

Please reread the L17 slides on Euclid's Algorithm. This homework is entirely practice running Euclid's Algorithm forward and backward as in L17.

For each of the following pairs of natural numbers,  $a, b$ , do the following:

- a. run Euclid's Algorithm to compute  $\gcd(a, b)$ .
- b. run Euclid's Algorithm backwards to compute  $x, y \in \mathbf{Z}$  s.t.  $ax + by = \gcd(a, b)$ .
- c. If  $\gcd(a, b) = 1$ , then compute  $a^{-1} \bmod b$  and  $b^{-1} \bmod a$ . When computing  $c^{-1} \bmod m$ , the answer should be greater than 0 and less than  $m$ .

1. 85, 79
2. 102, 48
3. 222, 163
4. 341, 227
5. 1056, 823