# EXERCISES

## 1 Solving NTRU over the integers ($\star$)

The objective of this exercise is to determine whether $h = 402$ can be written as $h = f \cdot g^{-1} \bmod q$ for $q = 1\,009$ and some $f, g \in \mathbb{Z}$ with $|f|, |g| \leq B := 8$. In other words, we want to test whether $h$ is an NTRU instance or not (for our simplified variant of NTRU over the integers). To solve this question, we will construct the lattice $\mathcal{L}_h$ associated to $h$, and then use the Lagrange-Gauss algorithm to compute a shortest non-zero vector of this lattice.

**Note:** recall that the true NTRU assumption should be defined with polynomials instead of integers. Here, we can efficiently break the NTRU assumption precisely because we are working with integers instead of polynomials of large degree.

1. Let $\mathbf{B}_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ and $\mathcal{L}_h = \mathcal{L}(\mathbf{B}_h)$ be the lattice spanned by the columns of $\mathbf{B}_h$. Prove that $\begin{pmatrix} u \\ v \end{pmatrix} \in \mathcal{L}_h$ if and only if $h = v \cdot u^{-1} \bmod q$ or $u = v = 0 \bmod q$. (Recall that $q$ is prime, so any $u$ not divisible by $q$ is invertible modulo $q$.)

2. Try to compute a shortest possible basis of $\mathcal{L}_h$ using the Lagrange-Gauss algorithm (see the video). You can use a calculator for the computation of square roots, or even SageMath to compute directly the QR-factorization of your matrices. If this is too hard, skip this question. ($\star\star\star$)
   (Note: computing QR-factorization is not really important in Lagrange-Gauss algorithm. You can actually run the algorithm without this, and manipulate only integers and rational numbers. Given two vectors $\mathbf{b}_1$ and $\mathbf{b}_2$, you want to reduce $\mathbf{b}_2$ as much as possible by adding to it an integer multiple of $\mathbf{b}_1$ (i.e., you want to update $\mathbf{b}_2 \leftarrow \mathbf{b}_2 + k\mathbf{b}_1$ for some $k \in \mathbb{Z}$ that minimizes the length of the new vector). The optimal choice of $k$ is $k = -\lfloor \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \langle \mathbf{b}_1, \mathbf{b}_1 \rangle \rceil$. Why? (make a picture))

3. You can check with SageMath that your short basis is indeed a shortest basis, by running the commands

```
B = Matrix(ZZ,2,[1, 402, 0, 1009])
B_red = B.LLL()
print(B_red.transpose())
```

   in SageMath. Note that SageMath use row convention for matrices, which is why we provided it with a matrix `B` which is the transpose of our $\mathbf{B}_h$ above, and which is why we transpose the output before printing it.

4. Answer the initial question: is $h$ an NTRU instance (with $B = 8$)? If yes, provide some $(f, g) \in \mathbb{Z}^2$ such that $h = f \cdot g^{-1} \bmod q$ and $|f|, |g| \leq B$.

## 2 Some properties of NTRU ($\star\star$)

Let $q$ be a prime integer and $B < \frac{\sqrt{q}-1}{2}$ be an integer. Recall that we defined an NTRU instance as an element $h \in \mathbb{Z}/q\mathbb{Z}$ that can be written $h = f \cdot g^{-1} \bmod q$ for some $(f, g) \in \mathbb{Z}^2$ with $|f|, |g| \leq B$.

**Note:** Recall that the true NTRU assumption should be defined with polynomials instead of integers. In this exercise, we use integers for simplicity, but all the properties that we will prove can be adapted to the polynomial setting.

1. Show that if $h$ is chosen uniformly at random in $\mathbb{Z}/q\mathbb{Z}$, then the probability that $h$ is an NTRU instance is $\leq \frac{(2B+1)^2}{q}$ (note that this quantity is $< 1$ since $2B+1 < \sqrt{q}$ by assumption on $B$). This means that the smaller $B$ is compared to $\sqrt{q}$, the less likely it becomes to find an NTRU instance when sampling a random element in $\mathbb{Z}/q\mathbb{Z}$. (Hint: the number of NTRU instances is upper bounded by the number of pairs $(f, g) \in \mathbb{Z}^2$ with $|f|, |g| \leq B$.)

2. Let $h = f \cdot g^{-1} \bmod q$ be an NTRU instance (with $|f|, |g| \leq B$). The pair $(f, g)$ is called a trapdoor for $h$. Is this trapdoor necessarily unique? I.e., can we find $(f', g') \neq (f, g)$ such that $h = f' \cdot (g')^{-1} \bmod q$ and $|f'|, |g'| \leq B$? If yes, prove it. If no, find a counter-example. (Hint: what if we multiply $f$ and $g$ by a small constant?)

   Recall that, to an NTRU instance $h = f \cdot g^{-1}$, we can associate the basis $\mathbf{B}_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix}$ and the lattice $\mathcal{L}_h = \mathcal{L}(\mathbf{B}_h)$ which is spanned by the columns of $\mathbf{B}_h$. Recall also that, under the NTRU assumption, computing a short basis of $\mathcal{L}_h$ from $\mathbf{B}_h$ is computationally hard. The objective of the next questions is to show that if we know the trapdoor $(f, g)$ in addition to the basis $\mathbf{B}_h$, then computing a short basis of $\mathcal{L}_h$ becomes easy.

3. Let $\mathbf{x} = (x_1, x_2) \neq (0, 0)$ and $\mathbf{y} = (y_1, y_2)$ be any vectors of $\mathbb{Z}^2$. Show that one can efficiently compute $k \in \mathbb{Z}$ such that $\|\mathbf{y} + k\mathbf{x}\| \leq \sqrt{\|\mathbf{x}\|^2/4 + |x_1y_2 - x_2y_1|^2/\|\mathbf{x}\|^2}$. ($\star\star\star$)
   (Hint: make a picture. Let $\tilde{\mathbf{y}} = \mathbf{y} + k\mathbf{x}$ be the vector you are looking for. Observe that the projection of $\tilde{\mathbf{y}}$ orthogonally to $\mathbf{x}$ always has euclidean norm $|x_1y_2 - x_2y_1|/\|x\|$ (this does not depend on the choice of $k$). Then observe that you can choose $k \in \mathbb{Z}$ such that the orthogonal projection of $\tilde{\mathbf{y}}$ onto $\mathrm{Span}_{\mathbb{R}}(\mathbf{x})$ has euclidean norm $\leq \|\mathbf{x}\|/2$. Conclude using the Pythagorean theorem.)

4. From now on, we assume that $f$ and $g$ are coprime and that $B/2 \leq |f|, |g| \leq B$. Let $u, v \in \mathbb{Z}$ be Bezout coefficients, such that $uf + vg = 1$. Show that, given $(u, v)$ and the pair $(f, g)$, one can compute $(F, G) \in \mathbb{Z}^2$ such that $fG - gF = q$ and $|F|, |G| \leq \sqrt{B^2/2 + 2(q/B)^2}$. ($\star\star$)
   (Hint: you may want to first compute any $(\tilde{F}, \tilde{G})$ from $(u, v)$ such that $f\tilde{G} - g\tilde{F} = q$. Then try to reduce $(\tilde{F}, \tilde{G})$ by adding a good multiple of $(g, f)$ and using the previous question.)

5. Show that $\begin{pmatrix} g \\ f \end{pmatrix} \in \mathcal{L}_h$ and that $\begin{pmatrix} G \\ F \end{pmatrix} \in \mathcal{L}_h$.

6. Reciprocally, show that $\begin{pmatrix} 1 \\ h \end{pmatrix}$ and $\begin{pmatrix} 0 \\ q \end{pmatrix}$ can be written as integer linear combinations of $\begin{pmatrix} g \\ f \end{pmatrix}$ and $\begin{pmatrix} G \\ F \end{pmatrix}$. ($\star\star$)
   (Hint: you may want to start by $\begin{pmatrix} 0 \\ q \end{pmatrix}$, and also prove that $\begin{pmatrix} q \\ 0 \end{pmatrix}$ is an integer combination of $\begin{pmatrix} g \\ f \end{pmatrix}$ and $\begin{pmatrix} G \\ F \end{pmatrix}$, before moving on to $\begin{pmatrix} 1 \\ h \end{pmatrix}$.)

7. Conclude that $\begin{pmatrix} g & G \\ f & F \end{pmatrix}$ is a basis of $\mathcal{L}_h$, and that if $B = \sqrt{q}/2$, then this basis has vectors of euclidean norm $\leq 5\sqrt{q}$.

## 3 Lattice bases ($\star$)

*The objective of this exercise is to prove a bunch of properties regarding bases of lattices. Throughout this exercise, the matrix $B$ (or the matrices $B_1$, $B_2$) are invertible matrices in $\mathrm{GL}_n(\mathbb{R})$ for some dimension $n > 0$. Recall that we write $\mathcal{L}(B)$ for the lattice spanned by the columns of the matrix $B$.*

1. Let $B_1, B_2 \in \mathrm{GL}_n(\mathbb{R})$. Show that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ if and only if $B_1 = B_2 \cdot U$ for some $U \in \mathbb{Z}^{n \times n}$ such that $\det(U) = \pm 1$. Such a matrix $U$ is called unimodular. It is an invertible integer matrix whose inverse is also an integer matrix.

2. Let $B_1$ and $B_2$ be two bases of the same lattice $\mathcal{L}$. Prove that $|\det(B_1)| = |\det(B_2)|$.
   This shows that the quantity $|\det(B)|$ does not depend on the choice of the basis $B$ of $\mathcal{L}$, but only on the lattice $\mathcal{L}$. It is usually called the volume or the determinant of the lattice $\mathcal{L}$, and written $\mathrm{vol}(\mathcal{L})$ or $\det(\mathcal{L})$.

3. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two lattices of rank $n$. Show that if $\mathcal{L}_1 \subseteq \mathcal{L}_2$, then $\det(\mathcal{L}_1) = k \cdot \det(\mathcal{L}_2)$ for some integer $k > 0$. This integer $k$ is called the index of $\mathcal{L}_1$ inside $\mathcal{L}_2$ and is written $[\mathcal{L}_2 : \mathcal{L}_1]$.

   *The determinant of a lattice is an important quantity, mostly useful in cryptography thanks to Minkowski's first theorem. This theorem states that in any lattice $\mathcal{L}$ of dimension $n$, there exists a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.*

4. Show that the upper bound in Minkowski's first theorem can be quite loose for some lattices: construct a lattice with $\det(\mathcal{L}) = 1$ and which contains a non-zero vector $v$ whose euclidean norm is arbitrarily close to $0$.

   *The objective of the next questions is to observe that when dealing with lattices, a maximal set of independent vectors is not always a basis, and a minimal set of generating vectors is also not always a basis (which differs from what we are used to in vector spaces).*

5. Exhibit a family of $n$ linearly independent vectors in $\mathbb{Z}^n$ which do not form a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

6. Exhibit a family of $n + 1$ vectors generating $\mathbb{Z}^n$ such that it is not possible to remove any vector from this set to obtain a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.