Period of a linear recurrence

by

A. Vinco (Ann Arbor, Mich.)

1. Introduction. There is a long history of research involving the period of repeating sequences of integers. The period of decimal fractions was the subject of early investigation by Leibnitz and Gaus. The period modulo \( \alpha \) of sequence \( \{a^0, a^1, \ldots\} \) is important in the context of Lehmer's frequently utilized congruential method for computer generation of pseudo-random numbers ([2], [4]). Lucas was a major figure among many investigators into divisibility properties of the Fibonacci and other second order recurrences — and these properties are related to the period of such sequences modulo \( \alpha \) ([5]).

In this article we investigate the period of repetition in a general setting. We first note that the repeating sequences mentioned above fall within the following framework: Let \( \mathbb{Z} \) be an algebraic number field and \( A \) its ring of integers. Let \( T \) be an \( N \times N \) matrix and \( X_0 \) an \( N \)-column vector, both with entries in \( A \). Define the sequence \( X_0, X_1, \ldots \) by the linear recurrence

\[ X_{n+1} = TX_n, \quad n = 0, 1, 2, \ldots \]

Let \( \alpha \) be an ideal in \( A \). Since \( A/\alpha \) is finite, the sequence must, after a perhaps erratic initial segment, repeat periodically modulo \( \alpha \). Define \( \varphi = \varphi(T, X_0, A/\alpha) \) to be this period. That is, \( \varphi \) is the least positive integer for which there is an \( m_\alpha \) giving \( X_{n+m_\alpha} = X_n \) for all \( n \geq m_\alpha \). Equality here means coordinatewise equality in the ring \( A/\alpha \). As an example, consider

\[
T = \begin{bmatrix}
0 & 1 & \cdots & 0 \\
0 & 0 & \cdots & 0 \\
a_0 & a_1 & \cdots & a_{N-1} \\
0 & 0 & \cdots & 1
\end{bmatrix}, \quad X_0 = \begin{bmatrix}
a_0 \\
\vdots \\
a_N
\end{bmatrix}
\]

(1.1)

Then \( \varphi(T, X_0, A/\alpha) \) is the period (mod \( \alpha \)) of the general \( N \)-th order linear recurrence defined by

\[ a_m = a_1a_{m-1} + a_2a_{m-2} + \ldots + a_{N}a_{m-N} \]

\( T \) is often referred to as the companion matrix of this recurrence.
By looking at the remainders upon division, it is easy to verify that the period of the decimal representation of \( 1/p \) for \( p \) prime is \( \sigma(10^n) \). (1) \( Z/pZ \). When \( p \) is not 2 or 5, this is just the multiplicative order of the element 10 in the field \( Z/pZ \) of residues mod \( p \). The general situation for a prime ideal \( p \) is analogous. By our Theorem 1, \( \nu(T, X_0, A/p) \) is essentially determined by the multiplicative orders of special elements in a finite extension field of the residue class field \( A/p \). This will enable us to make some new estimates of the value of \( v \) and to unify known results, many otherwise proved by complicated recurrence identities.

In Section 2 the problem of determining \( v \) is reduced to the case where \( a \) is a prime ideal and Section 3 deals with a prime. In Section 4 these results are applied to certain second and third order recurrences.

2. Preliminary results. The sequence \( \{X_m\} \) is called simply periodic if \( X_m = X_0 \), i.e. \( X_m \) is the first term to repeat. In this case it is apparent that \( X_m = X_0 \) if and only if \( m \) is a multiple of \( v \).

Lemma 1. If \( \det T \) is not a zero divisor of \( A/p \) then \( \{X_m\} \) is simply periodic.

Proof. For some integer \( m \), \( T^m X_0 = X = X_0 \). When \( \det T = 0 \) this implies that \( X_{m+1} = X_0 \).

The next lemma reduces the problem of determining \( \nu(a) = \nu(T, X_0, A/p) \) to the case where \( a \) is a power of a prime ideal.

Lemma 2. Let \( a = p_1^e_1 \cdot p_2^e_2 \cdots p_s^e_s \) be the factorization of \( a \) into prime ideals. Then

\[
\nu(a) = \text{LCM} [\nu(p_1^{e_1}), \nu(p_2^{e_2}), \ldots, \nu(p_s^{e_s})].
\]

Proof. The proof is immediate since, for any column vectors \( X \) and \( Y \), we have \( X = X (\text{mod } a) \) if and only if \( X = X (\text{mod } p_i^{e_i}) \) for all \( i \).

In considering a power of a prime \( a = p^e \), regard \( T \) as a linear transformation on \( K^n \), the vector space of \( N \)-tuples of elements of the number field \( K \). Suppose that the minimal polynomial \( F(x) \) of \( T \) is irreducible over \( K \). Let \( L \) be the splitting field of \( F(x) \) over \( K \) and let \( C \) be the integral closure of \( A \) in \( L \). Now regard \( T \) as a linear transformation on \( L^n \). Since the roots of the minimal polynomial are distinct, there is a diagonal matrix \( D \) and an invertible matrix \( H \) such that \( D = HTH^{-1} \). It is easily seen that the entries of \( H \) can be chosen to lie in \( C \); we do so. Let \( x_0 \) denote any coordinate of \( HX_0 \) and let \( NX_0 \) be the norm of \( x_0 \) considered as an element of \( L/K \). A short matrix calculation suffices to show that the coordinates of \( HX_0 \) are conjugate and therefore \( NX_0 \) is independent of the choice of \( x_0 \). Finally let \( p \) be the rational prime over which \( p \) lies, i.e. the characteristic of \( A/p \), and let \( e \) be the ramification index of \( p \) over \( p \). Let \( s \) denote the greatest positive integer such that \( \nu(p^s) = \nu(p) \).

Lemma 3. If \( (1) \) the minimal polynomial for \( T \) is irreducible over \( K \), (2) neither \( NX_0 \) nor \( \det T \) is divisible by \( p \), (3) \( \det H \) is not divisible by \( p \), (4) \( e > 1 \), then \( \nu(p^s) = p^{sM} \nu(p) \) where \( M \) is the least non-negative integer greater than or equal to \( (r - 1)e \).

It is not always true that \( s = 1 \). Take, for example,

\[
T = \begin{bmatrix} 0 & 1 \\ 1 & 5 \end{bmatrix}, \quad X_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{and} \quad p = (3).
\]

The assumptions of Lemma 3 are satisfied yet \( \nu(Z/27Z) = \nu(Z/9Z) = \nu(Z/3Z) = 8 \). Though the hypotheses of the lemma are numerous, note that (2) and (3) can fail for at most a finite number of primes.

Proof of Lemma 3. Consider \( \{X_m\} \) as a sequence in \( A/p^n \). To avoid confusion let \( = (\text{mod } p^n) \) signify equality in the ring \( A/p^n \) and \( = (\text{mod } p^M C) \) is equality in the ring \( C/p^n C \). Since \( \det T \) is assumed not divisible by \( p \), \( \{X_m\} \) is simply periodic by Lemma 1. Hence there is a positive integer \( m \) such that \( T^m = I (\text{mod } p^n) \); let \( |T| \) denote the least such integer. We first show that \( \nu(T, X_0, A/p^n) = |T| \). One direction is easy:

\[
T^m = I (\text{mod } p^n) = X = X_0 = T^m X_0 = HX_0 = HX_0 = D^m I = (\text{mod } p^n C).
\]

Conversely assume that \( X_m = X_0 (\text{mod } p^n) \). Then we have the following implications:

\[
T^m X_0 = X_0 \Rightarrow D^m H X_0 = H T^m X_0 = H X_0 = D^m I = (\text{mod } p^n C).
\]

The last implication is due to the fact that \( NX_0 \) not divisible by \( p \) implies that each coordinate of \( HX_0 \) is relatively prime to \( p^n \). Furthermore

\[
D^m = I = H T^m = D^m H = H = H (T^m - I) = 0 (\text{mod } p^n C).
\]

Letting \( \tilde{H} \) be the matrix such that \( \tilde{H} H = (\text{det } H) I \) we have \( (\text{det } H) (T^m - I) = H (T^m - I) = 0 (\text{mod } p^n C) \). Because \( \text{det } H \) is not divisible by \( p \), \( T^m \) is \( (\text{mod } p^n C) \).

Let \( \nu \) be the function such that \( \nu(T, X_0, A/p) \). By the hypotheses of the lemma \( T^m = I + p^n U \) where not all entries in the matrix \( U \) are divisible by \( p \). A simple calculation using the binomial expansion then substantiates that \( (I + p^n U)^{p^M} = I (\text{mod } p^n) \) and \( M \) is the least integer for which this is true. That \( \nu(p) \) | \( \nu(p^n) \) | \( \nu(p^n) (p^{M-1} v(p)) \) and \( \nu(p^n) (p^{M-1} v(p)) \) imply that \( \nu(p^s) = p^{sM} \nu(p) \).

3. The period modulo a prime. In this section we are interested in determining \( \nu(T, X_0, A/p) \) when \( p \) is a prime ideal in \( A \). Let \( \tilde{A} = A/p \) and now let \( F(x) \) be the minimal polynomial for \( T \) considered as a linear transformation on \( K^n \). Then we can write

\[
F = (F_1^p) (F_2^p) \cdots (F_r^p)
\]

where each \( F_i \) is irreducible over \( \tilde{A} \). The value of \( \nu \) is highly dependent.
on this factorization. In order to concisely state the results, we introduce some notation. Within some algebraically closed field containing \(\mathbb{F}\) let \(a_i\) be any root of \(F(x)\) and let \(\text{ord}(a_i)\) denote the multiplicative order of \(a_i\) in the extension field \(\mathbb{K}(a_i)\). For any integer \(h \geq 0\) let \(H_i(x, h) = F(a_i)/F_i(x)^{n-h}\). Then define \(h_i\) to be the least integer \(h\) for which \(H_i(x, h)\) is zero. Finally if \(h_i > 0\) let \(v_i\) be the unique integer such that \(p^{v_i} \geq h_i > p^{v_i-1}\). Here \(p\) is the characteristic of the field \(\mathbb{K}\). Intuitively, the \(h_i\) measure certain "cancellations" due to the initial vector \(X_0\). The maximum possible value of \(v(T, X_0, A/\mathbb{p})\) is the order of the matrix \(T\). Loosely speaking, the smaller the values of the \(h_i\), the greater the variation of \(v(T, X_0, A/\mathbb{p})\) from this maximum. Theorem 1 and its corollaries will make these notions more precise. The proofs follow the statements of the theorem and corollaries.

**Theorem 1.** With notation as above,

\[
v(T, X_0, A/\mathbb{p}) = \text{LCM}[v_i] \quad \text{where} \quad v_i = \begin{cases} 1 & \text{if } a_i = 0 \text{ or } h_i = 0, \\ p^{\text{ord}(a_i)} & \text{otherwise}. \end{cases}
\]

When \(F(x)\) is irreducible we have the immediate simplification.

**Corollary 1.** If \(\det T \neq 0\), \(X_0 \neq 0\) and the minimal polynomial \(F(x)\) is irreducible over \(\mathbb{K}\), then \(v(T, X_0, A/\mathbb{p}) = \text{ord}(a_i)\) where \(a_i\) is any root of \(F(x)\).

In the case where \(T\) is the companion matrix of a linear recurrence we can define a norm map: \(\mathbb{N} : \mathbb{K}^n \rightarrow \mathbb{K}\). The norm \(\mathbb{N}X_0\) of the initial vector \(X_0\) is significant in assessing the effect of \(X_0\) on the period of the sequence \(\{X_n\}\) (mod \(\mathbb{p}\)). To define this norm let \(L_i/\mathbb{K}\) be the splitting field of \(F'(x)\); let \(a_1, a_2, \ldots, a_N\) be all the roots of \(F'(x)\) in \(L_i\); and let \(G_i(x) = F'(x)/(x - a_i)\). Now consider \(T\) as a linear transformation on \(\mathbb{L}^n\). For a matrix of the form (1.1), \(G_i(T)\) is a transformation of rank 1. So there is, for each \(i\), a fixed vector \(Y_i\) and a linear functional \(g_i\) on \(\mathbb{L}^n\) such that \(G_i(T)X = g_i(X)Y_i\). If we express \(X\) as an \(N\)-tuple \(X = (x_1, x_2, \ldots, x_N)\) then the \(g_i\) may be written in the form \(g_i(X) = \sum_{j=1}^{N} c_j a_j\) where the \(c_j\) are constants in \(\mathbb{L}\). Now \(\prod_{i=1}^{N} g_i(X)\) is a homogeneous polynomial in the variables \(a_1, a_2, \ldots, a_N\) and is well defined up to a non-zero multiplicative constant in \(\mathbb{L}\). It is possible to choose this multiplicative constant so that the coefficients of this homogeneous polynomial lie in \(\mathbb{K}\). Letting \(g(X)\) be this form with coefficients in \(\mathbb{K}\) (well defined up to a non-zero constant in \(\mathbb{K}\)) define the norm as a mapping \(\mathbb{N} : \mathbb{K}^n \rightarrow \mathbb{K}\) given by \(X \rightarrow g(X)\). In practice, the norm is easily calculated. For example, consider

\[
T = \begin{bmatrix} 0 & 1 \\ a & b \end{bmatrix},
\]

the companion matrix of the second order recurrence \(a_n = ba_{n-1} + a_{n-2}\) over the integers. For \(X = (a, b)\) a short computation yields

\[
N = (y - a_2)(y - a_1) = y^2 - ax_1 - bx_0.
\]

The next corollary states a sufficient condition for \(v\) to take its maximum possible value.

**Corollary 2.** If \(\det T \neq 0\) and \(\mathbb{N}X_0 \neq 0\), then

\[
v(T, X_0, A/\mathbb{p}) = p^{\text{LCM}[\text{ord}(a_i)]}
\]

where \(a_i\) is the unique integer such that \(p^{v_i} \geq \text{max}_i v_i > p^{v_i-1}\).

The two corollaries give estimates of \(v\). Since \(\mathbb{K}\) is a finite field, its order is a power of \(p\); say \(|\mathbb{K}| = q\). Let \(f_i\) be the degree of the polynomial \(F_i\) in the factorization of the minimal polynomial \(F\), and let \(b_i\) be the constant term of \(F_i\). Let \(\rho_i\) denote the multiplicative order of \(b_i(\mathbb{K})/|\mathbb{K}|\). Then

\[
\text{Proof of Theorem 1.} \quad \text{In } \mathbb{L}\text{ the polynomial } F(x) \text{ can be factored as } F(x) = \prod_{i=1}^{N} (x - a_i) \quad \text{where the } a_i \text{ are distinct. If } V_i \text{ denotes the kernel of } (T - a_i)^{\rho_i} \text{ then } \mathbb{L} = V_i \oplus V_i \oplus \cdots \oplus V_i \text{ and } T \text{ is the direct sum of the transformations } T_i \text{ induced by } T \text{ restricted to the subspace } V_i. \text{ Let } X_i^t \text{ be the projection of } X_0 \text{ on the subspace } V_i. \text{ It is then apparent that}
\]

\[
(3.1) \quad v(T, X_0, \mathbb{K}) = \text{LCM}[v(T, X_i^t, \mathbb{L})].
\]

In order to determine \(v(T, X_i^t, \mathbb{L})\) let \(w_i\) be the least integer such that \((T - a_i)^{\rho_i} X_i^t = 0\) but \((T - a_i)^{\rho_i+1} X_i^t \neq 0. \text{ If } w_i = 0 \text{ or } a_i = 0, \text{ then trivially } v(T, X_i^t, \mathbb{L}) = 1. \text{ Otherwise } a_i \neq 0 \text{ implies that } T_i \text{ is invertible on } V_i \text{ and hence } v(T, X_i^t, \mathbb{L}) \text{ is the least integer } m \text{ such that } T^m X_i^t = X_i^t. \text{ To simplify the notation we drop the subscripts and let } a \text{ be any of the } a_i \text{ and let } V, w, n \text{ and } X \text{ be the corresponding } V_i, w_i, n_i \text{ and } X_i^t. \text{ Then the condition on } m \text{ stated above is equivalent to}
\]

\[
(a^{m-1}) X + \left(\frac{m}{1}\right) a^{m-1} (T - a) X + \cdots + \left(\frac{m}{w-1}\right) a^{m-1} (T - a)^{w-1} X = 0.
\]

A short induction using this equation suffices to show that the following conditions must be satisfied:

\[
a^{m-1} = 1,
\]

\[
\left(\frac{m}{1}\right) = \left(\frac{m}{2}\right) = \cdots = \left(\frac{m}{w-1}\right) = 0 \mod p
\]
where \( p \) is the characteristic of \( K \). For the validity of the set of congruences it is necessary and sufficient that \( p^t \mid m \) where \( t \) is the unique integer such that \( p^t \gg w \gg p^{t-1} \). Rescaling equation (3.1) we have \( v(T, X_0, K) = \text{LCM}(v_t) \) where

\[
  v_t = \begin{cases} 
    1 & \text{if } a_i = 0 \text{ or } a_t = 0, \\
    p^t \text{ord}(a_t) & \text{otherwise}
  \end{cases}
\]

and \( t \) is the unique integer such that \( p^t \gg w \gg p^{t-1} \). To complete the proof we have only to show that if \( a_i \) and \( a_t \) are roots of the same factor \( f(x) \) of \( F(x) \), irreducible over \( K \), then (1) \( \text{ord}(a_i) = \text{ord}(a_t) \) and (2) \( v_i = v_t = h \) where we recall that \( h \) is the least integer for which \( H(T, K) X_0 = 0 \) where \( H(a, h) = F(a)/(f(a))^s \). These facts follow easily from the existence of an isomorphism of \( K(a_i) \) onto \( K(a_t) \) taking \( a_i \) to \( a_t \) and leaving the elements of \( K \) fixed. We omit the details.

**Proof of Corollary 2.** Det \( T \neq 0 \) insures that \( a_t \neq 0 \) for all \( t \). Now assume that \( X_0 = 0 \). Using the notation \( G(T) \) with the same meaning as in the definition of the norm, we have \( G(T) X_0 = 0 \) for all \( t \). As in the proof of the theorem, this implies \( H(T, a_t - 1) = 0 \), which is equivalent to \( h_t = a_t \). The result now follows from Theorem 1.

**Proof of Corollary 3.** The norm \( N \) of an element \( \gamma \) of \( K(a_t) \) is defined as the product of the conjugates of \( \gamma \). Then \( N : K(a_t)^* \rightarrow K^* \) is a surjective homeomorphism of the multiplicative subgroup of \( K(a_t) \) onto the multiplicative subgroup of \( K \). Let \( U_t \) be the kernel of this homeomorphism; then \( [U_t] = (g^t - 1)/(g - 1) \). Since \( N(a_t) = (-1)^t b_{1t} \), we have \( a_t^t \in U_t \). Therefore \( \text{ord}(a_t) = [v_t(g^t - 1)/(g - 1)] \). The corollary then follows from Theorem 1.

**Proof of Corollary 4.** The group \( K(a_t)^* \) of invertible elements of \( K(a_t) \) is cyclic; let \( g \) be a generator. Then \( g^{t+1} \) is a generator of \( U_t \), the kernel of the norm map \( N : K(a_t)^* \rightarrow K^* \). Let \( m \) be the exponent such that \( a_t = g^m \). By definition \( g^{m+t} = a_t^t \in U_t \). Therefore we have the congruence \( m r_t = j (g - 1) (g^t - 1) \) for some integer \( j \). So there must exist an integer \( J \) such that \( m = J (g - 1)/r_t \). In this we claim that \( (J, r_t) = 1 \). Otherwise we would have

\[
  a_t^{(J, r_t)} = g^{J (g - 1)/r_t} = g^{(g - 1)(g - 1)/r_t} \in U_t
\]

which contradicts the fact that \( r_t \) is the order of \( N(a_t) \). By Theorem 1 we have \( 1 = a_t = g^m = g^{(g - 1)/r_t} \), which implies that \( g^{(g - 1)/r_t} \mid J (g - 1)/r_t \). This in turn implies that \( r_t^{(g - 1)/r_t} \mid J (g - 1)/r_t \). Therefore \( v_t^{(g - 1)/r_t} \) and Corollary 4 follows.

**4. Examples.** To illustrate the theory let

\[
  T = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad X_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}
\]

and let \( n \) be a positive integer. Consider \( v(n) = v(T, X_0, Z/nZ) \). We choose this as our first example because \( v(n) \) is the period of the Fibonacci sequence \( (x_{n+1} = ax_n + x_{n-1}) \) with \( x_0 = 0 \) and \( x_1 = 1 \), and there is an extensive literature on this subject [11, 3, 8, 9]. The following theorem is a direct consequence of Lemmas 2 and 3 and Corollaries 3 and 4. The usual proof is based on lengthy Fibonacci identities.

**Theorem 2.** (i) If \( n = p_1^{t_1} p_2^{t_2} \ldots p_t^{t_t} \) then

\[
  v(n) = \text{LCM}(v(p_1^{t_1}), \ldots, v(p_t^{t_t})).
\]

(ii) If \( s \) is the greatest integer \( s \leq r \) such that \( v(p^n) = v(p) \), then

\[
  v(p^n) = p^{s-1} v(p)
\]

for any prime \( p \).

(iii) If \( p = \pm 3 \mod 10 \) then \( v(p)|2^{(p+1)} \) and \( v(p)|p+1 \). If \( p = \pm 1 \mod 10 \) then \( v(p)|p-1 \) and \( v(p)|2p \).

In part (iii) it is often, but not always, true that \( v(p) = 2^{(p+1)} \) or \( v(p) = p+1 \). For example \( v(47) = 32 \) and \( v(101) = 50 \). In Section 2 we gave an example of a matrix for which \( v(p^n) = v(p) \). For the Fibonacci matrix, however, it has been an unsolved conjecture for at least 18 years [8] that \( v(p^n) = v(p) \). This would imply that always \( s = 1 \) in part (ii). Penny and Pommance [6] have verified it by computer for all \( p < 177469 \). By the methods of this paper, the conjecture is equivalent to \( a^{2p-1} \equiv 1 \mod p \) for some integer \( j \) where \( B \) is the set of algebraic integers in \( Q(\sqrt{5}) \) and \( a = (1 + \sqrt{5})/2 \). A similar congruence \( 2^{p-1} \equiv 1 \mod p \) has been studied extensively. The first counterexample is \( p = 1093 \). The analogy between the two congruences makes the existence of a large counterexample to \( v(p^n) = v(p) \) seem likely. Finally we note that for arbitrary initial vector \( Y_0 \) we do not necessarily have \( v(Y_0) = v(1) \). For example \( v(3) = 5 \) while

\[
  v(1) = 10. \quad \text{However, it can be shown via Theorem 1 that either } v(Y_0) = v(0) \text{ or } v(Y_0) = v(0)/5.
\]

As a second example consider the sequence of integers \( a_1, a_2, \ldots \) defined by the integral second order recurrence

\[
  x_{n+1} = ax_n + bx_{n-1}, \quad x_0 = 0; \quad x_1 = 1.
\]

Historically more attention has been focused on the rank than on the period. The rank \( \mu(n) \) of an integer \( n \) is defined as the least positive integer \( m \) such that \( n \) divides \( a_m \). We will assume that the recurrence is non-degenerate, i.e. \( a, b \neq 0 \mod n \). Then for a prime \( p \)

\[
  \mu(p) = v(\delta, X_0, Z/pZ) \quad \text{where } \delta = \begin{bmatrix} 0 & 1 \\ -1 & -2 + a/b \end{bmatrix} \text{ and } X_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.
\]
(We leave the proof to the reader.) The following theorem has occurred in the literature in various forms. It is a special case of our Corollary 3. Here \( \left( \frac{a}{p} \right) \) denotes the Legendre symbol.

**Theorem 3.** Let \( p \) be an odd prime. If \( a^2 + 4b = 0 \pmod{p} \) then \( \mu(p) = p \). If \( a^2 + 4b \neq 0 \pmod{p} \) then

\[
\mu(p)|p-1 \quad \text{when} \quad \left( \frac{a^2 + 4b}{p} \right) = 1
\]

and

\[
\mu(p)|p+1 \quad \text{when} \quad \left( \frac{a^2 + 4b}{p} \right) = -1.
\]

As a final example consider the recurrence \( x_m = x_{m-1} + x_{m-2} + x_{m-3} \) with the initial values \( x_0 = x_1 = 0 \) and \( x_2 = 1 \). This is a likely third order generalization of the Fibonacci sequence. The companion matrix is

\[
U = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
1 & 1 & 1
\end{bmatrix}
\quad \text{and} \quad
X_0 = \begin{bmatrix}
0 \\
0 \\
1
\end{bmatrix}.
\]

The minimal polynomial for \( U \) over \( \mathbb{Z}/p\mathbb{Z} \) for any prime \( p \) is \( F(x) = x^3 - 2x - x - 1 \). Modulo Lemmas 2 and 3, the determination of \( v(U, X_0, \mathbb{Z}/n\mathbb{Z}) \) is reduced to the case of \( n \) prime. The Newton formulas can be used to calculate the discriminant of \( F(x) \): \( d(F) = -44 \). Hence the only primes for which \( F(x) \) has a multiple root are 2 and 11. For all other primes we apply a long known criteria for the factorability of cubics mod \( p \) and Corollary 3 to derive the following theorem. \( v(p) \) means \( v(U, X_0, \mathbb{Z}/p\mathbb{Z}) \).

**Theorem 4.** Assume that \( p \) is a prime other than 2 or 11.

\[
\text{If } \left( \frac{p}{11} \right) = 1 \text{ then } v(p)|p^2 - 1 \text{ if } F(x) \text{ is irreducible mod } p,
\]

\[
v(p)|p+1 \text{ otherwise.}
\]

\[
\text{If } \left( \frac{p}{11} \right) = -1 \text{ then } v(p)|p^2 - 1.
\]

**References**
