Introduction to Homomorphic Cryptosystems
Exercise Sheet 5: CKKS

Task 1 – Modular Inverse through Extended Euclidean Algorithm

The extended euclidean algorithm[1] can be used to find the greatest common divisor of two integers a and b and the coefficients x and y ($\in \mathbb{Z}$), such that

$$ax + by = \gcd(a, b)$$

If we want to find a modular inverse $\in \mathbb{Z}_b$ for a (which means find a integer a^{-1} such that $aa^{-1} \equiv 1 \mod b$) we can use this algorithm as $\gcd(a, b) = 1$:

$$ax + by = \gcd(a, b) = 1$$

$$ax \equiv 1 \mod b$$

This means, that in order to find the modular inverse of an integer a, we can use the extended euclidean algorithm with intput parameters a and the modulus (b) to compute x. x is a modular inverse of a

Use the extended euclidean algorithm to compute the modular inverse of $11 \in \mathbb{Z}_{26}$

Task 2 – Using the OpenFHE library

For this task, see the task2.cpp file in WueCampus. It shows how the CKKS algorithms can be used through the OpenFHE library to encrypt and compute with data.

Try to run and understand the code. Play around with the parameters to get a feeling for the algorithms.

[1] https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm