PSEUDOCODE FOR FINDING THE SHORTEST MULTIPLIERS
FOR THE EXTENDED GCD PROBLEM

KEITH MATTHEWS

Input: \( m \) positive integers \( d_1, \ldots, d_m \).
Output: \( \gcd(d_1, \ldots, d_m) \) and all multiplier vectors \((y_1, \ldots, y_m) \in \mathbb{Z}^m\) such that \( y_1d_1 + \cdots + y_md_m = g \).

Perform the LLLGCD algorithm to get a \( m \times m \) unimodular matrix \( A \) whose last row is a small multiplier vector.

The general multiplier has the form \( Y = A_m - x_1A_1 - \cdots - x_{m-1}A_{m-1} \), where \( x_1, \ldots, x_{m-1} \) are integers.

Get the Cholesky decomposition of \( G = AA^t \):

\[
G = Q^t D Q
\]

where

\[
D = \text{diag}(\Delta_1, \Delta_2/\Delta_1, \ldots, \Delta_m/\Delta_{m-1}) = \text{diag}(q_{11}, q_{22}, \ldots, q_{mm})
\]

and \( Q = \begin{bmatrix} 1 & q_{1,2} & \cdots & N_1 \\
0 & 1 & q_{2,3} & \cdots & N_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \cdots & 1 & q_{m-1,m-1} & N_{m-1} \\
0 & \cdots & 0 & 1 & 1 \end{bmatrix} \)

is a unit upper triangular matrix.

We solve the inequality \( ||Y||^2 \leq ||A_m||^2 \) until either a shorter \( Y \) is found - in which case the old \( Y \) is replaced by the shorter one, otherwise the \( Y \) of minimum length are determined.

\[
||Y||^2 = q_{1,1}(x_1 + \cdots + q_{1,m-1}x_{m-1} - N_1)^2 \\
+ q_{2,2}(x_2 + \cdots + q_{2,m-1}x_{m-1} - N_2)^2 \\
+ \cdots + q_{m-1,m-1}(x_{m-1} - N_{m-1} - q_{m,m} - 1)^2 + q_{m,m} = Q(x) + q_{m,m}.
\]

We note that

\[
q_{1,1}N_1^2 + \cdots + q_{m-1,m-1}N_{m-1}^2 = ||A_m||^2 - q_{m,m}.
\]

Also

\[
||Y||^2 \leq ||A_m||^2 \iff Q(x) \leq ||A_m||^2 - q_{m,m} = \sum_{i=1}^{m-1} q_{i,i}N_i^2.
\]

The rest of the code is a modification of the Fincke-Pohst algorithm in [1].

\[
m \leftarrow m - 1; \quad \text{count} = 0 \\
C \leftarrow \sum_{i=1}^{m} q_{i,i}N_i^2 \\
i \leftarrow m; \quad T_i \leftarrow C; \quad U_i \leftarrow 0 \\
\textbf{while} 1 \quad (\text{forever}) \quad \textbf{do} \\
\quad Z \leftarrow (T_i/q_{i,i})^{1/2} \\
\quad U_{Bi} \leftarrow \lfloor Z + N_i - U_i \rfloor \\
\quad x_i \leftarrow -\lfloor Z + U_i - N_i \rfloor - 1
\]

Date: 18th August 2011.
while2 (forever) do
x_i ← x_i + 1
if1 x_i ≤ UB_i then
   if2 i = 1 then
      count ← count + 1, found multiplier
      if4 this is shorter than A_m
         repeat with A_m replaced by this smaller multiplier
      else
         continue while2 loop
   end if4
else
   i ← i − 1
   U_i ← \sum_{j=i+1}^m q_{i,j}x_j
   T_i ← T_{i+1} - q_{i+1,i+1}(x_{i+1} + U_{i+1} - N_{i+1})^2
   break out of while2 loop
end if2
else
   i ← i + 1
   if3 i > m then
      print the count shortest multipliers and exit
   end if3
   continue while2 loop
end if1
end while2
end while1

References
