MA 341: Advanced Problems for Fun: # 3

In this set we'll explore the relationships between solving congruence equations $f(x) \equiv 0 \bmod p$ and $f(x) \equiv 0 \bmod p^k$ where p is prime. Once we understand this well enough, by the CRT we will understand how to solve $f(x) \equiv 0 \bmod n$ for general n once we can solve $f(x) \equiv 0 \bmod p$ for p prime, thus completing the reduction to the prime modulus case. We'll push these ideas far enough to discover an important number system used widely in modern number theory.

1. Let $f(x) = x^2 - 4x + 3$. Solve $f(x) \equiv 0 \bmod 5$. Then solve $f(x) \equiv 0 \bmod 25$.
2. Compare with $f(x) = x^2 - 3x + 1$. Solve $f(x) \equiv 0 \bmod 5$ and then again $\bmod 25$.
3. Suppose $f(a) \equiv 0 \bmod p$ where $f(x) = x^2 + bx + c$. Show there exists a unique $A \in \mathbb{Z}_{p^2}$ such that $f(A) \equiv 0 \bmod p^2$ and $A \equiv a \bmod p$ if $2a + b \not\equiv 0 \bmod p$. (This process is called "lifting" a solution mod p to one mod p^2.)
4. In general, show if $f(a) \equiv 0 \bmod p$, then there exists unique $A \in \mathbb{Z}_{p^2}$ with $f(A) \equiv 0 \bmod p$ and $A \equiv a \bmod p$ if $f'(a) \not\equiv 0 \bmod p$.
5. Show by example the converse to the above fails: i.e. there may or may not exist solutions to $f(A) \equiv 0 \bmod p^2$ with $A \equiv a \bmod p$ if $f'(a) \equiv 0 \bmod p$.
6. Show if $f(a) \equiv 0 \bmod p$ and $f'(a) \not\equiv 0 \bmod p$, then there exists a unique $A_k \in \mathbb{Z}_{p^k}$ with $f(A_k) \equiv 0 \bmod p^k$ and $A_k \equiv a \bmod p$ for all $k \geq 1$.
7. Let $\mathcal{O}_p$ be the following ring[1]: the elements are sequences (a_k) where $a_k \in \mathbb{Z}_{p^k}$ and $a_{k+1} \equiv a_k \bmod p^k$ for all k. Let $p = 3$. Write down some examples of elements in $\mathcal{O}_3$. You can add them term by term. How should we multiply them?
8. Let $p \equiv 1 \bmod 4$. Show that the polynomial $x^2 + 1$ has a solution in the ring $\mathcal{O}_p$.
9. Determine the units in $\mathcal{O}_p$.
10. Write down a polynomial with no roots in $\mathcal{O}_p$. (Hint: Your answer may depend on p.)
11. Show that we may view $\mathbb{Z}$ inside of $\mathcal{O}_p$ for any p: send $n \in \mathbb{Z}$ to the sequence $(n \bmod p^k)$. Show no 2 integers map to the same place, but generally there are elements of $\mathcal{O}_p$ not in $\mathbb{Z}$.

[1] These are one way of representing p-adic integers, where p is acting like a variable. So there are 2-adic, 3-adic, 5-adic numbers, etc.