LLL example according to method in Hofstein, p. 444



One more important note:

In the algorithm above, .



We denote by ‘[i]=>’ and ‘[note]=>’ execution according to respective instruction and updates according to Note of the Fig. 7.8,

[2]=>

[3]=>

[note]=>

[5]-[7] yield no change since

[8] =>

[9]

[note]=>

[6] =>j=2=>

[note]=>

[note]=>

[6]=>j=1=>

.

[note]=>

[8]=>

[11]=>

.

[12]=>

[note]=>

[5]-[7] yield no change since

[note]=>

[8]=>

[11]=>

.

[12]=>

[note]=>

[6]=>j=1=>

.

[note]=>

[8]=>

(5)

[9]=>

[note]=>

[6]=>j=2 yields no change since

[note]=>

[6]=>j=1 yields no change since

[note]=>

[8]=>

[9]=>

[4]=>

Reduced basis is

.