Theorem (Nagell-Lutz). *Let $A, B \in \mathbb{Z}$ with $\Delta := -16 \cdot (4A^3 + 27B^2) \neq 0$. Let $E : y^2 = x^3 + Ax + B =: f(x)$. Let $\infty \neq P \in E(\mathbb{Q})_{\text{tors.}}$. Then:*

- *$x(P), y(P) \in \mathbb{Z}$, and*
- *either $y(P) = 0$ or else $y(P)^2 \mid \Delta$.*

Proof. The first claim implies the second because $2 \cdot P \in E(\mathbb{Q})_{\text{tors.}}$,

$$x(2 \cdot P) = \frac{f'(x(P))^2}{4 \cdot f(x(P))} - 2 \cdot x(P),$$

and Δ is a $\mathbb{Z}$-linear combination of $y^2 = f(x)$ and $f'(x)^2$.

Now write $\varphi_n \in \mathbb{Z}[x, y, A, B]$ for the usual division polynomials, so that

$$x(n \cdot Q) = \frac{x \cdot \varphi_n(x,y)^2 - \varphi_{n-1}(x,y) \cdot \varphi_{n+1}(x,y)}{\varphi_n(x,y)^2} =: \frac{\text{num.}_n(x,y)}{\text{den.}_n(x,y)}$$

when $Q =: (x, y) \in E$. From the defining recurrence we see that $\text{num.}_n(x,y), \text{den.}_n(x,y) \in \mathbb{Z}[x, A, B] \subsetneq \mathbb{Z}[x, y, A, B]/(y^2 - f(x))$ and have degrees n^2 and $n^2 - 1$ in x and leading coefficients 1 and n^2, respectively. Also recall that $\varphi_2(x, y) = 2y$ and $\varphi_n(x, y) \in \mathbb{Z}[x, A, B]$ when n is odd.

Write now $x(P) =: \frac{s}{d^2}$ with $s, d \in \mathbb{Z}$ and $(s, d) = 1$. Thus, clearing denominators, $x(n \cdot P) = \frac{s^{n^2} + (\in d^2 \cdot \mathbb{Z})}{(\in d^2 \cdot \mathbb{Z})}$, so that if $x(n \cdot P) \in \mathbb{Z}$ then certainly $d = 1$, i.e. $x(P) \in \mathbb{Z}$ (and consequently $y(n \cdot P), y(P) \in \mathbb{Z}$ as well).

Let m be the order of $(x, y) \in E(\mathbb{Q})_{\text{tors.}}$ and $p \mid m$ a prime. It therefore suffices to show the first claim for $\frac{m}{p} \cdot (x, y)$, i.e. to assume without loss of generality that (x, y) has prime order p. By definition this means that $\text{den.}_p(x, y) = 0$, so $\varphi_p(x, y) = 0$. If $p = 2$ then $y = 0$ and we are done. Otherwise p is odd and so, writing $x =: \frac{s}{d^2}$ and clearing denominators, we find that $p \cdot s^{\frac{p^2-1}{2}} + (\in d^2 \cdot \mathbb{Z}) = 0$, so $d^2 \mid p$, whence $d = 1$. ∎