Math 261 — Exercise sheet 6

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

Version: November 3, 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.

Solution 6.1:

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 $n = 1005$: since the sum of digits is 6, $3 \mid n$ 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 $n \equiv 5 \not\equiv 7 \pmod 8$, 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 $n = 1007$ works.

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

Solution 6.2:

This is the same principle as in $\mathbb{Z}$: we do euclidian 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 euclidian division of α by β. We have

$$\frac{\alpha}{\beta} = \frac{(4+6i)(5+3i)}{34} = \frac{(2+3i)(5+3i)}{17} = \frac{1 = 21i}{17} \approx i,$$

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

Next, we divide the divisor by the remainder, that is to say $5-3i$ by $1+i$. We have

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

exactly, so this time the remainder is 0. This means that $\boxed{\gcd(\alpha,\beta) = 1+i}$. Besides, we have

$$1+i = (4+6i)-(5-3i)i,$$

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

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

$$\frac{8+i}{5-2i} = \frac{(8+i)(5+2i)}{29} = \frac{38+21i}{29} \approx 1+i$$

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

Next, we divide $5-2i$ by $1-2i$:

$$\frac{5-2i}{1-2i} = \frac{(5-2i)(1+2i)}{5} = \frac{9+8i}{5} \approx 2+2i,$$

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

Finally, we divide $1-2i$ by -1. We of course get quotient $-1+2i$ and remainder 0, so we stop. We have found that $\gcd(\alpha,\beta) = -1$, which we normalise as $\boxed{\gcd(\alpha,\beta) = 1}$ since -1 is a unit and the gcd is only defined up to units. We note that α and β are coprime.

To find ξ and η, we start with

$$1 = (5-2i)(-1) + (1-2i)(2+2i)$$

and we plug in the relation $1-2i = (8+i)-(5-2i)(1+i)$ to get

$$1 = (5-2i)(-1) + \big((8+i)-(5-2i)(1+i)\big)(2+2i) = (8+i)(2+2i) + (5-2i)(-1-4i),$$

so we can take $\boxed{\xi = 2+2i, \eta = -1-4i}$.

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

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

Solution 6.3:

We first compute that

$$N(19 + 17i) = 19^2 + 17^2 = 650 = 2 \times 5^2 \times 13.$$

This tells us that $19 + 17i$ factors as

$$19 + 17i = \alpha_2 \alpha_{5^2} \alpha_{13},$$

where α_N has norm N. Now, 2 and 13 are prime so α_2 and α_{13} are irreducible, and since $5 \equiv +1 \pmod 4$, the irreducibles dividing 5 have norm 5^1, so we have

$$19 + 17i = \pi_2 \pi_5 \pi_5' \pi_{13},$$

where $N(\pi_2) = 2$, $N(\pi_5) = N(\pi_5') = 5$ and $N(\pi_{13}) = 13$, and the π_n are irreducible.

But we know the irreducibles of $\mathbb{Z}[i]$, so we deduce that up to units, we must have $\pi_2 = 1 + i$, $\pi_5 = a \pm bi$, $\pi_5' = a \pm bi$, and $\pi_{13} = c \pm di$, where a, b (resp. c, d) is a solution to $a^2 + b^2 = 5$ (resp. $c^2 + d^2 = 13$). We see that we can take $a = 2$, $b = 1$, $c = 3$, $d = 2$.

Besides, if $\pi_5' \neq \pi_5$, then up to units $\pi_5' = \overline{\pi_5}$, so we would have $5 = \pi_5 \pi_5' \mid (19 + 17i)$, which is clearly not the case. Thus we can assume that $\pi_5' = \pi_5$. As a result, the factorization looks like

$$19 + 17i = u(1 + i)(2 \pm i)^2(3 \pm 2i)$$

where $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ is a unit. We can remove the factor immediately, by computing

$$u(2 \pm i)^2(3 \pm 2i) = \frac{19 + 17i}{1 + i} = \frac{(19 + 17i)(1 - i)}{2} = 18 - i.$$

We now need to determine if $\pi_5 = 2 + i$ or $2 - i$, and similarly for π_{13}. For this, we test whether $18 - i$ is divisible by $2 + i$: if it is, then $\pi_5 = 2 + i$, else we must have $\pi_5 = 2 - i$. We compute that

$$\frac{18 - i}{2 + i} = \frac{(18 - i)(2 - i)}{5} = 7 - 4i \in \mathbb{Z}[i],$$

so $(2+i) \mid (18-i)$ so $\pi_5 = 2+i$. We can thus remove another factor π_5, by computing

$$\frac{7 - 4i}{2 + i} = \frac{(7 - 4i)(2 - i)}{5} = 2 - 3i.$$

Thus $u\pi_{13} = 2-3i$, and we can absorb the unit u into π_{13} by redefining $\pi_{13} = 2-3i$, which is still irreducible since we have only changed it by a unit.

Conclusion: our complete factorization is

$$\boxed{19 + 17i = (1 + i)(2 + i)^2(2 - 3i).}$$

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?

Solution 6.4:

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 units, 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 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?

Solution 6.5:

1. We first notice that an element of norm p^a must factor as a product of irreducibles dividing p. We also notice that if α is a nonzero element of $\mathbb{Z}[i]$, then the 4 elements $\pm\alpha$, $\pm i\alpha$ are all distinct. Therefore,

   (a) if $p \equiv -1 \pmod 4$, then up to units the only irreducible dividing p is p itself, so an element of norm p^a must factor as up^b where u is a unit and b is an integer. In order to have $N(up^b) = p^a$, we need $a = 2b$, which is impossible if a is odd; and if a is even, then we must have $b = a/2$ and we get 4 distinct elements up^b since we have 4 units u in $\mathbb{Z}[i]^\times$;

   (b) if $p \equiv 1 \pmod 4$, then up to units thre are exactly 2 irreducibles dividing p, say π and $\bar{\pi}$, so an element of norm p^a must factor as $u\pi^b\bar{\pi}^c$ where u is a unit and b, c are integers. In order to have $N(u\pi^b\bar{\pi}^c) = p^a$, we need $a = b + c$, whence $a + 1$ possible values for b (the integers from 0 to a included), each of which determines the value of $c = a - b$. Since we have 4 units u in $\mathbb{Z}[i]^\times$, we thus get $4(a+1)$ elements of norm p^a; they are all distinct since the $\pi^b\bar{\pi}^{a-b}$ are non-associate by the uniqueness of factorization in $\mathbb{Z}[i]$;

   (c) finally, if $p = 2$, then up to units the only irreducible dividing p is $1 + i$, so an element of norm p^a must factor as $u(1+i)^b$ where u is a unit and b is an integer. In order to have $N(u(1+i)^b) = p^a$, we need $a = b$ so b is fixed, so we get 4 distinct elements $u(1+i)^a$ from the 4 units u in $\mathbb{Z}[i]^\times$.

2. First of all, the number of ways to write n as a sum of 2 squares is the same as the number of elements of $\mathbb{Z}[i]$ of norm n. Now, if $\alpha \in \mathbb{Z}[i]$ has norm $n = \prod_k p_k^{a_k}$ with the p_k distinct primes, then its factorization in $\mathbb{Z}[i]$ must be of the form
$$\alpha = u \prod_k \alpha_k$$
where $\alpha_k \in \mathbb{Z}[i]$ is the part of the factorisation formed of the irreducibles dividing p_k, and we must have $N(\alpha_k) = p_k^{a_k}$. By the previous question ,we

have a formula for the number of such α_k's, but we must count them up to units since we can gather the units in the factorization of α_k into the unit u at the front of the factorisation of α. Therefore, we must divide the formulas from the previous question by 4, multiply them, and multiply the result by 4 to take the unit u into account. As a conclusion, the number of ways to write n as a sum of 2 squares is

$$4 \prod_{\substack{k \\ p_k \equiv 1 (4)}} (1+a_k) \prod_{\substack{k \\ p_k \equiv -1 (4)}} \mathbb{1}_{a_k \text{ even}} = \begin{cases} 4 \prod_{p \equiv 1 (4)} (1+v_p(n)), \text{ if } v_p(n) \text{ is even for all } p \equiv 1 \ (4), \\ 0, \text{ else,} \end{cases}$$

where $\mathbb{1}_{a_k \text{ even}}$ means 1 if a_k is even and 0 else.

Remark: This is also either 0 or the number of divisors of n that are products of primes $\equiv 1 \pmod 4$ only.

3. Since $2000 = 2^4 \times 5^3$ and $5 \equiv 1 \pmod 4$, the number of ways to write 2000 as a sum of 2 squares is
$$4(3+1) = \boxed{16.}$$
Also, since $6000 = 2^4 \times 3 \times 5^3$ and since $3 \equiv -1 \pmod 4$ has odd multiplicity, there are $\boxed{0}$ ways to write 6000 as a sum of 2 squares.

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 $\mathbb{Z}$.

Solution 6.6:

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 a unit, 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 units 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 units. But ω is a unit since $1 = \omega\bar{\omega} = \omega(1 - \omega)$, so all powers of ω are a also units, and since $\omega = e^{\pi i/3}$, the sequence of powers of ω is periodic of period exactly 6, so all 6 units 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 5.4) 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-units. 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 units, 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 units).

(This is either 0 or the number of divisors of n that are products of primes $\equiv 1 \pmod 3$ only.)