Exercises for "Lattice-based cryptography: Episode V: the ring strikes back" (Daniel J. Bernstein; joint work with Tanja Lange)

Fix an integer $n \geq 0$. Define R as the ring $\mathbf{Z}^n$. The elements of R are vectors $(v_1, v_2, \ldots, v_n)$ with $v_1, v_2, \ldots, v_n \in \mathbf{Z}$. Addition and multiplication in R are componentwise: e.g., $(3, 5) \cdot (7, 11) = (21, 55)$ for $n = 2$.

Exercise 1. Fix integers $c_1, c_2, \ldots, c_n$. Show that the following set is an ideal of R: $\{(v_1, v_2, \ldots, v_n) : v_1 \in c_1\mathbf{Z}, v_2 \in c_2\mathbf{Z}, \ldots, v_n \in c_n\mathbf{Z}\}$.

Exercise 2. Show that every ideal of R can be expressed in this way.

Exercise 3. Fix a real number $\gamma \geq 1$. The γ-approximate shortest-vector problem for R, abbreviated R-SVP$_\gamma$, is the following problem.

You are given elements $r_1, r_2, \ldots, r_n \in R$, not all zero. Define I as the ideal $r_1R + r_2R + \cdots + r_nR$. Your task is to find a nonzero vector in I whose length is at most γ times the length of the shortest nonzero vector in I.

Explain how to efficiently solve R-SVP$_\gamma$. Solve it for $n = 2$, $\gamma = 1$, $r_1 = (314, 159)$, $r_2 = (271, 828)$.

Exercise 4. Fix an integer $q > 0$. Fix a distribution χ on $\mathbf{Z}$: e.g., choosing $i \in \mathbf{Z}$ with chance proportional to $\exp(-i^2/n)$. The learning-with-χ-errors problem for R modulo q, abbreviated R/q-LWE$_\chi$, is the following problem.

There are random elements $s, r_1, e_1, r_2, e_2, r_3, e_3, \ldots \in R$, with all entries chosen independently. Each entry of $s, r_1, r_2, r_3, \ldots$ is chosen uniformly from $\{0, 1, \ldots, q-1\}$. Each entry of $e_1, e_2, e_3, \ldots$ is chosen from χ.

You are given r_1; $sr_1 + e_1 \bmod q$; r_2; $sr_2 + e_2 \bmod q$; r_3; $sr_3 + e_3 \bmod q$; etc. Here "$\bmod q$" means that each entry is reduced modulo q to the range $\{0, 1, \ldots, q-1\}$; and "$a + b \bmod q$" means $(a + b) \bmod q$, not $a + (b \bmod q)$. Your task is to find s.

Show that R/q-LWE$_\chi$ is "provably secure": specifically, prove that any attack A against R/q-LWE$_\chi$ implies an attack A' against R-SVP$_\gamma$ where the time and success probability of A' are at most polynomially worse than the time and success probability of A. (Hint: Use the previous exercise.)

Exercise 5. Explain how to efficiently solve R/q-LWE$_\chi$.

Exercise 6. Literature review: Figure out why this type of "security proof" is often claimed to be an indication of security, rather than an indication of insecurity. Identify weaknesses in the underlying arguments.