Lattice-based Cryptography

1. $\tilde{U} = B_2^{-1} B_1 = U^{-1} = \begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$.
2. $\Lambda_{10}^{\perp}(A)^* = \frac{1}{10}\Lambda_{10}(A)$. The lattice is given by the columns of the matrix $\frac{1}{10}\begin{pmatrix} 4 & 2 \\ -1 & 2 \end{pmatrix}$.
3. $\det(\Lambda) = \frac{\sqrt{3}}{2}$. The lattice contains the vector $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ with $\|v\| = 1$. By definition of Hermite's constant, one has $\frac{\|v\|^2}{\det(\Lambda)} \leq \gamma_2$. Hence $\frac{2}{\sqrt{3}} \leq \gamma_2$.
4. Let $w = (42,\, 25)^T$. Then $B_1^{-1} w = (3.4,\, 14.2)^T$. The rounded coordinates are $x = (3, 14)^T$ giving the lattice vector $B_1 x = (40,\, 25)^T$. This is the closest lattice vector the target vector w. On the other hand, using the 'bad' basis gives $B_2^{-1} w = (67,\, -49.4)^T$. The rounded coordinate vector is $y = (67,\, -49)^T$ and $B_2 y = (46, 21)^T$. This is not the closest lattice vector to w.
5. $\Lambda_q(A)$ is generated by the rows of A, where the coordinates are lifted from $\mathbb{Z}_q$ to $\mathbb{Z}$, and $q\,\mathbb{Z}^n$. Using the definition of the dual lattice, we see that $\Lambda_q(A)^*$ is the set of all $y \in \frac{1}{q}\,\mathbb{Z}^n$ such that $x \cdot y \in \mathbb{Z}^n$ for all lifted rows x of A. Hence $q\Lambda_q(A)^*$ is the set of all $y \in \mathbb{Z}^n$ such that $x \cdot y \in q\,\mathbb{Z}^n$, or equivalently, $x \cdot y \equiv 0 \bmod q$. This shows that
$$q\Lambda_q(A)^* = \Lambda_q^{\perp}(A).$$
Since $(\Lambda^*)^* = \Lambda$ and $(q\Lambda)^* = \frac{1}{q}\,\Lambda^*$, taking the dual of the above equality of lattices gives
$$\frac{1}{q}\,\Lambda_q(A) = (q\Lambda_q(A)^*)^* = (\Lambda_q^{\perp}(A))^* \Longrightarrow \Lambda_q(A) = q(\Lambda_q^{\perp}(A))^*.$$
6. $\lambda_1(\Lambda) \leq \sqrt{100}\,(2^{104})^{\frac{1}{100}} \approx 20.56$. The Gaussian heuristic for $\lambda_1(\Lambda)$ gives:
$$\sqrt{\frac{100}{2\pi e}}\,(2^{104})^{1/100} \approx 4.98.$$
7. (a) $\det(\Lambda) = 611$ and the orthogonality defect is ≈ 2.59.
   (b) Let $b_1 = (-13, 31)^T$ and $b_2 = (0, 47)$. We get $\mu_{21} = \frac{1457}{1130}$ and the GSO basis is b_1, b_2^*, where $b_2^* = (\frac{18941}{1130}, \frac{7943}{1130})^T$. The square norms are $B_1 = 1130$ and $B_2 = \frac{373321}{1130}$. We can check that $b_1 \cdot b_2^* = 0$. Now run the size reduction algorithm:
   $$b_2 \leftarrow b_2 - \lfloor \mu_{21} \rceil b_1 = b_2 - b_1 = (13,\, 16)^T$$
   μ_{21} is set to $\mu_{21} - 1 = \frac{327}{1130}$.
   (c) The Lovacz condition $\frac{3}{4} B_1 \leq B_2 + \mu_{21}^2 B_1$ is not satisfied. The vectors b_1 and b_2 are swapped: $b_1 = (13, 16)^T$ and $b_2 = (-13,\, 31)^T$. We compute $\mu_{21} = \frac{327}{425}$. The GSO basis is b_1, b_2^*, where $b_2^* = (-\frac{9776}{425}, \frac{7943}{425})^T$. The square norms are $B_1 = 425$ and $B_2 = \frac{373321}{425}$. We run the size reduction algorithm:
   $$b_2 \leftarrow b_2 - \lfloor \mu_{21} \rceil b_1 = b_2 - b_1 = (-26, 15)^T.$$
   μ_{21} is set to $\mu_{21} - 1 = -\frac{98}{425}$.
   (d) Now the Lovacz condition is satisfied and the LLL-reduced basis is $b_1 = (13, 16)^T$ and $b_2 = (-26, 15)^T$. The orthogonality defect is ≈ 1.01.

   (e) The shortest nonzero vector is b_1.

8. (a) $c = Hm + r = (-1, -4, -20)^T$.
   (b) $m' = \lfloor H^{-1}c \rceil = (-1, -4, 1) \neq m$. Decryption fails since H is the public 'bad' basis.
   (c) SageMath computes the short LLL-reduced basis B:

```
sage: H=matrix([[1,0,0],[0,1,0],[14,18,63]])
sage: H.transpose().LLL().transpose()
[-2 -1  4]
[-2  1 -3]
[-1  4  2]
```

   (d) We recover the plaintext using the private basis B.

$$H^{-1}B\lfloor B^{-1}c \rceil = H^{-1}B \left\lfloor \begin{pmatrix} \frac{22}{21} \\ -\frac{13}{3} \\ -\frac{17}{21} \end{pmatrix} \right\rceil = H^{-1}B \begin{pmatrix} 1 \\ -4 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ -3 \\ 1 \end{pmatrix}$$

9. The ciphertext is

$$c = p\,rh + m \equiv 22x^4 + 25x^3 + 18x^2 + 18x + 3 \bmod 29.$$

For decryption, we compute

$$a = fc \equiv 28x^4 + 25x + 4 \equiv -x^4 - 4x + 4 \bmod 29.$$

We lift a to $\mathbb{Z}[x]$ and recover the plaintext

$$m = f_p\, a \equiv 2x^4 + 2x^2 + 1 \equiv -x^3 - x^2 + 1 \bmod 3.$$

10. The ciphertext is the polynomial $c = p\,rh + m \bmod q$ and hence

$$c(1) = p\,r(1)h(1) + m(1) \bmod q.$$

By construction, $r \in \mathcal{T}(d, d)$ and so $r(1) = 0$. It follows that $c(1) = m(1) \bmod q$. An adversary can exploit this to win the IND-CPA experiment. They choose two plaintexts m_0 and m_1 with $m_0(1) = 0$ and $m_1(1) = 1$, and can thus distinguish between the plaintexts given the ciphertext c.

This problem can be fixed by reserving one coefficient of m and setting this coefficient so that $m(1) = 0 \bmod q$.

11. (a) We choose $a = (0, 1, 1, 1, 0, 0, 1, 0)^T$. Then $u = (0, 16, 9, 7)^T$ and $c = (20, 2, 22, 15)^T$.
   (b) For decryption, we get $c - S^T u = (12, 20, 22, 10)^T$. Coefficients close to $0 \bmod 23$ give 0 and coefficients close to $12 \bmod 23$ give 1. Hence we recover the plaintext $v = (1, 0, 0, 1)^T$.
   (c) We can assume that the coefficients of $E^T a$ are integers between $-\frac{q}{2}$ and $\frac{q}{2}$. A decryption error occurs if the magnitude (absolute value) of a coordinate of $E^T a$ is greater than $\frac{q}{4} = \frac{23}{4}$. However, with the given matrix E and any binary vector a, the magnitude of the coefficients is 4 at most and encryption errors are impossible. In our example, we have $E^T a = (0, -3, -1, -2) \bmod 23$.
   Now suppose one of the columns of E is $e = (0, 0, 1, 1, 2, 2, -1, -1)^T$. Then a decryption error occurs if $a = (0, 0, 1, 1, 1, 1, 0, 0)^T$, since $e \cdot a = 6$.

12. Follow the example on Kannan's embedding technique to attack LWE, but use the *second* column of P, i.e., `P[:,1]`. For $M = 1$, 2 or 3, the shortest vector of the lattice is $\begin{pmatrix} e \\ M \end{pmatrix}$, where $e = (-1,-1,-1,0,0,0,-1,0)^T$ is the second column of E. Choosing $M = 4$ gives $\begin{pmatrix} e \\ 4 \end{pmatrix}$ as the second shortest vector.

13. Follow the instructions. Note: in part (d), the last line should read `return ZZ(round(y)) % 2`. Alternatively, interpret multiples of 2 in the coordinates of w and $v - w$ as 0.

    Decryption should recover the plaintext, possibly up to one or two bit errors, i.e., almost all coordinates of $v - w \bmod 2$ are zero. The difference $(c - S^T u) - 1002v$ is equal to the error vector $E^T a$. We observe that the coefficients of the difference between $c - S^T u$ and $1002v$ are close to multiples of 2003, with an error of less than $\frac{q}{4} = \frac{2003}{4}$, except at the error positions.

    The public key (A, P) contains $2008 \cdot 136 + 2008 \cdot 136 = 546{,}176$ integers modulo 2003, the private key S has $136^2 = 18{,}496$ integers modulo 2003, the plaintext length is 136 bits, and the ciphertext length is $136 + 136 = 272$ integers modulo 2003.