Math 261 — Exercise sheet 8

http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html

Version: November 20, 2018

Answers are due for Monday 26 November, 11AM.

The use of calculators is allowed.

Exercise 8.1: How many squares? (20 pts)

1. (10 pts) Find an integer > 2000 which is the sum of 3 squares, but not of 2 squares.
2. (10 pts) Find an integer > 2000 which is the sum of 4 squares, but not of 3 squares.

Exercise 8.2: Bézout in $\mathbb{Z}[i]$ (40 pts)

Compute $\gcd(\alpha, \beta)$, and find $\xi, \eta \in \mathbb{Z}[i]$ such that $\alpha\xi + \beta\eta = \gcd(\alpha, \beta)$, when

1. (20 pts) $\alpha = 4 + 6i$, $\beta = 5 + 3i$,
2. (20 pts) $\alpha = 8 - i$, $\beta = 5 - 2i$.

Exercise 8.3: Factorization in $\mathbb{Z}[i]$ (40 pts)

Factor $29 + 3i$ into irreducibles in $\mathbb{Z}[i]$.

The exercises below are not mandatory. They are not worth any points, and are given here for you to practise. The solutions will be made available with the solutions to the other exercises.

Exercise 8.4: Number of ways

For each of the following $n \in \mathbb{N}$, give the number $N(n)$ of pairs $(x, y) \in \mathbb{Z}^2$ such that $n = x^2 + y^2$, and explain how the elements of $\mathbb{Z}[i]$ of norm n factor.

1. $n = 261$,
2. $n = 2000$,
3. $n = 6000$.

Exercise 8.5: Forcing a common factor

Let $\alpha, \beta \in \mathbb{Z}[i]$.

1. Prove that $N\big(\gcd(\alpha,\beta)\big) \mid \gcd\big(N(\alpha), N(\beta)\big)$.
2. Explain why we can have $N\big(\gcd(\alpha,\beta)\big) < \gcd\big(N(\alpha), N(\beta)\big)$.
3. Suppose now that $\gcd\big(N(\alpha), N(\beta)\big)$ is a prime $p \in \mathbb{N}$. Prove that $p \not\equiv 3 \pmod 4$.
4. Still assuming that that $\gcd\big(N(\alpha), N(\beta)\big)$ is a prime $p \in \mathbb{N}$, prove that either α and β are not coprime, or α and $\bar{\beta}$ are not coprime (or both).
5. Suppose more generally that $\gcd\big(N(\alpha), N(\beta)\big)$ is a integer $n \geqslant 2$, which we no longer assume to be prime. Is it true that either α and β are not coprime, or α and $\bar{\beta}$ are not coprime (or both)? Is it true that at least one of $N\big(\gcd(\alpha,\beta)\big)$ and $N\big(\gcd(\alpha,\bar{\beta})\big)$ is n?

Exercise 8.6: Integers of the form $x^2 + xy + y^2$ (difficult)

Let $\omega = e^{\pi i/3} = \frac{1+i\sqrt{3}}{2} \in \mathbb{C}$, and let $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$. Note that ω satisfies $\omega^2 - \omega + 1 = 0$ and $\omega^6 = 1$.

We define the norm of an element $\alpha \in \mathbb{Z}[\omega]$ by $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$.

1. Check that $\mathbb{Z}[\omega]$ is a domain.
2. Prove that $N(a + b\omega) = a^2 + ab + b^2$. Deduce that the set of integers of the form $x^2 + xy + y^2$, $x, y \in \mathbb{Z}$, is stable under multiplication.
3. Prove that an element of $\mathbb{Z}[\omega]$ is invertible iff. its norm is 1. Deduce that the set of invertibles of $\mathbb{Z}[\omega]$ is
$$\mathbb{Z}[\omega]^\times = \{\omega, \omega^2, \omega^3 = -1, \omega^4, \omega^5, \omega^6 = 1\}.$$
4. Prove that $\mathbb{Z}[\omega]$ is euclidean.
Hint: $\{1, \omega\}$ is an $\mathbb{R}$-basis of $\mathbb{C}$.
5. Deduce that $\mathbb{Z}[\omega]$ is a UFD.
6. Let $p \neq 3$ be a prime. Prove that if $p \neq 2$, then $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, and deduce that the equation $x^2 + x + 1 = 0$ has solutions in $\mathbb{Z}/p\mathbb{Z}$ iff. $p \equiv 1 \pmod 3$.
7. Prove that the primes $p \in \mathbb{N}$ decompose in $\mathbb{Z}[\omega]$ as follows:
   (a) if $p = 3$, then $3 = \omega^5(1 + \omega)^2$ (note that ω^5 is invertible),
   (b) if $p \equiv 1 \pmod 3$, then $p = \pi\bar{\pi}$, where $\pi \in \mathbb{Z}[\omega]$ is irreducible and has norm p,
   (c) if $p \equiv -1 \pmod 3$, then p remains irreducible in $\mathbb{Z}[\omega]$.
   Hint: Prove that if $p = a^2 + ab + b^2$, then at least one of a and b is not divisible by p.

8. What are the irreducibles in $\mathbb{Z}[\omega]$?

9. Deduce from the previous questions that an integer $n \in \mathbb{N}$ is of the form $x^2 + xy + y^2$, $x, y \in \mathbb{Z}$ iff. for all primes $p \equiv -1 \pmod 3$, the p-adic valuation $v_p(n)$ is even.

10. Adapt the previous exercise to find a formula for the number of pairs (x, y), $x, y \in \mathbb{Z}$ such that $x^2 + xy + y^2 = n$ in terms of the factorization of n in $\mathbb{Z}$.