Provided Reference for the Fall 2015 MATH 135 Final Exam

(You do not need to submit this page with your exam.)

A Note About Natural Numbers

Recall that for Math 135, we are using the notation $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ to denote the set of positive integers. This may be different from your CS course, where the set of natural numbers is often said to include zero as well.

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.

Note that some of the statements below are abbreviated versions of the formal propositions in the course notes.

Transitivity of Divisibility (TD)
Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Divisibility of Integer Combinations (DIC)
Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then for all $x, y \in \mathbb{Z}$, $a \mid (bx + cy)$.

Bounds by Divisibility (BBD)
Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Division Algorithm (DA)
If $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then there exist unique integers q and r such that $a = qb + r$ where $0 \leq r < b$.

GCD With Remainders (GCD WR)
Let $a, b, q, r \in \mathbb{Z}$. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

GCD Characterization Theorem (GCD CT)
Let $a, b \in \mathbb{Z}$. If d is a positive common divisor of a and b, and $ax + by = d$ has an integer solution, then $d = \gcd(a, b)$.

Extended Euclidean Algorithm (EEA) (known as Bézout's Lemma outside of MATH 135)
Let $a, b \in \mathbb{Z}$. If $d = \gcd(a, b)$, then d can be computed and there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.

Coprimeness and Divisibility (CAD)
Let $a, b, c \in \mathbb{Z}$. If $c \mid ab$ and a, c are coprime, then $c \mid b$.

Primes and Divisibility (PAD) (known as Euclid's Lemma outside of MATH 135)
If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

GCD of One (GCD OO)
Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there exist integers x and y with $ax + by = 1$.

Division by GCD (DB GCD)
Let $a, b \in \mathbb{Z}$, not both 0. If $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Infinitely Many Primes (INF P) (known as Euclid's Theorem outside of MATH 135)
The number of primes is infinite.

Fundamental Theorem of Arithmetic (UFT)
Every integer greater than 1 can be uniquely expressed as a product of primes (apart from the order of the factors).

Divisors from Prime Factorization (DFPF)
If x can be written as $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ where $p_1, p_2, \ldots, p_n$ are distinct primes and each a_i is a natural number, then d is a positive divisor of x if and only if d can be written as $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ where $0 \leq d_i \leq a_i$ for each i.

GCD from Prime Factorization (GCD PF)
If a can be written as $p_1^{a_1}\cdots p_k^{a_k}$ and b can be written as $p_1^{b_1}\cdots p_k^{b_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and each a_i and b_i is a non-negative integer, then $\gcd(a,b) = p_1^{d_1}\cdots p_k^{d_k}$ where $d_i = \min\{a_i, b_i\}$ for each i.

Linear Diophantine Equation Theorem Part 1 (LDET 1)
Let $a, b, c \in \mathbb{Z}$ and $d = \gcd(a,b)$. The linear Diophantine equation $ax + by = c$ has an integer solution if and only if $d \mid c$.

Linear Diophantine Equation Theorem Part 2 (LDET 2)
Let $a, b, c \in \mathbb{Z}$ and $d = \gcd(a,b) \neq 0$. If (x_0, y_0) is one particular integer solution to $ax + by = c$, then the complete set of integer solutions is

$$\left\{\left(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n\right) : \ n \in \mathbb{Z}\right\}.$$

Congruence is an Equivalence Relation (CER)
Let $m \in \mathbb{N}$, and $a, b, c \in \mathbb{Z}$. Then each of the following statements are true.

1. $a \equiv a \pmod{m}$.
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Properties of Congruence (PC)
If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then $a + b \equiv a' + b' \pmod{m}$, $a - b \equiv a' - b' \pmod{m}$, and $a \cdot b \equiv a' \cdot b' \pmod{m}$.

Congruences and Division (CD)
If $ac \equiv bc \pmod{m}$ and $\gcd(m,c) = 1$, then $a \equiv b \pmod{m}$.

Congruent Iff Same Remainder (CISR)
Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Then $a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

Linear Congruence Theorem 1 (LCT 1)
Let $\gcd(a,m) = d \geq 1$. The linear congruence $ax \equiv c \pmod{m}$ has a solution if and only if $d \mid c$.
Moreover, if x_0 is one solution, then the complete solution is $x \equiv x_0 \pmod{\frac{m}{d}}$.
Equivalently, $x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod{m}$.

Linear Congruence Theorem 2 (LCT 2)
Let $\gcd(a,m) = d \geq 1$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x_0]$ is one solution, then the complete solution in $\mathbb{Z}_m$ is

$$\left\{[x_0], [x_0 + \frac{m}{d}], \cdots, [x_0 + (d-1)\frac{m}{d}]\right\}.$$

Fermat's Little Theorem (FlT)
Let $a \in \mathbb{Z}$. If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Existence of Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)
Let p be a prime number. If $[a]$ is any non-zero element in $\mathbb{Z}_p$, then $[a]^{-1}$ exists.

Chinese Remainder Theorem (CRT)
If $\gcd(m_1, m_2) = 1$, then for any choice of $a_1, a_2 \in \mathbb{Z}$, there exists a solution to the simultaneous congruences

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

Moreover, if n_0 is one solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2}$.

Splitting the Modulus (SM)
Let m_1 and m_2 be coprime positive integers. Then for any two integers x and a,

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases} \text{(simultaneously)} \iff x \equiv a \pmod{m_1 m_2}.$$

RSA Theorem (RSA)
Let p and q be two distinct primes. If we define the following variables

1. $n = pq$ and $\phi(n) = (p-1)(q-1)$, and
2. e is a positive integer, $2 \leq e < \phi(n)$, such that $\gcd(e, \phi(n)) = 1$, and
3. d is a positive integer, $2 \leq d < \phi(n)$, such that $ed \equiv 1 \pmod{\phi(n)}$, and
4. M is an integer such that $0 \leq M < n$, and
5. C is an integer, $0 \leq C < n$, such that $C \equiv M^e \pmod{n}$, and
6. R is an integer, $0 \leq R < n$, such that $R \equiv C^d \pmod{n}$,

then $R = M$.

Properties of Conjugates (PCJ)
If z and w are complex numbers, then

1. $\overline{z + w} = \overline{z} + \overline{w}$.
2. $\overline{zw} = \overline{z}\,\overline{w}$.
3. $\overline{\overline{z}} = z$.
4. $z + \overline{z} = 2\mathrm{Re}(z)$.
5. $z - \overline{z} = 2i\mathrm{Im}(z)$.

Properties of Modulus (PM)
If z and w are complex numbers, then

1. $|z| = 0$ if and only if $z = 0$.
2. $|\bar{z}| = |z|$.
3. $|z|^2 = z\bar{z}$.
4. $|zw| = |z|\,|w|$.
5. $|z + w| \leq |z| + |w|$.

Polar Multiplication of Complex Numbers (PMCN)
If $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$ are complex numbers in polar form, then $z_1 z_2 = r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$.

De Moivre's Theorem (DMT)
For any $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$.

Properties of Complex Exponentials (PCE)
If θ and ϕ are real numbers, then

$$e^{i\theta}\cdot e^{i\phi} = e^{i(\theta+\phi)}$$
$$\left(e^{i\theta}\right)^n = e^{in\theta} \qquad \forall n \in \mathbb{Z}$$

Complex n-th Roots Theorem (CNRT)
If $a = r(\cos\theta + i\sin\theta)$, then the solutions to $z^n = a$ are $\sqrt[n]{r}\left[\cos\frac{\theta+2k\pi}{n} + i\sin\frac{\theta+2k\pi}{n}\right], \quad k = 0, 1, \ldots, n-1$.

Division Algorithm for Polynomials (DAP)
If $f(x), g(x) \in \mathbb{F}[x]$ and $g(x)$ is not the zero polynomial, then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg(r(x)) < \deg(g(x))$ or $r(x)$ is the zero polynomial.

Fundamental Theorem of Algebra (FTA)
For all complex polynomials $f(x)$ with $\deg(f(x)) \geq 1$, there exists $x_0 \in \mathbb{C}$ such that $f(x_0) = 0$.

Remainder Theorem, (RT)
The remainder when a polynomial $f(x)$ is divided by $(x-c)$ is $f(c)$.

Factor Theorem (FT)
The linear polynomial $(x-c)$ is a factor of the polynomial $f(x)$ if and only if $f(c) = 0$.

Complex Polynomials of Degree n Have n Roots (CPN)
If $f(z)$ is a complex polynomial of degree $n \geq 1$, then $f(z)$ has n roots $c_1, c_2, \ldots, c_n \in \mathbb{C}$ and can be written as $c(z-c_1)(z-c_2)\cdots(z-c_n)$ for some $c \in \mathbb{C}$.

Rational Roots Theorem (RRT)
Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ where $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$.
If $\frac{p}{q}$ is a root of $f(x)$ with $p, q \in \mathbb{Z}$ and $\gcd(p,q) = 1$, then $p \mid a_0$ and $q \mid a_n$.

Conjugate Roots Theorem (CJRT)
Let $f(x) \in \mathbb{R}[x]$. If $c \in \mathbb{C}$ is a root of $f(x)$, then $\overline{c}$ is also a root of $f(x)$.

Real Quadratic Factors (RQF)
Let $f(x) \in \mathbb{R}[x]$. If $c \in \mathbb{C}$, $\mathrm{Im}(c) \neq 0$, is a root of $f(x)$, then there exists a real quadratic factor of $f(x)$ with c as a root.

Real Factors of Real Polynomials (RFRP)
Let $f(x) \in \mathbb{R}[x]$. Then $f(x)$ can be written as a product of real linear and real quadratic factors.