The Euclidean Algorithm and its Applications

Reading

- Section 4.1
- Section 4.2

Practice Problems

4.1 3, 5, 6, 7, 8
Challenge 4.1 (optional) 10
4.2 1, 2, 3, 6
Challenge 4.2 13, 14
Computer 4.2 (optional) 5

Notes

Euclidean Algorithm

Euclidean algorithm is a stepwise process that starts from two numbers a and b, and produces a series of equations.

In each step, you divide the previous divisor with the previous remainder, like so:

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b$$

$$b = q_1 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = q_1 r_2 + r_3, \quad 0 \leq r_3 < r_2$$

$$r_2 = q_1 r_3 + r_4, \quad 0 \leq r_4 < r_3$$

$$\vdots$$

$$r_{n-1} = q_{n+1} r_n + 0$$

We can be guaranteed that eventually we will end up with a 0 remainder, as the integers r_i keep getting smaller and smaller.

Euclidean Algorithm and GCD

The main relation between the Euclidean algorithm and the greatest common divisor is simple:

> The $\gcd(a, b)$ is the last non-zero remainder in the Euclidean algorithm that starts from a and b.

The proof follows directly from the following lemma:

> If a, b, q, r are integers with $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Let us prove this lemma:

- Any divisor of a and b must also divide $r = a - qb$. (Linear combination lemma)
- Any divisor of b and r must also divide $a = r + qb$.
- So $\gcd(a, b)$ and $\gcd(b, r)$ must divide each other, so must be equal.

The Euclidean algorithm is extremely fast. We will not show this here, but for two numbers a, b the algorithm takes $\log_2(ab)$ steps. Even for 100-digit numbers, this will be no more than around 650 steps, something a computer can handle quickly. Better bounds can be obtained.