involve

a journal of mathematics

Recursive sequences and polynomial congruences

J. Larry Lehman and Christopher Triola

mathematical sciences publishers

2010 vol. 3, no. 2

INVOLVE 3:2(2010)

Recursive sequences and polynomial congruences

J. Larry Lehman and Christopher Triola

(Communicated by Kenneth S. Berenhaut)

We consider the periodicity of recursive sequences defined by linear homogeneous recurrence relations of arbitrary order, when they are reduced modulo a positive integer m. We show that the period of such a sequence with characteristic polynomial f can be expressed in terms of the order of $\omega = x + \langle f \rangle$ as a unit in the quotient ring $\mathbb{Z}_m[\omega] = \mathbb{Z}_m[x]/\langle f \rangle$. When $m = p$ is prime, this order can be described in terms of the factorization of f in the polynomial ring $\mathbb{Z}_p[x]$. We use this connection to develop efficient algorithms for determining the factorization types of monic polynomials of degree $k \leq 5$ in $\mathbb{Z}_p[x]$.

1. Introduction

This article grew out of an undergraduate research project, performed by the second author under the direction of the first, to determine if results about the periodicity of second-order linear homogeneous recurrence relations modulo positive integers could be extended to higher orders. We arrived, somewhat unexpectedly, at algorithms to determine the degrees of the irreducible factors of quintic and smaller degree polynomials modulo prime numbers. The algebraic properties of certain finite rings, particularly automorphisms of those rings, provided the connection between these two topics.

To illustrate some of the ideas in this article, we begin with the famous example of the Fibonacci sequence, defined by $F_n = F_{n-1} + F_{n-2}$ with $F_0 = 0$ and $F_1 = 1$. If, for some positive integer m, we replace each F_n by its remainder on division by m, we obtain a new sequence of integers. For example, the Fibonacci sequence modulo $m = 10$ begins

$$0, 1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, 4, 3, 7, 0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5, \ldots,$$

with the n-th term simply the last digit of F_n. We can also view such a sequence as having terms in $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$, the ring of integers modulo m. This has the advantage

MSC2000: 11B50, 11C08, 11T06.

Keywords: linear homogeneous recurrence relations, polynomial congruences, finite rings, finite fields.

that, rather than computing each F_n and dividing that term by m, we can merely begin with 0 and 1 and calculate successive terms of the sequence by adding the two preceding terms in $\mathbb{Z}_m$. This viewpoint makes it obvious that if there is a positive integer ℓ for which $F_\ell = 0$ and $F_{\ell+1} = 1$ (in $\mathbb{Z}_m$), the sequence will then repeat the pattern of $F_0, F_1, \ldots, F_{\ell-1}$ indefinitely. For the Fibonacci sequence, it is known that such a value of ℓ exists for every positive integer m. (For $m = 10$, it can be verified that $\ell = 60$.)

Upper limits on the period length of the Fibonacci sequence modulo prime numbers are implicit in Theorem 180 of [Hardy and Wright 1979], one proof of which employs properties of the powers of a root of $f(x) = x^2 - x - 1$, the characteristic polynomial of the Fibonacci sequence. Expanding on this approach, when considering recursive sequences of arbitrary order in this article, we work in rings, $\mathbb{Z}_m[\omega]$, of integers modulo m with a purely formal root ω of the characteristic polynomial f of the sequence adjoined. Our first main result (Corollary 5) is that under minor restrictions on m and the initial terms of the sequence, the period of the recursive sequence modulo m is equal to the order of ω in the group of units in $\mathbb{Z}_m[\omega]$.

Possible orders of ω in the group of units $\mathbb{Z}_p[\omega]^\times$, where p is prime, are determined by the factorization of f in the polynomial ring $\mathbb{Z}_p[x]$. In particular, using properties of ring automorphisms of $\mathbb{Z}_p[\omega]$, we find in Theorem 9 that if f has no repeated factors in $\mathbb{Z}_p[x]$, and t is the least common multiple of the degrees of the irreducible factors of f in $\mathbb{Z}_p[x]$, then t is the smallest positive integer for which the order of ω divides $p^t - 1$. For the Fibonacci sequence, and for other second-order recursive sequences, the important details of the factorization are obtained from standard results about quadratic congruences (particularly calculation of Legendre symbols via the quadratic reciprocity theorem). For sequences of higher order, with characteristic polynomials of higher degree, methods of determining this factorization are less apparent. Finally though, reversing the approach taken with second-order sequences, we show, in Theorem 11 and its corollaries, that information about powers of ω in the rings $\mathbb{Z}_p[\omega]$ lead to highly efficient algorithms for determining the factorization types of monic polynomials f with $\deg f \le 5$ modulo most primes p.

To outline this article: In Section 2, we define recursive sequences of order k, we consider the simple but instructive case in which $k = 1$, and we establish a criterion for periodicity of recursive sequences modulo arbitrary positive integers m. We introduce the characteristic polynomial f of a recursive sequence in Section 3, which we use to define the rings $\mathbb{Z}_m[\omega]$ referred to above. We show that the periodicity of recursive sequences modulo m can be easily described in terms of powers of the element ω in the ring $\mathbb{Z}_m[\omega]$. This leads us, in Section 4, to consider algebraic properties of these rings. We find that, for a prime modulus p, the relevant properties depend on the factorization of f (e.g., the degrees of irreducible factors, existence of repeated factors) in the ring of polynomials $\mathbb{Z}_p[x]$. In Section 5, we apply well known properties of quadratic congruences to obtain general results about periodicity modulo primes when $k = 2$, with the Fibonacci sequence as a special case. Finally, in Section 6, we obtain efficient algorithms for finding the factorization type of cubic, quartic, and quintic polynomials f modulo most primes p, using calculation of periods of recursive sequences modulo p, or computation of powers of ω. (Adams [1984] and Sun [2003] have separately used certain recursive sequences to develop algorithms for factorization of cubic and quartic polynomials modulo primes. Our algorithm differs in details from both of these.)

The authors are grateful to the referee for pointing out several sources of which we were not aware during the preparation of this article. Engstrom [1931], Ward [1933], and Fillmore and Marx [1968] have extensive details on linear recurrence relations modulo positive integers. See in particular Chapter 8 of [Lidl and Niederreiter 1983] for more results and notes about this aspect of the problem. Furthermore, Skolem [1952] has provided criteria for the factorization type of quartic polynomials modulo primes, similar to our result in Corollary 13, and [Sun 2006] notes a criterion for the factorization of a polynomial into linear factors modulo a prime number, which is essentially the same as the statement of part (1) in our Theorem 15.

2. Periodicity of recursive sequences modulo integers

Let m be a positive integer. We say that a sequence $\{a_n\}_{n=0}^{\infty}$ of integers is *periodic modulo m* or *ℓ-periodic modulo m* if there is a positive integer ℓ such that $a_{\ell+i} \equiv a_i \pmod{m}$ for all $i \geq 0$. We also say that $\{a_n\}_{n=0}^{\infty}$ is periodic in $\mathbb{Z}_m$ in this case, and when it is clear that we are referring to equality in this ring, we write $a_{\ell+i} = a_i$ rather than $a_{\ell+i} \equiv a_i \pmod{m}$. If ℓ is the smallest positive integer for which $\{a_n\}_{n=0}^{\infty}$ is ℓ-periodic modulo m, we call ℓ the *period* of the sequence modulo m.

Proposition 1. *If a sequence $\{a_n\}_{n=0}^{\infty}$ is periodic modulo m with period ℓ, then for a positive integer k, the sequence is k-periodic modulo m if and only if ℓ divides k.*

Proof. Suppose that $\{a_n\}_{n=0}^{\infty}$ is periodic in $\mathbb{Z}_m$ with period ℓ. Then $a_{2\ell+i} = a_{\ell+(\ell+i)} = a_{\ell+i} = a_i$ for all i, and inductively, $a_{\ell q+i} = a_i$ for all positive integers q. So if ℓ divides $k > 0$, then $\{a_n\}_{n=0}^{\infty}$ is k-periodic in $\mathbb{Z}_m$. Conversely then, suppose that $\{a_n\}_{n=0}^{\infty}$ is k-periodic in $\mathbb{Z}_m$ for some positive integer k. We can write $k = \ell q + r$ for some integers q and r with $0 \leq r < \ell$. Now for every $i \geq 0$, we have $a_i = a_{k+i} = a_{\ell q+(r+i)} = a_{r+i}$, since, as noted above, the sequence is ℓq-periodic. If $r > 0$, this contradicts the definition of ℓ as the period of the sequence. So we must conclude that $r = 0$ and so that ℓ divides k. □

In this article, we are primarily interested in the periodicity of sequences defined recursively. We fix the following notation for the sequences of interest. Let k be a positive integer, let $r_1, r_2, \dots, r_k$ be integers, and let $(a_0, a_1, \dots, a_{k-1})$ be a k-tuple of integers. Define a sequence of integers $\{a_n\}_{n=0}^{\infty}$ by setting

$$a_n = r_1 a_{n-1} + r_2 a_{n-2} + \cdots + r_{k-1} a_{n-k+1} + r_k a_{n-k} = \sum_{i=1}^{k} r_i a_{n-i}, \tag{2-1}$$

when $n \geq k$. A sequence of this form is called a *linear homogeneous recurrence relation of order* k; we will refer to it as a *recursive sequence of order* k for short. We call $r_1, r_2, \dots, r_k$ the *coefficients*, and $a_0, a_1, \dots, a_{k-1}$ the *initial terms* of this recursive sequence.

Remark. To establish that $\{a_n\}_{n=0}^{\infty}$ as defined in (2-1) is ℓ-periodic in $\mathbb{Z}_m$, it suffices, as we noted in Section 1 for the Fibonacci sequence, to show that $a_{\ell+i} = a_i$ for $0 \leq i \leq k-1$.

We can describe the periodicity of recursive sequences of order $k = 1$ using standard results about linear congruences from elementary number theory.

Example. Define a_n for $n \geq 0$ by setting $a_n = r a_{n-1}$ when $n > 0$, with r and a_0 integers. Then $a_n = a_0 r^n$ for all n, and the sequence is periodic modulo m if there is a positive integer ℓ such that $a_0 r^{\ell} \equiv a_0 \pmod{m}$. If $\gcd(a_0, m) = d$, this congruence is equivalent to $r^{\ell} \equiv 1 \pmod{m/d}$, and such a value of ℓ exists if and only if r is relatively prime to m/d. In that case, the period of the sequence equals $\mathrm{ord}_{m/d}(r)$, the order of r in the group $\mathbb{Z}_{m/d}^{\times}$ of units in $\mathbb{Z}_{m/d}$.

Remark. This example illustrates that we are unlikely to obtain a precise formula for the period of a recursive sequence modulo every positive integer m. For example, if $a_0 = 1$ and $a_n = 2a_{n-1}$ for $n > 0$, then the sequence $\{a_n\}_{n=0}^{\infty}$ is periodic modulo every odd positive integer m, with period the order of 2 in $\mathbb{Z}_m^{\times}$. We know that this order divides $\phi(m) = |\mathbb{Z}_m^{\times}|$, but a more specific formula for this value is difficult to obtain. Similarly, for larger values of k, we will generally be able to provide only upper limits on the period of a recursive sequence modulo an arbitrary integer m.

The following theorem provides a criterion for the periodicity of recursive sequences modulo positive integers m. Our proof follows that of a similar result in [Wall 1960] for the Fibonacci sequence.

Theorem 2. *Let $\{a_n\}_{n=0}^{\infty}$ be a recursive sequence with coefficients $r_1, r_2, \dots, r_k$, defined as in (2-1). Let m be a positive integer. If $\gcd(r_k, m) = 1$, then the sequence is periodic modulo m.*

Proof. There are m^k distinct k-tuples of elements of $\mathbb{Z}_m$. By the pigeonhole principle, it follows that there are integers s and t with $0 \leq s < t \leq m^k$ such that $a_{s+i} = a_{t+i}$

in $\mathbb{Z}_m$ for $0 \le i \le k-1$. We may assume that s is the smallest nonnegative integer for which this is true. But if $s > 0$, then $a_{s+k-1} = a_{t+k-1}$ implies that

$$r_1 a_{s+k-2} + r_2 a_{s+k-3} + \cdots + r_{k-1} a_s + r_k a_{s-1} \\ = r_1 a_{t+k-2} + r_2 a_{t+k-3} + \cdots + r_{k-1} a_t + r_k a_{t-1}$$

in $\mathbb{Z}_m$, by the recursive definition of the sequence. It follows that $r_k a_{s-1} = r_k a_{t-1}$, and if $\gcd(r_k, m) = 1$, so that r_k is a unit in $\mathbb{Z}_m$, then $a_{s-1} = a_{t-1}$ in $\mathbb{Z}_m$. This contradicts our assumption about s, so we must conclude that $s = 0$. By the note above, it follows that $\{a_n\}_{n=0}^{\infty}$ is periodic modulo m. □

Remark. If $\gcd(r_k, m) > 1$, then $\{a_n\}_{n=0}^{\infty}$ defined by (2-1) may or may not be periodic modulo m, depending on the initial terms of the sequence. For example, if $(a_0, a_1, \ldots, a_{k-1}) = (1, 0, \ldots, 0)$, then it is easy to see that r_k divides a_n for all $n > 0$, and so $a_\ell \equiv a_0 \pmod{m}$ is not possible for any $\ell > 0$. On the other hand, the sequence with initial terms $(a_0, a_1, \ldots, a_{k-1}) = (0, 0, \ldots, 0)$ is clearly 1-periodic modulo m. This trivial example is generally not exclusive. For instance, if $a_n = a_{n-1} + a_{n-2} + 2a_{n-3}$, with $(a_0, a_1, a_2) = (1, 0, 1)$, then the sequence $\{a_n\}_{n=0}^{\infty}$ is 3-periodic modulo $m = 2$. In any event, the proof of Theorem 2 shows that every recursive sequence defined as in (2-1) will exhibit an infinitely repeating pattern of terms modulo m, possibly following some initial terms. In the remainder of this article, given a recursive sequence of order k, we will restrict our attention to moduli m that are relatively prime to the k-th order coefficient r_k.

3. Polynomial extensions of $\mathbb{Z}_m$

If $\{a_n\}_{n=0}^{\infty}$ is a recursive sequence given as in (2-1), then we define the *characteristic polynomial* of that sequence to be

$$f(x) = x^k - r_1 x^{k-1} - r_2 x^{k-2} - \cdots - r_{k-1} x - r_k.$$

It is well known that each a_n can be expressed in terms of n-th powers of the solutions of $f(x) = 0$, with the combination of those powers determined by the initial terms of the sequence. In considering arithmetic properites of the sequence $\{a_n\}_{n=0}^{\infty}$ modulo m, we will find it useful to work in rings, $\mathbb{Z}_m[\omega]$, of the integers modulo m with a purely formal solution, ω, of $f(x) = 0$ adjoined. We define these rings as follows.

For a positive integer m, consider the quotient ring $\mathbb{Z}_m[x]/\langle f \rangle$, where $\mathbb{Z}_m[x]$ is the ring of polynomials with coefficients in $\mathbb{Z}_m$ and $\langle f \rangle$ is the principal ideal of $\mathbb{Z}_m[x]$ generated by f. Since f is a *monic* polynomial, that is, its leading coefficient is 1, then for every polynomial g in $\mathbb{Z}_m[x]$, there exist unique polynomials q and r in $\mathbb{Z}_m[x]$ such that $g = f \cdot q + r$, with r of smaller degree than f, or $r = 0$. In that case, $g+\langle f\rangle = r+\langle f\rangle$. Writing the coset $x+\langle f\rangle$ as ω_f, or as ω when f is apparent from context, we can identify $\mathbb{Z}_m[x]/\langle f\rangle$ with the ring $\mathbb{Z}_m[\omega]$ defined by

$$\mathbb{Z}_m[\omega] = \Big\{ b_{k-1}\omega^{k-1}+b_{k-2}\omega^{k-2}+\cdots+b_1\omega+b_0 \,\Big|\, b_i\in\mathbb{Z}_m \text{ and } \omega^k=\sum_{i=1}^{k} r_i\omega^{k-i}\Big\}. \tag{3-1}$$

Here $b_{k-1}\omega^{k-1}+\cdots+b_0 = c_{k-1}\omega^{k-1}+\cdots+c_0$ if and only if $b_i=c_i$ in $\mathbb{Z}_m$ for $0\le i\le k-1$, so in general, $\mathbb{Z}_m[\omega]$ has m^k elements. We refer to $\mathbb{Z}_m[\omega]$ as the *extension of* $\mathbb{Z}_m$ *by the polynomial* f or more generally as a *polynomial extension* of $\mathbb{Z}_m$. We write elements of $\mathbb{Z}_m[\omega]$ using Greek letters, or in the form $g(\omega)$ where g is a polynomial in $\mathbb{Z}_m[x]$.

We establish a connection between the ring $\mathbb{Z}_m[x]/\langle f\rangle$ and recursive sequences with characteristic polynomial f as follows. Let $\{a_n\}_{n=0}^{\infty}$ be defined as in (2-1), and for $1\le j\le k$ and $n\ge k$, let $a(j,n)=\sum_{i=j}^{k} r_i a_{n-i}$. Notice that, for all $n\ge k$,

$$a(k,n)=r_k a_{n-k} \tag{3-2}$$

and

$$a(j+1,n)+r_j a_{n-j} = a(j,n) \quad \text{if } 1\le j<k. \tag{3-3}$$

Now define α to be the following element of $\mathbb{Z}_m[\omega]$, determined by the initial terms and coefficients of the sequence:

$$\begin{aligned}\alpha &= a_{k-1}\omega^{k-1}+a(2,k)\omega^{k-2}+a(3,k+1)\omega^{k-3}+\cdots+a(k-1,2k-3)\omega+a(k,2k-2)\\ &= a_{k-1}\omega^{k-1}+\sum_{j=2}^{k} a(j,k+j-2)\cdot\omega^{k-j},\end{aligned} \tag{3-4}$$

here viewing a_{k-1} and each $a(j,k+j-2)$ as elements of $\mathbb{Z}_m$.

Theorem 3. *Let $\{a_n\}_{n=0}^{\infty}$ be defined recursively as in (2-1), and let α be defined by (3-4). Then for every integer $n\ge 0$,*

$$\alpha\omega^n = a_{n+k-1}\omega^{k-1}+\sum_{j=2}^{k} a(j,n+k+j-2)\cdot\omega^{k-j}. \tag{3-5}$$

Remark. If $n\ge 1$, then $a_{n+k-1}=\sum_{i=1}^{k} r_i a_{n+k-1-i} = a(1,n+k-1)$ by the recursive definition of the sequence. So for $n\ge 1$, we can also express (3-5) as

$$\alpha\omega^n = \sum_{j=1}^{k} a(j,n+k+j-2)\cdot\omega^{k-j}. \tag{3-6}$$

Proof. We use induction on n. Equation (3-5) is true for $n=0$ by (3-4). So suppose that (3-5) holds for some integer $n\ge 0$. Then

$$\alpha\omega^{n+1} = (\alpha\omega^n)\omega = a_{n+k-1}\omega^k + \sum_{j=2}^{k} a(j, n+k+j-2)\cdot\omega^{k-j+1}$$
$$= \sum_{j=1}^{k} r_j a_{n+k-1}\cdot\omega^{k-j} + \sum_{j=2}^{k} a(j, n+k+j-2)\cdot\omega^{k-j+1},$$

using the equation for ω^k in (3-1). Splitting off the last term in the first sum, and replacing j by $j+1$ in the second sum, we have that

$$\alpha\omega^{n+1} = r_k a_{n+k-1} + \sum_{j=1}^{k-1} r_j a_{n+k-1}\cdot\omega^{k-j} + \sum_{j=1}^{k-1} a(j+1, n+k+j-1)\cdot\omega^{k-j}$$
$$= r_k a_{n+k-1} + \sum_{j=1}^{k-1} (r_j a_{n+k-1} + a(j+1, n+k+j-1))\cdot\omega^{k-j}$$
$$= r_k a_{n+k-1} + \sum_{j=1}^{k-1} a(j, n+k+j-1)\cdot\omega^{k-j},$$

using (3-3). But $r_k a_{n+k-1} = a(k, n+2k-1)$ by (3-2), so that

$$\alpha\omega^{n+1} = \sum_{j=1}^{k} a(j, n+k+j-1)\cdot\omega^{k-j}.$$

This is (3-6) with $n+1$ in place of n. Since $n+1 \geq 1$, (3-5) is then true with $n+1$ in place of n, and so (3-5) holds for all integers $n \geq 0$ by induction. $\square$

Theorem 4. *Let k be a positive integer, and let $\{a_n\}_{n=0}^{\infty}$ be a recursive sequence with coefficients $r_1, \ldots, r_k$ and characteristic polynomial f, defined as in (2-1). Let m be a positive integer such that $\gcd(r_k, m) = 1$, let $\mathbb{Z}_m[\omega] = \mathbb{Z}_m[x]/\langle f\rangle$, and let α be given as in (3-4). Then $\{a_n\}_{n=0}^{\infty}$ is ℓ-periodic modulo m if and only if $\alpha\omega^{\ell} = \alpha$ in $\mathbb{Z}_m[\omega]$.*

Proof. If $a_{\ell+i} = a_i$ for all $i \geq 0$, then, in particular, $a_{\ell+k-1} = a_{k-1}$, and it is easy to see that $a(j, \ell+k+j-2) = a(j, k+j-2)$ for $2 \leq j \leq k$. Thus $\alpha\omega^{\ell} = \alpha$ by (3-5).

Conversely, suppose that $\alpha\omega^{\ell} = \alpha$. Comparing the equations in (3-4) and (3-5), we know that $a_{\ell+k-1} = a_{k-1}$ and $a(j, \ell+k+j-2) = a(j, k+j-2)$ in $\mathbb{Z}_m$ for $2 \leq j \leq k$. But if $\gcd(r_k, m) = 1$, so that r_k is a unit in $\mathbb{Z}_m$, we can use the latter equations to show inductively that $a_{\ell+j-2} = a_{j-2}$ for $2 \leq j \leq k$, which is sufficient to establish that the sequence is ℓ-periodic. If $j = k$, then $a(k, \ell+2k-2) = a(k, 2k-2)$ implies that $r_k a_{\ell+k-2} = r_k a_{k-2}$, so that $a_{\ell+k-2} = a_{k-2}$. Now let j be an integer with $2 \leq j < k$, and suppose that we have shown that $a_{\ell+i-2} = a_{i-2}$ for $j < i \leq k$.

Then $a(j, \ell+k+j-2) = a(j, k+j-2)$ implies that

$$r_j a_{\ell+k-2} + r_{j+1} a_{\ell+k-3} + \cdots + r_{k-1} a_{\ell+j-1} + r_k a_{\ell+j-2} \\ = r_j a_{k-2} + r_{j+1} a_{k-3} + \cdots + r_{k-1} a_{j-1} + r_k a_{j-2},$$

which, by the inductive hypothesis and the assumption that r_k is a unit, implies that $a_{\ell+j-2} = a_{j-2}$. The result follows by induction. □

Corollary 5. *Let k be a positive integer, and let $\{a_n\}_{n=0}^{\infty}$ be a recursive sequence with coefficients $r_1, \ldots, r_k$ and characteristic polynomial f, defined as in (2-1). Let m be a positive integer such that $\gcd(r_k, m) = 1$, let $\mathbb{Z}_m[\omega] = \mathbb{Z}_m[x]/\langle f \rangle$, and let α be given as in (3-4). Then ω is a unit in $\mathbb{Z}_m[\omega]$, and $\{a_n\}_{n=0}^{\infty}$ is periodic modulo m, with period ℓ dividing $\operatorname{ord}_m(\omega)$, the order of ω in the group, $\mathbb{Z}_m[\omega]^\times$, of units in $\mathbb{Z}_m[\omega]$. If $A = \{\beta \in \mathbb{Z}_m[\omega] \mid \alpha\beta = 0\}$, then ℓ is the order of $\omega + A$ in the group of units of the quotient ring $\mathbb{Z}_m[\omega]/A$.*

Remark. It is easy to see that the set A defined in the corollary is an ideal of $\mathbb{Z}_m[\omega]$. This ideal, called the *annihilator* of α in $\mathbb{Z}_m[\omega]$, is trivial if α is a unit in $\mathbb{Z}_m[\omega]$, so in that case, $\ell = \operatorname{ord}_m(\omega)$.

Proof. If $\gcd(r_k, m) = 1$, then r_k is a unit in $\mathbb{Z}_m$, say with inverse r_k^{-1}. Then it is easy to verify that $r_k^{-1}(\omega^{k-1} - r_1\omega^{k-2} - \cdots - r_{k-2}\omega - r_{k-1}) \cdot \omega = 1$, so that ω is a unit in $\mathbb{Z}_m[\omega]$. Since $\mathbb{Z}_m[\omega]^\times$ is finite, there is an integer $t = \operatorname{ord}_m(\omega)$ for which $\omega^t = 1$. But then $\alpha\omega^t = \alpha$, and Theorem 4 implies that $\{a_n\}_{n=0}^{\infty}$ is t-periodic modulo m. If ℓ is the period of this sequence modulo m, we know that ℓ divides t by Proposition 1. Furthermore, ℓ is the smallest positive integer such that $\alpha\omega^\ell = \alpha$, which is true if and only if $\omega^\ell - 1$ is in the annihilator of α. But then ℓ is the the order of $\omega + A$ as a unit in the quotient ring $\mathbb{Z}_m[\omega]/A$. □

Example. Consider the recursive sequence of order $k = 1$ defined by $a_n = r a_{n-1}$ for $n > 0$, with a_0 and r fixed integers, as in a previous example. Let m be a positive integer that is relatively prime to r, in which case the sequence is periodic modulo m. The characteristic polynomial of $\{a_n\}_{n=0}^{\infty}$ is $f(x) = x - r$, so that $\omega = x + \langle f \rangle = r + \langle f \rangle$ in $\mathbb{Z}_m[x]/\langle f \rangle$. It is easy to see that $\mathbb{Z}_m[x]/\langle f \rangle$ is isomorphic to $\mathbb{Z}_m$, so that we can identify ω with r. By (3-4), we have that $\alpha = a_0$, and if $\gcd(a_0, m) = d$, then we find that the annihilator A of α in $\mathbb{Z}_m[\omega]$ is generated by m/d. Corollary 5 implies that the period of $\{a_n\}_{n=0}^{\infty}$ is the order of $r + A$ in $(\mathbb{Z}_m[\omega]/A)^\times$, which we can view as the order of r in $\mathbb{Z}_{m/d}^\times$. Thus we see that Corollary 5 generalizes our results for recursive sequences of order $k = 1$ to higher orders.

Example. It can be verified that the period of the Fibonacci sequence modulo $m = 5$ is 20. On the other hand, the *Lucas sequence*, defined for $n \geq 0$ by $(L_0, L_1) = (2, 1)$, and $L_n = L_{n-1} + L_{n-2}$ if $n > 1$, has period four modulo $m = 5$. This is possible because, for the Fibonacci sequence, $\alpha = \omega$ is a unit in $\mathbb{Z}_5[\omega]$, where $\omega^2 = \omega + 1$, while for the Lucas sequence, $\alpha = \omega + 2$ has a nontrivial annihilator in $\mathbb{Z}_5[\omega]$.

Remark. If the initial terms of a recursive sequence are $(a_0, \ldots, a_{k-2}, a_{k-1}) = (0, \ldots, 0, 1)$, then $\alpha = \omega^{k-1}$ is a unit, when ω is a unit in $\mathbb{Z}_m[\omega]$. In this case, Corollary 5 implies that the period of the sequence modulo m is the same as the order of ω in $\mathbb{Z}_m[\omega]^\times$. We will restrict our attention to this special case for the initial terms in what follows.

In the remainder of this article, we will further restrict our attention to the case in which the modulus m of interest is prime, using the following observations. First suppose that $\{a_n\}_{n=0}^\infty$ is periodic modulo s with period k, and periodic modulo t with period ℓ. If $\gcd(s, t) = 1$, it is straightforward to show, using Proposition 1, that $\{a_n\}_{n=0}^\infty$ is periodic modulo st with period $\operatorname{lcm}(k, \ell)$. (This does not require the assumption that the sequence is defined recursively.) For powers of primes, we can invoke the following result.

Theorem 6. *Let p be a prime number and j a positive integer. Let f be a polynomial with integer coefficients, and suppose that p does not divide the constant coefficient of f, so that ω is a unit in $\mathbb{Z}_{p^j}[\omega] = \mathbb{Z}_{p^j}[x]/\langle f \rangle$. Let $s = \operatorname{ord}_{p^j}(\omega)$ and $t = \operatorname{ord}_{p^{j+1}}(\omega)$. Then either $t = s$ or $t = ps$.*

Remark. If d divides m, then it is easy to see that the function $\phi : \mathbb{Z}_m[\omega] \to \mathbb{Z}_d[\omega]$ defined by $\phi(g(\omega)) = g(\omega)$ is a well-defined ring homomorphism, with kernel $\langle d \rangle$. So if $g(\omega) = h(\omega)$ in $\mathbb{Z}_m[\omega]$, then $g(\omega) = h(\omega)$ in $\mathbb{Z}_d[\omega]$. On the other hand, if $g(\omega) = h(\omega)$ in $\mathbb{Z}_d[\omega]$, then the strongest statement that we can make is that $g(\omega) = h(\omega) + d \cdot \delta$ for some element δ in $\mathbb{Z}_m[\omega]$.

Proof. Let s be the order of ω in $\mathbb{Z}_{p^j}[\omega]$ and let t be the order of ω in $\mathbb{Z}_{p^{j+1}}[\omega]$. Since $\omega^t = 1$ in $\mathbb{Z}_{p^{j+1}}[\omega]$, then $\omega^t = 1$ in $\mathbb{Z}_{p^j}[\omega]$ by the remark above, so that s divides t. By the same remark, since $\omega^s = 1$ in $\mathbb{Z}_{p^j}[\omega]$, then $\omega^s = 1 + p^j \cdot \delta$ for some δ in $\mathbb{Z}_{p^{j+1}}[\omega]$. But now

$$\omega^{ps} = (\omega^s)^p = (1 + p^j \cdot \delta)^p = 1 + \binom{p}{1} p^j \cdot \delta + \binom{p}{2} p^{2j} \cdot \delta^2 + \cdots + p^{pj} \cdot \delta^p = 1$$

in $\mathbb{Z}_{p^{j+1}}[\omega]$, since all terms in the sum aside from the first are divisible by p^{j+1}. Thus t divides ps. Since $s \mid t$ and $t \mid ps$, with p prime, we conclude that $t = s$ or $t = ps$. □

So if ℓ is the period of a recursive sequence modulo p, then the period of the same sequence modulo p^j must divide $p^{j-1} \cdot \ell$. Interesting questions about periods of recursive sequences modulo prime powers remain open. For example, Sun and Sun [1992] showed that if a prime exponent p were a counterexample to the first case of Fermat's Last Theorem, then the period of the Fibonacci sequence modulo

p and modulo p^2 would have to be the same. It is not known whether any such primes exist for the Fibonacci sequence. (Of course, it is now known that no such counterexamples to Fermat's Last Theorem can exist.) For our purposes, we will simply note that the upper limit given above is not always obtained as the exact period of a recursive sequence modulo p^j, as the following example shows.

Example. Define a_n for $n \geq 0$ by $(a_0, a_1, a_2) = (0, 0, 1)$ and

$$a_n = a_{n-1} + a_{n-2} + 2a_{n-3}$$

for $n > 2$. We find that $\{a_n\}_{n=0}^{\infty}$ has period $\ell = 6$ both modulo $p = 3$ and modulo $p^2 = 9$.

4. Algebraic properties of $\mathbb{Z}_p[\omega]$

With these restrictions in place, our main task, given the characteristic polynomial f of a recursive sequence, is to describe the order of $\omega = \omega_f = x + \langle f \rangle$ as a unit in the quotient ring $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$, for all primes p not dividing the constant coefficient of f. We will see that our description of $\mathrm{ord}_p(\omega)$ depends largely on how f factors in the polynomial ring $\mathbb{Z}_p[x]$. We begin by compiling some useful general statements about these polynomial extensions.

(1) If g divides f, then the function $\phi : \mathbb{Z}_p[\omega_f] \to \mathbb{Z}_p[\omega_g]$ defined by $\phi(h(\omega_f)) = h(\omega_g)$ is a well-defined ring homomorphism with kernel $\langle g(\omega_f) \rangle$. It follows that if $r(\omega_f) = s(\omega_f)$ in $\mathbb{Z}_p[\omega_f]$, then $r(\omega_g) = s(\omega_g)$ in $\mathbb{Z}_p[\omega_g]$, while if $r(\omega_g) = s(\omega_g)$ in $\mathbb{Z}_p[\omega_g]$, then $r(\omega_f) = s(\omega_f) + g(\omega_f) \cdot \delta$ for some δ in $\mathbb{Z}_p[\omega_f]$.

(2) The set of all (ring) automorphisms of $\mathbb{Z}_p[\omega]$ forms a group under composition. If h is a polynomial in $\mathbb{Z}_p[x]$ and $\sigma : \mathbb{Z}_p[\omega] \to \mathbb{Z}_p[\omega]$ is an automorphism, then $\sigma(h(\omega)) = h(\sigma(\omega))$. In particular, $0 = \sigma(0) = \sigma(f(\omega)) = f(\sigma(\omega))$, so that $\sigma(\omega)$ is a root of f.

(3) For an automorphism σ of $\mathbb{Z}_p[\omega]$, if $\sigma(\omega) = \omega$, then $\sigma(h(\omega)) = h(\sigma(\omega)) = h(\omega)$ for all $h \in \mathbb{Z}_p[x]$. That is, $\sigma(\omega) = \omega$ if and only if σ is the identity automorphism.

(4) The function $\sigma_p : \mathbb{Z}_p[\omega] \to \mathbb{Z}_p[\omega]$ defined by $\sigma_p(\beta) = \beta^p$ is a ring homomorhism, since $\mathbb{Z}_p[\omega]$ has characteristic p. Furthermore, σ_p is an automorphism if and only if the polynomial f has no repeated irreducible factors in $\mathbb{Z}_p[x]$. (If $f = g^2 h$ for some irreducible polynomial g, then $g(\omega)h(\omega)$ is a nonzero element in the kernel of σ_p. On the other hand, if f has no repeated irreducible factors, then the uniqueness of irreducible factorization in $\mathbb{Z}_p[x]$ shows that f divides h^p if and only if f divides h. In that case, the kernel of σ_p is trivial, and since $\mathbb{Z}_p[\omega]$ is finite, σ_p is a bijection.)

(5) If f is irreducible in $\mathbb{Z}_p[x]$, with $\deg f = k$, then $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$ is a field with p^k elements. In this case, the group $\mathrm{Aut}(\mathbb{Z}_p[\omega])$ of automorphisms of $\mathbb{Z}_p[\omega]$ is cyclic of order k, generated by σ_p [Dummit and Foote 2004, p. 556].

(6) If $f = f_1 \cdot f_2 \cdots f_j$ is a product of pairwise relatively prime polynomials in $\mathbb{Z}_p[x]$, then the quotient ring $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$ is isomorphic to the direct product of quotient rings $\mathbb{Z}_p[x]/\langle f_1 \rangle \times \mathbb{Z}_p[x]/\langle f_2 \rangle \times \cdots \times \mathbb{Z}_p[x]/\langle f_j \rangle$ [Dummit and Foote 2004, p. 313].

We can draw some conclusions about the order of ω in $\mathbb{Z}_p[\omega]^\times$ from these statements. We begin with the case in which f is irreducible in $\mathbb{Z}_p[x]$.

Theorem 7. *Let $f(x) = x^k - r_1 x^{k-1} - \cdots - r_k$. Let p be a prime for which $p \nmid r_k$, and suppose that f is irreducible in $\mathbb{Z}_p[x]$. Let t be the order of $(-1)^{k+1} r_k$ as an element of $\mathbb{Z}_p^\times$. Then $\mathrm{ord}_p(\omega)$, the order of ω as a unit in $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$, divides $\frac{p^k-1}{p-1} t$, but $\mathrm{ord}_p(\omega)$ divides neither $p^i - 1$ for $0 < i < k$ nor $\frac{p^k-1}{p-1} s$ for $0 < s < t$.*

Proof. By statement (5), we know that $\mathrm{Aut}(\mathbb{Z}_p[\omega])$ is cyclic of order k, generated by σ_p. The composition of i copies of σ_p is the same as σ_{p^i}, defined by $\sigma_{p^i}(\beta) = \beta^{p^i}$. Statement (3) implies that $\omega^{p^i} \neq \omega$, and so $\omega^{p^i - 1} \neq 1$, for $0 < i < k$.

Statement (2) now implies that f has k distinct roots in $\mathbb{Z}_p[\omega]$, each of the form $\sigma_{p^i}(\omega) = \omega^{p^i}$ for $0 \leq i < k$, and therefore

$$f(x) = (x - \omega)(x - \omega^p)(x - \omega^{p^2}) \cdots (x - \omega^{p^{k-1}}).$$

Comparing constant coefficients of these polynomials, we find that $-r_k = (-1)^k \omega \cdot \omega^p \cdot \omega^{p^2} \cdots \omega^{p^{k-1}}$, and so

$$(-1)^{k+1} r_k = \omega^{1+p+p^2+\cdots+p^{k-1}} = \omega^{\frac{p^k-1}{p-1}}.$$

If t is the order of $(-1)^{k+1} r_k$ in $\mathbb{Z}_p^\times$, then $\omega^{\frac{p^k-1}{p-1} t} = 1$, but $\omega^{\frac{p^k-1}{p-1} s} \neq 1$ for $0 < s < t$. $\square$

Secondly, we consider the case in which f is a power of an irreducible polynomial.

Theorem 8. *Let f be a monic polynomial of degree k with integer coefficients. Suppose that $f = g^t$, where g is an irreducible polynomial of degree s in $\mathbb{Z}_p[x]$ (so that $st = k$). Let p be a prime number not dividing the constant coefficient of g (and so not dividing the constant coefficient of f). Let j be the smallest nonnegative integer for which $p^j \geq t$. Let $\mathbb{Z}_p[\omega_f] = \mathbb{Z}_p[x]/\langle f \rangle$ and $\mathbb{Z}_p[\omega_g] = \mathbb{Z}_p[x]/\langle g \rangle$, and suppose that ω_g has order ℓ as a unit in $\mathbb{Z}_p[\omega_g]$. Then the order of ω_f as a unit in $\mathbb{Z}_p[\omega_f]$ equals $p^i \ell$ for some i with $0 \leq i \leq j$.*

Proof. Let m be the order of ω_f in the group $\mathbb{Z}_p[\omega_f]^\times$. Since $(\omega_f)^m = 1$ in $\mathbb{Z}_p[\omega_f]$, then $(\omega_g)^m = 1$ in $\mathbb{Z}_p[\omega_g]$ by statement (1), so that ℓ divides m. Since $(\omega_g)^\ell = 1$ in $\mathbb{Z}_p[\omega_g]$, statement (1) also implies that $(\omega_f)^\ell = 1 + g(\omega_f)\cdot\delta$ for some δ in $\mathbb{Z}_p[\omega_f]$. Now note that

$$(\omega_f)^{p^j\ell} = ((\omega_f)^\ell)^{p^j} = (1 + g(\omega_f)\cdot\delta)^{p^j} = 1 + g(\omega_f)^{p^j}\cdot\delta^{p^j} = 1,$$

in $\mathbb{Z}_p[\omega_f]$, using the facts that $\mathbb{Z}_p[\omega_f]$ has characteristic p and that $f = g^t$ divides g^{p^j}, by the definition of j. So m divides $p^j\ell$, and the conclusion of Theorem 8 follows immediately. $\square$

Finally, if f factors as a product of pairwise relatively prime polynomials, say $f = f_1\cdot f_2\cdots f_j$ with each f_i a power of a distinct irreducible polynomial in $\mathbb{Z}_p[x]$, then $\mathbb{Z}_p[\omega_f]$ is isomorphic to

$$\mathbb{Z}_p[\omega_{f_1}] \times \mathbb{Z}_p[\omega_{f_2}] \times \cdots \times \mathbb{Z}_p[\omega_{f_j}]$$

by statement (6). If a prime number p does not divide the constant coefficient of f, then it is easy to see that the order of ω_f in $\mathbb{Z}_p[\omega_f]^\times$ is the least common multiple of the orders of each ω_{f_i} in the appropriate group of units. We can place a further restriction on the order of ω_f when no irreducible factor of f is repeated.

Theorem 9. *Let f be a monic polynomial of degree k with integer coefficients, and let p be a prime number not dividing the constant coefficient of f. Suppose that $f = f_1\cdot f_2\cdots f_j$ for distinct irreducible polynomials f_i of degree k_i in $\mathbb{Z}_p[x]$ (so that $k = k_1 + k_2 + \cdots + k_j$). Let $t = \operatorname{lcm}(k_1, k_2, \ldots, k_j)$. Then in the group $\mathbb{Z}_p[\omega]^\times$ of units in the ring $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f\rangle$, the order of ω divides $p^t - 1$, but does not divide $p^i - 1$ for $0 < i < t$.*

Proof. By statement (4), the function $\sigma_p : \mathbb{Z}_p[\omega] \to \mathbb{Z}_p[\omega]$ defined by $\sigma_p(\beta) = \beta^p$ is an automorphism of $\mathbb{Z}_p[\omega]$. With $\mathbb{Z}_p[\omega_f]$ isomorphic to $\mathbb{Z}_p[\omega_{f_1}] \times \mathbb{Z}_p[\omega_{f_2}] \times \cdots \times \mathbb{Z}_p[\omega_{f_j}]$ and each $\mathbb{Z}_p[\omega_{f_i}]$ a field, it is straightforward to show that the order of σ_p in $\operatorname{Aut}(\mathbb{Z}_p[\omega])$ is $t = \operatorname{lcm}(k_1, k_2, \ldots, k_j)$. By statement (3), it follows that $\omega^{p^t} = \omega$, but $\omega^{p^i} \neq \omega$ if $0 < i < t$. Since ω is a unit in $\mathbb{Z}_p[\omega]$, the conclusion of Theorem 9 follows. $\square$

5. Recursive sequences of order two

We illustrate our results so far with some general statements about recursive sequences of order two. Define a_n for $n \geq 0$ by $(a_0, a_1) = (0, 1)$, and $a_n = r_1 a_{n-1} + r_2 a_{n-2}$ for $n > 1$, where r_1 and r_2 are integers. Let p be a prime number, let $f(x) = x^2 - r_1 x - r_2$, and let $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f\rangle$. If $p \nmid r_2$, then $\{a_n\}_{n=0}^\infty$ is periodic modulo p, with period ℓ equal to the order of ω in $\mathbb{Z}_p[\omega]^\times$. The factorization of f in $\mathbb{Z}_p[x]$ is determined by its *discriminant*, $D = D(f) = r_1^2 + 4r_2$, and we can use that factorization to describe ℓ.

Case 1: *f is irreducible in $\mathbb{Z}_p[x]$.* For odd p, this is the case if and only if the Legendre symbol $\left(\frac{D}{p}\right)$ equals -1, while for $p = 2$ this occurs precisely when $D \equiv 5 \pmod 8$. Theorem 7 implies that ℓ divides $(p+1)t$, where t is the order of $-r_2$ in $\mathbb{Z}_p^\times$, but that ℓ divides neither $p-1$ nor $(p+1)s$ for $0 < s < t$.

Case 2: *f factors as a product of distinct linear polynomials in $\mathbb{Z}_p[x]$.* For odd p, this is the case if and only if $\left(\frac{D}{p}\right) = 1$, while for $p = 2$, this occurs in general when $D \equiv 1 \pmod 8$. (Of course, it is impossible for a quadratic polynomial f to factor into distinct linear terms in $\mathbb{Z}_2[x]$ unless 2 divdes its constant coefficient, which we assume is not the case here.) Theorem 9 implies that ℓ divides $p-1$. More precisely, if $f(x) = (x-b)(x-c)$ in $\mathbb{Z}_p[x]$, then ℓ is the least common multiple of the orders of b and c in $\mathbb{Z}_p^\times$. (If $f_1(x) = x - b$, then $\omega_{f_1} = x + \langle f_1\rangle = b + \langle f_1\rangle$ in $\mathbb{Z}_p[x]/\langle f_1\rangle$, which is isomorphic to $\mathbb{Z}_p$.)

Case 3: *f factors as the square of a linear polynomial in $\mathbb{Z}_p[x]$.* This is the case if and only if p divides D. Since $p \geq 2$ for every prime p, Theorem 8 implies that ℓ divides $p(p-1)$. In this case, we can make the following precise statement as a corollary of Theorem 8.

Corollary 10. *Let $f(x) = x^2 - r_1x - r_2$ with r_1 and r_2 integers. Let p be a prime number dividing $D = r_1^2 + 4r_2$ but not dividing r_2, so that $f(x) = (x-c)^2$ in $\mathbb{Z}_p[x]$ for some $c \neq 0$ in $\mathbb{Z}_p$. If t is the order of c in $\mathbb{Z}_p^\times$, then the order of $\omega = x + \langle f\rangle$ as a unit in $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f\rangle$ is pt.*

Proof. Let $g(x) = x - c$, and let t be the order of c in $\mathbb{Z}_p^\times$. Since $\omega_g = x + \langle g\rangle = c + \langle g\rangle$, then t is the order of ω_g as a unit in $\mathbb{Z}_p[\omega_g]$. Theorem 8 implies that the order of ω_f in $\mathbb{Z}_p[\omega_f]^\times$ is either t or pt. But $(\omega_f)^t = 1$ if and only if $f(x) = (x-c)^2$ divides $h(x) = x^t - 1$ in $\mathbb{Z}_p[x]$. If so, then $h(c)$ and $h'(c)$ are both zero in $\mathbb{Z}_p$. This is impossible since $h'(c) = tc^{t-1}$, but $p \nmid t$ (a divisor of $p-1$) and $p \nmid c$. So the order of ω_f in $\mathbb{Z}_p[\omega_f]^\times$ must be pt. □

Example. For the Fibonacci sequence, $r_1 = 1$, $r_2 = 1$, and $D = 5$. Since $p \nmid r_2$ for all primes p, the Fibonacci sequence is periodic modulo p, say with period ℓ_p. The polynomial $x^2 - x - 1$ is irreducible in $\mathbb{Z}_2[x]$, since $D \equiv 5 \pmod 8$. The order of $-r_2 = -1$ in $\mathbb{Z}_2^\times$ is 1, and so for $p = 2$, we have that ℓ_p is a divisor of $p + 1 = 3$, but not $p - 1 = 1$. The only possibility is $\ell_2 = 3$, which is easy to verify directly. Since $x^2 - x - 1 = (x-3)^2$ in $\mathbb{Z}_5[x]$, and $c = 3$ has order four in $\mathbb{Z}_5^\times$, Corollary 10 implies that $\ell_5 = 20$. (Note that these two results, together with the remark preceding Theorem 6, verify the claim made in the introduction that the Fibonacci sequence has period $\ell = 60$ modulo $m = 10$.)

If $p \neq 2, 5$, then since $5 \equiv 1 \pmod 4$, quadratic reciprocity implies that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, so that factorization of $x^2 - x - 1$ is determined by the value of p modulo 5. If $p \equiv 1$ or $4 \pmod 5$, then $\left(\frac{5}{p}\right) = 1$ and $x^2 - x - 1$ factors as a product of linear factors in $\mathbb{Z}_p[x]$. Theorem 9 implies that ℓ_p divides $p-1$. If $p \equiv 2$ or $3 \pmod 5$ for an odd prime p, then $\left(\frac{5}{p}\right) = -1$ and $x^2 - x - 1$ is irreducible in $\mathbb{Z}_p[x]$. In this case, the order of $-r_2 = -1$ in $\mathbb{Z}_p^\times$ is 2, and so ℓ_p divides $2(p+1)$, but divides neither $p+1$ nor $p-1$. The period of the Fibonacci sequence modulo p can be smaller than the upper limits noted here for $p \neq 2, 5$. For example, $\ell_{29} = 14$, a proper divisor of $29-1$, and $\ell_{47} = 32$, a proper divisor of $2(47+1) = 96$ that divides neither 48 nor 46.

As we see here, unless the discriminant D of a quadratic polynomial f is identically zero, there are only finitely many primes p for which f has repeated factors in $\mathbb{Z}_p[x]$. The following generalization of the discriminant for higher degree polynomials similarly allows us (in theory) to determine all values of p for which a given polynomial f factors into distinct irreducible terms in $\mathbb{Z}_p[x]$. Let f be a monic polynomial of degree k with integer coefficients, which we can view as elements of $\mathbb{Z}$ or of $\mathbb{Z}_p$ for a prime p. Then f has k roots (not necessarily distinct) in some extension field of $\mathbb{Q}$ or $\mathbb{Z}_p$, and we can write

$$f(x) = x^k - r_1 x^{k-1} - \cdots - r_{k-1}x - r_k = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k).$$

By definition, the *discriminant* of f is the product of the squares of all differences between the roots of f:

$$D = D(f) = \prod_{1 \le i < j \le k} (\alpha_j - \alpha_i)^2.$$

It immediately follows that $D(f) = 0$ if and only if f has a repeated root, that is, $\alpha_i = \alpha_j$ for some $i \neq j$. Note that D is a *symmetric polynomial* in $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, meaning that it is unchanged by any permutation of the elements of that set. It is known that any such symmetric polynomial can be expressed in terms of *elementary* symmetric polynomials, which are, up to sign, the same as the coefficients of f. In general, if the coefficients of f are integers, then $D(f)$ is an integer which can be expressed in terms of those coefficients. (See [Edwards 1984] or [Swan 1962] for more details on computation of D.)

6. Criteria for factorization of polynomials modulo primes

Let f be a monic polynomial with integer coefficients, having degree k and discriminant D. In this section, we restrict our attention to primes p for which $p \nmid D$, so that f has no repeated irreducible factors in $\mathbb{Z}_p[x]$. We say that f has *factorization type* $[k_1, k_2, \ldots, k_j]$ modulo p if f can be written in $\mathbb{Z}_p[x]$ as a product of distinct irreducible polynomials having degrees $k_1 \ge k_2 \ge \cdots \ge k_j$. The number of possible factorization types of a polynomial of degree k is the number of *partitions* of k, that is, the number of ways of writing k as a sum of positive integers.

Theorem 9 implies that if we know the factorization type of a polynomial f modulo a prime p that divides neither $D(f)$ nor the constant coefficient of f, then we can use the order of the automorphism σ_p of $\mathbb{Z}_p[x]/\langle f\rangle$ to obtain information about the period length of a corresponding recursive sequence modulo p. We show in this section that we can reverse this implication for polynomials f of degree $k \leq 5$, using Theorem 9 together with the following application of the discriminant due to Stickelberger, adapted from [Driver et al. 2005] and [Swan 1962].

Stickelberger's parity theorem. Let f be a monic polynomial of degree k in $\mathbb{Z}[x]$ and let p be a prime number not dividing the discriminant D of f. Suppose that f factors as a product of j distinct irreducible polynomials in $\mathbb{Z}_p[x]$. If p is odd, then $\left(\frac{D}{p}\right) = (-1)^{k-j}$, while if $p = 2$, then $D \equiv 5^{k-j} \pmod 8$.

Before stating our main theorem for this section, we illustrate, with an example, how knowledge of the period of a recursive sequence modulo p can help determine the factorization type of its characteristic polynomial modulo p.

Example. Define a_n for $n \geq 0$ by $(a_0, a_1, a_2, a_3) = (0, 0, 0, 1)$ and $a_n = a_{n-3} + a_{n-4}$ for $n \geq 4$. The characteristic polynomial for $\{a_n\}_{n=0}^{\infty}$ is

$$f(x) = x^4 - x - 1,$$

which can be shown to have discriminant $D = -283$. So f is a product of distinct irreducible polynomials in $\mathbb{Z}_p[x]$ for all primes $p \neq 283$. Suppose that we calculate that modulo $p = 61$, the sequence $\{a_n\}_{n=0}^{\infty}$ has period $\ell = 75660$, which must be the same as the order of ω as a unit in $\mathbb{Z}_{61}[\omega] = \mathbb{Z}_{61}[x]/\langle f\rangle$. We find that ℓ divides neither $p-1$ nor p^2-1, but does divide p^3-1. Theorem 9 implies that $t = 3$ is the least common multiple of the degrees of the irreducible factors of f in $\mathbb{Z}_{61}[x]$, and we conclude that f must have factorization type $[3, 1]$. Modulo $p = 71$, the same sequence has period $\ell = 1008$. This time we find that ℓ does not divide $p-1$, but does divide p^2-1. Now f could have factorization type either $[2, 2]$ or $[2, 1, 1]$. But since $\left(\frac{-283}{71}\right) = 1$, Stickelberger's theorem implies that the number of irreducible factors of f in $\mathbb{Z}_{71}[x]$ has the same parity as $k = 4$, and so f has factorization type $[2, 2]$.

Remark. For computational purposes in this application, we can bypass direct calculation of the period of a recursive sequence. As noted in the example, this period ℓ is the same as the order of ω as a unit in a corresponding ring $\mathbb{Z}_p[\omega]$, so that ℓ divides an integer n precisely when $\omega^n = 1$. Powers of ω can be computed very efficiently by the process of *successive squaring*. If we write n in its binary expansion as

$$n = c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + c_3 \cdot 2^3 + \cdots,$$

where $c_i = 0$ or 1 for all i, with only finitely many nonzero values of c_i, then

$$\omega^n = \omega^{c_0} \cdot (\omega^2)^{c_1} \cdot (\omega^4)^{c_2} \cdot (\omega^8)^{c_3} \cdots .$$

Each power of ω in parentheses is the square of the preceding power of ω, and only those values for which $c_i = 1$ contribute to the product. Squares and other products in

$$\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$$

are easily calculated by multiplying polynomials, replacing products by their remainders on division by f, when necessary.

Our next theorem states that we can determine the factorization type of a polynomial f of degree $k \leq 5$ modulo most primes p (assuming that neither the discriminant nor the constant coefficient of f is identically zero) from knowledge of the discriminant of f and calculation of certain powers of ω in the ring $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$.

Theorem 11. *Let f be a monic polynomial with integer coefficients, having degree $k \leq 5$ and discriminant D. Let p be a prime number that divides neither D nor the constant coefficient of f. Let $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$, and let t be the smallest positive integer such that $\omega^{p^t - 1} = 1$ in $\mathbb{Z}_p[\omega]$. Then the following statements are true about the factorization of f in the ring $\mathbb{Z}_p[x]$.*

(1) *If $t = 1$, then f is a product of k distinct linear polynomials.*

(2) *If $t = 2$, and p is odd and $\left(\frac{D}{p}\right) = 1$, then f is a product of two distinct irreducible quadratic polynomials and $k - 4$ linear polynomials.*

(3) *If $t = 2$, and p is odd and $\left(\frac{D}{p}\right) = -1$, or $p = 2$ and $D \equiv 5 \pmod 8$, then f is a product of an irreducible quadratic polynomial and $k - 2$ distinct linear polynomials.*

(4) *If $t = 3$, then f is a product of an irreducible cubic polynomial and $k - 3$ distinct linear polynomials.*

(5) *If $t = 4$, then f is a product of an irreducible quartic polynomial and $k - 4$ linear polynomials.*

(6) *If $t = 5$, then f is an irreducible quintic polynomial.*

(7) *If $t = 6$, then f is a product of an irreducible cubic polynomial and an irreducible quadratic polynomial.*

Remark. As defined, the integer t is the same as the order of the automorphism σ_p in $\mathrm{Aut}(\mathbb{Z}_p[\omega])$, so must exist. It is understood that not all of the cases listed above can occur for every value of $k \leq 5$, nor for every prime p. For example, case (2) is impossible when $p = 2$, since there are not two distinct irreducible quadratic polynomials in $\mathbb{Z}_2[x]$.

Proof. The table lists the seven partitions $[k_1, k_2, \ldots, k_j]$ of $k = 5$.

$[k_1, k_2, \ldots, k_j]$	$(-1)^{k-j}$	$t = \operatorname{lcm}(k_1, k_2, \ldots, k_j)$
[1, 1, 1, 1, 1]	1	1
[2, 1, 1, 1]	−1	2
[3, 1, 1]	1	3
[2, 2, 1]	1	2
[4, 1]	−1	4
[3, 2]	−1	6
[5]	1	5

In the second column of the table, we note the parity of $k - j$ by listing $(-1)^{k-j}$, and in the third column, we list the least common multiple of the summands of the partition, which we label as t. Theorem 9 implies that if a polynomial f of degree five has factorization type $[k_1, k_2, \ldots, k_j]$, then t is the smallest positive integer for which $\omega^{p^t-1} = 1$ in $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$, as in the statement of Theorem 11. The table shows that $t \le 6$, and that if $t \ne 2$, the factorization type of f is determined by the value of t. If $t = 2$, the factorization type of f is determined by t together with the value of $\left(\frac{D}{p}\right) = (-1)^{k-j}$ or $D \equiv 5^{k-j} \pmod 8$.

Removal of a term of 1, from those partitions containing 1, affects neither $(-1)^{k-j}$ nor t. (If a 1 is removed, both k and j are decreased by one, so that the value of $k - j$ is unchanged.) So the first five rows of the table lead to the same conclusion about polynomials of degree four; the first three rows imply the same about polynomials of degree three; and so forth. □

We now state three corollaries of Theorem 11, which can be viewed as algorithms for determining the factorization types of cubic, quartic, and quintic polynomials modulo prime values. Here we take better advantage of the Legendre symbol $\left(\frac{D}{p}\right)$, which is easy to calculate for a given D and odd prime p, as a first test to distinguish between factorization types. We omit the proofs, which follow the same arguments from the table exhibited in the proof of Theorem 11.

Corollary 12. *Let f be a monic polynomial of degree three with discriminant D, let p be a prime number that divides neither D nor the constant coefficient of f, and let $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f \rangle$.*

- *If p is odd and $\left(\frac{D}{p}\right) = 1$ or $p = 2$ and $p \equiv 1 \pmod 8$, then:*

(1) *If $\omega^{p-1} = 1$, then f has factorization type* [1, 1, 1].

(2) *If $\omega^{p-1} \ne 1$, then f has factorization type* [3].

- *If p is odd and $\left(\frac{D}{p}\right) = -1$ or $p = 2$ and $p \equiv 5 \pmod 8$, then:*

(3) *f has factorization type* [2, 1].

Corollary 13. *Let f be a monic polynomial of degree four with discriminant D, let p be a prime number that divides neither D nor the constant coefficient of f, and let $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f\rangle$.*

- *If p is odd and $\left(\frac{D}{p}\right) = 1$ or $p = 2$ and $p \equiv 1 \pmod 8$, then*:

(1) *If $\omega^{p-1} = 1$, then f has factorization type* $[1, 1, 1, 1]$.

(2) *If $\omega^{p-1} \neq 1$, but $\omega^{p^2-1} = 1$, then f has factorization type* $[2, 2]$.

(3) *If $\omega^{p^2-1} \neq 1$, then f has factorization type* $[3, 1]$.

- *If p is odd and $\left(\frac{D}{p}\right) = -1$ or $p = 2$ and $p \equiv 5 \pmod 8$, then*:

(4) *If $\omega^{p^2-1} = 1$, then f has factorization type* $[2, 1, 1]$.

(5) *If $\omega^{p^2-1} \neq 1$, then f has factorization type* $[4]$.

Corollary 14. *Let f be a monic polynomial of degree five with discriminant D, let p be a prime number that divides neither D nor the constant coefficient of f, and let $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f\rangle$.*

- *If p is odd and $\left(\frac{D}{p}\right) = 1$ or $p = 2$ and $p \equiv 1 \pmod 8$, then*:

(1) *If $\omega^{p-1} = 1$, then f has factorization type* $[1, 1, 1, 1, 1]$.

(2) *If $\omega^{p-1} \neq 1$, but $\omega^{p^2-1} = 1$, then f has factorization type* $[2, 2, 1]$.

(3) *If $\omega^{p^2-1} \neq 1$, but $\omega^{p^3-1} = 1$, then f has factorization type* $[3, 1, 1]$.

(4) *If $\omega^{p^2-1} \neq 1$ and $\omega^{p^3-1} \neq 1$, then f has factorization type* $[5]$.

- *If p is odd and $\left(\frac{D}{p}\right) = -1$ or $p = 2$ and $p \equiv 5 \pmod 8$, then*:

(5) *If $\omega^{p^2-1} = 1$, then f has factorization type* $[2, 1, 1, 1]$.

(6) *If $\omega^{p^2-1} \neq 1$, but $\omega^{p^4-1} = 1$, then f has factorization type* $[4, 1]$.

(7) *If $\omega^{p^4-1} \neq 1$, then f has factorization type* $[3, 2]$.

Remark. If t is the order of σ_p in the group of automorphisms of $\mathbb{Z}_p[\omega]$, then $\omega^{p^s-1} = 1$ if and only if t divides s. For example, in case (7) of Corollary 14, if $\omega^{p^4-1} \neq 1$, we are also claiming that $\omega^{p^2-1} \neq 1$.

Remark. As an example to illustrate the efficiency of these algorithms, a computer program written by the first author, based on Corollary 13, found the factorization type of $f(x) = x^4 - x - 1$ modulo all primes $p < 10000$ ($p \neq 283$) in approximately two seconds. On the same computer, a program to factor f in $\mathbb{Z}_p[x]$ for the same primes p, using brute force calculations, required four hours and 42 minutes to run. (The second program confirmed all of the results predicted by the first program.)

Polynomials of degree $k > 5$ cannot be distinguished from each other, in every case, by the same data. For example, if a polynomial f of degree six satisfies

$$\left(\frac{D(f)}{p}\right) = -1 \quad \text{and} \quad (\omega_f)^{p-1} \neq 1 \quad \text{but} \quad (\omega_f)^{p^2-1} = 1,$$

then f could have factorization type either $[2, 2, 2]$ or $[2, 1, 1, 1, 1]$. We conclude, however, with some results that hold for any value of k.

Theorem 15. *Let f be a monic polynomial of degree k with discriminant D, let p be a prime number that divides neither D nor the constant coefficient of f, and let $\mathbb{Z}_p[\omega] = \mathbb{Z}_p[x]/\langle f\rangle$.*

(1) *If $\omega^{p-1} = 1$, then f is a product of k linear factors in $\mathbb{Z}_p[x]$.*

(2) *If $\omega^{p^2-1} = 1$, then all irreducible factors of f in $\mathbb{Z}_p[x]$ have degree one or two. The number of irreducible quadratic factors of f is even if and only if p is odd and $\left(\frac{D}{p}\right) = 1$ or $p = 2$ and $D \equiv 1 \pmod 8$.*

(3) *If $\omega^{p^q-1} = 1$ for some odd prime q, then all irreducible factors of f in $\mathbb{Z}_p[x]$ have degree one or q. This case can occur only when p is odd and $\left(\frac{D}{p}\right) = 1$ or $p = 2$ and $D \equiv 1 \pmod 8$.*

Proof. Let the factorization type of f modulo p be $[k_1, k_2, \ldots, k_j]$, and let $t = \operatorname{lcm}(k_1, k_2, \ldots, k_j)$. If $\omega^{p-1} = 1$, then $t = 1$, which is possible only when $k_i = 1$ for $1 \le i \le j$, so that $j = k$. If $\omega^{p^q-1} = 1$ for some prime q, then t divides q. This is possible only when there is some $0 \le \ell \le j$ so that $k_i = q$ for $i \le \ell$ and $k_i = 1$ for $\ell < i \le j$. (We allow the possibility that $\ell = 0$, so that $t = 1$.) In this case, notice that $k = \ell \cdot q + (j - \ell)$, so that $k - j = \ell(q - 1)$. If $q = 2$, then $k - j$ has the same parity as ℓ. If q is odd, then $k - j$ is even in every case. □

Acknowledgement

The authors thank the Jepson Summer Science Institute at the University of Mary Washington for its financial support during the research project that led to this article.

References

[Adams 1984] W. W. Adams, "Splitting of quartic polynomials", *Math. Comp.* **43**:167 (1984), 329–343. MR 85f:12005 Zbl 0551.12017

[Driver et al. 2005] E. Driver, P. A. Leonard, and K. S. Williams, "Irreducible quartic polynomials with factorizations modulo p", *Amer. Math. Monthly* **112**:10 (2005), 876–890. MR 2006f:11027

[Dummit and Foote 2004] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., Wiley, Hoboken, NJ, 2004. MR 2007h:00003 Zbl 1037.00003

[Edwards 1984] H. M. Edwards, *Galois theory*, Graduate Texts in Mathematics **101**, Springer, New York, 1984. MR 87i:12002 Zbl 0532.12001

[Engstrom 1931] H. T. Engstrom, "On sequences defined by linear recurrence relations", *Trans. Amer. Math. Soc.* **33**:1 (1931), 210–218. MR 1501585 Zbl 0001.14002

[Fillmore and Marx 1968] J. P. Fillmore and M. L. Marx, "Linear recursive sequences", *SIAM Rev.* **10** (1968), 342–353. MR 38 #1936 Zbl 0169.51004

[Hardy and Wright 1979] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford University Press, New York, 1979. MR 81i:10002 Zbl 0423.10001

[Lidl and Niederreiter 1983] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications **20**, Addison-Wesley, Reading, MA, 1983. MR 86c:11106 Zbl 0554.12010

[Skolem 1952] T. Skolem, "The general congruence of the 4th degree modulo p, p prime", *Norsk Mat. Tidsskr.* **34** (1952), 73–80. MR 14,353e Zbl 0048.02905

[Sun 2003] Z.-H. Sun, "Cubic and quartic congruences modulo a prime", *J. Number Theory* **102**:1 (2003), 41–89. MR 2004e:11004 Zbl 1033.11003

[Sun 2006] Z.-H. Sun, "A criterion for polynomials to be congruent to the product of linear polynomials $\pmod p$", *Fibonacci Quart.* **44**:4 (2006), 326–329. MR 2008c:11005 Zbl 1160.11302

[Sun and Sun 1992] Z. H. Sun and Z. W. Sun, "Fibonacci numbers and Fermat's last theorem", *Acta Arith.* **60**:4 (1992), 371–388. MR 93e:11025 Zbl 0725.11009

[Swan 1962] R. G. Swan, "Factorization of polynomials over finite fields", *Pacific J. Math.* **12** (1962), 1099–1106. MR 26 #2432 Zbl 0113.01701

[Wall 1960] D. D. Wall, "Fibonacci series modulo m", *Amer. Math. Monthly* **67** (1960), 525–532. MR 22 #10945 Zbl 0101.03201

[Ward 1933] M. Ward, "The arithmetical theory of linear recurring series", *Trans. Amer. Math. Soc.* **35**:3 (1933), 600–628. MR 1501705 Zbl 0007.24901

Received: 2007-10-29 Accepted: 2010-01-26

llehman@umw.edu *University of Mary Washington, Department of Mathematics, 1301 College Avenue, Fredericksburg, VA 22401, United States*

ctriola@mw.edu *9 Seneca Terrace, Fredericksburg, VA 22401, United States*

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2010 is US $100/year for the electronic version, and $120/year (+$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2010 vol. 3 no. 2