(1) (4 marks) Show that a $\delta = 3/4$ LLL-reduced basis of a lattice L (assume L is of full rank n) satisfies the following properties where $\mathbf{b}_1$ is the first vector in the LLL-reduced basis:

$$\|\mathbf{b}_1\| \leq 2^{(n-1)/4} \det(L)^{1/n}.$$

(2) (8 marks) A variant of textbook RSA generates the keys using the following procedure,

- generate two distinct primes p and q where $p < q < 2p$
- set $N = pq$
- choose d coprime to $p-1$ and $q-1$
- compute $e \equiv d^{-1} \pmod{\lambda(N)}$ where the Carmichael function

$$\lambda(N) = \text{lcm}(p-1, q-1).$$

Then the public keys are (N, e). Show

- how to encrypt and decrypt and prove the correctness of your decryption.
- how to perform Wiener's attack for such scheme when d is sufficiently small and determine the bound on the size of d for which Wiener's attack works.
- how to factor N after Wiener's attack.

(3) (8 marks) Let $N = pq$ be a RSA modulus such that $p < q < 2p$. Show that given half of the most-significant bits of p, one can efficiently factor N.

More specifically, one knows some p_0 such that $p - p_0 \leq N^{1/4-\epsilon}$ for some $0 < \epsilon < 1/4$. Then show that given N and p_0 one can factor N in time polynomial in $\log N$ and $1/\epsilon$. The idea is to use the Coppersmith's method as follows:

- Let h be some integer to be determined later. Find some linear polynomial $f(x)$ such that all $h+1$ polynomials $f(x)^h, xf(x)^h, x^2f(x)^h, \cdots, x^hf(x)^h$ share some common zero modulo p^h. And find h more such polynomials.
- Work out an appropriate lattice basis using the above $2h+1$ polynomials.
- Analyze determinant of the lattice and length bound guaranteed by LLL.
- Prove that for an appropriate choice of h, the LLL can be used to factor N in time polynomial in $\log N$ and $1/\epsilon$.