PROBLEM SET 4

18.781 SPRING 2023

Due Monday, April 10. 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) 1.6.4
(2) 1.7.1–1.7.4 ("the curve" means $y^2 = x^3 - 2$)
(3) 6.4.1, 6.4.3 (consider negatives)
(4) 6.6.1
(5) 6.6.4–6.6.6
(6) 7.3.1–7.3.4
(7) 7.3.5–7.3.7
(8) 7.4.2
(9) 8.8.5–8.8.8
(10) 9.3.1–9.3.3 (q is prime)

Non-Book. In Problems 4 and 5, let $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Problem 1. For each element $\beta \in \mathbf{Z}[i]$ below, find $\mu, \rho \in \mathbf{Z}[i]$ such that $100 = \mu\beta + \rho$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$.

(1) $\beta = 3 + 2i$.
(2) $\beta = 3 - 2i$.
(3) $\beta = 2 + i$.

Problem 2. Show that no integer congruent to either 3 or 4 modulo 7 can be a sum of two perfect cubes.

Problem 3. The Simpsons episode "The Wizard of Evergreen Terrace" includes the equation

$$3987^{12} + 4365^{12} \stackrel{!}{=} 4472^{12},$$

an apparent counterexample to Fermat's Last Theorem.

(1) Use the fact that 13 divides 4472, along with an actual theorem of Fermat, to disprove the equation.
(2) Why will a handheld calculator appear to verify it?

Problem 4. Find all primes of $\mathbf{Z}[\omega]$ of norm less than 10, and plot them on the complex plane.

Problem 5. Show that any element of $\mathbf{Z}[\omega]$ can be written as $2\mu + \rho$ for some $\mu \in \mathbf{Z}[\omega]$ and $\rho \in \{0, 1, \omega, \omega^2\}$.