**3.2 Solving ax + by = d**

We did not use the quotients in the Euclidean algorithm. Here is how we can use them. A very basic fact, proved in the last section, is that, given integers a and b, there are integers x and y such that:

How do we find x and y? Suppose we start by dividing a into b, so , and then proceed as in the Euclidean algorithm. Let the successive quotients be , ,..., so in the first example of Section 3.1., we have qi = 2, q2 = 2, q3 = 4, q4 = 3, qs = 8. Form the following sequences:

Then

In the first example, we have the following calculation:

Similarly, we calculate An easy calculation shows that

Notice that we did not use the final quotient. If we had used it, we would have calculated, which is the original number 1180 divided by the gcd, namely 2. Similarly, is 482/2. The preceding method is often called the extended Euclidean algorithm. It will be used in the next section for solving certain congruences. For small numbers, there is another way to find x and y that does not involve as much book keeping with subscripts. Let's consider the example gcd (12345,11111) = 1 from the previous section. We’ll use the numbers from that calculation. The idea is to work back through the remainders 1, 4, 5, 1234, and the original numbers 11111 and 12345, and eventually obtain the gcd 1 as a combination of 12345 and 11111. From the line that revealed the gcd, we find

So we have 1 as a combination of the previous two remainders. Moving up one line, we write the remainder 4 as a combination of 1234 and 5, then substitute into the preceding equation:

So,

We have now used the last two remainders from the gcd calculation. Write the last unused remainder, namely 5, as a combination of 11111 and 1234, then substitute into the preceding equation:

Finally, we substitute for 1234 to obtain

This yields the gcd 1 as a combination of 12345 and 11111, as desired. As long as the gcd calculation takes only a few steps, this procedure is quite easy to do by hand. But, in general, the previous method is better and adapts well to a computer.