

5 Euclid's Algorithm

Definition 5.1 Let $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the maximal number c such that $a : c$ and $b : c$:

$$\gcd(a, b) = \max\{c \in \mathbb{N} \mid a : c \text{ and } b : c\}$$

Problem 5.1 Suppose $a > b$. Show that $\gcd(a, b) = \gcd(b, a - b)$.

Problem 5.2 Suppose $a : b$. Show that $\gcd(a, b) = b$.

Problem 5.3 Suppose a is *not* divisible by b . Divide a by b to get the remainder r . Show that $\gcd(a, b) = \gcd(b, r)$.

Definition 5.2 Euclid's Algorithm The algorithm for finding gcd is based on Problems 5.2 and 5.3.

Given a pair (a, b) , divide a by b with remainder r . If $r = 0$ then stop: $\gcd(a, b) = b$. If $r > 0$ then replace the pair (a, b) with the pair (b, r) and repeat.

Let $\text{EL}(a, b)$ denote the number of steps in Euclid's algorithm for a pair (a, b) .

Problem 5.4 Find gcd and EL of $(2322, 654)$.

Problem 5.5 Find gcd and EL of $(13471836, 8359848)$.

Problem 5.6 Prove that Euclid's algorithm works, i.e. it always stops and produces $\gcd(a, b)$.

Problem 5.7 Prove that for any $a, b \in \mathbb{N}$ there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. (*Hint*: use induction on $\text{EL}(a, b)$.)

Problem 5.8 Prove that $\gcd(a, b)$ is the least natural number representable in the form $ax + by$ with $x, y \in \mathbb{Z}$.

Problem 5.9 For a perfect breakfast, a math professor decides to boil an egg exactly 15 minutes. He has two hour glasses - one for 7 minutes, another for 11. How should he go about preparing his breakfast? How many times will he have to turn hour glasses? How long will he have to wait for his egg? How is this problem related to gcd?