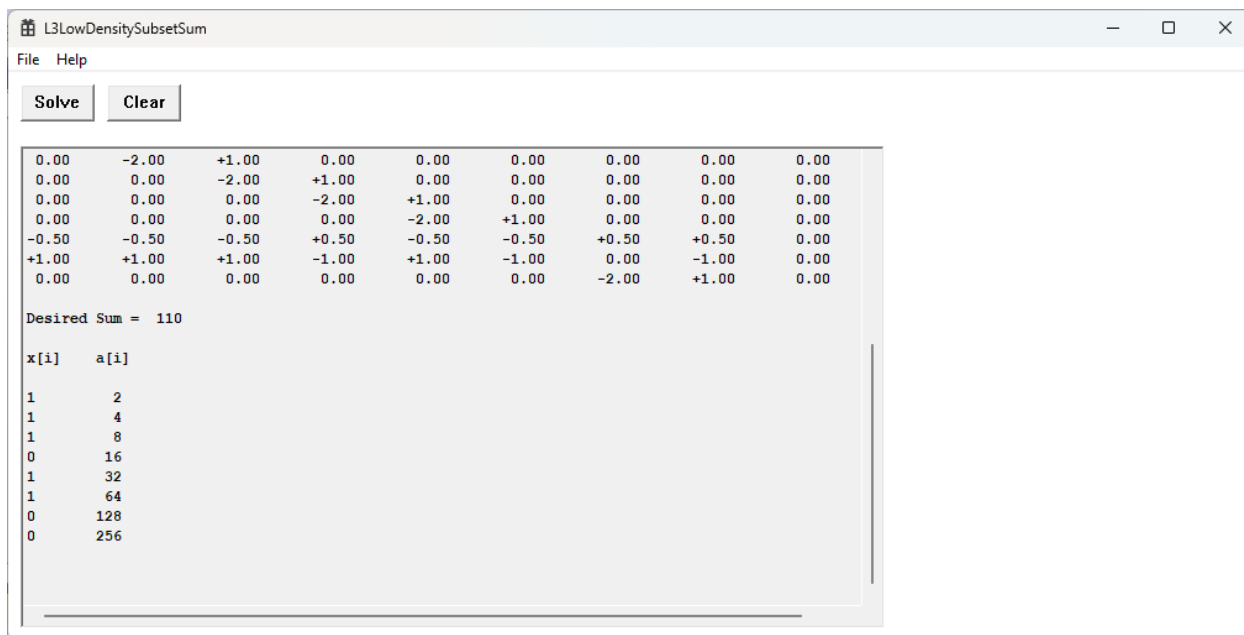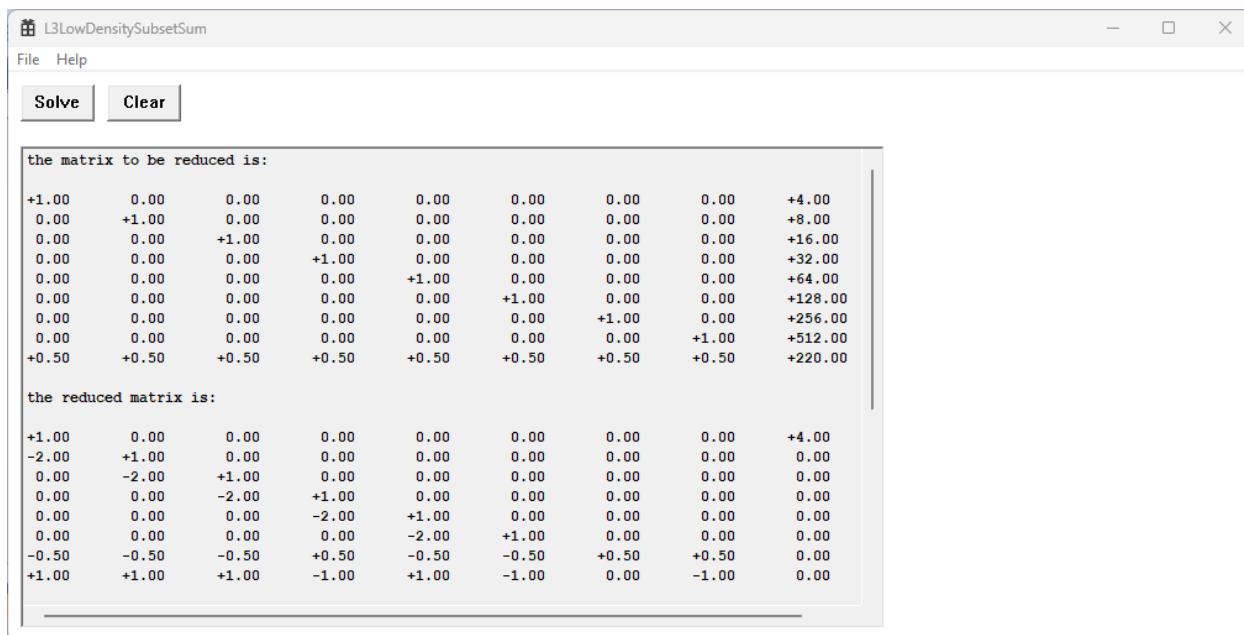Blog Entry © Tuesday, October 21, 2025, by James Pate Williams, Jr., Solving Low Density Subset Sum Problems Using the LLL-Lattice Reduction Algorithm

Reference: Algorithm found in the "Handbook of Applied Cryptography" (c) 1997 by Alfred J. Menezes, Paul C van Oorschot, and Scott Vanstone 3.105 Algorithm Chapter 3 pages 120 – 121. The app was created using Microsoft Visual Studio 2022 Win32 C/C++ Desktop Release x64 Configuration. The density of the two solved problems was 5 / 8 = 0.625.

```
L3LowDensitySubsetSum                                              —  □  X
File   Help

  Solve     Clear

the matrix to be reduced is:

+1.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00      +4.00
 0.00     +1.00      0.00      0.00      0.00      0.00      0.00      0.00      +8.00
 0.00      0.00     +1.00      0.00      0.00      0.00      0.00      0.00     +16.00
 0.00      0.00      0.00     +1.00      0.00      0.00      0.00      0.00     +32.00
 0.00      0.00      0.00      0.00     +1.00      0.00      0.00      0.00     +64.00
 0.00      0.00      0.00      0.00      0.00     +1.00      0.00      0.00    +128.00
 0.00      0.00      0.00      0.00      0.00      0.00     +1.00      0.00    +256.00
 0.00      0.00      0.00      0.00      0.00      0.00      0.00     +1.00    +512.00
+0.50     +0.50     +0.50     +0.50     +0.50     +0.50     +0.50     +0.50    +220.00

the reduced matrix is:

+1.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00      +4.00
-2.00     +1.00      0.00      0.00      0.00      0.00      0.00      0.00       0.00
 0.00     -2.00     +1.00      0.00      0.00      0.00      0.00      0.00       0.00
 0.00      0.00     -2.00     +1.00      0.00      0.00      0.00      0.00       0.00
 0.00      0.00      0.00     -2.00     +1.00      0.00      0.00      0.00       0.00
 0.00      0.00      0.00      0.00     -2.00     +1.00      0.00      0.00       0.00
-0.50     -0.50     -0.50     +0.50     -0.50     -0.50     +0.50     +0.50       0.00
+1.00     +1.00     +1.00     -1.00     +1.00     -1.00      0.00     -1.00       0.00
```

```
L3LowDensitySubsetSum                                              —  □  X
File   Help

  Solve     Clear

 0.00     -2.00     +1.00      0.00      0.00      0.00      0.00      0.00       0.00
 0.00      0.00     -2.00     +1.00      0.00      0.00      0.00      0.00       0.00
 0.00      0.00      0.00     -2.00     +1.00      0.00      0.00      0.00       0.00
 0.00      0.00      0.00      0.00     -2.00     +1.00      0.00      0.00       0.00
-0.50     -0.50     -0.50     +0.50     -0.50     -0.50     +0.50     +0.50       0.00
+1.00     +1.00     +1.00     -1.00     +1.00     -1.00      0.00     -1.00       0.00
 0.00      0.00      0.00      0.00      0.00      0.00     -2.00     +1.00       0.00

Desired Sum =  110

x[i]    a[i]

1        2
1        4
1        8
0       16
1       32
1       64
0      128
0      256
```

By modifying two lines of code, we can change from base 2 to base 3 for solutions to the low density subset sum problem.

File Help

Solve **Clear**

```
the matrix to be reduced is:

+1.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00     +6.00
 0.00     +1.00      0.00      0.00      0.00      0.00      0.00      0.00    +18.00
 0.00      0.00     +1.00      0.00      0.00      0.00      0.00      0.00    +54.00
 0.00      0.00      0.00     +1.00      0.00      0.00      0.00      0.00   +162.00
 0.00      0.00      0.00      0.00     +1.00      0.00      0.00      0.00   +486.00
 0.00      0.00      0.00      0.00      0.00     +1.00      0.00      0.00  +1458.00
 0.00      0.00      0.00      0.00      0.00      0.00     +1.00      0.00  +4374.00
 0.00      0.00      0.00      0.00      0.00      0.00      0.00     +1.00 +13122.0
+0.50     +0.50     +0.50     +0.50     +0.50     +0.50     +0.50     +0.50 +13860.0

the reduced matrix is:

+1.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00     +6.00
-3.00     +1.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00
 0.00     -3.00     +1.00      0.00      0.00      0.00      0.00      0.00      0.00
 0.00      0.00     -3.00     +1.00      0.00      0.00      0.00      0.00      0.00
 0.00      0.00      0.00     -3.00     +1.00      0.00      0.00      0.00      0.00
 0.00      0.00      0.00      0.00     -3.00     +1.00      0.00      0.00      0.00
 0.00      0.00      0.00      0.00      0.00     -3.00     +1.00      0.00      0.00
+0.50     -1.50     -0.50     -0.50     -0.50     +0.50     +0.50     -0.50      0.00
```

File Help

Solve **Clear**

```
 0.00     -3.00     +1.00      0.00      0.00      0.00      0.00      0.00      0.00
 0.00      0.00     -3.00     +1.00      0.00      0.00      0.00      0.00      0.00
 0.00      0.00      0.00     -3.00     +1.00      0.00      0.00      0.00      0.00
 0.00      0.00      0.00      0.00     -3.00     +1.00      0.00      0.00      0.00
 0.00      0.00      0.00      0.00      0.00     -3.00     +1.00      0.00      0.00
+0.50     -1.50     -0.50     -0.50     -0.50     +0.50     +0.50     -0.50      0.00
-0.50     +1.50     +0.50     +0.50     +0.50     -0.50     -3.50     +1.50      0.00

Desired Sum = 6930

x[i]      a[i]

0          3
2          9
1         27
1         81
1        243
0        729
0       2187
1       6561
```