Let $A, B \in \mathbb{Z}$, $P = (x_P, y_P) \in E(\mathbb{Q})$ and let p be a prime. One can try to reduce P modulo p. Two things can go wrong:

(1) $4A^3 + 27B^2 \equiv 0 \mod p$, or $p = 2$, and so E is not an elliptic curve over $\mathbb{F}_p$;
(2) $P = (x_1/x_2, y_1/y_2)$ where $p \mid x_2$ or $p \mid y_2$.

Definition 26.1. Let p be a prime. Then p is called a *prime of good reduction* if $p > 2$ and $p \nmid (4A^3 + 27B^2)$. If p is a prime of good reduction then define

$$E^{(p,1)} = \{P \in E(\mathbb{Q}) : P = (x_1/x_2, y_1/y_2), \gcd(x_1, x_2) = \gcd(y_1, y_2) = 1, p \mid x_2 \text{ or } p \mid y_2\} \cup \{\infty\}.$$

Lemma 26.2. Let $(x_1/x_2, y_1/y_2) \in E^{(p,1)}$ as above. Then there is some $n \in \mathbb{N}$ such that $p^{2n} \| x_2$ and $p^{3n} \| y_2$.

Lemma 26.3. $E^{(p,1)}$ is a subgroup of $E(\mathbb{Q})$.

Theorem 26.4. Let p be a prime of good reduction of $E(\mathbb{Q})$. Then $E(\mathbb{F}_p)$ is a group, reduction modulo p is a group homomorphism, and $E(\mathbb{Q})/E^{(p,1)}$ is a subgroup of $E(\mathbb{F}_p)$.

Application 26.5. One can use reduction modulo p to give information about points of finite order in $E(\mathbb{Q})$. If $[n]P = \infty$ in $E(\mathbb{Q})$ then either $P \in E^{(p,1)}$ or $[n]P = \infty$ in $E(\mathbb{F}_p)$.

Example 26.6. $E : y^2 = x^3 + 2x + 7$.
$\#E(\mathbb{F}_{241}) = 3 \cdot 73$, $\#E(\mathbb{F}_{281}) = 283$, $\#E(\mathbb{F}_{307}) = 2^3 \cdot 41$.
This suggests $E(\mathbb{Q})$ has no non-trivial points of finite order. Indeed, this is true. The point $(-1, 2) \in E(\mathbb{Q})$ has infinite order.

Example 26.7. $E : y^2 = x^3 + x + 2$. $P = (1, 2)$ has order 4.
$\#E(\mathbb{F}_{227}) = 2^2 \cdot 59$, $\#E(\mathbb{F}_{229}) = 2^2 \cdot 5 \cdot 11$, $\#E(\mathbb{F}_{233}) = 2^8$, $\#E(\mathbb{F}_{239}) = 2^3 \cdot 29$.
This suggests $E(\mathbb{Q})$ has no other points of finite order. Indeed, $\#E(\mathbb{Q}) = 4$.

Theorem 26.8. Let $A, B \in \mathbb{Z}$ be such that $4A^3 + 27B^2 \neq 0$. If $(x, y) \in E(\mathbb{Q}) - \{\infty\}$ has finite order then $x, y \in \mathbb{Z}$ and $y = 0$ or $y^2 \mid (4A^3 + 27B^2)$.

Theorem 26.9. (Mazur) If $P \in E(\mathbb{Q})$ has finite order n then $n \leq 12$.

Theorem 26.10. (Hasse) $|p + 1 - \#E(\mathbb{F}_p)| < 2\sqrt{p}$.

Exercise 26.11. Let $E : y^2 = x^3 + x + 3$. Determine the primes of good reduction. Compute $\#E(\mathbb{F}_5)$ and $\#E(\mathbb{F}_7)$. Given that $\#E(\mathbb{F}_{233}) = 11 \cdot 23$ what is your guess for the order of the point $P = (-1, 1)$?