3.4 The Euclidean Algorithm

What is the gcd of 82,652 and 178,293?
Well, it does not look easy to find.

There is an algorithm that works quite efficiently.

Theorem 3.11 (The Euclidean Algorithm)

Let $r_0 = a$ and $r_1 = b$ be integers such that $a \geq b > 0$. If the division algorithm is successively applied to obtain $r_j = r_{j+1} q_{j+1} + r_{j+2}$ with $0 < r_{j+2} < r_{j+1}$ for $j = 0, 1, 2, \ldots, n-2$ and $r_{n+1} = 0$, then $\gcd(a,b) = r_n$, the last nonzero remainder.

ex: Let's find $\gcd(324, 126)$.

$$\underbrace{324}_{r_0} = \underbrace{126}_{r_1} \times \underbrace{2}_{q_1} + \underbrace{72}_{r_2}$$

$$\underbrace{126}_{r_1} = \underbrace{72}_{r_2} \times \underbrace{1}_{q_2} + \underbrace{54}_{r_3}$$

$$\underbrace{72}_{r_2} = \underbrace{54}_{r_3} \times \underbrace{1}_{q_3} + \underbrace{18}_{r_4}$$

$$\underbrace{54}_{r_3} = \underbrace{18}_{r_4} \times \underbrace{3}_{q_4} + \underbrace{0}_{r_5}$$

$$\therefore \gcd(324, 126) = 18$$

First we state and prove a lemma.

Lemma 3.3: Let $e, d \in \mathbb{Z}$ s.t. $e = dq + r$. Then, $\gcd(e,d) = \gcd(d,r)$.

Proof: This follows from Theorem 3.7.

Now, we prove Theorem 3.11.

Proof of Theorem 3.11:

By successively applying the division algorithm, we get

$$r_0 = r_1 q_1 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \qquad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n$$

The sequence

$$a = r_0 \geq r_1 > r_2 > r_3 > \cdots \geq 0$$

should end with 0. Then, by Lemma 3.3,

$$(a,b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_n, 0) = r_n$$

Hence the proof.