34.1. Background: Let $p \geq 5$ be prime. Recall that

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

Denote by D the ring of integers of $\mathbb{Q}(\zeta_p)$ and h_p the class number. Kummer showed how to prove Fermat's last theorem (FLT) when $p \nmid h_p$. Kummer's approach splits FLT into two cases:

- First case of Fermat's last theorem: $x^p + y^p = z^p$ has no solutions $x, y, z \in \mathbb{Z}$ with $p \nmid x$ and $p \nmid y$ and $p \nmid z$.
- Second case of Fermat's last theorem: $x^p + y^p = z^p$ has no solutions $x, y, z \in \mathbb{Z}$ with $p \mid x$ or $p \mid y$ or $p \mid z$.

Exercise 34.2. Prove that if $u \in D$ satisfies $N(u) = 1$ then u is a unit. [Hint: Let σ_i be the embeddings of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$ and recall that $N(u) = \sigma_1(u)\prod_{i=2}^{p-1}\sigma_i(u)$. Apply σ_1^{-1} judiciously.]

Exercise 34.3. Let $1 \leq i \leq p-1$. Prove that $\epsilon = (1-\zeta_p^i)/(1-\zeta_p)$ is a unit. [Hint: Prove that $\epsilon \in D$ and that $N(\epsilon) = 1$.]

Kummer's Lemma: If $\epsilon \in D$ is a unit then

$$\epsilon = \zeta_p^i \eta$$

where $0 \leq i \leq p-1$ and where $\eta \in \mathbb{R}$.
For proof see Lemma 11.7 of Stewart and Tall, or Lemma 3.1.4 of Borevich and Shafarevich.

Lemma 34.4. Let $x, y, m, n \in \mathbb{N}$ with $m \not\equiv n \mod p$. Then $\gcd(x+\zeta_p^m y, x+\zeta_p^n y) = 1$ if and only if $\gcd(x,y) = 1$ and $p \nmid (x+y)$.

Proof: ($\Rightarrow$) The case $\gcd(x,y) > 1$ is obvious. If $p \mid (x+y)$ then note that $x+\zeta_p^m y = (x+y) + (\zeta_p^m - 1)y$ and both $(x+y)$ and $(\zeta_p^m - 1)$ are divisible by $\lambda = 1-\zeta_p$ (recall $N(\lambda) = p$).
($\Leftarrow$) We will show that there exist $\alpha_0, \beta_0 \in D$ such that $\alpha_0(x+\zeta_p^m y) + \beta_0(x+\zeta_p^n y) = 1$. To do this consider

$$A = \{\alpha(x+\zeta_p^m y) + \beta(x+\zeta_p^n y) : \alpha, \beta \in D\}.$$

Note that A is an ideal of D.
Now $(x+\zeta_p^m y) - (x+\zeta_p^n y) = \zeta_p^m \epsilon(\zeta_p - 1)y \in A$ for some unit ϵ. Similarly, $\zeta_p^n(x+\zeta_p^m y) - \zeta_p^m(x+\zeta_p^n y) = -\zeta_p^m \epsilon(\zeta_p - 1)x \in A$. It follows that $\lambda x, \lambda y \in A$. Since $\gcd(x,y) = 1$ it follows that $\lambda \in A$, and hence $p = N(\lambda) \in A$. But $p \nmid (x+y)$ implies $1 \in A$. $\square$

Theorem 34.5. (Kummer's first case of FLT) Let $p \geq 5$ be a prime such that $\mathbb{Q}(\zeta_p)$ has class number 1. Let $x, y, z \in \mathbb{N}$ be such that $x^p + y^p = z^p$. Then $p \mid x$ or $p \mid y$ or $p \mid z$.

Proof: We may assume that $\gcd(x,y) = \gcd(x,z) = \gcd(y,z) = 1$. Since $x+y \equiv x^p + y^p = z^p \mod p$ we have $p \nmid (x+y)$. Hence, by Lemma 34.4, the factors in the right hand side of equation (1) are all coprime.
Using unique factorisation in $D = \mathbb{Z}[\zeta_p]$ one therefore has

$$x + \zeta_p y = \epsilon\alpha^p$$

for some $\alpha \in D$. Similarly, considering $x^p + (-z)^p = (-y)^p$ one has

$$x - \zeta_p z = \epsilon_1 \alpha_1^p$$

for some $\alpha_1 \in D$.
Now observe that if $\alpha = \sum_{i=0}^{p-2} a_i \zeta_p^i$ then $\alpha^p \equiv M := \sum_{i=0}^{p-2} a_i \mod p$. Writing $\epsilon = \zeta_p^s \eta$ as in Kummer's Lemma we have

$$x + \zeta_p y \equiv \zeta_p^s \eta M \mod p.$$

Taking complex conjugates

$$\zeta_p^s (x + \zeta_p^{-1} y) \equiv \eta M \mod p.$$

Hence

$$x\zeta_p^s - x\zeta_p^{-s} + y\zeta_p^{s-1} - y\zeta_p^{1-s} \equiv 0 \mod p.$$

Since $p \nmid xy(x+y)$ this is only possible if $\zeta_p^s = \zeta_p^{1-s}$. In other words, $s = (p+1)/2$, which implies $x \equiv y \mod p$.
Repeating the analysis for $x - \zeta_p z = \epsilon_1 \alpha_1^p$ one gets $x \equiv -z \mod p$, from which one deduces $p \mid x$. □

Theorem 34.6. (Kummer's second case of FLT) Let $p \geq 5$ be a prime such that $\mathbb{Q}(\zeta_p)$ has class number 1. There are no $x, y, z \in \mathbb{N}$ such that $x^p + y^p = z^p$ and $p \mid x$ or $p \mid y$ or $p \mid z$.
For proof see Section 5.7.1 of Borevich and Shafarevich.

Definition 34.7. A prime $p \geq 5$ is *regular* if p does not divide the class number of $\mathbb{Q}(\zeta_p)$. Otherwise it is called *irregular*.

Kummer's Theorem: If p is a regular prime then there are no solutions $x, y, z \in \mathbb{N}$ to $x^p + y^p = z^p$.

Theorem 34.8. A prime $p \geq 5$ is regular if none of the numbers

$$S_k = \sum_{i=1}^{p-1} i^k$$

for $i = 2, 4, \ldots, p-3$ is divisible by p.

The first 10 irregular primes are 37, 59, 67, 101, 103, 131, 149, 157, 233, 257.

Theorem 34.9. There are infinitely many irregular primes.