Selected Areas in Cryptology - Part 1: Post-quantum cryptography

Exercise sheet 7, 25 April 2024

1. Gauss reduction in dimension 2 matches computations you know from the Euclidean algorithm. For basis vectors $b_1, b_2 \in \mathbb{R}^2$ perform the following steps

   - If $||b_1|| > ||b_2||$ swap b_1 and b_2.
   - While $||b_2 \pm b_1|| < ||b_2||$ replace b_2 with $b_2 \pm b_1$ (using the same sign that makes it smaller).

   repeatedly until no more changes happen.

   Perform Gauss reduction on $b_1 = (144, 0)$ and $b_2 = (89, 1)$.

2. Make a two-dimensional toy example of the GGH encryption scheme and signature scheme.