Math 408
The Extended GCD Algorithm

Given integers A and B, Euclid's algorithm computes $D = gcd(A, B)$, the greatest common divisor. Using the Extended GCD algorithm, we can also find integers x and y that satisfy the equation $Ax + By = D$. Here is an illustration of the process. Suppose $A = 198061$ and $B = 115948$.

row	N	q	x	y	$Ax + By$
1	198061		1	0	198061
2	115948	1	0	1	115948
3	82113	1	1	-1	82113
4	33835	2	-1	2	33835
5	14443	2	3	-5	14443
6	4949	2	-7	12	4949
7	4545	1	17	-29	4545
8	404	11	-24	41	404
9	101	4	281	-480	101
10	0		-1148	1961	0

In row 1 we see the obvious formula $A \times 1 + B \times 0 = A$.

In row 2 we see the obvious formula $A \times 0 + B \times 1 = B$.

The first step in the Euclidean algorithm is to compute $A = Bq_1 + r_1$. In this case $q = 1$, which is recorded in column 3 of row 2. The remainder r_1 is 82113, which is recorded in column 2 of line 3. We subtract the equation in row 2 from the equation in row 1 to get the new equation $A \times 1 + B \times (-1) = 82113 = r_1$.

Now we repeat the process using $115948 = 82113q_2 + r2$ and find $q_2 = 1$ and $r_2 = 33835$. We can write r_2 as the difference between the previous two expressions:

$$(A \times 0 - B \times 1) - 1(A \times 1 + B \times (-1)) = A \times (-1) + B \times (2) = r_2 = 33835$$

Row 9 gives the formula

$$281 \times A - 480 \times B = 101 = D.$$

Row 10 gives the equation $(-1148)A+(1961)B = 0$. Note that $1148\times 101 = 115948$ and $1961 \times 101 = 198061$. So the last line expresses the formula

$$A \times (-\frac{B}{D}) + B \times \frac{A}{D} = 0.$$

We can add any multiple of the last equation to the previous equation to get combinations of A and B equal to D. The result is the formula:

$$(281 - 1148t)198061 + (1961t - 480)115948 = 101 \quad t = \cdots - 2, -1, 0, 1, 2, \ldots$$