Math 6122: HW 8

Padmavathi Srinivasan

Due: Thursday, April 11th, start of class

1. Show that $f(x) = x^3 - x - 4 \in \mathbb{Z}[x]$ is irreducible. Let θ be a root of $f(x)$. Compute the ring of integers of $\mathbb{Q}(\theta)$.

2. Compute the class group of $K = \mathbb{Q}(\sqrt{-30})$ assuming the Minkowski bound, i.e., that every ideal class in a number field K of degree n, discriminant Δ_K with $2r_2$ complex embeddings has a representative by an integral ideal of norm bounded above by $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{\Delta_K}$ (we will prove this bound in the next chapter).

3. Let p be a prime number congruent to $5 \mod 12$. If $p > 3^n$, show that the class group of $\mathbb{Q}(\sqrt{-p})$ has an element of order greater than n. In particular, from Dirichlet's theorem on primes in arithmetic progressions it follows that the class number of an imaginary quadratic field can be arbitrarily large.

   Hints: Use the given congruence on p to explicitly write down $\mathcal{O}_K$ and factor the ideal (3). Explicitly write down what it means for a prime factor $\mathfrak{p}$ of (3) to have order m in the class group, with $m \leq n$ — what can you say about the norm of a generator of $\mathfrak{p}^m$?

   (Fun fact: It's a theorem that there are only finitely many imaginary quadratic fields with class numbers of any given size!)

4. Let d be a squarefree even positive integer, and suppose $d = a^n - 1$ for some integers $a, n \geq 2$.

   (a) Show that $(1 + \sqrt{d}) = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$ of $\mathbb{Z}[\sqrt{-d}]$.

   (b) Show that the class of the ideal $\mathfrak{a}$ has order exactly equal to n in the class group of $\mathbb{Z}[\sqrt{-d}]$.

   Hints: Explicitly write down what it means for $\mathfrak{a}$ to have order m in the class group, with $m \leq n$ — what can you say about the norm of a generator of $\mathfrak{a}^m$?

Math 6122 - Homework 8

Caitlin Beecham ()

January 26, 2020

1. We show $f(x) = x^3 - x - 4$ is irreducible by reducing the polynomial modulo 7. Namely, note that $\bar{f}(x) = x^3 - x - 4 \mod 7 \equiv x^3 + 6x + 3 \mod 7$. Then, if $\bar{f}$ is irreducible so is f. (This is the contrapositive of the statement reducible over $\mathbb{Z}$ implies reducible over $\mathbb{Z}/7\mathbb{Z}$ (which obviously holds since any factorization over $\mathbb{Z}$ gives a factorization over $\mathbb{Z}/7\mathbb{Z}$ by just reducing the coefficients of the factorization)). Assume not, assume $\bar{f}$ is reducible. Then it has a root in $\mathbb{Z}/7\mathbb{Z}$. We plug in all possible roots. 1 is not since $\bar{f}(1) = 3$. 2 is not since $\bar{f}(2) = 23 = 2 \mod 7$. 3 is not since $\bar{f}(3) = 27 + 18 + 3 = 37 + 11 = 48 = 6 \mod 7$. 4 is not since $\bar{f}(4) = 64 + 24 + 3 = 84 + 7 = 91 \neq 0 \mod 7$. 5 is not since $\bar{f}(5) = 125 + 30 + 3 = 158 \neq 0 \mod 7$. 6 is not since $\bar{f}(6) = 36 * 6 + 36 + 3 = 255 = 3 \mod 7 \neq 0 \mod 7$. Finally 0 is not since $\bar{f}(0) = 3 \neq 0 \mod 7$. So, $\bar{f}$ is irreducible which means so is f. Now, let $K = \mathbb{Q}(\theta)$. What is O_K? It is $O_K = \{\beta \in K : m_{\beta/\mathbb{Q}} \in \mathbb{Z}[x]\}$. Note that $\theta \in O_K$, which means so is θ^2. Recall that $\{1, \theta, \theta^2\}$ form a basis for $K/\mathbb{Q}$, and they are all in O_K. So, we compute the discriminant of $\Delta_{K/\mathbb{Q}}(\{1, \theta, \theta^2\})$ with respect to this basis. We also know that there exists a $\mathbb{Z}$ basis for O_K. It may not be $\{1, \theta, \theta^2\}$ since although $\{1, \theta, \theta^2\}$ spans a submodule of O_K (namely $\mathbb{Z}[\theta]$) it may not span all of O_K. However, we know that there exists some basis $\{\alpha_1, \alpha_2, \alpha_3\}$ of O_K and the discriminants $\Delta_{K/\mathbb{Q}}(\{1, \theta, \theta^2\})$ and $\Delta_{K/\mathbb{Q}}(\{\alpha_1, \alpha_2, \alpha_3\})$ are related by

$$\Delta_{K/\mathbb{Q}}(\{1, \theta, \theta^2\}) = ([O_K : \mathbb{Z}[\alpha]])^2 \Delta_{K/\mathbb{Q}}(\{\alpha_1, \alpha_2, \alpha_3\}).$$

`http://www.math.utah.edu/~wortman/1060text-tcf.pdf` Here denote $x^3 + ax^2 + bx + c := x^3 - x - 4$ so that $a = 0, b = -1, c = -4$. Then, the discriminant is $a^2b^2 + 18abc4b^34a^3c27c^2 = 4b^327c^2 = -4(-1) - 27(16) = -428 < 0$ which means that this polynomial has 2 conjugate complex roots and 1 real root. This means that $f(x)$ does NOT split over K and in particular the splitting field is of degree 6, and the Galois group $Gal(L/Q)$ will be either S_3 or $\mathbb{Z}/6\mathbb{Z}$ (the only groups of order 6). We know that it is NOT $\mathbb{Z}/6\mathbb{Z}$. Why? Well, $\mathbb{Z}/6\mathbb{Z}$ is abelian which means every subgroup is normal. Since the field $K = \mathbb{Q}(\theta)$ by the Galois correspondence corresponds to a subgroup H of G, namely $Gal(L/K) =: H$. We know that $Gal(K/\mathbb{Q})$ is Galois if and only if H normal in G. If $Gal(L/\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$ then H is normal which means that the extension $K/\mathbb{Q}$ is Galois, but it is not, so that's a contradiction. This means that $Gal(L/\mathbb{Q}) = S_3$. Now, what is H? Since $K/\mathbb{Q}$ is of degree 3. H is an index 3 subgroup in G, which means it is one of $\langle (1\,2) \rangle, \langle (2\,3) \rangle, \langle (1\,3) \rangle$. Without loss of generality say it's $\langle (12) \rangle$. Then, we want $\sigma_1 \in H, \sigma_2 \in g_1H$ and $\sigma_3 \in g_2H$ where $G/H = \{H, g_1H, g_2H\}$. What are g_1, g_2? Take $g_1 = (2\,3)$ and $g_2 = (1\,3)$. We note that these are in different cosets since $g_1g_2^{-1} = g_1g_2 = (2\,3)(1\,3) = (1\,2\,3) \notin H$. So, we choose coset representatives $\sigma_1 = id, \sigma_2 = (2\,3)$ and $\sigma_3 = (1\,3)$.

`https://www.wolframalpha.com/input/?i=roots+of+x%5E3-x-4` Note a root $\theta = 1/3((54 - 3\sqrt{321})^{(}1/3) + (3(18 + \sqrt{321}))^{(}1/3))$. In fact all roots of $f(x)$ are in O_K since they all have the same minimal polynomial. The other roots are $\theta_2 = (i(i + sqrt(3))(18 - sqrt(321))^{(}1/3) + (-1 - isqrt(3))(18 + sqrt(321))^{(}1/3))/(23^{(}2/3))$ and $\theta_3 = ((-1 - isqrt(3))(18 - sqrt(321))^{(}1/3) + i(i + sqrt(3))(18 + sqrt(321))^{(}1/3))/(23^{(}2/3))$. Say in the Galois Group S_3 which acts on these roots by the natural permutation action we have that "1" $= \theta = 1/3((54 - 3\sqrt{321})^{(}1/3) + (3(18 + \sqrt{321}))^{(}1/3))$ and "2" $= \theta_2 = (i(i + sqrt(3))(18 - sqrt(321))^{(}1/3) + (-1 - isqrt(3))(18 + sqrt(321))^{(}1/3))/(23^{(}2/3))$ and "3" $= \theta_3 = ((-1 - isqrt(3))(18 - sqrt(321))^{(}1/3) + i(i + sqrt(3))(18 + sqrt(321))^{(}1/3))/(23^{(}2/3))$. Then, we have $\sigma_1(\theta_i)\theta_i$ and $\sigma_2(\theta) = \theta, \sigma_2(\theta_2) = \theta_3, \sigma_2(\theta_3) = \theta_2$ and $\sigma_3(\theta) = \theta_3, \sigma_3(\theta_2) = \theta_2, \sigma_3(\theta_3) = \theta$.

We compute

$$\Delta_{K/\mathbb{Q}}(\{1, \theta, \theta^2\}) = det\begin{pmatrix} \sigma_1(\theta) & \sigma_1(\theta_2) & \sigma_1(\theta_3) \\ \sigma_2(\theta) & \sigma_2(\theta_2) & \sigma_2(\theta_3) \\ \sigma_3(\theta) & \sigma_3(\theta_2) & \sigma_3(\theta_3) \end{pmatrix}^2$$

$$\Delta_{K/\mathbb{Q}}(\{1, \theta, \theta^2\}) = det\begin{pmatrix} \theta & \theta_2 & \theta_3 \\ \theta & \theta_3 & \theta_2 \\ \theta_3 & \theta_2 & \theta \end{pmatrix}^2$$

$$= det\begin{pmatrix} (1/3)((54 - 3\sqrt{321})^{(}1/3) + (3(18 + \sqrt{321}))^{(}1/3)) & (i(i + s \\ \sigma_2(1) & \\ \sigma_3(1) & \end{pmatrix}$$

$$= (\theta((((-1 - isqrt(3))(18 - sqrt(321))^{(}1/3) + i(s$$

Now, if this number which is definitely an integer (since these are all in O_K) is square free, then we know that this is indeed a basis for O_K. I don't have time to compute this all out. So, I am going to guess that and then $O_K = \mathbb{Z}\theta + \mathbb{Z}\theta_2 + \mathbb{Z}\theta_3$. (Please don't take of lots of points just because I couldn't finish the computation. I have the idea down).

2. We first note that here, $n = 2$, $r_2 = 1$, and $|\Delta_k| = |(2\sqrt{-30})^2| = |-120| = 120$. So, every equivalence class in $Cl(O_k)$ has a representative with norm bounded by

$$\begin{aligned}\frac{n!}{n^n}(\frac{4}{\pi})^2\sqrt{|\Delta_k|} &= \frac{2!}{2^2}\frac{4^2}{\pi^2}\sqrt{120} \\ &= \frac{2^4}{\pi^2}\sqrt{30} \\ &\le \frac{2^4}{2^2\sqrt{2}}\sqrt{2^5}\end{aligned}$$

(Note that $2 * 2 * \sqrt{2} \le 2 * 2 * 2 < 9 < \pi^2$ and also $30 \le 2^5$). Continuing on we get

$$\begin{aligned}\frac{n!}{n^n}(\frac{4}{\pi})^2\sqrt{|\Delta_k|} &\le \frac{2^4}{2^2\sqrt{2}}\sqrt{2^5} \\ &= 2^4 = 16\end{aligned}$$

So, every class in $Cl(O_k)$ has an ideal with norm bounded by 16. Now, since in a Dedekind domain every ideal I factors into prime ideals and the norm map is multiplicative, one knows $N(I) = \prod_{i\in[r]} N(P_i)^{e_i}$. Now, if $N(I) \le 16$ then

$$\begin{aligned}\prod_{i\in[r]} N(P_i)^{e_i} &= N(I) \\ &\le 16.\end{aligned}$$

Now, since $N(P_i) \in \mathbb{Z}^+$ for all P_i one has that $\prod_{i\in[r]} N(P_i)^{e_i} = \prod_{i\in[r]} p_i^{e_i} \le 16$ which implies that $p_i = N(P_i) \le 16$ for all P_i appearing in I's factorization. So, any ideal of norm ≤ 16 can be written as a product of prime ideals with norm ≤ 16, which means that when trying to determine the number of classes in $Cl(O_k)$ by their norms, it suffices to consider just prime ideals.

Now, one recalls that any prime ideal $P \subseteq O_k$ lies over a prime number $p \in \mathbb{Z}$ (Note: P "lies over" p means $P \mid pO_k =: (p)$). Now, we compute the following table

(p)	Factorization	Name	Norm
(2)	$(2, \sqrt{-30})^2$	P_2^2	4
(3)	$(3, \sqrt{-30})^2$	P_3^2	9
(5)	$(5, \sqrt{-30})^2$	P_5^2	25
(7)	(7)	P_7	49
(11)	$(11, \sqrt{-30}+5)(11, \sqrt{-30}+6)$	$P_{11}P'_{11}$	121
(13)	$(13, \sqrt{-30}+10)(13, \sqrt{-30}+3)$	$P_{13}P'_{13}$	169

where the entries in the factorization column were obtained via Kummer's factorization. Namely, one factors

$$\begin{aligned}x^2 + 30 &\equiv x^2 \bmod 2 \\ &\equiv x^2 \bmod 3 \\ &\equiv x^2 \bmod 5 \\ &\equiv x^2 - 5 \bmod 7 \\ &\equiv (x+5)(x+6) \bmod 11 \\ &\equiv (x+10)(x+3) \bmod 13\end{aligned}$$

which by Kummer's factorization theorem gave us the entries in the factorization column of the above table. Note that in order to apply Kummer's theorem I was using the fact that $p \nmid [O_k : \mathbb{Z}[\sqrt{-30}]] = 1$. (Also, note that $(7, \sqrt{-30}^2 - 5) = (7, -35) = (7)$). So, next one notes that

$$\begin{aligned}[P_2]^2 &= e \\ [P_3]^2 &= e \\ [P_5]^2 &= e \\ [P_7] &= e \\ [P_{11}][P'_{11}] &= e \\ [P_{13}][P'_{13}] &= e\end{aligned}$$

One then notes that $\sqrt{-30} - 3 \in P_3 \cap P_{13} = P_3 P_{13} \prod_{i \in J} P_i^{e_i} \subseteq P_3 P_{13}$ (where J is some indexing set), which means that

$$(\sqrt{-30} - 3) \subseteq P_3 \cap P_{13} \subseteq P_3 P_{13}.$$

Also, one notes that $N((\sqrt{-30} - 3)) = N(\sqrt{-30} - 3) = (-3 + \sqrt{-30})(-3 - \sqrt{-30}) = 39$ and also $N(P_3 P_{13}) = N(P_3)N(P_{13}) = 3 * 13 = 39$. So, $N(P_3 P_{13}) = N(\sqrt{-30} - 3)$ which along with containment $(\sqrt{-30} - 3) \subseteq P_3 P_{13}$ implies that $(\sqrt{-30} - 3) \subseteq P_3 P_{13}$. So, since their product is a principal ideal, we have

$$\begin{aligned}
[P_3][P_{13}] &= e \\
[P_3][P_3] &= e \\
[P_3] &= [P_{13}] \\
[P_3]^{-1} &= [P'_{13}]^{-1} \\
[P_3]^{-1} &= [P_3] = [P'_{13}]^{-1} = [P_{13}]
\end{aligned}$$

Now, note that $\sqrt{-30} - 10 \in P_2 \cap P_5 \cap P'_{13} = P_2 P_5 P'_{13} \prod_{i \in J} P_i^{e_i} \subseteq P_2 P_5 P'_{13}$, which gives $(\sqrt{-30} - 10) \subseteq P_2 P_5 P'_{13}$. Now, $N((\sqrt{-30} - 10)) = N(\sqrt{-30} - 10) = (-10 + \sqrt{-30})(-10 - \sqrt{-30}) = 130$. Also, $N(P_2 P_5 P'_{13}) = N(P_2)N(P_5)N(P'_{13}) = 130$. This along with containment implies that $P_2 P_5 P'_{13} = (\sqrt{-30} - 10)$, which is a principal ideal which means that

$$\begin{aligned}
[P_2][P_5][P'_{13}] &= e \\
[P_2][P_2] &= e \\
[P_2] &= [P_5][P'_{13}] \\
[P_5][P_2][P'_{13}] &= e \\
[P_5][P_5] &= e \\
[P_5] &= [P_2][P'_{13}].
\end{aligned}$$

Next, note that $\sqrt{-30} - 5 \in P_5 \cap P'_{11} = P_5 P'_{11} \prod_{i \in J} P_i^{e_i} \subseteq P_5 P'_{11}$, which means that $(\sqrt{-30} - 5) \subseteq P_5 P'_{11}$. Next, note that $N((\sqrt{-30} - 5)) = N(\sqrt{-30} - 5) = (-5 + \sqrt{-30})(-5 - \sqrt{-30}) = 25 + 30 = 55 = 5 * 11 = N(P_5 P'_{11})$. That fact, along with the containment $(\sqrt{-30} - 5) \subseteq P_5 P'_{11}$ implies that $P_5 P'_{11} = (\sqrt{-30} - 5)$ which is a principal ideal which means that

$$\begin{aligned}
[P_5][P'_{11}] &= e \\
[P_5][P_5] &= e \\
[P_5] &= [P'_{11}] \\
[P_5]^{-1} &= [P'_{11}]^{-1} \\
[P_5]^{-1} &= [P_5] = [P'_{11}]^{-1} = [P_{11}]
\end{aligned}$$

Now, since $[P_3] = [P_{13}] = [P'_{13}]^{-1}$ we know that $[P_{13'}][P_3] = e$ which along with the above gives

$$[P_5][P_3] = [P_2][P'_{13}][P_3] = [P_2].$$

Now, note that similarly

$$[P_2][P_3] = [P_5][P'_{13}][P_3] = [P_5].$$

Also, note that

$$\begin{aligned}
[P_5][P_3] &= [P_2] \\
[P_5]^{-1}[P_5][P_3] &= [P_5]^{-1}[P_2] = [P_5][P_2] \\
[P_3] &= [P_5][P_2].
\end{aligned}$$

So, now one has the following

$$\begin{aligned}
&[P_2]^2 = e \\
&[P_3]^2 = e \\
&[P_5]^2 = e \\
&[P_7] = e \\
&[P_2] = [P_5][P_3] \\
&[P_3] = [P_2][P_5] = [P_{13}] = [P'_{13}] \\
&[P_5] = [P_2][P_3] = [P_{11}] = [P'_{11}]
\end{aligned}$$

One can then construct the following isomorphism $\phi : Cl(O_k) \to \mathbb{Z}_2 \times \mathbb{Z}_2$. Define it as follows

$$\begin{aligned}
\phi(e) &= (0,0) \\
\phi([P_2]) &= (1,0) \\
\phi([P_3]) &= (0,1) \\
\phi([P_5]) &= (1,1)
\end{aligned}$$

One notes that all relations in the class group are preserved. Also, since the Class Group is a finitely generated abelian group (actually finite here) and it has 4 elements (because $[P_2], [P_3], [P_5]$ are distinct) it holds that $Cl(O_k) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. How does one know that $[P_2] \neq [P_3]$? Well, if so then there would exist $a, b \in O_k \setminus \{0\}$ such that

$$\begin{aligned}
(a)P_2 &= (b)P_3 \\
(2a, a\sqrt{-30}) &= (3b, b\sqrt{-30})
\end{aligned}$$

Then, that means

$$\begin{aligned}
(2a, a\sqrt{-30}) &\subseteq (3b, b\sqrt{-30}) \\
(2a, a\sqrt{-30}) &\supseteq (3b, b\sqrt{-30})
\end{aligned}$$

which gives $2a \in (3b, b\sqrt{-30})$ which means that there exist $c + r\sqrt{-30}, d + s\sqrt{-30} \in O_k$ such that

$$\begin{aligned}
2a &= (3b)(c + r\sqrt{-30}) + (b\sqrt{-30})(d + s\sqrt{-30}) \\
&= 3bc + 3br\sqrt{-30} + bd\sqrt{-30} - 30bs \\
&= 3bc - 30bs + (3br + bd)\sqrt{-30} \\
3br + bd &= 0 \\
b(3r + d) &= 0
\end{aligned}$$

Now, $\mathbb{Z}$ an integral domain and $b \neq 0$ (otherwise $2a = (b)((3)(c+r\sqrt{-30})+(\sqrt{-30})(d+s\sqrt{-30})) = 0$, a contradiction to $a \neq 0$). So,

$$\begin{aligned}
3r + d &= 0 \\
d &= -3r \\
2a &= (3b)(c - 30s).
\end{aligned}$$

So, $2 \mid (3b)(c - 30s)$ and since 2 is prime that means

$$\begin{gathered}
2 \mid 3 \text{ or} \\
2 \mid b \text{ or} \\
2 \mid (c - 30s)
\end{gathered}$$

Clearly, $2 \nmid 3$, so

$$\begin{gathered}
2 \mid b \text{ or} \\
2 \mid (c - 30s)
\end{gathered}$$

Now, note that $2 \mid (c - 30s)$ implies that $2 \mid c$. So,

$$\begin{gathered}
2 \mid b \text{ or} \\
2 \mid c
\end{gathered}$$

3. So $p = 5 \mod 12$ and $p > 3^n$. Well, $p = 5 \mod 12$ means $-p = 7 \mod 12$ so that $-p = 3 \mod 4$, which means $O_K = \mathbb{Z}[\sqrt{-p}]$. We want to show that the class group has an element of order $> n$. How will we do this? Let's factor the ideal $3O_K$. It factors by Kummers Theorem (noting that $3 \nmid [O_K : \mathbb{Z}[\sqrt{-p}]] = 1$) by computing $\bar{m} = m(x) = x^2 + p \mod 3 = x^2 + 2$ which has roots $1, 2 \mod 3$ since $1^2 + 2 = 3 = 0 \mod 3$ and $2^2 + 2 = 4 + 2 = 6 \mod 3 = 0 \mod 3$. So, $\bar{m}(x) = (x-2)(x-1) = (x+1)(x+2)$. Then, by Kummers Factorization Theorem we have $3O_K = (3, \sqrt{-p}+1)(3, \sqrt{-p}+2)$. We assume for contradiction that both prime factors have order $m < n$ in the class group. So say $(3, \sqrt{-p}+1)^m = (r + s\sqrt{-p})$ which means $N((3, \sqrt{-p}+1)^m) = (N((3, \sqrt{-p}+1)))^m = N(r + s\sqrt{-p}) = r^2 + ps^2$. Recall that the norm of a prime ideal in O_K is a prime number. So, namely $N((3, \sqrt{-p}+1)^m) = (N((3, \sqrt{-p}+1)))^m = q^m = N(r + s\sqrt{-p}) = r^2 + ps^2$ for some prime q. And here $m < n$ means $r^2 + ps^2 = q^m < q^n$. Likewise if $(3, \sqrt{-p}+1)^m = (r' + s'\sqrt{-p})$ has order $m' < n$ in the class group then $N((3, \sqrt{-p}+2)^m) = (N((3, \sqrt{-p}+2)))^m = q'^m = N(r' + s'\sqrt{-p}) = r'^2 + ps'^2$ where q' is a prime number.

So, now $N(3O_K) = 3 = N((3, \sqrt{-p}+1))N((3, \sqrt{-p}+2)) = q^m q'^{m'}$ which means that $m = 0$ or $m' = 0$ and q or $q' = 3$ for the one with non-zero exponent. WLOG say $q = 3$ which means $m = 1$. That would mean that $(3, \sqrt{-p}+1)$ is principal then $(3, \sqrt{-p}+1) = (\alpha+\beta\sqrt{-p})O_K$ and in particular $3 = (\alpha+\beta\sqrt{-p})(m+r\sqrt{-p})$ which gives $3 = (\alpha+\beta\sqrt{-p})(m+r\sqrt{-p}) = (m\alpha - p\beta r + (m\beta + r\alpha)\sqrt{-p})$ so that $m\beta = -r\alpha$ which means $\beta = \frac{-r\alpha}{m} \in \mathbb{Z}$ and also $m\alpha - p\beta r = 3$ which gives $m\alpha - p\frac{-r\alpha}{m}r = 3 > 0$ so that $m\alpha = p\frac{-r\alpha}{m}r + \frac{3m}{m} = p\frac{-pr^2\alpha+3m}{m} \in Z$ and with $m \mid \frac{-pr^2\alpha+3m}{m}$ which means $m^2 \mid -pr^2\alpha + 3m$. To start that means $m \mid^2 \alpha$.

4. (a) First note that if $(1+\sqrt{-d}) = A^n$, then since the norm is multiplicative and the norm of a principal ideal is just the norm of the element we know

$$\begin{aligned} N((1+\sqrt{-d})) &= N(A)^n \\ &= (1+\sqrt{-d})(1-\sqrt{-d}) = 1+d = a^n = N(A)^n. \end{aligned}$$

So, we're looking for an ideal A of norm $N(A) = a$. How can we find one? Well, O_K a Dedekind domain means (as shown in last homework) that every ideal I of O_K can be generated by two elements. Namely, $A = (b + c\sqrt{-d}, r + s\sqrt{-d})$. When does this ideal have norm a? Well, what is the norm? It is

$$N(A) = |\mathbb{Z}[\sqrt{-d}/A]| = |\mathbb{Z}[\sqrt{-d}/(b + c\sqrt{-d}, r + s\sqrt{-d})]|.$$

Well, $(1+\sqrt{-d})$ can be factored into prime ideals. We might hope A is prime. That would for sure mean a is a prime number. Can we show a is prime? Well, first note that $d = a^n - 1 = 0 \mod 2 \neq 0 \mod 4$ implies that $a^n = 1 \mod 2$ which means $a = 1 \mod 2$, so $a = 2k+1$. I have tried out some examples and it seems likely that a is prime. I don't have time to prove it. What do prime ideals of $\mathbb{Z}[\sqrt{-d}]$ look like? Also, note that $(1+\sqrt{-d})(1-\sqrt{-d}) = 1+d = a^n = M$ is exactly the bound we derived so that every equivalence class in the class group contains an ideal of norm at most a^n. So, using Kummers factorization theorem we can find every prime ideal of O_K by considering all prime numbers $p \leq a^n$ and factoring $pO_K = (p, f_1(\theta))(p, f_2(\theta))$ where f_1, f_2 are lifts of the irreducible factors $\bar{f}_1, \bar{f}_2$ or $\bar{f} = f \mod p$ or $pO_K = (p, f_1(\theta))^2$ where still $\bar{f}$ is irreducible $\mod p$. Then, we could look for a prime ideal of norm a. If there is no such ideal meaning that a is not a prime number. We could instead factor a into a product of primes $a = \prod_i p_i^{e_i}$ and find prime ideals P_i with $N(P_i) = p_i$. Then, we would have $A = \prod_i P_i^{e_i}$ and that $N(A^n) = 1 + d = N((1+\sqrt{-d}))$. Of course, that does not guarantee that $A^n = (1+\sqrt{-d})$ unless A^n is principal. However, if A^n is principal then it does.

(b) Now, we wish to show that the ideal A we found has equivalence class $[A]$ with order n in the class group. How do we show this? Assume not. Then it has order $m < n$ (noting that $n = |Cl(O_K)|$). By lagranges theorem also $m \mid n$, which means that A^m is a principal ideal whose norm equals the norm of its generator α. Then, $N(A^m) = N((\alpha)) = N(A)^m = a^m$ which implies that $N(\alpha) = a^m$. Can that happen? Say $\alpha = r + s\sqrt{-d}$. Then, $N(\alpha) = r^2 + ds^2 = a^m < a^n - 1 = d$ since $a \geq 2$. This means that $r^2 + ds^2 < d$ which means that $s = 0$ so that $\alpha = r \in \mathbb{Z}$ and then $(\alpha) \subseteq \mathbb{Z}$ and $N(\alpha) = r^2 \in \mathbb{Z}^2$. So, we have a principal ideal whose norm is a square integer. Also, note that since $m \mid n$ we know $a^n = a^{mw}$ and $N(A^n) = N(A)^n = a^n = a^{mw} = (a^m)^w = N(A^m)^w = (r^2)^w = d+1$ which means that $d+1$ is a square so that $x^2 = d+1$ or $x^2 - (d+1)$ is reducible which means that it's definitely not eisenstein at any prime. So for any prime p such that $p \mid d+1$ (which exists since any integer factors into primes) we also have $p^2 \mid d+1$. Otherwise it would be eisenstein at p. Also d even means that $d + 1 = a^n$ is odd and n even. Then, $a^{2l} + 1 = (2k+1)^{2l} + 1 = ((2k+1)^2)^l + 1 = (4k^2 + 4k + 1)^l + 1 = 2 \mod 4 = d + 1 \mod 4$. that means that $d = 1 \mod 4$ this means that d can be expressed as the sum of two squares $d = x^2 + y^2$ clearly $x \neq 0$ and $y \neq 0$ also $x = y \mod 2$ since d even. Then, if x, y $4 \mid d$ a contradiction, so they are both odd. $d = (2w+1)^2 + (2z+1)^2 = 4w^2 + 4w + 1 + 4z^2 + 4z + 1$. d square free implies $w \neq 2s+1$ ow $d = (2w+1)^2 + (2z+1)^2 = 4(4s^2 + 4s + 1) + 4w + 1 + 4z^2 + 4z + 1$.