Proving for $d = 5$

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

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

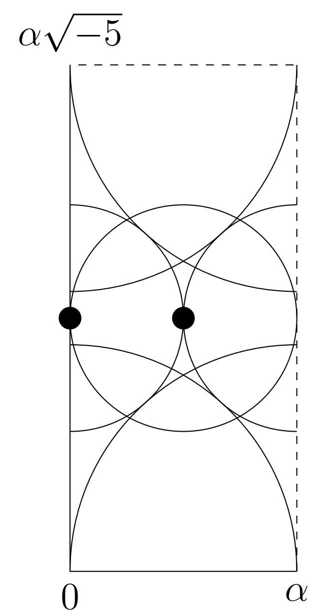
Proof. Let $\mathfrak{p} = \left(p, k + \sqrt{-5}\right)$. Then $\mathfrak{p}\overline{\mathfrak{p}} = \left(p^2, pk \pm p\sqrt{-5}, k^2 + 5\right)$. All the generators are divisible by p, hence $\mathfrak{p}\overline{\mathfrak{p}} \subseteq (p)$. However, the gcd of p^2 and $\left(pk + p\sqrt{-5}\right)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

$$\begin{cases} a_1 p + k b_1 + 5 b_2 = k \\ a_2 p - b_1 + k b_2 = 1 \end{cases} \quad \Rightarrow \quad (a_1 + k a_2)p + (5 + k^2) b_2 = 2k$$

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 $\mathbb{Z}\left[\sqrt{-5}\right]$ is C_2.

Proof. It suffices to prove that there are only two types of sublattices in $\mathbb{Z}\left[\sqrt{-5}\right]$ up to orientation-preserving transformations. Let $\mathcal{L}$ be a sublattice of $\mathbb{Z}\left[\sqrt{-5}\right]$ and α be nonzero with minimal norm. Therefore $\mathcal{L}$ contains the sublattice $\mathcal{A}$ spanned by $\left(\alpha, \alpha\sqrt{-5}\right)$. 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 $\left(\alpha, \frac{1+\sqrt{-5}}{2}\alpha\right)$. $\square$



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 $x \in \mathbb{Z}\left[\sqrt{-5}\right]$. We know $x \neq p$ otherwise $\mathfrak{p} = \overline{\mathfrak{p}}$ by the cancellation law, hence

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

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

Generalising.

The ring of integers $\mathcal{O}$ of $\mathbb{Q}\left[\sqrt{-d}\right]$ is $\mathbb{Z}\left[\sqrt{-d}\right]$ for $-d \equiv 2, 3 \pmod 4$ squarefree. I will only analyse the case $-d \equiv 2, 3 \pmod 4$ for simplicity. We see that

$$\frac{\mathcal{O}}{(p)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+d)} \cong \frac{\mathbb{F}_p[x]}{(x^2+d)} \cong \frac{\mathbb{F}_p[x]}{(x+k)} \times \frac{\mathbb{F}_p[x]}{(x-k)}$$

where $p \mid k^2 + d$. The last step holds because when $p > d$, the numbers k and $-k$ are distinct mod p and we apply CRT. The maximal ($\Leftrightarrow$ prime) ideals of $\mathcal{O}/(p)$ are thus the preimages of $(x+k)$ and $(x-k)$, which are $\mathfrak{p} = (p, \sqrt{-d}+k)$ and $\overline{\mathfrak{p}} = (p, \sqrt{-d}-k)$ respectively. Therefore $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ (so p does not ramify).

Claim. There exists an expression $p^2 = m^2 + dn^2$ $(n \neq 0)$ for all integer primes $p > d$ if and only if the class group of $\mathcal{O}$ is

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

Proof. ($\Leftarrow$) The order of every class is 1 and 2, thus $\mathfrak{p}\overline{\mathfrak{p}} = (x)$ for some x. Since p does not ramify, $\mathfrak{p} \neq \overline{\mathfrak{p}}$ and hence $x \neq p$. Therefore $(p^2) = (p)(p) = \mathfrak{p}\mathfrak{p}\overline{\mathfrak{p}\mathfrak{p}} = (x)(\overline{x}) \Rightarrow p^2 = x\overline{x}$.
($\Rightarrow$) 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 $\mathfrak{p}\mathfrak{p}$ is not principal. Let $\mathfrak{p}\overline{\mathfrak{p}} = (p) \Rightarrow (p^2) = \mathfrak{p}\mathfrak{p}\overline{\mathfrak{p}\mathfrak{p}}$ 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, $\mathbb{Z}\left[\sqrt{-21}\right]$ 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. $\square$

Problem 2.

Let $\mathcal{S} \subseteq \mathbb{N}$ be the set of integers expressible as a sum of distinct squares. Denote $N_4 = \{4^n \mid n \in \mathbb{N}\}$, $N_9 = \{9^n \mid n \in \mathbb{N}\}$. Denote $[x, y] = \{x, x+1, \cdots, y\}$.

Claim 1. $\forall \varepsilon > 0$, there exists infinitely many $(a, b) \in \mathbb{N}$ such that $\left|\frac{4^a}{9^b} - 1\right| < \varepsilon$.

Proof. If $\varepsilon \geq 1$ it is obvious. Assume $\varepsilon < 1$. The statement is equivalent to

$$\ln(1-\varepsilon) < a \ln 4 - b \ln 9 < \ln(1+\varepsilon) \tag{$*$}$$

It is well-known (Dirichlet) that any $n \in \mathbb{N}$, there exists infinitely many a, b such that

$$-\frac{1}{n} < a \cdot \frac{\ln 4}{\ln 9} - b < \frac{1}{n}$$
$$\Leftrightarrow -\frac{\ln 9}{n} < a \ln 4 - b \ln 9 < \frac{\ln 9}{n}$$

hence we just have to choose $n > \dfrac{\ln 9}{\min(|\ln(1-\varepsilon)|, |\ln(1+\varepsilon)|)}$ so $(*)$ is satisfied. $\square$

Claim 2. $x \in \mathcal{S} \;\Rightarrow\; 4x, 4x+1, 4x+10, 4x+35 \in \mathcal{S}$.

Proof. $x = \sum x_i^2 \;\Rightarrow\; 4x + k = \sum (2x_i)^2 + k$ for $k = 0, 1^2, 1^2+3^2, 1^2+3^2+5^2$. $\square$

Claim 3. $x \in \mathcal{S} \;\Rightarrow\; 9x, 9x+1, 9x+20, 9x+21, 9x+4, 9x+5, 9x+42, 9x+16, 9x+17 \in \mathcal{S}$.

Proof. $x = \sum x_i^2 \;\Rightarrow\; 9x + k = \sum (3x_i)^2 + k$ for k a sum of numbers in $\{1^2, 2^2, 4^2, 5^2\}$. $\square$

Claim 4. If $[x, y] \subseteq \mathcal{S}$, then $[k(x+12), ky] \subseteq \mathcal{S}$ for any $k \in N_4 \cup N_9$.

Proof. From Claim 2 and Claim 3, we have $[x, y] \subseteq \mathcal{S} \Rightarrow [4x+35, 4y], [9x+42, 9y] \subseteq \mathcal{S}$. By induction, for any $m, n \in \mathbb{N} \cup \{0\}$

$$[4^n x + 35(1 + 4 + \cdots + 4^{n-1}),\ 4^n y] \subseteq \mathcal{S} \qquad [9^m x + 42(1 + 9 + \cdots + 9^{m-1}),\ 9^m y] \subseteq \mathcal{S}$$
$$\left[4^n x + \frac{35}{3}(4^n - 1),\ 4^n y\right] \subseteq \mathcal{S} \qquad \left[9^m x + \frac{42}{8}(9^m - 1),\ 9^m y\right] \subseteq \mathcal{S}$$
$$\Rightarrow [4^n (x+12),\ 4^n y] \subseteq \mathcal{S} \qquad \Rightarrow [9^m (x+6),\ 9^m y] \subseteq \mathcal{S}$$

Since $12 > 6$, we are done. $\square$

Define the *scale* of $[a, b]$ as $\frac{b}{a}$.

Claim 5. Assume there is $[x,y] \subseteq \mathcal{S}$ with $y \geq x+13$. There exists $[x,y] \subseteq \mathcal{S}$ $(x>0)$ with arbitrarily large scales.

Proof. By claim 1, there exists infinitely many $a, b \in N_4 \cup N_9$ such that $1 < \dfrac{b}{a} < \dfrac{y}{x+12.5}$. Choose a, b such that $a > 25$. We will prove by induction that there always exists $[x,y] \subseteq \mathcal{S}$ with $\dfrac{y}{x+12.5} > \left(\dfrac{b}{a}\right)^n$. The base case $n=1$ is done. Assume $[x,y] \subseteq \mathcal{S}$ such that $\dfrac{y}{x+12.5} > \left(\dfrac{b}{a}\right)^{n-1} \geq \dfrac{b}{a}$. By claim 4,

$$[a(x+12), ay], [b(x+12), by] \subseteq \mathcal{S}$$

but $ay > b(x+12.5) > b(x+12)$, hence $[a(x+12), by] \subseteq \mathcal{S}$ and

$$\begin{aligned} \frac{by}{a(x+12)+12.5} &> \frac{b}{a} \cdot \frac{y}{x+12.5} \iff a > 25 \text{ is true, thus} \\ \frac{by}{a(x+12)+12.5} &> \frac{b}{a} \cdot \frac{y}{x+12.5} > \frac{b}{a} \cdot \left(\frac{b}{a}\right)^{n-1} = \left(\frac{b}{a}\right)^n. \end{aligned}$$

Thus $\forall n \geq 1 : \exists [x,y] \subseteq \mathcal{S}$ with $\dfrac{y}{x} > \dfrac{y}{x+12.5} > \left(\dfrac{b}{a}\right)^n$. When $n \to \infty$, $\left(\dfrac{b}{a}\right)^n \to \infty$. $\square$

Claim 6. Assume there is $[x,y] \subseteq \mathcal{S}$ with $y \geq x+13$. Then there exists N such that all integers $x \geq N$ are in $\mathcal{S}$.

Proof. By claim 5, there exists some $[x,y] \subseteq \mathcal{S}$ such that $y \geq 39x \geq 4x+35$. Assume $[x, k-1] \subseteq \mathcal{S}$ for some integer $k-1 \geq 4x+35$. Suppose $k \notin \mathcal{S}$, then by claim 2, one of $k/4, (k-1)/4, (k-10)/4, (k-35)/4$ is not in $\mathcal{S}$. This is impossible as they are all at least x. Therefore $k \in \mathcal{S}$, and by induction we are done. $\square$

It remains to find some $[x, x+13] \in \mathcal{S}$:

$$\begin{aligned} 144 &= 12^2 & 151 &= 1^2+2^2+5^2+11^2 \\ 145 &= 1^2+12^2 & 152 &= 4^2+6^2+10^2 \\ 146 &= 5^2+11^2 & 153 &= 1^2+4^2+6^2+10^2 \\ 147 &= 1^2+5^2+11^2 & 154 &= 1^2+3^2+12^2 \\ 148 &= 2^2+12^2 & 155 &= 3^2+5^2+11^2 \\ 149 &= 1^2+2^2+12^2 & 156 &= 1^2+3^2+5^2+11^2 \\ 150 &= 2^2+5^2+11^2 & 157 &= 2^2+3^2+12^2 \end{aligned}$$

and boom. $\square$

Problem 2 (Extra).

Let $\mathcal{S} \subseteq \mathbb{N}$ be the set of integers expressible as a sum of distinct m-th powers. We similarly have

$$x \in \mathcal{S} \Rightarrow 2^m x, 2^m x + \sum_{i=0}^{k} (2^m i + 1)^m \in \mathcal{S}$$

for any $k = 0, \cdots, 2^m - 2$. Therefore, if we could verify that $[x, y] \subseteq \mathcal{S}$ for some $y \geq 2^m x + \sum_{i=0}^{2^m-2} (2^m i + 1)^m$, then all $n \geq x$ lie in $\mathcal{S}$. $\square$