MATH 350 ASSIGNMENT 10, FALL 2015

Due in class on Monday, November 23

The following problems are about Hensel's lemma, which was discussed in class on November 6th, 13th and 16th. Hensel's lemma is usually found in more advanced books on algebra or number theory; it is not treated in Silverman's book. (You can find a statement of it in wikipedia.)

1. Let p be a prime number. Combine the version of Hensel's lemma given in class and quadratic reciprocity to give a *sufficient condition* for a general monic quadratic polynomial

$$f(X) = X^2 + bX + c \in \mathbb{Z}[X]$$

with integer coefficients to have solutions in $\mathbb{Z}/p^n\mathbb{Z}$ for *every* positive integer n. Please provide a *complete proof*.

2. (a more general version of Hensel's lemma) Let $f(X)$ be a polynomial with integer coefficients. Let p be a prime number. Recall that

$$\mathrm{ord}_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$$

is the function such that $\mathrm{ord}_p(0) = \infty$,

$$n \equiv 0 \pmod{p^{\mathrm{ord}_p(n)}} \quad \text{and} \quad n \not\equiv 0 \pmod{p^{1+\mathrm{ord}_p(n)}}$$

for every non-zero integer n. Suppose that a_0 is an integer such that $f'(a_0) \neq 0$ and

$$2\mathrm{ord}_p(f'(a_0)) < \mathrm{ord}_p(f(a_0)).$$

Here $f'(X)$ is the derivative of the polynomial $f(X)$. Show that for every positive integer n, there exists an integer b_n such that

$$f(b_n) \equiv 0 \pmod{p^n} \quad \text{and} \quad \mathrm{ord}_p(b_n - a_0) \geq \mathrm{ord}_p(f(a_0)) - \mathrm{ord}_p(f'(a_0)) > 0$$

3. (extra credit) (a) Use the more general version of Hensel's lemma in problem 2 to give a better (more general) sufficient condition to problem 1, with a complete proof.

(b) Is the sufficient condition you obtain also necessary? Either provide a proof, or give a counter-example.