

Extended Euclidean Algorithm (EEA)

Input: positive integers r_0 and r_1 with $r_0 > r_1$

Output: $\gcd(r_0, r_1)$, as well as s and t such that $\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$.

Initialization:

$$s_0 = 1 \quad t_0 = 0$$

$$s_1 = 0 \quad t_1 = 1$$

$$i = 1$$

Algorithm:

```
1 DO
  1.1  $i = i + 1$ 
  1.2  $r_i = r_{i-2} \bmod r_{i-1}$ 
  1.3  $q_{i-1} = (r_{i-2} - r_i) / r_{i-1}$ 
  1.4  $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$ 
  1.5  $t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$ 
  WHILE  $r_i \neq 0$ 
2 RETURN
    $\gcd(r_0, r_1) = r_{i-1}$ 
    $s = s_{i-1}$ 
    $t = t_{i-1}$ 
```