1 The Extended Euclidean Algorithm

The Euclidean Algorithm not only computes greatest common divisors quickly, but also, with only slightly more work, yields a very useful fact: $\gcd(a, b)$ can be expressed as a linear combination of a and b. That is, there exist integers x and y such that $\gcd(a, b) = ax + by$. For example,

$$1 = \gcd(45, 13) = 45 \cdot (-2) + 13 \cdot 7$$
$$7 = \gcd(259, 119) = 259 \cdot 6 - 119 \cdot 13.$$

The **Extended Euclidean Algorithm** will tell us how to find x and y. Rather than give a set of equations, we'll show how it works with the two examples we calclated in Section 3.1.3.

When we computed $\gcd(12345, 11111)$, we did the following calculation:

$$\begin{aligned} 12345 &= 1 \cdot 11111 + 1234 \\ 11111 &= 9 \cdot 1234 + 5 \\ 1234 &= 246 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1. \end{aligned}$$

For the Extended Euclidean Algorithm, we'll form a table with three columns and explain how they arise as we compute them.

We begin by forming two rows and three columns. The first entries in the rows are the original numbers we started with, namely 12345 and 11111. We will do some calculations so that we always have

$$\text{entry in first column } = 12345x + 11111y,$$

where x and y are integers. The first two lines are trivial: $12345 = 1 \cdot 12345 + 0 \cdot 11111$ and $11111 = 0 \cdot 12345 + 1 \cdot 11111$:

	x	y
12345	1	0
11111	0	1

The first line in our gcd(12345, 11111) calculation tells us that $12345 = 1 \cdot 11111 + 1234$. We rewrite this as $1234 = 12345 - 1 \cdot 11111$. Using this, we compute

$$(\text{1st row}) \ - 1 \cdot (\text{2nd row}),$$

yielding the following:

	x	y	
12345	1	0	
11111	0	1	
1234	1	-1	(1st row) $-$ 1$\cdot$(2nd row).

The last line tells us that $1234 = 12345 \cdot 1 + 11111 \cdot (-1)$.

We now move to the second row of our gcd calculation. This says that $11111 = 9 \cdot 1234 + 5$, which we rewrite as $5 = 11111 - 9 \cdot 1234$. This tells us to compute (2nd row) $-9\cdot$(3rd row). We write this as

	x	y	
12345	1	0	
11111	0	1	
1234	1	-1	
5	-9	10	(2nd row) $-9\cdot$(3rd row).

The last line tells us that $5 = 12345 \cdot (-9) + 11111 \cdot 10$.

The third row of our gcd calculation tells us that $4 = 1234 - 246 \cdot 5$. This becomes

	x	y	
12345	1	0	
11111	0	1	
1234	1	-1	
5	-9	10	
4	2215	-2461	(3rd row) $-$ 246$\cdot$(4th row).

Finally, we obtain:

12345	1	0	
11111	0	1	
1234	1	-1	
5	-9	10	
4	2215	-2461	
1	-2224	2471	(4th row) $-$ (5th row).

This tells us that $1 = 12345 \cdot (-2224) + 11111 \cdot 2471$.

Notice that as we proceeded, we were doing the Euclidean Algorithm in the first column. The first entry of each row is a remainder from the gcd calculation, and the entries in the second and third columns allow us to express the number in the first column as a linear combination of 12345 and 11111. The quotients in the Euclidean Algorithm tell us what to multiply a row by before subtracting it from the previous row.

Let's do another example using 482 and 1180 and our previous calculation that $\gcd(1180, 482) = 2$:

	x	y	
1180	1	0	
482	0	1	
216	1	-2	(1st row) $-$ 2·(2nd row)
50	-2	5	(2nd row) $-$ 2·(3rd row)
16	9	-22	(3rd row) $-$ 4·(4th row)
2	-29	71	(4rd row) $-$ 3·(5th row).

The end result is $2 = 1180 \cdot (-29) + 482 \cdot 71$.

To summarize, we state the following.

Theorem 1. *Let a and b be integers with at least one of a, b nonzero. There exist integers x and y, which can be found by the Extended Euclidean Algorithm, such that*

$$\gcd(a, b) = ax + by.$$