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 $|f|, |g| \le B := 8$. 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.)

   A: Let us prove the two implications. First, let $\begin{pmatrix} u \\ v \end{pmatrix} \in \mathcal{L}_h$. Since $\mathcal{L}_h$ is the lattice spanned by $\mathbf{B}_h$, there must exists $x_1, x_2 \in \mathbb{Z}$ such that $\begin{pmatrix} u \\ v \end{pmatrix} = x_1 \cdot \begin{pmatrix} 1 \\ h \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ q \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1 \cdot h + x_2 \cdot q \end{pmatrix}$. So $x_1 = u$ and $x_1 \cdot h + x_2 \cdot q = v$, i.e., $v = x_1 \cdot h = u \cdot h \bmod q$. Assume first that $u = 0 \bmod q$, then $v = u \cdot h \bmod q = 0 \bmod q$ too, and so we are in the case $u = v = 0 \bmod q$. Otherwise, $u = x_1$ is invertible modulo q (since q is prime), so we can divide by u and we obtain $h = v \cdot u^{-1} \bmod q$ as desired.

   In the other direction, let us define $x_1 = u$ and $x_2 = (v - u \cdot h)/q$. By what we have seen above, we know that $\begin{pmatrix} u \\ v \end{pmatrix} = x_1 \cdot \begin{pmatrix} 1 \\ h \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ q \end{pmatrix}$. So to prove that $\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathcal{L}_h$, it suffices to prove that both x_1 and x_2 are integers. We always have $x_1 \in \mathbb{Z}$ since $u \in \mathbb{Z}$. For x_2, notice that either $v = u = 0 \bmod q$ and so $v - u \cdot h$ is divisible by q, or we have $h = v \cdot u^{-1}$ and again, $v - u \cdot h$ is divisible by q. In both cases, we conclude that x_2 is an integer, and so $\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathcal{L}_h$ as desired.

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))

   A: Let $\mathbf{b}_0$ and $\mathbf{b}_1$ be the two initial basis vectors $\begin{pmatrix} 1 \\ h \end{pmatrix}$ and $\begin{pmatrix} 0 \\ q \end{pmatrix}$. We will try to avoid computing QR-factorization (which would imply manipulating real numbers and so more difficult computations by hand) of the Lagrange-Gauss algorithm. The key point is that the QR-factorization in Lagrange-Gauss is used for convenience, but it is not really necessary. The important step is the reduction step. In this step, we want to update $\mathbf{b}_1 \leftarrow \mathbf{b}_1 + k \cdot \mathbf{b}_0$ and make the new $\mathbf{b}_1$ as small as possible. Removing $\mathbf{b}_0$ to $\mathbf{b}_1$ will not change the projection of $\mathbf{b}_1$ orthogonally to $\mathbf{b}_0$. But it can reduce the orthogonal projection of $\mathbf{b}_1$ onto $\mathbf{b}_0$. In other words, we want to find k that minimizes the inner product $\langle \mathbf{b}_0, \mathbf{b}_1 + k\mathbf{b}_0 \rangle$. Let's develop the computation

$$\begin{aligned}\langle \mathbf{b}_0, \mathbf{b}_1 + k\mathbf{b}_0 \rangle &= \langle \mathbf{b}_0, \mathbf{b}_1 \rangle + k\langle \mathbf{b}_0, \mathbf{b}_0 \rangle \\ &= 402 \times 1009 + k(1 + 402^2) \\ &= 405618 + k \times 161605.\end{aligned}$$

Finding an integer k that minimizes this sum is exactly performing the (centered) Euclidean division of -405618 by 161605. Put differently, we can find k by dividing -405618 by 161605 and rounding to the closest integer. We obtain $k = -3$.

So we want to update $\mathbf{b}_1$ by replacing it by $\mathbf{b}_1 - 3\mathbf{b}_0 = \begin{pmatrix} -3 \\ -197 \end{pmatrix}$. We then swap $\mathbf{b}_0$ and $\mathbf{b}_1$, and we start again with our new vectors $\mathbf{b}_0 = \begin{pmatrix} -3 \\ -197 \end{pmatrix}$ and $\mathbf{b}_1 = \begin{pmatrix} 1 \\ 402 \end{pmatrix}$.

Let's find k that minimizes

$$\langle \mathbf{b}_0, \mathbf{b}_1 + k\mathbf{b}_0 \rangle = \langle \mathbf{b}_0, \mathbf{b}_1 \rangle + k\langle \mathbf{b}_0, \mathbf{b}_0 \rangle = -79197 + k \times 38818.$$

We have that $k = \lfloor 79197/38818 \rceil = 2$, and so we update $\mathbf{b}_1 \leftarrow \mathbf{b}_1 + 2\mathbf{b}_0 = \begin{pmatrix} -5 \\ 8 \end{pmatrix}$.

Now we swap $\mathbf{b}_0$ and $\mathbf{b}_1$ and we start again with $\mathbf{b}_0 = \begin{pmatrix} -5 \\ 8 \end{pmatrix}$ and $\mathbf{b}_1 = \begin{pmatrix} -3 \\ -197 \end{pmatrix}$. We take $k = \lfloor -\langle \mathbf{b}_0, \mathbf{b}_1 \rangle / \langle \mathbf{b}_0, \mathbf{b}_0 \rangle \rceil = \lfloor 1561/89 \rceil = 18$ and we obtain $\mathbf{b}_1 \leftarrow \mathbf{b}_1 + 18 \cdot \mathbf{b}_0 = \begin{pmatrix} -93 \\ -53 \end{pmatrix}$.

Let's swap $\mathbf{b}_1$ and $\mathbf{b}_0$ and do a last iteration with $\mathbf{b}_0 = \begin{pmatrix} -93 \\ -53 \end{pmatrix}$ and $\mathbf{b}_1 = \begin{pmatrix} -5 \\ 8 \end{pmatrix}$. This time, we have $k = \lfloor 41/11458 \rceil = 0$. So we cannot reduce $\mathbf{b}_1$ anymore, we have reached an optimal basis.

We conclude that a shortest basis of $\mathcal{L}_h$ is given (in columns) by $\begin{pmatrix} -5 & -93 \\ 8 & -53 \end{pmatrix}$.

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.

A: The LLL algorithm from SageMath (version 9.5) produces the same reduced basis $\begin{pmatrix} -5 & -93 \\ 8 & -53 \end{pmatrix}$. (Note that the shortest basis is not unique: we can always permute columns or multiply some column by -1).

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 $|f|, |g| \leq B$.

A: The first vector of the reduced basis is $\begin{pmatrix} -5 \\ 8 \end{pmatrix}$. Using question 1, this means that taking $f = 8$ and $g = -5$, we have $h = f \cdot g^{-1} \bmod q$ (we can check that this is indeed the case: $402 = 8 \cdot (-5)^{-1} \bmod 1009$). Such f and g satisfy $|f|, |g| \leq B = 8$, so h was an NTRU instance.

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 $|f|, |g| \leq B$.)

   A: We use the hint: for each NTRU instance $h \in \mathbb{Z}/q\mathbb{Z}$, there is a pair $(f, g) \in \mathbb{Z}^2$ such that $h = f \cdot g^{-1} \bmod q$ and $|f|, |g| \leq B$, and such pair cannot be used for a different NTRU instance h' (otherwise $h' = f \cdot g^{-1} = h \bmod q$). So we can upper bound the number of NTRU instances in $\mathbb{Z}/q\mathbb{Z}$ by counting the number of pairs $(f, g) \in \mathbb{Z}^2$ with $|f|, |g| \leq B$. There are at most $2B + 1$ choices for both f and g, so the number of pairs (and the number of NTRU instances) is upper bounded by $(2B + 1)^2$. The probability to find an NTRU instance when sampling h uniformly at random in $\mathbb{Z}/q\mathbb{Z}$ is then $\frac{|\text{NTRU instances}|}{|\mathbb{Z}/q\mathbb{Z}|} \leq \frac{(2B+1)^2}{q}$.

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?)

   A: The trapdoor is never unique, indeed, we can always multiply f and g by -1, and we still have $(-f) \cdot (-g)^{-1} = f \cdot g^{-1} = h \bmod q$ and $| - f| = |f| \leq B$ and $| - g| = |g| \leq B$. More generally, if $|f|$ and $|g|$ are smaller than $B/2$ for instance, one can multiply f and g by 2 (or -2) to obtain yet another valid trapdoor.

   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.)

   A: Finding such a k is know as size-reduction of $\mathbf{y}$ by $\mathbf{x}$. This is the key step of the Lagrange-Gauss algorithm for reducing a basis in dimension 2 (and also a key step for the LLL algorithm in larger dimension).

   As explained in the hint, adding multiples of $\mathbf{x}$ to $\mathbf{y}$ will not change the projection of $\mathbf{y}$ orthogonally to $\mathbf{x}$, but it can reduce the orthogonal projection of $\mathbf{y}$ onto $\mathbf{x}$, and this is this projection that we will try to minimize. More formally, let us decompose $\mathbf{y} = \mathbf{y}_1 + \mathbf{y}_2$ with $\langle \mathbf{y}_1, \mathbf{x} \rangle = 0$ and $\mathbf{y}_2 = \alpha \cdot \mathbf{x}$ for some $\alpha \in \mathbb{R}$. We see that $\mathbf{y} + k\mathbf{x} = \mathbf{y}_1 + (\alpha + k)\mathbf{x}$. By the Pythagorean theorem, since $\mathbf{y}_1$ and $\mathbf{x}$ are orthogonal, we obtain that $\|\mathbf{y} + k\mathbf{x}\|^2 = \|\mathbf{y}_1\|^2 + (\alpha + k)^2 \cdot \|\mathbf{x}\|^2$.

   The only parameter we can choose in the equation above is k, which has to be an integer. If we want to minimize $\|\mathbf{y}+k\mathbf{x}\|^2$, we must take $k = \lfloor -\alpha \rceil$, which ensures that the quantity $(\alpha + k)$ is in $[-1/2, 1/2]$. If we pick such a k, then we obtain that $\|\mathbf{y} + k\mathbf{x}\|^2 \leq \|\mathbf{y}_1\|^2 + 1/4 \cdot \|\mathbf{x}\|^2$.

Let us now estimate $\|\mathbf{y}_1\|$. We know that $\det(\mathbf{x}, \mathbf{y}) = \det(\mathbf{x}, \mathbf{y}_1 + \alpha\mathbf{x}) = \det(\mathbf{x}, \mathbf{y}_1) + \alpha \det(\mathbf{x}, \mathbf{x})$ by linearity of the determinant. But $\det(\mathbf{x}, \mathbf{x}) = 0$ and $|\det(\mathbf{x}, \mathbf{y}_1)| = \|\mathbf{x}\| \cdot \|\mathbf{y}_1\|$ since $\mathbf{x}$ and $\mathbf{y}_1$ are orthogonal. We conclude that $\|\mathbf{y}_1\| = |\det(\mathbf{x}, \mathbf{y})|/\|\mathbf{x}\| = |x_1y_2 - x_2y_1|/\|\mathbf{x}\|$. From this, we obtain the upper bound

$$\|\mathbf{y} + k\mathbf{x}\|^2 \leq \|\mathbf{y}_1\|^2 + 1/4 \cdot \|\mathbf{x}\|^2 \leq |x_1y_2 - x_2y_1|^2/\|\mathbf{x}\|^2 + 1/4 \cdot \|\mathbf{x}\|^2$$

as desired.

As a last remark, it remains to prove that k can be efficiently computed. Since $k = \lfloor -\alpha \rceil$, it suffices to show that α can be efficiently computed. But α is simply $\frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\langle \mathbf{x}, \mathbf{x} \rangle}$ (you can check that $\mathbf{y} - \alpha\mathbf{x}$ is orthogonal to $\mathbf{x}$), which can be efficiently computed.

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.)

A: Let us define $\tilde{F} = -q \cdot v$ and $\tilde{G} = q \cdot u$. Then we have $f\tilde{G} - g\tilde{F} = q$ as desired. Now, we call $\mathbf{x} = (f, g)$ and $\mathbf{y} = (\tilde{F}, \tilde{G})$, and we apply the previous question to compute an integer k such that $\|\mathbf{y} + k\mathbf{x}\| \leq \sqrt{\|\mathbf{x}\|^2/4 + |f\tilde{G} - g\tilde{F}|^2/\|\mathbf{x}\|^2}$. Note that by choice of $\tilde{F}$ and $\tilde{G}$, we have $|f\tilde{G} - g\tilde{F}| = q$. Moreover, by assumption, we know that $B/2 \leq |f|, |g| \leq B$, which implies that $B^2/2 \leq \|\mathbf{x}\|^2 \leq 2 \cdot B^2$. Hence, we obtain that

$$\|\mathbf{y} + k\mathbf{x}\| \leq \sqrt{B^2/2 + 2q^2/B^2}.$$

Let us define $F = \tilde{F} + k \cdot f$ and $G = \tilde{G} + k \cdot g$ the coefficients of the vector $\mathbf{y} + k\mathbf{x}$. Then $|F|, |G| \leq \|\mathbf{y} + k\mathbf{x}\| \leq \sqrt{B^2/2 + 2(q/B)^2}$.

It remains to prove that $f \cdot G - g \cdot F = q$. This comes from the fact that

$$\begin{aligned} f \cdot G - g \cdot F &= f \cdot (\tilde{G} + k \cdot g) - g \cdot (\tilde{F} + k \cdot f) \\ &= f \cdot \tilde{G} - g \cdot \tilde{F} + k \cdot (fg - gf) = q. \end{aligned}$$

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

A: Recall from Exercice 1 (question 1), that $\begin{pmatrix} u \\ v \end{pmatrix} \in \mathcal{L}_h$ if and only if $h = v \cdot u^{-1} \bmod q$ or $u = v = 0 \bmod q$. For $\begin{pmatrix} g \\ f \end{pmatrix}$, we know by definition of f, g and h that $h = f \cdot g^{-1} \bmod q$, so $\begin{pmatrix} g \\ f \end{pmatrix} \in \mathcal{L}_h$.

For $\begin{pmatrix} G \\ F \end{pmatrix} \in \mathcal{L}_h$, recall that $f \cdot G - g \cdot F = q$, so we have $g \cdot F = f \cdot G \bmod q$, i.e., $F = f \cdot g^{-1} \cdot G \bmod q = h \cdot G \bmod q$. If $G = 0 \bmod q$, then necessarily we also have $F = 0 \bmod q$, and so $\begin{pmatrix} G \\ F \end{pmatrix} \in \mathcal{L}_h$. Otherwise, G must be invertible modulo q (since q is prime), and so we can rewrite the equation $F \cdot G^{-1} = h \bmod q$, from which we conclude again 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 $\begin{pmatrix} 1 \\ h \end{pmatrix}$.)

A: Let us start with the vector $\begin{pmatrix}0\\q\end{pmatrix}$. We have $\begin{pmatrix}0\\q\end{pmatrix} = G \cdot \begin{pmatrix}g\\f\end{pmatrix} - g \cdot \begin{pmatrix}G\\F\end{pmatrix}$, with G and g integers (here we use the equation $f \cdot G - g \cdot F = q$).

Similarly, we can also prove that the vector $\begin{pmatrix}q\\0\end{pmatrix} = -F \cdot \begin{pmatrix}g\\f\end{pmatrix} + f \cdot \begin{pmatrix}G\\F\end{pmatrix}$ is an integer linear combination of the vectors $\begin{pmatrix}g\\f\end{pmatrix}$ and $\begin{pmatrix}G\\F\end{pmatrix}$.

So it remains to prove that $\begin{pmatrix}1\\h\end{pmatrix}$ is an integer linear combination of $\begin{pmatrix}g\\f\end{pmatrix}$, $\begin{pmatrix}G\\F\end{pmatrix}$, $\begin{pmatrix}q\\0\end{pmatrix}$ and $\begin{pmatrix}0\\q\end{pmatrix}$. Let $\tilde{g}, r \in \mathbb{Z}$ be such that $g\tilde{g} = 1 + q \cdot r$ (such elements exist because g is invertible modulo q). Then

$$\begin{pmatrix}1\\h\end{pmatrix} = \tilde{g} \cdot \begin{pmatrix}g\\f\end{pmatrix} - r \begin{pmatrix}q\\0\end{pmatrix} + r' \begin{pmatrix}0\\q\end{pmatrix},$$

where $r' = (h - f \cdot \tilde{g})/q$. Note that $f \cdot \tilde{g} = f \cdot g^{-1} \bmod q = h \bmod q$, so q divides $(h - f \cdot \tilde{g})$ and r' is an integer.

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 $\leq 5\sqrt{q}$.

   A: We have seen that the vectors $\begin{pmatrix}g\\f\end{pmatrix}$ and $\begin{pmatrix}G\\F\end{pmatrix}$ are in $\mathcal{L}_h$ and that any vector of $\mathcal{L}_h$ can be written as an integer linear combination of these vectors, so they form a basis of $\mathcal{L}_h$. By assumption, the euclidean norm of $\begin{pmatrix}g\\f\end{pmatrix}$ is upper bounded by $\sqrt{2}B \leq 5\sqrt{q}$. For $\begin{pmatrix}G\\F\end{pmatrix}$, we have seen that $|F|, |G| \leq \sqrt{B^2/2 + 2(q/B)^2} \leq \sqrt{q/8 + 2 \cdot (2\sqrt{q})^2} \leq \sqrt{q \cdot (1/8 + 8)} \leq 3\sqrt{q}$. Hence, the euclidean norm of the vector $\begin{pmatrix}G\\F\end{pmatrix}$ is upper bounded by $\sqrt{2} \cdot 3\sqrt{q} \leq 5\sqrt{q}$.

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.

   A: Assume first that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. Then, every column of B_1 belongs to $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. Hence, by definition of the lattice $\mathcal{L}(B_2)$ (integer linear combinations of the columns of B_2), we know that there exists an integer square matrix U_1 such that $B_1 = B_2 \cdot U_1$. Since B_1 and B_2 are both invertible, then U_1 is also invertible (over $\mathbb{R}$). Our objective is to show that U_1 is invertible over $\mathbb{Z}$ (i.e., it's inverse is also an integer matrix). By a similar argument, we know that there exist an invertible (over $\mathbb{R}$) integer matrix U_2 such that $B_2 = B_1 \cdot U_2$.

   Combining both equations, we obtain $B_1 = B_2 \cdot U_1 = B_1 \cdot U_2 \cdot U_1$. Since B_1 is invertible, we can simplify this into $I_n = U_2 \cdot U_1$. Since U_1 and U_2 are invertible over $\mathbb{R}$, their inverse is unique and we conclude that $U_1^{-1} = U_2$ is an integer matrix as desired.

   To conclude, observe that since U_1 and U_2 are integer matrices, then their determinant is also an integer. But we have $1 = \det(I_n) = \det(U_1 \cdot U_2) = \det(U_1) \cdot \det(U_2)$. Hence, the only possibility for $\det(U_1)$ is 1 or -1 (these are the only invertible elements in $\mathbb{Z}$).

   In the other direction, assume that $B_1 = B_2 \cdot U$ with U integer and $\det(U) = \pm 1$. Then, U is invertible over $\mathbb{R}$ and its inverse matrix U^{-1} has integer coefficients (recall that $U^{-1} = 1/\det(U) \cdot \mathrm{adj}(U)$ where the adjugate matrix $\mathrm{adj}(U)$ is integral since U is).

Since U is integral, then by definition every column of $B_1 = B_2 \cdot U$ is in the lattice spanned by B_2. Hence we have $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$. Since U^{-1} is also integral, then every column of $B_2 = B_1 \cdot U^{-1}$ is in the lattice spanned by B_1, and we conclude that $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$.

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 $\det(\mathcal{L})$.

A: We have seen in the previous questions that if $\mathcal{L}(B_1) = \mathcal{L}(B_2)$, then $B_1 = B_2 \cdot U$ for some matrix U with $\det(U) = \pm 1$. Taking the absolute value of the determinant of this equation proves that $|\det(B_1)| = |\det(B_2)|$.

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 $[\mathcal{L}_2 : \mathcal{L}_1]$.

A: Let B_1 be a basis of $\mathcal{L}_1$ and B_2 be a basis of $\mathcal{L}_2$. Since $\mathcal{L}_1 \subseteq \mathcal{L}_2$, then every column of B_1 is in $\mathcal{L}(B_2)$, i.e., there is an integer matrix X such that $B_1 = B_2 \cdot X$. Taking the determinant, we have $\det(B_1) = \det(B_2) \cdot \det(X)$. Hence, $k = |\det(X)|$ and k is indeed an integer since X has integer coefficients (and k is non-zero since B_1 and B_2 are both invertible).

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 $\|v\| \le \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

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.

A: Take $\varepsilon > 0$ and define $\mathcal{L}$ to be the lattice with basis $b_1 = (\varepsilon, 0)^T$ and $b_2 = (0, \varepsilon^{-1})^T$. Then $\det(\mathcal{L}) = 1$ but $\mathcal{L}$ contains the vector b_1 whose norm can be 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 $\mathbb{Z}^n$.

A: One example is the family $b_i = (0, \dots, 0, 2, 0, \dots, 0)$ with a 2 in i-th position, for $i = 1$ to n. Those vectors are linearly independent but they generate the lattice $(2\mathbb{Z})^n$, which is included strictly in $\mathbb{Z}^n$. Note that one cannot add a vector to this family of vectors and still have independent vectors (because independence is defined over $\mathbb{R}$, where things work as expected: the maximal size of an independent set of vectors in $\mathbb{R}^n$ is 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 $\mathbb{Z}^n$.

A: Take $b_0 = (2, 0, \dots, 0)$, $b_1 = (3, 0, \dots, 0)$ and $b_i = (0, \dots, 0, 1, 0, \dots, 0)$ with a i at the i-th position for $i = 2$ to n. Then $(b_i)_{0 \le i \le n}$ generates $\mathbb{Z}^n$. This is because 2 and 3 are coprime, hence one can find an integer linear combination of b_1 and b_2 with a 1 in its first coordinate (just take $b_1 - b_0 = (1, 0, \dots, 0)$).

However, one can check that removing b_0 or b_1 from the list of generator does not generate $\mathbb{Z}^n$ anymore: the first coordinate will always be a multiple of 2 or 3. Similarly, we cannot remove one of the b_i for $i \ge 2$ since the i-th coordinate would always be 0.