Exercises: Euclidean Algorithm

Spreadsheet Exercise: Extended Euclidean Algorithm

In this part we will get Excel to run the Extended Euclidean Algorithm, so that next week we can use it to calculate decryption exponents for RSA.

1. First, use the extended Euclidean algorithm and, by hand, show that the highest common factor of 17 and 60 is 1. Show that the algorithm also gives you that $2 \times 60 - 7 \times 17 = 1$.

2. First make sure you are in the worksheet name '`RSA Decryption`'. Ignore the values in the range H1:H6 for now, these will come into play next week for RSA.

3. First we will calculate how many times the second number goes into the first. In Cell D3, use the INT function to find the value of C1 divided by C2, rounded down.

4. In Cells A3:C3, we now want to take the second number (in Row 2), multiplied by the value in Cell D3, from the first number (in Row 1). E.g., in Cell A3 we would use a formula like `=A1-D3*A2`, except you will need to put in appropriate absolute referencing so that you can copy it across to Cells B3 and C3.

5. Now drag the formulas from A3:D3 down for about ten or twenty rows. Don't worry about `#DIV/0!` errors. If you have done this correctly you should find that the number 1 is in Cell C5 - this is the highest common factor of 60 and 17. Try putting in 112 into Cell C1 and 986 into Cell C2 to see that the highest common factor is 2.

Exercises

1. Use the Euclidean algorithm to find the highest common factor of:

   (a) 24 and 36,

   (b) 56 and 36,

(c) 1200 and 256.

2. Use the extended Euclidean algorithm to find integer solutions to the following equations:

   (a) $24x + 36y = 12$,

   (b) $24x + 36y = 0$,

   (c) $56x + 36y = 4$,

   (d) $56x + 36y = 8$,

   (e) $1200x + 256y = 80$,

   (f) $1200x + 256y = 32$.