Reference for MATH 135 Final Exam, F19

Notation

In MATH 135, we define the natural numbers $\mathbb{N} = \{1, 2, 3, \cdots, \}$ to be the set of positive integers.

List of Propositions

You may use any of the results below without proof. When you do, make sure to clearly state the name (e.g. Transitivity of Divisibility) or the acronym (e.g. TD) associated with the result that you are using.

Transitivity of Divisibility (TD)
For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

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, $a \mid (bx + cy)$.

Pascal's Identity (PI)
For all positive integers n and m with $m \leq n$, we have $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$.

Binomial Theorem (BT)
For all integers $n \geq 0$ and for all complex numbers a and b, $(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^{n-m} b^m$.

Bounds By Divisibility (BBD)
For all integers a and b, if $b \mid a$ and $a \neq 0$ then $b \leq |a|$.

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

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

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

Bézout's Lemma (BL)
For all integers a and b, there exist integers s and t such that $as + bt = d$, where $d = \gcd(a, b)$.

Common Divisor Divides GCD (CDD GCD)
For all integers a, b and c, if $c \mid a$ and $c \mid b$ then $c \mid \gcd(a, b)$.

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 $as + bt = 1$.

Division by the GCD (DB GCD)
For all integers a and b, not both zero, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, where $d = \gcd(a, b)$.

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

Euclid's Lemma (EL)
For all integers a and b, and prime numbers p, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Unique Factorization Theorem (UFT)
Every natural number $n > 1$ can be written as a product of prime factors uniquely, apart from the order of factors.

Divisors From Prime Factorization (DFPF)
Let $n \geq 2$ and $c \geq 1$ be positive integers, and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the unique representation of n as a product of distinct primes $p_1, p_2, \ldots, p_k$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. 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 $i = 1, 2, \ldots, k$.

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 $p_1, p_2, \ldots, p_k$, 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 $i = 1, 2, \ldots, k$.

Linear Diophantine Equation Theorem, Part 1 (LDET 1)
For all integers a, b and c, with a and b not both zero, the linear Diophantine equation $ax + by = c$ (in variables x and y) has an integer solution if and only if $d \mid c$, where $d = \gcd(a, b)$.

Linear Diophantine Equation Theorem, Part 2, (LDET 2)
Let a, b and c be integers with a and b not both zero, and define $d = \gcd(a, b)$. If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + by = c$, then the set of all solutions is given by
$\{(x, y) : x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ n \in \mathbb{Z}\}$.

Congruence Add and Multiply (CAM)
For all positive integers n, if $a_i \equiv b_i \pmod{m}$ for all $1 \leq i \leq n$, then $a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod{m}$, and $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod{m}$.

Congruence Power (CP)
For all positive integers n and integers a and b, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

Congruence Divide (CD)
For all integers a, b and c, if $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Congruent Iff Same Remainder (CISR))
For all integers a and b, $a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

Congruent To Remainder (CTR)
For all integers a and b with $0 \leq b < m$, $a \equiv b \pmod{m}$ if and only if a has remainder b when divided by m.

Linear Congruence Theorem (LCT)
For all integers a and c, with a non-zero, the linear congruence $ax \equiv c \pmod{m}$ has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$. Moreover, if $x = x_0$ is one particular solution to this congruence, then the set of all solutions is given by $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$, or, equivalently, $\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod{m}\}$.

Modular Arithmetic Theorem (MAT)
For all integers a and c, with a non-zero, the equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$. Moreover, when $d \mid c$, there are d solutions, given by $[x_0], \left[x_0 + \frac{m}{d}\right], \left[x_0 + 2\frac{m}{d}\right], \ldots, \left[x_0 + (d-1)\frac{m}{d}\right]$, where $[x] = [x_0]$ is one particular solution.

Inverses in $\mathbb{Z}_m$ (INV $\mathbb{Z}_m$)
Let a be an integer with $1 \leq a \leq m - 1$. The element $[a]$ in $\mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$. Moreover, when $\gcd(a, m) = 1$, the multiplicative inverse is unique.

Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)
For all prime numbers p and non-zero elements $[a]$ in $\mathbb{Z}_p$, the multiplicative inverse $[a]^{-1}$ exists and is unique.

Fermat's Little Theorem (FℓT)
For all prime numbers p and integers a not divisible by p, we have $a^{p-1} \equiv 1 \pmod{p}$.

Corollary of Fermat's Little Theorem (Corollary of FℓT)
For all prime numbers p and integers a, we have $a^p \equiv a \pmod{p}$.

Chinese Remainder Theorem (CRT)
For all integers a_1 and a_2, and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

have a unique solution modulo $m_1 m_2$. Thus, if $n = n_0$ is one particular solution, then the solutions are given by the set of all integers n such that $n \equiv n_0 \pmod{m_1 m_2}$.

Splitting Modulus Theorem (SMT)
For all integers a and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$, then the simultaneous congruences

$$\begin{aligned} n &\equiv a \pmod{m_1} \\ n &\equiv a \pmod{m_2} \end{aligned}$$

have exactly the same solutions as the single congruence $n \equiv a \pmod{m_1 m_2}$.

Properties of Conjugate (PCJ)
For the complex conjugate, the following properties hold for all $z, w \in \mathbb{C}$:

1. $\overline{(\overline{z})} = z$
2. $\overline{z + w} = \overline{z} + \overline{w}$
3. $z + \overline{z} = 2\,\mathrm{Re}(z) \quad$ and $\quad z - \overline{z} = 2\,\mathrm{Im}(z)\,i$
4. $\overline{z\,w} = \overline{z}\,\overline{w}$
5. If $z \neq 0$, then $\overline{(z^{-1})} = (\overline{z})^{-1}$.

Triangle Inequality (TIQ)
For all $z, w \in \mathbb{C}$, we have $\quad |z + w| \leq |z| + |w|$.

Properties of Modulus (PM)
For the modulus, the following properties hold for all $z, w \in \mathbb{C}$:

1. $|z| = 0$ if and only if $z = 0$
2. $|\overline{z}| = |z|$
3. $\overline{z}\,z = |z|^2$
4. $|z\,w| = |z|\,|w|$
5. If $z \neq 0$, then $|z^{-1}| = |z|^{-1}$.

Polar Multiplication in $\mathbb{C}$ (PM$\mathbb{C}$)
For all complex numbers $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$, we have $z_1 z_2 = r_1 r_2\big(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\big)$.

De Moivre's Theorem (DMT)
For all real numbers θ and integers n, we have $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$.

Complex n-th Roots Theorem (CNRT)
For all complex numbers $a = r(\cos\theta + i\sin\theta)$ and natural numbers n, the complex n-th roots of a are given by
$\sqrt[n]{r}\left(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right), k = 0, 1, 2, \ldots, n-1.$

Quadratic Formula (QF)
For all complex numbers a, b and c, with $a \neq 0$, the solutions to $az^2 + bz + c = 0$ are given by $z = \frac{-b \pm w}{2a}$, where w is a solution to $w^2 = b^2 - 4ac$.

Degree of a Product (DP)
For all fields $\mathbb{F}$, and all non-zero polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, we have $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

Division Algorithm for Polynomials (DAP)
For all fields $\mathbb{F}$, and all polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$ with $g(x)$ not the zero polynomial, there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$, where $r(x)$ is the zero polynomial, or $\deg r(x) < \deg g(x)$.

Remainder Theorem (RT)
For all fields $\mathbb{F}$, all polynomials $f(x) \in \mathbb{F}[x]$, and all $c \in \mathbb{F}$, the remainder polynomial when $f(x)$ is divided by $x - c$ is the constant polynomial $f(c)$.

Factor Theorem (FT)
For all fields $\mathbb{F}$, all polynomials $f(x) \in \mathbb{F}[x]$, and all $c \in \mathbb{F}$, the linear polynomial $x - c$ is a factor of the polynomial $f(x)$ if and only if $f(c) = 0$ (equivalently, c is a root of the polynomial $f(x)$).

Fundamental Theorem of Algebra (FTA)
For all complex polynomials $f(z)$ with $\deg f(z) \geq 1$, there exists a $z_0 \in \mathbb{C}$ such that $f(z_0) = 0$.

Complex Polynomials of Degree n Have n Roots (CPN)
For all integers $n \geq 1$, and all complex polynomials $f(z)$ of degree $n \geq 1$, there exist complex numbers $c \neq 0$ and $c_1, c_2, \ldots, c_n$ such that $f(z) = c(z - c_1)(z - c_2)\cdots(z - c_n)$. Moreover, the roots of $f(z)$ are $c_1, c_2, \ldots, c_n$.

Conjugate Roots Theorem (CJRT)
For all polynomials $f(x)$ with real coefficients, if $c \in \mathbb{C}$ is a root of $f(x)$, then $\overline{c} \in \mathbb{C}$ is a root of $f(x)$.

Real Quadratic Factors (RQF)
For all polynomials $f(x)$ with real coefficients, if $c \in \mathbb{C}$ is a root of $f(x)$, and $\mathrm{Im}(c) \neq 0$, then there exists a real quadratic polynomial $g(x)$ and a real polynomial $q(x)$ such that $f(x) = g(x)q(x)$. Moreover, the quadratic factor $g(x)$ is irreducible in $\mathbb{R}[x]$.

Real Factors of Real Polynomials (RFRP)
For all real polynomials $f(x)$ of positive degree, $f(x)$ can be written as a product of real linear and real quadratic factors.

Rational Roots Theorem (RRT)
For all polynomials $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ with integer coefficients and $n \geq 1$, if $\frac{p}{q}$ is a rational root of $f(x)$ with $\gcd(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.