Math 40520 Theory of Number
Homework 10

Due Wednesday, 12/7

Do 5.

1. Suppose $P(X) \in \mathbb{Z}[X]$, p is a prime, $P(a) \equiv 0 \pmod{p^n}$ for an integer a such that $P'(a) \equiv 0 \pmod{p^n}$. This means we cannot apply, as stated in class, Hensel's lifting lemma. Show that there are only two possibilities:
   (a) Either $P(a) \equiv 0 \pmod{p^{n+1}}$, in which case ALL numbers $\equiv a \pmod{p^n}$ (namely $a, a + p^n, a + 2p^n, \ldots, a + (p-1)p^n$) are roots of $P(X) \equiv 0 \pmod{p^{n+1}}$ lifting $a \pmod{p^n}$, or
   (b) $P(a) \not\equiv 0 \pmod{p^{n+1}}$, in which case there are NO solutions of $P(X) \equiv 0 \pmod{p^{n+1}}$ lifting $a \pmod{p^n}$.

2. Determine all the roots of the equation $X^5 - 2X^3 - 20X + 6 \equiv 0 \pmod{3^4}$. [Hint: You may/should use the previous problem, without proof.]

3. Find all solutions of the equation $X^3 - X - 1 \equiv 0 \pmod{7^4}$.

4. Show that the polynomial
$$P(X) = (X^2 - 13)(X^2 - 17)(X^2 - 13 \cdot 17)$$
has solutions modulo every positive integer.

5. Consider the equation $x^2 + 11y^2 = 3$.
   (a) Find the smallest rational solution, i.e., $x, y \in \mathbb{Q}$ with smallest possible numerator and denominator. In particular, that this equation has no integer solutions.
   (b) Show that for all n it has solutions mod 2^n of the form $(0, y)$. [Hint: Recall that $x^2 \equiv u \pmod{2^n}$ has solutions for all n as long as $u \equiv 1 \pmod 8$.]
   (c) Show that $x^2 + 11y^2 \equiv 3 \pmod N$ has solutions modulo every positive integer N.

6. Find all rational numbers x and y satisfying the equation $x^2 + y^2 = 5$.

7. Find all rational numbers x and y satisfying the equation $x^2 + 2xy + 3y^2 = 2$.

8. In this exercise you will solve the equation
$$x^2 + y^2 + z^2 = 1$$
with $x, y, z \in \mathbb{Q}$. Clearing denominators, this gives a complete list of rectangular boxes whose sides and long diagonal are integers.

(a) Suppose $(x, y, z) \neq (0, 0, 1)$ is a solution. Let (a, b) be the point of intersection of the (xy)-plane with the line through (x, y, z) and $(0, 0, 1)$. Show that

$$\frac{x}{a} = \frac{y}{b} = 1 - z$$

(b) Show, mimicking the procedure from the Pythagorean triples case, that every rational solution of the diophantine equation (other than $(0, 0, 1)$) is of the form

$$x = \frac{2a}{1 + a^2 + b^2} \qquad y = \frac{2b}{1 + a^2 + b^2} \qquad z = \frac{a^2 + b^2 - 1}{1 + a^2 + b^2}$$

for rationals a, b.