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 $2 \cdot P \in E(\mathbb{Q})_{\text{tors.}}$,

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

and the resultant of $y^2 = f(x)$ and $f'(x)^2$ divides Δ.

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

$$x(n \cdot Q) = \frac{X \cdot \varphi_n(X,Y)^2 - \varphi_{n-1}(X,Y) \cdot \varphi_{n+1}(X,Y)}{\varphi_n(X,Y)^2}$$

when $Q =: (X, Y) \in E$. Recall that, from e.g. the defining recurrence,

$$x \cdot \varphi_n(x,y)^2 - \varphi_{n-1}(x,y) \cdot \varphi_{n+1}(x,y), \varphi_n(x,y)^2 \in \mathbb{Z}[x, A, B] \hookrightarrow \mathbb{Z}[x, y, A, B]/(y^2 - f(x))$$

have degrees n^2 and $n^2 - 1$ in x and leading coefficients 1 and n^2, respectively. Moreover the coefficient of x^{n^2-2} in $\varphi_n(x, y)^2$ is 0.

Write now $x(P) =: \frac{s}{d^2}$ with $d, s \in \mathbb{Z}$ and $(d, s) = 1$. 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 $P \in E(\mathbb{Q})_{\text{tors.}}$ and $p \mid m$ a prime. It therefore suffices to show the first claim for $\frac{m}{p} \cdot P$, i.e. to assume without loss of generality that P has prime order p. By definition this means that $\varphi_p(P)^2 = 0$. Clearing denominators, we find that $p^2 \cdot s^{n^2-1} + (\in d^4 \cdot \mathbb{Z}) = 0$, and so $d = 1$. □