MATH 135 - Number Theory Review

Based on *Language and Proofs in Algebra: An Introduction Version 1.3* by *University of Waterloo Faculty of Mathematics*. Sheet created in 2023 by *wkennedy* under fair use for education.

3.4.1 Transitivity of Divisibility (TD)

For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

3.4.2 Divisibility of Integer Combinations (DIC)

For all integers a, b and c, if $a \mid b$ and $a \mid c$, then for all integers x and y, $a \mid (bx + cy)$.

Proof:
Let a, b and c be arbitrary integers, and assume that $a \mid b$ and $a \mid c$.
Since $a \mid b$, there exists an integer r such that $b = ra$.
Since $a \mid c$, there exists an integer s such that $c = sa$.

Let x and y be arbitrary integers. Then $bx + cy$ is also an integer.
Using the assumptions, we have $bx + cy = (ra)x + (sa)y = rax + say = a(rx + sy)$.
Since $rx + sy$ is an integer, it follows from the definition of divisibility that $a \mid (bx + cy)$.

6.1 Division Algorithm (DA)

For all integers a and positive integers b, there exist unique integers q and r such that $a = qb + r$ where $0 \leq r < b$.

6.2 GCD with Remainders (GCD WR)

For all integers a, b, q and r, if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

6.3 GCD Characterization Theorem (GCD CT)

For all integers a and b, and non-negative integers d,
if d is a common divisor of a and b, and there exist integers s and t such that $as + bt = d$,
then $d = \gcd(a, b)$.

6.3 Bézout's Lemma (BL)

For all integers a and b, there exist integers s and t such that $as + bt = d$, where $d = \gcd(a, b)$.

6.4 Extended Euclidean Algorithm (EEA)

yes

6.5 Common Divisor Divides GCD (CDD GCD)

For all integers a, b and c, if $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.

6.5 Coprimeness Characterization Theorem (CCT)

For all integers a and b,
$\gcd(a, b) = 1$ if and only if there exist integers s and t such that $as + bt = 1$.

6.5 Division by the GCD (DB GCD)

For all integers a and b, not both zero, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, where $d = \gcd(a, b)$.

6.5 Coprimeness and Divisibility (CAD)

For all integers a, b and c, if $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

6.6 Prime Factorization (PF)

Every natural number $n > 1$ can be written as a product of primes.

6.6 Euclid's Theorem (ET)

The number of primes is infinite.

6.7 Euclid's Lemma (EL)

For all integers a and b, and prime numbers p, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

6.7 Generalized Euclid's Lemma (Proposition 14) - Note: Not Proved

Let p be a prime number, n be a natural number, and $a_1, a_2, \cdots, a_n$ be integers.
If $p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_n)$, then $p \mid a_i$ for some $i = 1, 2, \cdots, n$.

6.7 Unique Factorization Theorem (UFT) - Fundamental Theorem of Arithmetic

Every natural number $n > 1$ can be written as a product of prime factors uniquely, apart from the order of factors.

6.7 Finding a Prime Factor (FPF)

Every natural number $n > 1$ is either prime or has a prime factor less than or equal to $\sqrt{n}$.

6.8 Divisors From Prime Factorization (DFPF)

Let n and c be positive integers, and
let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$
be a way to express n as a product of the distinct primes $p_1, p_2, \cdots, p_k$
where some or all of the exponents may be zero.

The integer c is a positive divisor of n if and only if c can be represented as a product
$c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, where $0 \leq \beta_i \leq \alpha_i$ for $i = 1, 2, \cdots, k$.

6.8 Number of Divisors - Note: Exercise

The number of positive divisors of an integer n with unique prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is given by the product $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

6.8 GCD From Prime Factorization (GCD PF)

Let a and b be positive integers, and
let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,
and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$
be ways to express a and b as products of the distinct primes $p_1, p_2, \cdots, p_k$,
where some or all of the exponents may be zero.

We have $\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$
where $\gamma_i = \min\{\alpha_i, \beta_i\}$ for $i = 1, 2, \cdots, k$.