Solution 1.

Let $B = \mathbb{R}[x]$, clearly B is an integral domain. Let $\mathfrak{p} = (x)$, clearly $\mathfrak{p}$ is maximal and hence prime in B. Let $A = \mathbb{R}$, clearly A is a subring of B and satisfies the property that $\mathfrak{p} \cap A = 0$. □

Solution 2.

Let $\mathfrak{a}$ be a non-zero integral ideal and let $\mathfrak{b}$ be a non-zero fractional ideal in a Dedekind domain B. We will show that $\beta\mathfrak{b} + \mathfrak{a} = B$ for some $\beta \in \mathfrak{b}^{-1}$. Note that as $\beta \in \mathfrak{b}^{-1}$ we have that $\beta\mathfrak{b} \subseteq B$ and thus $\beta\mathfrak{b}$ is an integral ideal. We will thus have shown that given any integral ideal $\mathfrak{a}$ and an ideal class of $Cl(B)$ represented by a fractional ideal $\mathfrak{b}$ there is an integral ideal $(\beta)\mathfrak{b}$ (which is clearly in the same ideal class as $\mathfrak{b}$) that is relatively prime to $\mathfrak{a}$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the distinct prime ideals that show up in the factorization of $\mathfrak{a}$. Let

$$\mathfrak{b}_i = \mathfrak{b}^{-1}\mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_n$$

And let $\beta_i \in \mathfrak{b}_i \backslash \mathfrak{b}_i\mathfrak{p}_i$. (Note that $\mathfrak{b}_i \backslash \mathfrak{b}_i\mathfrak{p}_i$ is non-empty as otherwise $\mathfrak{b}_i = \mathfrak{b}_i\mathfrak{p}_i$, which upon multiplication by $\mathfrak{b}_i^{-1}$ yields $B = \mathfrak{p}_i$, a contradiction). Let $\beta = \sum_{i=1}^{n} \beta_i$. Note that $(\beta_i)\mathfrak{b} \subseteq \mathfrak{b}_i\mathfrak{b} = \mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_m \subseteq \mathfrak{p}_j$ for $i \neq j$, and consequently we have that $(\beta_i)\mathfrak{b} \not\subseteq \mathfrak{p}_i$ as otherwise $(\beta_i)\mathfrak{b} \subseteq \mathfrak{p}_1 \ldots \mathfrak{p}_n$ which implies that $\beta_i \in \mathfrak{b}^{-1}\mathfrak{p}_1 \ldots \mathfrak{p}_n = \mathfrak{b}_i\mathfrak{p}_i$, which is a contradiction by our choice of β_i.

We claim that $(\beta)\mathfrak{b} \not\subseteq \mathfrak{p}_i$ for all $1 \leq i \leq n$, as otherwise $(\beta)\mathfrak{b} \subseteq \mathfrak{p}_i$, for some i, which implies that $\mathfrak{b}\left(\sum_{j=1}^{n} \beta_j\right) \subseteq \mathfrak{p}_i$, but as $(\beta_j)\mathfrak{b} \subseteq \mathfrak{p}_i$ for $j \neq i$ we consequently have that $(\beta_i)\mathfrak{b} \subseteq \mathfrak{p}_i$, a contradiction. Thus, $\beta\mathfrak{b}$ and $\mathfrak{a}$ have disjoint prime factorizations (i.e any prime factor of one is not a prime factor of the other) and consequently $\beta\mathfrak{b}^{-1} + \mathfrak{a} = B$, as required. □

Solution 3.

By our previous problem, in a Dedekind domain B, given any integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{b}$ we can find $\beta \in \mathfrak{b}^{-1}$ such that $(\beta)\mathfrak{b} + \mathfrak{a} = B$. Let $\mathfrak{c}$ be an arbitrary ideal in B and let $x \in \mathfrak{c}$ with $x \neq 0$ (clearly the zero ideal is principal). Note that $(x)\mathfrak{c}^{-1} \subseteq B$ and is thus an integral ideal. Setting $\mathfrak{a} = (x)\mathfrak{c}^{-1}$ and $\mathfrak{b} = \mathfrak{c}^{-1}$ in the statement obtained from the previous problem we get that there is some $\beta \in \mathfrak{c}$ such that

$$(\beta)\mathfrak{c}^{-1} + (x)\mathfrak{c}^{-1} = B$$

which implies that $\mathfrak{c} = (\beta) + (x)$, i.e $\mathfrak{c}$ can be generated by two elements, as required. □

Solution 4.

Let d, K, p be as stated in the problem

First, assume that $x^2 \equiv d \mod p$ has a solution. This implies that $(x+\sqrt{d})(x-\sqrt{d}) = np$ for some $n \in \mathbb{Z}$. Thus, $(x+\sqrt{d})(x-\sqrt{d}) \in pO_K$ but clearly p does not divide either $x+\sqrt{d}$ or $x-\sqrt{d}$, hence pO_K is not a prime ideal. Contrapositively, we have thus shown that if pO_K is a prime ideal then $x^2 \equiv d \mod p$ has no solutions.

Conversely, suppose $x^2 \equiv d \mod p$ has no solutions. Assuming that pO_K is not a prime ideal we will derive a contradiction which will consequently give us that $x^2 \equiv d \mod p$ has no solutions implies that pO_K is a prime ideal. If pO_K is not a prime ideal then there exist $\alpha, \beta, \gamma \in O_K$ such that $\alpha\beta = \gamma p$ but p does not divide α or β. Taking norms we then have $N(\alpha)N(\beta) = p^2 N(\gamma)$, moving to modulo p we have that $N(\alpha)N(\beta) \equiv 0 \mod p$. Note that $\mathbb{Z}/(p)$ is a field and thus without loss of generality we may assume that $N(\alpha) \equiv 0 \mod p$. We will now consider two cases

(a) $d \not\equiv 1 \mod 4$
In this case $O_K = \mathbb{Z}[\sqrt{d}]$ and $\alpha = x+y\sqrt{d}$ where $x, y \in \mathbb{Z}$ and thus $N(\alpha) = x^2 - y^2 d$ which implies that $x^2 \equiv y^2 d \mod p$ clearly $y \not\equiv 0 \mod p$ as otherwise $x^2 \equiv 0$ which implies that $x \equiv y \equiv 0 \mod p$ (as we are in a field), and consequently p divides α, which contradicts our choice of α. But now as $y \neq 0$ and we are working in a field, we have some $y^{-1} \in \mathbb{Z}/(p)$ such that

$$(xy^{-1})^2 \equiv d \mod p$$

which is a contradiction, as required.

(b) $d \equiv 1 \mod 4$
In this case $O_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ and consequently $N(\alpha) = (x + \frac{y}{2})^2 - (\frac{y}{2})^2 d \equiv 0 \mod p$. Thus

$$4[(x + \frac{y}{2})^2 - (\frac{y}{2})^2 d] \equiv (2x+y)^2 - y^2 d \equiv 0 \mod p$$

But note that as before $y \not\equiv 0 \mod p$ as otherwise $2x \equiv 0$ but by assumption of the problem we know that $2 \not\equiv 0 \mod p$ so, $x \equiv 0$ and consequently p divides α, which contradicts our choice of α. But now as $y \neq 0$ and we are working in a field, we have some $y^{-1} \in \mathbb{Z}/(p)$ such that

$$(y^{-1}(2x+y))^2 \equiv d \mod p$$

which is a contradiction as required.

□