Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 3

B3.3: Algebraic Number Theory

28 February, 2021

Topics covered: factorisation of ideals.

Remark. To avoid confusion, the ideal generated by the subset S will be denoted by $\langle S\rangle$ instead of (S) throughout this problem sheet.

Question 1

Prove that the equivalence relation defined in the lectures on the set of non-zero ideals is indeed an equivalence relation.

Proof. For $I, J \lhd \mathcal{O}_K$,

$$I \sim J \iff \exists \alpha, \beta \in \mathcal{O}_K \; I\langle\alpha\rangle = J\langle\beta\rangle$$

- Reflexivity: $I = I\langle 1\rangle \sim I\langle 1\rangle$.
- Symmetry: Obvious from definition.
- Transitivity: Suppose that $I \sim J$ and $J \sim K$. There exists $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$ such that $I\langle\alpha\rangle = J\langle\beta\rangle$ and $J\langle\gamma\rangle = K\langle\delta\rangle$. Then

A

$$I\langle\alpha\gamma\rangle = I\langle\alpha\rangle\langle\gamma\rangle = J\langle\beta\rangle\langle\gamma\rangle = K\langle\delta\rangle\langle\beta\rangle = K\langle\beta\delta\rangle$$

  Hence $I \sim K$.

We conclude that $\sim$ is an equivalence relation. □

Question 2

Let P be a prime ideal of $\mathcal{O}_K$, the ring of integers of a number field K. Show that if $\alpha \in P, \alpha \neq 0$, is chosen so that $\left|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)\right|$ is minimal, then α is an irreducible element. Deduce that if $\mathcal{O}_K$ is a UFD then every prime ideal is principal, and so $\mathcal{O}_K$ is a PID.

Proof. Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathcal{O}_K$. Since P is prime, we have $\beta \in P$ or $\gamma \in P$. Without loss of generality let $\beta \in P$. Since the norm is multiplicative, we have

$$\left|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\right| = \left|\mathrm{Norm}_{K|\mathbb{Q}}(\beta)\right|\left|\mathrm{Norm}_{K|\mathbb{Q}}(\gamma)\right| \implies \left|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\right| \geqslant \left|\mathrm{Norm}_{K|\mathbb{Q}}(\beta)\right|$$

A

By minimality of the norm of α, we must have

$$\left|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\right| = \left|\mathrm{Norm}_{K|\mathbb{Q}}(\beta)\right| \implies \left|\mathrm{Norm}_{K|\mathbb{Q}}(\gamma)\right| = 1$$

Hence γ is a unit in $\mathcal{O}_K$. We deduce that α is irreducible.

Suppose that $\mathcal{O}_K$ is a UFD. Then α is also a prime. In particular $\langle\alpha\rangle$ is a prime ideal contained in P. Since $\mathcal{O}_K$ is integral over $\mathbb{Z}$, $\langle\alpha\rangle \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. But since $\mathbb{Z}$ is a PID, $\langle\alpha\rangle \cap \mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, and hence $\langle\alpha\rangle$ is a maximal ideal of $\mathcal{O}_K$. We must have $\langle\alpha\rangle = P$. P is a principal ideal. (*The ring of integers has Krull dimension 1.*)

Next we shall present a proof, which is valid for general integral domains, that the condition that all prime ideals are principal implies that $\mathcal{O}_K$ is a PID.

Suppose for contradiction that $\mathcal{O}_K$ is not a PID. Let S be the set of all non-principal ideals of $\mathcal{O}_K$. By assumption $S \neq \varnothing$. For an ascending chain $\{I_j : j \in J\} \subseteq S$, it is clear that $I := \bigcup\{I_j : j \in J\}$ is an ideal of $\mathcal{O}_K$. Suppose that $I = \langle x\rangle$ for some $x \in \mathcal{O}_K$. Then $x \in I_j$ for some $j \in J$ and hence $I = \langle x\rangle \subsetneq I_j$, which is a contradiction. Hence $I \in S$. Now Zorn's lemma suggests that S has a maximal element Q. We claim that Q is prime.

Suppose that Q is not prime. Then there exists $a, b \in \mathcal{O}_K$ such that $ab \in Q$ and $a, b \notin Q$. Note that $Q + \langle a\rangle$ contains Q and a, and hence is principal by maximality of Q in S. There exists $c \in \mathcal{O}_K$ such that $Q + \langle a\rangle = \langle c\rangle$. Also, note that the ideal quotient $(Q : \langle a\rangle) := \{r \in \mathcal{O}_K : \; ra \in Q\}$ contains Q and b, and hence is also principal. There exists $d \in \mathcal{O}_K$ such that $(Q : \langle a\rangle) = \langle d\rangle$. We claim that $Q = \langle cd\rangle$.

Since $(Q : \langle a\rangle) = \langle d\rangle$, we have $d \in (Q : \langle a\rangle)$ and hence $ad \in Q$. Since $Q + \langle a\rangle = \langle c\rangle$, there exists $q \in Q$ and $r \in R$ such that $c = q + ra$. Then $cd = qd + rad \in Q$. $\langle cd\rangle \subseteq Q$. On the other hand, consider $s \in Q$. Since $Q \subseteq \langle c\rangle$, there exists $t \in R$ such that $s = tc$. Since $a \in \langle c\rangle$, there exists $u \in R$ such that $a = uc$. Then $ts = utc = ua \in Q$. We have $u \in (Q : \langle a\rangle) = \langle d\rangle$. Then there exists $v \in R$ such that $t = vd$. We have $s = tc = vcd \in \langle cd\rangle$. Hence $Q \subseteq \langle cd\rangle$. We deduce that $Q = \langle cd\rangle$ is a principal.

But $Q \in S$, which is a contradiction. Hence Q is a prime ideal. But by assumption, every prime ideal is principal, which is also a contradiction. We must have $S = \varnothing$. We conclude that $\mathcal{O}_K$ is a PID.

(*Alternatively, we can invoke the prime decomposition and write the proof in one line. However this is uninteresting...*) □

Nice!

Question 3

The rings $\mathbb{Z}[\sqrt{6}]$ and $\mathbb{Z}[\sqrt{7}]$ are PIDs. Exhibit generators for their ideals $(3, \sqrt{6}), (5, 4+\sqrt{6}), (2, 1+\sqrt{7})$

[*Hint: Compute the norm of each of the given ideals of the form* (p, α) *and find an element* $\beta \in \mathcal{O}_K$ *of suitable norm.*]

Proof.

- The first one is simple. By direct observation we claim that $\langle 3, \sqrt{6}\rangle = \langle 3+\sqrt{6}\rangle$.

  It is clear that $3+\sqrt{6} \in \langle 3, \sqrt{6}\rangle$. On the other hand, we observe that $3 = (3+\sqrt{6})(3-\sqrt{6})$ and $\sqrt{6} = (3+\sqrt{6}) - 3$. Hence $3, \sqrt{6} \in \langle 3+\sqrt{6}\rangle$.

- Suppose that $\langle 5, 4+\sqrt{6}\rangle = \langle a+b\sqrt{6}\rangle$ for some $a, b \in \mathbb{Z}$. We can compute the norms:

A

$$\mathrm{Norm}(5) = 25, \qquad \mathrm{Norm}(4+\sqrt{6}) = 10, \qquad \mathrm{Norm}(a+b\sqrt{6}) = a^2 - 6b^2$$

  Hence $a^2 - 6b^2 \mid \gcd(25, 10) = 5$. Since $\langle a+b\sqrt{6}\rangle \neq \mathbb{Z}[\sqrt{6}]$, we deduce that $a^2 - 6b^2 = \pm 5$.

  We try $a+b\sqrt{6} = 1-\sqrt{6}$. Note that $1-\sqrt{6} = 5-(4+\sqrt{6}) \in \langle 5, 4+\sqrt{6}\rangle$. On the other hand, we observe that $5 = (1-\sqrt{6})(-1-\sqrt{6})$ and $4+\sqrt{6} = 5-(1-\sqrt{6})$. Hence $\langle 5, 4+\sqrt{6}\rangle \subseteq \langle 1-\sqrt{6}\rangle$. We deduce that $\langle 5, 4+\sqrt{6}\rangle = \langle 1-\sqrt{6}\rangle$.

- Suppose that $\langle 2, 1+\sqrt{7}\rangle = \langle a+b\sqrt{7}\rangle$ for some $a, b \in \mathbb{Z}$. We can compute the norms:

$$\mathrm{Norm}(2) = 4, \qquad \mathrm{Norm}(1+\sqrt{7}) = -6, \qquad \mathrm{Norm}(a+b\sqrt{6}) = a^2 - 7b^2$$

  Hence $a^2 - 7b^2 \mid \gcd(4, -6) = 2$. Since $\langle a+b\sqrt{7}\rangle \neq \mathbb{Z}[\sqrt{7}]$, we deduce that $a^2 - 6b^2 = \pm 2$.

  We try $a+b\sqrt{7} = 3+\sqrt{7}$. Note that $2 = (3+\sqrt{7})(3-\sqrt{7})$ and $1+\sqrt{7} = 2+(3+\sqrt{7})$. we deduce that $\langle 2, 1+\sqrt{7}\rangle = \langle 3+\sqrt{7}\rangle$. □

Question 4

Find the prime factorisations of the ideals (3),(5) and (7) in $\mathbb{Z}[\sqrt{-5}]$. Show that the prime ideal factors of (7) are not principal.

Proof. We follow the procedure outlined in Example 7.4.

For prime $p \in \mathbb{Z}$, by prime factorisation, there are three possible cases:

A

$$\langle p\rangle = \begin{cases} P & P \in \mathrm{Spec}(\mathbb{Z}[\sqrt{-5}]); & (p \text{ inert}) \\ P^2 & P \in \mathrm{Spec}(\mathbb{Z}[\sqrt{-5}]); & (p \text{ ramifies}) \\ PQ & P, Q \in \mathrm{Spec}(\mathbb{Z}[\sqrt{-5}]),\ P \neq Q; & (p \text{ splits}) \end{cases}$$

The minimal polynomial of $\sqrt{-5}$ over $\mathbb{Q}$ is $m(x) = x^2 + 5$.

- When $p = 3$, we have $m(x) \equiv x^2 - 1 \equiv (x+1)(x-1) \bmod 3$. By Theorem 7.2, we have $\langle 3\rangle = \langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle$.
- When $p = 5$, we have $m(x) \equiv x^2 \bmod 5$. By Theorem 7.2, we have $\langle 5\rangle = \langle 5, \sqrt{-5}\rangle^2 = \langle \sqrt{-5}\rangle^2$.
- When $p = 7$, we have $m(x) \equiv x^2 - 2 \equiv (x+3)(x-3) \bmod 7$. By Theorem 7.2, we have $\langle 7\rangle = \langle 7, 3+\sqrt{-5}\rangle\langle 7, 3-\sqrt{-5}\rangle$. We shall show that $\langle 7, 3\pm\sqrt{-5}\rangle$ are non-principal. Suppose that they are principal. Then there exists $a, b \in \mathbb{Z}$ such that $\langle a+b\sqrt{-5}\rangle = \langle 7, 3\pm\sqrt{-5}\rangle$. The norms

$$\mathrm{Norm}(a+b\sqrt{5}) = a^2 + 5b^2, \qquad \mathrm{Norm}(7) = 49, \qquad \mathrm{Norm}(3\pm\sqrt{-5}) = 14$$

  Hence we must have $a^2 + 5b^2 = \gcd(49, 14) = 7$. It is clear that the equation has no integer solutions. Hence the prime factors $\langle 7, 3\pm\sqrt{-5}\rangle$ are non-principal. □

Question 5

Let $K \subseteq L$ be fields and let I be an ideal of $\mathscr{O}_K$. Define $I\cdot\mathscr{O}_L$ to be the ideal of $\mathscr{O}_L$ generated by the products $i\ell$, such that $i \in I, \ell \in \mathscr{O}_L$. Show that, for any ideals I, J of $\mathscr{O}_K$, any $n \in \mathbb{N}$ and any principal ideal $(a) = a\mathscr{O}_K$ of $\mathscr{O}_K$, $(IJ)\cdot\mathscr{O}_L = (I\cdot\mathscr{O}_L)(J\cdot\mathscr{O}_L)$, $I^n\cdot\mathscr{O}_L = (I\cdot\mathscr{O}_L)^n$ and $(a)\cdot\mathscr{O}_L = a\mathscr{O}_L$ (the principal ideal of $\mathscr{O}_L$ generated by the same element). Let $K = \mathbb{Q}(\sqrt{-13})$ and let $I = (2, \sqrt{-13}+1)$. Show that $I^2 = (2)$ and that I is not principal. Let $L = \mathbb{Q}(\sqrt{-13}, \sqrt{2})$. Show that $I\cdot\mathscr{O}_L$ is the principal ideal of $\mathscr{O}_L$ generated by $\sqrt{2}$ (we say that I has been *made principal* in the extension).

Proof. $I \mapsto I\cdot\mathscr{O}_L$ is the *ideal extension* under the ring extension $\mathscr{O}_K \to \mathscr{O}_L$.

Suppose that $I, J \lhd \mathscr{O}_K$. The elements in $(IJ)\cdot\mathscr{O}_L$ are of the form $\sum_{k=1}^{n} i_k j_k \ell$ for some $i_1, \ldots, i_n \in I$, $j_1, \ldots, j_n \in J$ and $\ell \in \mathscr{O}_L$. Each $i_k j_k \ell \in (I\cdot\mathscr{O}_L)(J\cdot\mathscr{O}_L)$. Hence $\sum_{k=1}^{n} i_k j_k \ell \in (I\cdot\mathscr{O}_L)(J\cdot\mathscr{O}_L)$. On the other hand, the elements of $(I\cdot\mathscr{O}_L)(J\cdot\mathscr{O}_L)$ are of the form $\sum_{k=1}^{n} i_k \ell_k j_k m_k$ for some $i_1, \ldots, i_n \in I$, $j_1, \ldots, j_n \in J$ and $\ell_1, \ldots, \ell_n, m_1, \ldots, m_n \in \mathscr{O}_L$. It is clear that $\sum_{k=1}^{n} i_k \ell_k j_k m_k \in (IJ)\cdot\mathscr{O}_L$. We deduce that $(IJ)\cdot\mathscr{O}_L = (I\cdot\mathscr{O}_L)(J\cdot\mathscr{O}_L)$.

Next, by induction on n, we have $(I\cdot\mathscr{O}_L)^n = I^n\cdot\mathscr{O}_L$ for each $n \in \mathbb{N}$.

A

For $r \in a\mathscr{O}_L$, $r = a\ell$ for some $\ell \in \mathscr{O}_L$. Hence $r \in \langle a\rangle\,\mathscr{O}_L$. For $r \in \langle a\rangle\,\mathscr{O}_L$, $r = ak\ell$ for some $k \in \mathscr{O}_K$ and $\ell \in \mathscr{O}_L$. But $k\ell \in \mathscr{O}_L$. Hence $r \in a\mathscr{O}_L$. We deduce that $a\mathscr{O}_L = \langle a\rangle\,\mathscr{O}_L$.

Now $K = \mathbb{Q}(\sqrt{-13})$. Since $-13 \equiv 3 \bmod 4$, we have $\mathscr{O}_K = \mathbb{Z}[\sqrt{-13}]$. Let $I = \left\langle 2, 1+\sqrt{-13}\right\rangle_{\mathscr{O}_K}$. Suppose that I is principal. There exists $a, b \in \mathbb{Z}$ such that $I = \left\langle a + b\sqrt{-13}\right\rangle$. Note that $\mathrm{Norm}_{K|\mathbb{Q}}(a+b\sqrt{-13}) = a^2 + 13b^2$ divides $\mathrm{Norm}_{K|\mathbb{Q}}(2) = 4$ and $\mathrm{Norm}_{K|\mathbb{Q}}(1+\sqrt{-13}) = 14$. We must have $a^2 + 13b^2 = \pm 2$. But it is clear that the equation has no solution. I is not principal.

$$I^2 = \left\langle 2, 1+\sqrt{-13}\right\rangle_{\mathscr{O}_K}\left\langle 2, 1+\sqrt{-13}\right\rangle_{\mathscr{O}_K} = \left\langle 4, -12+2\sqrt{-13}, 2+2\sqrt{-13}\right\rangle_{\mathscr{O}_K} \subseteq \langle 2\rangle_{\mathscr{O}_K}$$

And $2 = 4\times 4 + (-12+2\sqrt{-13}) - (2+2\sqrt{-13})$. We deduce that $I^2 = \langle 2\rangle_{\mathscr{O}_K}$.

Let $L = \mathbb{Q}(\sqrt{-13}, \sqrt{2})$. Note that $2/\sqrt{2} = \sqrt{2} \in \mathscr{O}_L$, so $2 \in \left\langle\sqrt{2}\right\rangle_{\mathscr{O}_L}$. We claim that $\alpha := \dfrac{1+\sqrt{-13}}{\sqrt{2}} \in \mathscr{O}_L$. Indeed,

$$\alpha = \frac{1+\sqrt{-13}}{\sqrt{2}} \implies 2\alpha^2 = (1+\sqrt{-13})^2 = -12+2\sqrt{-13} \implies (\alpha^2+6)^2 = -13 \implies \alpha^4 + 12\alpha^2 + 49 = 0$$

Hence $1+\sqrt{-13} \in \left\langle\sqrt{2}\right\rangle_{\mathscr{O}_L}$. We deduce that $I\cdot\mathscr{O}_L \subseteq \left\langle\sqrt{2}\right\rangle_{\mathscr{O}_L}$. By Proposition 6.23, there exists $J \lhd \mathscr{O}_L$ such that $(I\cdot\mathscr{O}_L)J = \left\langle\sqrt{2}\right\rangle_{\mathscr{O}_L}$. But we know that $(I\cdot\mathscr{O}_L)^2 = \langle 2\rangle_{\mathscr{O}_L} = \left\langle\sqrt{2}\right\rangle_{\mathscr{O}_L}^2$. Hence $N(I\cdot\mathscr{O}_L) = N(\langle\sqrt{2}\rangle_{\mathscr{O}_L})$ by multiplicativity of the ideal norm. Hence $N(J) = 1$. We deduce that $J = \mathscr{O}_L$ and $I\cdot\mathscr{O}_L = \left\langle\sqrt{2}\right\rangle_{\mathscr{O}_L}$. □

Question 6

Let P, Q be distinct nonzero prime ideals in $\mathscr{O}_K$. Show that $P+Q = \mathscr{O}_K$ and $P \cap Q = PQ$.

A

Proof. In Question 2, we have shown that all non-zero prime ideals in $\mathscr{O}_K$ are maximal (by contracting the ideals to $\mathbb{Z}$). Therefore P and Q are distinct maximal ideals. Note that $P \subsetneq P+Q$. We must have $P+Q = \mathscr{O}_K$. Hence P and Q are coprime. There exists $p \in P$ and $q \in Q$ such that $p+q = 1$. For $x \in P\cap Q$, $x = xp + xq \in PQ$. Hence $P\cap Q \subseteq PQ$. The other direction $PQ \subseteq P\cap Q$ is immediate by definition. □

Question 7

Let $d \not\equiv 1 \bmod 4$ be a square-free integer and define $K := \mathbb{Q}(\sqrt{d})$; so $\mathscr{O}_K = \mathbb{Z}[\sqrt{d}]$. Let p be a rational prime. Suppose that $d \equiv a^2 \bmod p$. Define $P := (p, a+\sqrt{d}), P' := (p, a-\sqrt{d}) \subseteq \mathscr{O}_K$. Show that P and P' are both prime ideals with $N(P) = N(P') = p$, and that $(p) = PP'$. Show that $P = P'$ if and only if $p \mid 2d$.

Proof. This question can be answered directly by invoking the Dedekind Theorem (7.2). Here we mimic the proof to give a complete answer.

A

The minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$ is $m(x) = x^2 - d$. We have

$$x^2 - d \equiv x^2 - a^2 \equiv (x-a)(x+a) \bmod p$$

Consider the composition of ring homomorphisms $\varphi = \pi \circ \mathrm{ev}_{\sqrt{d}}$:

$$\mathbb{Z}[x] \xrightarrow{\mathrm{ev}_{\sqrt{d}}} \mathbb{Z}[\sqrt{d}] \xrightarrow{\pi} (\mathbb{Z}/p\mathbb{Z})[\sqrt{d}]$$

We note that $\ker\varphi = \langle p, m(x)\rangle$. By the first isomorphism theorem, we have

$$(\mathbb{Z}/p\mathbb{Z})[\sqrt{d}] \cong \frac{\mathbb{Z}}{\langle p, m(x)\rangle} \cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{\langle \overline{m}(x)\rangle} = \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{\langle (\overline{x}+\overline{a})(\overline{x}-\overline{a})\rangle}$$

where $\overline{m}(x)$ is the image of $m(x)$ under $\pi : \mathbb{Z}[x] \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})[x]$.

The prime ideals of $\dfrac{(\mathbb{Z}/p\mathbb{Z})[x]}{\langle (\overline{x}+\overline{a})(\overline{x}-\overline{a})\rangle}$ are $\langle \overline{x}+\overline{a}\rangle$ and $\langle \overline{x}-\overline{a}\rangle$, which corresponds to $\left\langle \sqrt{d}+a\right\rangle$ and $\left\langle \sqrt{d}-a\right\rangle$ in $(\mathbb{Z}/p\mathbb{Z})[\sqrt{d}]$. Contracting back to $\mathbb{Z}[\sqrt{d}]$, we find that $P = \left\langle p, a+\sqrt{d}\right\rangle$ and $P' = \left\langle p, a-\sqrt{d}\right\rangle$ are prime ideals of $\mathbb{Z}[\sqrt{d}]$.

Therefore

$$PP' = \left\langle p, a+\sqrt{d}\right\rangle \left\langle p, a-\sqrt{d}\right\rangle \subseteq \langle p, a^2-d\rangle = \langle p\rangle$$

Hence there exists $Q \lhd \mathbb{Z}[\sqrt{d}]$ such that $PP'Q = \langle p\rangle$. Taking norm:

$$p^2 = N(\langle p\rangle) = N(P)N(P')N(Q)$$

Since $N(P), N(P') \neq 1$, we must have $N(P) = N(P') = p$ and $N(Q) = 1$. Hence $Q = \mathbb{Z}[\sqrt{d}]$ and $\langle p\rangle = PP'$.

Suppose that $p \mid 2d$. Then $p \mid 2a^2$. Since p is a prime, then $p \mid 2a$. Hence $P = \left\langle p, a+\sqrt{d}\right\rangle = \left\langle p, -a+\sqrt{d}\right\rangle = \left\langle p, a-\sqrt{d}\right\rangle = P'$. Conversely, suppose that $P = P'$. Then $\overline{x}-\overline{a} = \overline{x}+\overline{a}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Hence $p \mid 2a$. But $d = a^2$. Then $p \mid 2d = 2a^2$. □

Question 8

Let $d \equiv 1 \bmod 4$ be a square-free integer, with $d \neq 1$. Show that the ring $\mathbb{Z}[\sqrt{d}]$ is never a UFD.

[*Hint: Consider factoring* $d-1$.]

Proof. Suppose that $\mathbb{Z}[\sqrt{d}]$ is a UFD. Note that $d - 1 = (\sqrt{d}+1)(\sqrt{d}-1)$.

We claim that $2 \in \mathbb{Z}[\sqrt{d}]$ is an irreducible. Suppose that $2 = (u+v\sqrt{d})(x+y\sqrt{d})$ for some $u, v, x, y \in \mathbb{Z}$. Taking the norm,

$$4 = (u^2 - dv^2)(x^2 - dy^2)$$

A

If $u+v\sqrt{d}$ and $x+y\sqrt{d}$ are non-units, then by unique factorisation in $\mathbb{Z}$, we have $x^2 - dy^2 = \pm 2$. Using congruence modulo 4, we have $x^2 - y^2 \equiv 2 \bmod 4$. But this is impossible, as $x^2, y^2 \equiv 0, 1 \bmod 4$. Hence either $u+v\sqrt{d}$ or $x+y\sqrt{d}$ is a unit. We deduce that 2 is irreducible.

Since $\mathbb{Z}[\sqrt{d}]$ is a UFD, 2 is prime in $\mathbb{Z}[\sqrt{d}]$. Note that $d-1 \equiv 0 \bmod 4$. So we have $2 \mid (\sqrt{d}+1)(\sqrt{d}-1)$. Then either $2 \mid \sqrt{d}+1$ or $2 \mid \sqrt{d}-1$, both of which are impossible. We conclude that $\mathbb{Z}[\sqrt{d}]$ cannot be a UFD. □