Enumerating Ramification Polygons of Degree p^2

Juan E. Quiroa [1] Alex Jenny [2]

[1]University of North Carolina at Greensboro [2]Midwestern State University

Introduction

Let p be a prime. Every positive integer can be written as a finite base-p expansion. For example the base 5 expansion of 1776 is

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

A ***p* -adic number** is an infinite base p expansion that may include finitely many negative powers of p. The collection of all p-adic numbers is denoted $\mathbb{Q}_p$. The ***p* -adic valuation** $v_p(n)$ is the lowest exponent of p in the base p expansion of n. For example $v_5(1776) = 0$. On the other hand, $v_5(400) = 2$ because $400 = 1 \cdot 5^2 + 3 \cdot 5^3$.

A **monic polynomial of degree *n*** has the form

$$\varphi(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1 x + c_0$$

A **root** of $\varphi(x)$ is a number r such that $\varphi(r) = 0$. For example, the quadratic formula gives the roots of the polynomial $x^2 + bx + c$ in terms of b and c:

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

The **discriminant** of a polynomial is the product of all the differences of its roots. For instance the discriminant of the quadratic $x^2 + bx + c$ is $b^2 - 4c$.

For a polynomial φ of degree n with coefficents in $\mathbb{Q}_p$, its ***j* -invariant** is defined by

$$v_p(\mathrm{disc}(\varphi)) = n + j - 1$$

There are only finitely many distinct polynomials with p-adic coefficients of a given degree. This project studied an invariant of degree p^2 polynomials over $\mathbb{Q}_p$ for an odd prime p.

Ramification Polygons

The **Newton polygon** of

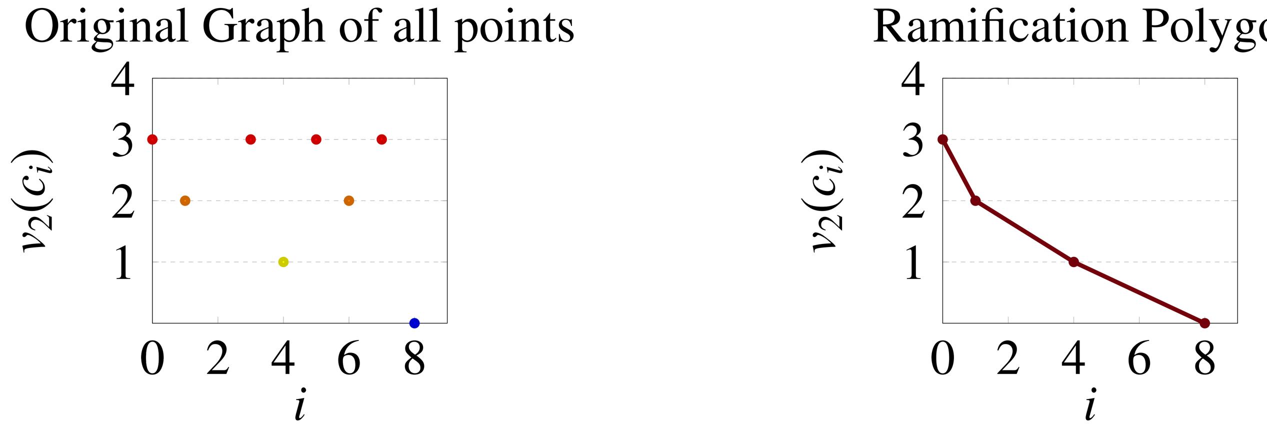
$$\varphi(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1 x + c_0$$

is the lower convex hull of the set of points $(i, v(c_i))$.

Let r be a root of φ. The **ramification polygon** of φ is the Newton polygon of the ramification polynomial $\rho(x) = r^{-n}\varphi(rx + r)$

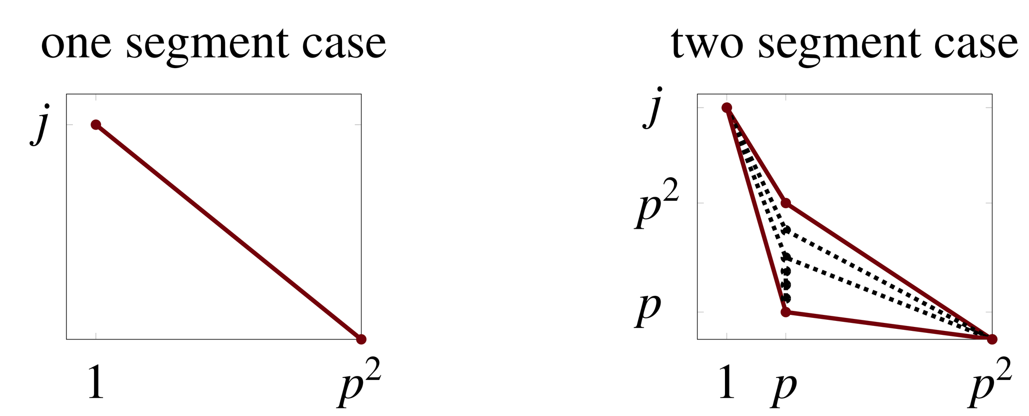
For example, consider the polynomial $\varphi(x) = x^8 - 2$ over the field $\mathbb{Q}_2$. The associated ramification polynomial is

$$\rho(x) = x^8 + 8x^7 + 28x^6 + 56x^5 + 70x^4 + 56x^3 + 28x^2 + 8x + 1$$



Research and Methods

In the case of degree p^2 extensions of $\mathbb{Q}_p$, there are the two possible shapes that a ramification polygon can have.



We defined a function $n(j)$ that returns the number of distinct ramification polygons for a given j-value. In addition we found the total number of distinct ramification polygons over all possible j-values.

The Function $n(j)$

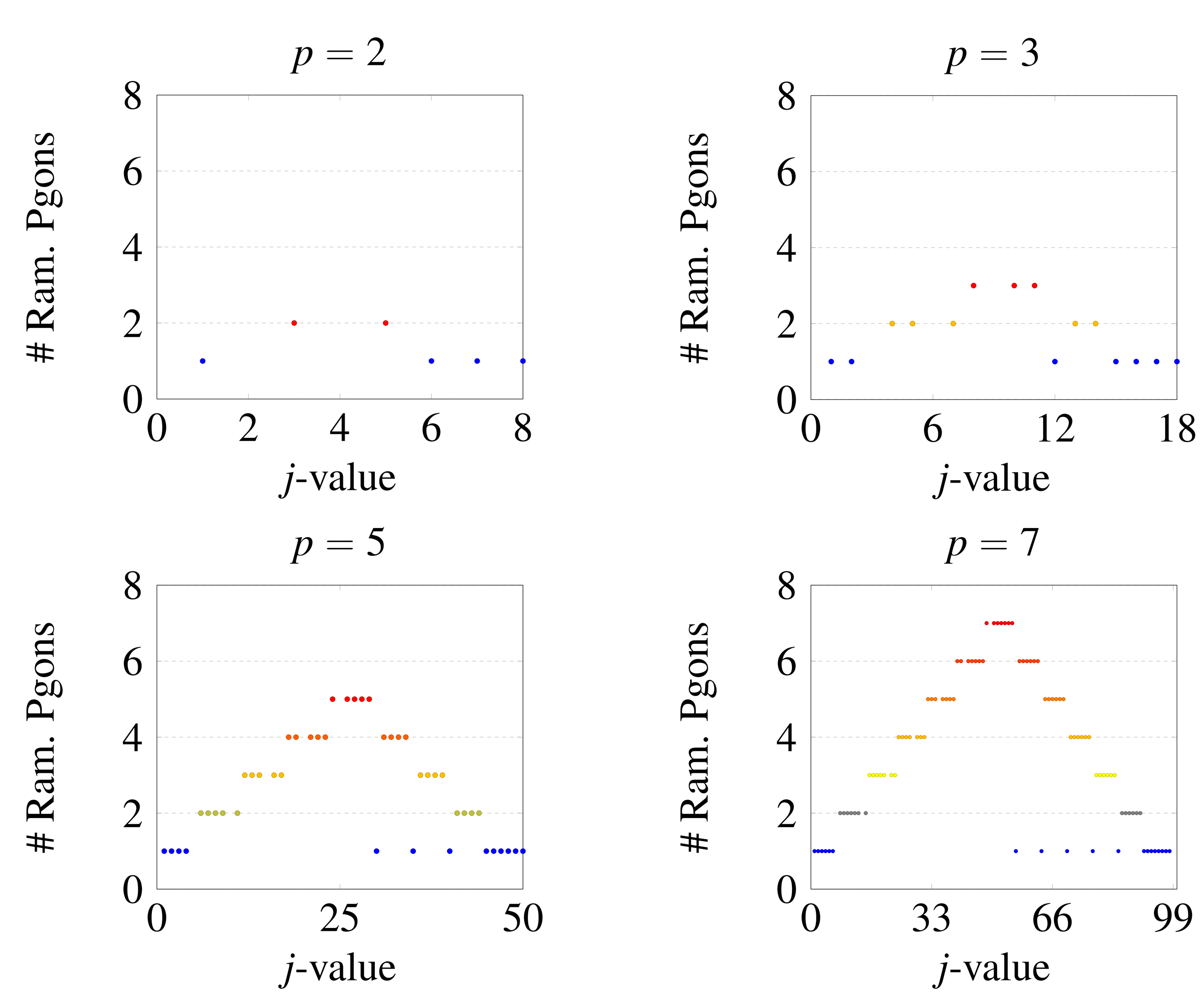
Let $j = a_2 p^2 + a_1 p + a_0$ be the base p expansion of j. Then $n(j)$ is defined by

$$n(j) = \begin{cases} a_1 + \delta & \text{if } j < p^2 \\ p & \text{if } p^2 < j < p(p+1) \\ 1 & \text{if } j \geq p(p+1) \text{ and } p \mid j \\ p - a_1 & \text{if } j > p(p+1) \text{ and } p \nmid j \end{cases}$$

where $\delta = 0$ if $a_0 < a_1$ and $\delta = 1$ otherwise.

Visualization of $n(j)$

In the graphs below, "# Ram. Pgons" refers to the number of distinct ramification polygons.



Classification And Implications

Let $\mathcal{R}_j$ denote the complete set of all distinct ramification polygons for a given j-value. As before let $j = a_2 p^2 + a_1 p + a_0$ be the base p expansion of j and set $\delta = 0$ if $a_0 < a_1$ and $\delta = 1$ otherwise. The table below provides a classification of all possible ramification polygons for possible j-values.

j	$\mathcal{R}_j$
$1 \leq j < p^2$	$\{\{(1,j),(p^2,0)\}\} \cup \{\{(1,j),(p,pc),(p^2,0)\} : 1 \leq c < a_1 + \delta\}$
$p^2 < j < p(p+1)$	$\{\{(1,j),(p^2,0)\}\} \cup \{\{(1,j),(p,pc),(p^2,0)\} : 1 \leq c < p\}$
$p(p+1) \leq j \leq 2p^2$ and $p \mid j$	$\{\{(1,j),(p,j-p^2),(p^2,0)\}\}$
$p(p+1) < j < 2p^2$ and $p \nmid j$	$\{\{(1,j),(p,pc),(p^2,0)\} : a_1 < c \leq p\}$

Observe that $n(j) = |\mathcal{R}_j|$. Consequently the following hold:

1. $|\mathcal{R}_j| \in \{1, 2, ..., p\}$.
2. The number of distinct ramification polygons for a given j-value is summarized below.
   - $|\mathcal{R}_j| = 1$ for $3p - 2$ different j-values.
   - $|\mathcal{R}_j| = p$ for p different j-values.
   - For each $k \in \{2, 3, \ldots, p-1\}$, $|\mathcal{R}_j| = k$ for $2p - 1$ different j-values.
3. The total number of distinct ramification polygons is

$$p^3 - \frac{p^2 - 3p}{2} - 1.$$

Impact And Future Research

While there are only finitely many polynomials of given degree with p-adic coefficients, a complete classification of these polynomials and their invariants has not been completed in generality. Polynomials of degree p and $2p$ were classified by Amano [1] and Awtrey-Hadgis [2], respectively. For all other degrees divisible by p, the only known cases are when the degree ≤ 15. So nothing is known for degree p^2 beyond $p = 3$.

We observed that the number of non-isomorphic generating polynomials for a given j-value, could be expressed as

$$(p-1) + (n(j) - 1)(p-1)^2.$$

References

[1] Shigeru Amano.
Eisenstein equations of degree p in a p-adic field.
J. Fac. Sci. Univ. Tokyo Sect. IA Math., 18:1–21, 1971.

[2] Chad Awtrey and Nick Hadgis.
Totally ramified p-adic fields of degree $2p$.
submitted.

This work was supported in part by NSA grant # H98230-18-1-0012.