Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Patterns and Periodicity in a Family of Resultants

par Kevin G. Hare, David McKinnon et Christopher D. Sinclair

Abstract. Given a monic degree N polynomial $f(x) \in \mathbb{Z}[x]$ and a non-negative integer ℓ, we may form a new monic degree N polynomial $f_\ell(x) \in \mathbb{Z}[x]$ by raising each root of f to the ℓth power. We generalize a lemma of Dobrowolski to show that if $m < n$ and p is prime then $p^{N(m+1)}$ divides the resultant of f_{p^m} and f_{p^n}. We then consider the function $(j,k) \mapsto \mathrm{Res}(f_j, f_k) \bmod p^m$. We show that for fixed p and m that this function is periodic in both j and k, and exhibits high levels of symmetry. Some discussion of its structure as a union of lattices is also given.

1. Introduction

Here and throughout $f(x) \in \mathbb{Z}[x]$ will be a monic polynomial of degree $N > 0$. We will assume that $f(x)$ is irreducible unless stated otherwise. Further, we will assume that $f(x)$ is not a cyclotomic polynomial, or, in the case where $f(x)$ is reducible, that none of the factors are cyclotomic polynomials. (The questions studied in this paper are uninteresting and trivial for cyclotomic polynomials.) If $\alpha_1, \alpha_2, \ldots, \alpha_N$ are the roots of f, and ℓ is an integer, then we may construct a new degree N polynomial, $f_\ell(x)$, specified by

$$f_\ell(x) := \prod_{i=1}^{N} (x - \alpha_i^\ell).$$

If $\ell \geq 0$ then f_ℓ has integer coefficients. To see this, we note that $f_\ell(x)$ can be written as the resultant of $f(y)$ and $x - y^\ell$:

$$f_\ell(x) = \mathrm{Res}(f(y), x - y^\ell).$$

By writing the latter resultant as the determinant of a Sylvester matrix we conclude that f_ℓ is monic with integer coefficients.

If the constant coefficient of f is ± 1, then $f_{-\ell}$ also has integer coefficients. This can be seen by noticing that

$$f_{-1}(x) = \pm x^N f(1/x).$$

Research of Kevin G. Hare and David McKinnon supported in part by NSERC of Canada
Research of Christopher D. Sinclair supported in part by the Pacific Institute for the Mathematical Sciences.

That is, f_{-1} can also be realized as the polynomial whose coefficient vector is formed by reversing the coefficient vector of f (and possibly alternating the sign). In this situation f_{-1} clearly has integer coefficients, and we conclude that $f_{-\ell}$ has integer coefficients by noticing that $f_{-\ell} = (f_{-1})_\ell$.

We use $\mathbb{N}$ to represent the set of non-negative integers, and define $R_f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ by

$$R_f(j,k) := \mathrm{Res}(f_j, f_k).$$

For each integer $M \geq 2$, we define the functions $R_{f,M} : \mathbb{N}\times\mathbb{N} \to \{0, 1, \ldots, M-1\}$ and $Q_{f,M} : \mathbb{N} \times \mathbb{N} \to \{0, 1\}$ by

$$R_{f,M}(j,k) \equiv R_f(j,k) \bmod M$$

and

$$Q_{f,M}(j,k) := \begin{cases} 0 & \text{if } R_f(j,k) \equiv 0 \bmod M; \\ 1 & \text{otherwise.} \end{cases}$$

We notice that if we know the properties of R_{f,M_1} and R_{f,M_2} where M_1 and M_2 are co-prime, then we know the properties of $R_{f,M_1 \cdot M_2}$ by the Chinese remainder theorem. Hence, it suffices to look at this problem for $M = p^m$, a prime power.

For example, let $f(x) = x^4 - x^3 + x^2 + 1$. Figure 1 shows patterns in the density graphs of $Q_{f,5}$, where we plot a black square if $Q_{f,5}(j,k) = 0$.

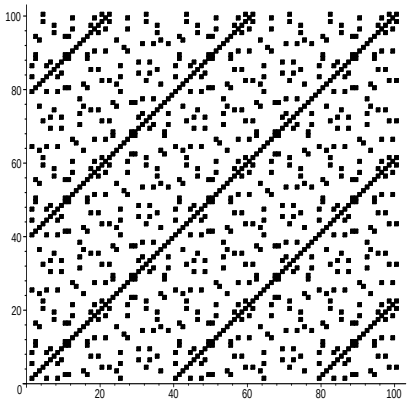


FIGURE 1. A density plot of $Q_{f,5}$ for $f(x) = x^4 - x^3 + x^2 + 1$.

Even more striking patterns emerge when we consider *reciprocal* polynomials. A monic polynomial f is called reciprocal if $f_{-1} = f$. In this case R_f, and hence Q_f, are even in both variables (i.e. $R_f(j,k) = R_f(\pm j, \pm k)$, and this symmetry induces new patterns in the range of Q_f. For instance, Figure 2 shows $Q_{f,5}$ where $f(x) = x^4 - x^3 - x^2 - x + 1$.

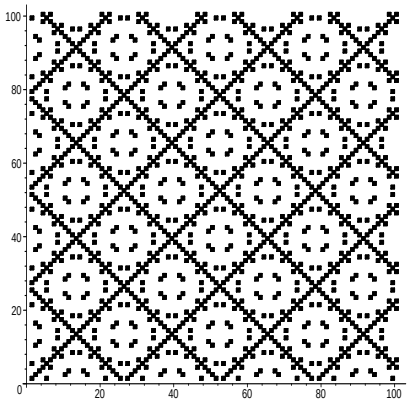


FIGURE 2. A density plot of $Q_{f,5}$ for $f(x) = x^4 - x^3 - x^2 - x + 1$.

If the constant coefficient of f is ± 1 then we extend the domains of R_f and $Q_{f,p}$ to $\mathbb{Z} \times \mathbb{Z}$. The purpose of this manuscript is to partially explain patterns of the sort which appear in the range of $Q_{f,p}$ and Q_{f,p^m} for primes and prime powers. Here and throughout p will always represent a prime number.

2. Statement of Results

In order to partially explain these patterns that arise *e.g.* in Figures 1 and 2, we will show that for any monic $f(x) \in \mathbb{Z}[x]$, of degree N, that $R_f(j,k)$ is 'often' divisible by p^N, a fact which implies that there are 'a lot' of black squares in the density graph of Q_{f,p^N}. We will then show that R_{f,p^m}, and hence Q_{f,p^m}, are periodic in both arguments. We will also give an algorithm for computing the period of R_{f,p^m} which takes f and p^m as inputs. Lastly, we will show a number of symmetry results that this function exhibits.

The first result we give is an extension of Dobrowolski's Lemma.

Theorem 2.1 (Extended Dobrowolski's Lemma)**.** *If $0 \leq m < n$, then $p^{N(m+1)}$ divides $R_f(p^n, p^m)$.*

E. Dobrowolski [1] proved the case when $m = 0$ and $n = 1$. The proof of this extended result is the subject of Section 3.

Given a positive integer M, we define the *period* of $R_{f,M}$ as the least positive integer $t = t(M)$ such that

$$R_{f,M}(j,k) = R_{f,M}(j+t,k) = R_{f,M}(j,k+t)$$

for all j and k in the domain of R_f. This will be denoted by $\mathrm{Per}_f(M)$.

The main results of Section 4 is showing that these periods exist (Theorem 4.2) and how to compute periods for $M = p^m$ a prime power (Theorem 4.3).

Sections 5 and 6 discuss some of the internal structure of the density graph modulo p^m. We show that these density graphs can be decomposed into a finite number of different lattices (Theorem 5.1). Moreover for $m \leq N$, all of these lattices have discriminant equal to the period $\mathrm{Per}_f(p^N)$ (Theorem 5.2).

Lastly, in Section 7 we look at the symmetry of the density graph of $Q_{f,M}(j,k)$ to get the following result:

Theorem 2.2. *Consider the density graph of $Q_{f,M}(j,k)$.*

- *There is a symmetry along the line $y = x$.*
- *There is a symmetry along the line $y = \mathrm{Per} - x$.*
- *If $f(x)$ is reciprocal, then there is a symmetry along the line $y = \mathrm{Per}/2$ and along $x = \mathrm{Per}/2$.*

The first of these results is immediate from noticing that $\mathrm{Res}(f,g) = \pm\,\mathrm{Res}(g,f)$. The second and third are given as corollaries of Theorems 7.2 and 7.3.

The last section, Section 8 makes some comments and suggests possible directions for future work.

3. Extended Dobrowolski's Lemma

In 1991, E. Dobrowolski proved the result (using a different language) that:

Lemma 3.1 (Dobrowolski [1])**.** *For any prime p and positive integer N, p^N divides $R_f(p,1)$.*

He used this result to find lower bounds on the Mahler measure of non-cyclotomic polynomial, based on the number of non-zero coefficients. We extend this result to show that $p^{m+1}N$ divides $R_f(p^m,p^n)$ for $0 \leq m < n$ (Theorem 2.1). An obvious corollary to this is that $Q_{f,p}(p^n,p^m) = 0$ for all positive integers n and m.

We will denote by K the splitting field of f over $\mathbb{Q}$, and by $\mathcal{O}_K$ its ring of integers. Furthermore $(p) \subseteq \mathcal{O}_K$ will denote the principal ideal generated by p. The following two congruences will prove useful in our analysis of resultants of the form $\mathrm{Res}(f_{p^n}, f_{p^m})$. If α and β are in $\mathcal{O}_K$ then $(\alpha+\beta)^p \equiv \alpha^p+\beta^p \bmod (p)$. This follows from the fact that when $0 < k < p$, p divides $\binom{p}{k}$. A similar analysis of multinomial coefficients together with Fermat's Little Theorem implies that

$$f(x^p) \equiv f(x)^p \bmod p \tag{1}$$

(By this we mean that there exists $h(x) \in \mathbb{Z}[x]$ so that $f(x^p) = f(x)^p + p \cdot h(x)$.) This second congruence is the key to the proof of Dobrowolski's Lemma. We provide the proof of Lemma 3.1 for illustration only.

Proof of Lemma 3.1. Let $g(x) := f(x^p) - f(x)^p$, and let $\alpha_1, \ldots, \alpha_N$ be the roots of $f(x)$ in $\mathbb{C}$. Since $g(x) \equiv 0 \bmod p$, we may find $h(x) \in \mathbb{Z}[x]$ such that $g(x) = p \cdot h(x)$. And thus,

$$\begin{aligned} R_f(p,1) &= \operatorname{Res}(f_p, f) \\ &= \prod_{i=1}^{N} f(\alpha_i^p) \\ &= \prod_{i=1}^{N} f(\alpha_i^p) - f(\alpha_i)^p \\ &= \prod_{i=1}^{N} g(\alpha_i) \\ &= p^N \prod_{i=1}^{N} h(\alpha_i) \\ &= p^N \operatorname{Res}(f, h). \end{aligned}$$

This proves the lemma since $\operatorname{Res}(f, h)$ is an integer. □

The proof of Theorem 2.1 relies on several lemmas including that of Dobrowolski. The following lemma is of some independent interest in our understanding of the patterns which arise in the range of $R_f(j,k)$.

Lemma 3.2. *Suppose j, k and ℓ are positive integers. Then $R_f(j,k)$ divides $R_f(j \cdot \ell, k \cdot \ell)$.*

Proof. First, notice that

$$\begin{aligned} R_f(j \cdot \ell, k \cdot \ell) &= \operatorname{Res}(f_{j \cdot \ell}, f_{k \cdot \ell}) \\ &= \prod_{i'=1}^{N} \prod_{i=1}^{N} (\alpha_{i'}^{j \cdot \ell} - \alpha_i^{k \cdot \ell}) \\ &= \operatorname{Res}\left(f(y), \prod_{i=1}^{N} (y^{j \cdot \ell} - \alpha_i^{k \cdot \ell}) \right) \qquad (2) \\ &= \prod_{i=1}^{N} \operatorname{Res}\left(f(y), y^{j \cdot \ell} - \alpha_i^{k \cdot \ell} \right), \qquad (3) \end{aligned}$$

where in the last equality we have used the fact that the resultant is multiplicative in each of its arguments. Notice that

$$y^{j\cdot\ell} - \alpha_i^{k\cdot\ell} = (y^j)^\ell - (\alpha_i^k)^\ell = (y^j - \alpha_i^k)\, H_\ell(y^j, \alpha_i^k), \tag{4}$$

where

$$H_\ell(x,y) := \frac{y^\ell - x^\ell}{y-x} = y^{\ell-1} + y^{\ell-2}x + \cdots + yx^{\ell-2} + x^{\ell-1} \tag{5}$$

Substituting (5) into (3) and exploiting the multiplicativity of the resultant, we find

$$\begin{aligned} R_f(j\cdot\ell, k\cdot\ell) &= \left(\prod_{i=1}^N \operatorname{Res}\left(f(y), y^j - \alpha_i^k\right)\right) \cdot \left(\prod_{i=1}^N \operatorname{Res}(f(y), H_\ell\big(y^j, \alpha_i^k\big))\right) \\ &= R_f(j,k) \cdot \operatorname{Res}\left(f(y), \prod_{i=1}^N H_\ell(y^j, \alpha_i^k)\right). \end{aligned} \tag{6}$$

It suffices to prove that the second resultant in (6) is an integer. We do this by noticing that

$$\prod_{i=1}^N H_\ell(y^j, \alpha_i^k) = \operatorname{Res}\big(f(x), H_\ell(y^j, x^k)\big). \tag{7}$$

The latter is in $\mathbb{Z}[y]$ since $H_\ell(y^j, x^k) \in \mathbb{Z}[x,y]$. It follows that the second resultant in (6) is an integer. □

Lemma 3.3. *Let m be a positive integer, then*

$$f_{p^m}(x) \equiv f(x) \bmod p.$$

Proof. Let $A = \{\alpha_1, \cdots, \alpha_N\}$ be the multiset of roots of $f(x) \bmod p$. Then the Frobenius map

$$\sigma : \alpha_i \mapsto \alpha_i^{p^m}$$

is an automorphism of the splitting field of $f(x)$ over $\mathbb{Z}/p\mathbb{Z}$, and therefore permutes A. Thus, $f_{p^m}(x)$ and $f(x)$ have the same multiset of roots over $\mathbb{Z}/p\mathbb{Z}$, and so, since $f(x)$ and $f_{p^m}(x)$ are both monic, they must be congruent modulo p. □

Lemma 3.4. *Suppose $F(x,y)$ and $H(x,y)$ are polynomials in $\mathbb{Z}[x,y]$ such that $F \equiv H \bmod p^m$. Then, as polynomials in $\mathbb{Z}[x]$,*

$$\operatorname{Res}\big(f(y), F(x,y)\big) \equiv \operatorname{Res}\big(f(y), H(x,y)\big) \bmod p^m.$$

Proof. This follows directly by considering the resultant as the determinant of the Sylvester matrix modulo p^m. In fact, it is easy to see that we need not require p^m to be a prime power. □

We are finally ready to prove Theorem 2.1, the Extended Dobrowolski's Lemma.

Proof of Theorem 2.1. We will induct on m. By noticing that $f(x^{p^n}) \equiv f(x)^{p^n}$ we see that the proof of Lemma 3.1 can be modified to show that p^N divides $R_f(1, p^n)$ for all $n \geq 1$. This is our base case $m = 0$.

Assume the result is true for $m-1$. By combining equations (6) and (7) we get

$$R_f(p^n, p^m) = R_f\big(p^{n-1}, p^{m-1}\big) \operatorname{Res}\left(f(y), \operatorname{Res}\left(f(x), H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big)\right)\right).$$

By the inductive hypothesis p^{Nm} divides $R(p^{n-1}, p^{m-1})$. To complete the induction, we need to prove p^N divides

$$\operatorname{Res}\left(f(y), \operatorname{Res}\left(f(x), H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big)\right)\right).$$

Notice that by equation (1)

$$\begin{aligned} H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big)\big(y^{p^{n-1}} - x^{p^{m-1}}\big) &= \big(y^{p^n} - x^{p^m}\big) \\ &\equiv \big(y^{p^{n-1}} - x^{p^{m-1}}\big)^p \bmod p. \end{aligned}$$

This in turn implies that

$$H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big) \equiv \big(y^{p^{n-1}} - x^{p^{m-1}}\big)^{p-1} \bmod p,$$

and hence

$$\begin{aligned} \operatorname{Res}\left(f(x), H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big)\right) &\equiv \operatorname{Res}\left(f(x), \big(y^{p^{n-1}} - x^{p^{m-1}}\big)^{p-1}\right) \bmod p \\ &\equiv \prod_{i=1}^{N} \big(y^{p^{n-1}} - \alpha_i^{p^{m-1}}\big)^{p-1} \bmod p \\ &\equiv f_{p^{m-1}}\big(y^{p^{n-1}}\big)^{p-1} \bmod p \\ &\equiv f\big(y^{p^{n-1}}\big)^{p-1} \bmod p \\ &\equiv f(y)^{p^{n-1}(p-1)} \bmod p. \end{aligned}$$

If we set

$$p \cdot g(y) = \operatorname{Res}\left(f(x), H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big)\right) - f(y)^{p^{n-1}(p-1)},$$

then

$$\begin{aligned} \operatorname{Res}\left(f(y), \operatorname{Res}\left(f(x), H_p\big(x^{p^{m-1}}, y^{p^{n-1}}\big)\right)\right) &= \operatorname{Res}\left(f(y), p \cdot g(y) + f(y)^{p^{n-1}(p-1)}\right) \\ &= \prod_{i=1}^{N} \left(p \cdot g(\alpha_i) + f(\alpha_i)^{p^{n-1}(p-1)}\right) \\ &= p^N \prod_{i=1}^{N} g(\alpha_i), \end{aligned}$$

which gives the required divisibility by p^N. □

4. Periodicity

Recall, we define the *period* of $R_{f,M}$ as the least positive integer $t = t(M)$ such that

$$R_{f,M}(j,k) = R_{f,M}(j+t,k) = R_{f,M}(j,k+t)$$

for all j and k in the domain of R_f. This will be denoted by $\mathrm{Per}_f(M)$.

It is not immediately obvious that $\mathrm{Per}_f(M)$ need exist. The next result will show that for certain primes p, $\mathrm{Per}_f(p)$ does in fact exist, and moreover gives an upper bound for $\mathrm{Per}_f(p)$.

First we recall the definition and some results about the order of a polynomial.

Definition (Definition 3.2 of [3])**.** Let $f \in \mathbb{F}_p$ be a irreducible polynomial with $f(0) \neq 0$. Then the least positive integers e for which $f(x)$ divides $x^e - 1$ is called the *order* of f, and denoted $\mathrm{ord}(f)$.

Theorem 4.1 (Theorem 3.3 of [3])**.** *Let $f \in \mathbb{F}_p$ be an irreducible polynomial over $\mathbb{F}_p$ of degree N with $f(0) \neq 0$. Then* $\mathrm{ord}(f)$ *is equal to the order of any root of f in the multiplicative group $\mathbb{F}^*_{p^N}$.*

Corollary 4.1 (Corollary 3.4 of [3])**.** *If $f \in \mathbb{F}_p$ is an irreducible polynomial over $\mathbb{F}_p$ of degree N, then* $\mathrm{ord}(f)$ *divides $p^N - 1$.*

These results give us:

Theorem 4.2. *Suppose $f(x)$ is irreducible modulo p. Then* $\mathrm{Per}_f(p) = \mathrm{ord}(f)$. *Furthermore* $\mathrm{Per}_f(p) \mid p^{\deg(f)} - 1$.

Proof. Let f be a monic polynomial of degree N. Since f is irreducible modulo p, it follows that its splitting field over $\mathbb{Z}/p\mathbb{Z}$ is the field F with p^N elements. This is a Galois extension of $\mathbb{Z}/p\mathbb{Z}$ with a cyclic Galois group generated by the Frobenius map $x \mapsto x^p$. Thus, if γ is a root of $f(x) \bmod p$, then we know that the complete set of roots of $f(x)$ is

$$\left\{\gamma, \gamma^p, \gamma^{p^2}, \cdots, \gamma^{p^{N-1}}\right\}.$$

See for example [2, Section 14.1]. Let e be the order of γ, (hence the order of f by Theorem 4.1). This order is independent of the choice of γ as $f(x)$ is irreducible mod p and thus all its roots are conjugate mod p. Hence $\gamma^e \equiv 1 \bmod p$ for all roots γ.

$$\begin{aligned} R_f(j,k+e) &\equiv \prod\prod(\gamma_i^j - \gamma_{i'}^{k+e}) \bmod p \\ &\equiv \prod\prod(\gamma_i^j - \gamma_{i'}^e\gamma_{i'}^k) \bmod p \\ &\equiv \prod\prod(\gamma_i^j - \gamma_{i'}^k) \bmod p \\ &\equiv R_f(j,k) \bmod p. \end{aligned}$$

In the same way $R_f(j+e,k) \equiv R_f(j,k) \bmod p$. The last comment follows directly from Corollary 4.1. □

Before stating the next theorem regarding the period of f modulo prime powers, we pause to make a few remarks. Again suppose that f is irreducible modulo p and let $t = \mathrm{Per}_f(p)$. Let $\mathbb{Q}_p$ be the p-adic extension of $\mathbb{Q}$, and $\gamma \in \mathbb{Q}_p$ be a p-adic root of f. Then by Theorem 4.2 we know that

$$\gamma^t \equiv 1 \bmod p.$$

Further, as $f(x)$ is not a cyclotomic polynomial, then there exists a $\kappa = \kappa(\gamma)$ such that

$$\begin{aligned} \gamma^t &\equiv 1 \bmod p^{\kappa} \\ \gamma^t &\not\equiv 1 \bmod p^{\kappa+1}. \end{aligned}$$

Proposition 4.1. *If f is irreducible modulo p, and γ and γ' are any two roots of f over $\mathbb{Q}_p$, then $\kappa(\gamma) = \kappa(\gamma')$. That is, κ is a function of f and p.*

Proof. To see that κ is independent of γ, we note that if $f(x)$ is monic and irreducible modulo p, then $f(x)$ is irreducible over $\mathbb{Q}_p$. Let F be a splitting field for $f(x)$ over $\mathbb{Q}_p$. Then $F/\mathbb{Q}_p$ is Galois, and the Galois group acts transitively on the roots of $f(x)$ in $\mathbb{Q}_p$. Moreover, for any prime power p^m, the set of roots of $f(x)$ in F will have the same reduction modulo p^m as the set of roots of $f(x)$ in $\mathbb{C}$. (This is because $f(x) \bmod p^m$ doesn't remember whether it was reduced from $\mathbb{Q}$ or from $\mathbb{Q}_p$.) Thus, if we can show that for every element $\sigma \in \mathrm{Gal}(F/\mathbb{Q}_p)$ and every root γ of $f(x)$ in F, we have $\kappa(\gamma) = \kappa\big(\sigma(\gamma)\big)$, then we will have shown that κ is independent of γ since it only depends on the reduction of γ modulo powers of p. To see this, we appeal to a classical result in p-adic number theory. Since $\mathbb{Q}_p$ is complete with respect to the non-archimedean p-adic valuation, there is a unique extension of this valuation to $\mathbb{Q}_p(\gamma)$ for any root γ of $f(x)$. By [4, Theorem II.4.8], the valuation of an element γ of a degree N extension of $\mathbb{Q}_p$ is $\big(N_{F/\mathbb{Q}_p}(\gamma)\big)^{1/N}$. Since the norm of $\sigma(\gamma)$ equals the norm of γ, we conclude that κ is independent of γ. □

Lemma 4.1. *Let p be a prime, and f irreducible of degree N. Then* $\mathrm{Per}_f(p) = \mathrm{Per}_f(p^N)$. *Moreover,* $\mathrm{Per}_f(p^m) = \mathrm{Per}_f(p^{\lceil (m/N) \rceil \cdot N})$.

Proof. We know that the Galois action on the roots of an irreducible polynomial mod p is cyclic, generated by the Frobenius map σ. If p^m divides $\gamma_i^j - \gamma_{i'}^k$ then $\sigma^r\left(\gamma_i^j - \gamma_{i'}^k\right)$ is in the ideal (p^m) for $r = 0, 1, \cdots, N-1$, hence if p^m divides $R_f(j,k)$ then $p^{\lceil (m/N) \rceil \cdot N}$ divides $R_f(j,k)$ which proves the desired result. □

Theorem 4.3. *Let p be prime and $f(x)$ be an irreducible polynomial mod p. Let $t = \mathrm{Per}_f(p) = \mathrm{Per}_f(p^N)$. Let $\kappa = \kappa(f,p)$. Then, if $p = 2$ and $\kappa = 1$ we have*

$$\mathrm{Per}_f(2^{Ns}) = \begin{cases} t & \text{for } s = 1; \\ t \cdot 2^{s+1} & \text{for } s \geq 2. \end{cases}$$

otherwise

$$\mathrm{Per}_f(p^{Ns}) = \begin{cases} t & \text{for } s = 1, 2, \cdots, \kappa; \\ t \cdot p^{s-\kappa} & \text{for } s \geq \kappa + 1. \end{cases}$$

As was noted earlier, it suffices to know what happens to prime powers by the Chinese remainder theorem. For example, if M_1 and M_2 are co-prime, then we can see that $\mathrm{Per}_f(M_1 \cdot M_2) = \mathrm{lcm}(\mathrm{Per}_f(M_1), \mathrm{Per}_f(M_2))$.

Theorem 4.3 is a consequence of Lemma 4.1 and the following lemma.

Lemma 4.2. *If p is an odd prime and $\kappa \geq 1$, or if p is any prime and $\kappa \geq 2$, then*

$$\left(\gamma^t\right)^p \equiv 1 \bmod p^{\kappa+1} \quad \text{and} \quad \left(\gamma^t\right)^p \not\equiv 1 \bmod p^{\kappa+2}$$

Proof. There exists some n with $\gcd(n,p) = 1$ such that

$$\gamma^t \equiv 1 + np^\kappa \bmod p^{\kappa+2}.$$

This implies that

$$\begin{aligned} \left(\gamma^t\right)^p &\equiv (1 + np^\kappa)^p \bmod p^{\kappa+2} \\ &\equiv 1 + \binom{p}{1} np^\kappa + \sum_{i=2}^{p} \binom{p}{i} n^i p^{i\kappa} \bmod p^{\kappa+2} \\ &\equiv 1 + np^{\kappa+1} \bmod p^{\kappa+2} \end{aligned}$$

under the hypotheses of the lemma. □

We will use the notation $p^m \parallel M$ to mean that m is the highest power of p to divide M. From a computational point of view, to find κ we notice that $p^{\kappa N} \parallel (1 - \gamma_1^t) \cdots (1 - \gamma_N^t) = f_t(1)$, where the last quantity is easily computed.

So far we have used the assumption that f is irreducible modulo p. This might not be the case. It is probably easiest to demonstrate how one would compute the period for a reducible polynomial by example.

Example. Let us look at two examples

$$f := x^4 + 2x^3 + 2x + 1$$

$$g := f + 11(5x^3 + 3x^2 + 5x)$$

Both of these factor as

$$g \equiv f \equiv (x+4)(x+3)(x^2 + 6x + 1) \bmod 11$$

It is easily verified that $(x+4)$ and $(x+3)$ have order 10 and x^2+6x+1 has order 12. This tells us that $\mathrm{Per}_g(11) = \mathrm{Per}_f(11) = \mathrm{lcm}(10,12) = 60$.

Let us factor f as $f = f' \cdot f''$ where $f' \equiv (x+4)(x+3) \bmod 11$ and $f'' \equiv x^2+6x+1 \bmod 11$. So f' is the order 10 factor of f, and f'' is the order 12. Similarly, let us factor g as $g' \cdot g''$.

To determine the κ associated with f' we need to check the divisibility by powers of 11 of $f'_{10}(1)$. We know that $11 \nmid f''_{10}(1)$ hence we can instead check the divisibility by powers of 11 of $f_{10}(1)$. Similarly we can figure out the κ associated with f'', g' and g''.

We see that $11^2 \parallel f_{10}(1)$, $11^4 \parallel g_{10}(1)$, $11^2 \parallel f_{12}(1)$ and $11^4 \parallel g_{12}(1)$. This tells us that

- $\mathrm{Per}_{f'}(11^{2k}) = 10 \cdot 11^{k-1}$
- $\mathrm{Per}_{f''}(11^{2k}) = 12 \cdot 11^{k-1}$
- $\mathrm{Per}_{g'}(11^{2k}) = \max(10, 10 \cdot 11^{k-2})$
- $\mathrm{Per}_{g''}(11^{2k}) = \max(12, 12 \cdot 11^{k-1})$

Hence this implies that

- $\mathrm{Per}_f(11^{2m}) = \mathrm{lcm}(\mathrm{Per}_{f'}(11^{2m}), \mathrm{Per}_{f''}(11^{2m})) = 60 \cdot 11^{m-1}$
- $\mathrm{Per}_g(11^{2m}) = \mathrm{lcm}(\mathrm{Per}_{g'}(11^{2m}), \mathrm{Per}_{g''}(11^{2m})) = \max(60, 60 \cdot 11^{m-2})$.

See Figure 3.

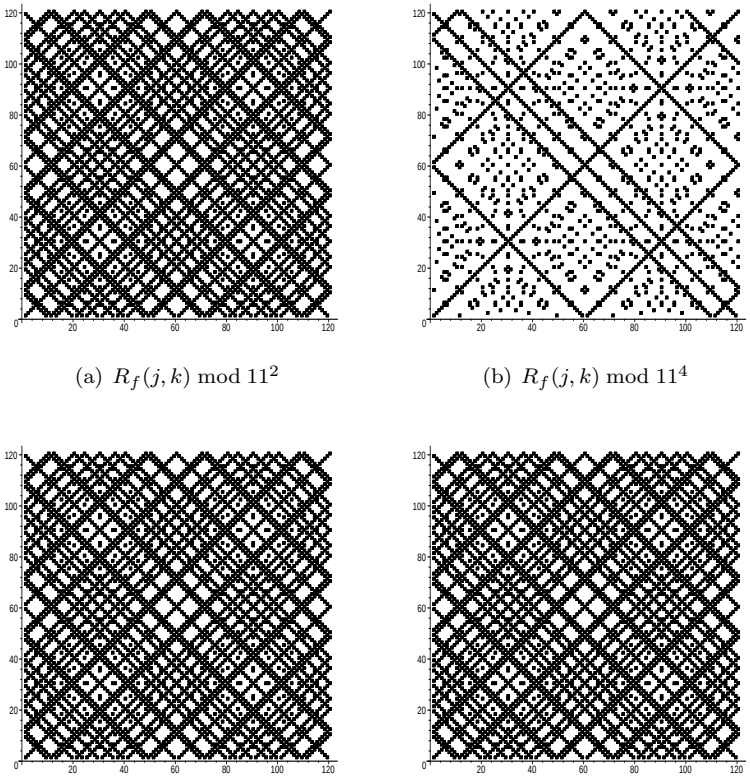
5. Lattices

Let us revisit Theorem 2.1, the Extended Dobrowolski's Lemma, now that we have the added notation of periodicity. First though, let us examine in more detail $R_{f,p}(j,k)$ for f irreducible modulo p.

Let f be a degree N monic irreducible polynomials modulo p. We know that the Galois group for f over $\mathbb{F}_p$ is cyclic, generated by the Frobenius map σ. We see that

$$\begin{aligned}
\mathrm{Res}(f_j, f_k) &= \prod_{i=1}^{N} \prod_{i'=1}^{N} \alpha_i^j - \alpha_{i'}^k \\
&= \prod_{i=1}^{N} \prod_{i'=0}^{N-1} \sigma^{i'}(\alpha_1^j - \alpha_i^k) \\
&= \prod_{i=1}^{N} \mathrm{norm}(\alpha_1^j - \alpha_i^k)
\end{aligned}$$

Here the norm is the norm over $\mathbb{F}_p$, and is typically different from the norm over $\mathbb{Q}$. We see that each factor $\mathrm{norm}(\alpha_1^j - \alpha_i^k)$ is in $\mathbb{F}_p$, so it suffices to find m such that $\mathrm{norm}(\alpha_1^j - \alpha_i^k) \equiv 0 \bmod p^m$ for each i, and then combine them together, to find the number of factors of p in $\mathrm{Res}(f_j, f_k)$. As was



(a) $R_f(j,k) \bmod 11^2$ (b) $R_f(j,k) \bmod 11^4$

(c) $R_g(j,k) \bmod 11^2$ (d) $R_g(j,k) \bmod 11^4$

FIGURE 3. Periodicity modulo 11^2 and 11^4

the case for Lemma 4.1, if $(\alpha_1^j - \alpha_i^k) \equiv 0 \bmod p^n$ then $\operatorname{norm}(\alpha_1^j - \alpha_i^k) \equiv 0 \bmod p^{nN}$.

Now each of these factors $\operatorname{norm}(\alpha_1^j - \alpha_i^k)$ has a different set of j and k that give rise to a factor of p. Let $\Lambda_i = \{(j,k) : \operatorname{norm}(\alpha_1^j - \alpha_{i+1}^k) \equiv 0 \bmod p\}$. Now, something that is worth observing is that

Theorem 5.1. *The set Λ_i is a lattice in $\mathbb{Z}$.*

Proof. We see that $(j,k) \in \Lambda_i$ implies that $\alpha_1^j \equiv \alpha_i^k \bmod p$. This relationship is clearly closed under addition and inversion of $(j,k) \in \Lambda_i$ □

As f is irreducible modulo p we know that we can write the roots as

$$\gamma^1, \gamma^p, \cdots, \gamma^{p^{N-1}}.$$

Reordering as necessary, we let $\alpha_i = \gamma^{p^{i-1}}$. Then

$$\Lambda_i = \{(j,k) : \gamma^j \equiv \gamma^{k \cdot p^i} \bmod p\} \tag{8}$$

Using this notation, we get $\Lambda_i = \Lambda_{i+N}$.

Example. Consider $f(x) = x^4 - x^3 - x^2 - x + 1 \bmod 5$. This polynomial is irreducible, and has period 26. In Figure 4 we give Λ_0, Λ_1, Λ_2 and Λ_3, on the grid $[0, 52]^2$. A quick check shows that the combination of the four lattices gives the complete description of $\mathrm{Res}(f_j, f_k) \bmod p$.

So in particular, we have

$$\{(j,k) : Q_{f,p}(j,k) = 1\} = \Lambda_1 \cup \cdots \cup \Lambda_N.$$

As a point of interest, to check if $(j,k) \in \Lambda_i$, we checked if $x^j - x^{k \cdot p^i} \equiv 0 \bmod f$, where the calculation is done modulo p.

By equation (8) we have a few elements that are clearly in Λ_i. Namely

$$(p^i, 1),\ (1, p^{N-i}),\ (0, \mathrm{Per}_f(p)),\ (\mathrm{Per}_f(p), 0) \in \Lambda_i.$$

The next result gives us an idea of how to find the discriminant of Λ_i.

Theorem 5.2. *The generators of Λ_i are given by*

$$\Lambda_i = \langle (0, \mathrm{Per}_f(p)), (1, p^{N-i}) \rangle$$

Thus $\mathrm{disc}(\Lambda_i) = \mathrm{Per}_f(p)$.

Proof. Assume that $(j,k) \in \Lambda_i$. Clearly this implies that $(j,k) - j(1, p^{N-i}) = (0, k - jp^{N-i}) \in \Lambda_i$. But then $\mathrm{Per}(f) \mid (k - jp^{N-i})$ which proves the result. □

It is worth observing that this simplifies immensely in the case when f is an irreducible quadratic.

Theorem 5.3. *Let f be an irreducible monic quadratic of norm $\mathcal{N}$. Then*

$$\mathrm{Res}(f_j, f_k) = \mathcal{N}^{k-j} f_{j-k}(1) f_{k+j}(\mathcal{N}^j)$$

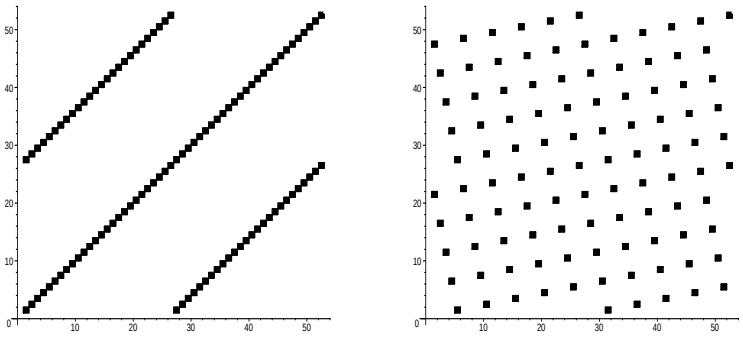
Corollary 5.1. *If f has norm 1 we have*

$$\mathrm{Res}(f_j, f_k) = f_{j-k}(1) f_{j+k}(1)$$

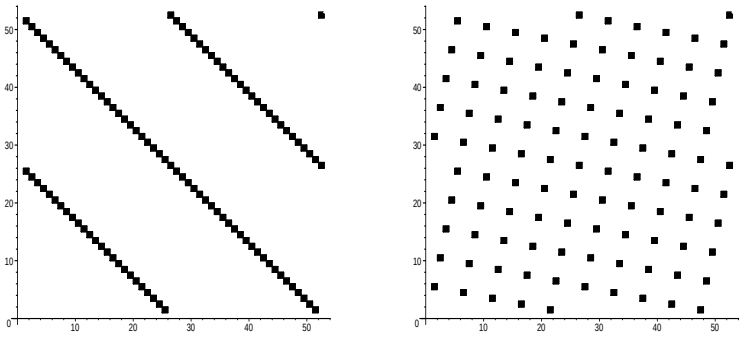
Proof. Let f have roots α and β. Without loss of generality let $j \geq k$, as $\mathrm{Res}(f_j, f_k) = \mathrm{Res}(f_k, f_j)$ when f has even degree.

$$\begin{aligned} \mathrm{Res}(f_j, f_k) &= (\alpha^j - \alpha^k)(\beta^j - \beta^k)(\beta^j - \alpha^k)(\alpha^j - \beta^k) \\ &= (\alpha\beta)^k (\alpha^{j-k} - 1)(\beta^{j-k} - 1)(\alpha\beta)^{-j}((\beta\alpha)^j - \alpha^{k+j})((\alpha\beta)^j - \beta^{k+j}) \\ &= \mathcal{N}^{k-j} f_{j-k}(1) f_{j+k}(\mathcal{N}^j) \end{aligned}$$

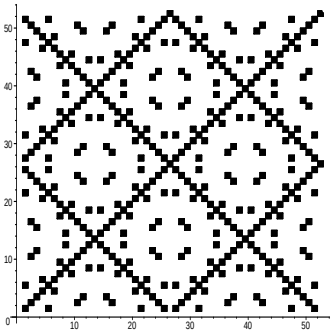
□



(a) Λ_0 (b) Λ_1

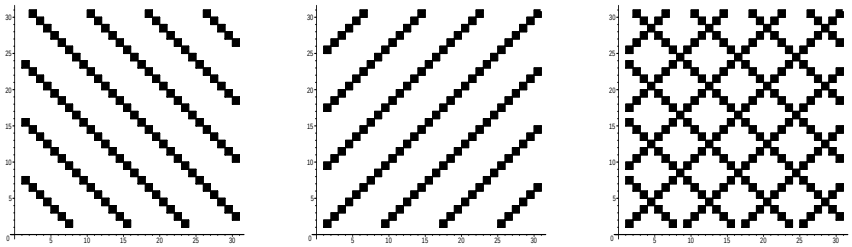


(c) Λ_2 (d) Λ_3



(e) Sum of the Lattices

FIGURE 4. Combining the lattices



(a) $8|m+n$ (b) $8|m-n$ (c) $\mathrm{Res}(f_j, f_k)$

FIGURE 5. $f = x^2 - 3x + 1$

Example. Consider $f = x^2 - 3x + 1$, which is irreducible modulo 7. This has $\mathrm{Per}_f(7) = 8$. Notice that $f_0(1) = 0$. This gives us that $f_{j+k}(1) \equiv 0$ when $8 \mid j+k$, and $f_{j-k}(1) \equiv 0$ when $8 \mid j-k$. The first of these conditions gives diagonal lines, with slope -1, and the second gives diagonal lines with slope 1. (See Figure 5.)

We could consider instead the polynomial $f = x^2 - 3x - 1$, which is irreducible modulo 7. This has $\mathrm{Per}_f(7) = 16$. By Theorem 5.3 we have $\mathrm{Res}(f_j, f_k) \equiv 0$ implies $f_{j-k}(1) \equiv 0$ or $f_{j+k}((-1)^k) \equiv 0$.

We first notice that $f_0(1) = 0$. This implies that $f_{m-n}(1) \equiv 0$ when $16 \mid m-n$.

By noticing that $f_0(-1) \equiv 4 \not\equiv 0$ along with the above comment, we have that $f_{m+n}((-1)^m) \equiv 0$ when $16 \mid m+n$ and m even.

Next we notice that $f_8(x) \equiv x^2+2x+1 \bmod 7$, and in particular $f_8(-1) \equiv 0$ and $f_8(1) \equiv 4 \not\equiv 0$. This gives us that $f_{m+n}((-1)^m) \equiv 0$ when $16 \mid m+n+8$ and m is odd.

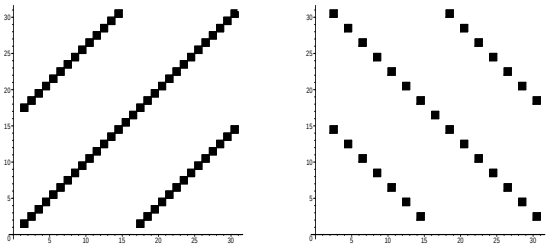
The first condition (that $16 \mid m-n$) gives the diagonal line with slope 1. The second condition (that $16 \mid m+n$ with m even) gives the dotted diagonal line with slope -1 thought $(8, 8)$. The third condition (that $16 \mid m+n+8$ with m odd) gives the dotted diagonal line with slope -1 thought $(3, 5)$. (See Figure 6.)

6. Sub-lattices modulo p^m

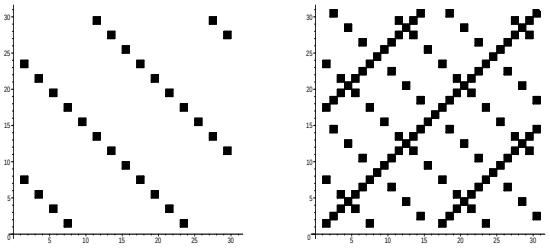
In the previous section, we looked at the lattices that combine to give the density plot of $Q_{f,p}(j, k)$. Here we look at the equivalent problem, when we examine the density plot modulo p^m.

We start with two definitions, which are the obvious extensions for the definition of Λ_i in the previous section.

Definition. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree N whose reduction mod p is irreducible, and let γ be a root of f in a finite extension of the



(a) $16|m-n$ (b) $16|m+n$ with m even



(c) $16|m+n+8$ with m odd (d) $\mathrm{Res}(f_j, f_k)$

FIGURE 6. $f = x^2 - 3x - 1$

p-adic field $\mathbb{Q}_p$. We define

$$\begin{aligned}\Lambda_{i,i'} &= \{(j,k) : (j,k) \in \Lambda_i \text{ and } (j,k) \in \Lambda_{i'}\} \\ &= \Lambda_i \cap \Lambda_{i'}\end{aligned}$$

and

$$\begin{aligned}\Lambda_{i,i} &= \{(j,k) : \gamma^j - \gamma^{kp^i} \equiv 0 \bmod p^2\} \\ &= \{(j,k) : \mathrm{norm}(\gamma^j - \gamma^{kp^i}) \equiv 0 \bmod p^{2N}\}\end{aligned}$$

We can extend these definitions in a straightforward way to $\Lambda_{i_1,i_2,\cdots,i_n}$.

6.1. Structure of $\Lambda_{i,i}$. If $\kappa = 1$, then $\Lambda_{i,i} = p\Lambda_i$; namely, $\Lambda_{i,i}$ is the sublattice of Λ_i of index p^2 obtained by multiplying every vector in Λ_i by p. If $\kappa \geq 2$ then $\Lambda_i = \Lambda_{i,i}$.

This follows directly from Lemma 4.2, and noticing that $\gamma^m - \gamma^{np^i} \equiv 0 \bmod p^2$ if and only if $\gamma^{m-np^i} \equiv 1 \bmod p^2$.

6.2. Structure of $\Lambda_{i,i'}$. This is the more interesting case. Assume without loss of generality that $i < i'$. Assume that $(j,k) \in \Lambda_{i,i'}$. This then

implies that we have

$$\begin{aligned}(j,k) &\in \Lambda_i \cap \Lambda_{i'} \\ &\in \langle (0,\mathrm{Per}),(1,p^{k-i})\rangle \cap \langle (0,\mathrm{Per}),(1,p^{k-i'})\rangle\end{aligned}$$

where $\mathrm{Per} = \mathrm{Per}_f(p)$. This in turn implies that

$$\begin{aligned}k &= k_1\mathrm{Per} + j\cdot p^{k-i} \\ &= k_2\mathrm{Per} + j\cdot p^{k-i'}\end{aligned}$$

This in turn implies that

$$(k_2-k_1)\mathrm{Per} = j(p^{k-i}-p^{k-i'})$$

hence

$$\mathrm{Per} \mid j(p^{k-i}-p^{k-i'})$$

We see that p is co-prime to Per as $\mathrm{Per} \mid p^N-1$, hence we can rewrite this to get

$$\mathrm{Per} \mid j(p^{i'-i}-1)$$

Using a similar argument, we also get that

$$\mathrm{Per} \mid k(p^{i'-i}-1)$$

Example. Consider the polynomial $x^3-x-1 \bmod 3$. We see that this has period 13. This in turn implies that if $(j,k) \in \Lambda_{i,i'}$ then $j \equiv k \equiv 0 \bmod \mathrm{Per}$ as $\gcd(\mathrm{Per}, 3^{i'-i}-1) = 1$ for $0 \le i < i' \le 2$. In fact, we see in this case that $\Lambda_{i,i'} = \langle (0,\mathrm{Per}),(\mathrm{Per},0)\rangle$ is a square lattice. (See Figure 7.)

7. Symmetry

A nice consequence of Sections 5 and 6 is that it helps explain some of the symmetry that is observed. Let $\mathrm{Per} = \mathrm{Per}_f(p)$.

Theorem 7.1. *If $(j,k) \in \Lambda_i$ then $(k,j) \in \Lambda_{N-i}$.*

Proof. Assume that $(k,j) \in \Lambda_i$. This implies that $\gamma^k = \gamma^{jp^i} \bmod p$. Here we can apply σ^{N-i} to both sides to get $(\gamma^{p^{N-i}})^k = (\gamma^{p^{N-i}})^{jp^i}$ which implies $\gamma^{kp^{N-i}} = \gamma^{jp^ip^{N-i}}$ which implies $\gamma^{kp^{N-i}} = \gamma^j$ which implies $(k,j) \in \Lambda_{N-i}$. □

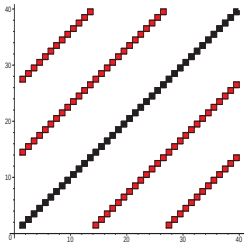
Theorem 7.2. *If $(j,k) \in \Lambda_i$ then $(\mathrm{Per}-j, \mathrm{Per}-k) \in \Lambda_i$.*

Proof. As Λ_i is a lattice, then $(j,k) \in \Lambda_i$ implies $(-j,-k) \in \Lambda_i$. By periodicity this implies $(\mathrm{Per}-j, \mathrm{Per}-k) \in \Lambda_i$. □

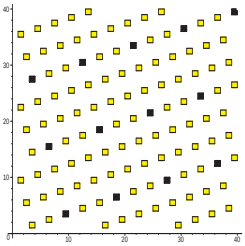
Corollary 7.1. *There is a symmetry along the line $y = \mathrm{Per} - x$.*

We get a further symmetry if $p(x)$ is reciprocal.

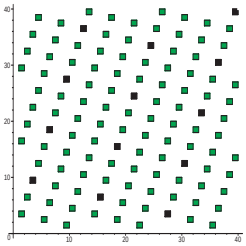
Theorem 7.3. *If $f(x)$ is a reciprocal polynomial, and $(j,k) \in \Lambda_i$, then there exists integers i_1, i_2 such that $(j, \mathrm{Per}-k) \in \Lambda_{i_1}$ and $(\mathrm{Per}-j, k) \in \Lambda_{i_2}$.*



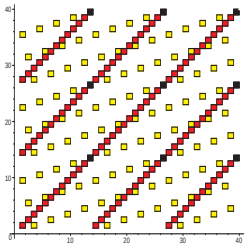
(a) Λ_0 - red, $\Lambda_{0,0}$ - black



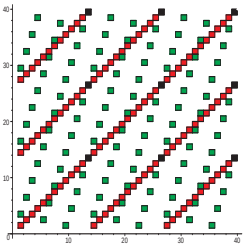
(b) Λ_1 - yellow, $\Lambda_{1,1}$ - black



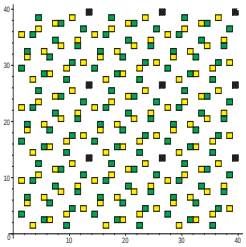
(c) Λ_2 - green, $\Lambda_{2,2}$ - black



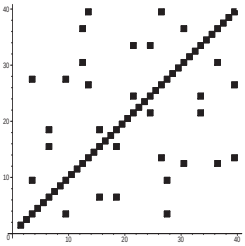
(d) Λ_0 - red, Λ_1 - yellow, $\Lambda_{0,1}$ - black



(e) Λ_0 - red, Λ_2 - green, $\Lambda_{0,2}$ - black



(f) Λ_1 - yellow, Λ_1 - green, $\Lambda_{1,2}$ - black



(g) Lattice sum modulo 3^6

FIGURE 7. $f = x^3 - x - 1$

Proof. If γ is a root then so is $1/\gamma$, which gives us the desired result. □

Corollary 7.2. *If $f(x)$ is reciprocal, then there is a symmetry along the line $y = \mathrm{Per}/2$ and along $x = \mathrm{Per}/2$.*

By observing that $\Lambda_{i_1,\cdots,i_n}$ is an intersection and/or sub-lattice of lattices of the form $\Lambda_{i'_1,\cdots,i'_{n-1}}$, we get that these symmetries results carry over to higher powers of p by induction.

8. Comments and Questions

The original motivation for this study was to see if this extended result of Dobrowolski could be used to improve the bounds on the Mahler measure of the polynomial. It was only after looking at the problem that we realized how rich the area was, and we never followed up on the original motivation. This would still be worthwhile doing.

Two other obvious generalizations of this problem would be looking at $\mathrm{Res}(f_j, g_k)$ where f and g are not the same polynomial, and to look at this problem where f, (or f and g) are multivariate polynomials instead of univariate polynomials.

9. Acknowledgments

The authors would like to thank the referee for many useful comments in general, and in particular for reference [3], and its applications for a cleaner proof of Theorem 4.2.

References

[1] E. Dobrowolski. *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta. Arith., 34:391–401, 1979.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra.* Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[3] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications.* Cambridge University Press, Cambridge, 1986.

[4] Jürgen Neukirch. *Algebraic number theory, volume 322 of* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

Kevin G. Hare
Department of Pure Mathematics,
University of Waterloo,
Waterloo, Ontario
E-mail : kghare@math.uwaterloo.ca

David McKinnon
Department of Pure Mathematics,
University of Waterloo,
Waterloo, Ontario
E-mail : dmckinno@math.uwaterloo.ca

Christopher D. Sinclair
Department of Mathematics,
University of Colorado at Boulder
E-mail : Christopher.Sinclair@Colorado.EDU