MATH3301/6114 ADD-ON MODULE (ASE/HPO/6114) POST-QUANTUM CRYPTOGRAPHY ASSIGNMENT 2 DUE FRIDAY 20 OCTOBER AT 6PM

ANTHONY HENDERSON

There are 25 marks in total. Explain your reasoning in sufficient detail to demonstrate your understanding, unless the question specifies otherwise.

(1) This question relates to the Toy NTRU cryptosystem from Add-on Lecture 4 (Week 7). Suppose that Alice's public key consists of $q = 131$ and $h = 100$, so that the relevant lattice L is the one with basis $(1, 100)$, $(0, 131)$.

(a) (3 marks) Use Gauss' lattice basis reduction algorithm to find a reduced basis of L. (You can use a calculator or computer to do any required calculations, but show all the steps.)

(b) (2 marks) Suppose that Bob sends the encrypted message $e = 78$. What was his message m before encryption?

(2) This question shows some applications of the upper bound on $\lambda_1(L)$ proved in Add-on Lecture 6 (Week 9). Let q be an odd prime.

(a) (2 marks) In this part, suppose that $q \equiv 1 \pmod 4$. Recall that it was shown in the main lectures that there exists an integer h such that $h^2 \equiv -1 \pmod q$. Let L be the lattice with basis $(1, h)$, $(0, q)$, and let (x, y) be a shortest nonzero vector of L. Show that $x^2 + y^2 = q$. (Thus any prime $\equiv 1 \pmod 4$ can be written as the sum of two integer squares.)

(b) (3 marks) Now allow $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. You can assume (it is shown by an easy counting argument) that there exist integers u, v such that $u^2 + v^2 \equiv -1 \pmod q$. By considering the 4-dimensional lattice with generating matrix

$$\begin{bmatrix} 1 & 0 & u & v \\ 0 & 1 & -v & u \\ 0 & 0 & q & 0 \\ 0 & 0 & 0 & q \end{bmatrix},$$

show that q can be written as a sum of four integer squares.

(3) Suppose that we know that there is a positive integer $n < 10^4$ such that $\sqrt{n} - \lfloor \sqrt{n} \rfloor$ has a decimal expansion beginning $0.888812\cdots$. How can we find n (without programming a computer to check all the possibilities in turn)? Here is a method using lattice theory.

(a) (3 marks) Let $k = 888812$ and $m = \lfloor \sqrt{n} \rfloor$. Let L be the lattice with basis $\mathbf{v}_1 = (0, 10^6)$ and $\mathbf{v}_2 = (2, 2k + 1)$. Show that the (unknown) lattice vector $\mathbf{v} = (n - m^2)\mathbf{v}_1 - m\mathbf{v}_2 \in L$ satisfies

$$\left\| \mathbf{v} - \left(-100, \frac{k^2+k}{10^6}\right) \right\| < 100\sqrt{2}.$$

(b) (3 marks) Explain why, given the result of (a), we can reasonably expect $\mathbf{v}$ to be the closest vector in L to $\mathbf{x} = (-100, \frac{k^2+k}{10^6})$.

(c) (2 marks) You can take for granted that Gauss' algorithm produces the following reduced basis for L:

$$\mathbf{v}_1' = (18, -1375), \quad \mathbf{v}_2' = (1448, 500).$$

We know that $\mathbf{x} = s_1\mathbf{v}_1' + s_2\mathbf{v}_2'$ for some $s_1, s_2 \in \mathbb{R}$. Determine $\mathbf{v}' = \lfloor s_1 \rceil \mathbf{v}_1' + \lfloor s_2 \rceil \mathbf{v}_2' \in L$. (You can use a calculator or computer to do the calculations. Feel free to round the second component of $\mathbf{x}$ to the nearest integer; that won't change $\mathbf{v}'$.)

(d) (2 marks) Working on the assumption that the unknown $\mathbf{v}$ defined in (a) equals the known $\mathbf{v}'$ defined in (c), find n. (You can use a calculator or computer to do the calculations.)

(4) One way you might attempt to make the Toy NTRU cryptosystem more secure is to use the *Gaussian integers*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

instead of the integers $\mathbb{Z}$. But this turns out to have the same vulnerability, because there is an analogue of Gaussian lattice basis reduction for $\mathbb{Z}[i]$-lattices in $\mathbb{C}^2$. On $\mathbb{C}^2$ we use (instead of the dot product) the complex scalar product $\langle -, - \rangle$ defined by

$$\langle (z_1, w_1), (z_2, w_2) \rangle = \overline{z_1} z_2 + \overline{w_1} w_2, \text{ for } z_1, w_1, z_2, w_2 \in \mathbb{C},$$

where $\overline{z}$ is the usual complex conjugate of z. A $\mathbb{Z}[i]$-*lattice* in $\mathbb{C}^2$ is a subset of the form

$$\{u_1(z_1, w_1) + u_2(z_2, w_2) \mid u_1, u_2 \in \mathbb{Z}[i]\}$$

where (z_1, w_1), (z_2, w_2) is a given $\mathbb{C}$-basis of $\mathbb{C}^2$. We say that this basis is $\mathbb{Z}[i]$-*reduced* if it satisfies the two conditions:

(i) $\langle (z_1, w_1), (z_1, w_1) \rangle \leq \langle (z_2, w_2), (z_2, w_2) \rangle$;

(ii) both the real part and the imaginary part of

$$\frac{\langle (z_1, w_1), (z_2, w_2) \rangle}{\langle (z_1, w_1), (z_1, w_1) \rangle}$$

belong to the interval $(-\frac{1}{2}, \frac{1}{2}]$.

(a) (2 marks) Imitate Gauss' algorithm to find a $\mathbb{Z}[i]$-reduced basis for the $\mathbb{Z}[i]$-lattice with basis $(1, i)$, $(0, 2+3i)$.

(b) (3 marks) Show that if (z_1, w_1), (z_2, w_2) is a $\mathbb{Z}[i]$-reduced basis for the $\mathbb{Z}[i]$-lattice L, then every $(z, w) \in L$ with $(z, w) \neq (0, 0)$ satisfies

$$\langle (z, w), (z, w) \rangle \geq \langle (z_1, w_1), (z_1, w_1) \rangle.$$