The Extended Euclidean Algorithm

As we know from grade school, when we divide one integer by another (nonzero) integer we get an integer *quotient* (the "answer") plus a *remainder* (generally a rational number). For instance,

13/5 = 2 ("the quotient") + 3/5 ("the remainder").

We can rephrase this division, totally in terms of integers, without reference to the division operation:

13 = 2(5) + 3.

Note that this expression is obtained from the one above it by multiplying through by the divisor 5.

We refer to this way of writing a division of integers as the **Division Algorithm for Integers**. More formally stated:

> If a and b are positive integers, there exist integers unique non-negative integers q and r so that
> $$a = qb + r, \text{ where } 0 \leq r < b.$$

q is called the *quotient* and r the *remainder*.

The *greatest common divisor* of integers a and b, denoted by *gcd(a,b)*, is the largest integer that divides (without remainder) both a and b. So, for example:

$$\gcd(15, 5) = 5, \quad \gcd(7, 9) = 1, \quad \gcd(12, 9) = 3, \quad \gcd(81, 57) = 3.$$

The gcd of two integers can be found by repeated application of the division algorithm, this is known as the ***Euclidean Algorithm***. You repeatedly divide the divisor by the remainder until the remainder is 0. The gcd is the last non-zero remainder in this algorithm. The following example shows the algorithm.

Finding the gcd of 81 and 57 by the Euclidean Algorithm:

$$81 = 1(57) + 24$$
$$57 = 2(24) + 9$$
$$24 = 2(9) + 6$$
$$9 = 1(6) + \mathbf{3}$$
$$6 = 2(3) + 0.$$

It is well known that if the gcd(a, b) = r then there exist integers p and s so that:

$$p(a) + s(b) = r.$$

By reversing the steps in the Euclidean Algorithm, it is possible to find these integers p and s. We shall do this with the above example:

Starting with the next to last line, we have:

$$\mathbf{3} = 9 - 1(6)$$

From the line before that, we see that 6 = 24 - 2(9), so:

$$\mathbf{3} = 9 - 1(24 - 2(9)) = 3(9) - 1(24).$$

From the line before that, we have 9 = 57 - 2(24), so:

$$\mathbf{3} = 3(57 - 2(24)) - 1(24) = 3(57) - 7(24).$$

And, from the line before that 24 = 81 - 1(57), giving us:

$$\mathbf{3} = 3(57) - 7(81 - 1(57)) = 10(57) - 7(81).$$

So we have found p = -7 and s = 10.