M1C03 Lecture 28

Greatest common divisors and the Euclidean Algorithm

Jeremy Lane

Nov 22, 2021

Announcement(s)

1. Test 2 Friday
2. No quiz this week

Overview

Reference: Lakins, section 6.2.

The Division Algorithm (positive case)

Let a, b positive integers. Want to find q, r such that $a = bq + r$ and $0 \leq r < b$.

```
1. q <- 0
2. r <- a

while r >= b do:

    3. r <- r - b
    4. q <- q + 1

return q, r
```

Example $a = 924$, $b = 114$.

Definition: An integer a *divides* an integer b if there exists an integer k such that $b = ka$.

Definition: The *greatest common divisor* of two integers a and b is the largest positive integer c such that $c|a$ and $c|b$.

Theorem (Lakins, Lemma 6.2.3)

Let $a, b \in \mathbb{Z}$*,* $a \neq 0$ *and* $b \neq 0$*. If* $q, r \in \mathbb{Z}$ *have the property that* $a = bq + r$*, then*

$$\gcd(a, b) = \gcd(b, r).$$

Proof:

The Euclidean Algorithm

Given positive integers a, b. Assume W.L.O.G. $b < a$. Want to compute $\gcd(a, b)$.

```
while b does not divide a do:

    1. Use the division algorithm to compute q, r
       such that a = b * q + r and 0 <= r < b

    2. a <- b

    3. b <- r

return b
```

Theorem (The Euclidean Algorithm)

The Euclidean algorithm returns $\gcd(a, b)$.

Lakins, Example 6.2.5

Find $\gcd(924, 114)$.

Proof of the Euclidean Algorithm:

Bézout's identity

Theorem

Let a and b be integers not both equal to zero. There exists integers n and m such that

$$\gcd(a, b) = n \cdot a + m \cdot b.$$