MA2316: Introduction to Number Theory
Tutorial problems for February 20, 2014

"Polynomial congruences and Hensel's Lemma"

1. Prove that for each odd prime p, for each a coprime to p, and for each n, the congruence $x^2 \equiv a \pmod{p^n}$ has at most two solutions.

2. Find all solutions to the congruence $x^2 \equiv 2 \pmod{7^4}$.

3. Find all solutions to the congruence $x^2 \equiv -3 \pmod{13^3}$.

4. Show that for every prime $p \neq 2, 17$ the polynomial $(x^2-2)(x^2-17)(x^2-34)$ has roots in $\mathbb{Z}/p^n\mathbb{Z}$ for all n.

5. Show that for $p = 2$ and for $p = 17$ the polynomial $(x^2-2)(x^2-17)(x^2-34)$ also has roots in $\mathbb{Z}/p^n\mathbb{Z}$ for all n.

6. Show that for every prime $p \neq 2, 3$ the polynomial $(x^3-37)(x^2+3)$ has roots in $\mathbb{Z}/p^n\mathbb{Z}$ for all n. (*Hint*: if $p \not\equiv 1 \pmod 3$, the mapping $x \mapsto x^3$ of the group $(\mathbb{Z}/p\mathbb{Z})^\times$ to itself is injective.)

7. Show that for $p = 2$ and for $p = 3$ the polynomial $(x^3-37)(x^2+3)$ also has roots in $\mathbb{Z}/p^n\mathbb{Z}$ for all n. (*Hint*: if $p \not\equiv 1 \pmod 3$, the mapping $x \mapsto x^3$ of the group $(\mathbb{Z}/p\mathbb{Z})^\times$ to itself is injective.)