PROBLEM SET 5

18.781 SPRING 2023

Due Monday, April 24. You may consult books, papers, and websites as long as you cite them and write up your solutions in your own words. Do not request answers on forums online. To get full points on a proof-based problem, *please write in complete sentences.*

Book. (Stillwell, *Elements of Number Theory*)

(1) 9.1.1–9.1.2
(2) 9.1.3
(3) 9.2.1–9.2.2
(4) 9.2.3
(5) 9.2.5 (assume the prime divisor property for $\mathbf{Z}[\sqrt{3}]$)
(6) 9.4.1–9.4.3
(7) 9.6.3–9.6.4 (read about Sun Zi's problem at the top of page 173)
(8) 9.8.1
(9) 9.8.2–9.8.3
(10) 9.8.4–9.8.5

Non-Book.

Problem 1. Using quadratic reciprocity repeatedly(!), determine whether 781 is a quadratic residue modulo 2027. *Hint:* $781 = 11 \cdot 71$.

Problem 2. Find all invertible quadratic residues modulo 27 and 35, solely by working modulo 3, 5, 7. *(4/23: Typo fixed)*

Problem 3. For each pair of groups below, find a full set of coset representatives for H in G.

(1) $G = \mathbf{Z}[i]$ and $H = (1+i)\mathbf{Z}[i]$, both under addition.
(2) $G = \mathbf{Z}^3$ and $H = \{(x, y, z) \in \mathbf{Z}^3 \mid x + y + z \text{ is even}\}$, both under coordinatewise addition.
(3) $G = (\mathbf{Z}/7\mathbf{Z})^\times$ and $H = \{1 + 7\mathbf{Z}, -1 + 7\mathbf{Z}\}$, both under multiplication.

Hint: (2) is like a three-dimensional version of (1).

Problem 4. Recall that a field is a ring where every nonzero element has an inverse under multiplication. Show that:

(1) $\mathbf{Z}[\omega]/2\mathbf{Z}[\omega]$ is a field. As usual, $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.
(2) $\mathbf{Z}[i]/3\mathbf{Z}[i]$ is a field.
(3) $\mathbf{Z}[i]/2\mathbf{Z}[i]$ is not a field. *Hint:* $(1+i)^2 \equiv 0 \pmod 2$.