TEST 3 GUIDE

18.781 SPRING 2023

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

(1) 7.2. $\mathbf{Z}[\sqrt{-2}]$, its norm, and its long division.
(2) 7.4. $\mathbf{Z}[\sqrt{-3}]$ and $\mathbf{Z}[\omega]$ and their norms, where $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. More generally, quadratic integers.
(3) 7.6. Congruences of quadratic integers: *e.g.*, modulo $\sqrt{-3}$ in $\mathbf{Z}[\omega]$.
(4) 7.7. Fermat's Last Theorem for exponent 3.
(5) 9.1. Primes of the form $x^2 + 2y^2$ and $x^2 + 3y^2$, and their relation to $\mathbf{Z}[\sqrt{-2}]$ and $\mathbf{Z}[\omega]$.
(6) 9.2, 9.8. Quadratic reciprocity for odd primes.
(7) 9.3. Euler's criterion for quadratic residues.
(8) 9.4. The formula for $\left(\frac{2}{p}\right)$.

Know how to. . .

(1) Calculate conjugates and norms for quadratic integers in $\mathbf{Z}[\alpha]$, where α satisfies $\alpha^2 + b\alpha + c = 0$ for some integers b, c.
(2) Determine all of the units in $\mathbf{Z}[i]$ or $\mathbf{Z}[\sqrt{-2}]$ or $\mathbf{Z}[\omega]$ (*see below*).
(3) Do congruence arithmetic in $\mathbf{Z}[i]$ or $\mathbf{Z}[\sqrt{-2}]$ or $\mathbf{Z}[\omega]$.
(4) Do long division in $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-2}]$.
(5) Decide whether a small prime in $\mathbf{Z}$ stays prime in $\mathbf{Z}[\sqrt{-2}]$ or $\mathbf{Z}[\omega]$.
(6) Give an example of the failure of uniqueness of prime factorization in $\mathbf{Z}[\sqrt{-3}]$.
(7) State the definition of the Legendre symbol.
(8) State Euler's criterion.
(9) Decide whether an odd prime p is a quadratic residue modulo a prime q.
(10) Decide whether 2 is a quadratic residue modulo a prime q.
(11) For a fixed small prime p, classify all primes q such that p is a quadratic residue modulo q.

Hard Problems.

(1) Show that there are six units in $\mathbf{Z}[\omega]$. Then show that for any integer $n \geq 2$, there are only two units in $\mathbf{Z}[\sqrt{-n}]$. *Hint:* Use norms.
(2) Find all positive prime integers $p < 100$ that split into smaller primes in both $\mathbf{Z}[\sqrt{-2}]$ and $\mathbf{Z}[\omega]$, then explicitly factor the smallest such p. *Hint:* Use Stillwell §9.1. You want a congruence condition modulo $8 \cdot 3 = 24$.
(3) Show that -11 is a quadratic residue modulo an odd (positive) prime p if and only if $p \equiv 0, 1, 3, 4, 5, 9 \pmod{11}$. *Hint:* The formula for $\left(\frac{-1}{p}\right)$ and quadratic reciprocity. *(4/19: Typo fixed)*