Math 104B, Winter 2019

Number Theory II, HW 4

Due Thursday February 7th by 10AM in Shubham Sinha's box.

From Niven, Zuckerman, Montgomery (5th Ed.):

- Problems (Section 9.7, page 431):

  1, 3, 4, 5

- Problems (Section 9.8, page 432):

  1, 2

  `Hint`: Approximate $x + y\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ by $\frac{a+b\sqrt{D}}{2}$ where $a, b \in \mathbb{Z}$ satisfy

$$|b - 2y| \leq \frac{1}{2} \qquad |a - 2x| \leq 1 \qquad a \equiv b (\text{mod } 2).$$

Problem A. From the previous Exercise 2 in Section 9.8 we know $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ has the unique factorization property.

(a) Verify that the units of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ all have the form $\pm\left(\frac{1+\sqrt{5}}{2}\right)^n$ for some exponent $n \in \mathbb{Z}$. (`Hint`: Check that the golden ratio $\frac{1+\sqrt{5}}{2}$ is the smallest unit > 1 by mimicking the argument for $\mathbb{Z}[\sqrt{2}]$ from last weeks homework.)

(b) Let $p \neq 5$ be an odd prime number. Using quadratic reciprocity explain why p **splits** in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ precisely when $p \equiv \pm 1 \pmod 5$.

(c) Similarly find congruence conditions on p modulo 5 describing when p is **inert** in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$; meaning p remains prime.

Problem B. We consider the ring $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ of Kleinian integers.

(a) Adapting earlier arguments (from Section 9.8) show that $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ has a division algorithm and therefore the unique factorization property. What are the units?

(b) Let $p \neq 7$ be an odd prime number. Justify why p **splits** in $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ exactly when $p \equiv 1, 2, 4 \pmod 7$. When is p inert? Factor 7 into irreducible elements.

(c) Find **all** primes p of the form $x^2 + xy + 2y^2$ for suitable $x, y \in \mathbb{Z}$.