SECOND-ORDER LINEAR DIVISIBILITY SEQUENCES

DEVIN LI

Abstract. A divisibility sequence is an integer sequence $(a_n)_{n\geq 1}$ such that $m \mid n$ implies $a_m \mid a_n$. We study divisibility sequences that also satisfy a second-order linear recurrence with integer coefficients, with an emphasis on the Lucas sequences $U_n(P,Q)$ and $V_n(P,Q)$. After developing basic matrix and addition identities, we prove divisibility and strong divisibility results for $U_n(P,Q)$ under standard coprimality assumptions, and we discuss when divisibility of terms forces divisibility of indices. We then study the recurrence modulo primes, including periodicity from the start, ranks of apparition, and the law of apparition. Next we explain primitive prime divisors and Zsigmondy-type theorems, including results of Carmichael and the Bilu–Hanrot–Voutier theorem. Finally, we discuss p-adic valuations of U_n and give combinatorial models (tilings, matchings, and state graphs) that model these recurrences and help explain the modular behavior.

1. Introduction

Divisibility sequences connect arithmetic in the index to arithmetic in the terms. The rule is simple. If m divides n, then a_m divides a_n.

If a sequence also satisfies a linear recurrence, then divisibility becomes much more rigid. In particular, classical work of Ward and Lehmer shows that strong divisibility behavior often forces a Lucas-type structure [War37, Leh30].

This paper focuses on second-order linear recurrences

$$a_{n+2} = Pa_{n+1} - Qa_n,$$

where P and Q are fixed integers. The main examples are the Lucas sequences $U_n(P,Q)$ and $V_n(P,Q)$. They have strong addition identities, and in many cases $U_n(P,Q)$ is a strong divisibility sequence.

Later sections explain what happens after reducing the recurrence modulo a prime p. This leads to ranks of apparition, which measure where a prime first appears in the sequence. We then connect ranks of apparition to primitive prime divisors and to Zsigmondy-type theorems, including the theorem of Bilu, Hanrot, and Voutier [Zsi92, BHV01].

2. Divisibility sequences and strong divisibility

Definition 2.1. An integer sequence $(a_n)_{n\geq 1}$ is a *divisibility sequence* if for all positive integers m, n,

$$m \mid n \quad \Longrightarrow \quad a_m \mid a_n.$$

Definition 2.2. An integer sequence $(a_n)_{n\geq 1}$ is a *strong divisibility sequence* if for all positive integers m, n,

$$\gcd(a_m, a_n) = |a_{\gcd(m,n)}|.$$

Remark 2.3. Throughout the paper, $\gcd(x,y)$ means the positive gcd of the integers x and y. This is why Definition 2.2 uses an absolute value. For many standard examples such as Fibonacci and Pell, the terms are positive for $n \geq 1$, so the absolute value does not change anything.

Lemma 2.4. *If (a_n) is a strong divisibility sequence, then it is a divisibility sequence.*

Date: July 12, 2026.

Proof. Assume (a_n) is strong divisibility. If $m \mid n$, then $\gcd(m,n) = m$. Using Definition 2.2,

$$\gcd(a_m, a_n) = |a_{\gcd(m,n)}| = |a_m|.$$

So $|a_m|$ divides a_n. Since $a_m = \pm|a_m|$, this implies a_m divides a_n. □

Remark 2.5. If (a_n) is strong divisibility and $\gcd(m,n) = 1$, then $\gcd(a_m, a_n) = |a_1|$. In particular, if $a_1 = \pm 1$ then $\gcd(a_m, a_n) = 1$ whenever $\gcd(m,n) = 1$.

Example 2.6 (Fibonacci)**.** The Fibonacci numbers (F_n) defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ form a strong divisibility sequence. This is the Lucas sequence $U_n(1,-1)$ from Section 3. This follows from Theorem 4.8 with $(P,Q) = (1,-1)$.

Example 2.7 (A basic exponential example)**.** Fix an integer $b \geq 2$ and set $a_n = b^n - 1$. If $m \mid n$ with $n = km$, then

$$a_n = b^{km} - 1 = (b^m)^k - 1,$$

which is divisible by $b^m - 1 = a_m$. So $(b^n - 1)$ is a divisibility sequence.

The main question for the rest of the paper is what happens when we combine divisibility with a linear recurrence. For second-order recurrences, this leads naturally to Lucas sequences.

3. Second-order linear recurrences and Lucas sequences

A second-order linear recurrence with constant coefficients has the form

$$a_{n+2} = Pa_{n+1} - Qa_n \qquad (n \geq 0), \tag{3.1}$$

where $P, Q \in \mathbb{Z}$ are fixed and $a_0, a_1 \in \mathbb{Z}$ are initial values. The characteristic polynomial is

$$f(x) = x^2 - Px + Q.$$

Let α and β be its roots in $\mathbb{C}$, so $\alpha + \beta = P$ and $\alpha\beta = Q$. Its discriminant is

$$D = P^2 - 4Q.$$

When $D \neq 0$ the roots are distinct. When $D = 0$ the polynomial has a repeated root.

Definition 3.1 (Lucas sequences)**.** Fix integers P, Q. The Lucas sequence of the first kind $U_n = U_n(P,Q)$ is defined by

$$U_0 = 0, \qquad U_1 = 1, \qquad U_{n+2} = PU_{n+1} - QU_n \quad (n \geq 0).$$

The Lucas sequence of the second kind $V_n = V_n(P,Q)$ is defined by

$$V_0 = 2, \qquad V_1 = P, \qquad V_{n+2} = PV_{n+1} - QV_n \quad (n \geq 0).$$

Remark 3.2. Many arithmetic statements are cleanest when we rule out degenerate behavior. A common nondegeneracy assumption is

$$Q \neq 0 \quad \text{and} \quad \alpha/\beta \text{ is not a root of unity.}$$

This prevents periodic behavior coming from $\alpha^n = \beta^n$ too often, which can produce extra zeros and accidental divisibility.

Proposition 3.3 (Binet-type formulas)**.** *Assume $\alpha \neq \beta$. Then for all integers $n \geq 0$,*

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n.$$

Proof. Define $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ and $v_n = \alpha^n + \beta^n$. Since α and β satisfy $\alpha^2 = P\alpha - Q$ and $\beta^2 = P\beta - Q$, both (α^n) and (β^n) satisfy the recurrence (3.1). By linearity, (u_n) and (v_n) satisfy (3.1) as well. Also $u_0 = 0$ and $u_1 = 1$, so $u_n = U_n$ by uniqueness of solutions of a second-order recurrence with given initial values. Similarly, $v_0 = 2$ and $v_1 = P$, so $v_n = V_n$. □

Remark 3.4. The expressions in Proposition 3.3 involve algebraic numbers. Even so, the sequences U_n and V_n are integers because they are defined by integer initial values and an integer recurrence. The formulas are mainly used to prove identities.

3.1. **Matrices and an addition formula.** Let

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

If (a_n) satisfies (3.1), then the recurrence can be written as

$$\begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix} = M^n \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}.$$

For Lucas sequences this gives clean addition formulas.

Proposition 3.5. *For every integer $n \geq 1$,*

$$M^n = \begin{pmatrix} U_{n+1} & -Q\,U_n \\ U_n & -Q\,U_{n-1} \end{pmatrix}.$$

Proof. We use induction on n. For $n = 1$, the right side becomes

$$\begin{pmatrix} U_2 & -Q\,U_1 \\ U_1 & -Q\,U_0 \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} = M,$$

since $U_2 = PU_1 - QU_0 = P$. Assume the identity holds for n. Then

$$M^{n+1} = M^n M = \begin{pmatrix} U_{n+1} & -Q\,U_n \\ U_n & -Q\,U_{n-1} \end{pmatrix} \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

The $(1,1)$ entry is $PU_{n+1} - QU_n = U_{n+2}$. The $(2,1)$ entry is $PU_n - QU_{n-1} = U_{n+1}$. The $(1,2)$ entry is $-Q\,U_{n+1}$. The $(2,2)$ entry is $-Q\,U_n$. So

$$M^{n+1} = \begin{pmatrix} U_{n+2} & -Q\,U_{n+1} \\ U_{n+1} & -Q\,U_n \end{pmatrix},$$

which is the desired formula with n replaced by $n+1$. □

Corollary 3.6 (Addition formula for U_n)**.** *For all integers $m, n \geq 1$,*

$$U_{m+n} = U_m U_{n+1} - Q\,U_{m-1} U_n. \tag{3.2}$$

Proof. From Proposition 3.5, we have $M^{m+n} = M^m M^n$. Compare the $(2,1)$ entries. The $(2,1)$ entry of M^{m+n} is U_{m+n}. The $(2,1)$ entry of $M^m M^n$ is

$$(U_m)(U_{n+1}) + (-Q\,U_{m-1})(U_n) = U_m U_{n+1} - Q\,U_{m-1} U_n.$$

This gives (3.2). □

Corollary 3.7 (Cassini-type identity)**.** *Assume $Q \neq 0$. For all $n \geq 1$,*

$$U_n^2 - U_{n-1} U_{n+1} = Q^{\,n-1}.$$

Proof. Take determinants in Proposition 3.5. Since $\det(M) = Q$, we have $\det(M^n) = Q^n$. On the other hand,

$$\det(M^n) = \det \begin{pmatrix} U_{n+1} & -Q\,U_n \\ U_n & -Q\,U_{n-1} \end{pmatrix} = Q\big(U_n^2 - U_{n-1} U_{n+1}\big).$$

Divide by Q to get the identity. □

Remark 3.8. Identity (3.2) is the main tool for gcd arguments later. It rewrites U_{m+n} in terms of U_m and U_n. Because of this, proofs about $\gcd(U_m, U_n)$ often follow the Euclidean algorithm on the indices.

4. Divisibility and strong divisibility for $U_n(P,Q)$

The divisibility behavior of Lucas sequences is well known. In particular, $U_k \mid U_n$ when $k \mid n$. Under standard coprimality assumptions on (P,Q), one also has a strong gcd identity

$$\gcd(U_m, U_n) = |U_{\gcd(m,n)}|.$$

See, for example, [BG21] for discussion and references.

Throughout this section we fix integers P, Q and write $U_n = U_n(P,Q)$. Unless we explicitly say otherwise, we assume

$$Q \neq 0 \quad \text{and} \quad \gcd(P,Q) = 1. \tag{4.1}$$

The condition $Q \neq 0$ avoids a few special cases where some statements need different formulas.

4.1. **A coprimality fact involving Q.**

Lemma 4.1. *Assume (4.1). Then $\gcd(U_n, Q) = 1$ for every $n \geq 1$.*

Proof. Let p be a prime divisor of Q. Since $\gcd(P,Q) = 1$, we have $p \nmid P$. Reduce the recurrence $U_{n+2} = PU_{n+1} - QU_n$ modulo p. Because $Q \equiv 0 \pmod p$, we get $U_{n+2} \equiv PU_{n+1} \pmod p$ for all $n \geq 0$. Starting from $U_1 = 1$, this implies $U_n \equiv P^{n-1} \pmod p$ for all $n \geq 1$. Since $p \nmid P$, we have $P^{n-1} \not\equiv 0 \pmod p$, so $p \nmid U_n$. This holds for every prime $p \mid Q$, so $\gcd(U_n, Q) = 1$. □

4.2. **Divisibility.** We now prove the basic divisibility property for U_n.

Remark 4.2. If $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a 2×2 matrix, then its *trace* is

$$\operatorname{tr}(N) = a + d.$$

It is the sum of the diagonal entries.

Lemma 4.3. *Let N be a 2×2 integer matrix, and define $b_k = (N^k)_{2,1}$ for $k \geq 0$. Then (b_k) satisfies the recurrence*

$$b_{k+2} = \operatorname{tr}(N)\, b_{k+1} - \det(N)\, b_k \qquad (k \geq 0),$$

with initial values $b_0 = 0$ and $b_1 = (N)_{2,1}$.

Proof. Every 2×2 matrix satisfies its characteristic polynomial. So $N^2 - \operatorname{tr}(N)N + \det(N)I = 0$. Multiply this identity on the right by N^k to get

$$N^{k+2} = \operatorname{tr}(N)\, N^{k+1} - \det(N)\, N^k \qquad (k \geq 0).$$

Taking the $(2,1)$ entry gives the stated recurrence for b_k. Also $N^0 = I$, so $b_0 = (I)_{2,1} = 0$ and $b_1 = (N)_{2,1}$. □

Theorem 4.4 (Divisibility of U_n)**.** *If $m \mid n$, then $U_m \mid U_n$. Equivalently, $(U_n)_{n \geq 1}$ is a divisibility sequence.*

Proof. Write $n = km$ with $k \geq 1$. Let $M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$. By Proposition 3.5, the $(2,1)$ entry of M^t equals U_t for every $t \geq 1$.

Set $N = M^m$. Then $M^{km} = (M^m)^k = N^k$, so

$$U_{km} = (M^{km})_{2,1} = (N^k)_{2,1}.$$

Define $b_k = (N^k)_{2,1}$ for $k \geq 0$. By Lemma 4.3, (b_k) satisfies a second-order linear recurrence with integer coefficients, and $b_0 = 0$ and $b_1 = (N)_{2,1} = U_m$.

We claim that U_m divides b_k for every $k \geq 0$. This follows by induction using the recurrence for (b_k). It holds for $k = 0$ since $b_0 = 0$. It holds for $k = 1$ since $b_1 = U_m$. If $U_m \mid b_k$ and $U_m \mid b_{k+1}$, then the recurrence expresses b_{k+2} as an integer linear combination of b_{k+1} and b_k, so $U_m \mid b_{k+2}$.

Therefore $U_m \mid b_k = U_{km} = U_n$. □

Corollary 4.5. *Let $n > 1$. If $n = ab$ with $1 < a < n$, then $U_a \mid U_n$.*

In particular, if $|U_n|$ is prime and n is composite, then for every divisor a of n with $1 < a < n$ we have $|U_a| = 1$ or $|U_a| = |U_n|$.

Proof. If $n = ab$ with $1 < a < n$, then $a \mid n$ and Theorem 4.4 gives $U_a \mid U_n$.

Now assume $|U_n|$ is prime and $1 < a < n$ with $a \mid n$. Since $U_a \mid U_n$, we must have $U_a = \pm 1$ or $U_a = \pm U_n$. Taking absolute values gives $|U_a| = 1$ or $|U_a| = |U_n|$. □

4.3. **Strong divisibility.** To run the Euclidean algorithm on indices, we need one more ingredient. We first show that consecutive terms are coprime when (4.1) holds.

Lemma 4.6. *Assume (4.1). Then $\gcd(U_n, U_{n+1}) = 1$ for every $n \geq 1$.*

Proof. By Corollary 3.7,

$$U_n^2 - U_{n-1}U_{n+1} = Q^{n-1}.$$

Let $d = \gcd(U_n, U_{n+1})$. Then d divides U_n^2 and d divides $U_{n-1}U_{n+1}$, so d divides their difference. Hence $d \mid Q^{n-1}$.

By Lemma 4.1, we have $\gcd(U_{n+1}, Q) = 1$, and therefore $\gcd(U_{n+1}, Q^{n-1}) = 1$. Since d divides both U_{n+1} and Q^{n-1}, this forces $d = 1$. □

Lemma 4.7. *Assume (4.1). Then for all $m, n \geq 1$,*

$$\gcd(U_m, U_{m+n}) = \gcd(U_m, U_n).$$

Proof. Use the addition formula (3.2) with the roles of m and n swapped

$$U_{m+n} = U_nU_{m+1} - Q\,U_{n-1}U_m.$$

Reduce this identity modulo U_m. The second term is divisible by U_m, so

$$U_{m+n} \equiv U_nU_{m+1} \pmod{U_m}.$$

So

$$\gcd(U_m, U_{m+n}) = \gcd(U_m, U_nU_{m+1}).$$

By Lemma 4.6, $\gcd(U_m, U_{m+1}) = 1$. So any common divisor of U_m and U_nU_{m+1} must divide U_n. This gives

$$\gcd(U_m, U_{m+n}) \mid \gcd(U_m, U_n).$$

For the reverse divisibility, let $d = \gcd(U_m, U_n)$. Then d divides U_m and U_n. So d divides U_nU_{m+1} and it also divides $Q\,U_{n-1}U_m$. The addition formula shows that d divides their difference, which is U_{m+n}. So d divides $\gcd(U_m, U_{m+n})$. Therefore

$$\gcd(U_m, U_n) \mid \gcd(U_m, U_{m+n}).$$

Combining the two divisibilities gives the desired equality. □

Theorem 4.8 (Strong divisibility of U_n)**.** *Assume (4.1). Then for all $m, n \geq 1$,*

$$\gcd(U_m, U_n) = |U_{\gcd(m,n)}|.$$

Proof. Assume $n \geq m$. Write $n = qm + r$ with $q \geq 0$ and $0 \leq r < m$. Applying Lemma 4.7 q times gives

$$\gcd(U_m, U_n) = \gcd(U_m, U_{n-qm}) = \gcd(U_m, U_r).$$

This matches the reduction step in the Euclidean algorithm.

Now run the Euclidean algorithm on (m, n). After finitely many steps, it produces $d = \gcd(m, n)$ and a remainder 0. Applying the reduction above at each step gives

$$\gcd(U_m, U_n) = \gcd(U_d, U_0).$$

Since $U_0 = 0$ and $\gcd(x, 0) = |x|$ for any integer x, we have $\gcd(U_d, U_0) = |U_d|$. This gives the claim. □

Remark 4.9. The hypothesis $\gcd(P,Q) = 1$ is needed for a clean strong divisibility rule. For example, take $(P,Q) = (3,3)$. Then $U_1 = 1$, $U_2 = 3$, $U_3 = 6$, $U_4 = 9$, and $U_5 = 9$. So $\gcd(U_4, U_5) = 9$ but $|U_{\gcd(4,5)}| = |U_1| = 1$.

5. Index divisibility and ranks of apparition

In Section 4 we proved that $U_m \mid U_n$ whenever $m \mid n$. A natural next question is whether a converse can hold.

5.1. **Index divisibility.** A sequence (a_n) is sometimes said to have the *index divisibility property* if

$$a_m \mid a_n \quad \Longrightarrow \quad m \mid n,$$

at least for most pairs (m,n). For Lucas sequences, the cleanest way to prove such a converse is to understand which primes divide which terms. That leads to ranks of apparition.

Throughout this section we assume (4.1) and write $U_n = U_n(P,Q)$.

5.2. **Rank of apparition.**

Definition 5.1. Let p be a prime. If there exists $n \geq 1$ such that $p \mid U_n$, then the *rank of apparition* of p in (U_n) is the least such n. We denote it by $r_U(p)$, or simply $r(p)$ when the sequence is clear. If no such n exists, we say that the rank of apparition of p does not exist.

The next lemma says that once a prime appears, it repeats exactly at multiples of its rank. This is often called a law of repetition for primes.

Lemma 5.2. *Assume that $r(p)$ exists. Then for every $n \geq 1$,*

$$p \mid U_n \quad \Longleftrightarrow \quad r(p) \mid n.$$

Proof. If $r(p) \mid n$, then $U_{r(p)} \mid U_n$ by Theorem 4.4, so $p \mid U_n$.

Conversely, assume $p \mid U_n$. Then p divides both U_n and $U_{r(p)}$, so $p \mid \gcd(U_n, U_{r(p)})$. By Theorem 4.8,

$$\gcd(U_n, U_{r(p)}) = |U_{\gcd(n,r(p))}|.$$

So $p \mid U_{\gcd(n,r(p))}$. By minimality of $r(p)$, this forces $\gcd(n, r(p)) = r(p)$, and therefore $r(p) \mid n$. □

Remark 5.3. The definition does not guarantee that $r(p)$ exists for every prime p. For primes dividing Q, Lemma 4.1 shows that p never divides any U_n with $n \geq 1$. For primes not dividing Q, ranks often exist and can be studied using reduction modulo p as in Section 6. Classical discussions include [Des78, Wal60, Jar05].

5.3. **A converse statement.** The cleanest way to force a converse $U_m \mid U_n \Rightarrow m \mid n$ is to know that U_m contains a prime that appears for the first time at index m.

Definition 5.4. Let $m \geq 2$. A prime p is a *primitive prime divisor* of U_m if

$$p \mid U_m \quad \text{and} \quad p \nmid U_k \text{ for every } 1 \leq k < m.$$

Lemma 5.5. *If p is a primitive prime divisor of U_m, then $r(p)$ exists and $r(p) = m$.*

Proof. Since $p \mid U_m$, the rank $r(p)$ exists and satisfies $r(p) \leq m$ by definition. If $r(p) < m$, then $p \mid U_{r(p)}$ with $1 \leq r(p) < m$, which contradicts primitiveness. So $r(p) = m$. □

Proposition 5.6 (A converse divisibility statement)**.** *Assume that U_m has a primitive prime divisor. If $U_m \mid U_n$, then $m \mid n$.*

Proof. Let p be a primitive prime divisor of U_m. If $U_m \mid U_n$, then $p \mid U_n$. By Lemma 5.5, we have $r(p) = m$. Now Lemma 5.2 gives $m = r(p) \mid n$. □

Remark 5.7. Proposition 5.6 reduces an index divisibility question to the existence of primitive prime divisors. Primitive prime divisor theorems are discussed in Section 7. For nondegenerate Lucas sequences, the results of Carmichael and of Bilu, Hanrot, and Voutier show that primitive prime divisors exist for all but finitely many indices [Car13, BHV01].

6. Reduction modulo primes

This section studies the sequence (U_n) modulo a prime p. The idea is to look at the residues $U_n \bmod p$. Since there are only finitely many residues, the sequence must eventually repeat. For second-order recurrences, we can say something stronger. If $p \nmid Q$, then the recurrence can be run forward and backward modulo p, and this forces repetition to start immediately.

Throughout this section we assume (4.1). We set

$$D = P^2 - 4Q$$

and write $U_n = U_n(P, Q)$.

6.1. **The state of a recurrence.** Fix a prime p. Write $\mathbb{F}_p$ for the field with p elements. We can think of $\mathbb{F}_p$ as the set $\{0, 1, \dots, p-1\}$ with arithmetic done modulo p.

Reducing the recurrence

$$U_{n+2} = PU_{n+1} - QU_n$$

modulo p gives the same recurrence inside $\mathbb{F}_p$.

A second-order recurrence is determined by two consecutive values. So it is convenient to treat two consecutive terms as a single object.

Definition 6.1. The *state* at time n is the ordered pair

$$S_n = (U_{n+1}, U_n) \in \mathbb{F}_p^2.$$

Knowing S_n determines S_{n+1}. Indeed, the recurrence gives

$$S_{n+1} = (U_{n+2}, U_{n+1}) = (PU_{n+1} - QU_n,\ U_{n+1}).$$

Definition 6.2. Define the *update map* $T\colon \mathbb{F}_p^2 \to \mathbb{F}_p^2$ by

$$T(x, y) = (Px - Qy,\ x).$$

Then $S_{n+1} = T(S_n)$ for all $n \geq 0$.

Remark 6.3. Starting from $S_0 = (U_1, U_0) = (1, 0)$, we get a sequence

$$S_0,\ S_1,\ S_2,\ \dots$$

where each state is obtained by applying T again. This list is sometimes called the *orbit* of S_0 under T. We will not need any group theory. We only use the fact that $\mathbb{F}_p^2$ is a finite set with p^2 elements.

6.2. **Matrices and invertibility modulo p.** The update map has a clean matrix form. Let

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

Then

$$\begin{pmatrix} U_{n+2} \\ U_{n+1} \end{pmatrix} = M \begin{pmatrix} U_{n+1} \\ U_n \end{pmatrix}.$$

Iterating gives

$$\begin{pmatrix} U_{n+1} \\ U_n \end{pmatrix} = M^n \begin{pmatrix} U_1 \\ U_0 \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{6.1}$$

To justify periodicity, we need a standard fact.

Definition 6.4. A 2×2 matrix A with entries in $\mathbb{F}_p$ is *invertible* if there exists a matrix B over $\mathbb{F}_p$ such that $AB = BA = I$.

Lemma 6.5. *A 2×2 matrix A over $\mathbb{F}_p$ is invertible if and only if $\det(A) \neq 0$ in $\mathbb{F}_p$.*

Proof. This is the usual formula for the inverse of a 2×2 matrix. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$A \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \det(A)\, I.$$

If $\det(A) \neq 0$, then it has a multiplicative inverse in $\mathbb{F}_p$, so we can divide by $\det(A)$ and obtain an inverse for A. If $\det(A) = 0$, then the columns of A are linearly dependent, so A cannot be invertible. □

Since $\det(M) = Q$, the matrix M is invertible modulo p exactly when $p \nmid Q$.

6.3. **Periodicity from the start.**

Proposition 6.6. *Assume $p \nmid Q$. Then the sequence $(U_n \bmod p)$ is periodic from the start. Equivalently, there exists a least positive integer $\pi(p)$ such that*

$$U_{n+\pi(p)} \equiv U_n \pmod{p} \qquad \text{for all } n \geq 0.$$

Moreover, $\pi(p)$ is the least positive integer t such that

$$M^t \equiv I \pmod{p}.$$

Proof. Assume $p \nmid Q$. Then M is invertible modulo p by Lemma 6.5. So the update map T is bijective on $\mathbb{F}_p^2$.

Because $\mathbb{F}_p^2$ has only p^2 elements, the orbit

$$S_0,\ S_1,\ S_2,\ \ldots$$

must repeat a state. So there exist $0 \leq i < j$ such that $S_i = S_j$.

Now use bijectivity. Since T is a bijection, it has an inverse map T^{-1}. Apply T^{-1} to the identity $S_i = S_j$ exactly i times. This gives

$$S_0 = S_{j-i}.$$

So the starting state repeats. Once a state repeats, the future repeats with the same step size. Therefore $S_n = S_{n+(j-i)}$ for all $n \geq 0$. In particular, $U_n \equiv U_{n+(j-i)} \pmod{p}$ for all n. This proves periodicity from the start.

Let $\pi(p)$ be the least positive period for $(U_n \bmod p)$. We now relate it to powers of M.

First assume $M^t \equiv I \pmod{p}$. Then (6.1) gives

$$\begin{pmatrix} U_{n+t+1} \\ U_{n+t} \end{pmatrix} = M^{n+t} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = M^n M^t \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} U_{n+1} \\ U_n \end{pmatrix} \pmod{p}.$$

So $U_{n+t} \equiv U_n \pmod{p}$ for all n. This shows that any such t is a period.

Conversely, assume t is a period for the state sequence, meaning $S_{n+t} = S_n$ for all n. In particular, $S_t = S_0$ and $S_{t+1} = S_1$. Write vectors in $\mathbb{F}_p^2$ as columns. From (6.1), we have

$$S_n = \begin{pmatrix} U_{n+1} \\ U_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

So $S_t = S_0$ means $M^t \binom{1}{0} = \binom{1}{0}$. Also $S_{t+1} = S_1$ means

$$M^{t+1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = M \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Cancel one M on the left by multiplying by M^{-1}, which exists since $p \nmid Q$. This gives

$$M^t \left(M \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = M \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

So M^t fixes both vectors $\binom{1}{0}$ and $M\binom{1}{0} = \binom{P}{1}$. These two vectors form a basis of $\mathbb{F}_p^2$ because the determinant of the 2×2 matrix with these as columns is 1. A linear map that fixes a basis is the identity map. Therefore $M^t \equiv I \pmod{p}$.

So the periods t are exactly the positive integers with $M^t \equiv I \pmod{p}$. The smallest such t is $\pi(p)$. □

Remark 6.7. It is common to write $\mathrm{GL}_2(\mathbb{F}_p)$ for the set of all invertible 2×2 matrices with entries in $\mathbb{F}_p$. With matrix multiplication, $\mathrm{GL}_2(\mathbb{F}_p)$ is a finite group. In this language, Proposition 6.6 says that $\pi(p)$ is the order of M in $\mathrm{GL}_2(\mathbb{F}_p)$. You do not need group theory to use this statement. You can treat it as an alternative way to say that some power of M becomes the identity modulo p.

Remark 6.8. Proposition 6.6 also gives a rough bound for $\pi(p)$. There are exactly $p^2 - 1$ choices for the first column of an invertible matrix, since it can be any nonzero vector in $\mathbb{F}_p^2$. After choosing the first column, there are $p^2 - p$ choices for the second column, since it can be any vector not in the span of the first. Therefore

$$|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p).$$

The order of any element of a finite group divides the group size, so

$$\pi(p) \leq (p^2 - 1)(p^2 - p).$$

This bound is far from sharp in many cases, but it shows that $\pi(p)$ is always finite when $p \nmid Q$.

6.4. **The law of apparition.** We now explain why, for many odd primes p, the rank of apparition $r(p)$ must divide either $p - 1$ or $p + 1$. This is a standard result for Lucas sequences.

We first introduce a small piece of notation.

Definition 6.9. For a prime p, write $\mathbb{F}_p^\times$ for the set of nonzero elements of $\mathbb{F}_p$. With multiplication, $\mathbb{F}_p^\times$ is a cyclic group of size $p - 1$.

We also need the Legendre symbol.

Definition 6.10. Let p be an odd prime and let $a \in \mathbb{Z}$. The *Legendre symbol* is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a nonzero square modulo } p, \\ -1 & \text{if } a \text{ is a nonsquare modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

We also write $\varepsilon(p) = \left(\frac{D}{p}\right)$.

Remark 6.11. The characteristic polynomial is $f(x) = x^2 - Px + Q$. If $p \nmid D$, then f has two distinct roots modulo p when $\varepsilon(p) = 1$, and it has no roots modulo p when $\varepsilon(p) = -1$. If $\varepsilon(p) = -1$, the roots still exist in a larger field with p^2 elements, usually denoted by $\mathbb{F}_{p^2}$.

Definition 6.12. For an odd prime p, $\mathbb{F}_{p^2}$ denotes the field with p^2 elements. It contains $\mathbb{F}_p$ as a subfield. Every element of $\mathbb{F}_{p^2}$ satisfies $x^{p^2} = x$.

Definition 6.13. The *Frobenius map* on $\mathbb{F}_{p^2}$ is the function

$$\varphi \colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}, \qquad \varphi(x) = x^p.$$

It is a field automorphism. It fixes every element of $\mathbb{F}_p$.

Theorem 6.14 (Law of apparition)**.** *Let p be an odd prime.*

If $p \mid Q$, then $p \nmid U_n$ for every $n \geq 1$.

Assume $p \nmid Q$. Let $r(p)$ be the rank of apparition of p in (U_n), assuming it exists. Then

$$r(p) \mid p - \varepsilon(p).$$

In particular, $r(p) \mid p-1$ when D is a square modulo p, and $r(p) \mid p+1$ when D is a nonsquare modulo p.

Proof. If $p \mid Q$, then $p \nmid P$ since $\gcd(P, Q) = 1$. Reducing the recurrence modulo p gives $U_{n+2} \equiv PU_{n+1} \pmod{p}$. Since $U_1 = 1$, we get $U_n \equiv P^{n-1} \pmod{p}$ for all $n \geq 1$. This is never 0 modulo p, so $p \nmid U_n$ for all $n \geq 1$.

Now assume $p \nmid Q$ and p is odd. Work in a field where the roots of $f(x) = x^2 - Px + Q$ exist. If $p \nmid D$, then f has two distinct roots in $\mathbb{F}_p$ when $\varepsilon(p) = 1$, and in $\mathbb{F}_{p^2}$ when $\varepsilon(p) = -1$. Call the two roots α and β. In that field, the Binet formula still holds,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Since $\alpha \neq \beta$, we have $\alpha - \beta \neq 0$. So $p \mid U_n$ is equivalent to $\alpha^n = \beta^n$. Because $Q = \alpha\beta$ is nonzero modulo p, we can divide by β^n and obtain

$$\left(\frac{\alpha}{\beta}\right)^n = 1.$$

Set $t = \alpha/\beta$. Then $r(p)$ is the multiplicative order of t, meaning the smallest positive n with $t^n = 1$.

Case 1. $\varepsilon(p) = 1$. Then $\alpha, \beta \in \mathbb{F}_p$ and $t \in \mathbb{F}_p^\times$. Every element of $\mathbb{F}_p^\times$ satisfies $x^{p-1} = 1$. So $t^{p-1} = 1$, which implies $r(p) \mid p - 1$.

Case 2. $\varepsilon(p) = -1$. Then $\alpha, \beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Because f has coefficients in $\mathbb{F}_p$, if α is a root then $\alpha^p = \varphi(\alpha)$ is also a root. There are only two roots, so α^p must be the other one. So $\alpha^p = \beta$ and similarly $\beta^p = \alpha$. Then

$$t^p = \left(\frac{\alpha}{\beta}\right)^p = \frac{\alpha^p}{\beta^p} = \frac{\beta}{\alpha} = t^{-1}.$$

So $t^{p+1} = 1$, which implies $r(p) \mid p + 1$.

Case 3. $\varepsilon(p) = 0$. This means $p \mid D$. Then $f(x)$ has a repeated root modulo p. Write $\lambda = P/2$ in $\mathbb{F}_p$, which makes sense since p is odd. Since $p \mid D$, we have $P^2 \equiv 4Q \pmod{p}$, so $Q \equiv \lambda^2 \pmod{p}$ and $P \equiv 2\lambda \pmod{p}$. Also $p \nmid Q$ implies $\lambda \neq 0$ in $\mathbb{F}_p$.

We claim that in this case

$$U_n \equiv n\,\lambda^{n-1} \pmod{p} \qquad \text{for all } n \geq 0.$$

This holds for $n = 0$ and $n = 1$ since $U_0 = 0$ and $U_1 = 1$. Assume it holds for n and $n+1$. Reducing the recurrence modulo p gives

$$U_{n+2} \equiv 2\lambda U_{n+1} - \lambda^2 U_n \pmod{p}.$$

Substitute the induction hypothesis

$$U_{n+2} \equiv 2\lambda(n+1)\lambda^n - \lambda^2 n\lambda^{n-1} = (n+2)\lambda^{n+1} \pmod{p}.$$

So the formula holds for all n.

Since $\lambda \neq 0$ modulo p, this implies $U_n \equiv 0 \pmod{p}$ if and only if $n \equiv 0 \pmod{p}$. In particular, $p \mid U_p$ and $p \nmid U_n$ for $1 \leq n < p$. So $r(p) = p$, and in particular $r(p) \mid p$. Since $\varepsilon(p) = 0$, this is the same as $r(p) \mid p - \varepsilon(p)$.

Combining the three cases gives $r(p) \mid p - \varepsilon(p)$. □

Corollary 6.15. *Let p be an odd prime with $p \nmid Q$ and assume $r(p)$ exists. Then $r(p) \leq p + 1$ and*

$$p \mid U_n \quad \iff \quad r(p) \mid n.$$

Proof. Theorem 6.14 gives $r(p) \mid p - \varepsilon(p)$, so $r(p) \le p + 1$. The equivalence $p \mid U_n \iff r(p) \mid n$ is Lemma 5.2. □

Example 6.16 (Fibonacci)**.** For Fibonacci we have $(P, Q) = (1, -1)$, so $D = 5$. If $p \neq 5$ is an odd prime, then

$$r(p) \mid p - \left(\frac{5}{p}\right).$$

For example, $\left(\frac{5}{7}\right) = -1$, so the theorem predicts $r(7) \mid 8$. In fact $r(7) = 8$ since $7 \mid F_8 = 21$ and 7 does not divide any earlier Fibonacci number.

Remark 6.17. The case $p \mid D$ behaves differently because the characteristic polynomial has a repeated root modulo p. These primes are sometimes called special primes for the Lucas pair (P, Q). They also play a role in p-adic valuation formulas for U_n, see [Bal19].

7. Primitive prime divisors in Lucas sequences

Primitive prime divisors give a way to say that new primes keep appearing as the index grows. This section expands the vocabulary used in primitive divisor theorems and explains why some primes are excluded from the definition. We also connect primitive prime divisors to ranks of apparition from Section 5.

Throughout this section we assume (4.1). We continue to write $D = P^2 - 4Q$.

7.1. **What can go wrong.** A first attempt at a definition is the one used earlier.

A prime p is primitive for U_n if $p \mid U_n$ but $p \nmid U_k$ for every $1 \le k < n$.

This definition formalizes the idea of a prime that appears for the first time at index n. However, when dealing with Lucas sequences one usually also excludes primes dividing the discriminant D. The reason is that primes dividing D correspond to the situation where the two roots α and β become equal modulo p. When that happens, the Binet expression

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

is no longer a good measurement, because the denominator becomes 0 modulo p. This repeated root behavior can make a prime divide U_n for structural reasons that do not reflect the usual primitive divisor pattern.

7.2. **The standard definition.** A common definition in research over Lucas and Lehmer is the one used by Voutier [Vou96].

Definition 7.1. Let $n \ge 2$. A prime number p is called a *primitive prime divisor* of $U_n = U_n(P, Q)$ if

$$p \mid U_n \quad \text{and} \quad p \nmid D\, U_1 U_2 \cdots U_{n-1}.$$

Since $U_1 = 1$, this means $p \mid U_n$, $p \nmid D$, and $p \nmid U_k$ for every $1 \le k < n$.

Remark 7.2. Definition 7.1 is slightly stronger than Definition 5.4. The only difference is that we also require $p \nmid D$. In practice, excluding primes dividing D removes a small and finite set of primes that often need separate casework.

7.3. **Rank equaling the index.** Ranks of apparition were defined in Section 5. The next lemma explains why primitive prime divisors are exactly the primes with rank equal to the index.

Lemma 7.3. *Assume (4.1). If p is a primitive prime divisor of U_n, as in Definition 7.1, then the rank of apparition $r(p)$ exists and*

$$r(p) = n.$$

Proof. Since $p \mid U_n$, the rank $r(p)$ exists and satisfies $r(p) \le n$ by definition. If $r(p) < n$, then $p \mid U_{r(p)}$ with $1 \le r(p) < n$. This contradicts primitiveness, since p would divide an earlier term. Therefore $r(p) = n$. □

Combining Lemma 7.3 with Theorem 6.14 gives a congruence restriction.

Corollary 7.4. *Assume (4.1). Let p be an odd prime with $p \nmid QD$. If p is a primitive prime divisor of U_n, then*

$$n \mid p - \left(\frac{D}{p}\right).$$

In particular, $n \mid p-1$ when D is a square modulo p, and $n \mid p+1$ when D is a nonsquare modulo p.

Proof. By Lemma 7.3 we have $r(p) = n$. Theorem 6.14 gives $r(p) \mid p - \left(\frac{D}{p}\right)$. Substituting $r(p) = n$ gives the result. □

7.4. **A simpler case.** Before stating results for Lucas sequences, it helps to look at a simpler type of sequence. This is the case studied by Zsigmondy.

Definition 7.5. Let $a > b > 0$ be integers. A prime p is a *primitive prime divisor* of $a^n - b^n$ if

$$p \mid (a^n - b^n) \quad \text{and} \quad p \nmid (a^k - b^k) \ \text{ for every } 1 \le k < n.$$

Lemma 7.6. *Let $a > b > 0$ be coprime integers and let p be a prime with $p \nmid ab$. If p is a primitive prime divisor of $a^n - b^n$, then the residue class of ab^{-1} modulo p has multiplicative order exactly n. In particular, $n \mid (p-1)$.*

Proof. Because $p \nmid b$, the inverse b^{-1} exists modulo p. From $p \mid (a^n - b^n)$ we get $a^n \equiv b^n \pmod p$, and after multiplying by b^{-n} we obtain

$$(ab^{-1})^n \equiv 1 \pmod p.$$

Let t be the order of ab^{-1} modulo p. Then $t \mid n$.

If $t < n$, then $(ab^{-1})^t \equiv 1 \pmod p$, so $a^t \equiv b^t \pmod p$. This means $p \mid (a^t - b^t)$, which contradicts primitiveness. Therefore $t = n$.

Finally, $(\mathbb{Z}/p\mathbb{Z})^\times$ has size $p-1$, so every element has order dividing $p-1$. Thus $n \mid (p-1)$. □

Zsigmondy's theorem says that primitive prime divisors almost always exist.

Theorem 7.7 (Zsigmondy)**.** *Let $a > b > 0$ be coprime integers. Then for every integer $n \ge 2$, the number $a^n - b^n$ has a primitive prime divisor, with the following exceptions:*

$$(a, b, n) = (2, 1, 6), \quad \text{and} \quad n = 2 \text{ with } a + b \text{ a power of } 2.$$

Remark 7.8. Theorem 7.7 is due to Zsigmondy [Zsi92]. Related refinements and properties also appear in work of Birkhoff and Vandiver [BirVan04].

7.5. **Primitive divisor theorems for Lucas sequences.** Lucas sequences behave similarly to expressions of the form $(\alpha^n - \beta^n)/(\alpha - \beta)$, so Zsigmondy-type results are expected. They exist, but the proofs are harder because α and β are in a quadratic number field.

The first general theorem in the real-root case goes back to Carmichael. Voutier notes that in the real case, work of Carmichael, Ward, and Durst implies that the nth term has a primitive divisor for $n > 12$ [Vou96]. We record a standard version for $U_n(P, Q)$.

Theorem 7.9 (Carmichael in the real-root case)**.** *Assume (4.1), assume $D = P^2 - 4Q > 0$, and assume $U_n(P, Q)$ is nondegenerate, as in Remark 3.2. Then $U_n(P, Q)$ has a primitive prime divisor for all $n > 12$, as in Definition 7.1.*

Remark 7.10. For Fibonacci, this implies that every F_n with $n > 12$ has a primitive prime divisor under Definition 7.1. Small indices show why a restriction is needed. We have $F_1 = 1$ and $F_2 = 1$, so there is no prime divisor. Also $F_6 = 8$ has only prime divisor 2, but 2 already divides $F_3 = 2$, so F_6 has no primitive prime divisor. Similarly, $F_{12} = 144$ has prime divisors 2 and 3, but both appear earlier. Carmichael's original work is [Car13].

The strongest general theorem for Lucas sequences is due to Bilu, Hanrot, and Voutier.

Theorem 7.11 (Bilu–Hanrot–Voutier)**.** *Assume $U_n(P, Q)$ is nondegenerate, as in Remark 3.2 and assume (4.1). Then for every $n > 30$, the term $U_n(P, Q)$ has a primitive prime divisor, as in Definition 7.1.*

Remark 7.12. Theorem 7.11 implies that for any fixed nondegenerate Lucas sequence, new primes appear regularly as n grows. In particular, only finitely many indices n can fail to have a primitive prime divisor. The proof is complex and uses lower bounds for linear forms in logarithms together with extensive case analysis [BHV01].

8. Examples and computations

This section gives two explicit types of second-order linear divisibility sequences. The goal is to make the definitions in Sections 5 and 7 feel more intuitive. In each example we list the first several terms, factor them, and point out at least one primitive prime divisor when it exists.

In the tables below, a prime p is called *primitive for U_n* if it is a primitive prime divisor, as in Definition 7.1. This means $p \mid U_n$ but p does not divide $D = P^2 - 4Q$ and it does not divide any earlier term $U_1, \dots, U_{n-1}$.

8.1. **Fibonacci numbers.** Take $(P, Q) = (1, -1)$, so $U_n(1, -1) = F_n$ is the Fibonacci sequence. Here $D = 5$. Because $5 \mid D$, the prime 5 is not counted as primitive in Definition 7.1.

Table 1 lists F_n for $2 \le n \le 16$. In the last column, we list one primitive prime divisor when it exists.

n	F_n	factorization of F_n	a primitive prime divisor of F_n
2	1	1	none
3	2	2	2
4	3	3	3
5	5	5	none (since $5 \mid D$)
6	8	2^3	none
7	13	13	13
8	21	$3 \cdot 7$	7
9	34	$2 \cdot 17$	17
10	55	$5 \cdot 11$	11
11	89	89	89
12	144	$2^4 \cdot 3^2$	none
13	233	233	233
14	377	$13 \cdot 29$	29
15	610	$2 \cdot 5 \cdot 61$	61
16	987	$3 \cdot 7 \cdot 47$	47

Table 1. Fibonacci numbers and primitive prime divisors (excluding primes dividing $D = 5$).

From the table, F_6 and F_{12} have no primitive prime divisor. Theorems 7.9 and 7.11 explain why this kind of failure only happens at small indices in nondegenerate Lucas sequences.

It is also useful to compute a few ranks of apparition. For Fibonacci, the rank $r(p)$ is the first index where p divides F_n. From the values above we see

$$r(2) = 3, \qquad r(3) = 4, \qquad r(7) = 8, \qquad r(11) = 10, \qquad r(13) = 7.$$

Lemma 5.2 says that once p appears at $r(p)$, it divides exactly those F_n with $r(p) \mid n$.

8.2. **Pell numbers.** Take $(P, Q) = (2, -1)$. Then $U_n(2, -1)$ is the Pell sequence. The discriminant is $D = 8$. Because $2 \mid D$, the prime 2 is excluded from being primitive in Definition 7.1.

Table 2 lists $U_n(2, -1)$ for $2 \le n \le 12$.

n	$U_n(2,-1)$	factorization	a primitive prime divisor
2	2	2	none (since $2 \mid D$)
3	5	5	5
4	12	$2^2 \cdot 3$	3
5	29	29	29
6	70	$2 \cdot 5 \cdot 7$	7
7	169	13^2	13
8	408	$2^3 \cdot 3 \cdot 17$	17
9	985	$5 \cdot 197$	197
10	2378	$2 \cdot 29 \cdot 41$	41
11	5741	5741	5741
12	13860	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	11

TABLE 2. Pell numbers $U_n(2, -1)$ and primitive prime divisors (excluding primes dividing $D = 8$).

The ranks of apparition are easy to read from Table 2. For example,

$$r(3) = 4, \qquad r(5) = 3, \qquad r(7) = 6, \qquad r(13) = 7, \qquad r(17) = 8, \qquad r(29) = 5.$$

So Lemma 5.2 predicts that 7 divides $U_n(2, -1)$ exactly when $6 \mid n$. This agrees with the table since 7 first appears at $U_6 = 70$ and it divides $U_{12} = 13860$.

Remark 8.1. These examples show the general behavior of such sequences. Divisibility in the indices impose a strong constraint in the prime factors of U_n. Primitive prime divisors are a direct way to see that new primes appear. Proposition 5.6 explains why the appearance of a primitive prime divisor at index m often leads to the converse $U_m \mid U_n \Rightarrow m \mid n$.

9. p-ADIC VALUATIONS AND HIGHER DIVISIBILITY

This section changes the question "when does p divide U_n" and makes it more detailed. Rather than only asking if p divides U_n, we ask how many powers of p divide U_n. This leads to the p-adic valuation.

A basic idea in this section is the following. If a prime p shows up in a Lucas sequence, then higher powers of p often show up later, and the indices where this happens often follow a pattern. For Fibonacci and several related Lucas sequences, this gives strong divisibility patterns for the tiling counts in Section 10.

Throughout this section we assume $\gcd(P, Q) = 1$ and $Q \neq 0$. We write $U_n = U_n(P, Q)$ and $D = P^2 - 4Q$.

9.1. The p-adic valuation.

Definition 9.1. Let p be a prime and let N be an integer. If $N \neq 0$, the *p-adic valuation* $v_p(N)$ is the largest integer $e \ge 0$ such that p^e divides N. We also set $v_p(0) = +\infty$.

The statement $p^e \mid N$ means the same thing as $v_p(N) \geq e$. So $v_p(N)$ measures divisibility by powers of p.

Here is a quick way to read it. If $v_p(N) = 0$, then p does not divide N. If $v_p(N) = 1$, then p divides N but p^2 does not. If $v_p(N) = 3$, then p^3 divides N and p^4 does not.

9.2. **Ranks and first appearance.** In Section 5 we defined the rank of apparition. We recall the notation here.

Definition 9.2. Let p be a prime. Assume there exists $n \geq 1$ such that $p \mid U_n$. The least such n is the *rank of apparition* of p, denoted $r(p)$.

When $p \mid Q$, Lemma 4.1 implies that $p \nmid U_n$ for all $n \geq 1$. So from now on we only consider primes p with $p \nmid Q$.

9.3. **A valuation law for Lucas sequences.** Sanna gives a complete and explicit description of $v_p(U_n)$ for nondegenerate Lucas sequences [San16]. We state a version in the notation of this paper, for primes $p \geq 3$.

There are two main situations. One is when $p \mid D$. The other is when $p \nmid D$. These two cases already looked different in our modular discussion in Section 6.

Theorem 9.3 (Sanna's valuation formulas for $p \geq 3$)**.** *Assume $U_n(P, Q)$ is nondegenerate and let $p \geq 3$ be a prime with $p \nmid Q$. Then for every $n \geq 1$,*

$$v_p(U_n) = \begin{cases} 0 & \text{if } p \mid D \text{ and } p \nmid n, \\ v_p(n) + v_p(U_p) - 1 & \text{if } p \mid D \text{ and } p \mid n, \\ 0 & \text{if } p \nmid D \text{ and } r(p) \nmid n, \\ v_p(n) + v_p(U_{r(p)}) & \text{if } p \nmid D \text{ and } r(p) \mid n. \end{cases}$$

Remark 9.4. Theorem 9.3 does two important things.

First, it gives back the basic rank rule from Section 5. If $p \nmid D$, then p divides U_n exactly when $r(p)$ divides n.

Second, it tells us about higher powers. If $p \nmid D$ and $r(p) \mid n$, then the number of extra factors of p in U_n is controlled by two parts. One part is $v_p(U_{r(p)})$, which comes from the first time p appears. The other part is $v_p(n)$, which comes from how many factors of p are already in the index.

Remark 9.5. We only stated Sanna's formulas for primes $p \geq 3$. The case $p = 2$ has extra subcases, and it often behaves differently in second-order recurrences.

Remark 9.6. Theorem 9.3 is a restatement of results in [San16]. Ballot studies related valuation behavior, including cases where the parameters force unusual behavior modulo p [Bal19]. Ballot uses the phrase "special prime" in a different way than just the condition $p \mid D$. Also, our standing assumption $\gcd(P, Q) = 1$ removes some parameter choices that Ballot discusses.

When $p \geq 5$ and $p \mid D$, Sanna proves that $v_p(U_p) = 1$. This makes the $p \mid D$ case much simpler, since the valuation depends only on $v_p(n)$.

Corollary 9.7 (Sanna, $p \mid D$ case for $p \geq 5$)**.** *Assume $U_n(P, Q)$ is nondegenerate and let $p \geq 5$ be a prime with $p \mid D$ and $p \nmid Q$. Then for every $n \geq 1$,*

$$v_p(U_n) = v_p(n).$$

Equivalently,

$$v_p(U_n) = \begin{cases} v_p(n) & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n. \end{cases}$$

Remark 9.8. Corollary 9.7 says that in the case $p \mid D$ and $p \geq 5$, the sequence does not add extra powers of p beyond what is already in the index. If n is not divisible by p, then U_n is not divisible by p. If n is divisible by p^k but not by p^{k+1}, then U_n is divisible by p^k but not by p^{k+1}.

9.4. **Divisibility at predictable indices.** Theorem 9.3 quickly gives a family of indices where large powers of p must divide U_n.

Proposition 9.9. *Assume $U_n(P,Q)$ is nondegenerate and let $p \geq 3$ be a prime with $p \nmid QD$. Let $r = r(p)$ and let $a = v_p(U_r)$. Then for every integer $k \geq 0$,*

$$p^{a+k} \mid U_{rp^k}.$$

Proof. We apply Theorem 9.3 with $n = rp^k$. Since $p \nmid D$ and $r \mid n$, the theorem gives

$$v_p(U_{rp^k}) = v_p(rp^k) + v_p(U_r).$$

Also $v_p(rp^k) = v_p(r) + k$. So

$$v_p(U_{rp^k}) = v_p(r) + k + a.$$

In particular, $v_p(U_{rp^k}) \geq a + k$. This is the same as saying p^{a+k} divides U_{rp^k}. □

Remark 9.10. The number $a = v_p(U_r)$ measures how strongly p divides its first appearance. In many examples, p divides U_r only once, so $a = 1$. One common situation is when p is a primitive prime divisor of U_r. Then Proposition 9.9 becomes

$$p^{k+1} \mid U_{rp^k} \quad \text{for all } k \geq 0.$$

9.5. **Two quick examples.** These examples are only here to show how to use the formulas.

Example 9.11. For the Fibonacci sequence we have $U_n(1,-1) = F_n$ and $D = 5$. Take $p = 5$. Then $p \mid D$, so Corollary 9.7 applies and gives

$$v_5(F_n) = v_5(n) \quad \text{for all } n \geq 1.$$

For instance, $v_5(F_{10}) = v_5(10) = 1$, and indeed $F_{10} = 55$ is divisible by 5 but not by 25. Also $v_5(F_{25}) = v_5(25) = 2$, and indeed $F_{25} = 75025$ is divisible by 25.

Example 9.12. Again take Fibonacci, and now take $p = 3$. Here $p \nmid D$. We have $F_4 = 3$, so $r(3) = 4$ and $a = v_3(F_4) = 1$. Proposition 9.9 implies

$$3^{k+1} \mid F_{4 \cdot 3^k} \quad \text{for all } k \geq 0.$$

For example, when $k = 1$ this says $3^2 \mid F_{12}$, and indeed $F_{12} = 144$ is divisible by 9.

9.6. **Connection to weighted grid tilings.** In Section 10 we build a model where, for many choices with $Q < 0$, the term $U_{n+1}(P,Q)$ is a weighted count of tilings of a $2 \times n$ grid. In that setting, the condition $v_p(U_{n+1}(P,Q)) \geq k$ means that the weighted tiling total is divisible by p^k.

For Fibonacci, $U_{n+1}(1,-1) = F_{n+1}$ counts the domino tilings of a $2 \times n$ rectangle. So Proposition 9.9 gives infinitely many board sizes n where the number of tilings is divisible by large powers of a fixed prime.

10. Grid combinatorics, lattice paths, and state graphs

In this section we model second-order recurrences using grid objects. The main examples are domino tilings of a $2 \times n$ rectangle and perfect matchings of the associated $2 \times n$ grid graph. These models make it easier to see why Fibonacci, Pell, and other Lucas-type sequences satisfy second-order recurrences.

These models also connect naturally to reduction modulo primes. The update rule for the recurrence acts on a finite set of states, namely the $p \times p$ grid $\mathbb{F}_p^2$. So periodicity and ranks can be pictured using a finite directed graph.

10.1. **Domino tilings of a $2 \times n$ grid and Fibonacci.**

Definition 10.1. A *domino* is a 1×2 rectangle or a 2×1 rectangle. A *domino tiling* of a $2 \times n$ rectangle is a covering by dominoes with no overlap and no gaps.

Let T_n be the number of domino tilings of the $2 \times n$ rectangle. We use the convention $T_0 = 1$, since the empty board has exactly one tiling. It is standard that (T_n) satisfies the Fibonacci recurrence [BenQui03, MathWorldDomino, Bel23].

Proposition 10.2. *For $n \geq 2$,*

$$T_n = T_{n-1} + T_{n-2}, \qquad T_n = F_{n+1}.$$

Proof. Look at the top left square of the rectangle.

If it is covered by a vertical domino, then that domino also covers the bottom left square. Removing it leaves a $2 \times (n-1)$ rectangle, which can be tiled in T_{n-1} ways.

If it is covered by a horizontal domino, then the bottom left square cannot be covered vertically. So it must also be covered by a horizontal domino. This forces a 2×2 block of two horizontal dominoes in the first two columns. Removing that block leaves a $2 \times (n-2)$ rectangle, which can be tiled in T_{n-2} ways.

These are the only possibilities, and they do not overlap. So $T_n = T_{n-1} + T_{n-2}$ for $n \geq 2$. With $T_0 = 1$ and $T_1 = 1$, this matches the Fibonacci recurrence shifted by one index. Therefore $T_n = F_{n+1}$. □

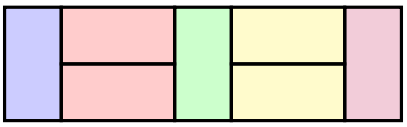


FIGURE 1. A domino tiling of a 2×7 rectangle.

10.2. **A weighted $2 \times n$ model for $U_{n+1}(P,Q)$ when $Q < 0$.** Proposition 10.2 already gives a second-order recurrence. We now build a weighted model that matches the Lucas sequence $U_{n+1}(P,Q)$ when $Q < 0$. If $Q < 0$, then $-Q > 0$, which helps if we want nonnegative weights.

Definition 10.3. Fix integers P, Q. A *weighted domino tiling* of a $2 \times n$ rectangle is a domino tiling where we assign weights like this.

A vertical domino has weight P.

Two horizontal dominoes that fill a 2×2 block have weight $-Q$.

The weight of a tiling is the product of the weights of all blocks in the tiling. Let $W_n(P,Q)$ be the sum of the weights of all tilings of a $2 \times n$ rectangle.

Remark 10.4. In a $2 \times n$ rectangle, horizontal dominoes always occur in pairs. A single horizontal domino creates a mismatch that must be fixed by another horizontal domino directly below it. So it is natural to treat the pair as one 2×2 block.

Theorem 10.5. *For every integer $n \geq 0$,*

$$W_n(P,Q) = U_{n+1}(P,Q).$$

If $Q < 0$ and $P \geq 0$, then all block weights are nonnegative. So in that case $U_{n+1}(P,Q)$ can be seen as a weighted counting function on a grid.

Proof. We show that (W_n) satisfies the same recurrence and the same starting values as (U_{n+1}).

First we check the starting values. For $n = 0$ there is one empty tiling, so $W_0 = 1$. Also $U_1 = 1$, so $W_0 = U_1$. For $n = 1$ the only tiling uses one vertical domino, so $W_1 = P$. Also $U_2 = P$, so $W_1 = U_2$.

Next we check the recurrence. Let $n \geq 2$. Every tiling begins with exactly one of the following choices in the leftmost columns.

Either it begins with a vertical domino. This contributes a factor of P and leaves a $2 \times (n-1)$ rectangle. So these tilings contribute $P\,W_{n-1}$ in total.

Or it begins with a 2×2 block of two horizontal dominoes. This contributes a factor of $-Q$ and leaves a $2 \times (n-2)$ rectangle. So these tilings contribute $(-Q)\,W_{n-2}$ in total.

Adding the two disjoint cases gives

$$W_n = PW_{n-1} + (-Q)W_{n-2} = PW_{n-1} - QW_{n-2}.$$

This is the recurrence for U_{n+1}, and the starting values match. So $W_n = U_{n+1}$ for all $n \geq 0$. □

10.3. **A grid proof of the addition formula.** The addition formula in Section 3 can also be proved by cutting a grid. This gives a geometric reason for why an identity like

$$U_{m+n} = U_m U_{n+1} - Q\,U_{m-1}U_n$$

should hold.

Proposition 10.6. *For all integers $m, n \geq 1$,*

$$U_{m+n} = U_m U_{n+1} - Q\,U_{m-1}U_n.$$

Proof. We first prove the identity assuming $Q < 0$, so that we can use the weighted tiling model from Theorem 10.5.

Both sides are polynomials in P and Q with integer coefficients. This can be seen by building $U_k(P, Q)$ from the recurrence. So it is enough to prove the identity for infinitely many integer values of Q. Negative integers give infinitely many choices, so proving it for all $Q < 0$ is enough. Then the identity holds for all integers P, Q.

Now assume $Q < 0$. By Theorem 10.5, the number U_{m+n} equals the total weight of all tilings of a $2 \times (m+n-1)$ rectangle.

Cut this rectangle between columns $m-1$ and m. A tiling falls into exactly one of two cases.

Case 1. No 2×2 horizontal block crosses the cut. Then the tiling splits into a tiling of the left $2 \times (m-1)$ rectangle and a tiling of the right $2 \times n$ rectangle. So the total weight in this case is

$$W_{m-1}(P, Q)\,W_n(P, Q) = U_m U_{n+1}.$$

Case 2. A 2×2 horizontal block crosses the cut. Remove that crossing block. What remains is a tiling of the left $2 \times (m-2)$ rectangle and a tiling of the right $2 \times (n-1)$ rectangle. The removed block contributes a factor of $-Q$. So the total weight in this case is

$$(-Q)\,W_{m-2}(P, Q)\,W_{n-1}(P, Q) = (-Q)\,U_{m-1}U_n.$$

Adding the two cases gives

$$U_{m+n} = U_m U_{n+1} + (-Q)U_{m-1}U_n = U_m U_{n+1} - Q\,U_{m-1}U_n.$$

□

10.4. **Perfect matchings of the $2 \times n$ grid graph.** Tilings can also be described using matchings in a graph. This is a standard viewpoint and it is helpful when we want to generalize to other regions.

Definition 10.7. Let $G_{2,n}$ be the cell adjacency graph of the $2 \times n$ grid. Its vertices are the $2n$ unit squares. Two vertices are connected by an edge if the corresponding squares share a side.

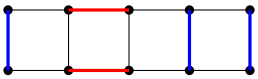
A *perfect matching* in $G_{2,n}$ is a set of edges so that every vertex is used exactly once.

A domino tiling of a $2 \times n$ rectangle gives the same information as a perfect matching of $G_{2,n}$ [MathWorldDomino, Bel23].

Proposition 10.8. *Domino tilings of a $2 \times n$ rectangle are in bijection with perfect matchings of $G_{2,n}$.*

Proof. Given a domino tiling, each domino covers two adjacent unit squares. Draw the edge in $G_{2,n}$ connecting those two squares. Different dominoes cover different squares, so the edges share no vertices. Every square is covered once, so every vertex is used once. So these edges form a perfect matching.

Conversely, given a perfect matching, each matching edge connects two adjacent squares. Place a domino covering that pair. Since every vertex is used exactly once, the dominoes cover the whole rectangle with no overlaps and no gaps. □



A perfect matching in $G_{2,5}$

FIGURE 2. A perfect matching picture for a 2×5 grid.

10.5. **Lattice paths and a binomial sum.** Tiling models often lead to binomial sums. A quick way to see the binomial coefficients is to encode a tiling by a path that records whether we used a 1-column block or a 2-column block.

Definition 10.9. A *step path* to length $n-1$ is a path in the plane that starts at $(0,0)$ and uses only the steps

$$S = (1,0), \qquad D = (2,0),$$

and ends at $(n-1,0)$.

If a path uses k steps of type D, then those steps cover horizontal distance $2k$. So the path must use $n-1-2k$ steps of type S to reach total distance $n-1$. The total number of steps is then

$$k + (n-1-2k) = n-1-k.$$

Choosing which k of these $n-1-k$ steps are the long steps D gives $\binom{n-1-k}{k}$ paths.

Proposition 10.10. *For every integer $n \geq 1$,*

$$U_n(P,Q) = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} P^{n-1-2k} (-Q)^k.$$

Proof. By Theorem 10.5, we have $U_n(P,Q) = W_{n-1}(P,Q)$. So we count weighted tilings of a $2 \times (n-1)$ rectangle.

Fix an integer $k \geq 0$. A tiling that uses k horizontal 2×2 blocks uses up $2k$ columns. The remaining $n-1-2k$ columns must be filled by vertical dominoes.

Now record the tiling from left to right. Write D for each 2×2 horizontal block and write S for each vertical column. This gives a word with k letters D and $n-1-2k$ letters S. The total number of blocks is $k + (n-1-2k) = n-1-k$, so the number of such words is $\binom{n-1-k}{k}$.

Each S contributes a factor P and each D contributes a factor $-Q$. So each such tiling has weight $P^{n-1-2k}(-Q)^k$. Summing over all possible k gives the formula. □

10.6. **Transfer matrices and weighted walks.** The companion matrix

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$$

showed up earlier in the algebra part of the paper. It also shows up in combinatorics as a transfer matrix. In this viewpoint, a recurrence comes from weighted walks on a small directed graph [BHS03].

Definition 10.11. Let G be a directed graph with vertex set $\{1, 2\}$. Assume each directed edge $i \to j$ has a weight $w(i \to j)$ in a commutative ring. A *walk* of length n is a sequence of vertices $(v_0, v_1, \ldots, v_n)$ such that there is an edge $v_{t-1} \to v_t$ for each t. The weight of the walk is the product of its edge weights.

Proposition 10.12. *Consider the directed graph on vertices* $\{1, 2\}$ *with edge weights*

$$1 \to 1 \text{ has weight } P, \qquad 1 \to 2 \text{ has weight } -Q, \qquad 2 \to 1 \text{ has weight } 1,$$

and no other edges. Then the total weight of walks of length n *from vertex* 2 *to vertex* 1 *equals* $U_n(P, Q)$.

Proof. Let A be the weighted adjacency matrix. This means $A_{i,j}$ is the total weight of all edges from i to j. By construction,

$$A = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} = M.$$

A standard matrix multiplication argument shows that $(A^n)_{i,j}$ equals the total weight of walks of length n from i to j. Each multiplication by A adds one more step, and the sum over intermediate vertices matches the choice of the next vertex in a walk.

By Proposition 3.5, we have $(M^n)_{2,1} = U_n$. So the total weight of length n walks from 2 to 1 is $U_n(P, Q)$. □

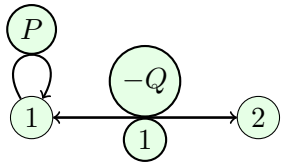


FIGURE 3. A two vertex transfer graph whose walk weights produce $U_n(P, Q)$.

10.7. **State grids modulo p, cycles, and ranks.** In Section 6 we studied the state

$$S_n = (U_{n+1}, U_n) \in \mathbb{F}_p^2$$

and the update rule

$$T(x, y) = (Px - Qy,\ x).$$

The state space $\mathbb{F}_p^2$ is a $p \times p$ grid of points. The map T sends each point to exactly one next point.

When $p \nmid Q$, Proposition 6.6 implies that T is a bijection. There is also a quick reason. The update rule is multiplication by the matrix M modulo p, and $\det(M) = Q$. So if $p \nmid Q$, then $\det(M) \not\equiv 0 \pmod{p}$, which means M is invertible over $\mathbb{F}_p$. So T permutes the p^2 points.

Because every state has exactly one outgoing arrow and exactly one incoming arrow, the directed graph of arrows is a disjoint union of directed cycles.

Proposition 10.13. *Assume* $p \nmid Q$. *Let* $\pi(p)$ *be the period of* $(U_n \bmod p)$ *from Proposition 6.6. If the rank of apparition* $r(p)$ *exists, then* $r(p)$ *divides* $\pi(p)$.

Proof. Since $p \nmid Q$, the state sequence (S_n) is periodic from the start with period $\pi(p)$. So $S_{n+\pi(p)} = S_n$ for all $n \geq 0$.

Assume $r(p)$ exists. Then $U_{r(p)} \equiv 0 \pmod{p}$, so

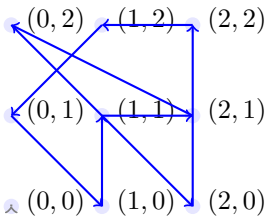
$$S_{r(p)} = (U_{r(p)+1}, 0)$$

lies on the horizontal axis of the state grid.

Because the orbit repeats with period $\pi(p)$, we have $S_{r(p)+\pi(p)} = S_{r(p)}$. In particular, $U_{r(p)+\pi(p)} \equiv 0 \pmod{p}$. So $r(p) + \pi(p)$ is another index where the sequence hits 0 modulo p.

By Lemma 5.2, the indices n such that $U_n \equiv 0 \pmod{p}$ are exactly the multiples of $r(p)$. So $r(p)$ divides $r(p) + \pi(p)$. This implies $r(p)$ divides $\pi(p)$. □

The next picture shows the full 3×3 state grid for Fibonacci modulo 3. In this case, there is one fixed point at $(0, 0)$ and one cycle containing the other eight points.



Fibonacci update map $T(x, y) = (x + y, x)$ modulo 3

FIGURE 4. The state grid modulo 3 decomposes into cycles.

This grid picture supports the divisibility ideas from earlier sections. The rank $r(p)$ is the first positive time when the orbit hits the axis $y = 0$. Strong divisibility then helps explain why this axis hit repeats at exactly the multiples of the first hit.

10.8. **A billiards connection.** There are also geometric models where a grid and the Euclidean algorithm show up together. One example comes from billiards in a square. A standard trick is to unfold reflections, which turns a bouncing path into a straight line in a reflected grid. This makes gcd computations show up naturally, and it can produce Fibonacci type patterns in families of allowed slopes, see [Jaud19].

A different billiards style construction that produces Fibonacci chains is studied by Berlekamp and Guy [BerGuy20]. These viewpoints are not needed for the main results in this paper. They fit the same theme, since grid motion, gcd steps, and second-order recurrences often show up together.

REFERENCES

[Bal19] C. Ballot, *The p-adic valuation of Lucas sequences when p is a special prime*, Fibonacci Quart. **57** (2019), no. 3, 265–275.

[Bel23] S.-M. Belcastro, *Domino Tilings of $2 \times n$ Grids (or Perfect Matchings of Grid Graphs) on Surfaces*, J. Integer Seq. **26** (2023), Article 23.5.6.

[BenQui99] A. T. Benjamin and J. J. Quinn, *Recounting Fibonacci and Lucas identities*, College Math. J. **30** (1999), no. 5, 359–366.

[BenQui03] A. T. Benjamin and J. J. Quinn, *Proofs That Really Count: The Art of Combinatorial Proof*, Dolciani Mathematical Expositions, vol. 27, Mathematical Association of America, Washington, DC, 2003.

[BG21] M. Broderius and J. Greene, *Lucas sequences containing few primes*, Fibonacci Quart. **59** (2021), no. 2, 136–144.

[BHV01] Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers* (with an appendix by M. Mignotte), J. Reine Angew. Math. **539** (2001), 75–122.

[BHS03] A. T. Benjamin, C. R. H. Hanusa, and F. E. Su, *Linear recurrences through tilings and Markov chains*, Utilitas Math. **64** (2003), 45–63.

[BirVan04] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. (2) **5** (1904), no. 4, 173–180.
[BerGuy20] E. Berlekamp and R. K. Guy, *Fibonacci Plays Billiards*, arXiv:2002.03705, 2020.
[Car13] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **15** (1913–1914), 30–70.
[Des78] J. E. Desmond, *On the existence of the rank of apparition of m in the Lucas sequence*, Fibonacci Quart. **16** (1978), no. 1, 7–10.
[Jar05] J. H. Jaroma, *On the appearance of primes in linear recursive sequences*, Adv. Difference Equ. **2005** (2005), no. 2, 145–151.
[Jaud19] D. Jaud, *Playing a game of billiard with Fibonacci*, arXiv:1906.01911, 2019.
[Leh30] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448.
[MathWorldDomino] E. W. Weisstein, *Domino Tiling*, MathWorld–A Wolfram Resource. Available at `https://mathworld.wolfram.com/DominoTiling.html`.
[San16] C. Sanna, *The p-adic valuation of Lucas sequences*, Fibonacci Quart. **54** (2016), no. 2, 118–124.
[Szi17] M. Szikszai, *Distinct products in Lucas sequences on a problem of Kimberling*, Fibonacci Quart. **55** (2017), no. 4, 291–296.
[Vou96] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences, II*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 251–274.
[Wal60] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), no. 6, 525–532.
[War33] M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. **35** (1933), no. 3, 600–628.
[War37] M. Ward, *Linear divisibility sequences*, Trans. Amer. Math. Soc. **41** (1937), no. 2, 276–286.
[Zsi92] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte für Math. und Phys. **3** (1892), 265–284.