten wir $xd = 1$, d. h. $x = \pm 1$.
Dann ist jedoch $N(x + iy) = 1$, d. h. $a + i$ und p sind teilerfremd. Da p keine Einheit ist, hat es einen Primteiler. Nach (*) muss dieser $a + i$ oder $a - i$ teilen.
Das heißt für $z \in \mathbb{Z}[i]$ Primelement gilt $z \mid p \mid kp = (a + i)(a - i) \Rightarrow z \mid (a + i)$ oder $\mid (a - i)$
Angenommen $z \mid a - i$ $z \mid p$ heißt mit der Teilbarkeitsdefinition $p = zz'$ mit geeignetem $z' \in \mathbb{Z}[i] \Rightarrow p = \overline{p} = \overline{z}\overline{z'}$, d. h. auch $\overline{z}$ teilt p; auf der anderen Seite gilt aber analog $z \mid a - i \Rightarrow \overline{z} \mid \overline{a - i} = a + i$
Daraus kann man folgern, dass man durch Ersetzung von z durch $\overline{z}$, annehmen kann, dass $z \mid a + i$. Hierfür beachten wir, dass auch $\overline{z}$ ein Teiler von p ist (s.o.) und sogar ein Primteiler, denn sei $z \in \mathbb{Z}[i]$ ein Primelement, dann ist auch $\overline{z} \in \mathbb{Z}[i]$ ein Primelement.
Das kann man leicht sehen: $z \neq 0 \Rightarrow \overline{z} \neq 0$ $z \notin \mathbb{Z}[i]^x \Rightarrow \overline{z} \notin \mathbb{Z}[i]^x$ wegen $\mathbb{Z}[i]^x = \pm 1, \pm i$

$\overline{z} \mid rs \Rightarrow z\overline{\overline{z}} \mid \overline{rs} = \overline{r}\overline{s} \Rightarrow z \mid \overline{r}$ oder $z \mid \overline{s} \Rightarrow \overline{z} \mid r$ oder $\overline{z} \mid s$.
Also folgt insgesamt, dass $a + i$ geteilt wird. Dies ist ein Widerspruch zur Teilerfremdheit von $a + i$ und p.

Satz 7 (Zweiter Quadratsatz): Sei $n \in \mathbb{N}$ und $n = 2^{\nu} \prod_{p \equiv 1 \ mod \ 4} p^{n_p} \prod_{q \equiv 3 \ mod \ 4} q^{n_q}$ seine Primfaktorzerlegung, aufgeteilt in Zweierpotenzen, Potenzen von Primzahlen $p \equiv 1 \ mod \ 4$ und Potenzen von Primzahlen $q = 3 \ mod \ 4$. Dann ist n genau dann als Summe zweier Quadrate darstellbar, wenn alle n_q gerade sind.

Beweis: Sei $n = 2^{\nu} \prod_{p \equiv 1 \ mod \ 4} p^{n_p} \prod_{q \equiv 3 \ mod \ 4} q^{n_q}$
Zwei Zahlen, die als Summe zweier Quadrate darstellbar sind, deren Produkt ist dann auch als Summe zweier Quadrate darstellbar. Mit $n = x^2 + y^2$ und $m = a^2 + b^2$ gilt:
$(x^2 + y^2)(a^2 + b^2) = N(x + yi)N(a + bi) = N((x + yi)(a + bi)) = N((xa - yb) + (ay + xb)i)) = (xa - yb)^2 + (ay + xb)^2$
Sei die Bedingung an die Primfaktorzerlegung von n nicht erfüllt, aber es gelte trotzdem $n = x^2 + y^2$. Wir können dann $x^2 + y^2 = mp^{2k+1}$ schreiben mit einem $p \in \mathbb{P}$ mit $p \equiv 3 \ mod \ 4$ und $ggT = 1$ Wir dürfen annehmen, dass $p \nmid y$ gilt, denn falls $p \mid y$, dann gilt auch $p \mid x$ und die ganze Gleichung kann durch p^2 dividiert werden.
Es folgt nun $x^2 + y^2 \equiv 0 \ mod \ p$
$\Rightarrow x^2 \equiv -y^2 \ mod \ p$
$\Rightarrow (\frac{x}{y})^2 \equiv -1 \ mod \ p$
Dies ist aber mit Lemma 5 unmöglich, da $p \equiv 3 \ mod \ 4$ **Satz 8** Sei $n = 2^{\nu} \prod_{p \equiv 1 mod 4} p^{n_p} \prod_{q \equiv 3 mod 4} q^{n_q}$ wie in Satz 7 und alle n_q gerade,
d. h. $H(n) \neq 0$.
Dann gilt:

$$H(n) = 4 \prod_{p \equiv 1 \ mod \ 4} (1 + n_p)$$

Um diesen Satz zu zeigen, definieren wir uns eine Abbildung:

$$\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\} \longrightarrow \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = n\}$$

mit

$$(x, y) \longmapsto x + iy,$$

was bijektiv ist, also

$$H(n) =\mid \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = n\} \mid$$

Wie wir oben bereits gezeigt haben, ist $\mathbb{Z}[i]$ faktoriell und die Primelemente lauten (bis auf Assoziiertheit):

- $1 + i$
- p, wobei $p \in \mathbb{N}$ eine Primzahl $\equiv 3\ mod\ 4$ ist
- $p_1 = x + iy$
  $p_2 = x - iy$, falls $x, y \in \mathbb{N}$ mit $p := x^2 + y^2$ prim in $\mathbb{Z}$
  (die Primzahlen p die hierbei auftauchen, sind genau diejenigen $p \equiv 3\ mod\ 4$)

Daraus können wir folgern:
Jedes $\alpha \in \mathbb{Z}_{[}i]$ besitzt eine eindeutige Darstellung

$$\alpha = u \cdot (1 + i)^{n(2)} \cdot \prod_{p \equiv 3 mod 4} p^{n(p)} \prod_{p \equiv 1 mod 4} ({p_1}^{n(p_1)} \cdot {p_2}^{n(p_2)})$$

mit einer eindeutig bestimmten Einheit $u \in \mathbb{Z}[i]^x = \pm 1, \pm i$ und eindeutig bestimmten natürlichen Zahlen $n(2), n(p), n(p_1), n(p_2)$, die fast alle 0 sind.
Das bedeutet, dass α ein endliches Produkt von Primelementen ist.
Wir nehmen an, dass $N(\alpha) = n$ ist.
Wir schreiben n als Primfaktorzerlegung in $\mathbb{Z}$:

$$n = 2^{m(2)} \cdot \prod_{p \equiv 3 mod 4} p^{m(p)} \prod_{p \equiv 1 mod 4} p^{m(p)}$$

Es gilt:

$$2^{m(2)} \cdot \prod_{p \equiv 3 mod 4} p^{m(p)} \prod_{p \equiv 1 mod 4} p^{m(p)} = n = N(\alpha) = N(u) \cdot N(1+i) \cdot \prod_{p \equiv 3 mod 4} N(p)^{n(p)} \cdot \prod_{p \equiv 1 mod 4} N(p_1)^{n(p_1)} \cdot N(p_2)^{n(p_2)} = 2^{n(2)} \cdot \prod_{p \equiv 3 mod 4} p^{2n(p)} \cdot \prod_{p \equiv 1 mod 4} p^{n(p_1)+n(p_2)})$$

Wegen der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ folgt

- $n(2) = m(2)$
- $2n(p) = m(p)$, falls $p \equiv 3 \ mod \ 4$
- $n(p_1) + n(p_2) = m(p)$, falls $N(p_1) = N(p_2) = p \equiv 1 \ mod \ 4$

Daraus folgt:

- $N(\alpha) = n$ kann nur gelten, wenn alle $m(p), p \equiv 3 \ mod \ 4$, gerade sind, d. h. alle Primteiler von n mit $p \equiv 3 \ mod \ 4$ müssen mit geradem Exponenten auftreten (andernfalls gilt $H(n) = 0$).
- In diesem Fall sind die Exponenten $n(2) = m(2)$ und $n(p) = \frac{m(p)}{2}, p \equiv 3 \ mod \ 4$, in der Primfaktorzerlegung von α in $\mathbb{Z}[i]$ eindeutig durch n bestimmt, d. h. es gibt keine Wahlmöglichkeiten.
- Bei den Exponenten $n(p_1)$ und $n(p_2)$ mit $N(p_1) = N(p_2) = p \equiv 1 \ mod \ 4$ hat man aber mehrere Möglichkeiten; es muss lediglich die Bedingung $n(p_1) + n(p_2) = m(p)$ erfüllt sein, d. h. dass das Paar $(n(p_1), n(p_2))$ in der Menge $\{(j, m(p) - j) \mid 0 \leq j \leq m(p)\}$ der Mächtigkeit $1 + m(p)$ liegt und für jedes solche p hat man $1 + m(p)$ Möglichkeiten, die Exponenten $n(p_1)$ und $n(p_2)$ zu wählen; aufgrund der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[i]$ erhälten wir dadurch paarweise verschiedene α's!

Insgesamt gibt es $H(n) = 4 \cdot \prod_{p \equiv 1 mod 4} 1 + m(p)$ verschiedene $\alpha \in \mathbb{Z}[i]$ mit $N(\alpha) = n$, sofern alle $m(p)$ mit $p \equiv 3 \ mod \ 4$ gerade sind. Andernfalls gilt $H(n) = 0$.

3. Ansatz

Abb.
Wir schauen uns an, wie groß die Anzahl der Gitterpunkte in einem Intervall über dem Punkt $(0,0)$ ist, ohne $(0,0)$ mitzuzählen. Diese Anzahl beträgt $[r]$. Analog verfahren wir für die Gitterpunkte unter $(0,0)$. Diese Anzahl beträgt auch $[r]$. Demnach erhalten wir für die Anzahl der Gitterpunkte:

$$G(r) = 2[r] + 1, \text{ wobei } +1 \text{ der Gitterpunkt in } (0,0) \text{ ist.}$$

Jede ganze Zahl auf der x-Achse im Kreis befindet sich im Intervall mit Radius $\sqrt{r^2 - x^2}$. Damit erhalten wir für die Anzahl der Gitterpunkte im Bereich von $[r]$ bis $-[r]$:

$$\begin{aligned}
G(r) &= \sum_{x=-[r]}^{[r]} 2[\sqrt{r^2 - x^2}] + 1 \\
&= 1 + 2[r] + \sum_{x=-[r]}^{[r]} 2[\sqrt{r^2 - x^2}] \\
&= 1 + 2[r] + 2[r] + 4\sum_{x=1}^{[r]} [\sqrt{r^2 - x^2}] \\
&= 1 + 4[r] + 4\sum_{x=1}^{[r]} [\sqrt{r^2 - x^2}] \\
&\overset{*}{=} 1 + 4\sum_{x=1}^{r^2} (-1)^{x-1} [\frac{r^2}{2x-1}] \\
&\overset{**}{=} 1 + 4\sum_{x=1}^{\infty} ([\frac{r^2}{4x+1}] - [\frac{r^2}{4x+3}])
\end{aligned}$$

Wir schauen uns nun an, warum * und ** gelten.
Für $x = r^2 + 1$ und festes $r^2 \in \mathbb{R}_{\geqslant 0}$ gilt:
$0 \leq [\frac{r^2}{2x-1}] = [\frac{r^2}{2(r^2+1)-1}] = [\frac{r^2}{2r^2+1}] < [\frac{r^2}{2r^2}] = [\frac{1}{2}] = 0,$

deshalb ist für $x > r^2 + 1$:

$[\frac{r^2}{2x-1}] = 1 + 4\sum_{x=1}^{r^2} (-1)^{x-1} [\frac{r^2}{2x-1}] = 1 + 4\sum_{x=1}^{\infty} (-1)^{x-1} [\frac{r^2}{2x-1}]$

**) $1 + 4\sum_{x=1}^{r^2}(-1)^{x-1}[\frac{r^2}{2x-1}] = 1 + 4([r^2] - [\frac{r^2}{3}] + [\frac{r^2}{5}] \pm ...)$

Für x gerade ersetzen wir x durch $x = 2a + 2$ und für x ungerade ersetzen wir x durch $x = 2b + 1$.
Damit erhalten wir:

$$
\begin{aligned}
1 + 4\sum_{x=1}^{r^2}(-1)^{x-1}[\frac{r^2}{2x-1}] &= 1 + 4\sum_{b\geq 0}(-1)^{2b+1-1}[\frac{r^2}{2(2b+1)-1)}] + 4\sum_{a\geq 0}(-1)^{2a+2-1}[\frac{r^2}{2(2a+2)} \\
&= 1 + 4\sum_{b\geq 0}[\frac{r^2}{4b+1}] - 4\sum_{a\geq 0}[\frac{r^2}{4a+3}] \\
&= 1 + 4[r^2] + 4[\frac{r^2}{5}] + ... - 4[\frac{r^2}{3}] - 4[\frac{r^2}{7}] - ... \\
&= 1 + 4([r^2] - [\frac{r^2}{3}] + 4[\frac{r^2}{5}] \pm ...) \\
&= 1 + 4\sum_{x\geq 0}[\frac{r^2}{4x+1}] - 4\sum_{x\geq 0}[\frac{r^2}{4x+3}] \text{ durch Rückbenennung} \\
&= 1 + 4\sum_{x\geq 0}([\frac{r^2}{4x+1}] - [\frac{r^2}{4x+3}]) \\
&= 1 + 4\sum_{x=1}^{\infty}([\frac{r^2}{4x+1}] - [\frac{r^2}{4x+3}])
\end{aligned}
$$

Das wollten wir zeigen.

*) ...

Quellenverzeichnis

[**1**] Cohn-Vossen, S.; Hilbert, D.: Geometry and the Imagination. AMS Chelsea Publishing, 1952

[**2**] Davidoff, Giuliana; Lax, Anneli; Olds, C. D.: The Geometry of Numbers. The Mathematical Association of America, 2000

[**3**] Fricker, Francois: Einführung in die Gitterpunktlehre. Birkhäuser, Basel, 1982

[**4**] Huxley, M. N.: Exponential Sums and Lattice Points III. London Mathematical Society, 2003

[**5**] Landau, Edmund: Handbuch der Lehre von der Verteilung der Primzahlen. Leipzig B. G. Teubner, 1909

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

[**7**] Schmieder, G.; Reiss, K.: Basiswissen Zahlentheorie. Eine Einführung in Zahlen und Zahlbereiche. 2. Auflage, Springer, Berlin Heidelberg, 2007

[**8**] Schoissengeier, Johannes: Neue Entwicklungen in der Zahlentheorie. In: Didaktikhefte, Band 26, 1996

[**9**] Weisstein, Eric W.: Gauss's Circle Problem. http://mathworld.wolfram.com/GausssCircleProblem.html