Theorems on the Division of Integers

Theorem (Division Theorem). *For any integer b and any positive integer a, there exist a unique pair of integers (q, r) such that $0 \leq r < a$ and $b = aq + r$.*

Definition (Divisibility Relation). *a divides b, $a|b$, if and only if the division theorem implies $b = aq + r$ where $r = 0$.*

Theorem (Division of a Linear Combination). *If a, b, and c are integers so $c|a$ and $c|b$, then $c|as + bt$ for any integers s and t.*

Definition (GCD). *The greatest common divisor of a and b, $\gcd(a, b) = \max\{d : d \in \mathbb{Z} \text{ and } d|a \text{ and } d|b\}$.*

Theorem (GCD bounds). *For every pair of positive integers (a, b), $1 \leq \gcd(a, b) \leq \min(a, b)$, where $\min(a, b)$ is the minimum of a and b.*

Theorem (GCD Duality Theorem). $\gcd(a, b) = \min\{as + bt : (s, t) \in \mathbb{Z} \times \mathbb{Z}, as + bt > 0\}$

Theorem (GCD--Divisibility distribution law). *$c| \gcd(a, b)$ if and only if ($c|a$ and $c|b$)*

Theorem (GCD remainder theorem). *If $b = aq + r$ where q and r are given by the Division Theorem, then either*

$$r = 0 \text{ and } \gcd(a, b) = a, \quad \text{or} \quad 0 < r \text{ and } \gcd(a, b) = \gcd(a, r).$$

Theorem (Euclid's algorithm theorem). *If you recursively apply the GCD remainder theorem to a pair of integers, one of the two numbers will eventually become 0, and the other will be the GCD of the original two numbers.*

Theorem (Associativity of GCD). *Suppose we have an infinite sequence of positive integers, $a_1, a_2, a_3, \ldots,$*

$$\gcd(a_1 \ldots a_n) = \gcd(\gcd(a_1 \ldots a_{n-1}), a_n).$$

Definition (Relatively Prime). *x and y are relatively prime to each other if and only if $\gcd(x, y) = 1$.*

Theorem (Division with Relative Primes). *(1) If $\gcd(a, b) = 1$ and $a|bc$, then $a|c$. (2) If $\gcd(a, b) = 1$ and $a|c$ and $b|c$, then $ab|c$.*

Definition (Prime). *p is prime if and only if $\{x : x \in \mathbb{N} \text{ and } x|p\} = \{1, p\}$.*

Theorem (Euclid's lemma). *If p is prime and $p|ab$ then $p|a$ or $p|b$.*

Theorem (General Euclid's lemma). *If p is prime and $p| \prod_{k=1}^{n} a_i$, then $p|a_k$ for some k.*

Theorem (Prime Factorization Theorem, Fundamental Theorem of Arithmetic). *Every integer $a \geq 2$ can be written a product of prime numbers*

$$a = \prod_{i=1}^{n} p_i.$$

This product is unique, except for the order of the primes.

Theorem. *There are infinitely many prime numbers.*