Introduction to number theory
Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU22301/index.html

Version: November 12, 2021

Email your answers to makindeo@tcd.ie by Monday November 22nd, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Bézout in $\mathbb{Z}[i]$ (30 pts)*

Let $\alpha = 4 + 6i$ and $\beta = 5 + 3i$.

1. (15 pts) Compute $\gcd(\alpha, \beta)$.
2. (15 pts) Find $\xi, \eta \in \mathbb{Z}[i]$ such that $\alpha\xi + \beta\eta = \gcd(\alpha, \beta)$.

Solution 1

This is the same principle as in $\mathbb{Z}$: we do euclidean divisions until we get a null remainder, and then we go back up the relations we have found to get ξ and η.

1. Let us first perform a euclidean division of α by β. We have

$$\frac{\alpha}{\beta} = \frac{(4+6i)(5-3i)}{34} = \frac{(2+3i)(5-3i)}{17} = \frac{19+9i}{17} \approx 1+i,$$

so the quotient is $1+i$ and the remainder is $(4+6i)-(5+3i)(1+i) = 2-2i$. We record this relation for later use.

Next, we divide the divisor by the remainder, that is to say $5+3i$ by $2-2i$. We have

$$\frac{5+3i}{2-2i} = \frac{(5+3i)(2+2i)}{8} = \frac{1}{2} + 2i \approx 2i,$$

so our quotient is $2i$ (but we could also take $1+2i$) and the remainder is $(5+3i)-(2-2i)2i = 1-i$. We record this relation for later use.

Next step: divide $2-2i$ by $1-i$. Obviously, this is an exact division, with quotient 2 and remainder 0. This means that $\boxed{\gcd(\alpha,\beta) = 1-i}$ (note that $1-i = -i(1+i)$ is associate to $1+i$, so $1+i$ is also a gcd).

2. Using the relations that we recorded in the previous question, we find

$$1-i = (5+3i)-(2-2i)2i = (5+3i)-\big((4+6i)-(5+3i)(1+i)\big)2i = (5+3i)(-1+2i)-(4+6i)(2i)$$

so we can take $\boxed{\xi = -2i,\ \eta = -1+2i}$.

Exercise 2 *Do it before next year! (35 pts)*

Find the complete factorisation of $21 + 22i$ in $\mathbb{Z}[i]$.

Solution 2

Let $\alpha = 21 + 22i$. We know that it has a factorisation of the form

$$\alpha = u\pi_1 \cdots \pi_r$$

where $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ and the π_j are irreducibles. This means that for each j, π_j is associate to an irreducible π'_j which is either $1+i$, a prime number $\equiv -1 \bmod 4$, or an irreducible of norm a prime number $\equiv +1 \bmod 4$. This $\pi_j = u_j\pi'_j$ for some $u_j \in \mathbb{Z}[i]^\times$; putting u_j into u, we may assume that $\pi_j = \pi'_j$ is of the above form.

We compute that

$$N(\alpha) = 21^2 + 22^2 = 925 = 5^2 \times 37.$$

Since 5 and 37 are primes $\equiv +1 \bmod 4$, this means that our factorisation actually has the shape

$$\alpha = u\pi_1\pi_2\pi_3$$

where $u \in \mathbb{Z}[i]^\times$, $N(\pi_1) = N(\pi_2) = 5$, and $N(\pi_3) = 37$.

As $5 \equiv +1 \bmod 4$, there exists an irreducible $\pi \in \mathbb{Z}[i]$ such that $5 = \pi\overline{\pi}$, and π_1 and π_2 are associate with π or $\overline{\pi}$. As $5 = 2^2 + 1^2$, we can take $\pi = 2 + i$. We compute that

$$\frac{\alpha}{\pi} = \frac{(21 + 22i)(2 - i)}{(2 + i)(2 - i)} = \frac{64}{5} + \frac{23}{5}i \notin \mathbb{Z}[i];$$

this shows that $\pi \nmid \alpha$, so neither π_1 nor π_2 can be associate with π, so both must be associate to $\overline{\pi} = 2 - i$. Changing u if necessary, we may thus assume that $\pi_1 = \pi_2 = 2 - i$.

We are then left with

$$u\pi_3 = \frac{\alpha}{(2 - i)^2} = \frac{20 + 21i}{3 - 4i} = \frac{(20 + 21i)(3 + 4i)}{(3 - 4i)(3 + 4i)} = -1 + 6i.$$

This has norm $(-1)^2 + 6^2 = 37$ (as predicted) which is prime, so it is irreducible (note that we already knew that, since associates to irreducibles are irreducible); in conclusion, we have the complete factorisation

$$21 + 22i = (2 - i)^2(-1 + 6i).$$

Personally, I prefer to pull the unit i out of $-1 + 6i = i(6 + i)$, and write

$$21 + 22i = i(2 - i)^2(6 + i).$$

Exercise 3 *Twice a sum of two squares (35 pts)*

Let $n \in \mathbb{N}$. Prove that if n is a sum of two squares, then so is $2n$.
Your proof must be constructive, meaning that given $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$, it must explain how to find $c, d \in \mathbb{Z}$ such that $2n = c^2 + d^2$.
Hint: $1 + i$.

Solution 3

Let $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$. Then $n = N(\alpha)$, where $\alpha = a + bi \in \mathbb{Z}[i]$. We would like to find $\beta \in \mathbb{Z}[i]$ such that $N(\beta) = 2n$. By multiplicativity of the norm, if $\gamma \in \mathbb{Z}[i]$ is such that $N(\gamma) = 2$, then we can take $\beta = \gamma\alpha$. And we know that $N(1+i) = 2$, so we take $\beta = (1+i)\alpha = (1+i)(a+bi) = (a-b) + (a+b)i$. We thus find that $2n = c^2 + d^2$ where $c = a - b$, $d = a + b$.

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 4 *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.

Solution 4

1. We know that if there is a prime $p \equiv -1 \pmod 4$ such that $p \mid n$ but $p^2 \nmid n$, then n won't be a sum of 2 squares. So let us take $p = 3$ for instance. We can take $n = 2001$: since the sum of digits is 3, $3 \mid n$ but $9 \nmid n$, so n is not a sum of 2 squares.

   Besides, if we had $n = 4^a(8b + 7)$, then necessarily $a = 0$ since n is odd. But $n \equiv 1 \not\equiv 7 \pmod 8$, so n is not of the form $4^a(8b + 7)$. As a result, n is a sum of 3 squares.

2. Since every integer is a sum of 4 squares, it suffices to take an n of the form $4^a(8b + 7)$ for any a and b. We can go the easy way and take $a = 0$, so we just need $n \equiv 7 \pmod 8$. So for instance $n = 2007$ works.

Exercise 5 *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. $a \mid_{\mathbb{Z}[i]} b$.

Solution 5

We prove both implications.

First of all, if $a \mid_{\mathbb{Z}} b$, then $b = ac$ for some $c \in \mathbb{Z}$. Thus $c \in \mathbb{Z}[i]$, so $a \mid_{\mathbb{Z}[i]} b$.

Conversely, suppose that $a \mid_{\mathbb{Z}[i]} b$. This means that $b = a\gamma$ for some $\gamma \in \mathbb{Z}[i]$. We now distinguish two cases. If $a \neq 0$, then we have $\gamma = b/a \in \mathbb{Q}$, so $\gamma \in \mathbb{Z}[i] \cap \mathbb{Q} = \mathbb{Z}$, which proves that $a \mid_{\mathbb{Z}} b$. And if $a = 0$, then $b = a\gamma = 0$ as well, so again $a \mid_{\mathbb{Z}} b$ since $b = ac$ for one, and in fact any, $c \in \mathbb{Z}$.

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?

Solution 6

1. Since the norm is multiplicative, we know that if $\delta \mid \alpha$ then $N(\delta) \mid N(\alpha)$. As a result, if $\delta \mid \alpha$ and $\delta \mid \beta$, then $N(\delta) \mid N(\alpha)$ and $N(\delta) \mid N(\beta)$, so $N(\delta) \mid \gcd\big(N(\alpha), N(\beta)\big)$. This applies in particular to $\delta = \gcd(\alpha, \beta)$, whence the result.

2. Let p be a prime such that $p \equiv 1 \pmod 4$, for instance $p = 5$. Then we know that in $\mathbb{Z}[i]$, p decomposes as $p = \pi\bar{\pi}$, where π and $\bar{\pi}$ are both irreducible of norm p and are not associate to each other. Let us take $\alpha = \pi$, $\beta = \bar{\pi}$. Then since they are irreducible and not associate to each other, they are coprime, so $N\big(\gcd(\alpha, \beta)\big) = 1$, even though $\gcd\big(N(\alpha), N(\beta)\big) = \gcd(p, p) = p$.

3. From $\gcd\big(N(\alpha), N(\beta)\big) = p$, we infer that possibly after swapping α and β we must have $p \mid N(\alpha)$ but $p^2 \nmid N(\alpha)$. By considering the factorization of α in $\mathbb{Z}[i]$, we deduce that α is divisible by an irreducible π of norm p. No such irreducible exists if $p \equiv -1 \pmod 4$, whence the result.

4. We have $p \mid N(\alpha)$, so α must be divisible by an irreducible π dividing p in $\mathbb{Z}[i]$. Similarly, there is an irreducible $\pi' \mid p$ such that $\pi' \mid \beta$. But if $p = 2$, then there is only one $\pi \mid p$ up to invertibles, so π' must be associate to π so that π divides both α and β, whereas if $p \equiv 1 \pmod 4$ (which is the only other possible case by the previous question), then π' is associate either ot π, in which case π divides both α and β again, or to $\bar{\pi}$, in which case π divides both α and $\bar{\beta}$.

5. Let $p \mid n$ be a prime. Then we have again $p \mid N(\alpha)$ and $p \mid N(\beta)$, so as in the previous question we find an irreducible of norm p which divides both α and either β or $\bar{\beta}$ (or both), so the answer to the first question is yes.

   However, the answer to the second question is no. Consider for instance two distinct primes $\ell, p \in \mathbb{N}$ which are both $\equiv 1 \pmod 4$, so that they decompose as $\ell = \lambda\bar{\lambda}$, $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$, and the irreducibles $\lambda, \bar{\lambda}, \pi, \bar{\pi}$ are pairwise coprime, and take $\alpha = \lambda\pi$, $\beta = \lambda\bar{\pi}$, so that $\bar{\beta} = \bar{\lambda}\pi$. Then we have $N(\alpha) = N(\beta) = \ell p$, so that $\gcd\big(N(\alpha), N(\beta)\big) = \ell p$, but $\gcd(\alpha, \beta) = \lambda$ and $\gcd(\alpha, \bar{\beta}) = \pi$ both have norm $< \ell p$ (ℓ for the former, p for the latter).

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. 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 $\mathbb{Z}$.

Solution 7

1. It is clear that $\mathbb{Z}[\omega]$ is stable under addition and subtraction, and for multiplication we have

   $$(a+b\omega)(c+d\omega) = ac+(ad+bc)\omega+bd(\omega-1) = (ac-bd)+(ad+bc+bd)\omega$$

   since $\omega^2 = \omega - 1$, so $\mathbb{Z}[\omega]$ is a ring. Besides, the product of 2 nonzero complexes is nonzero, so $\mathbb{Z}[\omega]$ is indeed a domain.

2. Since $\omega \in \mathbb{C} \setminus \mathbb{R}$, the complex roots of the polynomial x^2-x+1 are ω and $\bar{\omega}$, so we have $\omega+\bar{\omega} = 1$ and $\omega\bar{\omega} = 1$. Therefore,

   $$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) = a^2+ab(\omega+\bar{\omega})+b^2\omega\bar{\omega} = a^2+ab+b^2.$$

   Besides, since clearly $N(\alpha\beta) = N(\alpha)N(\beta)$, we deduce that the set of integers of the form a^2+ab+b^2, $a,b \in \mathbb{Z}$, is stable under multiplication.

3. If α is invertible, then $N(\alpha)N(\alpha^{-1}) = N(1) = 1$, whence $N(\alpha) = 1$ since norms are positive integers. Conversely, if $N(\alpha) = 1$, then α is invertible of inverse $\bar{\alpha}$. Therefore, the invertibles are the $a+b\omega$ with $a^2+ab+b^2 = 1$. From

$$a^2 + ab + b^2 = (a + b/2)^2 + \frac{3}{4}b^2$$

we see that $|b| \leqslant 1$.

For $b = -1$, we must have $a = 0$ or 1, for $b = 0$, we must have $a = \pm 1$, and for $b = 1$, we must have $a = 0$ or -1, so there are exactly 6 invertibles. But ω is invertible since $1 = \omega\bar{\omega} = \omega(1-\omega)$, so all powers of ω are a also invertibles, and since $\omega = e^{\pi i/3}$, the sequence of powers of ω is periodic of period exactly 6, so all 6 invertibles show up this way.

4. Observe first that if we extend the norm to all of $\mathbb{C}$ by setting $N(z) = z\bar{z}$, we have

$$N(\lambda + \mu\omega) = \lambda^2 + \lambda\mu + \mu^2 \quad (\star)$$

for all $\lambda, \mu \in \mathbb{R}$.

Let now $\alpha, \beta \in \mathbb{Z}[\omega]$, $\beta \neq 0$; we want to show that there exist $\gamma, \rho \in \mathbb{Z}[\omega]$ with $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$.

We have $\alpha/\beta \in \mathbb{C}$, so since $\{1, \omega\}$ is an $\mathbb{R}$-basis of $\mathbb{C}$ there are $\lambda, \mu \in \mathbb{R}$ such that $\alpha/\beta = \lambda + \mu\omega$. Let $l, m \in \mathbb{Z}$ be such that $|l - \lambda| \leqslant \frac{1}{2}$ and $|m - \mu| \leqslant \frac{1}{2}$, and let $\gamma = l + m\omega \in \mathbb{Z}[\omega]$ and $\rho = \alpha - \beta\gamma \in \mathbb{Z}[\omega]$. Then $N(\frac{\alpha}{\beta} - \gamma) \leqslant \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$ by $(\star)$, so

$$N(\rho) = N(\alpha - \beta\gamma) = N(\frac{\alpha}{\beta} - \gamma)N(\beta) \leqslant \frac{3}{4}N(\beta) < N(\beta).$$

5. The proof is the same as for $\mathbb{Z}$ and $\mathbb{Z}[i]$: now that we have euclidian division available, we can prove Bézout, and deduce Gauss's and Euclid's lemmas, and then the uniqueness of factorization from there.

6. (Compare with exercise 4 of the previous sheet) Suppose first that $p \neq 2, 3$. The we have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{p'}(-1)^{\frac{3-1}{2}p'}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

which is $+1$ if $p \equiv 1 \pmod 3$, and -1 if $p \equiv -1 \pmod 3$. Now, the discriminant of $x^2 + x + 1$ is -3, so we see that this polynomial has 2 roots mod p if $p \equiv 1 \pmod 3$, and none if $p \equiv -1 \pmod 3$. Also, it has no roots mod 2, so the conclusion is also true for $p = 2$.

7. (a) Checking that $3 = \omega^5(1+\omega)^2$ is a mere matter of calculation.

   (b) If $p \equiv 1 \pmod 3$, then by the previous question there exists $x \in \mathbb{Z}$ such that $p \mid (x^2 + x + 1) = (x - \omega)(x - \bar{\omega}) = (x - \omega)(x + 1 - \omega)$. Both of these fators lie in $\mathbb{Z}[\omega]$, and p clearly does not divide them, so by Euclid's lemma p is not irreducible, so we may write p=$\pi\pi'$ with $\pi, \pi' \in \mathbb{Z}[\omega]$ non-invertibles. Since $N(p) = p^2$, we must haveN$(\pi) = N(\pi') = p$, so π and π' are irreducible and $\pi' = \bar{\pi}$.

(c) If $p \equiv -1 \pmod 3$ were reducible in $\mathbb{Z}[\omega]$, then since $N(p) = p^2$, it would factor as a product of two irreducibles of norm p. Let $a + b\omega$ be one of them; then we would have $p = N(a + b\omega) = a^2 + ab + b^2$. If a and b were both divisible by p, then $a^2 + ab + b^2$ would be divisible by p^2, which is absurd. But if $p \nmid a$, then we get $x^2 + x + 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$ with $x = ba^{-1} \bmod p$, which contradicts the previous question. Same thing if $p \nmid b$. So we have reached a contradiction, which shows that p is irreducible.

8. Every $\alpha \in \mathbb{Z}[\omega]$ divides its norm, which lies in $\mathbb{N}$ and is thus a product of prime numbers. We have determined how these prime numbers decompose in $\mathbb{Z}[\omega]$ in the previous question, so we have found all irreducibles: they are $1+\omega$ (norm 3), the primes $p \equiv -1 \pmod 3$ (norm p^2), and the two conjugate irreducibles dividing each prime $p \equiv 1 \pmod 3$ (and we can check that these two are never associate to each other by testing all 6 invertibles, but this is tedious), which have norm p.

9. This is now the same proof as for $\mathbb{Z}[i]$, taking what we know about the irreducibles and their norms into account.

10. By the same logic as in class, we find that this number is

$$\begin{cases} 6 \prod_{p \equiv 1 (3)} (1 + v_p(n)), \text{ if } v_p(n) \text{ is even for all } p \equiv -1 \bmod 3, \\ 0, \text{ else} \end{cases}$$

(note that this time we have 6 units).