

7 GCD, LCM, Division and Euclidean Algorithms

(cf Stein Ch. 3)

Definition 7.1. *Let $A, B \in \mathbb{N}$*

LCM: *The least common multiple of A and B , $LCM(A, B)$, is the smallest M such that $A|M$ and $B|M$.*

GCD: *The greatest common divisor of A and B , $GCD(A, B)$, is the largest D such that $D|A$ and $D|B$.*

Examples (and finding LCM, GCD using Fund. Thm. of Arith.)

Remember the Division Algorithm:

Lemma 7.1. *Suppose a and d are positive integers; then there are unique $k, r \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$*

Proof. ‘Sketch’ in class. □

Lemma 7.2. *Suppose $a, k, d, r \in \mathbb{N}$ and $a = kd + r$. Then $GCD(a, d) = GCD(d, r)$*

Proof. Every common divisor of a and d is also a divisor of $a - kd$ (why?), which is r . Every common divisor of d and r is also a divisor of $kd + r$ (why?), which is a . Thus the largest common divisor of a and d must be the largest common divisor of d and r □

This lemma has remarkable consequences if we iterate the Division Algorithm. For example:

$$100 = (70)(1) + 30$$

$$70 = (30)(2) + 10$$

$$30 = (10)(3) + 0$$

At this point we have to stop, but see:

$$GCD(100, 70) = GCD(70, 30) = GCD(30, 10) = 10$$

This procedure for finding the GCD of two positive integers is called the **Euclidean Algorithm**.