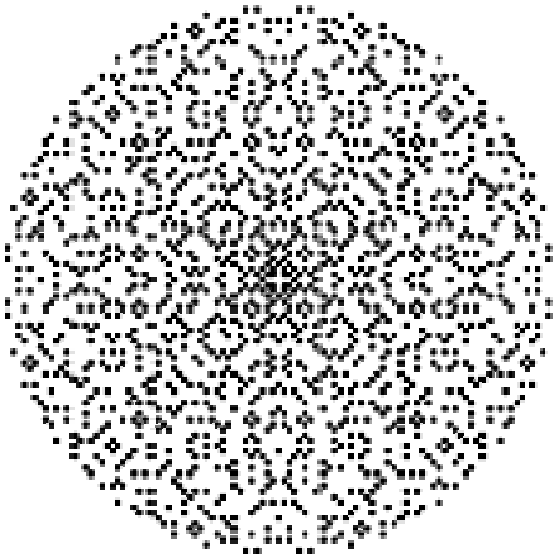
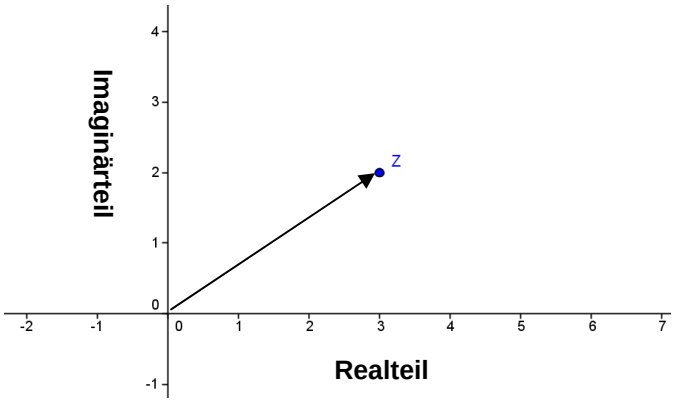
Kölner Mathematikturnier 2011
Das Turnierlogo



„Was sind denn das für komische Punkte im Turnierlogo?“, fragt Ihr Euch sicherlich. Unser Turnierlogo stellt eine Visualisierung der *Primzahlen in den Gaußschen Zahlen* oder kürzer, die *Gaußschen Primzahlen*, dar. Carl Friedrich Gauß (1777 – 1855) war ein berühmter Mathematiker, der schon als Neunjähriger eine Formel für die Summe der ersten *n aufeinander folgenden Zahlen* gefunden haben soll, den sogannten „Kleinen Gauß“, und später dann zu einem der bedeutendsten Mathematematiker wurde.

Um zu erfahren, was sich hinter den *Gaußschen Primzahlen* verbirgt, müssen wir etwas weiter ausholen und in die Tiefen der Mathematik eindringen…



Für das Verstehen der *Gaußschen Primzahlen* ist es notwendig, die komplexen Zahlen $\mathbb{C}$ zu kennen. Ihr seid vielleicht aus der Schule nur mit dem Zahlbereich der reellen Zahlen $\mathbb{R}$ vertraut, jedoch gibt es noch eine Erweiterung der reellen Zahlen, die komplexen Zahlen, deren charakteristische Eigenschaft es ist, dass alle Polynome eine Nullstelle besitzen, also auch das Polynom $x^2 + 1$.

Gaußsche Zahlen

In den reellen Zahlen ist die Gleichung $x^2 + 1 = 0$ nicht lösbar, da sich aus negativen Zahlen nicht die Wurzel ziehen lässt. Doch in den komplexen Zahlen ist dies möglich, denn das Quadrat der imaginären Einheit $i \in \mathbb{C}$ ist als -1 definiert ($i^2 = -1$). Daher schreibt mal auch schon mal $i = \sqrt{-1}$. Somit gilt beispielsweise $(1 + \sqrt{-1})\left(1 + \sqrt{-1}\right) = 2\sqrt{-1}$ bzw. $(1 + i)(1 + i) = 2i$, wie man leicht mit der ersten binomischen Formel nachrechnet. Jede komplexe Zahl lässt sich in der Form $a + i \cdot b$ für $a, b \in \mathbb{R}$ schreiben und man rechnet damit, wie man es von den reellen Zahlen kennt. Zusätzlich darf man benutzen, dass $i^2 = -1$ gilt. Während die reellen Zahlen auf einer Zahlengerade veranschaulicht werden können, werden die komplexen Zahlen in der *Gaußschen Zahlenebene* dargestellt. Auf der waagerechten Achse wird der *Realteil* a und auf der senkrechten der *Imaginärteil* b abgetragen. Die komplexe Zahl $z = 3 + i\ 2$ hat somit die Koordinaten $(3 \mid 2)$.

Zu einer komplexen Zahl $z = a + i \cdot b$ gibt es immer eine *komplex-konjugierte Zahl* $\bar{z} = a - i \cdot b$. Die konjugierte Zahl $\bar{z}$ erhält man also in der Gaußschen Zahlenebene durch Spiegelung von z an der waagerechten Achse.

Die *Gaußschen Zahlen* sind nun die komplexen Zahlen mit ganzzahligen Koordinaten, d.h. die komplexen Zahlen, für die gilt: $a + i \cdot b$, wobei $a, b \in \mathbb{Z}$. Die Menge der Gaußschen Zahlen bezeichnet man mit $\mathbb{Z}[i] = \{a + i \cdot b \mid a, b \in \mathbb{Z}\}$. Um nun endlich zu wissen, was die *Gaußschen Primzahlen* sind, gehen wir an dieser Stelle noch einen Schritt weiter. In der Schule habt Ihr gelernt, dass Primzahlen natürliche Zahlen sind, die sich nicht mehr weiter als Produkt anderer natürlicher Zahlen zerlegen lassen. Auch unter den Gaußschen Zahlen kann man solche Zahlen finden, die sich nicht als Produkt anderer Gaußscher Zahlen darstellen lassen. So ganz wörtlich ist das nicht zu nehmen. Schon bei den ganzen Zahlen kann man ja sowas wie 5=(-1)(-1) 5 schreiben, da man die Multiplikation mit (-1) in den ganzen Zahlen wieder rückgängig machen kann. Solche Zahlen nennt man *Einheiten*, d.h. Zahlen, zu denen es eine andere Zahl gibt, so dass das Produkt der beiden 1 ergibt. In $\mathbb{Z}[i]$ gibt es vier Einheiten, nämlich $\pm 1, \pm i$ und in $\mathbb{Z}$ hingegen gibt es nur zwei: ± 1.
Es ist nicht selbstverständlich, aber auch für die Gaußschen Primzahlen gilt die Eindeutigkeit der Primfaktorzerlegung – natürlich nur bis auf Einheiten.

Gaußsche Primzahlen
Betrachten wir als Beispiel die Zahl 5, die Ihr als Primzahl kennt. Doch ist sie auch eine Gaußsche Primzahl? Nein, denn 5 lässt sich schreiben als $5 = 4 + 1 = 4 - (-1) = 2^2 - i^2 = (2 + i)(2 - i)$ und somit als Produkt zweier Gaußscher Zahlen. Das heißt, dass nicht alle Primzahlen aus $\mathbb{Z}$ auch Primzahlen in $\mathbb{Z}[i]$ sind. Aus diesem Beispiel lässt sich zudem schließen, dass eine Primzahl $p \in \mathbb{Z}$, die als Summe zweier Quadrate geschrieben werden kann, also $p = a^2 + b^2$, KEINE *Gaußsche Primzahl* ist. Denn es gilt wegen der dritten binomischen Formel in $\mathbb{Z}[i]$:

$$p = a^2 + b^2 = a^2 - (ib)^2 = (a + ib)(a - ib).$$

Zerfällt dieses Produkt nun noch weiter? Zur Beantwortung solcher Fragen ist es sehr hilfreich, die *Norm* einer Gaußschen Zahl zu betrachten. Sei $\alpha = a + i \cdot b \in \mathbb{Z}[i]$ eine Gaußsche Zahl, dann ist die *Norm* von α definiert als

$$N(\alpha) = \alpha \cdot \bar{\alpha} = (a + i \cdot b) \cdot (a - i \cdot b) = a^2 + b^2.$$

Die Bedeutung der Norm kommt daher, dass für je zwei Gaußsche Zahlen v und w gilt: $N(v \cdot w) = N(v) \cdot N(w)$. Und die Einheiten sind die einzigen Gaußschen Zahlen mit Norm 1. Beides rechnet man leicht nach.

Nehmen wir an, dass eine Primzahl $p = a^2 + b^2 = (a + ib)(a - ib)$ mit $a, b \in \mathbb{Z}$ zerfällt. Würde dann einer der beiden Faktoren nochmal zerfallen, also etwa $(a + i \cdot b) = v \cdot w$ für zwei weitere Gaußsche Zahlen v und w, dann wäre auch $p = a^2 + b^2 = N(a + ib) = N(v) \cdot N(w)$ eine Zerlegung einer ganzzahligen Primzahl p in zwei ganzzahlige Faktoren. Also muss eine der beiden Zahlen v oder w eine Einheit sein.

Eine Primzahl p, die als Summe zweier Quadrate dargestellt werden kann, zerfällt demnach in zwei Faktoren $(a + ib)$ und $(a - ib)$, die beide Primzahlen in $\mathbb{Z}[i]$ sind.

Wie verhält es sich mit denjenigen Primzahlen $p \in \mathbb{Z}$, die nicht Summe zweier Quadrate sind? Angenommen, p wäre eine solche Primzahl mit $p = (a + ib)(c + id)$ und $a, b, c, d \in \mathbb{Z}$. Dann wäre $N(p) = N(a + ib)N(c + id) = p^2$. Also ist entweder einer der beiden Faktoren eine Einheit oder beide haben die Norm p. Im letzteren Fall wäre

$$p = N(a + ib) = a^2 + b^2$$

und somit doch Summe zweier Quadrate. Also sind genau die Primzahlen in $\mathbb{Z}$, die nicht Summe zweier Quadrate sind, auch Primzahlen in $\mathbb{Z}[i]$.

Summe zweier Quadrate

Stellt sich nun die Frage: Welche Primzahlen $p \in \mathbb{Z}$ lassen sich als Summe zweier Quadrate schreiben? Betrachten wir hierzu die Teilbarkeit durch 4 für beliebige Zahlen. Dabei können die Reste 0, 1, 2 und 3 auftreten. Bei Quadratzahlen sind jedoch nur die Reste 0 oder 1 möglich. Wenn wir eine Zahl der Form $4m + r$ mit möglichen Resten r=0, 1, 2, 3 quadrieren zu $16m^2 + 8m + r^2$, ergeben sich bei Division durch 4 nur die Reste 0 und 1. Das heißt, die Summe zweier Quadrate lässt bei Division durch 4 nie den Rest 3. Somit sind Primzahlen $p \in \mathbb{Z}$, die bei Division durch 4 den Rest 3 lassen, niemals als Summe zweier Quadrate darstellbar. Und auch die Umkehrung gilt (Fermatscher Zwei-Quadrate-Satz): Eine Primzahl, die bei Division durch 4 den Rest 1 lässt, ist als Summe zweier Quadrate darstellbar.

Keine zusätzlichen Primzahlen

Gibt es auch Primzahlen $\pi \in \mathbb{Z}[i]$, die nicht von Primzahlen in $\mathbb{Z}$ herrühren? Oder anders gefragt: Ist es immer so, dass jede Gaußsche Primzahl $\pi = a + b \cdot i$ in $\mathbb{Z}[i]$ entweder selbst schon bis auf Einheiten ganzzahlig und prim ist oder aber ihre Norm

$$N(\pi) = a^2 + b^2$$

prim in $\mathbb{Z}$ ist. Das hieße also, dass die Zahl π auf die oben beschriebene Weise von einer Primzahl in $\mathbb{Z}$ herrührt oder selbst schon eine ist.

Sei also in $\mathbb{Z}[i]$ eine Primzahl $\pi = a + i \cdot b$ mit der Norm $N(\pi) = a^2 + b^2$ gegeben. Angenommen $N(\pi)$ wäre nicht prim in $\mathbb{Z}$, dann ließe sich $N(\pi)$ schreiben als Produkt von Zahlen $s, t \in \mathbb{Z}$ und wir hätten $N(\pi) = (a + b \cdot i)(a - b \cdot i) = st$. Mit der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[i]$ folgern wir ohne Beschränkung der Allgemeinheit, dass $\pi = (a + i \cdot b)$ die Zahl s in $\mathbb{Z}[i]$ teilt.
Dieser Faktor s lässt sich demnach als Produkt schreiben: $s = (u + iv)(a + ib)$. Konjugieren wir s, erhalten wir $s = (u - iv)(a - ib)$. Also teilt auch $\bar{\pi} = (a - ib)$ die Zahl s. Falls nun $\bar{\pi} = (a - ib)$ sich von π nicht nur um eine Einheit unterscheidet, dann handelt es sich um unterschiedliche Primfaktoren und beide müssen in s vorkommen. In diesem Fall teilt die ganze Zahl $N(\pi) = (a + i \cdot b)(a - i \cdot b)$ die ganze Zahl s und stimmt daher mit ihr überein. Also ist $N(\pi) = a^2 + b^2$ eine Primzahl in $\mathbb{Z}$.

Nun kann es jedoch sein, dass $\pi = (a + i \cdot b)$ und $(a - i \cdot b)$ sich nur um eine Einheit unterscheiden, d.h. dass $(a + ib) = e(a - ib)$ gilt für eine der der vier Einheiten e in $\mathbb{Z}[i]$. Dann sind die Primzahlen $\pi = (a + i \cdot b)$ und $(a - i \cdot b)$ nicht wirklich verschieden und die Primfaktorzerlegung sagt uns nur, dass eine von ihnen s teilen müsste. Falls sich eine Primzahl $\pi = (a + i \cdot b)$ von $(a - i \cdot b)$ nur um eine Einheit unterscheidet, berechnet man leicht, dass entweder π reell (und damit auch prim in $\mathbb{Z}$), rein imaginär (dann ist $i\pi$ prim in $\mathbb{Z}$) oder von der Form ist $\pi = a(1 \pm i)$, für ein $a \in \mathbb{Z}$. Falls π reell oder rein imaginär ist, dann handelt es sich ja bis auf Einheiten schon um eine Primzahl in $\mathbb{Z}$. Falls jedoch π von der Form $\pi = a(1 \pm i)$ ist, dann ist π offensichtlich nur dann eine Primzahl in $\mathbb{Z}[i]$, wenn a eine Einheit ist. Und $N(\pi) = N\big(a(1 \pm i)\big) = N(a)N(1 \pm i) = 1 \cdot 2 = 2$ ist prim.
Nun wissen wir also, dass alle Primzahlen von den Primzahlen in $\mathbb{Z}$ her stammen.

Resumé

Die *Gaußschen Primzahlen* in $\mathbb{Z}[i]$ stammen also alle von den Primzahlen in $\mathbb{Z}$ ab: Eine Primzahl p aus $\mathbb{Z}$ und alle Produkte mit Einheiten sind auch noch prim in $\mathbb{Z}[i]$, wenn p bei Division durch 4 den Rest 3 lässt. Falls dieser Rest 1 ist, dann zerfällt in p in zwei Primzahlen

$$p = (a + i \cdot b)(a - i \cdot b).$$

Im Allgemeinen gehören dann zur Primzahl p die acht Gaußschen Primzahlen $(\pm a \pm i \cdot b)$ und $(\pm a \mp i \cdot b)$ sowie $(\pm b \pm i \cdot a)$ und $(\pm b \mp i \cdot a)$. Alle haben die Norm p. Falls jedoch $(a + i \cdot b)$ und $(a - i \cdot b)$ sich nur um eine Einheit unterscheiden, sind dies jeweils nur vier.

Da die Norm zwar nicht den Abstand vom Koordinatenursprung direkt, aber das Quadrat dieses Abstands darstellt, liegen alle Primzahlen mit gleicher Norm auf einem Kreis. Diese Kreise repräsentieren also die Primzahlen in $\mathbb{Z}$. Zeichnet man die Primelemente und die Kreise in die Gaußsche Zahlenebene ein, dann ergibt sich das unten stehende Bild, das nur einen Ausschnitt um den Koordinatenursprung darstellt.

Das Logo unseres Turniers zeigt uns also, wie interessant und voller schöner Entdeckungen, Muster und Phänomene Mathematik sein kann.

Vielleicht entdeckt Ihr nun beim Turnier noch viele weitere solcher schönen Phänomene.

Viel Spaß!