PROBLEM SET 3

18.781 SPRING 2023

Due Monday, March 20. 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) 3.6.2–3.6.3
(2) 3.7.1–3.7.4
(3) 5.1.1–5.1.2 (read about "diagonal" and "side numbers")
(4) 5.2.1–5.2.2
(5) 5.3.1–5.3.3 (answer to 5.3.1 in terms of u_k, v_k)
(6) 5.4.1–5.4.2 ($\mathbf{Q}[n]$ is a typo for $\mathbf{Q}[\sqrt{n}]$)
(7) 5.4.4–5.4.5
(8) 5.8.2
(9) 6.1.1–6.1.3
(10) 6.2.2–6.2.4 (in 6.2.3, "a unit" is a typo for "some unit")
(11) 6.3.2–6.3.3
(12) 6.3.4–6.3.6

Non-Book. Throughout, $+$ means coordinate-wise addition where necessary.

Problem 1. Let $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $H = (\mathbf{Z}/12\mathbf{Z})^\times$. Show that:

(1) Any homomorphism from $(G, +)$ into another group is determined by where it sends $(1, 0)$ and $(0, 1)$.
(2) There are sixteen distinct homomorphisms $(G, +) \to (H, \times)$, six of which are isomorphisms.

Problem 2. In each part below, find all $m \in \mathbf{N}$ that satisfy the stated property.

(1) $\varphi(m) = 4$. *Hint:* Use Stillwell Exercise 3.6.3 and the remark below it.
(2) $((\mathbf{Z}/m\mathbf{Z})^\times, \times)$ is isomorphic to $(\mathbf{Z}/4\mathbf{Z}, +)$.
(3) $((\mathbf{Z}/m\mathbf{Z})^\times, \times)$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, +)$.

Problem 3. In the style of Stillwell Figure 5.7, draw (the start of) the maps of the quadratic forms $x^2 - 2y^2$ and $x^2 - 5y^2$. In the style of Figure 5.8, trace out the rivers on both maps. What are the repeating values along the riverbanks, and how long do the sequences take to repeat?

Problem 4. Find all Gaussian primes of norm less than 10, and plot them on the complex plane. *Hint 1:* What are the possible norms? *Hint 2:* If ϖ is a Gaussian prime, then so is $u\varpi$ for $u \in \{\pm 1, \pm i\}$.