HW #1

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, January 23 by 11:59pm on Gradescope.

Question 1. Show that $\mathbb{Z}[\zeta_3]$ is a Euclidean domain, where

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2},$$

is a primitive third root of unity, by exhibiting the division algorithm with[1]

$$N(a+b\zeta_3) = a^2 - ab + b^2.$$

Question 2. Let p be an odd prime, and $a \in \mathbb{Z}$. Using that $\mathbb{F}_p^\times$ is a cyclic group, show that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Question 3. Show that there are no integer solutions to $y^2 = x^3 - 16$. You may start by showing that any hypothetical solution (x, y) should require x, y to be odd.

Question 4. Show that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some integer $d \in \mathbb{Z}$.

Question 5. This exercise aims to prove Fermat's theorem: an odd prime number $p \in \mathbb{N}$ is of the form $p = x^2 + y^2$ for some integers x, y if and only if $p \equiv 1 \pmod{4}$.

(1) Show that $p = x^2 + y^2$ implies that $p \equiv 1 \pmod{4}$.

(2) Conversely, if $p \equiv 1 \pmod{4}$, then we have $\left(\frac{-1}{p}\right) = 1$, so there is an integer n such that $n^2 \equiv -1 \pmod{p}$. This implies that $p | (n^2+1)$.
By using the UFD property of $\mathbb{Z}[i]$, show that p has to be a reducible element in $\mathbb{Z}[i]$.

(3) Show that p being reducible in $\mathbb{Z}[i]$ implies that $p = x^2 + y^2$ for some integers x, y.

[1] Here, this formula comes from

$$N(a+b\zeta_3) = (a+b\zeta_3)(a+b\overline{\zeta_3}),$$

where $\overline{\zeta_3} = \frac{-1-\sqrt{-3}}{2}$.