Question 2

(1)

First, notice that for the given shortest vector $\mathbf{v} \in \mathcal{L}$ and base vector $\mathbf{b}_i$, $\mathbf{v} + \mathbf{b}_i \in \mathcal{L}(B')$. This is true because:

$$\begin{aligned}
\mathbf{v} + \mathbf{b}_i &= \mathbf{b}_1 a_1 + \mathbf{b}_2 a_2 + \ldots + \mathbf{b}_i(a_i + 1) + \ldots + \mathbf{b}_n a_n \\
&= \mathbf{b}_1 a_1 + \mathbf{b}_2 a_2 + \ldots + \mathbf{b}_i(2k + 1 + 1) + \ldots + \mathbf{b}_n a_n \\
&= \mathbf{b}_1 a_1 + \mathbf{b}_2 a_2 + \ldots + 2\mathbf{b}_i(k + 1) + \ldots + \mathbf{b}_n a_n
\end{aligned}$$

Denote the output of $\text{CVP}_\gamma(B', \mathbf{b}_i)$ by $\mathbf{u}$, then by the definition of γ-CVP:

$$\begin{aligned}
\|\mathbf{u} - \mathbf{b}_i\| &\leq \gamma \min_{\mathbf{x} \in \mathcal{L}(B')} \|\mathbf{b}_i - \mathbf{x}\| \\
&\leq \gamma \|\mathbf{b}_i - (\mathbf{v} + \mathbf{b}_i)\| \\
&= \gamma \|\mathbf{v}\| = \gamma \lambda_1(\mathcal{L}(B))
\end{aligned}$$

In other words, $\mathbf{u} - \mathbf{b}_i$ is a solution to $\text{SVP}_\gamma(B)$

(2)

Let B be the basis of a lattice for which we want to solve $\text{SVP}_\gamma(B)$.

We can modify B by replacing one of its base vector $\mathbf{b}_i$ with $2\mathbf{b}_i$. For a chosen i, denote the modified basis by B_i. In other words:

$$B_i = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, 2\mathbf{b}_i, \ldots, \mathbf{b}_n\}$$

With a CVP_γ oracle, we can solve $\text{CVP}_\gamma(B_i, \mathbf{b}_i)$. Denote the output by $\mathbf{w}_i$. It's easy to see that $\mathbf{w}_i - \mathbf{b}_i \in \mathcal{L}(B)$ because B_i generates a sub-lattice of $\mathcal{L}(B)$.

Notice that if $\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{b}_i \in \mathcal{L}(B)$ is a shortest lattice point, then at least one of the coefficient a_i must be odd. This is true because if all of coefficients are even, then $\frac{1}{2}\mathbf{v}$ is necessarily a shorter vector than $\mathbf{v}$, creating a contradiction.

Therefore, for at least one such $i \in \{1, 2, \ldots, n\}$, $\mathbf{u}_i - \mathbf{b}_i$ falls into the scenario described in part (1), and is thus a solution to $\text{SVP}_\gamma(B)$. Any shorter $\mathbf{u}_j - \mathbf{b}_j$ will also suffice.

Algorithm 1 Solve γ-SVP with γ-CVP oracle

```
v ← b_1                                  ▷ Start with some arbitrary lattice point
for i ∈ {1, 2, ..., n} do
    B_i ← replacing b_i with 2b_i
    u_i ← CVP_γ(B_i, b_i)
    if u_i − b_i is shorter than v then
        v ← u_i − b_i
    end if
end for
    return v
```