Mathematical Reasoning, Chapter 6 Study Guide

Chapter 6. Number Theory.

The following is a *brief* list of topics covered in Chapter 6 of Larry Gerstein's *Introduction to Mathematical Structures and Proofs*, 2nd edition. This list is not meant to be comprehensive, but only gives a list of several important topics.

6.1. Operations.

Binary operation, algebraic structure/binary algebraic structure, commutative, associative, identity element, examples of binary structures (Example 6.3), uniqueness of identity (Theorem 6.4), inverse, uniqueness of inverse (Theorem 6.6), group, ring, commutative ring, field, algebraic comparisons of $\mathbb{N}/\mathbb{Z}/\mathbb{Q}/\mathbb{R}/\mathbb{C}$.

6.2. The Integers: Operations and Order.

Zero divisors, integral domain, interaction between addition and multiplication (Theorem 6.9), trichotomy law, order relation, ordering properties (Theorem 6.12), absolute value function, properties of the absolute value function (Theorem 6.2.A), the Triangle Inequality.

6.3. Divisibility: The Fundamental Theorem of Arithmetic.

"a divides b"/ factor/multiple/proper divisor (Definition 6.13), properties of divisors (Theorem 6.15), prime number, there are infinitely many primes (Eculid; Theorem 6.16), twin primes, Goldbach Conjecture, quotient/divisor/remainder, Division Algorithm (Theorem 6.17), greatest common divisor, existence and uniqueness of a greatest common divisor (Theorem 6.20), Euclid's Algorithm for the computation of a greatest common divisor (Note 6.23, Examples 6.24 and 6.25), divisibility of products by a prime (Theorem 6.26, Corollaries 6.27 and 6.28), the Fundamental Theorem of Arithmetic (Theorem 6.29), standard factorization of integer n (Corollary 6.30), proof that $\sqrt{2}$ is irrational (Theorem 6.31), using canonical factorizations to find greatest common divisors (Exercise 6.33), least common multiple, using canonical factorizations to find least common multiples (Note 6.3.A), relationship between least common multiples and greatest common divisors (Theorem 6.35).

6.4. Congruence; Divisibility Tests.

Congruence modulo m and modulus (Definition 6.37), application of congruence and "clock arithmetic" (Example 6.40(b), congruence modulo m is an equivalence relation (Theorem 6.41), addition and multiplication properties module m (Theorem 6.42 and Corollary 6.43), decimal representation, sum of decimal digits modulo 9 (Theorem 6.45), Test for Divisibility by 9 (Corollary 6.46), Test for Divisiblity by 11 (Theorem 6.48).

6.5. Introduction to Euler's Function.

Relatively prime/coprime integers, Euler φ function or "totient" function, Cancellation Law in congruences (Lemma 6.51), Euler's Theorem (Theorem 6.52), Fermat's Theorem (Corollary 6.53), residue of integer x modulo m/reduction modulo m, application of Fermat's Theorem to test for primality (Example 6.54).

6.6. The Inclusion-Exclusion Principle and Euler's Function.

$|A_1 \cup A_2|$ and $|A_1 \cup A_2 \cup A_3|$ (Note 6.6.A), $|\cup_{i=1}^{n} A_i|$ (Theorem 6.56), the Inclusion-Exclusion Principle (Corollary 6.57) and applications (Example 6.58), formula for $\varphi(n)$ in terms of the standard factorization of n and its proof using the Inclusion-Exclusion Principle (Theorem 6.59), $\varphi(p^k)$ (Corollary 6.60) and application (Example 6.61), $\varphi(n)$ is even for $n > 2$ (Theorem 6.62), $\varphi(n) > \sqrt{n}/2$ (Theorem 6.63), φ is not onto the odd integers (Theorem 6.64), Carmichael's Conjecture, Lehmer's Conjecture.

6.7. More on Prime Numbers.

Fermat numbers and Fermat primes, Pierre de Fermat, Fermat's conjecture concerning the primality of the Fermat numbers and his correspondence related to it, $n = 2^k + 1$ prime requires k is a power of 2 (Theorem 6.66), $F_n - 12 = F_0 F_1 \cdots F_{n-1}$ (Lemma 6.67), Fermat numbers are pairwise relatively prime (Theorem 6.68), the argument using Fermat primes that there are infinitely many primes (Corollary 6.69), analytic number theory, Euler's proof using analytic number theory that there are infinitely many prime numbers (Theorem 6.71).

6.8. Primitive Roots and Card Shuffling.

Reduction mod m, $\mathbb{Z}_m^*$, the binary operation on $\mathbb{Z}_m^*$ and the fact that it is a commutative group (Note 6.8.A), exponential notation and its meaning in $\mathbb{Z}_m^*$ (Note 6.8.C), the order of an integer modulo m, a primitive root modulo m, the order of an element in $\mathbb{Z}_m^*$ divides $\varphi(m)$ (Theorem 6.74), a primitive root mod m "generates" $\mathbb{Z}_m^*$ (Corollary 6.75 and Note 6.8.D), powers of a primitive root

mod m and residues mod m (Proposition 6.77), discrete logarithm (or index) with respect to a primitive root, discrete logarithm of a product (Proposition 6.80), computation of discrete logarithms (Example 6.82), the Primitive Root Theorem (Theorem 6.83), the riffle shuffle (Note 6.8.E), permutation notation, bounds on the order of a riffle shuffle (Note 6.8.F), the order of the riffle shuffle for 52 cards (Example 6.84), classification of when the riffle shuffle on n cars has order $2n$ (Theorem 6.8.A), Artin's conjecture.

6.9. Perfect Numbers, Mersenne Primes, Arithmetic Functions.

Arithmetic function, multiplicative arithmetic function, values of a multiplicative function in terms of the standard factorization (Theorem 6.85), $\sigma(n)$ (Definition 6.87), σ is multiplicative (Theorem 6.89), the value of $\sigma(n)$ in terms of the standard factorization of n (Corollary 6.90), Goldbach's conjecture/its history/Euler's involvement, Goldbach's weak conjecture and the ETSU connection, perfect numbers, the sum of the reciprocals of the divisors of a perfect number is 2 (Remark 6.92), the history of perfect numbers (Euclid's IX.36, Nichomachus, deficient/superabundant numbers, ibn Quarra, ibn Fallus, Regiomontanus, Regius, Cataldi, Mersenne), Mersenne prime, unsolved problems about perfect numbers and Mersenne prime, $2^n - 1$ not prime for composite n (Exercise 6.93), Euclid-Euler Theorem (Theorem 6.94, the converse of Euclid's IX.36), Möbius function, Möbius-Inversion Formula (Theorem 6.97), the use of Möbius inversion to evaluate $\varphi(n)$ (Theorem 6.99), Dirichlet convolution, the Dirichlet convolution of multiplicative functions is multiplicative (Theorem 6.101).

6.10. Number Theory and Cryptography: A Brief Glimpse.

Cryptography versus encoding, plaintext, cryptotext, affine encryption (Example 6.10.A), public key cryptography, RSA cryptosystem and large primes (Example 6.10.B), computationally equivalent, El Gamal system (Example 6.10.C).