Exercise sheet 7, 24 March 2022

1. Last time there were some questions about how to do enumeration when actual work is needed.
   Remember that
   $$b_2^* = b_2 - (\langle b_1, b_2\rangle / \langle b_1, b_1\rangle) b_1.$$
   Show that for $v = a_1 b_1 + a_2 b_2$ you have
   $$||v|| \geq |a_2| \cdot ||b_2^*||.$$
   Hint: Note that the square of the Euclidean norm matches the inner product
   $$||x||^2 = \langle x, x\rangle.$$
   Note that that limits the choices of a_2 you need to consider in enumeration.

2. Explain how $f' = x^i f$, instead of f, can be used to decrypt in the NTRU system for $0 \leq i < n$

3. Check out the lattice attack from slides 53 and 54 of the latticehacks talk to understand why the attack worked.

4. Let F be a multivariate-quadratic system of equations and G its polar form (as defined in the second video). We have shown that $G(\mathbf{x}, \mathbf{y})$ is bilinear if the constant terms $c^{(k)}$ in F are all zero. How can you change G so that it remains bilinear if the constant terms are nonzero? How does that change the system?

5. For the Sakumoto–Shirai–Hiwatari identification scheme we have shown that a malicious prover who does not know $\mathbf{s}$ can provide valid answers if he knows that $b = 0$ will be chosen.
   Investigate what the malicious signer can do in the other case. Does he need to know α as well before computing the commitments?

6. Use $g(z) = z^3 + z + 1$ to obtain the field extension $\mathbb{F}_{2^3} \cong \mathbb{F}_2[z]/g(z)$. Let $s(X) = X^{2^2+1}$ be the central map for a C^*/HFE system with $n = m$ and let $M = N = I_3$. Let $\phi \mathbb{F}_{2^3} \to \mathbb{F}_2^3$ for the basis $\{1, z, z^2\}$.
   Find a preimage for $(1, 0, 1)$.
   Use Sage or Magma for the computation.