Elementary Number Theory

Daniel Mao

Contents

Chapter 1

Greatest Common Divisor

1.1 Definition

Definition (Greatest Common Divisor)**.** *Let a and b be two integers, not all zero. We define the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, to be the greatest positive integer d that is a divisor of both a and b. i.e., $\exists e, f \in \mathbb{Z}$ such that $a = de$ and $b = df$.*

Proposition 1.1.1.

$$\forall a \in \mathbb{Z}, \quad \gcd(a, 0) = |a|.$$

1.2 Properties

Proposition 1.2.1. *Let A and B be two non-empty, finite sets of integers, not both $\{0\}$. Let $\gcd(A)$ denote the GCD of the elements in A and $\gcd(B)$ denote that of B. Then I claim that*

$$\gcd(A \cup B) = \gcd(\gcd(A), \gcd(B)).$$

Proof. Let a denote the number $\gcd(\gcd(A), \gcd(B))$. Then $a | \gcd(A)$ and $a | \gcd(B)$. Since $\gcd(A)$ is the GCD of elements in A, by definition, it divides all elements in A. Similarly, $\gcd(B)$ divides all elements in B. Since $a | \gcd(A)$ and $\gcd(A)$ divides all elements in A, a divides all elements in A. Similarly, a also divides all elements in B. Since a divides all elements in A and all elements in B, a is a common divisor of elements in $A \cup B$. Let a' be an arbitrary common divisor of elements in $A \cup B$. Since a' divides all elements in $A \cup B$, in particular, a' divides all elements in A. Since a' divides all elements in A and $\gcd(A)$ is the GCD of elements in A, $a' | \gcd(A)$. Similarly, $a' | \gcd(B)$. Since $a' | \gcd(A)$ and $a' | \gcd(B)$, a' is a common divisor of the two numbers $\gcd(A)$ and $\gcd(B)$. Since $a = \gcd(\gcd(A), \gcd(B))$

is the greatest common divisor, $a \geq a'$. That is, any common divisor of elements in $A \cup B$ is $\leq a$. Since a is a common divisor of elements in $A \cup B$ and any common divisor a' is $\leq a$, a is the GCD of $A \cup B$. That is, $a = \gcd(A \cup B)$. That is,

$$\gcd(A \cup B) = \gcd(\gcd(A), \gcd(B)),$$

as claimed. ■