Lecture 1. Material from “Language and Proofs in Algebra: An Introduction”

Extended Euclidean Algorithm (EEA)

Input: Integers a, b with $a \geq b > 0$.

Initialize: Construct a table with four columns so that

- the columns are labelled x, y, r and q,
- the first row in the table is $(1, 0, a, 0)$,
- the second row in the table is $(0, 1, b, 0)$.

Repeat: For $i \geq 3$,

- $q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$
- $\text{Row}_i \leftarrow \text{Row}_{i-2} - q_i \text{Row}_{i-1}$

Stop: When $r_i = 0$.

Output: Set $n = i - 1$. Then $\gcd(a, b) = r_n$, and $s = x_n$ and $t = y_n$ are a certificate of correctness.

Example 11 Let $d = \gcd(2172, 423)$.

1. Apply EEA to compute d and give a certificate of correctness for d.
2. Determine $d_1 = \gcd(423, -2172)$ and give a certificate of correctness for d_1.

Solution:

1.

x	y	r	q
1	0	2172	0
0	1	423	0
1	−5	57	5
−7	36	24	7
15	−77	9	2
−37	190	6	2
52	−267	3	1
−141	724	0	2

From the table constructed by applying EEA above, we have determined that $n = 7$, and $d = \gcd(2172, 423) = r_7 = 3$. The certificate of correctness is $s = x_7 = 52$ and $t = y_7 = -267$, and indeed we check that

$$2172 \times (52) + 423 \times (-267) = 112,944 - 112,941 = 3. \tag{6.7}$$

2. We have $d_1 = \gcd(423, -2172) = \gcd(2172, 423) = 3$, from part 1 above. Our certificate of correctness is $s = -267$ and $t = -52$, since we can rewrite equation (6.7) as

$$423 \times (-267) + (-2172) \times (-52) = 3.$$