Thank you for another very detailed solution, well done! A+

Algebra and Number Theory

35) Let $R = \mathbb{Z}[\sqrt{2}]$

i) Then $u = 1-\sqrt{2}$ is a unit in R since $1-\sqrt{2}, -1-\sqrt{2} \in R$ as $1, -1 \in \mathbb{Z}$, and we have:

$$\begin{aligned}(1-\sqrt{2})(-1-\sqrt{2}) &= (1\times -1 + 2\times -1\times -1) + (1\times -1 - 1\times -1)\sqrt{2} \\ &= 1 + 0\sqrt{2} \\ &= 1_R\end{aligned}$$ ✓

Since R is commutative — it is a subring of the field $\mathbb{R}$ which is (necessarily) commutative — we get:

$$(1-\sqrt{2})(-1-\sqrt{2}) = (-1-\sqrt{2})(1-\sqrt{2}) = 1_R$$

So there exists $v = -1-\sqrt{2} \in R$ such that for $u = 1-\sqrt{2} \in R$, we have

$$uv = vu = 1_R$$

as is required for u to be a unit in R, so u is a unit. ✓

The norm map $N: R \to \mathbb{Z}$ is defined by $a+b\sqrt{2} \longmapsto a^2-2b^2$, note that a^2-2b^2 is indeed an integer since $2, a, b \in \mathbb{Z}$, and $\mathbb{Z}$ is a ring. (The norm map was shown, in Question 12, to be well defined and to preserve multiplication)

To show that $\alpha \in R$ is a unit if and only if $N(\alpha) = \pm 1$, we need to show that α is a unit $\Rightarrow N(\alpha) = \pm 1$, and that $N(\alpha) = \pm 1 \Rightarrow \alpha$ is a unit. ✓

Let $\alpha = a + b\sqrt{2} \in R$, with $a, b \in \mathbb{Z}$

— α is a unit $\Rightarrow N(\alpha) = \pm 1$:

Suppose α is a unit, then there exists $\beta \in R$ such that:

$$\alpha\beta = \beta\alpha = 1_R$$

Applying N to this gives:

$$\begin{aligned} & N(\alpha\beta) = N(\beta\alpha) = N(1+0\sqrt{2}) \quad ; \text{ since } 1_R = 1+0\sqrt{2} \\ \Rightarrow\ & N(\alpha\beta) = N(\beta\alpha) = 1^2 - 2\cdot 0^2 \\ \Rightarrow\ & N(\alpha)N(\beta) = N(\beta)N(\alpha) = 1 \quad ; \text{ since } N \text{ preserves multiplication.}\end{aligned}$$ ✓

As $N(\alpha), N(\beta)$ are integers, we have that $N(\alpha)$ is a unit in $\mathbb{Z}$ since it satisfies the definition of a unit of $\mathbb{Z}$

The only units of $\mathbb{Z}$ are $1, -1$, so we must then have $N(\alpha) = \pm 1$ ✓ good.

So: α is a unit $\Rightarrow N(\alpha) = \pm 1$.

— $N(\alpha) = \pm 1 \Rightarrow \alpha$ is a unit:

Suppose $N(\alpha) = \pm 1$, this implies that $a^2 - 2b^2 = \pm 1$

Now consider $\beta = \pm(a - b\sqrt{2})$, where the sign matches that of $N(\alpha)$. Clearly β is in R since $\pm a, \pm b \in \mathbb{Z}$.

Then calculate:

$$\begin{aligned}
\alpha\beta &= (a + b\sqrt{2})(\pm(a - b\sqrt{2})) \\
&= \pm(a + b\sqrt{2})(a - b\sqrt{2}) \\
&= \pm((a \times a + 2 \times b \times -b) + (a \times -b + b \times a)\sqrt{2}) \\
&= \pm((a^2 - 2b^2) + 0\sqrt{2}) \\
&= \pm(\pm 1 + 0\sqrt{2}) \quad ; \text{ since } a^2 - 2b^2 = \pm 1 \\
&= 1 + 0\sqrt{2} \\
&= 1_R
\end{aligned}$$

So we have that for α with $N(\alpha) = \pm 1$, there exists $\beta \in R$ with:

$$\alpha\beta = \beta\alpha = 1_R$$

since R is commutative.

Thus α is a unit.

So: $N(\alpha) = \pm 1 \Rightarrow \alpha$ is a unit. ✓

Finally we have: α is a unit $\Leftrightarrow N(\alpha) = \pm 1$, for $\alpha \in R$.

✓

Algebra and Number Theory

ii) The elements $\pm u^n$ for $n \in \mathbb{Z}$ are indeed units of R:

If α is a unit of R, and $n \in \mathbb{Z}$, then:

For $n = 0$, $\alpha^n = \alpha^0 = 1_R$, which is a unit since $1_R \times 1_R = 1_R$.

If $n > 0$, then $N(\alpha^n) = N(\alpha)^n = (\pm 1)^n = 1$ or -1, depending on the sign of $N(\alpha)$ and on n, since N preserves multiplication and $N(\alpha) = \pm 1$ since α is a unit. So $N(\alpha^n) = \pm 1$, and so α^n is a unit of R by the previous part. ✓

If α is a unit of R, then α^{-1} — this exists since a unit is defined to be an element which has a multiplicative inverse — is also a unit of R since $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1_R$. So for $n < 0$, $\alpha^n = (\alpha^{-1})^{-n}$, which is a unit of R since α^{-1} is a unit and $-n > 0$, using the above. ✓

So α^n is a unit for any $n \in \mathbb{Z}$

If α is a unit of R, then $-\alpha$ is a unit since $(-\alpha)(-\alpha^{-1}) = (-\alpha^{-1})(-\alpha) = \alpha^{-1}\alpha = 1_R$.

So $\pm\alpha^n$ is a unit for any $n \in \mathbb{Z}$

So $\pm u^n$ is a unit for any $n \in \mathbb{Z}$ since $u = 1 - \sqrt{2}$ is a unit of R. ✓ good.

To show these elements are distinct, we must show that if $\pm u^n = \pm u^m$ for some $m, n \in \mathbb{Z}$, then $m = n$, and the signs match.

Suppose $\pm u^n = \pm u^m$, for some $m, n \in \mathbb{Z}$.

Since u^n is a unit, u^{-n} exists. Multiply both sides by u^{-n} to get:

$$\pm 1_R = \pm u^{m-n}.$$

Since $R \subseteq \mathbb{R}$, consider the above equality in $\mathbb{R}$, where $1_R = 1 + 0\sqrt{2} = 1$.

$$\pm 1 = \pm u^{m-n}$$

Take the absolute value of both sides:

$$|\pm 1| = |\pm u^{m-n}|$$
$$\Rightarrow 1 = |u^{m-n}|$$
$$\Rightarrow 1 = |u|^{m-n}$$

Since $u = 1 - \sqrt{2}$ satisfies $-1 < u < 0$ since $1 < \sqrt{2} < 2$, then $0 < |u| < 1$, so that $|u| \neq 1$.

Since $1 = |u|^{m-n}$ and $|u| \neq 1 \Rightarrow m - n = 0$, so $m = n$ in $\mathbb{R}$, and hence we must have $m = n$ in R as well. ✓

Now we have $m = n$, return to the original equality

$$\pm u^n = \pm u^m$$

Multiply both sides by $u^{-n} = u^{-m}$, to get

$$\pm 1_R = \pm 1_R.$$

Since $1_R = 1 + 0\sqrt{2} \neq -1 + 0\sqrt{2} = -1_R$ in R, we must have that this equality is either:

$$1_R = 1_R \quad \text{or} \quad -1_R = -1_R,$$

So that the sign on both sides of the equality matches.

Hence we have that if $\pm u^n = \pm u^m$ for some $m, n \in \mathbb{Z}$, then $m = n$ and the signs match, so that each $\pm u^n$ is distinct. ✓

Since n can run through the integers taking infinitely many values and each $\pm u^n$ is a distinct unit, R must have infinitely many units.

So R^*, the units of R, has infinitely many elements.

✓ Excellent.

Algebra and Number Theory

iii) Following the directions of the hint...

If (a,b) is a solution in integers of $x^2 - 2y^2 = \pm 1$, with $a > 1$, $b > 1$, then $a^2 - 2b^2 = \pm 1$.

Now $(a', b') = (2b - a, a - b)$ is another solution of $x^2 - 2y^2 = \pm 1$, since:

$$\begin{aligned} a'^2 - 2b'^2 &= (2b-a)^2 - 2(a-b)^2 \\ &= (4b^2 - 4ab + a^2) - 2(a^2 - 2ab + b^2) \\ &= 4b^2 - 4ab + a^2 - 2a^2 + 4ab - 2b^2 \\ &= 2b^2 - a^2 \\ &= -(a^2 - 2b^2) \\ &= -(\pm 1) \\ &= \mp 1 \end{aligned}$$ ✓

Note that this is a sdution in integers since $a, b \in \mathbb{Z}$ so that $a' = 2b - a$, $b' = a - b$ are also integers.

This solution has: $0 < a' < a$, $0 < b' < b$, since:

$$\begin{aligned} & 0 < a' < a \\ \iff\ & 0 < 2b - a < a \\ \iff\ & a < 2b < 2a \end{aligned}$$ ✓

and:

$$\begin{aligned} & 0 < b' < b \\ \iff\ & 0 < a - b < b \\ \iff\ & b < a < 2b \end{aligned}$$ ✓

And these inequalities hold since:

$$\begin{aligned} & a < 2b \\ \iff\ & a^2 < 4b^2 && \text{as } a \text{ and } b \text{ are positive by assumption} \\ \iff\ & a^2 < 2(2b^2) \\ \iff\ & a^2 < 2(a^2 \mp 1) && \text{since } a^2 - 2b^2 = \pm 1, \text{ above} \\ \iff\ & -a^2 < \mp 2 \\ \iff\ & a^2 > \pm 2 \end{aligned}$$

But a is an integer, and $a > 1 \Rightarrow a \geq 2 \Rightarrow a^2 \geq 4 > \pm 2$
So $a < 2b$ ✓

and:

$$
\begin{aligned}
& b < a \\
\iff\ & b^2 < a^2 && \text{as } a \text{ and } b \text{ are positive} \\
\iff\ & b^2 < 2b^2 \pm 1 && \text{as } a^2 - 2b^2 = \pm 1 \\
\iff\ & -b^2 < \pm 1 \\
\iff\ & b^2 > \mp 1
\end{aligned}
$$

But $b > 1 \Rightarrow b^2 > 1 \geq \mp 1$, so $b < a$ and $2b < 2a$ ✓

So as required if (a, b) is a solution of $X^2 - 2Y^2 = \pm 1$, with $a > 1$, $b > 1$, then $(a', b') = (2b - a, a - b)$ is also a solution with $0 < a' < a$, $0 < b' < b$, with a, b, a', b' integers.

For any integral solution with $a > 1$, $b > 1$ we can keep iterating down to new integral solutions with smaller a and b, until at least one of a, b equals 1, and both one greater than 0. ✓

If $a = 1$, then $a^2 - 2b^2 = \pm 1 \Rightarrow 2b^2 = a^2 \mp 1$
$\Rightarrow 2b^2 = 1^2 \mp 1 = 0, 2 \Rightarrow b^2 = 0, 1 \Rightarrow b = 1$
since we discount the solution $b = 0$.

If $b = 1$, then $a^2 - 2b^2 = \pm 1 \Rightarrow a^2 = 2b^2 \pm 1$
$\Rightarrow a^2 = 2 \cdot 1^2 \pm 1 = 1, 3 \Rightarrow a = 1$ since $a = \sqrt{3}$ is not an integer.

So the smallest solution with $a > 0$, $b > 0$ is $a = b = 1$, ✓ giving:

$$1^2 - 2 \times 1^2 = -1.$$

Note that, from the first part, any $a + b\sqrt{2} \in R$ such that (a, b) is a solution of this equation is a unit, and that any unit can be written as $a + b\sqrt{2} \in R$ such that (a, b) solves this equation.

Note that:

$$
\begin{aligned}
(a + b\sqrt{2})(-u) &= (a + b\sqrt{2})(-1 + \sqrt{2}) \\
&= (a \times -1 + 2 \times b \times 1) + (a \times 1 + b \times -1)\sqrt{2} \\
&= (2b - a) + (a - b)\sqrt{2}
\end{aligned}
$$

So the process of iterating down to a smaller solution of the equation corresponds to taking a unit $\alpha = a + b\sqrt{2}$ and multiplying it by $-u$ to get a new unit $\alpha' = a' + b'\sqrt{2}$ with a' and b' positive but strictly smaller than a and b respectively.

Algebra and Number Theory

Note also that the solution $a=b=1$, corresponds to the unit $1+\sqrt{2} = -(-1-\sqrt{2}) = -u^{-1}$, from part one. ✓

Now we will use this to show that any unit can be written in the form $\pm u^n$ for some $n \in \mathbb{Z}$.

Working through the cases for $a+b\sqrt{2}$ a unit.

Case 1: $a = 0$

If $a=0$, then $a^2 - 2b^2 = \pm 1 \Rightarrow 2b^2 = 0^2 \mp 1$
$\Rightarrow b^2 = \mp\left(\frac{1}{2}\right)$

In either case b is not an integer, so there are no units with $a=0$ ✓

Case 2: $b = 0$

If $b=0$, then $a^2 - 2b^2 = \pm 1 \Rightarrow a^2 = 2\cdot 0^2 \pm 1$
$\Rightarrow a^2 = \pm 1 \Rightarrow a = \pm 1$ since the square of an integer must be non-negative

So the possible units are $1 + 0\sqrt{2} = u^0$, and $-1 + 0\sqrt{2} = -u^0$.

In either case they are writable in the form $\pm u^n$ for $n \in \mathbb{Z}$. ✓

Case 3: $a > 0$, $b > 0$

Iterate down to smaller solutions as many times as necessary until the solution $a=b=1$ is reached. If m iterations are required, then:

$$(a+b\sqrt{2})(-u)^m = -u^{-1}$$

So that:

$$\begin{aligned} a+b\sqrt{2} &= -u^{-1}\cdot(-u)^{-m} \\ &= -1^{-1}\cdot -1^{-m}\cdot u^{-1}\cdot u^{-m} \\ &= -1^{(-1-m)}\cdot u^{-1-m} \\ &= \pm u^{-1-m}, \text{ depending on } m. \end{aligned}$$

In either case $a+b\sqrt{2} = \pm u^n$, for some appropriate $n = -1-m$ in $\mathbb{Z}$. ✓

Case 4: $a > 0$, $b < 0$

Then $(a, -b)$ is a solution to the equation with $a > 0$, $-b > 0$. By case 3 we can write:

$$a - b\sqrt{2} = \pm u^m, \text{ for some } m \in \mathbb{Z}.$$

But from part one, we have that:

$$(a + b\sqrt{2})(\pm(a - b\sqrt{2})) = 1$$

So that $a + b\sqrt{2} = \pm(a - b\sqrt{2})^{-1}$, where the sign is not necessarily the same as above.

Now we can write:

$$\begin{aligned} a + b\sqrt{2} &= \pm(\pm u^m)^{-1} \\ &= \pm u^{-m}, \text{ using the above} \end{aligned}$$

So $a + b\sqrt{2} = \pm u^n$ for some $n \in \mathbb{Z}$. ✓

Case 5: $a < 0$, $b > 0$

Then $(-a, -b)$ is a solution with $-a > 0$, $-b < 0$

So $-a - b\sqrt{2} = \pm u^m$, for some $m \in \mathbb{Z}$ by case 4.

And $a + b\sqrt{2} = -(-a - b\sqrt{2}) = \mp u^m$, for some $m \in \mathbb{Z}$.

So $a + b\sqrt{2} = \pm u^n$, for some $n \in \mathbb{Z}$.

Case 6: $a < 0$, $b < 0$

Then $(-a, -b)$ is a solution with $-a > 0$, $-b > 0$

So $-a - b\sqrt{2} = \pm u^m$, for some $m \in \mathbb{Z}$ by case 3.

And $a + b\sqrt{2} = -(-a - b\sqrt{2}) = \mp u^m$, for some $m \in \mathbb{Z}$.

So $a + b\sqrt{2} = \pm u^n$, for some $n \in \mathbb{Z}$

Combining all these cases shows that any unit $a + b\sqrt{2}$ can be written as $\pm u^n$ for some $n \in \mathbb{Z}$ so the units of the previous part are all units of R. ✓ Excellent!