

Short multipliers for the extended gcd problem

Keith Matthews

March 12, 2003

Abstract

For given non-zero integers s_1, \dots, s_m , the problem of finding integers a_1, \dots, a_m satisfying $s = \gcd(s_1, \dots, s_m) = a_1s_1 + \dots + a_ms_m$, with $a_1^2 + \dots + a_m^2$ minimal, is thought to be computationally hard. In this paper, we present an algorithm which takes as its starting point the recent LLL-based algorithm of Havas, Majewski and Matthews and which often finds a shorter vector (a_1, \dots, a_m) .

1 Introduction

Let s_1, \dots, s_m be integers and $s = \gcd(s_1, \dots, s_m)$. In a recent paper [Havas, Majewski, Matthews 1998], the author and his collaborators used variants of the LLL algorithm to find multiplier vectors (a_1, \dots, a_m) of small Euclidean length $\|X\| = (a_1^2 + \dots + a_m^2)^{1/2}$ such that $s = a_1s_1 + \dots + a_ms_m$. In each case a unimodular $m \times m$ matrix P is produced such that $P[s_1, \dots, s_m]^t = [0, \dots, 0, s]^t$. Rows p_1, \dots, p_{m-1} of P constitute a basis of short vectors for the $(m-1)$ -dimensional lattice Λ formed by the vectors $X = (a_1, \dots, a_m)$ with $a_1, \dots, a_m \in \mathbb{Z}$, satisfying $a_1s_1 + \dots + a_ms_m = 0$. In particular, every such X can be expressed uniquely as an integer linear combination $X = z_1p_1 + \dots + z_{m-1}p_{m-1}$. In addition, p_m , the last row of P , is a short multiplier vector and the general multiplier vector p is given by $p = p_m + x_1p_1 + \dots + x_{m-1}p_{m-1}$, where $x_1, \dots, x_{m-1} \in \mathbb{Z}$.

The matrix P has further properties: If the Gram-Schmidt basis corresponding to rows p_1, \dots, p_m is denoted by p_1^*, \dots, p_m^* , where

$$p_1^* = p_1, \quad p_k^* = p_k - \sum_{j=1}^{k-1} \mu_{kj} p_j^*, \quad \mu_{kj} = \frac{p_k \cdot p_j^*}{p_j^* \cdot p_j^*}, \quad (1)$$

then

$$\begin{aligned} \text{(a)} \quad & |\mu_{kj}| \leq 1/2 \text{ for } 1 \leq j < k \leq m, \\ \text{(b)} \quad & p_k^* \cdot p_k^* \geq (\alpha - \mu_{kk-1}^2) p_{k-1}^* \cdot p_{k-1}^* \text{ for } 2 \leq k \leq m-1. \end{aligned} \quad (2)$$

(Here $1/4 < \alpha \leq 1$.)

In what follows we assume $\alpha = 1$, so that (2) becomes

$$p_k^* \cdot p_k^* \geq (1 - \mu_{kk-1}^2) p_{k-1}^* \cdot p_{k-1}^*. \quad (3)$$

From the equations

$$p_1 = p_1^*, \quad p_k = p_k^* + \sum_{j=1}^{k-1} \mu_{kj} p_j^*, \quad (4)$$

a multiplier vector p may be written as

$$p = p_m + \sum_{k=1}^{m-1} x_k p_k = p_m^* + \sum_{k=1}^{m-1} y_k p_k^*, \quad (5)$$

where

$$y_k = x_k + \sum_{i=k+1}^{m-1} \mu_{ik} x_i + \mu_{mk}. \quad (6)$$

The orthogonality of p_1^*, \dots, p_m^* then implies

$$\begin{aligned} \|p\|^2 &= \|p_m + \sum_{k=1}^{m-1} x_k p_k\|^2 = \|p_m^*\|^2 + \sum_{k=1}^{m-1} y_k^2 \|p_k^*\|^2 \\ &= B_m + Q(x_1, \dots, x_{m-1}), \end{aligned} \quad (7)$$

where

$$\begin{aligned} Q(x_1, \dots, x_{m-1}) &= B_{m-1}(x_{m-1} + \mu_{m,m-1})^2 \\ &\quad + B_{m-2}(x_{m-2} + \mu_{m-1,m-2}x_{m-1} + \mu_{m,m-2})^2 \\ &\quad \vdots \\ &\quad + B_1(x_1 + \mu_{2,1}x_2 + \dots + \mu_{m-1,1}x_{m-1} + \mu_{m,1})^2 \end{aligned} \quad (8)$$

and $B_k = \|p_k^*\|^2$ for $k = 1, \dots, m$.

The equation $P[s_1, \dots, s_m]^t = [0, \dots, 0, s]^t$ and the fact that $[s_1, \dots, s_m]$ is orthogonal to each of p_1, \dots, p_{m-1} together imply

$$p_m^* = \frac{s}{s_1^2 + \dots + s_m^2} (s_1, \dots, s_m). \quad (9)$$

Hence

$$B_m = \|p_m^*\|^2 = \frac{s^2}{s_1^2 + \dots + s_m^2}. \quad (10)$$

From equations (4) and the fact that the determinant of the orthogonal matrix whose rows are p_1^*, \dots, p_m^* , is equal to $\det P = \pm 1$, we also have

$$B_1 \cdots B_m = \det(p_i^* \cdot p_j^*) = (\det P)^2 = 1.$$

Consequently

$$\Delta = (\det \Lambda)^2 = B_1 \cdots B_{m-1} = (s_1^2 + \dots + s_m^2)/s^2. \quad (11)$$

Also (3) becomes

$$B_k \geq (1 - \mu_{kk}^2) B_{k-1}, \quad (12)$$

for $2 \leq k \leq m-1$.

2 The motivation for the algorithm

Before we give our algorithm for generating possibly shorter multipliers than p_m , we give some background.

The minimum value 0 of the quadratic expression in equation (8) occurs at the point $(\rho_1, \dots, \rho_{m-1}) \in \mathbb{Q}^{m-1}$, where

$$\rho_{m-1} = -\mu_{mm-1}, \quad \rho_k = -\left(\sum_{i=k+1}^{m-1} \mu_{ik} \rho_i + \mu_{mk} \right), \quad 1 \leq k < m-1. \quad (13)$$

It is then an easy exercise in determinants to show that for $1 \leq k \leq m-1$

$$\rho_k = -\Delta_k / \Delta, \quad (14)$$

where Δ_k is the $(m-1) \times (m-1)$ determinant formed from the Gram determinant $\Delta = \det(p_i \cdot p_j)$, by replacing the k -th column by

$$(p_m \cdot p_1), \dots, (p_m \cdot p_{m-1}).$$

Consequently Δ_k is an integer.

We remark that in practice all ρ_k tend to be small.

We have also observed that each shortest multiplier is always associated via (5) with a point $(x_1, \dots, x_{m-1}) \in \mathbb{Z}^{m-1}$ in the vicinity of $(\rho_1, \dots, \rho_{m-1})$.

Let D be the set of points $(z_1, \dots, z_{m-1}) \in \mathbb{Q}^{m-1}$ satisfying

$$|z_k + \sum_{i=k+1}^{m-1} \mu_{ik} z_i + \mu_{mk}| < 1, \quad k = m-1, \dots, 1. \quad (15)$$

Then $(\rho_1, \dots, \rho_{m-1}) \in D$. Also $(0, \dots, 0) \in D$.

Definition. We say Property G holds if for each shortest multiplier p , the x_1, \dots, x_{m-1} of equation (5) satisfy $(x_1, \dots, x_{m-1}) \in D$.

Remarks. 1. In view of (15), if the integer vector $(x_1, \dots, x_{m-1}) \in D$, there are at most two possibilities for each x_k . So if property G holds for a given m -tuple (s_1, \dots, s_m) , then the number N of shortest multipliers is at most 2^{m-1} .

2. Given that a shortest multiplier p satisfies $\|p\|^2 \leq \|p_m\|^2$, (7) and (8) show that property G holds if $B_k > \|p_m\|^2$ for $1 \leq k \leq m-1$. This is the case in Example 1 below, but does not always hold, as Example 2 shows.

3. The examples where $s_i = 2$ for $1 \leq i \leq m-1$, $s_m = m$ if m is odd, but $s_m = m-1$ if m is even, produce values $\binom{m-1}{\frac{m-1}{2}}$ and $\binom{m-1}{\frac{m-2}{2}}$, respectively for N .

4. We prove below that property G holds when $m = 3$. The least value of m for which it fails to hold appears to be 11, as in Example 5. Failures occur extremely rarely.

5. We remark that in contrast to our situation, [Rosser 1942] gave an example of the quadratic expression $(2 - 47x - 13y)^2 + (2 - 7x - 2y)^2$, which assumes its minimum value 2 for integers x and y at the point $(-11, 40)$, whereas the minimum value 0 for real numbers x, y occurs at $(-22/3, 80/3)$.

3 The algorithm

We construct a sequence of multiplier vectors X_K , $K = m-1, \dots, 1$, which correspond to points (x_1, \dots, x_{m-1}) in D , close to $(\rho_1, \dots, \rho_{m-1})$, as follows.

Define $x_{m-1} = 0, \dots, x_{K+1} = 0$. Then define $x_K, \dots, x_1 \in \mathbb{Z}$ recursively by:

(i)

$$x_K = \begin{cases} 0 & \text{if } \mu_{mK} = 0 \\ 1 & \text{if } \mu_{mK} < 0 \\ -1 & \text{if } \mu_{mK} > 0; \end{cases}$$

(ii) for $1 \leq k < K$, $x_k = \lceil -\sigma_k \rceil$, where

$$\sigma_k = \sum_{i=k+1}^{m-1} \mu_{ik} x_i + \mu_{mk} \quad (16)$$

and $\lceil \theta \rceil$ is the nearest integer symbol, with $\lceil \theta \rceil = \theta - \frac{1}{2}$, if θ is a non-negative half-integer, but $\theta + \frac{1}{2}$ if θ is a negative half-integer.

We also let $X_0 = p_m$.

Remark. For $m = 3$, a perusal of the list of shortest multipliers in the Appendix reveals that our algorithm will produce all the shortest multipliers. For $m = 4$ the algorithm appears to deliver at least one shortest multiplier. For $5 \leq m \leq 10$, whenever the algorithm fails to deliver a shortest multiplier, the excess length-squared is always observed to be 1, as in Example 2. In example 5, the excess is 2.

4 The case $m = 3$.

Lemma. Let $(x_1, \dots, x_{m-1}) \in \mathbb{Z}^{m-1}$ correspond to a shortest multiplier p via equation (7). Then

$$|x_{m-1} + \mu_{mm-1}| \leq \left(\left(\frac{4}{3} \right)^{m-2} - \frac{3}{4} \right)^{\frac{1}{2}}.$$

Proof. The inequality $\|p\|^2 \leq \|p_m\|^2$ implies $Q(x_1, \dots, x_{m-1}) \leq Q(0, \dots, 0)$. Then equation (8) gives

$$\begin{aligned} (x_{m-1} + \mu_{mm-1})^2 B_{m-1} &\leq \mu_{mm-1}^2 B_{m-1} + \dots + \mu_{m1}^2 B_1 \\ (x_{m-1} + \mu_{mm-1})^2 &\leq \mu_{mm-1}^2 + \mu_{mm-2}^2 \frac{B_{m-2}}{B_{m-1}} + \dots + \mu_{m1}^2 \left(\frac{B_1}{B_{m-1}} \right)^{m-2} \end{aligned}$$

Now (3) gives $B_k \geq (1 - \mu_{kk-1}^2)B_{k-1} \geq \frac{3}{4}B_{k-1}$. Hence

$$\begin{aligned} (x_{m-1} + \mu_{mm-1})^2 &\leq \mu_{mm-1}^2 + \mu_{mm-2}^2 \frac{4}{3} + \cdots + \mu_{m1}^2 \left(\frac{4}{3}\right)^{m-2} \\ &\leq \frac{1}{4} \left(1 + \frac{4}{3} + \cdots + \left(\frac{4}{3}\right)^{m-2}\right) \\ &= \frac{1}{4} \left(\frac{\left(\frac{4}{3}\right)^{m-1} - 1}{\frac{4}{3} - 1}\right) = \left(\frac{4}{3}\right)^{m-2} - \frac{3}{4}. \end{aligned}$$

Corollary. Property G holds if $m = 3$.

Proof. Assume $m = 3$ and that $(x_1, x_2) \in \mathbb{Z}^2$ defines a minimum point for $Q(x_1, x_2) = (x_2 + \mu_{32})^2 B_2 + (x_1 + \mu_{21}x_2 + \mu_{31})^2 B_1$.

Then from the Lemma, we have

$$|x_2 + \mu_{32}| \leq \sqrt{7/12}. \quad (17)$$

Also the inequalities $x_2(x_2 + 2\mu_{32}) \geq 0$ and $Q(x_1, x_2) \leq Q(0, 0)$ give

$$|x_1 + \sigma_1| = |x_1 + \mu_{21}x_2 + \mu_{31}| \leq |\mu_{31}|. \quad (18)$$

Remark. From the Corollary, it follows that $N \leq 4$ if $m = 3$. In fact $N \leq 3$ if $m = 3$. For if $N = 4$, we see from (17) and (18) that $\mu_{32} = \epsilon_1/2 = \pm 1/2$, $\mu_{31} = \epsilon_2/2 = \pm 1/2$, $\mu_{21} = 0$. Then

$$1 = (\det P)^2 = \det(p_i \cdot p_j) = \begin{pmatrix} \|p_1\|^2 & 0 & \frac{\epsilon_1}{2}\|p_1\|^2 \\ 0 & \|p_2\|^2 & \frac{\epsilon_2}{2}\|p_2\|^2 \\ \frac{\epsilon_1}{2}\|p_1\|^2 & \frac{\epsilon_2}{2}\|p_2\|^2 & \|p_3\|^2 \end{pmatrix},$$

which gives $4 = \|p_1\|^2\|p_2\|^2(4\|p_3\|^2 - p_1 \cdot p_2 - \|p_2\|^2)$.

This leads to a contradiction, as the $p_i \cdot p_j$ are integers.

The example $(s_1, s_2, s_3) = (41, 43, 49)$ shows that the bound $N = 3$ is attained. Here the quadratic expression in (8) is

$$Q(x_1, x_2) = \frac{5931}{26}(x_2 - \frac{2899}{5931})^2 + 26(x_1 - \frac{7}{26}x_2 + \frac{13}{26})^2.$$

The unimodular matrix $P = \begin{bmatrix} 3 & -4 & 1 \\ -10 & -3 & 11 \\ 6 & 0 & -5 \end{bmatrix}$.

$$(\rho_1, \rho_2) = \left(-\frac{2185}{5931}, \frac{2899}{5931}\right).$$

Also X_2, X_1, X_0 are given by

K	(x_1, x_2)	X_K	$\ X_K\ ^2$
2	(0, 1)	(-4, -3, 6)	61
1	(-1, 0)	(3, 4, -6)	61
0	(0, 0)	(6, 0, -5)	61

and are the shortest multiplier vectors.

5 Numerical results

Example 1. Take s_1, s_2, s_3 to be 4, 6, 9.

The unimodular matrix $P = \begin{bmatrix} 3 & -2 & 0 \\ 0 & 3 & -2 \\ -2 & 0 & 1 \end{bmatrix}$.

The quadratic expression in (8) and the ρ_k of (14) are given by

$$Q(x_1, x_2) = \frac{133}{13} \left(x_2 - \frac{62}{133}\right)^2 + 13 \left(x_1 - \frac{6}{13}x_2 - \frac{6}{13}\right)^2,$$

$$(\rho_1, \rho_2) = \left(\frac{90}{133}, \frac{62}{133}\right).$$

Also X_2, X_1, X_0 are given by

K	(x_1, x_2)	X_K	$\ X_K\ ^2$
2	(1, 1)	(1, 1, -1)	3
1	(1, 0)	(1, -2, 1)	6
0	(0, 0)	(-2, 0, 1)	5

The shortest multiplier is $X_2 = p_3 + p_1 + p_2$.

Example 2. Take s_1, \dots, s_5 to be 10, 51, 104, 177, 307.

The unimodular matrix $P = \begin{bmatrix} -2 & 1 & -2 & 1 & 0 \\ -1 & 0 & 1 & -4 & 2 \\ -3 & -4 & 1 & -1 & 1 \\ 3 & -1 & -4 & -1 & 2 \\ -3 & 0 & 2 & -1 & 0 \end{bmatrix}$.

The quadratic expression in (8) is

$$Q(x_1, \dots, x_4) = \frac{139095}{4770} \left(x_4 - \frac{68385}{139095}\right)^2 + \frac{4770}{204} \left(x_3 - \frac{1320}{4770}x_4 + \frac{1566}{4770}\right)^2$$

$$+ \frac{204}{10} \left(x_2 + \frac{96}{204}x_3 + \frac{10}{204}x_4 + \frac{94}{204}\right)^2 + 10 \left(x_1 - \frac{4}{10}x_2 - \frac{1}{10}x_3 + \frac{1}{10}\right)^2.$$

$$(\rho_1, \rho_2, \rho_3, \rho_4) = \left(-\frac{38528}{139095}, -\frac{54861}{139095}, -\frac{26741}{139095}, \frac{68385}{139095}\right).$$

Also X_4, \dots, X_0 are given by

K	(x_1, x_2, x_3, x_4)	X_K	$\ X_K\ ^2$
4	$(0, -1, 0, 1)$	$(1, -1, -3, 2, 0)$	15
3	$(0, 0, -1, 0)$	$(0, 4, 1, 0, -1)$	18
2	$(0, -1, 0, 0)$	$(-2, 0, 1, 3, -2)$	18
1	$(-1, 0, 0, 0)$	$(-1, -1, 4, -2, 0)$	22
0	$(0, 0, 0, 0)$	$(-3, 0, 2, -1, 0)$	14

The shortest multiplier is $p = p_5 + p_4 = [0, -1, -2, -2, 2]$, with $\|p\|^2 = 13$. Property G holds here.

Example 3. (Example 7.2 of [Havas, Majewski, Matthews 1998])

Take s_1, \dots, s_{10} to be 763836, 1066557, 113192, 1785102, 1470060, 3077752, 114793, 3126753, 1997137, 2603018.

The unimodular matrix $P =$

$$\begin{bmatrix} -2 & 0 & -3 & 1 & 0 & 0 & 0 & -1 & -1 & 2 \\ 0 & -1 & 2 & 2 & -1 & -1 & 3 & -1 & 1 & 1 \\ -2 & 0 & 0 & -1 & 3 & -3 & -1 & 2 & 1 & 0 \\ 0 & 3 & 2 & 3 & 2 & -3 & 1 & 0 & 0 & -1 \\ -2 & 2 & 2 & 0 & -1 & 3 & -3 & -2 & -1 & 0 \\ 2 & 2 & -2 & -5 & -2 & 1 & 2 & 1 & 1 & 0 \\ 0 & 2 & 0 & -2 & -4 & -1 & -1 & 4 & -1 & 0 \\ -3 & 3 & -1 & 2 & -2 & 1 & 0 & 1 & 4 & -6 \\ 0 & 2 & -1 & 2 & -3 & -5 & -4 & -1 & 5 & 3 \\ -1 & 0 & 1 & -3 & 1 & 3 & 3 & -2 & -2 & 2 \end{bmatrix}.$$

Then X_9, \dots, X_0 are given by

K	(x_1, \dots, x_9)	X_K	$\ X_K\ ^2$
9	$(-1, -1, -1, 0, -1, -1, 0, 0, 1)$	$(3, -1, 1, 2, -1, -2, -2, -2, 2, 2)$	36
8	$(0, -1, 0, 0, -1, -1, 0, 1, 0)$	$(-4, 0, -2, 2, 3, 1, 1, 1, 1, -5)$	62
7	$(0, 0, 0, 0, -1, -1, 1, 0, 0)$	$(-1, -2, 1, 0, 0, -2, 3, 3, -3, 2)$	41
6	$(0, -1, 0, 0, -1, -1, 0, 0, 0)$	$(-1, -3, -1, 0, 5, 0, 1, 0, -3, 1)$	47
5	$(0, -1, -1, 1, -1, 0, 0, 0, 0)$	$(3, 2, -1, -1, 2, 1, 5, -1, -3, 0)$	55
4	$(0, -1, 0, 1, 0, 0, 0, 0, 0)$	$(-1, 4, 1, -2, 4, 1, 1, -1, -3, 0)$	50
3	$(0, 0, 1, 0, 0, 0, 0, 0, 0)$	$(-3, 0, 1, -4, 4, 0, 2, 0, -1, 2)$	51
2	$(0, -1, 0, 0, 0, 0, 0, 0, 0)$	$(-1, 1, -1, -5, 2, 4, 0, -1, -3, 1)$	59
1	$(-1, 0, 0, 0, 0, 0, 0, 0, 0)$	$(1, 0, 4, -4, 1, 3, 3, -1, -1, 0)$	54
0	$(0, 0, 0, 0, 0, 0, 0, 0, 0)$	$(-1, 0, 1, -3, 1, 3, 3, -2, -2, 2)$	42

Truncated to 2 decimals, $\rho = (-0.41, -0.80, -0.44, 0.02, -0.76, -0.73, 0.25, 0.25, 0.40)$

X_9 is the shortest multiplier vector. Property G holds here.

Example 4. Take s_1, \dots, s_{40} to be

324234553, 7856756, 3524634, 5675646857, 24364565, 8957897589789789, 464564564565,
67857965897897890, 4364564565, 6787867867, 43643564356, 67867867968, 546345756,
324524545, 678678967967, 3425462668, 76867896796, 43264576568678, 246456758678768,
2464564756746, 5367567568769898798, 4564564262462456, 578578678679689689678,
263464357567568578, 456437567586798679689685, 456426245624564, 567567567567, 462564564786,

87878678678, 4363645635758, 67867865786, 456435656, 678657865857, 789897689784, 343643564565, 678678657879, 678, 678678678678, 6345736756756867, 6575675678.

Here LLL delivers a p_{40} with $\|p_{40}\|^2 = 30$ and our algorithm gives a multiplier X_{27} with $\|X_{27}\|^2 = 18$.

There are 2 shortest multipliers, lengthsquared 14:

$$\begin{aligned}
& p_{40} - 2p_2 - p_3 - 2p_5 - p_6 + p_8 - p_{12} + p_{15} + p_{16} - p_{17} + p_{18} - p_{21} + p_{23} + p_{24} \\
& = (-1, 1, 0, 1, 0, 0, -1, 0, 0, 1, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, -1, -1, -1, 0, 1), \\
& p_{40} - p_1 - p_2 + 2p_4 + p_5 + p_6 + p_8 - p_9 + p_{11} + 3p_{13} + p_{14} + 2p_{16} - 2p_{17} + p_{18} - p_{20} + p_{21} + p_{22} + p_{27} - p_{28} \\
& = (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, -1, -1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, -1, 0, 0, 0, 1, 1, -1, -1, -1, 0, 1, 0, 0, -1).
\end{aligned}$$

Truncated to 2 decimals,

$$\begin{aligned}
\rho = & (-0.31, -1.36, -0.07, 1.91, -0.47, 0.14, -0.36, 0.61, -0.94, -0.26, 0.33, -0.30, 1.85, 0.66, 0.09, \backslash \\
& 1.31, -1.67, 0.75, 0.36, -0.63, 0.19, 0.68, -0.19, 0.40, 0.15, -0.29, 0.43, -0.44, -0.00, 0.00, 0.00, 0.00, \backslash \\
& -0.00, 0.00, -0.00, 0.00, 0.00, 0.00, 0.00)
\end{aligned}$$

Property G holds here.

Example 5. Take s_1, \dots, s_{11} to be 29196545, 2058462515, 354950953, 434047189, 333570961, 1208129565, 1676298297, 813677221, 224909089, 650841491, 1843221943. The shortest X_K is $X[7] = p_{11} + p_2 - p_7 = (-3, -4, 3, 4, -2, 0, 4, 0, 3, 1, -1)$ with $\|X_7\|^2 = 81$. The shortest multiplier is

$$p = p_{11} + p_2 - p_3 - p_5 - p_{10} = (3, 1, 1, -3, -3, 0, -2, 6, 1, -3, 0),$$

with $\|p\|^2 = 79$.

Property G does not hold, as

$$x_{10} = -1 \text{ and } \sigma_{10} = -469807408429549190/13467046613442016227 \approx -0.348.$$

Example 6. The following random examples illustrate the improved multipliers X_K that are produced by the algorithm in section 3. The shortest multiplier vectors are unknown here.

m	$\ p_m\ ^2$	$\ X_K\ ^2$
100	15	$\ X_{96}\ ^2 = 8$
150	17	$\ X_{147}\ ^2 = 9$
200	14	$\ X_{80}\ ^2 = 8$
250	12	$\ X_{96}\ ^2 = 9$

6 Appendix

In this section we present a complete classification of the possible shortest multipliers when $m = 3$, based on inequalities (17) and (18):

$$|x_2 + \mu_{32}| \leq \sqrt{7/12} \text{ and } |x_1 + \mu_{21}x_2 + \mu_{31}| \leq |\mu_{31}|.$$

1. $\mu_{32} = 0, |\mu_{31}| < 1/2$: p_3 .
2. $\mu_{32} = 0, \mu_{31} = 1/2$: p_3 and $p_3 - p_1$.
3. $\mu_{32} = 0, \mu_{31} = -1/2$: p_3 and $p_3 + p_1$.
4. $0 < \mu_{32} \leq 1/2, 0 \leq \mu_{31} < 1/2$:
 - (i) $\mu_{21} \geq 0$: p_3 or $p_3 - p_2$.
 - (ii) $\mu_{21} < 0$: p_3 or $p_3 - p_1 - p_2$.
5. $0 < \mu_{32} \leq 1/2, \mu_{31} = 1/2$: (Here $\|p_3\| = \|p_3 - p_1\|$)
 - (i) $\mu_{21} > 0$: p_3 and $p_3 - p_1$, or $p_3 - p_2$.
 - (ii) $\mu_{21} < 0$: p_3 and $p_3 - p_1$, or $p_3 - p_1 - p_2$.
 - (iii) $\mu_{21} = 0$: p_3 and $p_3 - p_1$. Note: $\mu_{32} < 1/2$ here.
 For if $\mu_{32} = 1/2$, we have 4 shortest multipliers:

$$p_3, p_3 - p_1, p_3 - p_2, p_3 - p_1 - p_2.$$
6. $0 < \mu_{32} \leq 1/2, -1/2 < \mu_{31} \leq 0$:
 - (i) $\mu_{21} > 0$: p_3 or $p_3 + p_1 - p_2$.
 - (ii) $\mu_{21} \leq 0$: p_3 or $p_3 - p_2$.
7. $0 < \mu_{32} \leq 1/2, \mu_{31} = -1/2$: (Here $\|p_3\| = \|p_3 + p_1\|$)
 - (i) $\mu_{21} > 0$: p_3 and $p_3 + p_1$, or $p_3 + p_1 - p_2$.
 - (ii) $\mu_{21} < 0$: p_3 and $p_3 + p_1$, or $p_3 - p_2$.
 - (iii) $\mu_{21} = 0$: p_3 and $p_3 + p_1$. ($\mu_{32} < 1/2$.)
8. $-1/2 \leq \mu_{32} < 0, -1/2 < \mu_{31} \leq 0$:
 - (i) $\mu_{21} \geq 0$: p_3 or $p_3 + p_2$.
 - (ii) $\mu_{21} < 0$: p_3 or $p_3 + p_1 + p_2$.
9. $-1/2 \leq \mu_{32} < 0, \mu_{31} = -1/2$: (Here $\|p_3\| = \|p_3 + p_1\|$)
 - (i) $\mu_{21} > 0$: p_3 and $p_3 + p_1$, or $p_3 + p_2$.

- (ii) $\mu_{21} < 0$: p_3 and $p_3 + p_1$, or $p_3 + p_1 + p_2$.
 - (iii) $\mu_{21} = 0$: p_3 and $p_3 + p_1$. ($-1/2 < \mu_{32}$.)
10. $-1/2 \leq \mu_{32} < 0, 0 \leq \mu_{31} < 1/2$:
- (i) $\mu_{21} \leq 0$: p_3 or $p_3 + p_2$.
 - (ii) $\mu_{21} > 0$: p_3 or $p_3 - p_1 + p_2$.
11. $-1/2 \leq \mu_{32} < 0, \mu_{31} = 1/2$: (Here $\|p_3\| = \|p_3 - p_1\|$)
- (i) $\mu_{21} > 0$: p_3 and $p_3 - p_1$, or $p_3 - p_1 + p_2$.
 - (ii) $\mu_{21} < 0$: p_3 and $p_3 - p_1$, or $p_3 + p_2$.
 - (iii) $\mu_{21} = 0$: p_3 and $p_3 - p_1$. ($-1/2 < \mu_{32}$.)

References

- [Havas, Majewski, Matthews 1998] G. Havas, B.S. Majewski, K.R. Matthews, *Extended gcd and Hermite normal form algorithms via lattice reduction*, Experimental Mathematics 7 No 2 (1998) 125–136.
- [Rosser 1942] J.B. Rosser, *A generalization of the Euclidean algorithm to several dimensions*, Duke Math 9 (1942) 59–95.

K. R. Matthews, Department of Mathematics, The University of Queensland, Brisbane 4072, Australia (krm@maths.uq.edu.au, <http://www.maths.uq.edu.au/~krm/>)