TEST 2 GUIDE

18.781 SPRING 2023

Topics. In Stillwell, *Elements of Number Theory*:

(1) 5.2–5.4. Brahmagupta's identity, Pell's equation, and $\mathbf{Z}[\sqrt{n}]$ and its norm.
(2) 5.5. The pigeonhole principle.
(3) 5.7–5.8. The Conway map of the quadratic form $x^2 - ny^2$.
(4) 1.6. Pythagorean triples.
(5) 1.7. The geometric classification of Pythagorean triples.
(6) 1.8, 6.1. $\mathbf{Z}[i]$ and its norm.
(7) 6.2. Divisibility and primes in $\mathbf{Z}[i]$.
(8) 6.3. Conjugacy in $\mathbf{Z}[i]$.
(9) 6.4. Long division and unique prime factorization in $\mathbf{Z}[i]$.
(10) 6.5. Fermat's two-squares theorem.
(11) 9.3. Quadratic residues.

Other topics:

(12) Group homomorphisms and isomorphisms.

Know how to...

(1) State, and rederive, Brahmagupta's identity.
(2) Find other integer solutions to $x^2 - ny^2 = 1$, starting from a solution $(x, y) \neq (\pm 1, 0)$.
(3) Calculate the norm of an element of $\mathbf{Z}[\sqrt{n}]$ or $\mathbf{Z}[i]$.
(4) State the pigeonhole principle (see Stillwell page 84).
(5) Draw the Conway map of $x^2 - ny^2$, including its river.
(6) Find all Pythagorean triples (x, y, z) satisfying $x^2 + y^2 = z^2$ with z below a fixed small bound, using their classification.
(7) Factor a small element of $\mathbf{Z}[i]$ into Gaussian primes.
(8) Decide whether a positive prime in $\mathbf{Z}$ stays prime in $\mathbf{Z}[i]$.
(9) Find all quadratic residues modulo p, for a small prime p.
(10) Decide whether -1 is a quadratic residue modulo p, for a large prime p.
(11) Check that a map between groups is a homomorphism or isomorphism.

Hard Problems.

(1) Suppose $(x, y) \in \mathbf{Z}^2$ satisfies $x > 1$ and $y > 0$ and $x^2 - 15y^2 = 1$. Find two other pairs $(x', y'), (x'', y'')$ with these properties, expressing x', y', x'', y'' as polynomials in x, y. Then find actual solutions for (x, y), (x', y'), (x'', y''). *Hint:* Look at powers of $x + y\sqrt{15}$.
(2) Find all Pythagorean triples (x, y, z) with $0 < x < y < z \leq 25$.
(3) Decide which positive prime integers less than 100 remain prime in $\mathbf{Z}[i]$, and factor those that do not into primes of $\mathbf{Z}[i]$.