Math 261 — Exercise sheet 6

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: October 23, 2017

Answers are due for Wednesday 01 November, 11AM.

The use of calculators is allowed.

Exercise 6.1: How many squares? (10 pts)

1. Find an integer between 1000 and 2000 which is the sum of 3 squares, but not of 2 squares.
2. Find an integer between 1000 and 2000 which is the sum of 4 squares, but not of 3 squares.

Exercise 6.2: Bézout in $\mathbb{Z}[i]$ (20 pts)

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

1. (10 pts) $\alpha = 4 + 6i$, $\beta = 5 - 3i$,
2. (10 pts) $\alpha = 8 + i$, $\beta = 5 - 2i$.

Exercise 6.3: Factorization in $\mathbb{Z}[i]$ (25 pts)

Factor $19 + 17i$ into irreducibles in $\mathbb{Z}[i]$.

Exercise 6.4: Forcing a common factor (25 pts)

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

1. (5 pts) Prove that $N\big(\gcd(\alpha, \beta)\big) \mid \gcd\big(N(\alpha), N(\beta)\big)$.
2. (5 pts) Explain why we can have $N\big(\gcd(\alpha, \beta)\big) < \gcd\big(N(\alpha), N(\beta)\big)$.
3. (5 pts) 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. (5 pts) 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. (5 pts) 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 6.5: Number of ways to write n as $x^2 + y^2$ (20 pts)

1. Let $p \in \mathbb{N}$ be a prime number, and $a \in \mathbb{N}$ be an integer.

   (a) (3 pts) Prove that if $p \equiv -1 \pmod 4$, then the number of elements of $\mathbb{Z}[i]$ of norm p^a is $\begin{cases} 0, & \text{if } a \text{ is odd,} \\ 4, & \text{if } a \text{ is even.} \end{cases}$

   (b) (5 pts) Prove that if $p \equiv 1 \pmod 4$, then the number of elements of $\mathbb{Z}[i]$ of norm p^a is $4(a+1)$.

   (c) (2 pts) Prove the number of elements of $\mathbb{Z}[i]$ of norm 2^a is 4 for all $a \in \mathbb{N}$.

2. (5 pts) Deduce from the previous questions a formula for the number of ways to write an integer $n \in \mathbb{N}$ as a sum of 2 squares in terms of its factorization $n = \prod_k p_k^{a_k}$ into primes in $\mathbb{Z}$.

3. (5 pts) How many ways are there to write 2000 as a sum of two squares? What about 6000?

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

Exercise 6.6: Integers of the form $x^2 + xy + y^2$

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 a unit iff. its norm is 1. Deduce that the set of units 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 euclidian.

   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 a unit),

(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 $\mathbb{Z}$.