33.1. Recall: p is **always** prime, $\zeta_p = e^{2\pi i/p}$. The p-th cyclotomic field is $\mathbb{Q}(\zeta_p)$.
Note that $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ and $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

Lemma 33.2. The minimal polynomial of ζ_p is

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

and

$$f(x) = \prod_{i=1}^{p-1}(x - \zeta_p^i).$$

Corollary 33.3.

(1) The degree of $\mathbb{Q}(\zeta_p)$ is $p-1$.
(2) A basis for $\mathbb{Q}(\zeta_p)$ as a vector space over $\mathbb{Q}$ is $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$.
(3) The $p-1$ embeddings $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ are given by $\sigma_i(\zeta_p) = \zeta_p^i$ for $1 \leq i \leq p-1$.
(4) $N(\zeta_p) = 1$.
(5) $\mathrm{Tr}(\zeta_p) = -1$.

Lemma 33.4. Let $\lambda = 1 - \zeta_p$. Then $N(\lambda) = p$.

Lemma 33.5.

$$\mathrm{Tr}(\zeta_p^i) = \begin{cases} -1 & i \not\equiv 0 \mod p \\ p-1 & i \equiv 0 \mod p. \end{cases}$$

Theorem 33.6. The ring of algebraic integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$.

Lemma 33.7. The discriminant of $\mathbb{Q}(\zeta_p)$ is $(-1)^{(p-1)/2}p^{p-2}$.

Theorem 33.8. (Deep) $\mathbb{Q}(\zeta_p)$ has class number one if and only if $p = 3, 5, 7, 11, 13, 17, 19$. $\mathbb{Q}(\zeta_p)$ never has class number 2.
(Ankeny-Chowla) There is some $P_0 \in \mathbb{N}$ such that the class number of $\mathbb{Q}(\zeta_p)$ is monotonically increasing for $p \geq P_0$.