Math 104A: Fall 2012
Running List of Definitions/Theorems/Concepts

Section 1.1: $\mathbb{Z}$, prime integer, Prime Number Theorem

Section 1.2: Binary operation, group, commutative/abelian group, group homomorphism, group isomorphism, ring, domain, field, ring homomorphism, ring isomorphism, ordered ring, well-ordered ordered ring, $\mathbb{R}, \mathbb{Q}, \mathbb{N}, \mathbb{C}$, polynomial rings, subgroups, Lagrange's Theorem

Section 1.3/4: Induction, the Division Theorem for $\mathbb{Z}$, Unique Factorization in $\mathbb{Z}$, p-components

Section 2.1: Greatest common divisors in $\mathbb{Z}$, relatively prime integers, Euclidean algorithm

Section 2.2: Prime elements in domains, Euclidean Domains, Unique Factorization Domains, every Euclidean domain is a UFD, greatest common divisors in UFDs and Euclidean domains, $\mathbb{Z}[i]$, $R[x]$ for R a ring.

Section 2.3/4: Linear diophantine equations over $\mathbb{Z}$ in two variables, the least common multiple

Section 3.1: Equivalence relations, equivalence classes, congruence modulo m, the ring $\mathbb{Z}_m$, definition of units, units in $\mathbb{Z}_m$, computing inverses in $\mathbb{Z}_m$.

Section 3.2: Complete residue systems, reduced residue systems, Euler's ϕ-function, explicit formula for $\phi(n)$ using prime factorization, multiplicative functions, Fermat's Little Theorem, Euler's Theorem, $\mathrm{ord}_m(a)$.

Section 3.3: Solving linear equations in $\mathbb{Z}_m$, direct sum of rings, the Chinese Remainder Theorem, solving systems of linear congruences with different moduli, criterion for when a system of linear congruences has at least one solution.

Section 3.4: Failure of unique factorization in $\mathbb{Z}_m[x]$ for m composite, properties of polynomials in $\mathbb{Z}_p[x]$ for p prime (number of roots $\leq$ degree, factorization of $x^p - x$, number of roots of $f(x)$ in $\mathbb{Z}_p$ in terms of greatest common divisors, Wilson's Theorem, Hensel's Lemma, the Legendre symbol, quadratic residues, Euler's Criterion.

Section 4.1: Primitive roots of m, $\mathrm{ord}_m(a^n)$ in terms of $\mathrm{ord}_m(a)$, $\mathrm{ord}_{p^n}(a)$ in terms of $\mathrm{ord}_p(a)$, U_m has a primitive root if and only if $m = 2, 4, p^n, 2p^n$ for $p > 2$ prime, the structure of U_{2^n}.

Section 4.2: The structure of U_m in terms of the prime factorization of m, the index vector.

Section 4.3: n^{th} power residues and non-residues modulo m, characterization of when an element of U_m is an n^{th} power residue if U_m has a primitive root, characterization of when an element of U_{2^e} is an n^{th} power residue.

Section 5.1: Reduction of quadratic residues modulo m to quadratic residues modulo odd primes p.

Section 5.2: Basic properties of the Legendre symbol (Euler's Criterion), Gauss's Lemma, Statement of Quadratic Reciprocity.