Übungen zur Algebraischen Zahlentheorie (WS 2023)

PD Dr. Jürgen Müller, **Ausgabe:** 12.10.2023

(1.1) Exercise: Euclidean number rings.
For $d \in \{-2, 2, 3\}$ show that $\mathcal{O}_d := \mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \in \mathbb{C}; a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ is Euclidean with respect to a suitable norm map.

Hint. Generalise the method used for $\mathbb{Z}[i]$.

(1.2) Exercise: Diophantine equations.
a) Show that $n = 0$ is the only integer such that $n^2 + 1$ is a cube.
b) Show that the equation $X^3 = Y^2 + 4$ has only the integer solutions $[x, y] = [2, \pm 2]$ and $[x, y] = [5, \pm 11]$.

Hint. Use the ring $\mathbb{Z}[i]$, and in b) distinguish the cases y even and odd.

(1.3) Exercise: Primes in arithmetic progressions.
We consider an (easy) special case of **Dirichlet's Theorem [1837]** on primes in coprime residue classes:

a) Show that there are infinitely many $p \in \mathcal{P}$ such that $p \equiv -1 \pmod 4$.
b) Show that there are infinitely many $p \in \mathcal{P}$ such that $p \equiv 1 \pmod 4$.

(1.4) Exercise: Wilson's Theorem [1770].
a) Show that $n \in \mathbb{Z}$, $n \geq 2$, is a prime if and only if $(n-1)! \equiv -1 \pmod n$.
b) For $p \in \mathcal{P}$ odd, show that $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$.

(1.5) Exercise: Primes as sums of two squares (GAP).
a) Write a GAP program implementing the (extended) Euclidean algorithm for the Gaussian integers $\mathbb{Z}[i]$. (Of course, any other computer algebra system may be used as well. As far as GAP is concerned, the Euclidean algorithm is readily available there, but you should implement it on your own, only building on GAP functions whose names do not contain capital letters.)

b) Write a GAP program which for a prime $p \in \mathcal{P}$ such that $p \equiv 1 \pmod 4$ computes its decomposition as a sum of two squares in $\mathbb{Z}$. (Think of a fast method to compute a primitive 4-th root of unity modulo p.) Try your implementation for a few large primes p. How far do you get?