Polynomial Congruences and Hensel's Lemma

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Via the CRT, the quadratic congruence $X^2 \equiv a \pmod{n}$ can be reduced to a system of congruences of the form $X^2 \equiv a \pmod{p^e}$, where p is prime.

For odd primes, one can show that solutions of $X^2 \equiv a \pmod{p}$, whose existence can be ascertained by evaluating the Legendre symbol $\left(\frac{a}{p}\right)$, uniquely "lift" to solutions modulo p^n for $n \geq 2$.

The techniques involved apply equally as well to the more general congruence $f(X) \equiv 0 \pmod{p^n}$, where $f(X)$ is a polynomial with integer coefficients, so this is where we choose to begin.

Polynomial Congruences and the CRT

Let $\mathbb{Z}[X]$ denote the ring of all polynomials in X with integer coefficients.

For $f(X) \in \mathbb{Z}[X]$ and $n \in \mathbb{N}$ we will be interested in the polynomial congruence

$$f(X) \equiv 0 \pmod{n}. \tag{1}$$

If $n = p_1^{e_1} p_2^{e^2} \cdots p_r^{e_r}$ is the canonical form of n, the CRT implies that (1) is equivalent to the system

$$f(X) \equiv 0 \pmod{p_i^{e_i}}, \;\; 1 \leq i \leq r.$$

Specifically, if R_i denotes the set of solutions to $f(X) \equiv 0 \pmod{p_i^{e_i}}$, then for each choice of $r_i \in R_i$ the solution to the system

$$X \equiv r_i \pmod{p_i^{e_i}}, \quad 1 \leq i \leq r,$$

provides a solution to $f(X) \equiv 0 \pmod{n}$, and *every* solution to the latter is obtained in this way.

So it suffices to assume that $n = p^e$ for some prime p and $e \in \mathbb{N}$.

Write $f(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$ with $a_i \in \mathbb{Z}$ and $d \geq 1$.

For convenience we assume $p \nmid a_d$.

Derivatives of Polynomials

Definition

For $f(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X]$ we define its formal derivative to be

$$Df(X) = d a_d X^{d-1} + (d-1) a_{d-1} X^{d-2} + \cdots + a_1 .$$

Remarks.

- The derivative Df is *purely algebraic*. We *do not* take limits to obtain it (as in Calculus).
- If $a \in \mathbb{Z}$, then $Da = D(aX^0) = 0$.
- One can show that the formal derivative is linear and obeys the product rule. That is, for $f, g \in \mathbb{Z}[X]$ and $a, b \in \mathbb{Z}$ one has

$$D(af + bg) = aDf + bDg \quad \text{and} \quad D(fg) = fDg + gDf .$$

Let $a \in \mathbb{Z}$. Recall that for any $f(X) \in \mathbb{Z}[X]$ there exists a unique $\widetilde{f}(X) \in \mathbb{Z}[X]$ so that

$$f(X) = (X - a)\widetilde{f}(X) + f(a). \tag{2}$$

Operating at the level of rational functions for a moment, this says that

$$\widetilde{f}(X) = \frac{f(X) - f(a)}{X - a},$$

which suggests that $\widetilde{f}(a) = Df(a)$.

This is indeed the case. If we differentiate (2) and apply the product rule, we have

$$Df(X) = \widetilde{f}(X) + (X - a)D\widetilde{f}(X) \;\Rightarrow\; Df(a) = \widetilde{f}(a).$$

We are now in a position to prove our main result on polynomial congruences with prime power moduli.

Theorem 1 (Hensel's Lemma)

Let p be a prime and let $f(X) \in \mathbb{Z}[X]$. If there exists an $r_1 \in \mathbb{Z}$ so that $f(r_1) \equiv 0 \pmod{p}$ and $Df(r_1) \not\equiv 0 \pmod{p}$, then there exists a sequence $\{r_n\}_{n \in \mathbb{N}}$ of integers satisfying:

1. $r_{n+1} \equiv r_n \pmod{p^n}$ *for all* $n \geq 1$.
2. $f(r_n) \equiv 0 \pmod{p^n}$ *for all* $n \geq 1$.

Moreover, r_n is unique modulo p^n for $n \geq 2$.

Proof. To prove the existence of r_n we induct on n, the case $n = 1$ being provided by our hypotheses.

So suppose $n \geq 1$ and we have found r_k for $1 \leq k \leq n$ satisfying conditions **1** and **2**.

Write $f(X) = (X - r_n)\widetilde{f}(X) + f(r_n)$ with $\widetilde{f}(X) \in \mathbb{Z}[X]$.

Since $f(r_n) \equiv 0 \pmod{p^n}$, we can write $f(r_n) = ap^n$ for some $a \in \mathbb{Z}$.

For $b \in \mathbb{Z}$, consider $r = r_n + bp^n$. Clearly $r \equiv r_n \mod p^n$, and we have

$$f(r) = bp^n\widetilde{f}(r) + f(r_n) = (b\widetilde{f}(r) + a)p^n.$$

Since $r \equiv r_n \equiv r_{n-1} \equiv r_{n-1} \equiv \cdots \equiv r_1 \pmod{p}$, we also have

$$\widetilde{f}(r) \equiv \widetilde{f}(r_n) \equiv Df(r_n) \equiv Df(r_1) \not\equiv 0 \pmod{p}.$$

Because $Df(r_1) \not\equiv 0 \pmod{p}$, there is a unique b_{n+1} (modulo p) solving the linear congruence

$$b_{n+1} Df(r_1) \equiv -a \pmod{p}.$$

Taking $r_{n+1} = r = r_n + b_{n+1} p^n$, we then have

$$b_{n+1} \widetilde{f}(r_{n+1}) \equiv b_{n+1} \widetilde{f}(r_n) \equiv b_{n+1} Df(r_1) \equiv -a \pmod{p}.$$

Thus

$$f(r_{n+1}) = \underbrace{\left(b_{n+1} \widetilde{f}(r_{n+1}) + a\right)}_{\text{div. by } p} p^n \equiv 0 \pmod{p^{n+1}}.$$

This completes the induction and proves the existence of the sequence $\{r_n\}$.

To prove uniqueness, suppose that $\{s_n\}$ is another sequence satisfying **1** and **2**.

We will inductively prove that $s_n \equiv r_n \pmod{p^n}$ for all $n \geq 1$. We have $r_1 \equiv s_1 \pmod{p}$ by definition.

Now assume that $r_n \equiv s_n \pmod{p^n}$ for some $n \geq 1$ and write $f(X) = (X - r_{n+1})\widetilde{f}(X) + f(r_{n+1})$ with $\widetilde{f}(X) \in \mathbb{Z}[X]$.

We then have

$$\begin{aligned} 0 \equiv f(s_{n+1}) &\equiv (s_{n+1} - r_{n+1})\widetilde{f}(s_{n+1}) + f(r_{n+1}) \pmod{p^{n+1}} \\ &\equiv (s_{n+1} - r_{n+1})\widetilde{f}(s_{n+1}) \pmod{p^{n+1}}. \end{aligned}$$

That is, $p^{n+1} | (s_{n+1} - r_{n+1})\widetilde{f}(s_{n+1})$.

However, working modulo p we have

$$\widetilde{f}(s_{n+1}) \equiv \widetilde{f}(s_n) \equiv \widetilde{f}(r_n) \equiv \widetilde{f}(r_{n+1}) \equiv Df(r_{n+1}) \equiv Df(r_1) \pmod{p}.$$

Since $Df(r_1) \not\equiv 0 \pmod{p}$ and p is prime, this implies that $(\widetilde{f}(s_{n+1}), p^{n+1}) = 1$.

Therefore, by Euclid's lemma we have

$$\begin{aligned} p^{n+1} | (s_{n+1} - r_{n+1})\widetilde{f}(s_{n+1}) &\Rightarrow p^{n+1} | s_{n+1} - r_{n+1} \\ &\Leftrightarrow s_{n+1} \equiv r_{n+1} \pmod{p^{n+1}}. \end{aligned}$$

This completes the induction and proves the uniqueness of the sequence $\{r_n\}$. $\square$

Remark

The proof of Hensel's lemma recursively constructs the solution $\{r_n\}$ of solutions to $f(X) \equiv 0 \pmod{p^n}$ starting from $f(r_1) \equiv 0 \pmod{p}$.

If we dissect the proof a bit, we find that $r_{n+1} = r_n + b_{n+1}p^n$, where $b_{n+1}Df(r_n) \equiv b_{n+1}Df(r_1) \equiv -a \pmod{p}$.

Since $p \nmid Df(r_n)$, we can write this final congruence as

$$b_{n+1} \equiv \frac{-a}{Df(r_n)} \pmod{p} \;\Leftrightarrow\; b_{n+1}p^n \equiv \frac{-ap^n}{Df(r_n)} \pmod{p^{n+1}},$$

where the inversion is meant to take place in $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$.

Since $f(r_n) = ap^n$, this tells us that

$$r_{n+1} \equiv r_n - \frac{f(r_n)}{Df(r_n)} \pmod{p^{n+1}}.$$

Compare this to *Newton's Method* for finding *real* solutions to $f(X) = 0$, which starts with an initial approximation x_1, then recursively forms

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

One can show that the sequence of integers $\{r_n\}$ successively approximates a true solution to $f(X) = 0$ in the ring $\mathbb{Z}_p$ of *p-adic integers*.

Example 1

Solve the polynomial congruence $X^3 - 2 \equiv 0 \pmod{5^n}$ for $1 \le n \le 6$.

Solution. When $n = 1$, one easily checks that $r_1 \equiv 3 \pmod 5$ is the only solution.

Hensel's lemma implies that for each $n \geq 1$ there is a unique solution r_n modulo 5^n, and it is given recursively by

$$r_{n+1} \equiv r_n - \frac{r_n^3 - 2}{3r_n^2} \pmod{5^{n+1}}.$$

We therefore have

$$\begin{aligned}
r_2 &\equiv 3 - \frac{3^3-2}{3\cdot 3^2} \equiv 3 - \frac{0}{2} \equiv 3 \pmod{5^2},\\
r_3 &\equiv 3 - \frac{3^3-2}{3\cdot 3^2} \equiv 3 - \frac{25}{27} \equiv 53 \pmod{5^3},\\
r_4 &\equiv 53 - \frac{53^3-2}{3\cdot 53^2} \equiv 53 - \frac{125}{302} \equiv 303 \pmod{5^4},\\
r_5 &= 303 - \frac{303^3-2}{3\cdot 303^2} \equiv 303 - \frac{2500}{427} \equiv 2178 \pmod{5^5},\\
r_6 &= 2178 - \frac{2178^3-2}{3\cdot 2178^2} \equiv 5303 \pmod{5^6}.
\end{aligned}$$

When expressed in base 5 these yield the 5-adic root

$$3 + 0\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4 + 1\cdot 5^5 + \cdots$$

of X^3-2. $\square$

Quadratic Congruences

Let p be an odd prime and consider the congruence

$$f(X) = aX^2 + bX + c \equiv 0 \pmod{p}$$

with $p \nmid a$ and discriminant $\Delta = b^2 - 4ac$.

We have shown that this has two distinct solutions modulo p if and only if $\left(\frac{\Delta}{p}\right) = 1$, both of which are given by the quadratic formula:

$$r \equiv \frac{-b \pm \sqrt{\Delta}}{2a} \equiv \frac{-b}{2a} \pm \frac{\sqrt{\Delta}}{2a} \not\equiv \frac{-b}{2a} \pmod{p},$$

since $\Delta \not\equiv 0 \pmod{p}$.

This implies that $Df(r) \equiv 2ar + b \not\equiv 0 \pmod{p}$.

Hensel's lemma therefore implies that the congruence

$$aX^2 + bX + c \equiv 0 \pmod{p^n}$$

has exactly two solutions modulo p^n for every $n \geq 1$, given by Newton's Method.

Theorem 2

Let p be an odd prime and $f(X) = aX^2 + bX + c$. If $p \nmid a$ and $\left(\frac{\Delta}{p}\right) = 1$, then the congruence $f(X) \equiv 0 \pmod{p^n}$ has exactly two solutions for each $n \geq 1$. If $r_1 \equiv \frac{-b \pm \sqrt{\Delta}}{2a} \pmod{p}$, these are given recursively by

$$r_{n+1} \equiv r_n - \frac{f(r_n)}{f'(r_n)} \pmod{p^{n+1}}.$$

Example 2

Solve the polynomial congruence $X^2 \equiv 17 \pmod{19^n}$ for $n \geq 1$.

Solution. The given congruence is equivalent to $X^2 - 17 \equiv 0 \pmod{19}$, which has discriminant

$$\Delta = 4 \cdot 17.$$

By the law(s) of quadratic reciprocity we have

$$\left(\frac{\Delta}{19}\right) = \left(\frac{17}{19}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = 1,$$

so there are two incongruent solutions modulo 19 by Theorem 2.

A quick computation shows that $(\pm 6)^2 \equiv 36 \equiv -2 \equiv 17 \pmod{19}$, so that $r_1 \equiv \pm 6 \pmod{19}$.

The general solutions are given by

$$r_{n+1} \equiv r_n - \frac{r_n^2 - 17}{2r_n} \equiv \frac{1}{2}\left(r_n + \frac{17}{r_n}\right) \pmod{19^{n+1}}.$$

With $r_1 = 6$ we obtain

$$r_2 \equiv \frac{1}{2}\left(6 + \frac{17}{6}\right) \equiv 215 \pmod{19^2},$$
$$r_3 \equiv \frac{1}{2}\left(215 + \frac{17}{215}\right) \equiv 937 \pmod{19^3},$$
$$r_4 \equiv \frac{1}{2}\left(937 + \frac{17}{937}\right) \equiv 14655 \pmod{19^4},$$

or 19-adically

$$r = 6 + 11 \cdot 19 + 2 \cdot 19^2 + 2 \cdot 19^3 + 2 \cdot 19^4 + 8 \cdot 19^5 + \cdots$$

Since the other solution modulo 19 is simply $r_1' = -r_1$, we are assured that the remaining solutions are given by

$$\begin{aligned} r_2' &\equiv -215 \equiv 146 \pmod{19^2}, \\ r_3' &\equiv -937 \equiv 5922 \pmod{19^3}, \\ r_4' &\equiv -14655 \equiv 111566 \pmod{19^4}, \end{aligned}$$

or 19-adically:

$$r' = 13 + 7 \cdot 19 + 16 \cdot 19^2 + 16 \cdot 19^3 + 16 \cdot 19^4 + 10 \cdot 19^5 + \cdots$$

$\square$

Remark. Because $\sqrt{17}$ is irrational, one can show that the 19-adic "digits" of $\sqrt{17}$ are *not* eventually periodic.