Vediamo che l'algoritmo è corretto.

1. che termina
2. che produce una base G-L ridotta

OSS. Nel ciclo while dopo aver effettuato la sostituzione $b_2 = b_2 - \lfloor \mu \rceil b_1$ $\quad \mu = \frac{(b_1, b_2)}{\|b_1\|^2}$

si ha che

$$\underline{(b_1, b_2)} = (b_1, b_2 - (\mu + \varepsilon) b_1) = \qquad |\varepsilon| \leq \frac{1}{2}$$

$$= (b_1, b_2) - (b_1, \mu b_1) - \varepsilon (b_1, b_1)$$

$$= (b_1, b_2) - (b_1, b_2) - \varepsilon (b_1, b_1)$$

$$= \underline{\varepsilon \|b_1\|^2}$$

OSS. Immediato vedere che se $\|b_i\|^2 \leq A$ il numero di bit-operations dell'algoritmo è $O(\log^3(A))$.

Dim. Certamente l'output $\{b_1, b_2\}$ è t.c.

$b_1, b_2 \in \mathcal{L}$ e $\|b_1\| \leq \|b_2\|$

Proviamo che $\forall b \in \mathcal{L}$ $\|b_1\| \leq \|b\|$ i.e. $\|b_1\| = \lambda_1$

Sia $b \in \mathcal{L}$ $b = a_1 b_1 + a_2 b_2$ $a_1, a_2 \in \mathbb{Z}$

$$\|b\|^2 = \|a_1 b_1 + a_2 b_2\|^2 =$$

$$= a_1^2 \|b_1\|^2 + 2 a_1 a_2 (b_1, b_2) + a_2^2 \|b_2\|^2 \geq$$ per l'OH.

$$\geq a_1^2 \|b_1\|^2 - a_1 a_2 \|b_1\|^2 + a_2^2 \|b_2\|^2 \geq$$ perché $\|b_1\| \leq \|b_2\|$

$$\geq (a_1^2 - a_1 a_2 + a_2^2) \|b_1\|^2 \geq \|b_1\|^2$$ $a_1, a_2$ non entrambi 0

Vediamo ora che $\|b_2\| \leq \|b\|$
$\forall\, b = a_1 b_1 + a_2 b_2$ con $a_2 \neq 0$

$$\|b\|^2 = \|a_1 b_1 + a_2 b_2\|^2 =$$

$$= a_1^2 \|b_1\|^2 + a_2^2 \|b_2\|^2 + 2a_1 a_2 (b_1, b_2) + (a_2\|b_1\|^2 - a_2\|b_1$$

$$= a_2^2 \left( \|b_2\|^2 - \|b_1\|^2 \right) + (a_1^2 + a_2^2) \|b_1\|^2 + 2a_1 a_2 (b_1, b_2)$$

$$\geq a_2^2 \left( \|b_2\|^2 - \|b_1\|^2 \right) + (a_1^2 + a_2^2 - a_1 a_2) \|b_1\|^2$$

$$\geq a_2^2 \left( \|b_2\|^2 - \|b_1\|^2 \right) + \|b_1\|^2 + \left( \|b_2\|^2 - \|b_2\|^2 \right)$$

$$= (a_2^2 - 1)\left( \|b_2\|^2 - \|b_1\|^2 \right) + \|b_2\|^2 \geq \|b_2\|^2$$
$$(a_2 \neq 0)$$

Inoltre $\min\{\|b_1\|, \|b_2\|\}$ decresce ad ogni passo (eccetto l'ultimo) e dal momento che ci sono solo un numero finito di vettori nel reticolo con $\| \, \| < r$ $\forall r > 0$ l'algoritmo termina.