Homework 2

Instructor: Chris Peikert
Student: YOUR NAME HERE

This homework is due by the **start of class on October 7** via the course Canvas page. Start early!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea.

You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators and/or sources*** for each problem.

1. Show that an LLL-reduced basis $\mathbf{B}$ of a lattice $\mathcal{L}$ satisfies the following properties:
   (a) $\|\mathbf{b}_1\| \leq 2^{(n-1)/4} \det(\mathcal{L})^{1/n}$.
   (b) $\|\mathbf{b}_2\| \leq 2^{n/4} \cdot (\det(\mathcal{L})/\|\mathbf{b}_1\|)^{1/(n-1)}$
   (c) There exists a shortest nonzero vector in $\mathcal{L}$ whose coefficients with respect to $\mathbf{B}$ all have magnitudes at most 2^{cn} for some constant c.[1]

2. The *covering radius* $\mu(\mathcal{L})$ of an n-dimensional lattice $\mathcal{L}$ is the smallest radius r such that balls of radius r centered at lattice points cover all of $\mathbb{R}^n$, i.e., $\mathbb{R}^n = \cup_{\mathbf{v}\in\mathcal{L}}(\mathbf{v} + r\mathcal{B})$. Equivalently, it is the maximum possible distance that a point in $\mathbb{R}^n$ can be from the lattice.
   (a) Prove that $\mu(\mathcal{L}) \geq \lambda_1(\mathcal{L})/2$.
   (b) Demonstrate a lattice whose ratio of covering radius to minimum distance is $\mu(\mathcal{L})/\lambda_1(\mathcal{L}) = \Omega(\sqrt{n})$.
   (c) Prove that if $\mathbf{B}$ is a basis of $\mathcal{L}$, then $\mu(\mathcal{L}) \leq \frac{1}{2}\sqrt{\sum_i \|\widetilde{\mathbf{b}}_i\|^2}$.
   (d) Another way of stating Minkowski's theorem is that $\lambda_1(\mathcal{L}) \leq 2(\det(\mathcal{L})/V_n)^{1/n}$, where V_n is the volume of an n-dimensional ball of radius 1.
   Prove the *lower* bound $\mu(\mathcal{L}) \geq (\det(\mathcal{L})/V_n)^{1/n}$. [2]

3. Suppose we are given $N = pq$ for some unknown n-bit primes p, q, along with a little more than half of the most significant bits of p. More precisely, we are given some P such that $p = P + x_0$ where $|x_0| \leq B = p^{1/2-\varepsilon}$. In this problem you will show that given this information, we can factor N efficiently.

   Modulo p, the polynomial $f(x) = P + x$ of degree $d = 1$ clearly has a small root $x_0 = p - P$, where $|x_0| \leq p^{1/2-\varepsilon} \ll p^{1/d}$. But we do not know p, so we cannot simply apply Coppersmith's theorem as-is. Fortunately, we do know a multiple of p, namely N. This will be enough to apply Coppersmith's method.
   (a) Let h be an integer to be determined later. The $h + 1$ polynomials
   $$f(x)^h, x \cdot f(x)^h, \ldots, x^h \cdot f(x)^h$$
   are clearly all zero modulo p^h when evaluated at x_0. Find h more polynomials having this property, and which work for the remainder of this problem.
   (b) Define an appropriate lattice basis using the $2h + 1$ polynomials from the previous part, and analyze the determinant and length bound guaranteed by LLL.
   (c) Prove that for an appropriate choice of h, LLL returns a vector corresponding to a polynomial having x_0 as a root over the integers, and argue that this allows us factor N efficiently.

[1] In particular, this lets us solve SVP in time $2^{O(n^2)} \cdot \mathrm{poly}(|\mathbf{B}|)$, by running LLL and then enumerating coefficient vectors.
[2] Note that this implies the statement from part (a), but with a much more sophisticated proof!