# Divisibility Sequences

Devin Li

Euler Circle

July 12, 2026

# Motivation and structure

## Motivation

- I like number theory, especially modular arithmetic and divisibility.
- Divisibility sequences basically capture everything I like about number theory.

## Structure

- I will build up results about divisibility sequences, then move to Lucas sequences.
- I will focus on the main ideas and examples, not full proofs.
- Please save questions for the end since we have limited time.

# Divisibility sequence

**Definition**

An integer sequence $(a_n)_{n\geq 1}$ is a divisibility sequence if

$$m \mid n \Rightarrow a_m \mid a_n.$$

What this means in practice

- divisibility in the indices leads to divisibility in the terms
- prime factors repeat along multiples of an index

# Strong divisibility sequence

**Definition**

An integer sequence $(a_n)_{n\geq 1}$ is strong divisibility if

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

Two quick consequences

- strong divisibility implies divisibility
- gcd computations become index gcd computations

# Warm up example: $b^n - 1$

Fix $b \geq 2$ and set $a_n = b^n - 1$.

If $n = km$, then

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

so $a_m \mid a_n$.

Takeaway

- powers behave well on multiples
- Lucas sequences have a closed form that also involves powers

# Second-order recurrences

We study

$$a_{n+2} = Pa_{n+1} - Qa_n \qquad (P, Q \in \mathbb{Z}).$$

Two initial values determine the whole sequence.

Characteristic polynomial and discriminant

$$f(x) = x^2 - Px + Q, \qquad D = P^2 - 4Q.$$

Next we choose special initial values and get Lucas sequences.

# Lucas sequences $U_n(P, Q)$ and $V_n(P, Q)$

$$U_0 = 0, \quad U_1 = 1, \quad U_{n+2} = PU_{n+1} - QU_n.$$
$$V_0 = 2, \quad V_1 = P, \quad V_{n+2} = PV_{n+1} - QV_n.$$

Examples

- Fibonacci is $U_n(1, -1)$
- Pell is $U_n(2, -1)$

# Assumptions you will see repeatedly

Most clean gcd statements assume

$$Q \neq 0, \qquad \gcd(P, Q) = 1.$$

Quick reason

- if $Q = 0$, the recurrence becomes closer to a one step rule
- if $\gcd(P, Q) \neq 1$, extra common factors can appear in many terms

Now we write down the closed form and the main identities.

# Closed forms and why we care

Let $\alpha, \beta$ be the roots of $x^2 - Px + Q$. If $\alpha \neq \beta$, then

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

This is the link to the warm up example. It is a difference of powers.

# Matrices

Define

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

Then

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

Also

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

Next we use this to get two identities that drive the gcd arguments.

# Two identities we keep using

Addition formula

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

Cassini type identity

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

Now we switch from identities to divisibility and gcd structure.

# Divisibility theorem for $U_n$

**Theorem**

*If $m \mid n$, then $U_m \mid U_n$.*

Proof outline

- write $n = km$
- express $U_{km}$ as a matrix entry of $(M^m)^k$
- that entry satisfies a recurrence in $k$ with first nonzero term $U_m$
- induction in $k$ shows $U_m$ divides $U_{km}$

# Strong gcd theorem for $U_n$

Assume $Q \neq 0$ and $\gcd(P, Q) = 1$.

**Theorem**

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

Proof outline

- Cassini gives $\gcd(U_n, U_{n+1}) = 1$
- the addition formula gives the Euclidean step

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

- repeat the Euclidean step as in the Euclidean algorithm on $(m, n)$

Next we use this gcd rule to control primes in the sequence.

# Rank of apparition

Let $p$ be a prime. If $p \mid U_n$ for some $n$, define

$$r(p) = \min\{n \geq 1 \mid p \mid U_n\}.$$

Strong divisibility gives the repetition law

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

To study $r(p)$, we look at the sequence modulo $p$.

# What is a field

We work mod $p$ inside the field $\mathbb{F}_p$.

**Field idea**

A field is a set where you can add, subtract, multiply, and divide by any nonzero element.

For a prime $p$,

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

with arithmetic done modulo $p$. Every nonzero element has an inverse because $p$ is prime.

# States mod $p$

A second-order recurrence is determined by two consecutive terms. So we define the state

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

Update rule

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

There are only $p^2$ states, so the state sequence must repeat.

# Why $p \nmid Q$ gives periodicity from the start

If $p \nmid Q$, then

$$\det(M) = Q \not\equiv 0 \pmod{p},$$

so $M$ is invertible over $\mathbb{F}_p$. That makes $T$ a bijection on the finite set $\mathbb{F}_p^2$.

A bijection on a finite set is a disjoint union of cycles. So the orbit of $S_0 = (1, 0)$ is a cycle. That means $(U_n \bmod p)$ is periodic starting at $n = 0$.

# Law of apparition

Let $p$ be an odd prime and let

$$\varepsilon(p) = \left(\frac{D}{p}\right)$$

be the Legendre symbol of the discriminant.

**Theorem**

*If $p \nmid QD$ and the rank $r(p)$ exists, then*

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

So usually $r(p) \mid p - 1$ or $r(p) \mid p + 1$.

# Primitive prime divisors

A prime $p$ is primitive for $U_n$ if

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

Two uses

- primitive at $n$ means $r(p) = n$
- if $U_m$ has a primitive prime divisor and $U_m \mid U_n$, then $m \mid n$

# Why primitive primes exist for large $n$

Zsigmondy says new primes appear in $a^n - b^n$ for all $n \geq 2$ except a short list.

For Lucas sequences there are many properties.

- Carmichael gives primitive primes in many cases once $n > 12$
- Bilu, Hanrot, and Voutier prove a uniform result

$$n > 30 \Rightarrow U_n(P, Q) \text{ has a primitive prime divisor}$$

for nondegenerate sequences

# Example: Fibonacci

Fibonacci is $U_n(1,-1)$ and $D = 5$, so 5 is excluded from primitiveness.

| $n$ | $F_n$ | factorization | one primitive prime |
|---|---|---|---|
| 3 | 2 | 2 | 2 |
| 4 | 3 | 3 | 3 |
| 5 | 5 | 5 | none $(5 \mid D)$ |
| 6 | 8 | $2^3$ | none |
| 7 | 13 | 13 | 13 |
| 8 | 21 | $3 \cdot 7$ | 7 |
| 10 | 55 | $5 \cdot 11$ | 11 |
| 12 | 144 | $2^4 \cdot 3^2$ | none |

Next we read ranks from this table.

# Ranks in Fibonacci

From small values

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

Example

- $7 \mid F_n$ exactly when $8 \mid n$
- one piece of data replaces infinitely many checks

Now we move from primes to prime powers.

# $p$-adic valuation

For a prime $p$ and $N \neq 0$, $v_p(N)$ is the largest $e$ with $p^e \mid N$.

This refines the question $p \mid U_n$. We ask how large $v_p(U_n)$ can be.

# Sanna's valuation formula in a common case

Assume $p \geq 3$ and $p \nmid QD$. Let $r = r(p)$ be the rank of apparition. Then Sanna proves *(in this case)* that for every $n \geq 1$,

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

So extra factors of $p$ in the index usually produce extra factors of $p$ in the term.

# A higher-power repetition pattern

Assume $p \geq 3$ and $p \nmid QD$. Let $r = r(p)$ and $a = v_p(U_r)$. Then for every $k \geq 0$,

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

This is a prime power version of the repetition law.

# Domino tilings and Fibonacci

Let $T_n$ be the number of domino tilings of a $2 \times n$ rectangle, and set $T_0 = 1$.

Leftmost column argument

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

So Fibonacci numbers count $2 \times n$ tilings. Next we weight the tiles to match $U_{n+1}(P, Q)$.

# Weighted tilings for $U_{n+1}(P, Q)$ when $Q < 0$

Model on a $2 \times n$ rectangle:

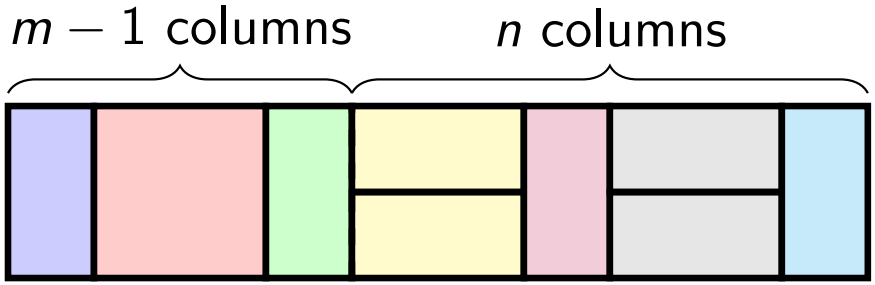
- a vertical domino has weight $P$
- a $2 \times 2$ horizontal block has weight $-Q$

Total weight over all tilings is

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

Now a cut in the grid explains the addition formula.

# Cut diagram for the addition formula




Rectangle is $2 \times (m+n-1)$, cut between columns $m-1$ and $m$.

# Addition formula from cutting

Addition formula

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

Two cases in the weighted grid model:

- no $2 \times 2$ block crosses the cut, contribution is $U_m U_{n+1}$
- one $2 \times 2$ block crosses, remove it and pick up a factor $-Q$, contribution is $-Q\, U_{m-1} U_n$

Add the two contributions to get the identity.

# Where to go next

- classify which recurrences produce divisibility sequences
- understand how $r(p)$ and periods behave as $p$ varies
- improve bounds and exception lists for primitive prime divisors
- study primes dividing the discriminant, where valuation behavior changes

Thank you for listening.