

Proving $d = 5$ Works.

Since $-5 \equiv 3 \pmod{4}$, $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of $\mathbb{Q}[\sqrt{-5}]$. Let $p \mid k^2 + 5$.

Claim 1. The ideal (p) can be decomposed as $\mathfrak{p}\bar{\mathfrak{p}}$ for some ideal $\mathfrak{p} \neq \bar{\mathfrak{p}}$.

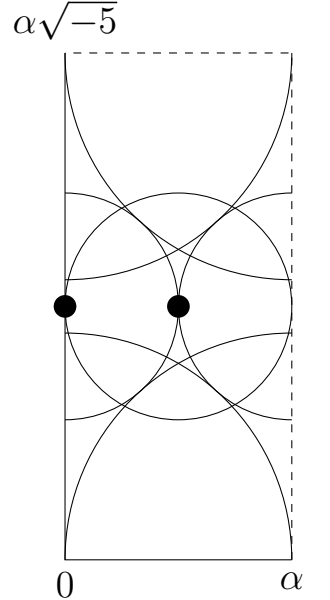
Proof. Let $\mathfrak{p} = (p, k + \sqrt{-5})$. Then $\mathfrak{p}\bar{\mathfrak{p}} = (p^2, pk \pm p\sqrt{-5}, k^2 + 5)$. All the generators are divisible by p , hence $\mathfrak{p}\bar{\mathfrak{p}} \subseteq (p)$. However, the gcd of p^2 and $(pk + p\sqrt{-5}) + (pk - p\sqrt{-5})$ is p , thus $(p) \subseteq \mathfrak{p}\bar{\mathfrak{p}}$. Assume $\mathfrak{p} = \bar{\mathfrak{p}}$, then $Ap + B(k - \sqrt{-5}) = k + \sqrt{-5}$ for some $A, B \in \mathbb{Z}[\sqrt{-5}]$. Write $A = a_1 + a_2\sqrt{-5}$ and $B = b_1 + b_2\sqrt{-5}$ and thus

$$\begin{cases} a_1p + kb_1 + 5b_2 = k \\ a_2p - b_1 + kb_2 = 1 \end{cases} \Rightarrow (a_1 + ka_2)p + (5 + k^2)b_2 = 2k$$

has solutions for integers a_1, a_2, b_1, b_2 . This is impossible as $p \mid \text{LHS}$ but $p \nmid \text{RHS}$. \square

Claim 2. The class group of $\mathbb{Z}[\sqrt{-5}]$ is C_2 .

Proof. It suffices to prove that there are only two types of sublattices in $\mathbb{Z}[\sqrt{-5}]$ up to orientation-preserving transformations. Let \mathcal{L} be a sublattice of $\mathbb{Z}[\sqrt{-5}]$ and α be nonzero with minimal norm. Therefore \mathcal{L} contains the sublattice \mathcal{A} spanned by $(\alpha, \alpha\sqrt{-5})$. If $\mathcal{L} = \mathcal{A}$ then this ideal is just (α) , otherwise let $\beta \in \mathcal{L} \setminus \mathcal{A}$ be situated in the parallelogram $x\alpha + y\alpha\sqrt{-5}$ where $0 \leq x, y < 1$. Note that β cannot lie inside the four quarter circles as shown on the right due to minimality of α . For the remaining region, any β lying there, multiplied by two, will be $< |\alpha|$ distance away from some point in \mathcal{A} (Verified by applying an origin-homothety with scale 2 onto the circle and the two semicircles). Therefore, $2\beta \in \mathcal{A}$, i.e. $\beta = \frac{\sqrt{-5}}{2}\alpha$ or $\frac{1+\sqrt{-5}}{2}\alpha$ (The two points labelled in the diagram). The former implies $-\frac{5}{2}\alpha \in \mathcal{L} \Rightarrow \frac{1}{2}\alpha \in \mathcal{L}$, contradicting minimality of α . Thus $\beta = \frac{1+\sqrt{-5}}{2}\alpha$. Therefore any ideal is in the form (α) or $(\alpha, \frac{1+\sqrt{-5}}{2}\alpha)$. \square



By claim 2, the product of any two ideals in the same ideal class belongs to the unit ideal class, i.e. is a principal ideal. Therefore $\mathfrak{p}\mathfrak{p} = (x)$ for some $x \in \mathbb{Z}[\sqrt{-5}]$. We know $x \neq p$ otherwise $\mathfrak{p} = \bar{\mathfrak{p}}$ by the cancellation law, hence

$$(p^2) = (p)(p) = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{p}\bar{\mathfrak{p}} = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{p}\bar{\mathfrak{p}} = (x)(\bar{x}) = (x\bar{x})$$

i.e. $p^2 = x\bar{x} = (m + n\sqrt{-5})(m - n\sqrt{-5}) = m^2 + 5n^2$ for some $(m, n) \neq (p, 0)$. \square

Generalising.

The ring of integers \mathcal{O}_K of $K = \mathbb{Q}[\sqrt{-d}]$ is

$$\begin{cases} \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} & \text{if } -d \equiv 2, 3 \pmod{4} \\ \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \text{ or } a + 0.5, b + 0.5 \in \mathbb{Z}\} & \text{if } -d \equiv 1 \pmod{4} \end{cases}$$

I will analyse the case $-d \equiv 2, 3 \pmod{4}$ for simplicity. We see that

$$\begin{aligned} & \text{The ideal } (p) \text{ is prime in } \mathbb{Z}[\sqrt{-d}] \\ & \iff \mathbb{Z}[\sqrt{-d}]/(p) \text{ is an integral domain} \\ & \iff \mathbb{F}_p[\sqrt{-d}] \text{ is an integral domain} \\ & \iff \mathbb{F}_p[x]/(x^2 + d) \text{ is an integral domain} \\ & \iff \text{The ideal } (x^2 + d) \text{ is prime in } \mathbb{F}_p[x] \end{aligned}$$

Since $-d$ has a quadratic residue mod p , the ideal (p) is not prime. Therefore $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ for some prime ideal \mathfrak{p} . The Dedekind-Kummer Theorem gives

$$p \text{ ramifies} \iff p \mid \Delta(x^2 + d) = -4d \quad (*)$$

Claim. $p^2 = m^2 + dn^2$ ($n \neq 0$) for all integer primes $p \nmid 2d$ iff the class group of \mathcal{O}_K is

$$C_2 \times C_2 \times \cdots \times C_2.$$

Proof. (\Leftarrow) The order of every class is 1 and 2, thus $\mathfrak{p}\bar{\mathfrak{p}} = (x)$ for some x . Since p does not ramify, $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and hence $x \neq p$. Therefore $(p^2) = (p)(p) = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{p}\bar{\mathfrak{p}} = (x)(\bar{x}) \Rightarrow p^2 = x\bar{x}$. (\Rightarrow) Assume some ideal class $\langle \mathfrak{a} \rangle$ has order > 2 . Then $\mathfrak{a}\mathfrak{a}$ is not principal. Decomposing \mathfrak{a} into prime ideals, there must exist some prime ideal \mathfrak{p} where $\mathfrak{p}\bar{\mathfrak{p}}$ is not principal. Let $\mathfrak{p}\bar{\mathfrak{p}} = (p) \Rightarrow (p^2) = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{p}\bar{\mathfrak{p}}$ is not expressible as a product of conjugate principal ideals. \square

Therefore, the problem statement after changing 5 to d works if and only if the class group is $C_2 \times C_2 \times \cdots \times C_2$. (From Internet:) The values of d for which the class group is C_2 are 5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427. The values of d for which the class group is C_1 are 1, 2, 3, 7, 11, 19, 43, 67, 163. Picking those with $-2, -3 \pmod{4}$, we have $d = 1, 2, 5, 6, 10, 13, 22, 37, 58$. Also, $\mathbb{Z}[\sqrt{-21}]$ has class group $C_2 \times C_2$, so $d = 21$ works too. Therefore,

$$d = 1, 2, 5, 6, 10, 13, 21, 22, 37, 58$$

all work. There might be others. \square