Solving polynomial congruences modulo prime powers

Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime.

Definition. Let x_0 be a reduced solution to $f(x) \equiv 0 \mod p^e$ for some $e \in \mathbb{N}$. A **lift of** x_0 is a reduced solution y to the congruence $f(x) \equiv 0 \mod p^{e+1}$ satisfying $y \equiv x_0 \mod p^e$.

It is clear that any reduced solution to $f(x) \equiv 0 \mod p^{e+1}$ arises as a lift of unique reduced solution to $f(x) \equiv 0 \mod p^e$.

Definition. A solution x_0 to $f(x) \equiv 0 \mod p^e$ will be called

regular if $p \nmid f'(x_0)$ and

singular if $p \mid f'(x_0)$

The following is the main result describing the possible number and type of lifts.

Lifting Theorem: *Let x_0 be a reduced solution to $f(x) \equiv 0 \mod p^e$*

(a) If x_0 is a regular solution, then x_0 has a unique lift.

(b) If x_0 is a singular solution, then x_0 has either p lifts or no lifts.

(c) Lifts of regular solutions are regular and lifts of singular solutions are singular.

Parts (a) and (c) imply the following:

Corollary: *If for some $e \in \mathbb{N}$ the congruence $f(x) \equiv 0 \mod p^e$ has k reduced solutions and all these solutions are regular, then the congruence $f(x) \equiv 0 \mod p^f$ has k reduced solutions for any $f \geq e$.*

Lifting solutions mod p to solutions mod p^2.

Write our polynomial $f(x)$ in the standard form $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with $a_n \neq 0$, and assume that $p \nmid a_i$ for some i, and let $\phi(x) = [a_n]x^n + \ldots + [a_1]x + [a_0] \in \mathbb{Z}_p[x]$ (thus ϕ is obtained from f by replacing each coefficient by its congruence class mod p). As discussed in class, there is a natural bijection between reduced solutions to $f(x) \equiv 0 \mod p$ and roots of $\phi(x)$, namely if $x_0 \in \mathbb{Z}$ with $0 \leq x_0 \leq p-1$, then

x_0 is a solution to $f(x) \equiv 0 \bmod p \iff [x_0]$ is a root of ϕ (***)

The assumption $p \nmid a_i$ for some i is equivalent to $\phi \neq 0$ (as a polynomial); since $\mathbb{Z}_p$ is a field, it implies that ϕ has at most $n = \deg(f)$ roots.

Now note that for any $x_0 \in \mathbb{Z}$ we have

(i) $p \mid f'(x_0) \iff \phi'([x_0]) = [0]$ and so

(ii) $p \nmid f'(x_0) \iff \phi'([x_0]) \neq [0]$

Thus, we can extend the observation (***) as follows. Suppose $x_0 \in \mathbb{Z}$ and $0 \leq x_0 \leq p - 1$. Then

(i) x_0 is a *singular* solution to $f(x) \equiv 0 \bmod p \iff [x_0]$ is a common root of ϕ and ϕ'

(ii) x_0 is a *regular* solution to $f(x) \equiv 0 \bmod p \iff [x_0]$ is a root of ϕ and not a root of ϕ'.

The point of this observation is that if we want to determine solutions mod p and their lifting types (singular or regular), all the relevant information can be expressed in terms of ϕ (which is a polynomial over a field and hence is easier to work with than f).