Solution 1.

(a) Note that, if $x \in \mathbb{Z}$ then $x^2 \equiv 0$ or $1 \mod 4$. Thus, checking the possibilities we see that if $a, b \in \mathbb{Z}$ then $a^2 + b^2 \equiv 0$ or 1 or $2 \mod 4$. Furthermore if $p = a^2 + b^2$ where p is an odd prime in $\mathbb{Z}$ then we can eliminate the possibilities 0 and 2 (as otherwise p would be even). Thus, we have that if $p = a^2 + b^2$, for some $a, b \in \mathbb{Z}$ and p is an odd prime, then $p \equiv a^2 + b^2 \equiv 1 \mod 4$ as required.

(b) For $r = a + bi \in \mathbb{Q}[i]$, define $N(r) = a^2 + b^2$. Now note that if $\alpha = a + bi$ and $\beta = c + di$; $a, b, c, d \in \mathbb{Q}$ then

$$\begin{aligned} N(\alpha\beta) &= N((ac - bd) + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (ac)^2 + (bd)^2 - 2abcd + (ad)^2 + (bc)^2 + 2abcd \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

Thus, N is multiplicative. (Also note that $N(r) \geq 0$, for all $r \in \mathbb{Q}[i]$ and that $N(r) = 0$ iff $r = 0$).
Let $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha, \beta \neq 0$. Since $\beta \neq 0$, $\frac{\alpha}{\beta}$ is in $\mathbb{Q}[i]$, so there are rational numbers x and y (obtained by "rationalizing the denominator") such that

$$\alpha = (x + yi)\beta$$

Choose integers a, b closest to x and y respectively. More precisely choose integers a and b such that $|x - a| \leq \frac{1}{2}$ and $|y - b| \leq \frac{1}{2}$. Then

$$\alpha = (a + bi)\beta + [(x - a) + (y - b)i]\beta$$

so if we take $\gamma = a + bi$ and $\delta = [(x - a) + (y - b)i]\beta$, we have

$$\alpha = \gamma\beta + \delta$$

Furthermore, as $a, b \in \mathbb{Z}$, this implies $\gamma \in \mathbb{Z}[i]$ and

$$\begin{aligned} \delta &= [(x - a) + (y - b)i]\beta \\ &= (x + yi)\beta - (a + bi)\beta \\ &= \alpha - (a + bi)\beta \end{aligned}$$

Thus, as $\alpha, \beta \in \mathbb{Z}[i]$ and $a, b \in \mathbb{Z}$ we have that $\delta \in \mathbb{Z}[i]$.

It now remains to show that $N(\delta) < N(\beta)$. We have that

$$\begin{aligned} N(\delta) &= N([(x-a)+(y-b)i]\beta) \\ &= N((x-a)+(y-b)i)N(\beta) \\ &= [(x-a)^2+(y-b)^2]N(\beta) \\ &\leq \left[\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right]N(\beta) \\ &= \frac{1}{2}N(\beta) \\ &< N(\beta) \end{aligned}$$

as required. Thus, $\mathbb{Z}[i]$ is a Euclidean domain and hence a PID which further implies that it is a UFD.

(c) Suppose p is a prime such that $p \equiv 1 \mod 4$. By the quadratic reciprocity law then $\exists a \in \mathbb{Z}$ such that

$$\begin{aligned} a^2 &\equiv -1 \mod p \\ \Rightarrow a^2+1 &\equiv 0 \mod p \end{aligned}$$

Thus, $p|a^2+1$ in $\mathbb{Z}$. This implies that $p|(a+i)(a-i)$ in $\mathbb{Z}[i]$. If p were a prime in $\mathbb{Z}[i]$ this would imply that p divides $a+i$ or $a-i$ in $\mathbb{Z}[i]$ which is clearly absurd (as $p \nmid \pm 1$). Hence, if $p \equiv 1 \mod 4$ then p is not a prime in $\mathbb{Z}[i]$, as required.

(d) Let p be as stated in the problem. By part (b) $\mathbb{Z}[i]$ is a UFD, hence if we have a non-unit non-zero element in $\mathbb{Z}[i]$ that is not prime then it is reducible. Further note that $u \in \mathbb{Z}[i]$ is a unit iff $N(u) = 1$, where N is as defined in part (b) (this follows from the multiplicative nature of N and the fact that $N(1) = 1$). Now by part (c) p is not prime and as $N(p) = p^2$ it is also a non-zero non-unit in $\mathbb{Z}[i]$. Thus, it is reducible in $\mathbb{Z}[i]$ i.e there exist $a, b, c, d \in \mathbb{Z}$ such that

$$p = (a+bi)(c+di)$$

where, $a+bi$ and $c+di$ are not units and consequently $a^2+b^2 \neq 1$ and $c^2+d^2 \neq 1$. Applying the map N we obtain that

$$p^2 = (a^2+b^2)(c^2+d^2)$$

Now using unique factorization in $\mathbb{Z}$ we have that $p = a^2+b^2$ as required.

□

Solution 2.

We will proceed analogously to solution 1. We see that if $x \in \mathbb{Z}$ then $x^2 \equiv 0$ or 1 or 4 mod 8. Thus checking the possibilities we see that if $a, b \in \mathbb{Z}$ then $a^2 - 2b^2 \equiv 0$ or $\pm$ 1 or -2 or 4 mod 8. Furthermore if $p = a^2 - 2b^2$ where p is an odd prime in $\mathbb{Z}$ then we can eliminate the possibilities 0, -2 and 4 (as otherwise p would be even). Thus, we

have that if $p = a^2 - 2b^2$, for some $a, b \in \mathbb{Z}$ and p is an odd prime, then $p \equiv a^2 + b^2 \equiv \pm 1 \mod 8$.

For $r = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, define $N(r) = |a^2 - 2b^2|$. Now note that if $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$ then

$$\begin{aligned} N(\alpha\beta) &= N((ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= |(ac + 2bd)^2 - 2(ad + bc)^2| \\ &= |(ac)^2 + 4(bd)^2 + 4abcd - 2(ad)^2 - 2(bc)^2 - 4abcd| \\ &= |a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2)| \\ &= |(a^2 - 2b^2)||(c^2 - 2d^2)| \\ &= N(\alpha)N(\beta) \end{aligned}$$

Thus, N is multiplicative. Also note that $N(r) \geq 0$, $r \in \mathbb{Q}[\sqrt{2}]$ and that $N(r) = 0$ iff $r = 0$ (this is easiest seen by noting that $N(a + b\sqrt{2}) = |(a + b\sqrt{2})(a - b\sqrt{2})|$ and then noting that we are in an integral domain).
Let $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$, $\alpha, \beta \neq 0$. Since $\beta \neq 0$, $\frac{\alpha}{\beta} = x + y\sqrt{2}$ for some $x, y \in \mathbb{Q}$ (obtained by "rationalizing the denominator").

Choose integers a, b closest to x and y repsectively, i.e such that $|x - a| \leq \frac{1}{2}$ and $|y - b| \leq \frac{1}{2}$. Then

$$\alpha = (a + b\sqrt{2})\beta + [(x - a) + (y - b)\sqrt{2}]\beta$$

so if we take $\gamma = a + b\sqrt{2}$ and $\delta = [(x - a) + (y - b)\sqrt{2}]\beta$, we have

$$\alpha = \gamma\beta + \delta$$

Furthermore, as $a, b \in \mathbb{Z}$, this implies $\gamma \in \mathbb{Z}[\sqrt{2}]$ and

$$\begin{aligned} \delta &= [(x - a) + (y - b)\sqrt{2}]\beta \\ &= (x + y\sqrt{2})\beta - (a + b\sqrt{2})\beta \\ &= \alpha - (a + b\sqrt{2})\beta \end{aligned}$$

Thus, as $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ and $a, b \in \mathbb{Z}$ we have that $\delta \in \mathbb{Z}[\sqrt{2}]$.
It remains to show that $N(\delta) < N(\beta)$. We have that

$$\begin{aligned} N(\delta) &= N([(x - a) + (y - b)\sqrt{2}]\beta) \\ &= N([(x - a) + (y - b)\sqrt{2})N(\beta) \\ &= |(x - a)^2 - 2(y - b)^2|N(\beta) \\ &\leq \left| \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 \right| N(\beta) \\ &= \frac{3}{4}N(\beta) \\ &< N(\beta) \end{aligned}$$

as required. Thus, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain and hence a PID which further implies that it is a UFD.

Suppose p is a prime such that $p \equiv \pm 1 \mod 8$. By the quadratic reciprocity law then $\exists a \in \mathbb{Z}$ such that

$$\begin{aligned} & a^2 \equiv 2 \mod p \\ \Rightarrow \quad & a^2 - 2 \equiv 0 \mod p \end{aligned}$$

Thus, $p|a^2 - 2$ in $\mathbb{Z}$. This implies that $p|(a+\sqrt{2})(a-\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}]$. If p were a prime in $\mathbb{Z}[\sqrt{2}]$ this would imply that p divides $a+\sqrt{2}$ or $a-\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ which is clearly absurd (as $p \nmid \pm 1$). Hence, if $p \equiv \pm 1 \mod 8$ then p is not a prime in $\mathbb{Z}[\sqrt{2}]$.

Let p be as just stated. We have shown that $\mathbb{Z}[\sqrt{2}]$ is a UFD, hence if we have a non-unit, non-zero element in $\mathbb{Z}[\sqrt{2}]$ that is not prime then it is reducible. Further note that $u \in \mathbb{Z}[i]$ is a unit iff $N(u) = 1$, (this again follows by the multiplicative nature of N and the fact that $N(1) = 1$), where N is as defined earlier. Hence, we have that p is not prime and as $N(p) = p^2$ it is also a non-zero, non-unit in $\mathbb{Z}[\sqrt{2}]$. Thus, it is reducible in $\mathbb{Z}[\sqrt{2}]$ i.e there exist $a, b, c, d \in \mathbb{Z}$ such that

$$p = (a + b\sqrt{2})(c + d\sqrt{2})$$

where $a + b\sqrt{2}$ and $c + d\sqrt{2}$ are not units. Applying the map N we obtain that

$$p^2 = |(a^2 - 2b^2)||(c^2 - 2d^2)|$$

As $a+b\sqrt{2}$ and $c+d\sqrt{2}$ are not units, $a^2 - 2b^2 \neq \pm 1$ and $c^2 - 2d^2 \neq \pm 1$. Thus by unique factorization in $\mathbb{Z}$ we have that $p = \pm(a^2 - 2b^2)$ as required. If $p = -(a^2 - 2b^2)$ then

$$\begin{aligned} (a+2b)^2 - 2(a+b)^2 &= a^2 + 4ab + 4b^2 - 2a^2 - 2b^2 - 4ab \\ &= -a^2 + 2b^2 \\ &= p \end{aligned}$$

Thus we have shown that if p is an odd prime in $\mathbb{Z}$ then, $p \equiv \pm 1 \mod 8$ iff $p = x^2 - 2y^2$ for some $x, y \in \mathbb{Z}$. (Note that $2 = (2)^2 - 2(1)^2$ and is thus also representable in this way).

For the second half of the problem, note that if $7 = a^2 - 2b^2$ then

$$\begin{aligned} (3a+4b)^2 - 2(2a+3b)^2 &= 9a^2 + 16b^2 + 24ab - 8a^2 - 18b^2 - 24ab \\ &= a^2 - 2b^2 \\ &= 7 \end{aligned}$$

This allows us to define an infinite family of representations $\{a_i - 2b_i^2\}_{i \in \mathbb{N}}$ for 7 given by $a_1 = 3$, $b_1 = 1$, $a_{i+1} = (3a_i + 4b_i)$ and $b_{i+1} = (2a_i + 3b_i)$, $i \in \mathbb{N}$. Note that if $a_i, b_i > 0$ then $a_{i+1} > a_i$ and $b_{i+1} > b_i$. Given our particular choice of a_1 and b_1 this then clearly shows that $\{a_i\}_{i \in \mathbb{N}}$ and $\{b_i\}_{i \in \mathbb{N}}$ form strictly increasing sequences, hence giving us an infinite family.

□

Solution 3.

We claim that 7 is a prime as required in the problem. First note that

$$(7)(2) = (3 + \sqrt{-5})(3 - \sqrt{-5})$$

Thus, $7|(3+\sqrt{-5})(3-\sqrt{-5})$, but $7 \nmid (3 \pm \sqrt{-5})$ (as otherwise $\exists x, y \in \mathbb{Z}$ such that $7(x+y\sqrt{-5}) = 3 \pm \sqrt{-5}$ which would imply that $7|3$ in $\mathbb{Z}$, which is absurd). Now to see that 7 cannot be represented as a^2+5b^2 notice that if it could be then

$$\begin{aligned} 7 &\equiv a^2+5b^2 \mod 5 \\ \Rightarrow 2 &\equiv a^2 \mod 5 \end{aligned}$$

which is not possible as $x^2 \equiv 0$ or $\pm 1 \mod 5$ for $x \in \mathbb{Z}$ $\square$