Department of Mathematics
Khon Kaen University

Introduction to Arithmetic Dynamics

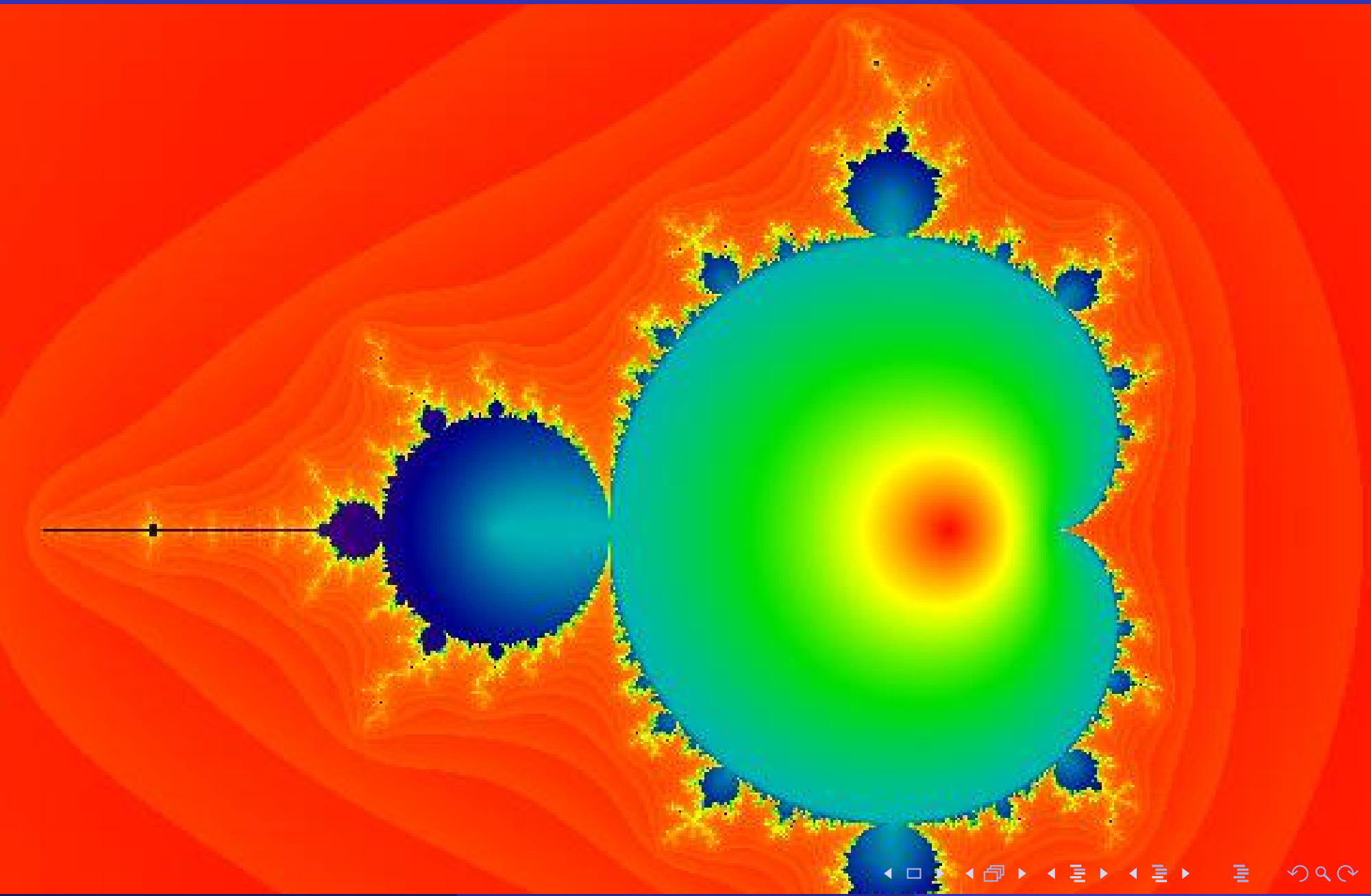
Chatchawan Panraksa

Mahidol University International College

chatchawan.pan@mahidol.edu

2 May 2023

Mandelbrot set $= \{c \in \mathbb{C} | z_0 = 0, z_{n+1} = z_n^2 + c \text{ is bounded}\}$



Some Definitions

- *A **(discrete) dynamical system** is a pair (f, S) of a set S and a map $f : S \longrightarrow S$.*

Some Definitions

- *A **(discrete) dynamical system** is a pair (f, S) of a set S and a map $f : S \longrightarrow S$.*
- *For $n \in \mathbb{N}$, define the n^{th}-**iteration** of f as*

$$f^{(n)} := \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

Some Definitions

- *A **(discrete) dynamical system** is a pair (f, S) of a set S and a map $f : S \longrightarrow S$.*
- *For $n \in \mathbb{N}$, define the n^{th}-**iteration** of f as*

$$f^{(n)} := \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

- *The (forward) **orbit** of $z \in S$ by f is defined as*

$$\mathscr{O}_f(z) := \{z, f(z), f^{(2)}(z), f^{(3)}(z), \dots\}.$$

Some Definitions (continued)

- *A point $z \in S$ is called **periodic** with respect to f if $f^{(k)}(z) = z$ for some $k \in \mathbb{N}$ and we call the smallest such k the **minimal period** of z.*

Some Definitions (continued)

- *A point $z \in S$ is called **periodic** with respect to f if $f^{(k)}(z) = z$ for some $k \in \mathbb{N}$ and we call the smallest such k the **minimal period** of z.*
- *The set of periodic points of f (in S) is denoted by* $\mathrm{Per}(f, S)$.

Some Definitions (continued)

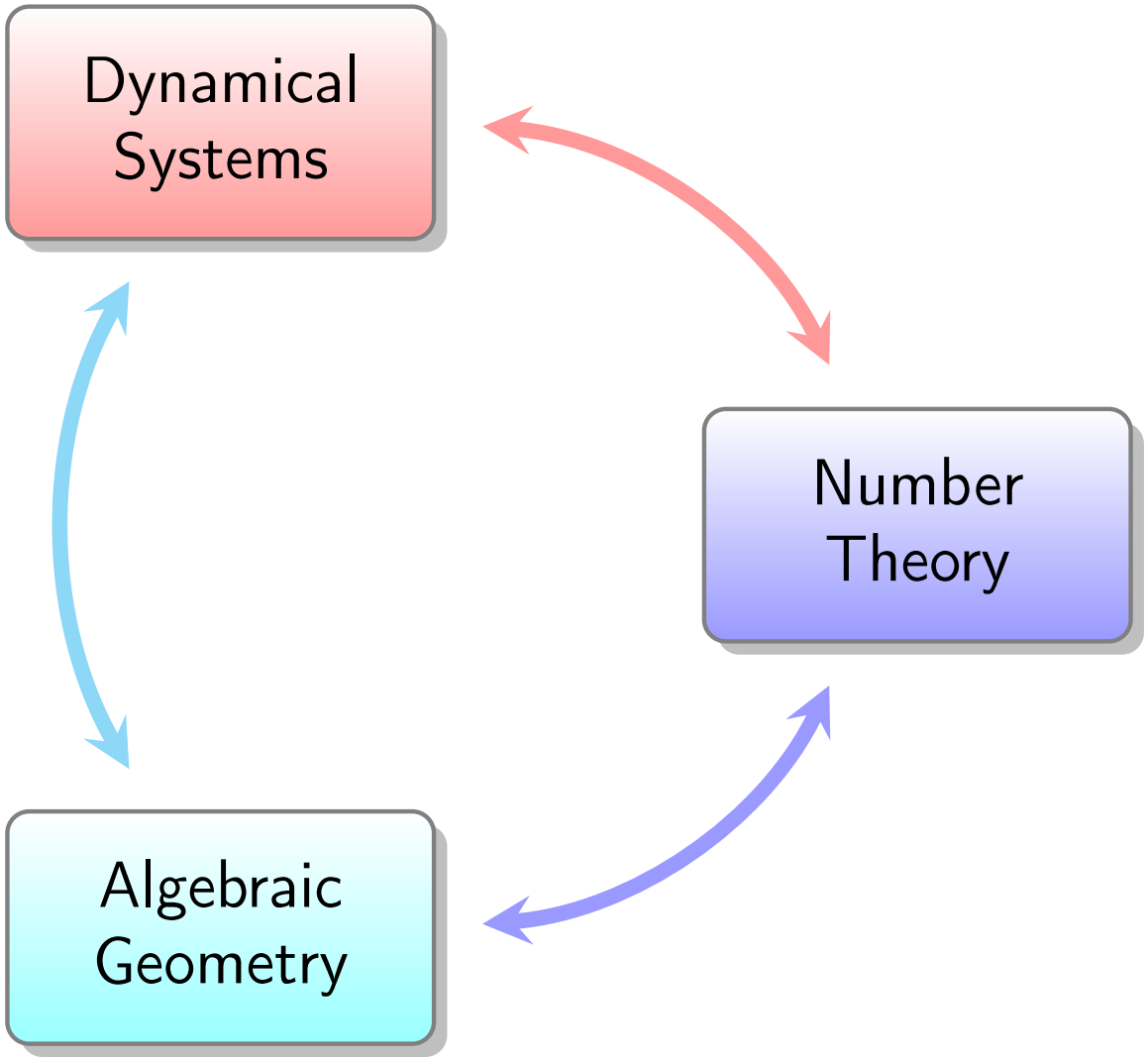
- *A point $z \in S$ is called **periodic** with respect to f if $f^{(k)}(z) = z$ for some $k \in \mathbb{N}$ and we call the smallest such k the **minimal period** of z.*
- *The set of periodic points of f (in S) is denoted by* $\mathrm{Per}(f, S)$.
- *A point $z \in S$ is called **preperiodic** with respect to f if $f^{(k)}(z)$ is periodic for some $k \in N$, which is equivalent to that $\mathscr{O}_f(z)$ is finite. The set of preperiodic points of f (in S) is denoted by* $\mathrm{PrePer}(f, S)$.

Some Definitions (continued)

- *A point $z \in S$ is called **periodic** with respect to f if $f^{(k)}(z) = z$ for some $k \in \mathbb{N}$ and we call the smallest such k the **minimal period** of z.*
- *The set of periodic points of f (in S) is denoted by* $\mathrm{Per}(f, S)$.
- *A point $z \in S$ is called **preperiodic** with respect to f if $f^{(k)}(z)$ is periodic for some $k \in N$, which is equivalent to that $\mathscr{O}_f(z)$ is finite. The set of preperiodic points of f (in S) is denoted by* $\mathrm{PrePer}(f, S)$.
- *We say that a point $z \in S$ is **wandering** if z is not preperiodic.*

For arithmetic interests, we can let S be $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{K}, \ldots$

Arithmetic Dynamics



Example

$\phi(z) = z^2 - \frac{29}{16}$.
Is $z = 0$ preperiodic?

Example

$\phi(z) = z^2 - \frac{29}{16}$.
Is $z = 0$ preperiodic?

$$0 \mapsto -\frac{29}{16} \mapsto \frac{377}{256} \mapsto \frac{23345}{65536} \mapsto \cdots$$

No, it's not preperiodic.

Example

$\phi(z) = z^2 - \frac{29}{16}$.
Is $z = 0$ preperiodic?

$$0 \mapsto -\frac{29}{16} \mapsto \frac{377}{256} \mapsto \frac{23345}{65536} \mapsto \cdots$$

No, it's not preperiodic.
Is $z = \frac{1}{4}$ preperiodic?

$$\frac{1}{4} \mapsto -\frac{7}{4} \mapsto -\frac{5}{4} \mapsto -\frac{1}{4} \mapsto -\frac{7}{4}$$

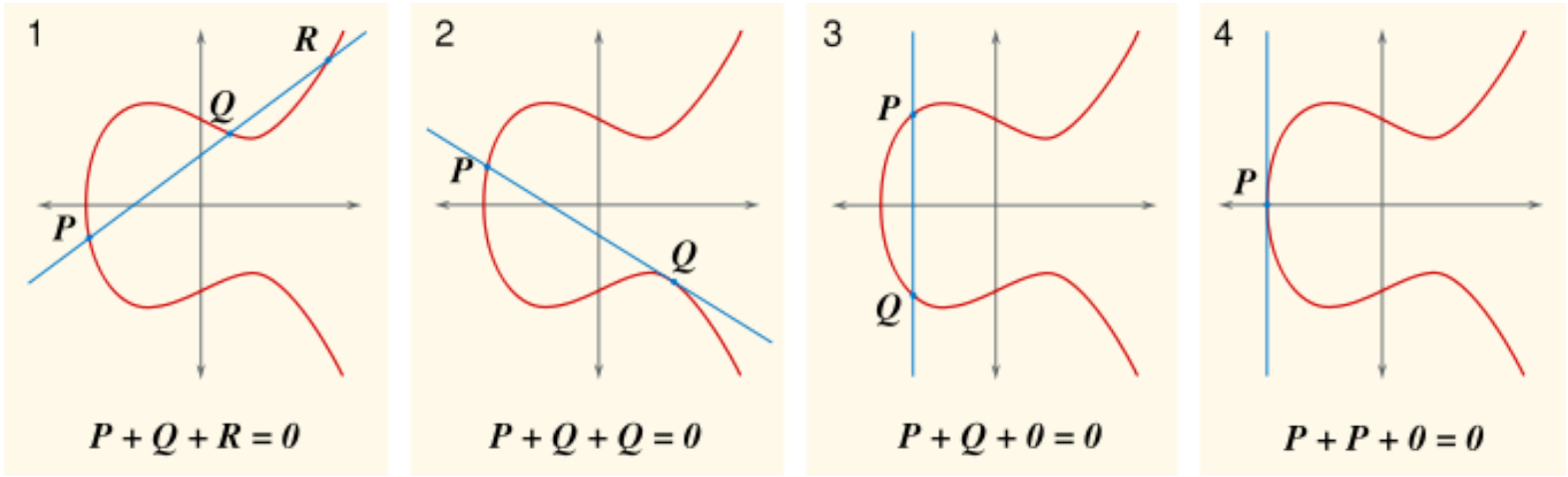
Dictionary

TABLE 1. An arithmetical/dynamical dictionary [218, §6.5]

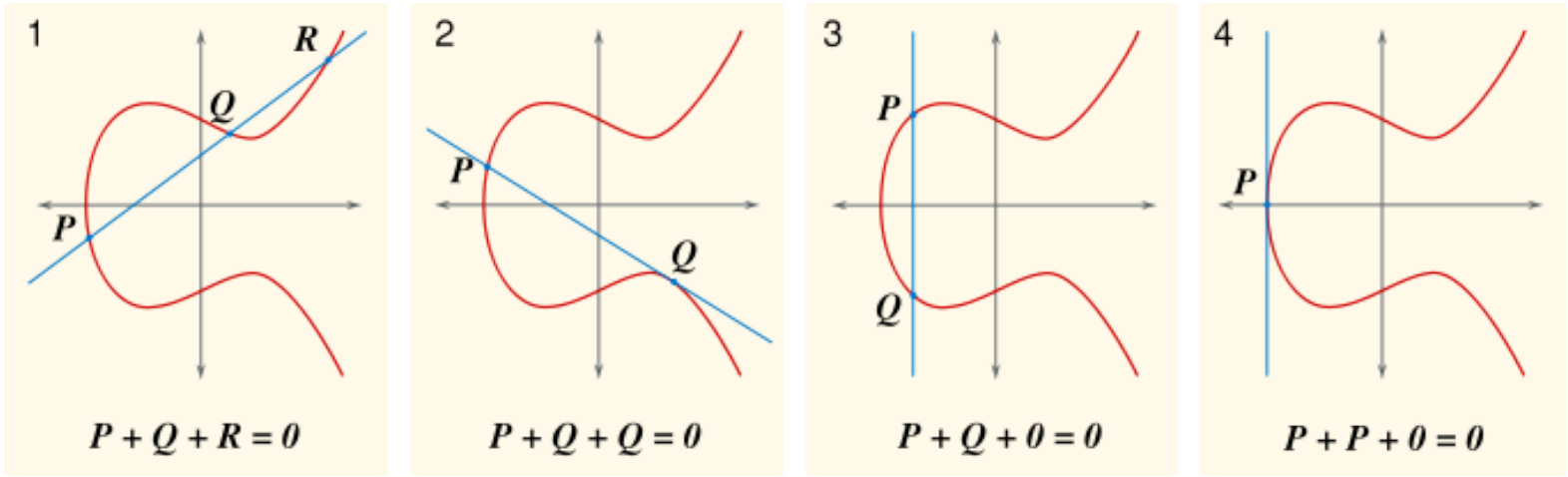
Arithmetic Geometry		**Dynamical Systems**
rational and integral points on varieties	⟷	rational and integral points in orbits
torsion points on abelian varieties	⟷	periodic and preperiodic points of rational maps
abelian varieties with complex multiplication	⟷	post-critically finite rational maps

Figure: From "Current Trends and Open Problems in Arithmetic Dynamics"

Rational map of $E(\mathbb{C}) : y^2 = x^3 + ax + b$

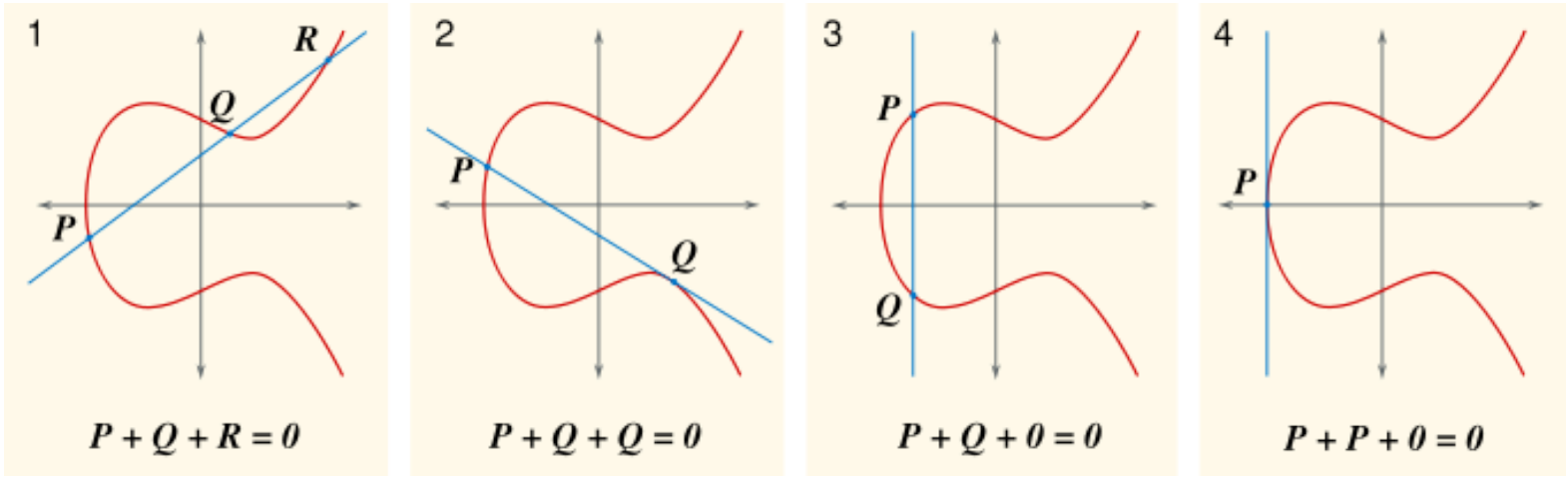


Rational map of $E(\mathbb{C}) : y^2 = x^3 + ax + b$



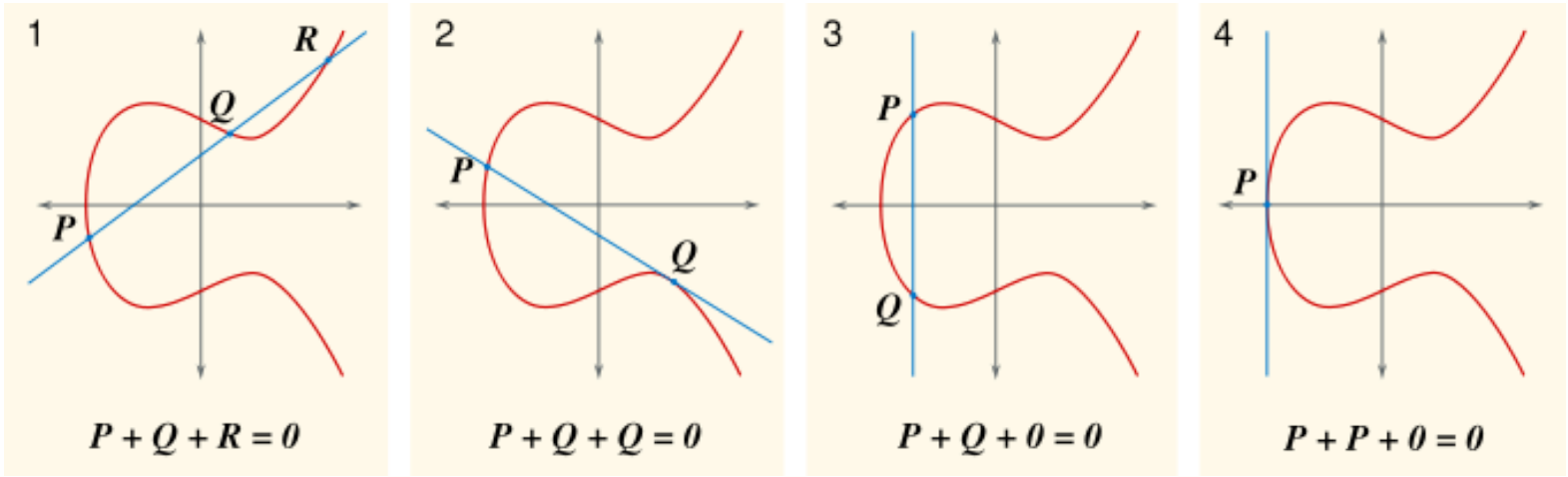
$$E(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}), (x, y) \longmapsto x$$

Rational map of $E(\mathbb{C}) : y^2 = x^3 + ax + b$



$$E(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}), (x, y) \longmapsto x \qquad \begin{array}{ccc} E(\mathbb{C}) & \xrightarrow{[2]} & E(\mathbb{C}) \\ \downarrow x & & \downarrow x \\ \mathbb{P}^1(\mathbb{C}) & \xrightarrow{\phi_{E,2}} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

Rational map of $E(\mathbb{C}) : y^2 = x^3 + ax + b$



$$E(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}), (x,y) \longmapsto x \qquad \begin{array}{ccc} E(\mathbb{C}) & \xrightarrow{[2]} & E(\mathbb{C}) \\ \downarrow x & & \downarrow x \\ \mathbb{P}^1(\mathbb{C}) & \xrightarrow{\phi_{E,2}} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

$$\phi_{E,2}(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b} \text{ (Lattès map)}$$

Torsion points of $E(\mathbb{C}) : y^2 = x^3 + ax + b$

Definition

Let $E(\mathbb{C})$ be an elliptic curve. $(x, y) \in E(\mathbb{C})$ is a **torsion point** if (x, y) has finite order under addition.

Torsion points of $E(\mathbb{C}) : y^2 = x^3 + ax + b$

Definition

Let $E(\mathbb{C})$ be an elliptic curve. $(x, y) \in E(\mathbb{C})$ is a **torsion point** if (x, y) has finite order under addition.

It is equivalent to

"x has finite orbit under $\phi_{E,2}(x) = \dfrac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$."

Torsion points of $E(\mathbb{C}) : y^2 = x^3 + ax + b$

Definition

Let $E(\mathbb{C})$ be an elliptic curve. $(x, y) \in E(\mathbb{C})$ is a **torsion point** if (x, y) has finite order under addition.

It is equivalent to

"x has finite orbit under $\phi_{E,2}(x) = \dfrac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$."

Remark The set of torsion points of an elliptic curve forms a group called "torsion subgroup".

Some results on torsion subgroups

- **Mordell-Weil Theorem(1922)** $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, where $T = E_{tors}(\mathbb{Q})$ is a finite group.

Some results on torsion subgroups

- **Mordell-Weil Theorem(1922)** $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, where $T = E_{tors}(\mathbb{Q})$ is a finite group.
- **Mazur Theorem(1978)** T is isomorphic to one of the following:
  $\mathbb{Z}_n$ with $1 \leq 10$ or $n = 12$,
  $\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$ with $1 \leq n \leq 4$.

Some results on torsion subgroups

- **Mordell-Weil Theorem(1922)** $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$, where $T = E_{tors}(\mathbb{Q})$ is a finite group.
- **Mazur Theorem(1978)** T is isomorphic to one of the following:
  $\mathbb{Z}_n$ with $1 \leq 10$ or $n = 12$,
  $\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$ with $1 \leq n \leq 4$.
- **Merel Theorem(1998)** For every integer $d \geq 1$ there is a constant $N(d)$ such that for all number fields $K/\mathbb{Q}$ of degree at most d and all elliptic curves $E(K)$,

$$E_{tors}(K) \leq N(d).$$

Conjecture (Morton-Silverman Uniform Boundedness, 1994)

There exists a bound $B = B(D, N, d)$ such that if K is a number field of degree D, and $\phi : \mathbb{P}^N(K) \longrightarrow \mathbb{P}^N(K)$ is a morphism of degree $d \geq 2$ defined over K, then the number of preperiodic points of ϕ is bounded by B.

This conjecture is remarkably strong. For $(D, N, d) = (1, 1, 4)$, the conjecture implies that the size of the torsion subgroup of an elliptic curve is uniformly bounded. This can be done via the associated Lattès map. Similarly, for $(D, N, d) = (D, 1, 4)$, the conjecture implies the Merel's theorem.

Theorem (Northcott, 1950)

Let $\phi \in K(z)$ of degree $d \geq 2$. Then

$$\mathrm{PrePer}(\phi, K) < \infty.$$

Theorem (Northcott, 1950)

Let $\phi \in K(z)$ of degree $d \geq 2$. Then

$$\mathrm{PrePer}(\phi, K) < \infty.$$

Conjecture (Morton-Silverman, $\mathbb{Q}$ version)

For any integer $d \geq 2$, there is a constant $C(d)$ such that for any $\phi \in \mathbb{Q}(z)$ of degree d,

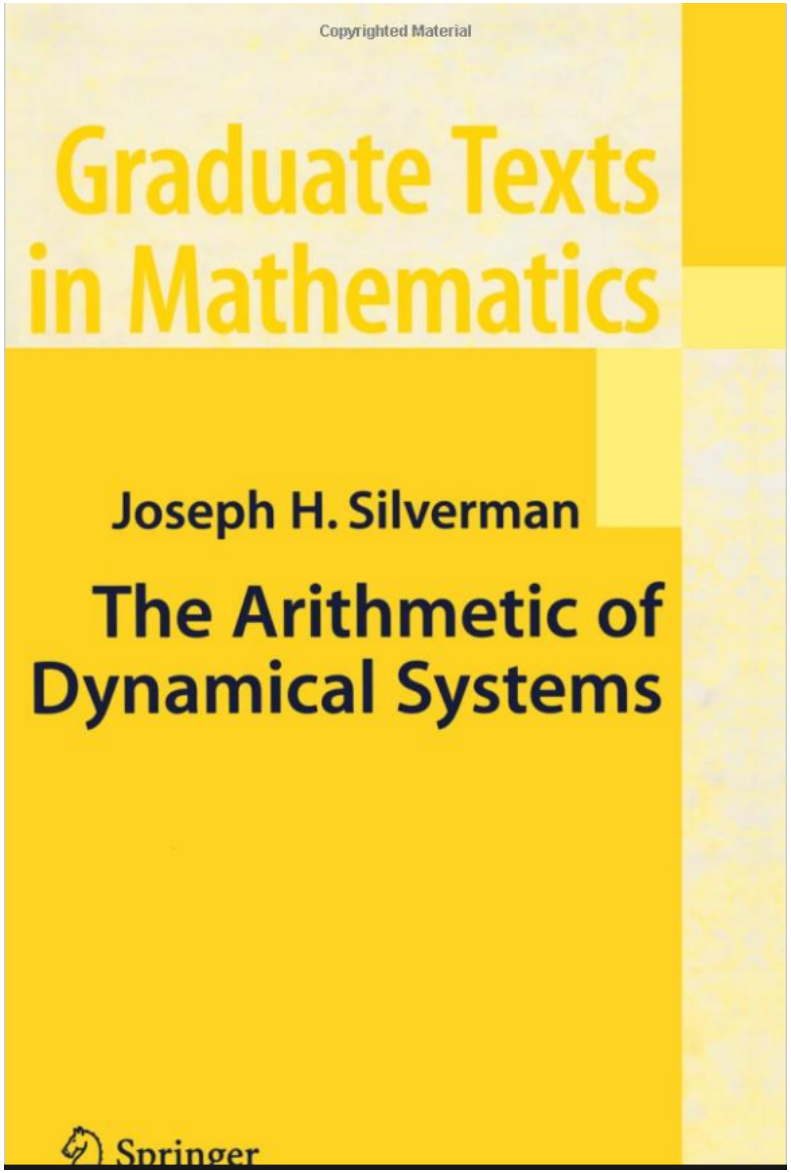
$$\mathrm{PrePer}(\phi) \leq C(d).$$

Theorem (Doyle-Poonen, 2020)

Fix integers $d \geq 2$, $D \geq 1$, and $N \geq 1$. Then there exists $B = B(d, D, N) > 0$ such that for every number field K satisfying $[K : Q] \leq D$ and every $c \in K$, the number of preperiodic points of $z^d + c$ in K with eventual period at most N is at most B.

In the paper, Doyle and Poonen also prove the **strong uniform boundedness theorem for preperiodic points over function fields**.

The ADS by Joseph H. Silverman



CURRENT TRENDS AND OPEN PROBLEMS IN ARITHMETIC DYNAMICS, 2019

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 56, Number 4, October 2019, Pages 611–685
https://doi.org/10.1090/bull/1665
Article electronically published on March 1, 2019

CURRENT TRENDS AND OPEN PROBLEMS IN ARITHMETIC DYNAMICS

ROBERT BENEDETTO, PATRICK INGRAM, RAFE JONES, MICHELLE MANES, JOSEPH H. SILVERMAN, AND THOMAS J. TUCKER

ABSTRACT. Arithmetic dynamics is the study of number theoretic properties of dynamical systems. A relatively new field, it draws inspiration partly from dynamical analogues of theorems and conjectures in classical arithmetic geometry and partly from p-adic analogues of theorems and conjectures in classical complex dynamics. In this article we survey some of the motivating problems and some of the recent progress in the field of arithmetic dynamics.

References

A. Bremner, On the equation $Y^2 = X^5 + k$, *Experiment. Math.* **17** (2008), no. 3, 371–374.

Kwok Chi Chim, T. N. Shorey, and S. B. Sinha, On Baker's explicit abc-conjecture, *Publ. Math. Debrecen* **94** (2019), no. 3-4, 435-453.

J. R. Doyle and B. Poonen, Gonality of dynatomic curves and strong uniform boundedness of preperiodic points, *Compos. Math.* **156** (2020), no. 4, 733-743.

E. V. Flynn, B. Poonen, and E. F. Schaefer, Cycles of quadratic polynomials and rational points on a genus-2 curve, *Duke Math. J.* **90** (1997), no. 3, 435–463.

B. Hutz, Determination of all rational preperiodic points for morphisms of PN, *Math. Comp.* **84** (2015), no. 291, 289–308.

S. Laishram and T. N. Shorey, Baker's explicit *abc*-conjecture and applications, *Acta Arith.* **155** (2012), no. 4, 419–429.

References

N. R. Looper, The Uniform Boundedness and Dynamical Lang Conjectures for polynomials, Preprint available at arXiv:2105.05240.

_____, Dynamical uniform boundedness and the *abc*-conjecture, Invent. Math. **225** (2021), no. 1, 1–44.

P. Morton, Arithmetic properties of periodic points of quadratic maps. II, *Acta Arith*. **87** (1998), no. 2, 89–102.

P. Morton and J. H. Silverman, Rational periodic points of rational functions, *Internat. Math. Res. Notices* **2** (1994), 97–110.

C. Panraksa, Rational periodic points of $x^d + c$ and Fermat-Catalan equations., Int. J. Number Theory **18** (2022), 1111 –1129.

B. Poonen, The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture, *Math Z*. **228** (1998), 11–29.

J. H. Silverman, The arithmetic of dynamical systems, *Graduate Texts in Mathematics*, vol. 241, Springer, New York, 2007.

References

M. Stoll, Rational 6-cycles under iteration of quadratic polynomials, *LMS J. Comput. Math.* **11** (2008), 367–380.

R. Walde and P. Russo, Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$, *Amer. Math. Monthly* **101** (1994), no. 4, 318–331.

THANK YOU!