Introduction to number theory
Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22301/index.html

Version: November 4, 2020

Answers are due for Friday November 20th, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Do it before next year! (50pts)*

Find the complete factorisation of $20 + 21i$ in $\mathbb{Z}[i]$.

Exercise 2 *How many ways? (50pts)*

Let $n \in \mathbb{N}$ be an integer. By separating prime factors into different types, we may factor n as

$$n = 2^a \prod_{j=1}^{r} p_j^{b_j} \prod_{k=1}^{s} q_k^{c_k},$$

where the p_j are distinct primes all $\equiv +1 \bmod 4$, the q_k are distinct primes all $\equiv -1 \bmod 4$, and a, the b_j, and the c_k are non-negative integers.

Find (and prove) a formula for the number of pairs (x, y) of $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. NB the order and the signs count, i.e. (x, y), and $(-x, y)$ count as distinct pairs unless $x = 0$, and so does (y, x) unless $x = y$.

Hint: This is the same thing as counting the $\alpha \in \mathbb{Z}[i]$ of norm n. Think in terms of factorisation. You may want to test your formula on small values of n.

These were the only mandatory exercises, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercises.

Exercise 3 *How many squares?*

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

Exercise 4 *The meaning of divisibility*

Let $a, b \in \mathbb{Z}$. We may also view a and b as elements of $\mathbb{Z}[i]$. Write $a \mid_{\mathbb{Z}} b$ if a divides b when we view them as elements of $\mathbb{Z}$, and $a \mid_{\mathbb{Z}[i]} b$ if a divides b when we view them as elements of $\mathbb{Z}[i]$.

Prove that in fact, $a \mid_{\mathbb{Z}} b$ iff. $a \mid_{\mathbb{Z}[i]} b$.

Exercise 5 *Bézout in* $\mathbb{Z}[i]$

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

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

Exercise 6 *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 7 *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 $\omega^3 = -1$.

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 closed under addition, subtraction, and multiplication.
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 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 Euclidean division is possible in $\mathbb{Z}[\omega]$.
Hint: $\{1, \omega\}$ is an $\mathbb{R}$-basis of $\mathbb{C}$.
5. Deduce that we have unique factorisation into irreducibles in $\mathbb{Z}[\omega]$.
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 first 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 $\mathbb{Z}$.