Mordell-Lang Questions

Thomas J. Tucker
Linear recurrence sequences

We say a sequence of complex numbers \( \{a_n\}_{n=0}^{\infty} \) is a *linear recurrence sequence* if there is a positive integer \( r \) and complex numbers \( \lambda_1, \ldots, \lambda_r \) such that for all \( i \geq 0 \) we have

\[
a_{i+r} = \lambda_1 a_i + \cdots + \lambda_r a_{i+r-1}.
\]

Skolem, Mahler, and Lech proved the following theorem.

**Theorem**

For any linear recurrence sequence \( \{a_n\}_{n=0}^{\infty} \) and any complex number \( \beta \), the set of \( n \) such that \( a_n = \beta \) is a (possibly empty) finite union of arithmetic progressions of integers.

An arithmetic sequence of integers is a sequence of integers \( k, k+m, k+2m, \ldots, k+\ell m, \ldots \) for some integers \( k \) and \( \ell \).

"Singleton sequences", those where \( m = 0 \), are allowed.
Linear recurrence sequences

We say a sequence of complex numbers \( \{a_n\}_{n=0}^{\infty} \) is a linear recurrence sequence if there is a positive integer \( r \) and complex numbers \( \lambda_1, \ldots, \lambda_r \) such that for all \( i \geq 0 \) we have

\[
a_{i+r} = \lambda_1 a_i + \cdots + \lambda_r a_{i+r-1}.
\]

Skolem, Mahler, and Lech proved the following theorem.

**Theorem**

*For any linear recurrence sequence \( \{a_n\}_{n=0}^{\infty} \) and any complex number \( \beta \), the set of \( n \) such that \( a_n = \beta \) is a (possibly empty) finite union of arithmetic progressions of integers.*
Linear recurrence sequences

We say a sequence of complex numbers \( \{a_n\}_{n=0}^{\infty} \) is a *linear recurrence sequence* if there is a positive integer \( r \) and complex numbers \( \lambda_1, \ldots, \lambda_r \) such that for all \( i \geq 0 \) we have

\[
a_{i+r} = \lambda_1 a_i + \cdots + \lambda_r a_{i+r-1}.
\]

Skolem, Mahler, and Lech proved the following theorem.

**Theorem**

For any linear recurrence sequence \( \{a_n\}_{n=0}^{\infty} \) and any complex number \( \beta \), the set of \( n \) such that \( a_n = \beta \) is a (possibly empty) finite union of arithmetic progressions of integers.

An *arithmetic sequence* of integers is a sequence of integers

\[
k, k + m, k + 2m, \ldots, k + \ell m, \ldots
\]

“Singleton sequences”, those where \( m = 0 \), are allowed.
Sketch of proof of Skolem-Mahler-Lech

With a little work, the values of a linear recurrence sequence can be converted into a problem from linear algebra. That is, we have
Sketch of proof of Skolem-Mahler-Lech

With a little work, the values of a linear recurrence sequence can be converted into a problem from linear algebra. That is, we have

- A “starting point” \( z \in \mathbb{C}^r \) (coming from \( a_0, \ldots, a_{r-1} \))
- An \( r \times r \) matrix \( A \).
- A hyperplane \( V \subseteq \mathbb{C}^r \).
- With \( a_n = \beta \iff A^n(z) \in V \).
Sketch of proof of Skolem-Mahler-Lech

With a little work, the values of a linear recurrence sequence can be converted into a problem from linear algebra. That is, we have

- A “starting point” \( z \in \mathbb{C}^r \) (coming from \( a_0, \ldots, a_{r-1} \))
- An \( r \times r \) matrix \( A \).
- A hyperplane \( V \subseteq \mathbb{C}^r \).
- With \( a_n = \beta \iff A^n(z) \in V \).

Hence, the problem is essentially dynamical, dealing with iterations of linear transformation. A simple proof of the Skolem-Mahler-Lech theorem then comes from taking \( p \)-adic logarithms of a suitable power of \( A \).
Let’s just do one very simple example.

**Example**

Let \( A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix} \) and let \( s = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \).
Let’s just do one very simple example.

Example

Let $A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$ and let $s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Let $V$ be the subspace consisting of all vectors of the form $\begin{pmatrix} x \\ -x \end{pmatrix}$.
Let's just do one very simple example.

**Example**
Let \( A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix} \) and let \( s = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \). Let \( V \) be the subspace consisting of all vectors of the form \( \begin{pmatrix} x \\ -x \end{pmatrix} \). Then \( A^n s \in V \) if and only if \( n \) is odd,
One very simple example

Let’s just do one very simple example.

Example
Let $A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$ and let $s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Let $V$ be the subspace consisting of all vectors of the form $\begin{pmatrix} x \\ -x \end{pmatrix}$. Then $A^n s \in V$ if and only if $n$ is odd, i.e. if $n \in 1 + 2\mathbb{Z}$.

A few points:
▶ This very atypical – more frequently, you will get at most finitely many $n$ in this situation
One very simple example

Let’s just do one very simple example.

Example
Let $A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$ and let $s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Let $V$ be the subspace consisting of all vectors of the form $\begin{pmatrix} x \\ -x \end{pmatrix}$. Then $A^n s \in V$ if and only if $n$ is odd, i.e. if $n \in 1 + 2\mathbb{Z}$.

A few points:

▶ This very atypical – more frequently, you will get at most finitely many $n$ in this situation (a bunch of “singleton cosets”).
One very simple example

Let’s just do one very simple example.

Example

Let \( A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix} \) and let \( s = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \). Let \( V \) be the subspace consisting of all vectors of the form \( \begin{pmatrix} x \\ -x \end{pmatrix} \). Then \( A^n s \in V \) if and only if \( n \) is odd, i.e. if \( n \in 1 + 2\mathbb{Z} \).

A few points:

- This very atypical – more frequently, you will get at most finitely many \( n \) in this situation (a bunch of “singleton cosets”).

- Note that \( A^2 \) sends \( V \) to itself, so once you get some \( A^i s \in V \), you must get \( A^{i+2k} s \in V \) for any \( k \).
Let’s just do one very simple example.

Example
Let $A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$ and let $s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Let $V$ be the subspace consisting of all vectors of the form $\begin{pmatrix} x \\ -x \end{pmatrix}$. Then $A^n s \in V$ if and only if $n$ is odd, i.e. if $n \in 1 + 2\mathbb{Z}$.

A few points:

- This very atypical – more frequently, you will get at most finitely many $n$ in this situation (a bunch of “singleton cosets”).
- Note that $A^2$ sends $V$ to itself, so once you get some $A^i s \in V$, you must get $A^{i+2k} s \in V$ for any $k$ (this is why you do not get any “singleton cosets” here).
$p$-adic logarithms and exponentials

The Skolem-Mahler-Lech theorem is proved using $p$-adic methods. One begins by embedding everything into $\mathbb{Z}_p$ for some $p$ (this can always be done by the Chebotarev density theorem).
The Skolem-Mahler-Lech theorem is proved using $p$-adic methods. One begins by embedding everything into $\mathbb{Z}_p$ for some $p$ (this can always be done by the Chebotarev density theorem).

The idea is very simple: take $p$-adic logarithms of $A$, in the usual way seen in differential equations, with $p$-adic logs instead of archimedean logs.
Let $A$ be a diagonalized matrix with all eigenvalues that are $p$-adic units.

Raising to the power $m$, we may suppose that all of the eigenvalues of $A^m$ are congruent to 1 (mod $p$) (this allows us to take $p$-adic logarithms).

For a point $(z_1, \ldots, z_r) \in \mathbb{Z}_p^r$, and any $i$, $k$ we have

$$A^{i+mk} \begin{pmatrix} z_1 & \cdots & z_r \end{pmatrix} = \begin{pmatrix} \lambda^i & 0 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & \lambda^i & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^r \\ \end{pmatrix} \begin{pmatrix} z_1 & \cdots & z_r \end{pmatrix}.$$

So we can parametrize within the coset $i+mk\mathbb{Z}_p$ by

$$\theta(i)(k) = (\exp p^{k \log p} \lambda^i z_1, \ldots, \exp p^{k \log p} \lambda^i z_r).$$
$p$-adic logarithms of matrices, continued

Let $A$ be a diagonalized matrix with all eigenvalues that are $p$-adic units. Raising to the power $m$, we may suppose that all of the eigenvalues of $A^m$ are congruent to 1 (mod $p$) (this allow us to take $p$-adic logarithms).
Let $A$ be a diagonalized matrix with all eigenvalues that are $p$-adic units. Raising to the power $m$, we may suppose that all of the eigenvalues of $A^m$ are congruent to 1 (mod $p$) (this allow us to take $p$-adic logarithms). For a point $(z_1, \ldots, z_r) \in \mathbb{Z}_p^r$, and any $i, k$ we have

\[
A^{i+mk} \begin{pmatrix}
  z_1 \\
  \vdots \\
  z_r
\end{pmatrix} = \begin{pmatrix}
  \lambda_1^{i+mk} & 0 & 0 \\
  \vdots & \ddots & \vdots \\
  0 & 0 & \lambda_r^{i+mk}
\end{pmatrix} \begin{pmatrix}
  z_1 \\
  \vdots \\
  z_r
\end{pmatrix}
= \begin{pmatrix}
  \exp_p(k \log_p \lambda_1^m) \lambda_1^i & 0 & 0 \\
  \vdots & \ddots & \vdots \\
  0 & 0 & \exp_p(k \log_p \lambda_r^m) \lambda_r^i z_r
\end{pmatrix} \begin{pmatrix}
  z_1 \\
  \vdots \\
  z_r
\end{pmatrix}.
\]
\textbf{*p*-adic logarithms of matrices, continued}

Let $A$ be a diagonalized matrix with all eigenvalues that are $p$-adic units. Raising to the power $m$, we may suppose that all of the eigenvalues of $A^m$ are congruent to 1 (mod $p$) (this allow us to take $p$-adic logarithms). For a point $(z_1, \ldots, z_r) \in \mathbb{Z}_p^r$, and any $i, k$ we have

$$A^{i+mk} \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = \begin{pmatrix} \lambda_1^{i+mk} & 0 & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 & \lambda_r^{i+mk} \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}$$

$$= \begin{pmatrix} \exp_p(k \log_p \lambda_1^m) \lambda_1^i & 0 & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 & \exp_p(k \log_p \lambda_r^m) \lambda_r^i z_r \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}.$$

So we can parametrize within the coset $i + m\mathbb{Z}$ by

$$\theta_i(k) = (\exp_p(k \log_p \lambda_1^m) \lambda_1^i z_1, \ldots, \exp_p(k \log_p \lambda_r^m) \lambda_r^i z_r)$$
Since the hypersurface is defined by $F(x_1, \ldots, x_r) = 0$ for some $F$, composing $F$ with $\theta_i$ gives a one-variable analytic power series $F \circ \theta_i$. The zeros must be isolated, so either this has finitely many zeros (giving us finitely many "singleton" arithmetic sequences); or this vanishes identically, giving us an entire coset $i, i + m, i + 2m, \ldots$. Thus, we have that the set of $n$ such that $A_n z \in H$ is a finite union of arithmetic sequences.
Finishing the proof

Since the hypersurface is defined by \( F(x_1, \ldots, x_r) = 0 \) for some \( F \), composing \( F \) with \( \theta_i \) gives a one-variable analytic power series \( F \circ \theta_i \). The zeros must be isolated, so either
Since the hypersurface is defined by \( F(x_1, \ldots, x_r) = 0 \) for some \( F \), composing \( F \) with \( \theta_i \) gives a one-variable analytic power series \( F \circ \theta_i \). The zeros must be isolated, so either

- this has finitely many zeros (giving us finitely many “singleton” arithmetic sequences); or
Finishing the proof

Since the hypersurface is defined by $F(x_1, \ldots, x_r) = 0$ for some $F$, composing $F$ with $\theta_i$ gives a one-variable analytic power series $F \circ \theta_i$. The zeros must be isolated, so either

- this has finitely many zeros (giving us finitely many "singleton" arithmetic sequences); or

- this vanishes identically, giving us an entire coset $i, i + m, i + 2m, \ldots$. 

Finishing the proof

Since the hypersurface is defined by $F(x_1, \ldots, x_r) = 0$ for some $F$, composing $F$ with $\theta_i$ gives a one-variable analytic power series $F \circ \theta_i$. The zeros must be isolated, so either

- this has finitely many zeros (giving us finitely many “singleton” arithmetic sequences); or
- this vanishes identically, giving us an entire coset $i, i + m, i + 2m, \ldots$.

Thus, we have that the set of $n$ such that $A^n z \in H$ is a finite union of arithmetic sequences.
A few notes on the SML theorem

- This works the same when the matrix is not diagonalizable, just using the formal expansions for matrix exponentials from sophomore linear algebra – these will converge $p$-adically when the matrix is congruent to the identity mod $p$. 
This works the same when the matrix is not diagonalizable, just using the formal expansions for matrix exponentials from sophomore linear algebra – these will converge $p$-adically when the matrix is congruent to the identity mod $p$.

In the arithmetic progressions

$$k, k + m, k + 2m, \ldots, k + \ell m, \ldots$$

the $m$ is simply the power you must raise $A$ to in order to get something congruent to the identity mod $p$. 
A few notes on the SML theorem

- This works the same when the matrix is not diagonalizable, just using the formal expansions for matrix exponentials from sophomore linear algebra – these will converge $p$-adically when the matrix is congruent to the identity mod $p$.

- In the arithmetic progressions

$$k, k + m, k + 2m, \ldots, k + \ell m, \ldots$$

the $m$ is simply the power you must raise $A$ to in order to get something congruent to the identity mod $p$.

- The argument immediately generalizes to any subvariety $V$ (not just hyperplanes).
There are in fact explicit bounds on how many “singletons” you can have before you must have an infinite arithmetic progression. These are due to Evertse-Schlickewei and others.
There are in fact explicit bounds on how many “singletons” you can have before you must have an infinite arithmetic progression. These are due to Evertse-Schlickewei and others.

But in the case of lines not passing through the origin, once you have a large finite number of $n$ such that $A^n z \in V$, you must have an entire coset.
There are in fact explicit bounds on how many “singletons” you can have before you must have an infinite arithmetic progression. These are due to Evertse-Schlickewei and others.

But in the case of lines not passing through the origin, once you have a large finite number of $n$ such that $A^n \mathbf{z} \in V$, you must have an entire coset. (In fact, there is an explicit bound on that number, 57, which is likely nowhere near sharp, since the best known example is 6.)
A more general question...and a counterexample

What if if we dealt with a non-cyclic group in $G \subseteq \text{GL}_r(\mathbb{C})$?
A more general question...and a counterexample

What if if we dealt with a non-cyclic group in $G \subseteq \text{GL}_r(\mathbb{C})$? Would it be true that the $g \in G$ such that $gz \in V$ form a finite union of cosets of subgroups of $G$?
A more general question...and a counterexample

What if if we dealt with a non-cyclic group in $G \subseteq \text{GL}_r(\mathbb{C})$? Would it be true that the $g \in G$ such that $gz \in V$ form a finite union of cosets of subgroups of $G$? The answer is “no”, in general.

Example

(GTZ) Working in $\mathbb{C}^3$, let $V$ be the subspace given by the $yz$-plane, i.e. the set of all $(0, y, z)$,
A more general question...and a counterexample

What if if we dealt with a non-cyclic group in \( G \subseteq \text{GL}_r(\mathbb{C}) \)? Would it be true that the \( g \in G \) such that \( gz \in V \) form a finite union of cosets of subgroups of \( G \)? The answer is “no”, in general.

Example

(GTZ) Working in \( \mathbb{C}^3 \), let \( V \) be the subspace given by the \( yz \)-plane, i.e. the set of all \((0, y, z)\), and let \( G \) be the group generated by the matrices

\[
A = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix}.
\]
A more general question...and a counterexample

What if if we dealt with a non-cyclic group in $G \subseteq \text{GL}_r(\mathbb{C})$? Would it be true that the $g \in G$ such that $gz \in V$ form a finite union of cosets of subgroups of $G$? The answer is “no”, in general.

**Example**

(GTZ) Working in $\mathbb{C}^3$, let $V$ be the subspace given by the $yz$-plane, i.e. the set of all $(0, y, z)$, and let $G$ be the group generated by the matrices $A = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix}$. This gives a commutative abelian group isomorphic to $\mathbb{Z}^2$. But we do not get the desired coset intersection result.
Laurent’s theorem

In the diagonal case, however, we have the following theorem of Laurent.
Laurent’s theorem

In the diagonal case, however, we have the following theorem of Laurent.

**Theorem (Laurent)**

*Let $G$ be a finitely generated group of simultaneously diagonalizable matrices in $\text{GL}_r(\mathbb{C})$. Then for any algebraic subvariety $V$ of $\mathbb{C}^r$ and any point $z \in \mathbb{C}^r$, the set*

$$\{ g \in G \mid gz \in V \}$$

*is a finite union of cosets of subgroups of $G$.***
Laurent’s theorem

In the diagonal case, however, we have the following theorem of Laurent.

**Theorem (Laurent)**

Let $G$ be a finitely generated group of **simultaneously diagonalizable** matrices in $\text{GL}_r(\mathbb{C})$. Then for any algebraic subvariety $V$ of $\mathbb{C}^r$ and any point $z \in \mathbb{C}^r$, the set

$$\{g \in G \mid gz \in V\}$$

is a finite union of cosets of subgroups of $G$.

The proof of this is completely different from the proof of the Skolem-Mahler-Lech theorem!
Group varieties acting on themselves

Note that if $G$ is a diagonal matrix acting on $\mathbb{C}^r$, then it is like an element of the multiplicative group $(\mathbb{C}^r)^*$ acting on itself in the usual way, i.e.

$$
\begin{pmatrix}
\lambda_1 & 0 & 0 \\
\vdots & \ddots & \vdots \\
0 & 0 & \lambda_r
\end{pmatrix}
\begin{pmatrix}
x_1 \\
\vdots \\
x_r
\end{pmatrix}
=
\begin{pmatrix}
\lambda_1 x_1 \\
\vdots \\
\lambda_r x_r
\end{pmatrix}
$$

In fact, Laurent's theorem is usually phrased as follows.

Theorem

The intersection of a finitely generated subgroup $G$ of $(\mathbb{C}^r)^*$ with a subvariety $V$ is a finite union of cosets of $G$.
Group varieties acting on themselves

Note that if $G$ is a diagonal matrix acting on $\mathbb{C}^r$, then it is like an element of the multiplicative group $(\mathbb{C}^r)^*$ acting on itself in the usual way, i.e.

$$
\begin{pmatrix}
\lambda_1 & 0 & 0 \\
\vdots & \ddots & \vdots \\
0 & 0 & \lambda_r
\end{pmatrix}
\begin{pmatrix}
x_1 \\
\vdots \\
x_r
\end{pmatrix}
=
\begin{pmatrix}
\lambda_1 x_1 \\
\vdots \\
\lambda_r x_r
\end{pmatrix}
$$

just as

$$(\lambda_1, \ldots, \lambda_r) \cdot (x_1, \ldots, x_r) = (\lambda_1 x_1, \ldots, \lambda_r x_r).$$
Group varieties acting on themselves

Note that if $G$ is a diagonal matrix acting on $\mathbb{C}^r$, then it is like an element of the multiplicative group $(\mathbb{C}^r)^*$ acting on itself in the usual way, i.e.

$$
\begin{pmatrix}
\lambda_1 & 0 & 0 \\
\vdots & \ddots & \vdots \\
0 & 0 & \lambda_r
\end{pmatrix}
\begin{pmatrix}
x_1 \\
\vdots \\
x_r
\end{pmatrix}
= 
\begin{pmatrix}
\lambda_1 x_1 \\
\vdots \\
\lambda_r x_r
\end{pmatrix}
$$

just as

$$(\lambda_1, \ldots, \lambda_r) \cdot (x_1, \ldots, x_r) = (\lambda_1 x_1, \ldots, \lambda_r x_r).$$

In fact, Laurent’s theorem is usually phrased as follows.
Group varieties acting on themselves

Note that if $G$ is a diagonal matrix acting on $\mathbb{C}^r$, then it is like an element of the multiplicative group $(\mathbb{C}^r)^*$ acting on itself in the usual way, i.e.

$$
\begin{pmatrix}
\lambda_1 & 0 & 0 \\
\vdots & \ddots & \vdots \\
0 & 0 & \lambda_r
\end{pmatrix}
\begin{pmatrix}
x_1 \\
\vdots \\
x_r
\end{pmatrix}
= 
\begin{pmatrix}
\lambda_1 x_1 \\
\vdots \\
\lambda_r x_r
\end{pmatrix}
$$

just as

$$(\lambda_1, \ldots, \lambda_r) \cdot (x_1, \ldots, x_r) = (\lambda_1 x_1, \ldots, \lambda_r x_r).$$

In fact, Laurent’s theorem is usually phrased as follows.

**Theorem**

*The intersection of a finitely generated subgroup $G$ of $(\mathbb{C}^*)^r$ with a subvariety $V$ is a finite union of cosets of $G$.***
The Mordell conjecture

The famous Mordell conjecture (now a theorem of Faltings) can be derived from a statement similar to Laurent’s theorem.
The Mordell conjecture

The famous Mordell conjecture (now a theorem of Faltings) can be derived from a statement similar to Laurent’s theorem. Recall what the Mordell conjecture says.
The Mordell conjecture

The famous Mordell conjecture (now a theorem of Faltings) can be derived from a statement similar to Laurent’s theorem. Recall what the Mordell conjecture says.

**Theorem (Faltings’ Theorem/Mordell Conjecture)**

If $C$ is an algebraic curve of genus $\geq 2$ defined over $\mathbb{Q}$, then there are at most finitely many $\mathbb{Q}$-rational points on $C$. 
The Mordell conjecture

The famous Mordell conjecture (now a theorem of Faltings) can be derived from a statement similar to Laurent’s theorem. Recall what the Mordell conjecture says.

Theorem (Faltings’ Theorem/Mordell Conjecture)

If $C$ is an algebraic curve of genus $\geq 2$ defined over $\mathbb{Q}$, then there are at most finitely many $\mathbb{Q}$-rational points on $C$.

Note that a typical equation two-variable polynomial $F(x, y) \in \mathbb{Q}[x, y]$ of degree $\geq 4$ gives rise to a curve of genus $\geq 2$. 
The Mordell conjecture

The famous Mordell conjecture (now a theorem of Faltings) can be derived from a statement similar to Laurent’s theorem. Recall what the Mordell conjecture says.

Theorem (Faltings’ Theorem/Mordell Conjecture)

If $C$ is an algebraic curve of genus $\geq 2$ defined over $\mathbb{Q}$, then there are at most finitely many $\mathbb{Q}$-rational points on $C$.

Note that a typical equation two-variable polynomial $F(x, y) \in \mathbb{Q}[x, y]$ of degree $\geq 4$ gives rise to a curve of genus $\geq 2$.

Thus, Faltings’ theorem says that, except in special cases, for any polynomial $F(x, y) \in \mathbb{Q}[x, y]$ of degree $\geq 4$, there are finitely many $(p/q, r/s) \in \mathbb{Q}^2$ such that

$$F(p/q, r/s) = 0.$$
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for *abelian varieties* rather than for $(\mathbb{C}^*)^r$. 

An abelian variety is $\mathbb{C}^r/\Lambda$ where $\Lambda$ is a lattice in $\mathbb{C}^r$. Since a lattice is an additive subgroup of $\mathbb{C}^r$, an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties.

We will now state the Lang conjecture (now a theorem of Faltings and Vojta).

Theorem (Lang conjecture, Faltings-Vojta, 1991)

Let $A$ be an abelian variety, let $G$ be a finitely generated subgroup of $A$, and let $V$ be a subvariety of $A$. Then $V \cap G$ is a finite union of cosets of subgroups of $G$.

When $A$ is defined over $\mathbb{Q}$, one may talk about the $\mathbb{Q}$-points on $A$ (these are literally the points on $A$ with rational coordinates under some embedding), which are denoted as $A(\mathbb{Q})$. 
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for *abelian varieties* rather than for \((\mathbb{C}^*)^r\). An abelian variety is

\[ \mathbb{C}^r / \Lambda \]

where \( \Lambda \) is a lattice in \( \mathbb{C}^r \). Since a lattice is an additive subgroup of \( \mathbb{C}^r \), an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties. We will now state the Lang conjecture (now a theorem of Faltings and Vojta).

**Theorem (Lang conjecture, Faltings-Vojta, 1991)**

Let \( A \) be an abelian variety, let \( G \) be a finitely generated subgroup of \( A \), and let \( V \) be a subvariety of \( A \). Then

\[ V \cap G \]

is a finite union of cosets of subgroups of \( G \).

When \( A \) is defined over \( \mathbb{Q} \), one may talk about the \( \mathbb{Q} \)-points on \( A \) (these are literally the points on \( A \) with rational coordinates under some embedding), which are denoted as \( A(\mathbb{Q}) \).
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for *abelian varieties* rather than for $(\mathbb{C}^*)^r$. An abelian variety is

$$\mathbb{C}^r/\Lambda$$

where $\Lambda$ is a lattice in $\mathbb{C}^r$. Since a lattice is an additive subgroup of $\mathbb{C}^r$, an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties.
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for \textit{abelian varieties} rather than for \((\mathbb{C}^*)^r\). An abelian variety is

\[ \mathbb{C}^r / \Lambda \]

where \( \Lambda \) is a lattice in \( \mathbb{C}^r \). Since a lattice is an additive subgroup of \( \mathbb{C}^r \), an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties. We will now state the Lang conjecture (now a theorem of Faltings and Vojta).
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for abelian varieties rather than for \((\mathbb{C}^*)^r\). An abelian variety is

\[
\mathbb{C}^r / \Lambda
\]

where \(\Lambda\) is a lattice in \(\mathbb{C}^r\). Since a lattice is an additive subgroup of \(\mathbb{C}^r\), an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties. We will now state the Lang conjecture (now a theorem of Faltings and Vojta).

**Theorem (Lang conjecture, Faltings-Vojta, 1991)**

Let \(A\) be an abelian variety, let \(G\) be a finitely generated subgroup of \(A\), and let \(V\) be a subvariety of \(A\). Then

\[
V \cap G \text{ is a finite union of cosets of subgroups of } G.
\]
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for *abelian varieties* rather than for \((\mathbb{C}^*)^r\). An abelian variety is

\[
\mathbb{C}^r / \Lambda
\]

where \(\Lambda\) is a lattice in \(\mathbb{C}^r\). Since a lattice is an additive subgroup of \(\mathbb{C}^r\), an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties. We will now state the Lang conjecture (now a theorem of Faltings and Vojta).

**Theorem (Lang conjecture, Faltings-Vojta, 1991)**

Let \(A\) be an abelian variety, let \(G\) be a finitely generated subgroup of \(A\), and let \(V\) be a subvariety of \(A\). Then

\[V \cap G \text{ is a finite union of cosets of subgroups of } G.\]

When \(A\) is defined \(\mathbb{Q}\), one may talk about the \(\mathbb{Q}\)-points on \(A\)
Abelian varieties and the Lang conjecture

The Mordell follows from a Laurent-line statement only for *abelian varieties* rather than for \((\mathbb{C}^\ast)^r\). An abelian variety is

\[ \mathbb{C}^r / \Lambda \]

where \(\Lambda\) is a lattice in \(\mathbb{C}^r\). Since a lattice is an additive subgroup of \(\mathbb{C}^r\), an abelian variety has a natural group structure.

Abelian varieties also have structures as varieties. We will now state the Lang conjecture (now a theorem of Faltings and Vojta).

**Theorem (Lang conjecture, Faltings-Vojta, 1991)**

*Let \(A\) be an abelian variety, let \(G\) be a finitely generated subgroup of \(A\), and let \(V\) be a subvariety of \(A\). Then*

\[ V \cap G \text{ is a finite union of cosets of subgroups of } G. \]

*When \(A\) is defined \(\mathbb{Q}\), one may talk about the \(\mathbb{Q}\)-points on \(A\) (these are literally the points on \(A\) with rational coordinates under some embedding), which are denoted as \(A(\mathbb{Q})\).*
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

The group \( A(\mathbb{Q}) \) is finitely generated.

One more fact.

Fact:

A curve of genus \( g \geq 1 \) admits an embedding into an abelian variety of dimension \( g \). Further, a curve is itself an abelian variety if and only if it has genus 1.

Derivation of Mordell conjecture from Mordell-Lang.

Considering a curve \( C \) of genus \( g \geq 2 \) as \( C \subset A \), for \( A \) an abelian variety, the rational points of \( C \) are in \( A(\mathbb{Q}) \cap C \).

By the Lang conjecture, these form a finite union of cosets of subgroups of \( A(\mathbb{Q}) \).

So if there are infinitely many \( \mathbb{Q} \)-rational points on \( C \), one of these cosets is infinite.

After shifting over, we can make this coset a subgroup.

Taking the (Zariski) closure of this subgroup, we must get something that is (a) itself a group and (b) equal to exactly \( C \).

But that would make \( C \) itself an abelian variety, a contradiction, since the genus of \( C \) is \( > 1 \).
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)
*The group \( A(\mathbb{Q}) \) is finitely generated.*

One more fact.

**Fact:** A curve of genus \( g \geq 1 \) admits an embedding into an abelian variety of dimension \( g \). Further, a curve is itself an abelian variety if and only if it has genus 1.
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

*The group $A(\mathbb{Q})$ is finitely generated.*

One more fact.

**Fact:** A curve of genus $g \geq 1$ admits an embedding into an abelian variety of dimension $g$. Further, a curve is itself an abelian variety if and only if it has genus 1.

**Derivation of Mordell conjecture from Mordell-Lang.**

Considering a curve $C$ of genus $g \geq 2$ as $C \subset A$, for $A$ an abelian variety, the rational points of $C$ are in $A(\mathbb{Q}) \cap C$. 
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

The group $A(\mathbb{Q})$ is finitely generated.

One more fact.

**Fact**: A curve of genus $g \geq 1$ admits an embedding into an abelian variety of dimension $g$. Further, a curve is itself an abelian variety if and only if it has genus 1.

**Derivation of Mordell conjecture from Mordell-Lang.**

Considering a curve $C$ of genus $g \geq 2$ as $C \subset A$, for $A$ an abelian variety, the rational points of $C$ are in $A(\mathbb{Q}) \cap C$. By the Lang conjecture, these form a finite union of cosets of subgroups of $A(\mathbb{Q})$. 
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

*The group $A(\mathbb{Q})$ is finitely generated.*

One more fact.

**Fact:** *A curve of genus $g \geq 1$ admits an embedding into an abelian variety of dimension $g$. Further, a curve is itself an abelian variety if and only if it has genus 1.*

**Derivation of Mordell conjecture from Mordell-Lang.**

Considering a curve $C$ of genus $g \geq 2$ as $C \subset A$, for $A$ an abelian variety, the rational points of $C$ are in $A(\mathbb{Q}) \cap C$. By the Lang conjecture, these form a finite union of cosets of subgroups of $A(\mathbb{Q})$. So if there are infinitely many $\mathbb{Q}$-rational points on $C$, one of these cosets is infinite.
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

The group $A(\mathbb{Q})$ is finitely generated.

One more fact.

Fact: A curve of genus $g \geq 1$ admits an embedding into an abelian variety of dimension $g$. Further, a curve is itself an abelian variety if and only if it has genus 1.

Derivation of Mordell conjecture from Mordell-Lang.
Considering a curve $C$ of genus $g \geq 2$ as $C \subset A$, for $A$ an abelian variety, the rational points of $C$ are in $A(\mathbb{Q}) \cap C$. By the Lang conjecture, these form a finite union of cosets of subgroups of $A(\mathbb{Q})$. So if there are infinitely many $\mathbb{Q}$-rational points on $C$, one of these cosets is infinite. After shifting over, we can make this coset a subgroup.
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

The group \(A(\mathbb{Q})\) is finitely generated.

One more fact.

Fact: A curve of genus \(g \geq 1\) admits an embedding into an abelian variety of dimension \(g\). Further, a curve is itself an abelian variety if and only if it has genus 1.

Derivation of Mordell conjecture from Mordell-Lang.
Considering a curve \(C\) of genus \(g \geq 2\) as \(C \subset A\), for \(A\) an abelian variety, the rational points of \(C\) are in \(A(\mathbb{Q}) \cap C\). By the Lang conjecture, these form a finite union of cosets of subgroups of \(A(\mathbb{Q})\). So if there are infinitely many \(\mathbb{Q}\)-rational points on \(C\), one of these cosets is infinite. After shifting over, we can make this coset a subgroup. Taking the (Zariski) closure of this subgroup, we must get something that is (a) itself a group and (b) equal to exactly \(C\).
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

The group $A(\mathbb{Q})$ is finitely generated.

One more fact.

Fact: A curve of genus $g \geq 1$ admits an embedding into an abelian variety of dimension $g$. Further, a curve is itself an abelian variety if and only if it has genus 1.

Derivation of Mordell conjecture from Mordell-Lang.

Considering a curve $C$ of genus $g \geq 2$ as $C \subset A$, for $A$ an abelian variety, the rational points of $C$ are in $A(\mathbb{Q}) \cap C$. By the Lang conjecture, these form a finite union of cosets of subgroups of $A(\mathbb{Q})$. So if there are infinitely many $\mathbb{Q}$-rational points on $C$, one of these cosets is infinite. After shifting over, we can make this coset a subgroup. Taking the (Zariski) closure of this subgroup, we must get something that is (a) itself a group and (b) equal to exactly $C$. But that would make $C$ itself an abelian variety,
The Mordell-Weil theorem and Faltings’ theorem

Theorem (Mordell-Weil theorem, 1922)

The group $A(\mathbb{Q})$ is finitely generated.

One more fact.

**Fact**: A curve of genus $g \geq 1$ admits an embedding into an abelian variety of dimension $g$. Further, a curve is itself an abelian variety if and only if it has genus 1.

**Derivation of Mordell conjecture from Mordell-Lang.**

Considering a curve $C$ of genus $g \geq 2$ as $C \subset A$, for $A$ an abelian variety, the rational points of $C$ are in $A(\mathbb{Q}) \cap C$. By the Lang conjecture, these form a finite union of cosets of subgroups of $A(\mathbb{Q})$. So if there are infinitely many $\mathbb{Q}$-rational points on $C$, one of these cosets is infinite. After shifting over, we can make this coset a subgroup. Taking the (Zariski) closure of this subgroup, we must get something that is (a) itself a group and (b) equal to exactly $C$. But that would make $C$ itself an abelian variety, a contradiction, since the genus of $C$ is $> 1$. 
Additive groups

The Lang conjecture generalizes to a theorem about any group variety of the form $A \times (\mathbb{C}^*)^r$, in other words an abelian variety crossed with a multiplicative group.
Additive groups

The Lang conjecture generalizes to a theorem about any group variety of the form $A \times (\mathbb{C}^*)^r$, in other words an abelian variety crossed with a multiplicative group. However, it is *not true* for the additive group $(\mathbb{C}^2, +)$.

Example

- Let $G$ be the additive subgroup of $\mathbb{C}^2$ consisting of all integers $(m, n)$. 


Additive groups

The Lang conjecture generalizes to a theorem about any group variety of the form $A \times (\mathbb{C}^*)^r$, in other words an abelian variety crossed with a multiplicative group. However, it is not true for the additive group $(\mathbb{C}^2, +)$.

Example

- Let $G$ be the additive subgroup of $\mathbb{C}^2$ consisting of all integers $(m, n)$.
- Let $V$ be the curve consisting of all $(x, y) \in \mathbb{C}^2$ such that
  \[ x^2 - dy^2 = 1 \]
  for some square-free integer $d > 1$.

  (this is called Pell’s equation)
Additive groups

The Lang conjecture generalizes to a theorem about any group variety of the form $A \times (\mathbb{C}^*)^r$, in other words an abelian variety crossed with a multiplicative group. However, it is not true for the additive group $(\mathbb{C}^2, +)$.

Example

- Let $G$ be the additive subgroup of $\mathbb{C}^2$ consisting of all integers $(m, n)$.
- Let $V$ be the curve consisting of all $(x, y) \in \mathbb{C}^2$ such that

$$x^2 - dy^2 = 1$$

for some square-free integer $d > 1$.

(this is called Pell’s equation)

Then it is known that there are infinitely many integer solutions $(m, n)$ to $m^2 - dn^2 = 1$, but they do not form a finite set of cosets of subgroups of $G$. The solutions are “too sparsely spaced” to be represented by cosets of subgroups.
The Skolem-Mahler-Lech approach generalizes to automorphisms of any algebraic variety, via a generalization of $p$-adic logarithms.
The Skolem-Mahler-Lech approach generalizes to automorphisms of any algebraic variety, via a generalization of $p$-adic logarithms. (Essentially one takes $p$-adic logarithms of Jacobian matrices, though this requires work.)
The Skolem-Mahler-Lech approach generalizes to automorphisms of any algebraic variety, via a generalization of $p$-adic logarithms. (Essentially one takes $p$-adic logarithms of Jacobian matrices, though this requires work.) Thus one obtains.

**Theorem**  
*(Bell-Ghioca-T)* Let $X$ be an algebraic variety over $\mathbb{C}$, let $G$ be a group generated by a single automorphism $\sigma : X \rightarrow X$, let $V$ be a subvariety of $X$, and let $z$ be point on $X$. Then the set of $g \in G$ such that $gz \in V$ is a finite union of cosets of $G$. 

**Extending Skolem-Mahler-Lech**
Dynamical Mordell-Lang question

Here is a question that ties together all the problems we have looked at.

Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $G$ be a finitely generated commutative semigroup of morphisms from $X$ to itself, and let $z \in X(\mathbb{C})$. Can the set $\{g \in G | g(z) \in V\}$ be written as a finite union of cosets of subsemigroups of $G$? We have seen that in some cases, the answer is "yes", in some it is "no". Is there a reasonable conjecture to be made here? If so, how can it be proved?
Dynamical Mordell-Lang question

Here is a question that ties together all the problems we have looked at.

**Question DML**

*Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $G$ be a finitely generated commutative semigroup of morphisms from $X$ to itself, and let $z \in X(\mathbb{C})$. Can the set

$$\{g \in G \mid gz \in V\}$$

be written as a finite union of cosets of subsemigroups of $G$?*
Dynamical Mordell-Lang question

Here is a question that ties together all the problems we have looked at.

**Question DML**

*Let* $X$ *be an algebraic variety defined over* $\mathbb{C}$, *let* $V$ *be a closed subvariety of* $X$, *let* $G$ *be a finitely generated commutative semigroup of morphisms from* $X$ *to itself, and let* $z \in X(\mathbb{C})$. *Can the set*

$$\{ g \in G \mid gz \in V \}$$

*be written as a finite union of cosets of subsemigroups of* $G$?

*We have seen that in some cases, the answer is “yes”, in some it is “no”. 


Dynamical Mordell-Lang question

Here is a question that ties together all the problems we have looked at.

**Question DML**

*Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $G$ be a finitely generated commutative semigroup of morphisms from $X$ to itself, and let $z \in X(\mathbb{C})$. Can the set*

$$\{g \in G \mid gz \in V\}$$

*be written as a finite union of cosets of subsemigroups of $G$?*

We have seen that in some cases, the answer is “yes”, in some it is “no”.

Is there a reasonable conjecture to be made here?
Dynamical Mordell-Lang question

Here is a question that ties together all the problems we have looked at.

**Question DML**

*Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $G$ be a finitely generated commutative semigroup of morphisms from $X$ to itself, and let $z \in X(\mathbb{C})$. Can the set

$$\{g \in G \mid gz \in V\}$$

be written as a finite union of cosets of subsemigroups of $G$?*

We have seen that in some cases, the answer is “yes”, in some it is “no”.

Is there a reasonable conjecture to be made here?

If so, how can it be proved?
The cyclic case

First, of all the question should have a positive answer in the general “cyclic semigroup” case (i.e. not just when the map is automorphism).
The cyclic case

First, of all the question should have a positive answer in the general “cyclic semigroup” case (i.e. not just when the map is automorphism).

Conjecture

Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $\Phi : X \rightarrow X$, and let $z \in X(\mathbb{C})$. Then the set of $n$ such that $\Phi^n(z) \in V$ is a finite union of arithmetic sequences.

One (might!) get this result by applying the Skolem-Mahler-Lech $p$-adic logarithm technique to the Jacobian matrix $J$ for $\Phi$ at a suitable point as long as $p \nmid \det J$. This can be done whenever the orbit of $z$ avoids the ramification locus of $\Phi$ modulo $p$. (Even though we are in $\mathbb{C}$, we can get a suitable embedding into $\mathbb{Z}_p$ so that the idea of “modulo $p$” makes sense.)
The cyclic case

First, of all the question should have a positive answer in the general “cyclic semigroup” case (i.e. not just when the map is automorphism).

Conjecture

Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $\Phi : X \to X$, and let $z \in X(\mathbb{C})$. Then the set of $n$ such that $\Phi^n(z) \in V$ is a finite union of arithmetic sequences.

One (might!) get this result by applying the Skolem-Mahler-Lech $p$-adic logarithm technique to the Jacobian matrix $J$ for $\Phi$ at a suitable point as long as $p \nmid \det J$. 
The cyclic case

First, of all the question should have a positive answer in the general “cyclic semigroup” case (i.e. not just when the map is automorphism).

**Conjecture**

Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $\Phi : X \rightarrow X$, and let $z \in X(\mathbb{C})$. Then the set of $n$ such that $\Phi^n(z) \in V$ is a finite union of arithmetic sequences.

One (might!) get this result by applying the Skolem-Mahler-Lech $p$-adic logarithm technique to the Jacobian matrix $J$ for $\Phi$ at a suitable point as long as $p \nmid \det J$.

This can be done whenever the orbit of $z$ avoids the ramification locus of $\Phi$ modulo $p$. 
The cyclic case

First, of all the question should have a positive answer in the general “cyclic semigroup” case (i.e. not just when the map is automorphism).

**Conjecture**

*Let $X$ be an algebraic variety defined over $\mathbb{C}$, let $V$ be a closed subvariety of $X$, let $\Phi : X \to X$, and let $z \in X(\mathbb{C})$. Then the set of $n$ such that $\Phi^n(z) \in V$ is a finite union of arithmetic sequences.*

One (might!) get this result by applying the Skolem-Mahler-Lech $p$-adic logarithm technique to the Jacobian matrix $J$ for $\Phi$ at a suitable point as long as $p \nmid \det J$.

This can be done whenever the orbit of $z$ avoids the ramification locus of $\Phi$ modulo $p$. (Even though we are in $\mathbb{C}$, we can get a suitable embedding into $\mathbb{Z}_p$ so that the idea of “modulo $p$” makes sense.)
Avoiding subvarieties mod \( p \)

Trying to avoid ramification modulo \( p \) leads to the natural question.

Let \( X \) be an algebraic variety defined over a number field \( K \), let \( V \) be a closed subvariety of \( X \), and let \( \Phi : X \to X \), let \( z \in X \).

Suppose that the orbit of \( z \) does not pass through \( V \). Is there a prime \( p \) of \( K \) such that the orbit of \( z \) does not pass through \( V \) modulo \( p \)?

(The orbit of \( z \) is as usual the set \( \{ z, \Phi(z), \Phi^2(z), \ldots \} \)).

If the answer were "yes" we could prove the full cyclic case of the Dynamical Mordell-Lang conjecture. (Work on using this avoidance principle has been done by Benedetto, Ghoica, Kurlberg, Scanlon, T, and others)
Avoiding subvarieties mod $p$

Trying to avoid ramification modulo $p$ leads to the natural question.

**Question**

Let $X$ be an algebraic variety defined over a number field $K$, let $V$ be a closed subvariety of $X$, and let $\Phi : X \rightarrow X$, let $z \in X$. Suppose that the orbit of $z$ does not pass through $V$. Is there a prime $p$ of $K$ such that the orbit of $z$ does not pass through $V$ modulo $p$?

(The orbit of $z$ is as usual the set \{ $z$, $\Phi(z)$, $\Phi^2(z)$, ... \}).

If the answer were "yes" we could prove the full cyclic case of the Dynamical Mordell-Lang conjecture. (Work on using this avoidance principle has been done by Benedetto, Ghoica, Kurlberg, Scanlon, T, and others)
Avoiding subvarieties mod \( p \)

Trying to avoid ramification modulo \( p \) leads to the natural question.

**Question**

*Let \( X \) be an algebraic variety defined over a number field \( K \), let \( V \) be a closed subvariety of \( X \), and let \( \Phi : X \to X \), let \( z \in X \). Suppose that the orbit of \( z \) does not pass through \( V \). Is there a prime \( p \) of \( K \) such that the orbit of \( z \) does not pass through \( V \) modulo \( p \)?*

(The orbit of \( z \) is as usual the set \( \{ z, \Phi(z), \Phi^2(z), \ldots \} \)).
Avoiding subvarieties mod $p$

Trying to avoid ramification modulo $p$ leads to the natural question.

**Question**

*Let $X$ be an algebraic variety defined over a number field $K$, let $V$ be a closed subvariety of $X$, and let $\Phi : X \longrightarrow X$, let $z \in X$. Suppose that the orbit of $z$ does not pass through $V$. Is there a prime $p$ of $K$ such that the orbit of $z$ does not pass through $V$ modulo $p$?*

(The orbit of $z$ is as usual the set $\{z, \Phi(z), \Phi^2(z), \ldots \}$.)

If the answer were “yes” we could prove the full cyclic case of the Dynamical Mordell-Lang conjecture. (}
Avoiding subvarieties mod $p$

Trying to avoid ramification modulo $p$ leads to the natural question.

**Question**

Let $X$ be an algebraic variety defined over a number field $K$, let $V$ be a closed subvariety of $X$, and let $\Phi : X \rightarrow X$, let $z \in X$. Suppose that the orbit of $z$ does not pass through $V$. Is there a prime $p$ of $K$ such that the orbit of $z$ does not pass through $V$ modulo $p$?

(The orbit of $z$ is as usual the set \{ $z, \Phi(z), \Phi^2(z), \ldots$ \}).

If the answer were “yes” we could prove the full cyclic case of the Dynamical Mordell-Lang conjecture. (Work on using this avoidance principle has been done by Benedetto, Ghoica, Kurlberg, Scanlon, T, and others)
A few notes on the question on the last page:

▶ The answer is “yes” when $X$ has dimension 1, but we not know of an elementary proof: it follows from Silverman’s dynamic Siegel’s theorem for dimension 1 (which uses Roth’s theorem).
Avoiding subvarieties mod $p$ (continued)

A few notes on the question on the last page:

- The answer is “yes” when $X$ has dimension 1, but we not know of an elementary proof: it follows from Silverman’s dynamic Siegel’s theorem for dimension 1 (which uses Roth’s theorem).

- Heuristically, we believe that there are counterexamples in higher dimension due to an argument of Kurlberg. But at present, we have no way to prove that the suggested counterexamples are in fact counterexamples.
A related problem

We now examine a related problem. We say that a map \( \Phi : X \rightarrow X \) is *polarized* if there is an ample line bundle \( L \) on \( X \) such that \( \Phi^* L \cong L \otimes^d \) for some \( d > 1 \) (this is like saying that \( \Phi \) has degree \( d \)).
A related problem

We now examine a related problem. We say that a map \( \Phi : X \to X \) is polarized if there is an ample line bundle \( L \) on \( X \) such that \( \Phi^* L \cong L \otimes d \) for some \( d > 1 \) (this is like saying that \( \Phi \) has degree \( d \)).

**Conjecture**

*(Zhang)* Let \( X \) be an algebraic variety defined over \( \overline{\mathbb{Q}} \) and \( X \) and let \( \Phi : X \to X \) be a polarized map. Then there is a point \( x \in X(\overline{\mathbb{Q}}) \) such that the orbit of \( x \) under \( \Phi \) is Zariski dense in \( X \).
A related problem, continued

Progress has been made on Zhang’s conjecture, using $p$-adic methods....
Progress has been made on Zhang’s conjecture, using $p$-adic methods....

Given $\Phi : X \rightarrow X$, we say that a point $x$ is \textit{preperiodic} if the orbit of $x$ under $\Phi$ is finite (in other words, if the orbit is “eventually periodic”). Otherwise, we say it is \textit{nonpreperiodic}. One expects that in characteristic 0, a “typical” point is nonpreperiodic, but this it not at all obvious (over finite fields, for example, all points are preperiodic).
A related problem, continued

Progress has been made on Zhang’s conjecture, using $p$-adic methods....

Given $\Phi : X \to X$, we say that a point $x$ is \textit{preperiodic} if the orbit of $x$ under $\Phi$ is finite (in other words, if the orbit is “eventually periodic”). Otherwise, we say it is \textit{nonpreperiodic}. One expects that in characteristic 0, a “typical” point is nonpreperiodic, but this is not at all obvious (over finite fields, for example, all points are preperiodic).

**Theorem**

(Amerik) Let $X$ be an algebraic variety defined over $\overline{\mathbb{Q}}$ and $\Phi : X \to X$ be a dominant rational map of infinite order. Then the nonpreperiodic points of $X(\overline{\mathbb{Q}})$ are dense in $X$.

This result holds even when $\Phi$ is a dominant rational map rather than a morphism, i.e. when $\Phi$ is not defined on all of $X$ but has a Zariski dense image in $X$. 

Towards a correct dynamical Mordell-Lang conjecture

Back to the dynamical Mordell-Lang conjecture....
Towards a correct dynamical Mordell-Lang conjecture

Back to the dynamical Mordell-Lang conjecture....

One idea is to use the fact that the $p$-adic parametrizations maps convert the various elements of the semigroup into their Jacobian matrices. Then one could ask that the theorem be true when the Jacobian matrices are simultaneously diagonalizable.
Towards a correct dynamical Mordell-Lang conjecture

Back to the dynamical Mordell-Lang conjecture....

One idea is to use the fact that the $p$-adic parametrizations maps convert the various elements of the semigroup into their Jacobian matrices. Then one could ask that the theorem be true when the Jacobian matrices are simultaneously diagonalizable.

That seems reasonable likely to be true, but it is a bit limited.
Towards a correct dynamical Mordell-Lang conjecture

Back to the dynamical Mordell-Lang conjecture....

One idea is to use the fact that the $p$-adic parametrizations maps convert the various elements of the semigroup into their Jacobian matrices. Then one could ask that the theorem be true when the Jacobian matrices are simultaneously diagonalizable.

That seems reasonable likely to be true, but it is a bit limited.
Counterexamples revisited

Let’s think back on our two counterexamples:

1. The Pell equation $x^2 - dy^2 = 1$ under additive translation of the Cartesian plane.

2. The subspace $x = 0$ under the action of a group of matrices.
Counterexamples revisited

Let’s think back on our two counterexamples:

1. The Pell equation $x^2 - dy^2 = 1$ under additive translation of the Cartesian plane.
2. The subspace $x = 0$ under the action of a group of matrices.
Counterexamples revisited

Let’s think back on our two counterexamples:

1. The Pell equation $x^2 - dy^2 = 1$ under additive translation of the Cartesian plane.

2. The subspace $x = 0$ under the action of a group of matrices.

Here is one explanation for what goes wrong. To be concrete let’s restrict to $d = 3$ for case 1.
Counterexamples revisited

Let’s think back on our two counterexamples:

1. The Pell equation $x^2 - dy^2 = 1$ under additive translation of the Cartesian plane.

2. The subspace $x = 0$ under the action of a group of matrices.

Here is one explanation for what goes wrong. To be concrete let’s restrict to $d = 3$ for case 1.

1. The Pell’s equation curve $x^2 - 3y^2 = 1$ is stable under the action of the map $\sigma : (x, y) \rightarrow (2x + 3y, 2y + x)$, which “almost” commutes with additive translation.
Let’s think back on our two counterexamples:

1. The Pell equation $x^2 - dy^2 = 1$ under additive translation of the Cartesian plane.

2. The subspace $x = 0$ under the action of a group of matrices.

Here is one explanation for what goes wrong. To be concrete let’s restrict to $d = 3$ for case 1.

1. The Pell’s equation curve $x^2 - 3y^2 = 1$ is stable under the action of the map $\sigma : (x, y) \rightarrow (2x + 3y, 2y + x)$, which “almost” commutes with additive translation.

2. The subspace $x = 0$ is stable under scalar multiplication, which commutes with matrices.
The future

This may be the only way to have counterexamples – by having maps that are related to our original semigroup stabilize the closed subvarieties.
The future

This may be the \textbf{only} way to have counterexamples – by having maps that are related to our original semigroup stabilize the closed subvarieties.

We hope to turn these ideas into a meaningful conjecture.
The future

This may be the **only** way to have counterexamples – by having maps that are related to our original semigroup stabilize the closed subvarieties.

We hope to turn these ideas into a meaningful conjecture. And then to prove it!