Solving Trinomials over $\mathbb{Q}_p$

Elliott Fairchild

July 27, 2021
Problem

Let \( f(x) = c_1x^{a_1} + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{Z}[x] \). How many roots of \( f \) over \( \mathbb{Z}/(p^k) \) are there, and where do they lie?
Problem

Let $f(x) = c_1 x^{a_1} + c_2 x^{a_2} + c_3 x^{a_3} \in \mathbb{Z}[x]$. How many roots of $f$ over $\mathbb{Z}/(p^k)$ are there, and where do they lie?

Can information about roots of $f$ over $\mathbb{Z}/(p)$ say anything about roots of $f$ over $\mathbb{Z}/(p^k)$?
Problem

Let \( f(x) = c_1 x^{a_1} + c_2 x^{a_2} + c_3 x^{a_3} \in \mathbb{Z}[x] \). How many roots of \( f \) over \( \mathbb{Z}/(p^k) \) are there, and where do they lie?

- Can information about roots of \( f \) over \( \mathbb{Z}/(p) \) say anything about roots of \( f \) over \( \mathbb{Z}/(p^k) \)?
- If the root is simple, then Hensel’s Lemma gives us the desired result.
Problem

Let \( f(x) = c_1 x^{a_1} + c_2 x^{a_2} + c_3 x^{a_3} \in \mathbb{Z}[x] \). How many roots of \( f \) over \( \mathbb{Z}/(p^k) \) are there, and where do they lie?

\begin{itemize}
  \item Can information about roots of \( f \) over \( \mathbb{Z}/(p) \) say anything about roots of \( f \) over \( \mathbb{Z}/(p^k) \)?
  \item If the root is simple, then Hensel’s Lemma gives us the desired result.
  \item Degenerate roots are more tricky...
\end{itemize}
Solving Trinomials

**Problem**

Let \( f(x) = c_1 x^{a_1} + c_2 x^{a_2} + c_3 x^{a_3} \in \mathbb{Z}[x] \). How many roots of \( f \) over \( \mathbb{Z}/(p^k) \) are there, and where do they lie?

- Can information about roots of \( f \) over \( \mathbb{Z}/(p) \) say anything about roots of \( f \) over \( \mathbb{Z}/(p^k) \)?
- If the root is simple, then Hensel’s Lemma gives us the desired result.
- Degenerate roots are more tricky...

**Example**

Let \( f(x) = x^2 \). Then \( f \) has a single degenerate root at 0 over \( \mathbb{Z}/(p) \), but over \( \mathbb{Z}/(p^2) \), the roots are given by \((0, p, \ldots, (p - 1)p)\).
Applications to Coding Theory

Just as strings of bits can represent words and data, we can consider a more general code $K$ written as a tuple $(q_1, \ldots, q_\rho)$ of elements of $\mathbb{Z}/(p^k)$. Applications in error-correction involve computing roots of a polynomial $G \in \mathbb{Z}/(p^k) [x][y]$ over $\mathbb{Z}/(p^k)[x]$. 
Applications to Coding Theory

Just as strings of bits can represent words and data, we can consider a more general code $K$ written as a tuple $(q_1, \ldots, q_\rho)$ of elements of $\mathbb{Z}/(p^k)$.

We can also represent $K$ with an element $F$ of $(\mathbb{Z}/(p^k))[x]_{<\rho}$ by letting $q_i$ equal the coefficient of $x^{i-1}$. 
Applications to Coding Theory

• Just as strings of bits can represent words and data, we can consider a more general code $K$ written as a tuple $(q_1, \ldots, q_\rho)$ of elements of $\mathbb{Z}/(p^k)$.

• We can also represent $K$ with an element $F$ of $(\mathbb{Z}/(p^k))[x]_{<\rho}$ by letting $q_i$ equal the coefficient of $x^{i-1}$.

• Applications in error-correction involve computing roots of a polynomial $G \in (\mathbb{Z}/(p^k))[x][y]$ over $(\mathbb{Z}/(p^k))[x]$. 
Passing to $\mathbb{Q}_p$

We can efficiently encode the roots of $f$ over $\mathbb{Z}/(p^k)$ for successively larger $k$ by finding the roots of $f$ over $\mathbb{Q}_p$.

- Observe we can uniquely write any rational $\frac{a}{b}$ as $\frac{a}{b} = p^k \frac{n}{d}$, where $k \in \mathbb{Z}$ and $\gcd(n, d) = 1$. The $p$-adic valuation $\text{ord}_p(\cdot)$ is defined on $\mathbb{Q}$ to be $\text{ord}_p(a/b) = k$.

**Figure 1:** 3-adic integers (Quanta Magazine, 2020)
We can efficiently encode the roots of $f$ over $\mathbb{Z}/(p^k)$ for successively larger $k$ by finding the roots of $f$ over $\mathbb{Q}_p$.

Observe we can uniquely write any rational $\frac{a}{b}$ as $\frac{a}{b} = p^k \frac{n}{d}$, where $k \in \mathbb{Z}$ and $\gcd(n, d) = 1$. The $p$-adic valuation $\text{ord}_p(\cdot)$ is defined on $\mathbb{Q}$ to be $\text{ord}_p(a/b) = k$.

Define the $p$-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by $|\frac{a}{b}|_p = p^{-\text{ord}_p(a/b)}$.

**Figure 1:** 3-adic integers (Quanta Magazine, 2020)
We can efficiently encode the roots of $f$ over $\mathbb{Z}/(p^k)$ for successively larger $k$ by finding the roots of $f$ over $\mathbb{Q}_p$.

- Observe we can uniquely write any rational $\frac{a}{b}$ as $\frac{a}{b} = p^k \frac{n}{d}$, where $k \in \mathbb{Z}$ and $\gcd(n, d) = 1$. The $p$-adic valuation $\text{ord}_p(\cdot)$ is defined on $\mathbb{Q}$ to be $\text{ord}_p(a/b) = k$.
- Define the $p$-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by $|\frac{a}{b}|_p = p^{-\text{ord}_p(a/b)}$.
- The completion of $\mathbb{Q}$ with respect to $|\cdot|$ is denoted by $\mathbb{Q}_p$, the $p$-adic numbers.

**Figure 1:** 3-adic integers (Quanta Magazine, 2020)
We can efficiently encode the roots of \( f \) over \( \mathbb{Z}/(p^k) \) for successively larger \( k \) by finding the roots of \( f \) over \( \mathbb{Q}_p \).

* Observe we can uniquely write any rational \( \frac{a}{b} \) as \( \frac{a}{b} = p^k \frac{n}{d} \), where \( k \in \mathbb{Z} \) and \( \gcd(n,d) = 1 \). The \( p \)-adic valuation \( \text{ord}_p(\cdot) \) is defined on \( \mathbb{Q} \) to be \( \text{ord}_p(a/b) = k \).

* Define the \( p \)-adic absolute value \( |\cdot|_p \) on \( \mathbb{Q} \) by \( |\frac{a}{b}|_p = p^{-\text{ord}_p(a/b)} \).

* The completion of \( \mathbb{Q} \) with respect to \( |\cdot| \) is denoted by \( \mathbb{Q}_p \), the \( p \)-adic numbers.

* \( p \)-adic numbers can also be expressed by formal series \( \sum_{j=s}^{\infty} a_j p^j \), where \( a_j \in \{0, \ldots, p-1\} \).
Consider the sequence obtained by extracting the digits of the non-1 root of $x^2 - 1$ over $\mathbb{Z}_3$: $2, 2 + 2 \cdot 3, 2 + 2 \cdot 3 + 2 \cdot 3^2, \ldots$

Both sequences converge at a geometric rate! Applying Newton’s method to either allows both to converge even faster!

Consider the sequence obtained by applying the bisection method to $\sqrt{2}$ in the interval $[1, 2]$: $1, 1.25, 1.375, 1.4375, \ldots$
# How to solve over $\mathbb{Q}_p$: Trees

## Definition

Let $f \in \mathbb{Z}[x]$ and let $\tilde{f}$ be its reduction mod $p$.

## An example over $\mathbb{Q}_{17}$:

$$f(x) = 1 - x^{340}$$
**Definition**

Let $f \in \mathbb{Z}[x]$ and let $\tilde{f}$ be its reduction mod $p$. For a degenerate root $\zeta \in \mathbb{F}_p$ of $\tilde{f}$, define

$$s(f, \zeta) := \min_{i \geq 0} \{ i + \text{ord}_p f^{(i)}(\zeta) \}.$$ 

An example over $\mathbb{Q}_{17}$:

$$f(x) = 1 - x^{340}$$

$$s(f, 1) = 2 \quad s(f, 4) = 2 \quad s(f, 13) = 2 \quad s(f, 16) = 2$$
How to solve over $\mathbb{Q}_p$: Trees

**Definition**

Let $f \in \mathbb{Z}[x]$ and let $\tilde{f}$ be its reduction mod $p$. For a degenerate root $\zeta \in \mathbb{F}_p$ of $\tilde{f}$, define

$$s(f, \zeta) := \min_{i \geq 0} \{ i + \ord_p \frac{f^{(i)}(\zeta)}{i!} \}.$$  

For $k \in \mathbb{N}$, $i \geq 1$, define inductively a set $T_{p,k}(f)$ of pairs $(f_{i-1}, k_{i-1}) \in \mathbb{Z}[x] \times \mathbb{N}$ as follows:

An example over $\mathbb{Q}_{17}$:

$$(f(x) = 1 - x^{340}, k \geq 3)$$

$s(f, 1) = 2$  
$s(f, 4) = 2$  
$s(f, 13) = 2$  
$s(f, 16) = 2$
How to solve over $\mathbb{Q}_p$: Trees

**Definition**

Let $f \in \mathbb{Z}[x]$ and let $\tilde{f}$ be its reduction mod $p$. For a degenerate root $\zeta \in \mathbb{F}_p$ of $\tilde{f}$, define $s(f, \zeta) := \min_{i \geq 0} \{ i + \text{ord}_p \frac{f(i)(\zeta)}{i!} \}$. For $k \in \mathbb{N}$, $i \geq 1$, define inductively a set $T_{p,k}(f)$ of pairs $(f_{i-1}, k_{i-1}) \in \mathbb{Z}[x] \times \mathbb{N}$ as follows: Set $(f_0, k_0) := (f, k)$, then for $i \geq 1$ with $(f_{i-1}, k_{i-1}) \in T_{p,k}(f)$, and any degenerate root $\zeta_{i-1} \in \mathbb{F}_p$ with $s_{i-1} := s(f_{i-1}, \zeta_{i-1})$, let $k_{i} := k_{i-1} - s_{i-1}$, $f_i(x) := p^{-s(f_{i-1}, \mu, \zeta_{i-1})} f_{i-1}(\zeta_{i-1} + px) \mod p^{k_{i}}$, and include $(f_i, k_i)$ in $T_{p,k}(f)$.

An example over $\mathbb{Q}_{17}$:

$$ (f(x) = 1 - x^{340}, k \geq 3) $$

$$ (14x, k - 2) \quad (12x + 10, k - 2) \quad (5x + 15, k - 2) \quad (3x + 3, k - 2) $$

$$ 1 + 0 \cdot 17 + \ldots 4 + 2 \cdot 17 + 13 + 14 \cdot 17 + 16 + 16 \cdot 17 + \ldots $$
How to solve over $\mathbb{Q}_p$: Trees

**Definition**

Define $T_{p,k}(f)$ inductively as follows: (i) Set $f_0 = f$, $k_0 = k$, and let $(f_0, k_0)$ be the label of the root node of $T_{p,k}(f)$.

An example over $\mathbb{Q}_3$: 

$(f_0(x) = x^9 - 1, k_0 \geq 3)$
How to solve over $\mathbb{Q}_p$: Trees

**Definition**

Define $T_{p,k}(f)$ inductively as follows: (i) Set $f_0 = f$, $k_0 = k$, and let $(f_0, k_0)$ be the label of the root node of $T_{p,k}(f)$. (ii) The non-root nodes of $T_{p,k}(f)$ are labeled by the $(f_i, k_i) \in T_{p,k}(f)$ for $i \geq 1$.

An example over $\mathbb{Q}_3$:

$(f_0(x) = 1 - x^9, k_0 \geq 3)$

$\tilde{f}_1 = x$
How to solve over $\mathbb{Q}_p$: Trees

**Definition**

Define $\mathcal{T}_{p,k}(f)$ inductively as follows: (i) Set $f_0 = f$, $k_0 = k$, and let $(f_0, k_0)$ be the label of the root node of $\mathcal{T}_{p,k}(f)$. (ii) The non-root nodes of $\mathcal{T}_{p,k}(f)$ are labeled by the $(f_i, k_i) \in T_{p,k}(f)$ for $i \geq 1$. (iii) There is an edge from node $(f_{i-1}, k_{i-1})$ to node $(f_i, k_i)$ iff there is a degenerate root $\zeta_{i-1} \in \mathbb{F}_p$ of $\tilde{f}_{i-1}$ with $s(f_{i-1}, \zeta_{i-1}) \in \{2, \ldots, k_{i-1} - 1\}$.

An example over $\mathbb{Q}_3$:

\[ (f_0(x) = 1 - x^9, k_0 \geq 3) \]

\[ (f_1, k - 2), \tilde{f}_1 = x \]
Theorem (Rojas and Zhu, 2021)

Following the notation of $\mathcal{T}_{p,k}(f)$ above, let $f = f_{0,0} = c_0 + c_1 x^d \in \mathbb{Z}[x]$ with $c_0 c_1 \neq 0 \mod p$. Then for all $k$, the tree $\mathcal{T}_{p,k}(f)$ has depth at most 1.
**Theorem (Rojas and Zhu, 2021)**

*Following the notation of $\mathcal{T}_{p,k}(f)$ above, let $f = f_{0,0} = c_0 + c_1x^d \in \mathbb{Z}[x]$ with $c_0 c_1 \neq 0 \mod p$. Then for all $k$, the tree $\mathcal{T}_{p,k}(f)$ has depth at most 1.*

- The tree gives approximate roots of $f$ in just two digits!
Theorem (Rojas and Zhu, 2021)

Following the notation of $T_{p,k}(f)$ above, let $f = f_{0,0} = c_0 + c_1 x^d \in \mathbb{Z}[x]$ with $c_0 c_1 \neq 0 \mod p$. Then for all $k$, the tree $T_{p,k}(f)$ has depth at most 1.

- The tree gives approximate roots of $f$ in just two digits!
- This gives complexity of root-approximating algorithms linear in $\gcd(d, p - 1)$ and polynomial in $\log(dpH)$, where $H = \max\{c_0, c_1\}$.
Trees and Binomials

**Theorem (Rojas and Zhu, 2021)**

Following the notation of $T_{p,k}(f)$ above, let $f = f_{0,0} = c_0 + c_1 x^d \in \mathbb{Z}[x]$ with $c_0 c_1 \neq 0 \mod p$. Then for all $k$, the tree $T_{p,k}(f)$ has depth at most 1.

- The tree gives approximate roots of $f$ in just two digits!
- This gives complexity of root-approximating algorithms linear in $\gcd(d, p - 1)$ and polynomial in $\log(dpH)$, where $H = \max\{c_0, c_1\}$
- Also, the roots are never less than $1/p$ apart.
Theorem (Rojas and Zhu, 2021)

Let \( f = c_1 + c_2 x^{a_2} + c_3 x^{a_3} \) be a trinomial with \( 0 < a_2 < a_3 \), \( p \nmid c_1 \). Define \( S_0 = \max\{s(f, \zeta_0) \mid \zeta_0 \text{ is a degenerate root of } f \text{ over } \{0, 1, \ldots, p - 1\}\} \) and \( D = \max\{\text{ord}_p(\zeta - \xi) \mid \zeta, \xi \text{ are non-degenerate roots of } f \text{ over } \mathbb{Q}_p\} \), setting either quantity to 0 if not applicable. Then \( k \geq 1 + S_0 \min\{1, D\} + M_p \max\{D - 1, 0\} \) (where \( M_p = 4, 3, \) or \( 2, \) according to \( p = 2, p = 3, p \geq 5 \)) guarantees \( T_{p,k} \) has depth at least \( D \).
Theorem (Rojas and Zhu, 2021)

Let \( f = c_1 + c_2 x^{a_2} + c_3 x^{a_3} \) be a trinomial with \( 0 < a_2 < a_3, \ p \nmid c_1 \). Define
\[ S_0 = \max\{s(f, \zeta_0) \mid \zeta_0 \text{ is a degenerate root of } f \text{ over } \{0, 1, \ldots p - 1\} \} \]
and
\[ D = \max\{\text{ord}_p(\zeta - \xi) \mid \zeta, \xi \text{ are non-degenerate roots of } f \text{ over } \mathbb{Q}_p\}, \]
setting either quantity to 0 if not applicable. Then \( k \geq 1 + S_0 \min\{1, D\} + M_p \max\{D - 1, 0\} \) (where \( M_p = 4, 3, \text{ or } 2, \text{ according to } p = 2, p = 3, p \geq 5 \)) guarantees \( T_{p,k} \) has depth at least \( D \).

\[ * \] Explicit, but worse (not \( O(1) \)) on \( k \) than in the binomial case.

\[ * \] The analogous root spacing bound induced is given by
\[ |\log |z_1 - z_2|_p| = O(p \log^2(dH) \log_p(d)). \]

\[ * \] Two simple families of examples prove that the minimal root spacing is at least linear in \( \log(dH) \) and that the depth of \( k \) has dependence on \( D \) and \( S_0 \).
Two families of examples

Example
The family $g_p(x) = x^2 - (2 + p^j)x + (1 + p^j)$ has roots $z_1 = 1$, $z_2 = 1 + p^j$, so that $\log |z_1 - z_2|_p = -\log(H - 2)$. 

[Continued on next page]
Two families of examples

Example

The family $g_p(x) = x^2 - (2 + p^i)x + (1 + p^i)$ has roots $z_1 = 1$, $z_2 = 1 + p^i$, so that $\log |z_1 - z_2|_p = - \log (H - 2)$.

It is clear from factoring that $g_p(x) = f_0(x)$ has its roots as claimed. We now make use of the tree $\mathcal{T}_{p,k}(g_p(x))$. 
Two families of examples

Example

The family $g_p(x) = x^2 - (2 + p^j)x + (1 + p^j)$ has roots $z_1 = 1$, $z_2 = 1 + p^j$, so that $\log |z_1 - z_2|_p = -\log(H - 2)$.

- It is clear from factoring that $g_p(x) = f_0(x)$ has its roots as claimed. We now make use of the tree $T_{p,k}(g_p(x))$.
- $g_p(x) = x^2 - 2x + 1$ has degenerate root 1 over $\mathbb{Z}_p$, with $s_0(g_p(x), 1) = 2$. We then have $k_1 = k_0 - 2$ and $f_1 = p^{-2}((1 + px)^2 - (2 + p^j)(1 + px) + 1 + p^j) = x^2 - p^{j-1}x$ mod $p^{k_1}$.
Two families of examples

Example

The family $g_p(x) = x^2 - (2 + p^j)x + (1 + p^j)$ has roots $z_1 = 1$, $z_2 = 1 + p^j$, so that

$$\log |z_1 - z_2|_p = -\log(H - 2).$$

\* It is clear from factoring that $g_p(x) = f_0(x)$ has its roots as claimed. We now make use of the tree $T_{p,k}(g_p(x))$.

\* $g_p(x) = x^2 - 2x + 1$ has degenerate root 1 over $\mathbb{Z}_p$, with $s_0(g_p(x), 1) = 2$. We then have $k_1 = k_0 - 2$ and $f_1 = p^{-2}((1 + px)^2 - (2 + p^j)(1 + px) + 1 + p^j) = x^2 - p^{j-1}x$ mod $p^{k_1}$.

\* Proceeding, we obtain a chain $f_i = x^2 - p^{j-i}x$ for $i \leq j$. At $i = j$, the mod-$p$ reduction of $f_i$ splits into non-degenerate roots 0 and 1.
Two families of examples

**Example**

The family $g_p(x) = x^2 - (2 + p^j)x + (1 + p^j)$ has roots $z_1 = 1$, $z_2 = 1 + p^j$, so that $\log |z_1 - z_2|_p = -\log(H - 2)$.

- It is clear from factoring that $g_p(x) = f_0(x)$ has its roots as claimed. We now make use of the tree $T_{p,k}(g_p(x))$.

- $g_p^\ast(x) = x^2 - 2x + 1$ has degenerate root 1 over $\mathbb{Z}_p$, with $s_0(g_p(x), 1) = 2$. We then have $k_1 = k_0 - 2$ and $f_1 = p^{-2}((1 + px)^2 - (2 + p^j)(1 + px) + 1 + p^j) = x^2 - p^{j-1}x \mod p^{k_1}$.

- Proceeding, we obtain a chain $f_i = x^2 - p^{j-i}x$ for $i \leq j$. At $i = j$, the mod-$p$ reduction of $f_i$ splits into non-degenerate roots 0 and 1.

- We see $k \geq 2j + 1 = 1 + S_0 + 2(D - 1)$ is required to detect both non-degenerate roots in the tree.
Two families of examples

Example

The family \( g_p(x) = x^2 - (2 + p^i)x + (1 + p^i) \) has roots \( z_1 = 1, z_2 = 1 + p^i \), so that \( \log|z_1 - z_2|_p = -\log(H - 2) \).

\* It is clear from factoring that \( g_p(x) = f_0(x) \) has its roots as claimed. We now make use of the tree \( T_{p,k}(g_p(x)) \).

\* \( g_p(x) = x^2 - 2x + 1 \) has degenerate root 1 over \( \mathbb{Z}_p \), with \( s_0(g_p(x), 1) = 2 \). We then have \( k_1 = k_0 - 2 \) and \( f_1 = p^{-2}((1 + px)^2 - (2 + p^i)(1 + px) + 1 + p^i) = x^2 - p^{i-1}x \mod p^{k_1} \).

\* Proceeding, we obtain a chain \( f_i = x^2 - p^{j-i}x \) for \( i \leq j \). At \( i = j \), the mod-\( p \) reduction of \( f_i \) splits into non-degenerate roots 0 and 1.

\* We see \( k \geq 2j + 1 = 1 + S_0 + 2(D - 1) \) is required to detect both non-degenerate roots in the tree.

Example

Similarly, we can prove family \( h_p(x) = x^{p^i+2} - 2x + 1 \) has roots \( z_1 = 1, z_2 = 1 + (p - 1)p^i + \ldots \) (so that \( \log|z_1 - z_2|_p = -\log(d - 2) \)) and extremal \( k \).
Acknowledgements

- Professor Rojas
- TAs and Professors
- TAMU and NSF

Thank you for listening!