Math 261 — Exercise sheet 8

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

Version: November 26, 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.

Solution 8.1:

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 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) $\alpha = 8 - i$, $\beta = 5 - 2i$.

Solution 8.2:

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 $1-i$. Obvously, 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). Besides, we have

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

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

2. (10 pts) Same process. First, we divide $8-i$ by $5-2i$:

$$\frac{8-i}{5-2i} = \frac{(8-i)(5+2i)}{29} = \frac{42+11i}{29} \approx 1$$

so the quotient is 1 and the reminder is $(8-i)-(5-2i) = 3+i$. We record this relation for later use.

Next, we divide $5-2i$ by $3+i$:

$$\frac{5-2i}{3+i} = \frac{(5-2i)(3-i)}{10} = \frac{13-11i}{10} \approx 1-i,$$

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

Finally, we should divide $3+i$ by 1. Of course the quotient is $3+i$ and remainder 0, so we stop. We have found that $\gcd(\alpha,\beta) = 1$, which means that α and β are coprime.

To find ξ and η, we compute

$$1 = (5-2i)-(3+i)(1-i) = (5-2i)-\big((8-i)-(5-2i)\big)(1-i) = (5-2i)(2-i)-(8-i)(1-i)$$

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

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

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

Solution 8.3:

We first compute that

$$N(29 + 3i) = 29^2 + 3^2 = 850 = 2 \times 5^2 \times 17.$$

This tells us that $29 + 3i$ factors as

$$29 + 3i = \pi_2 \pi_5 \pi_5' \pi_{17},$$

where π_p denotes an irreducible of norm p.

But we know the irreducibles of $\mathbb{Z}[i]$, so we deduce that up to invertibles, we must have $\pi_2 = 1 + i$, $\pi_5 = a \pm bi$, $\pi_5' = a \pm bi$, and $\pi_{17} = c \pm di$, where a, b (resp. c, d) is a solution to $a^2 + b^2 = 5$ (resp. $c^2 + d^2 = 17$). We see that we can take $a = 2$, $b = 1$, $c = 1$, $d = 4$.

Besides, if $\pi_5' \neq \pi_5$, then up to invertibles $\pi_5' = \overline{\pi_5}$, so we would have $5 = \pi_5 \pi_5' \mid (29 + 3i)$, which is clearly not the case. Thus we can assume that $\pi_5' = \pi_5$. As a result, the factorization looks like

$$29 + 3i = u(1 + i)(2 \pm i)^2(1 \pm 4i)$$

where $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ is invertible.

We can first remove the known factor $(1 + i)$: we find that

$$u(2 \pm i)^2(1 \pm 4i) = \frac{29 + 3i}{1 + i} = 16 - 13i.$$

We now need to determine if $\pi_5 = 2 + i$ or $2 - i$, and similarly for π_{17}. For this, we test whether $16 - 13i$ is divisible by $2 + i$: if it is, then $\pi_5 = 2 + i$, else we must have $\pi_5 = 2 - i$. We compute that

$$\frac{16 - 13i}{2 + i} = \frac{19 - 42i}{5} \notin \mathbb{Z}[i],$$

so $(2 + i) \nmid (16 - 13i)$ so π_5 is not $2 + i$, thus $\pi_5 = 2 - i$.

Removing the factor π_5^2 yields

$$u\pi_{17} = \frac{16 - 13i}{(2 - i)^2} = 4 + i.$$

But since π_{17} is irreducible, so is $u\pi_{17}$ (remember that u is invertible), so we may redefine π_{17} as $4 + i$.

Conclusion: our complete factorization is

$$\boxed{29 + 3i = (1 + i)(2 - i)^2(4 + i).}$$

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. $n = 6000$.

Solution 8.4:

Remember that if n factorsin $\mathbb{Z}$ as $2^a \prod_j p_j^{v_j} \prod_k q_k^{w_k}$ where the p_j are distinct primes $\equiv +1 \pmod 4$ and the q_k are distinct primes $\equiv -1 \pmod 4$, then the number of elements of $\mathbb{Z}[i]$ of norm n is

$$\begin{cases} 4 \prod_j (1 + v_{p_j}(n)), \text{ if } w_k \text{ is even for all } k, \\ 0, \text{ else,} \end{cases}$$

since such an element must factor as

$$u(1+i)^a \prod_j \pi_{p_j}^{b_j} \overline{\pi}_{p_j}^{v_j - b_j} \prod_k q_k^{w_k/2}$$

where $u \in \mathbb{Z}[i]^\times$ is invertible and π_p is an irreducible of norm p, which can be found by finding a solution to $x^2 + y^2 = p$. Therefore,

1. An $\alpha \in \mathbb{Z}[i]$ of norm $n = 261 = 3^2\, 29$ must factor as $u 3 \pi$ or $u 3 \overline{\pi}$ where π is a fixed irreducible of norm 29 (since $29 = 5^2 + 2^2$ we can take $\pi = 5 + 2i$), so $N(261) = 8$.
2. An $\alpha \in \mathbb{Z}[i]$ of norm $n = 2000 = 2^4\, 5^3$ must factor as $u(1+i)^4 \pi^b \overline{\pi}^{3-b}$ with $0 \leqslant b \leqslant 3$ where π is a fixed irreducible of norm 5 (for instance $\pi = 2 + i$), so $N(261) = 16$.
3. Since $6000 = 2^4 \times 3 \times 5^3$ and since $3 \equiv -1 \pmod 4$ has odd multiplicity, there is no $\alpha \in \mathbb{Z}[i]$ of norm 6000, so $N(6000) = 0$.

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?

Solution 8.5:

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 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 $\mathbb{Z}$.

Solution 8.6:

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 lemma and then the uniqueness of factorization from there.

6. (Compare with question 2 of exercise 7.4) 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 Gauss'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 have$N(\pi) = N(\pi') = p$, 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 abot the irreducibles and their norms into account.

10. We find that this number is

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

(note that this time we have 6 invertibles).