Math 103B, Winter 2018

Modern Algebra II, HW 6

**Due Friday February 23rd by 5PM in your TA's box**

**From Lauritzen's book**:

- Exercises 3.6 (starting page 138): *29, 30, 31*[1], *33, 38*

**Problem A**. Consider the subring $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$.

(a) Show that $N(a + b\sqrt{-2}) = a^2 + 2b^2$ defines an Euclidean function.

(b) Infer that $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain.

(c) Find a pair of integers $a, b$ such that

$$(3, 2 + \sqrt{-2}) = (a + b\sqrt{-2}).$$

(`Hint`: Run the Euclidean algorithm for $\mathbb{Z}[\sqrt{-2}]$.)

**Problem B**. Suppose $x, y \in \mathbb{Z}$ satisfy the equation $y^2 = x^3 - 1$.

(a) Observe that $x$ must be odd (and therefore $y$ must be even). (`Hint`: If $x$ is even $y^2 \equiv -1 \pmod 8$ but squares are $0, 1, 4$ modulo 8.)

(b) Verify that $y + i$ and $y - i$ are coprime elements of $\mathbb{Z}[i]$. (`Hint`: Suppose a non-unit $d$ divides both, hence their difference $2i = (1 + i)^2$. Deduce that the prime element $1 + i$ divides $d$, and consequently $1 + i$ divides $x$ since

$$(y + i)(y - i) = y^2 + 1 = x^3. \tag{1}$$

Take norms to see that $x$ must then be even, contradicting (a).)

(c) Using that $\mathbb{Z}[i]$ is a unique factorization domain, explain why $y + i$ and $y - i$ are cubes in $\mathbb{Z}[i]$. (`Hint`: The equation (1) shows $y \pm i$ are cubes up to a unit. Note that all elements of $\langle i \rangle$ are cubes by inspection.)

[1]`Hint`: $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 = 2 \cdot 2$ shows 2 is not prime in $\mathbb{Z}[\sqrt{-3}]$. Is 2 irreducible?

(d) Write $y + i = (a + bi)^3$ for suitable $a, b \in \mathbb{Z}$. Expand the right-hand side using the binomial theorem, compare real and imaginary parts, and deduce that $(a, b) = (0, -1)$.

(e) Conclude that $(x, y) = (1, 0)$ is the **only** integer solution to $y^2 = x^3 - 1$.

**Problem C**. Suppose $x, y, z \in \mathbb{Z}$ satisfy the equation $x^3 + y^3 + z^3 = 0$. Here we show that at least one of them must be a multiple[2] of 3. I.e, $xyz \equiv 0 \pmod 3$.

(a) Consider the Eisenstein integers $\mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + i\sqrt{3})$. Show that there is an isomorphism

$$\mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[\omega]/(1 - \omega) \qquad a + 3\mathbb{Z} \mapsto a + (1 - \omega)$$

and deduce that $\pi := 1 - \omega$ is a prime element of $\mathbb{Z}[\omega]$. (cf. 3.6.30(iv).)

(b) Use (a) to show that every element $\gamma \in \mathbb{Z}[\omega]$ is congruent to either 0 or $\pm 1$ modulo $\pi$. In other words $\gamma \equiv 0, \pm 1 \pmod \pi$.

(c) Assuming $\pi \nmid \gamma$ show that $\gamma^3 \equiv \pm 1 \pmod{\pi^4}$. (`Hint`: This is the key step. Replacing $\gamma$ by $-\gamma$ we may assume $\gamma \equiv 1 \pmod \pi$ by part (b). Substitute $\gamma = 1 + \pi x$ in the factorization

$$\gamma^3 - 1 = (\gamma - 1)(\gamma - \omega)(\gamma - \omega^2) \tag{2}$$

to see that $\gamma^3 - 1 = \pi^3 x(x+1)(x - \omega^2)$; this uses the relation $1 - \omega^2 = -\omega^2 \pi$ which you should check. Now use (b) to verify that at least one of the factors in $x(x + 1)(x - \omega^2)$ must be a multiple of $\pi$.)

(d) Suppose $x, y, z$ are all <u>not</u> divisible by 3. View the equation $x^3 + y^3 + z^3 = 0$ modulo $\pi^4$ to get a contradiction. (`Hint`: First note that $\pi \nmid x$ etc., since $3 \sim \pi^2$. Using (c) we obtain $\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{\pi^4}$ for all possible sign combinations. This leads to either $\pm 1 \equiv 0 \pmod{\pi^4}$ – which cannot happen since $\pi$ is not a unit – or $\pm 3 \equiv 0 \pmod{\pi^4}$. The latter cannot happen either since $3 \sim \pi^2$.)

[2] In fact $xyz = 0$ but this requires more work (cf. ”Fermat’s Last Theorem” on p. 137).