TEST 1 GUIDE

18.781 SPRING 2023

Topics in Stillwell, *Elements of Number Theory*.

(1) 1.1, 1.3. Natural numbers and integers.
(2) 1.2. Induction.
(3) 1.4, 2.2. Division with remainder and the Euclidean algorithm.
(4) 2.4. Primes and factorization.
(5) 2.5. Consequences of unique prime factorization.
(6) 2.6. Linear Diophantine equations.
(7) 3.1–3.2. Congruence classes.
(8) 3.3. Invertible congruence classes mod a prime p; groups and subgroups.
(9) 3.4. Fermat's little theorem.
(10) 3.6. Invertible congruence classes in general.
(11) 3.8. Primitive roots.
(12) 9.6–9.7. The (full) Chinese Remainder Theorem.

Know how to...

(1) Use Eratosthenes's sieve to find all primes below a given bound. Recognize the highest prime that needs to be sieved.
(2) State the well-ordering principle.
(3) Use induction to prove a statement for all natural numbers.
(4) Use the Euclidean algorithm to find the gcd of two natural numbers.
(5) List all divisors of a given natural number.
(6) Determine, for fixed integers a, b, c, whether $ax + by = c$ has a solution for x and y in integers.
(7) Add and multiply congruence classes efficiently. Use Fermat's little theorem to calculate exponents efficiently.
(8) List all invertible congruence classes mod m, for small natural numbers m.
(9) Find a primitive root mod p by brute force, for small primes p. Use it to find all other primitive roots mod p.
(10) Determine whether a set together with a binary operation forms a group.
(11) Determine whether a subset of a group defines a subgroup.
(12) Use the Chinese Remainder Theorem to calculate $\varphi(mn)$, *resp.* $\mathrm{ord}_{mn}(a)$, in terms of $\varphi(m), \varphi(n)$, *resp.* $\mathrm{ord}_m(a), \mathrm{ord}_n(a)$, for coprime m, n.

Extra-Hard Problems.

(1) Find all solutions to $252x - 105y = 63$ where x, y are integers.
(2) Verify by brute force that 5 is a primitive root mod 17. Use this fact to find all elements of order 4 in the group of units $(\mathbf{Z}/17\mathbf{Z})^\times$.
(3) List all subgroups of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ under coordinate-wise addition. *Hint:* Chinese Remainder Theorem, additive version.