Aufgaben: Gauss'sche Zahlen

1. Seien $\alpha, \beta \in \mathbb{Z}[i]$ Gauss'sche Zahlen, sodass ihre Normen $N(\alpha), N(\beta) \in \mathbb{Z}$ teilerfremd sind (als ganze Zahlen). Zeige, dass α und β teilerfremd sind als Gauss'sche Zahlen.

   Lösung:

   Sei γ ein geimsamer Teiler von α und β. Aus der Multiplikativität der Norm folgt $N(\gamma) \mid N(\alpha)$ und $N(\gamma) \mid N(\beta)$ als ganze Zahlen. Da nun $N(\alpha)$ und $N(\beta)$ teilerfremd sind als ganze Zahlen, gilt $N(\gamma) \mid 1$ also $N(\gamma) = 1$ und folglich ist γ eine Einheit. Es folgt, dass 1 ein grösster gemeinsamer Teiler von α und β in $\mathbb{Z}[i]$ ist, das heisst α und β sind teilerfremd als Gauss'sche Zahlen.

2. Sei $\mathbb{N} \ni p \equiv 1 \mod (4)$ eine ganze Primzahl und sei $x \in \mathbb{Z}$ eine ganze Zahl, sodass $x^2 \equiv -1 \mod (p)$ (Eine solche Zahl ist garantiert - siehe Vorlesung). Zeige, dass $x + i$ und p als Gauss'sche Zahlen nicht teilerfremd sind und folgere dass sich p als Summe von zwei ganzen Quadraten schreiben lässt.

   Lösung:

   Falls $x + i$ und p als Gauss'sche Zahlen teilerfremd sind, so existieren Gauss'sche Zahlen μ, ν sodass $\mu(x + i) + \nu p = 1$. Es gilt nun, dass $p \mid x^2 + 1 = N(x + i)$ als ganze Zahlen, also auch als Gauss'sche Zahlen, da $\mathbb{Z} \subset \mathbb{Z}[i]$. Es folgt

$$0 \equiv N(\mu)N(x + i) = (1 - \nu p)\overline{(1 - \nu p)} = (1 - \nu p)(1 - \overline{\nu} p) \equiv 1 \mod (p).$$

   Es folgt, dass $p \mid 1$ als Gauss'sche Zahl. Zum Schluss können wir auf verschiedene Arten argumentieren. Zum Beispiel gilt dann $p^2 = N(p) \mid N(1) = 1$ als ganze Zahl, ein Widerspruch, da p prim in $\mathbb{Z}$ ist und somit keine ganze Einheit ist. Eine Alternative wäre direkt zu zeigen, dass aus $p \mid 1$ als Gauss'sche Zahlen, sogar $p \mid 1$ als ganze Zahlen gilt, was wiederum zu einem Widerspruch führt.

   Sei nun α ein gemeinsamer Teiler von p und $x+i$, welcher keine Einheit ist. Es gilt nun $N(\alpha) \mid N(p) = p^2$ und $N(\alpha) \mid N(x + i) = x^2 + 1$. Das heisst es muss $N(\alpha) = p$ oder p^2 gelten. Im ersten Fall haben wir, dass $p = N(\alpha) = a^2 + b^2$, falls $\alpha = a + bi$ mit $a, b \in \mathbb{Z}$. Im zweiten Fall haben wir also $N(\alpha) = N(p)$ und $\alpha \mid p$, folglich ist $\frac{p}{\alpha}$ eine Einheit. Wir folgern, dass dann $p \mid x + i$, aber dies ist ein Widerspruch, denn Gauss'sche Zahlen, welche Vielfache von p sind haben sowohl Realteil als auch Imaginärteil teilbar durch p.