A solution to exercise V.5.10 in Silverman's *Arithmetic of Elliptic Curves*. I'm skipping the computations in (c) and (d).

Exercise

Let $E/\mathbb{F}_q$ be an elliptic curve, let $\phi\colon E \to E$ be the q^{th}-power Frobenius endomorphism, and let $p = \operatorname{char}(\mathbb{F}_q)$.

(a) Prove that E is supersingular if and only if

$$\operatorname{Tr}(\phi) \equiv 0 \pmod p.$$

(b) Suppose $q = p \geq 5$ is prime. Prove that E is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.

(e) Let p^i be the largest power of p such that $p^{2i} \mid q$. Prove that

$$\operatorname{Tr}(\phi) \equiv 0 \pmod p \equiv \operatorname{Tr}(\phi) \equiv 0 \pmod{p^i}.$$

(f) Prove that there do not exist any elliptic curves $E/\mathbb{F}_8$ satisfying either $\#E(\mathbb{F}_8) = 7$ or 11.

Proof. (a) This fact is actually embedded in the proof of Theorem 4.1 in the same chapter. We have that $\phi + \hat{\phi} = [\operatorname{Tr}(\phi)]$, so $\hat{\phi} = [\operatorname{Tr}(\phi)] - \phi$. So, $\operatorname{Tr}(\phi)$ is divisible by p if and only if $\hat{\phi}$ is inseparable by III.5.5, and therefore E is supersingular by V.3.1.

(b) By Hasse's theorem, we know that $\#E(\mathbb{F}_p) = p + 1 + \operatorname{Tr}(\phi)$, and $|\operatorname{Tr}(\phi)| \leq 2\sqrt{p}$. If $\operatorname{Tr}(\phi) \equiv 0 \pmod p$, then it must be 0 since $2\sqrt{p} < p$ (since we've assumed $p \geq 5$).

(e) Let ψ be the p-power Frobenius map. Let α, β be the roots of the characteristic polynomial of ψ. Then $\operatorname{Tr}(\psi^k) = \alpha^k + \beta^k$. Using the Newton identities for power symmetric polynomials, we have

$$\operatorname{Tr}(\psi^2) = (\operatorname{Tr}\psi)^2 - 2p,$$

and for $k > 2$

$$\operatorname{Tr}(\psi^k) = (\operatorname{Tr}\psi)(\operatorname{Tr}\psi^{k-1}) - p(\operatorname{Tr}\psi^{k-2}).$$

Thus, by induction we have that $\operatorname{Tr}(\psi^k) \equiv \operatorname{Tr}(\psi) \pmod p$, so if $\operatorname{Tr}(\phi) \equiv 0$ we must also have $\operatorname{Tr}(\psi) \equiv 0$. Let us track the p-adic valuation of $\operatorname{Tr}\psi^k$ through the recurrence. Let $V_k = v_p(\operatorname{Tr}\psi^k)$, then if $\operatorname{Tr}\psi$ is divisible by p, the recurrence relation above gives us that $V_k \geq 1 + \min(V_{k-1}, V_{k-2})$. This immediately gives us the statement in the problem.

For part (f), we will need this easy observation about the above construction: if $p = 2$, we in fact have that $\operatorname{Tr}\psi^2 \equiv 0 \pmod 4$. This means that when $p = 2$, we get the slightly better statement that $\operatorname{Tr}\phi \equiv 0 \pmod{p^j}$ where j is the greatest integer such that $p^{2j-1} \mid q$.

(f) If $\#E(\mathbb{F}_8) = 7$ or 11, then $\operatorname{Tr}(\phi) = \pm 2$, so $\operatorname{Tr}(\phi) \equiv 0 \pmod 2$. From our final comments in part (e), this implies that $\operatorname{Tr}(\phi) \equiv 0 \pmod 4$, and but that contradicts $\operatorname{Tr}(\phi) = \pm 2$.