Math 180B: Homework 6

Submit questions 2, 4 and 6 at the discussion on Thursday 31st May

1. Consider the ring $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Define the norm of $\alpha \in \mathbb{Z}[\sqrt{3}]$ to be

$$N(a + b\sqrt{3}) = a^2 - 3b^2$$

(a) Prove that $N$ is multiplicative: $N(\alpha \beta) = N(\alpha)N(\beta)$.
(b) If $\alpha \in \mathbb{Z}[\sqrt{3}]$ is a unit, prove that $N(\alpha) = 1$. (Hint: first show that $N(\alpha) = \pm 1$ then show that it cannot be $-1$.)
(c) If $N(\alpha) = 1$, show that $\alpha$ is a unit in $\mathbb{Z}[\sqrt{3}]$.
(d) Find six different units in $\mathbb{Z}[\sqrt{3}]$.
(e) Describe all the units in $\mathbb{Z}[\sqrt{3}]$ (recall Pell’s equation…).
(f) Show that for any non-zero $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ there exists $\gamma \in \mathbb{Z}[\sqrt{3}]$ such that

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < 1$$

(It follows that $\mathbb{Z}[\sqrt{3}]$ has a division algorithm, and unique factorization)

2. The ring $\mathbb{Z}[-\sqrt{5}] = \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$, the norm $N(a + bi\sqrt{5}) = a^2 + 5b^2$.

(a) Prove that $\alpha \in \mathbb{Z}[-\sqrt{5}]$ is a unit if and only if $N(\alpha) = 1 \iff \alpha = \pm 1$.
(b) Check that $3 + 2i\sqrt{5}$ divides $85 - 11i\sqrt{5}$.
(c) Prove that 2 is irreducible in $\mathbb{Z}[-\sqrt{5}]$.
(d) Let $\alpha = 11 + 2i\sqrt{5}$ and $\beta = 1 + i\sqrt{5}$. Show that it is not possible to find elements $\gamma, \rho \in \mathbb{Z}[-\sqrt{5}]$ for which

$$\alpha = \beta \gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta)$$

The norm does not define a division algorithm on $\mathbb{Z}[-\sqrt{5}]$.
(e) The irreducible element 2 clearly divides the product

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6$$

Show that 2 does not divide either of the factors $1 \pm i\sqrt{5}$.
(f) Show that the number 6 has two truly different factorizations into irreducible elements of $\mathbb{Z}[-\sqrt{5}]$ by verifying that the numbers in the factorizations

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

are irreducible.
(g) Find another number $\alpha \in \mathbb{Z}[-\sqrt{5}]$ which has two truly different factorisations into two irreducibles.
(h) Can you find any numbers $\beta \in \mathbb{Z}[-\sqrt{5}]$ which have three truly different factorizations into two irreducibles?
3. Let \( \zeta = e^{\frac{2\pi i}{3}} = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \) be a cube root of 1.

(a) Check that \( 1 + \zeta + \zeta^2 = 0 \).

(b) The ring \( \mathbb{Z}[\zeta] \) consists of all elements of the form \( a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + \cdots \) where each \( a_i \in \mathbb{Z} \). Explain why we can write

\[ \mathbb{Z}[\zeta] = \{ a + b\zeta : a, b \in \mathbb{Z} \} = \left\{ \frac{c + d\sqrt{-3}}{2} : c, d \in \mathbb{Z}, c \equiv d \pmod{2} \right\} \]

In particular, what is the relationship between \((a, b)\) and \((c, d)\)?

(c) The standard norm on \( \mathbb{Z}[\zeta] \) is defined by \( N(a) = a\bar{a} \); that is

\[ N\left(\frac{c + d\sqrt{-3}}{2}\right) = \left(\frac{c + d\sqrt{-3}}{2}\right)\left(\frac{c - d\sqrt{-3}}{2}\right) = \frac{1}{4}(c^2 + 3d^2) \]

By definition, \( N(a\beta) = N(a)N(\beta) \) for all \( a, \beta \in \mathbb{Z}[\zeta] \). Prove that \( N(a) \) is an integer and that \( a \in \mathbb{Z}[\zeta] \) is a unit if and only if \( N(a) = 1 \). Deduce that \( \pm 1, \pm \zeta, \pm \zeta^2 \) are the only units in \( \mathbb{Z}[\zeta] \).

(d) What is the expression for the norm in terms of \( a, b \)?

4. In this problem we see that the Eisenstein integers \( \mathbb{Z}[\zeta_3] \) have a Euclidean Algorithm, and thus unique factorization. You should use the norm as defined in the previous question.

(a) Show, given any rational numbers \( r, s \), that one can find integers \( x, y \) such that

\[ \left( r - x - \frac{1}{2}y \right)^2 + 3\left( s - \frac{1}{2}y \right)^2 < 1 \]

\[ \text{Hint: choose } y \text{ to be the integer closest to } 2s \ldots \]

(b) Given \( \alpha, \beta \in \mathbb{Z}[\zeta] \) with \( \beta \neq 0 \), show that the complex number \( \frac{\alpha}{\beta} \) can be written in the form \( r + s\sqrt{-3} \) where \( r, s \in \mathbb{Q} \).

(c) With \( r, s \) as in (b), and with \( x, y \) chosen as in (a), let

\[ \rho = \alpha - \beta \left( x + \frac{1}{2}y + \frac{1}{2}y\sqrt{-3} \right) \]

Prove that \( \delta \in \mathbb{Z}[\zeta] \) and that \( N(\rho) < N(\beta) \).

(d) Deduce that \( \mathbb{Z}[\zeta] \) has a Euclidean Algorithm.

5. In the ring \( \mathbb{Z}[\zeta_5] \), compute the expression \( \lambda \mu = (1 + \zeta_5)(\zeta_5 + \zeta_5^2) \). Explain why all of the powers \( \lambda^n \) are distinct and thus conclude that \( \mathbb{Z}[\zeta_5] \) has infinitely many units.

6. Consider Fermat’s curve \( C \) defined by \( f(x, y) = y^2 - x^3 + 2 = 0 \).

(a) Find the homeogenization \( \bar{C} \) of \( C \) and thus find any ideal points.

(b) Find the equation of the tangent line at the point \((3, 5)\) in two ways:

i. By working directly with \( f \) in \( \mathbb{R}^2 \).
ii. By working with the homogenized polynomial \( F \) in \( \mathbb{R}\mathbb{P}^2 \).

(c) Check that Fermat’s curve is everywhere non-singular, and is therefore elliptic.

(d) Find the equation of the tangent line to the curve at the ideal point.