Exercise sheet 6, 17 March 2022

For exercises about executing NTRU key generation.encryption/decryption I expect you to use Sage or Magma.
For Sage, you can find most of this implemented at `https://latticehacks.cr.yp.to/ntru.html`. Note that $d = 2t + 1$ is the total number of non-zero coefficients of f.

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.

   (a) Explain why the output of Gauss reduction is a basis of the same lattice.

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

2. Enumeration, as explained in part II, computes b_2^* as

   $$b_2^* = b_2 - (\langle b_1, b_2 \rangle / \langle b_1, b_1 \rangle) b_1.$$

   For the basis output by the previous exercise, perform the enumeration attack.
   Note, you don't want to do this on the input vectors as those are much longer.

3. For NTRU, let $n = 3$ and $f(x) = x^2 - x + 1$. Compute the inverse f_3 of f in R_3. Then compute $f \cdot f_3$ in R_3 to verify that the result is indeed 1.

4. For the NTRU ring $R = \mathbb{Z}[x]/(x^{11} - 1)$ find two nonzero polynomials $a, b \in R \setminus \{0\}$ with $a \cdot b = 0$.

5. Let $n = 32$. Let f have 4 coefficients equal to 1, and 3 equal to -1. Let g have 2 coefficients of each 1 and -1 and r have 4 coefficients of each 1 and -1.
   Explain how decryption errors in NTRU can happen and compute how large q has to be so that decryption is guaranteed to be correct, i.e., so that taking the coefficients of $a = f \cdot c$ in R_q as elements in $[-(q-1)/2, (q-1)/2]$ produces the correct message.

   Note: The parameter choices are different than in the lecture to ensure that you go through all steps of the argument. Make sure to justify all statements.

6. One tweak of NTRU is to use public key $h = 3g/F$ with $F = 1 + 3f$, where f is chosen to have t coefficients equal to 1 and the same number equal to -1.
   Explain how this simplifies the decryption procedure and compute lower bounds on q in terms of t to avoid decryption failures.

7. Let $n = 503$ and $q = 256$. The encryption equation $c = rh + m$ in R/q is the schoolbook version of NTRU and is not CCA-II secure. Show how you can use an oracle that decrypts any ciphertext but c to find m. Note that this has two parts: stating candidate ciphertexts c' to feed to the oracle and a verification whether the obtained message M matches the actual message m.

8. Explain how to attack NTRU using an algorithm to find short lattice vectors, i.e., explain how to translate the problem of finding the secret key into a problem of finding short lattice vectors.
   State the matrix for the lattice for $n = 11, q = 256$, and $h = 70x^{10} + 9x^9 + 36x^8 - 118x^7 + 40x^6 - 93x^5 - 122x^4 + 21x^3 + 69x^2 + 23x + 80$ and find the secret f and g.
   Note that h was generated using $t = 3$ for f.