Exercises, II.

Maciej Zakarczemny

Exercise 1. Define $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a+bi) = a^2 + b^2$.
Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using the fact that $N(a+bi) = (a+bi)(a-bi)$.
Conclude that if $\alpha|\gamma$ in $\mathbb{Z}[i]$, then $N(\alpha)|N(\gamma)$ in $\mathbb{Z}$.

Proof. Let $\alpha = a+bi$, $\beta = c+di$ we have:

$$N(\alpha\beta) = N((a+bi)(c+di)) = N(ac-bd+(ad+bc)i) = (ac-bd+(ad+bc)i)(ac-bd-(ad+bc)i) =$$

$$= (a+bi)(c+di)(a-bi)(c-di) = N(\alpha)N(\beta).$$

If $\alpha|\gamma$ in $\mathbb{Z}[i]$ then there exists $\beta \in \mathbb{Z}[i]$ such that

$$\alpha\beta = \gamma,$$

thus by above

$$N(\alpha)N(\beta) = N(\gamma),$$

since α, β, $\gamma \in \mathbb{Z}[i]$ we get $N(\alpha)$, $N(\beta)$, $N(\gamma) \in \mathbb{Z}$ and $N(\alpha)|N(\gamma)$ in $\mathbb{Z}$. $\square$

Exercise 2. Let $\alpha \in \mathbb{Z}[i]$. Show that α is a unit iff $N(\alpha) = 1$. Conclude that the only units are ± 1 and $\pm i$.

Proof. Let $\alpha = a+bi$. If $\alpha|1$ in $\mathbb{Z}[i]$ then there exists $\beta \in \mathbb{Z}[i]$ such that

$$\alpha\beta = 1,$$

thus

$$N(\alpha)N(\beta) = N(1) = 1,$$

since α, $\beta \in \mathbb{Z}[i]$ we get $N(\alpha)$, $N(\beta) \in \mathbb{Z}$ and $N(\alpha)|1$ in $\mathbb{Z}$. Therefore

$$a^2 + b^2 = N(\alpha) = \pm 1$$

Hence

$$(a, b) \in \{(1, 0),\ (-1, 0),\ (0, 1),\ (0, -1)\},$$

thus

$$\alpha \in \{1,\ -1,\ i,\ -i\}.$$

On the other hand we have

$$1 \cdot 1 = 1,\ (-1) \cdot (-1) = 1,\ i \cdot (-i) = 1.$$

Hence α is a unit iff $N(\alpha) = 1$. $\square$

Exercise 3. Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.

Proof. If $\alpha = \beta\gamma$ in $\mathbb{Z}[i]$ then $N(\alpha) = N(\beta)N(\gamma)$.
Since $N(\alpha)$ is a prime in $\mathbb{Z}$ and $N(\beta), N(\gamma)$ are nonnegative we obtain $N(\beta) = 1$ or $N(\gamma) = 1$.
Assume that $N(\gamma) = 1$ then γ is equal ± 1 or $\pm i$ hence γ is a unit in $\mathbb{Z}[i]$.
Analogously, if $N(\beta) = 1$ then β is a unit in $\mathbb{Z}[i]$.
We have shown that if $\alpha = \beta\gamma$ then β or γ is a unit in $\mathbb{Z}[i]$.
Therefore α is irreducible in $\mathbb{Z}[i]$.
Now we assume that $N(\alpha) = p^2$.
If $\alpha = \beta\gamma$ in $\mathbb{Z}[i]$ then $N(\alpha) = N(\beta)N(\gamma)$.
We denote $\beta = c + di$ and get $N(\beta) = c^2 + d^2 \not\equiv 3 \pmod 4$ thus $N(\beta) \neq p$, analogously $N(\gamma) \neq p$.
Since $p^2 = N(\beta)N(\gamma)$ we obtain $N(\beta) = 1$ or $N(\gamma) = 1$ and proceeding as above, we show that α is irreducible.

□

Exercise 4. Show that $1 - i$ is irreducible in $\mathbb{Z}[i]$ and that $2 = u(1 - i)^2$ for some unit u.

Proof. Since $N(1 - i) = 1^2 + (-1)^2 = 2$ is a prime number in $\mathbb{Z}$ by Exercise 3, we get that $1 - i$ is irreducible in $\mathbb{Z}[i]$.
We have $i(1 - i)^2 = i(1^2 - 2i + i^2) = i(-2i) = 2$ hence we may take $u = i$.
Since $i(-i) = 1$ we obtain that u is a unit in $\mathbb{Z}[i]$.
Note that $2 = i(1 - i)^2$ is a complete factorization of 2 in $\mathbb{Z}[i]$.

In polish:
Pokaż, że $1 - i$ jest nieprzywiedlne (niektórzy piszą nierozkładalne) w $\mathbb{Z}[i]$ oraz, że $2 = u(1 - i)^2$ dla pewnej jedności u.

Dowód: Ponieważ $N(1 - i) = 1^2 + (-1)^2 = 2$ jest całkowitą liczbą pierwszą, zatem na podstawie Zadania 3, dostajemy, że $1 - i$ jest nieprzewiedlne w $\mathbb{Z}[i]$.
Mamy $i(1 - i)^2 = i(1^2 - 2i + i^2) = i(-2i) = 2$, wobec tego możemy wziąć $u = i$. Skoro $i(-i) = 1$, zatem u to jedność w $\mathbb{Z}[i]$.
Zauważmy, że $2 = i(1 - i)^2$ to kompletny rozkład 2 w $\mathbb{Z}[i]$. □

Exercise 5. Notice that $(2+i)(2-i) = 5 = (1+2i)(1-2i)$. How is this consistent with unique factorization?

Proof. $\mathbb{Z}[i]$ is a unique factorization domain: every nonzero Gaussian integer can be expressed in a unique way (up to order and unit factors) as a product of Gaussian primes.
Since i is a unit in $\mathbb{Z}[i]$ and

$$(2+i) = i(1-2i),\ (2-i) = (-i)(1+2i)$$

equation

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

gives the same factorization of 5 up to order and unit factors.

$\square$

Exercise 6. Show that every nonzero, non-unit Gaussian integer α is a product of irreducible elements, by induction on $N(\alpha)$.

Proof. If $N(\alpha) = 1$ then by exercise 2, α is a unit.
Hence we may assume, that $N(\alpha) > 1$.
If $N(\alpha) = 2$ then by exercise 3 number α is irreducible in $\mathbb{Z}[i]$.
Let $s > 2$ be an integer.
We will proceed by induction on s.
Assume that every nonzero, non-unit $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) < s$ is a product of irreducible elements.
Let α be any element of $\mathbb{Z}[i]$ such that $N(\alpha) = s$.
If α is irreducible in $\mathbb{Z}[i]$ then α is a product of irreducible elements (product of one irreducible element namely α).
If α is reducible then $\alpha = \beta\gamma$ where $\beta, \gamma \in \mathbb{Z}[i]$ are not units.
By exercise 2 we get $N(\beta)$, $N(\gamma) > 1$, hence $N(\beta)$, $N(\gamma) < s$.
By inductive assumption β and γ are products of irreducible elements.
Therefore $\alpha = \beta\gamma$ is a product of irreducible elements.
Thus every nonzero, non-unit $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) < s + 1$ is a product of irreducible elements.
Therefore every nonzero, non-unit Gaussian integer α is a product of irreducible elements. $\square$

Exercise 7. Show that $\mathbb{Z}[i]$ is a principal ideal domain (PID), i.e., every ideal I is principal.

Proof. A subset I is called an ideal of $\mathbb{Z}[i]$ if it satisfies the following two conditions:

1. I is an additive subgroup of $\mathbb{Z}[i]$, i.e. $\forall_{\alpha,\beta\in I}\ \alpha-\beta\in I$,
2. $\forall_{\alpha\in I}\forall_{\gamma\in\mathbb{Z}[i]}\ \gamma\alpha\in I$.

A principal ideal is an ideal I in a ring $\mathbb{Z}[i]$ that is generated by a single element a of $\mathbb{Z}[i]$. The principal ideal generated by $\alpha\in\mathbb{Z}[i]$ can be expressed in the form $I=\{\gamma\alpha:\ \gamma\in\mathbb{Z}[i]\}$. We take $\alpha\in I-\{0\}$ such that $N(\alpha)\in\mathbb{Z}_+$ is minimized, and consider the multiples $\gamma\alpha,\ \gamma\in\mathbb{Z}[i]$.
These are the vertices of a lattice Λ which divide the whole of complex plane into congruent squares, copies of an $2-$dimensional fundamental square with vertices 0, α, $i\alpha$, $(1+i)\alpha$.
We have

$$\Lambda=\{v_1\alpha+v_2i\alpha, v_1,\, v_2\in\mathbb{Z}\}=\{\gamma\alpha,\gamma\in\mathbb{Z}[i]\}\subset I.$$

We take arbitrary $\beta\in I$.
The fundamental square K of the lattice $\beta+\Lambda$ is a translation of the fundamental square of the lattice Λ. Sides of square K have length equal $N(\alpha)$.
We may assume that the origin of coordinate system is in interior or on boundary of the square $ABCD$, where A,B,C,D are vertices of $\beta+\Lambda$ and square $ABCD$ is a translation of K.
Diagonals divide square $ABCD$ into four congruent triangles with diameters equal $N(\alpha)$. Therefore the distance between origin and the nearest from vertices A,B,C,D, say A, is smaller then $N(\alpha)$.
Thus $N(A)<N(\alpha)$. Since $A\in\beta+\Lambda\subset I$ by definition of α we obtain $A=0$. Hence $0\in\beta+\Lambda$. Therefore $\beta\in\Lambda$ and

$$I=\Lambda=\{\gamma\alpha,\gamma\in\mathbb{Z}[i]\}.$$

Thus ideal I is principal and $\mathbb{Z}[i]$ is a principal ideal domain. $\square$

Exercise 8. We will use unique factorization in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1(\mod 4)$ is a sum of two squares.

(a) Use the fact that the multiplicative group $\mathbb{Z}_p^*$ of integer $\mod p$ is cyclic to show that if $p \equiv 1(\mod 4)$ then $n^2 \equiv -1(\mod p)$ for some $n \in \mathbb{Z}$.

(b) Prove that p cannot be irreducible in $\mathbb{Z}[i]$.
(Hint: $p|n^2 + 1 = (n+i)(n-i)$.)

(c) Prove that p is a sum of two squares.(Hint: (b) shows that $p = (a+bi)(c+di)$ with neither factor a unit. Take norms.)

Proof. Let g be a generator of the cyclic group $\mathbb{Z}_p^*$, we have $g^{p-1} = 1$.
Hence $\left(g^{\frac{p-1}{4}}\right)^4 = 1$ in $\mathbb{Z}_p^*$ (note that $p \equiv 1(\mod 4)$).
We take $n = g^{\frac{p-1}{4}}$ in $\mathbb{Z}$ and obtain $n^2 \equiv -1(\mod p)$.
Since $p|n^2 + 1$ we get $p|(n+i)(n-i)$ in $\mathbb{Z}[i]$.
If p is irreducible in $\mathbb{Z}[i]$ then $p|n+i$ and also $p|n-i$.
Thus $p|2i$ and $p^2|4$ but $p \equiv 1(\mod 4)$ and we get contradiction.
Therefore p is reducible in $\mathbb{Z}[i]$.
We take $p = (a+bi)(c+di)$, $a, b, c, d \in \mathbb{Z}$ where neither factor is a unit.
Hence $p^2 = (a^2+b^2)(c^2+d^2)$ where a^2+b^2, $c^2+d^2 \neq 1$.
Thus $p = a^2 + b^2$, $a, b \in \mathbb{Z}$. $\square$

Exercise 9. Describe all irreducible elements in $\mathbb{Z}[i]$.

Proof. Non-unit, non-zero element in $\mathbb{Z}[i]$, is said to be irreducible if it is not a product of two non-units. Assume that α is irreducible in $\mathbb{Z}[i]$.
Let $\alpha\bar{\alpha} = N(\alpha) = {p_1}^{k_1}{p_2}^{k_2} \cdot \ldots \cdot {p_n}^{k_n}$ is a decomposition of $N(\alpha)$ in $\mathbb{Z}$.
Hence $\alpha | {p_1}^{k_1}{p_2}^{k_2} \cdot \ldots \cdot {p_n}^{k_n}$.
Since α is irreducible in $\mathbb{Z}[i]$ (and hence $\bar{\alpha}$ also) we may assume, that $\alpha, \bar{\alpha} | p_1$.
Therefore $N(\alpha) | p_1^2$. If $N(\alpha) = 1$ then α is a unit, contradiction.
If $N(\alpha) = p_1$ then α is irreducible, (if α is a product of two non-units, then $N(\alpha)$ is a product of two natural numbers neither equal to one).
If $\alpha\bar{\alpha} = N(\alpha) = p_1^2$ then $\alpha = up_1$, $\bar{\alpha} = u^{-1}p_1$, where u is a unit in $\mathbb{Z}[i]$ (note that $\alpha, \bar{\alpha} | p_1$).
Assume that $p_1 = (a+bi)(c+di)$ where $a, b, c, d \in \mathbb{Z}$ hence
$ac - bd = p_1$, $ad = -bc, (a, b) = (c, d) = 1$.
Therefore $a = c$, $b = -d$ and $p_1 = a^2 + b^2$. We obtain $p_1 \equiv 1 (\mod 4)$.
On the other hand if $p_1 \equiv 1 (\mod 4)$ then by Exercise 8 we may find $a, b \in \mathbb{Z}$ such that $p_1 = a^2 + b^2 = (a+bi)(a-bi)$, where neither factor is a unit ($N(a+bi) = N(a-bi) = a^2+b^2 = p_1 > 1$). Hence $\alpha = u(a+bi)(a-bi)$.
Therefore element α in $\mathbb{Z}[i]$ is irreducible if $N(\alpha)$ is a prime number in $\mathbb{Z}$ or α is a prime number in $\mathbb{Z}$ which is congruent to 3 modulo 4.

$\square$

Exercise 10. Let $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Define $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ by

$$N(a + b\omega) = a^2 - ab + b^2.$$

Show that if $a + b\omega$ is written in the form $u + vi$, where u and v are real, then $N(a + b\omega) = u^2 + v^2$.

Proof. We have $a + b\omega = a - \frac{1}{2}b + \frac{\sqrt{3}}{2}bi = u + vi$, hence

$$N(u+vi) = N(a-\frac{1}{2}b+\frac{\sqrt{3}}{2}bi) = N(a+b\omega) = a^2-ab+b^2 = (a-\frac{1}{2}b)^2+(\frac{\sqrt{3}}{2}b)^2 = u^2+v^2.$$

□

Exercise 11. Show that for all $\alpha, \beta \in \mathbb{Z}[\omega]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using exercise 10. Conclude that if $\alpha|\gamma$ in $\mathbb{Z}[\omega]$, then $N(\alpha)|N(\gamma)$ in $\mathbb{Z}$.

Proof. Let $\alpha = a + b\omega = u_\alpha + v_\alpha i$, $\beta = c + d\omega = u_\beta + v_\beta i$, then

$$\alpha\beta = (u_\alpha + v_\alpha i)(u_\beta + v_\beta i) = (u_\alpha u_\beta - v_\alpha v_\beta) + (u_\alpha v_\beta + u_\beta v_\alpha)i.$$

Whence

$$N(\alpha\beta) = (u_\alpha u_\beta - v_\alpha v_\beta)^2 + (u_\alpha v_\beta + u_\beta v_\alpha)^2 = (u_\alpha^2 + v_\alpha^2)(u_\beta^2 + v_\beta^2) = N(\alpha)N(\beta).$$

If $\alpha|\gamma$ in $\mathbb{Z}[\omega]$ then there exists $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = \gamma$.
Thus $N(\gamma) = N(\alpha\beta) = N(\alpha)N(\beta)$.
Since $N(\beta) \in \mathbb{Z}$ we get $N(\alpha)|N(\gamma)$ in $\mathbb{Z}$.

□

Exercise 12. Let $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Define $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ by

$$N(a + b\omega) = a^2 - ab + b^2.$$

Let $\alpha \in \mathbb{Z}[\omega]$. Show that α is a unit iff $N(\alpha) = 1$, and find all units in $\mathbb{Z}[\omega]$.

Proof. If α is a unit then $\alpha | 1$ in $\mathbb{Z}[\omega]$, by exercise 11 we get that $N(\alpha) | N(1) = 1$.
Since $N(\alpha) \geq 0$, $N(\alpha) \in \mathbb{Z}$ we obtain $N(\alpha) = 1$.
On the other hand.
Assume that $\alpha = a + b\omega$ and $N(\alpha) = 1$.
We have $a - b - b\omega \in \mathbb{Z}[\omega]$ and

$$(a+b\omega)(a-b-b\omega) = (a-\tfrac{1}{2}b+\tfrac{\sqrt{3}}{2}bi)(a-\tfrac{1}{2}b-\tfrac{\sqrt{3}}{2}bi) = (a-\tfrac{1}{2}b)^2+\tfrac{3}{4}b^2 = a^2-ab+b^2 = 1.$$

Hence α is a unit.
We will find all units in $\mathbb{Z}[\omega]$.
Let $\alpha = a + b\omega$ is a unit in $\mathbb{Z}[\omega]$.
Therefore $a^2 - ab + b^2 = 1$.
If $b = 0$ then $a^2 = 1$ and we have units $1, -1$.
If $a = 0$ then $b^2 = 1$ and we have units $\omega, -\omega$.
If $b \neq 0$ then $(a - b)^2 + a^2 + b^2 = 2(a^2 - ab + b^2) = 2$.
Since $b \in \mathbb{Z}$, $b \neq 0$, $(a - b)^2 + a^2 \geq 0$ we have $b^2 = 1$ and $(a - b)^2 + a^2 = 1$.
Since $a \in \mathbb{Z}$, $a \neq 0$, $(a - b)^2 \geq 0$ we have $a^2 = 1$, $a = b$.
Therefore we have units $1 + \omega$, $-1 - \omega$.
Finally, we have six units $1, -1, \omega, -\omega, 1 + \omega, -1 - \omega$. □

Exercise 13. Let $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Define $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ by

$$N(a + b\omega) = a^2 - ab + b^2.$$

Show that $1 - \omega$ is irreducible in $\mathbb{Z}[\omega]$, and that $3 = u(1-\omega)^2$ for some unit u.

Proof. Assume that in $\mathbb{Z}[\omega]$ we have

$$1 - \omega = \alpha\beta,$$

hence $N(1-\omega) = N(\alpha)N(\beta)$.
Therefore $3 = N(\alpha)N(\beta)$ and thus $N(\alpha) = 1$ or $N(\beta) = 1$.
By exercise 12 we get α or β is a unit in $\mathbb{Z}[\omega]$.
Hence $1 - \omega$ is irreducible in $\mathbb{Z}[\omega]$.
We have $\omega^2 + \omega + 1 = 0$ hence

$$3 = (1+\omega)(1-\omega)^2.$$

Note that $-\omega(1+\omega) = 1$ hence $u = 1 + \omega$ is a unit in $\mathbb{Z}[\omega]$. □

Exercise 14. Modify exercise 7 to show that $\mathbb{Z}[\omega]$ is a principal ideal domain (PID)(i.e., every ideal I is principal), hence a UFD. Here the squares are replaced by parallelograms; one of them has vertices $0, \alpha, \omega\alpha, (\omega+1)\alpha$ and all others are translates of this one. Use exercise 10 for the geometric argument at the end.

Proof. A subset I is called an ideal of $\mathbb{Z}[\omega]$ if it satisfies the following two conditions:

1. I is an additive subgroup of $\mathbb{Z}[\omega]$, i.e. $\forall_{\alpha,\beta\in I}\ \alpha - \beta \in I$,
2. $\forall_{\alpha\in I}\forall_{\gamma\in\mathbb{Z}[\omega]}\ \gamma\alpha \in I$.

A principal ideal is an ideal I in a ring $\mathbb{Z}[\omega]$ that is generated by a single element a of $\mathbb{Z}[\omega]$. The principal ideal generated by $\alpha \in \mathbb{Z}[\omega]$ can be expressed in the form $I = \{\gamma\alpha :\ \gamma \in \mathbb{Z}[\omega]\}$.
We take $\alpha \in I - \{0\}$ such that $N(\alpha) \in \mathbb{Z}_+$ is minimized, and consider the multiplies $\gamma\alpha,\ \gamma \in \mathbb{Z}[\omega]$.
These are the vertices of a lattice Λ which divide the whole of complex plane into congruent parallelograms, copies of an $2-$dimensional fundamental parallelogram with vertices $0,\ \alpha,\ \omega\alpha,\ (1+\omega)\alpha$.
We have

$$\Lambda = \{v_1\alpha + v_2\omega\alpha, v_1,\ v_2 \in \mathbb{Z}\} = \{\gamma\alpha, \gamma \in \mathbb{Z}[\omega]\} \subset I.$$

We take arbitrary $\beta \in I$.
The fundamental parallelogram K of the lattice $\beta + \Lambda$ is a translation of the fundamental parallelogram of the lattice Λ. Sides of parallelogram K have length equal $N(\alpha)$.
We may assume that the origin of coordinate system is in interior or on boundary of the parallelogram $ABCD$, where A, B, C, D are vertices of $\beta + \Lambda$ and parallelogram $ABCD$ is a translation of K.
Diagonals divide square $ABCD$ into four congruent triangles with diameters equal $N(\alpha)$. Therefore the distance between origin and the nearest from vertices A, B, C, D, say A, is smaller then $N(\alpha)$.
Thus $N(A) < N(\alpha)$. Since $A \in \beta + \Lambda \subset I$ by definition of α we obtain $A = 0$. Hence $0 \in \beta + \Lambda$. Therefore $\beta \in \Lambda$ and

$$I = \Lambda = \{\gamma\alpha, \gamma \in \mathbb{Z}[\omega]\}.$$

Thus ideal I is principal and $\mathbb{Z}[\omega]$ is a principal ideal domain, hence also unique factorization domain (UFD). $\square$

Exercise 15. Here is a proof of Farmat's conjecture for $n = 4$:
If $x^4 + y^4 = z^4$ has a solution in positive integers, then so does $x^4 + y^4 = w^2$. Let x, y, w be a solution with smallest possible w. Then x^2, y^2, w is a primitive Pythagorean triple. Assuming (without loss of generality) that x is odd, we can write

$$x^2 = m^2 - n^2,\ y^2 = 2mn,\ w = m^2 + n^2$$

with m and n relatively prime positive integers, not both odd.

(a) Show that

$$x = r^2 - s^2,\ n = 2rs,\ m = r^2 + s^2$$

with r and s relatively prime positive integers, not both odd.
Indeed:
Since $x^2 + n^2 = m^2$ and $(m, n) = 1$ we get that x, n, m is a primitive Pythagorean triple. We know that x is odd thus

$$x = r^2 - s^2,\ n = 2rs,\ m = r^2 + s^2$$

with r and s relatively prime positive integers, not both odd.

(b) Show that r, s, and m are pairwise relatively prime. Using $y^2 = 4rsm$, conclude that r, s, and m are all squares.
Indeed: Since $m = r^2 + s^2$, $(r, s) = 1$ we get that r, s, m are pairwise relatively prime.
We have that $(\frac{y}{2})^2 = rsm$, $(r, s) = (r, m) = (s, m) = 1$ hence

$$r = a^2,\ s = b^2,\ m = c^2$$

with a, b, c positive integers.

(c) Show that $a^4 + b^4 = c^2$, and that this contradicts minimality of w.
Indeed: Since $r^2 + s^2 = m$ we get $a^4 + b^4 = c^2$, and because $c \le c^2 = m \le m^2 < m^2 + n^2 = w$ this contradicts minimality of w.

Exercise 16. Let p be an odd prime, $\omega = e^{\frac{2\pi i}{p}}$. Show that

$$(1-\omega)(1-\omega^2)\cdot\ldots\cdot(1-\omega^{p-1}) = p.$$

Note that $1, \omega, \omega^2, \ldots, \omega^{p-1}$ are the p roots of the polynomial $t^p - 1$, hence we have the identity

$$(t-1)(t-\omega)(t-\omega^2)\cdot\ldots\cdot(t-\omega^{p-1}) = t^p - 1.$$

Thus

$$(t-\omega)(t-\omega^2)\cdot\ldots\cdot(t-\omega^{p-1}) = 1 + t + t^2 + \ldots + t^{p-1}.$$

We take $t = 1$ and obtain

$$(1-\omega)(1-\omega^2)\cdot\ldots\cdot(1-\omega^{p-1}) = p.$$

Exercise 17. Assume that

p is an odd prime in $\mathbb{Z}$;

x, y, z have no common integral factor and are not multiples of p;

$x^p + y^p = z^p$;

ω is the pth root of unity.

Suppose that $\mathbb{Z}[\omega]$ is a UFD (unique factorization domain) and $\pi | x + y\omega$, where π is a prime in $\mathbb{Z}[\omega]$. Show that π does not divide any of the other factors on the left side of equation

$$(x+y)(x+y\omega)(x+y\omega^2)\dots(x+y\omega^{p-1}) = z^p,$$

by showing that if it did, then π would divide both z and yp: but z and yp are relatively prime, hence $zm + ypn = 1$ for some $m, n \in \mathbb{Z}$. How is this a contradiction?

Proof. Since π is a prime in $\mathbb{Z}[\omega]$ unique factorization domain and

$$\pi | (x+y)(x+y\omega)(x+y\omega^2)\dots(x+y^{p-1}) = z^p$$

we get $\pi | z$.
If $\pi | x + y\omega^{i_0}$, where $0 \leq i_0 \leq p-1$, $i_0 \neq 1$ then

$$\pi | (x+y\omega^{i_0}) - (x+y\omega) = y(\omega^{i_0} - \omega) = y\omega^{i_0}(1-\omega^{1-i_0}),$$

π is not root of unity and $1 - i_0 \neq 0$ thus

$$\pi | y(1-\omega^{1-i_0}) | y(1-\omega)(1-\omega^2)\cdot\ldots\cdot(1-\omega^{p-1}) = yp.$$

But z and yp are relatively prime in $\mathbb{Z}$, hence $zm + ypn = 1$ for some $m, n \in \mathbb{Z}$. Therefore

$$\pi | zm + ypn = 1$$

which contradict the fact that prime number π is not a root of unity in $\mathbb{Z}[\omega]$. $\square$