# A glance into Arithmetic Dynamics

Sebastian Troncoso

January 30, 2018.

#### Overview:

- PART I:
  - Basic definitions and Notations
  - Examples
  - Conjectures
- PART II:
  - Extra hypothesis: Good reduction
  - Results
- PART III:
  - Current research
  - Projects

Arithmetic Dynamics is the study of arithmetic properties of dynamical systems.

Arithmetic Dynamics is the study of arithmetic properties of dynamical systems.

#### Definition

A dynamical system is a pair  $(S, \phi)$  consisting of a set S and a self-map  $\phi: S \to S$ .

Arithmetic Dynamics is the study of arithmetic properties of dynamical systems.

#### **Definition**

A dynamical system is a pair  $(S, \phi)$  consisting of a set S and a self-map  $\phi: S \to S$ .

For example consider

- $(\mathbb{C}, x^6 1)$
- $(\mathbb{R}, \frac{x^3+2}{x^4+7})$
- $(\mathbb{Q}, x^3 + 2)$
- $(\mathbb{Z}, x^2 1)$ .

The goal of dynamics is to study the behavior of points in  ${\cal S}$  as  $\phi$  is applied repeatedly.

The goal of dynamics is to study the behavior of points in S as  $\phi$  is applied repeatedly.

The *n*th iterate of  $\phi$  is denoted by

$$\phi^n(x) = \phi \circ \phi \circ \ldots \circ \phi(x)$$

The goal of dynamics is to study the behavior of points in S as  $\phi$  is applied repeatedly.

The *n*th iterate of  $\phi$  is denoted by

$$\phi^{n}(x) = \phi \circ \phi \circ \ldots \circ \phi(x)$$

The orbit of  $x \in S$  is the set of points obtained by applying the iterates of  $\phi$  to x and it is denoted by

$$\mathcal{O}_{\phi}(x) = \mathcal{O}(x) = \{x, \phi(x), \phi^{2}(x), \phi^{3}(x), \ldots\}$$

$$\mathcal{O}(1) = \{1$$

$$\mathcal{O}(1) = \{1, -1\}$$

$$\mathcal{O}(1) = \{1, -1\}$$
 
$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(1) = \{1, -1\}$$

$$1 \longrightarrow -1\circlearrowleft$$

$$\mathcal{O}(0) = \{0$$

$$\mathcal{O}(1)=\{1,-1\}$$

$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(0) = \{0, -2, 2\}$$

$$\mathcal{O}(1)=\{1,-1\}$$

$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(0) = \{0, -2, 2\}$$

$$0 \longrightarrow -2 \longrightarrow 2 \circlearrowleft$$

$$\mathcal{O}(1)=\{1,-1\}$$

$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(0) = \{0, -2, 2\}$$

$$0 \longrightarrow -2 \longrightarrow 2 \circlearrowleft$$

$$\mathcal{O}(3) = \{3$$

$$\mathcal{O}(1) = \{1, -1\}$$

$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(0) = \{0, -2, 2\}$$

$$0 \longrightarrow -2 \longrightarrow 2 \circlearrowleft$$

$$\mathcal{O}(3) = \{3, 7, 47\}$$

$$\mathcal{O}(1) = \{1, -1\}$$

$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(0) = \{0, -2, 2\}$$

$$0 \longrightarrow -2 \longrightarrow 2 \circlearrowleft$$

$$\mathcal{O}(3) = \{3, 7, 47, 2207, 4870847, 23725150497407, \ldots\}$$

$$\mathcal{O}(1) = \{1, -1\}$$

$$1 \longrightarrow -1 \circlearrowleft$$

$$\mathcal{O}(0) = \{0, -2, 2\}$$

$$0 \longrightarrow -2 \longrightarrow 2 \circlearrowleft$$

$$\mathcal{O}(3) = \{3, 7, 47, 2207, 4870847, 23725150497407, \ldots\}$$

$$3 \rightarrow 7 \longrightarrow 47 \longrightarrow 2207 \longrightarrow 4870847 \longrightarrow 23725150497407 \longrightarrow \ldots$$

$$\mathcal{O}(1)=\{1,-2\}$$

$$\mathcal{O}(1) = \{1, -2\}$$
 
$$1 \longleftrightarrow -2$$

$$\mathcal{O}(1)=\{1,-2\}$$

$$1 \longleftrightarrow -2$$

$$\mathcal{O}(0) = \{0, -3, 6, 33, 1086, \ldots\}$$

$$\mathcal{O}(1) = \{1, -2\}$$

$$1 \longleftrightarrow -2$$

$$\mathcal{O}(0) = \{0, -3, 6, 33, 1086, \ldots\}$$

$$0 \longrightarrow -3 \longrightarrow 6 \longrightarrow 33 \longrightarrow 1086 \longrightarrow \ldots$$



Given a dynamical system  $(S, \phi)$ . There are two possibilities for the orbits of a point  $P \in S$ 

• If the orbit  $\mathcal{O}_{\phi}(P)$  is infinite, we say that P is a **wandering point**.

Given a dynamical system  $(S, \phi)$ . There are two possibilities for the orbits of a point  $P \in S$ 

- If the orbit  $\mathcal{O}_{\phi}(P)$  is infinite, we say that P is a **wandering point**.
- If the orbit  $\mathcal{O}_{\phi}(P)$  is finite, we say that P is a **preperiodic point**.

Given a dynamical system  $(S, \phi)$ . There are two possibilities for the orbits of a point  $P \in S$ 

• If the orbit  $\mathcal{O}_{\phi}(P)$  is infinite, we say that P is a **wandering point**.

• If the orbit  $\mathcal{O}_{\phi}(P)$  is finite, we say that P is a **preperiodic point**.

A important subset of the preperiodic points consists of those points whose orbit eventually return to its starting point. These points are called **periodic points**.

$$1 \longrightarrow 0 \longleftrightarrow -1$$

- 1 is preperiodic.
- ullet 0 and -1 are periodic.
- $\bullet$  Every other element of  $\mathbb Q$  is a wandering point.

Consider the dynamical system  $(\mathbb{Q}, x^2 - 1)$ . Then

$$1\longrightarrow 0\longleftrightarrow -1$$

- 1 is preperiodic.
- ullet 0 and -1 are periodic.
- $\bullet$  Every other element of  $\mathbb Q$  is a wandering point.

#### **SEE SAGE**



Arithmetic Dynamics is the study of arithmetic properties of dynamical systems.

Arithmetic Dynamics is the study of arithmetic properties of dynamical systems.

From now on we will always consider the dynamical system  $(\mathbb{Q}, f)$  where f is a polynomial of degree d with coefficients in  $\mathbb{Q}$ .

Arithmetic Dynamics is the study of arithmetic properties of dynamical systems.

From now on we will always consider the dynamical system  $(\mathbb{Q}, f)$  where f is a polynomial of degree d with coefficients in  $\mathbb{Q}$ .

#### **Notation**

The set of preperiodic and periodic points of a map  $f:\mathbb{Q}\to\mathbb{Q}$  are denoted respectively by

 $PrePer(f, \mathbb{Q})$  and  $Per(f, \mathbb{Q}.)$ 

• Are the sets  $Per(f, \mathbb{Q})$  and  $PrePer(f, \mathbb{Q})$  finite?

• Are the sets  $Per(f, \mathbb{Q})$  and  $PrePer(f, \mathbb{Q})$  finite?

Yes.

• Are the sets  $Per(f, \mathbb{Q})$  and  $PrePer(f, \mathbb{Q})$  finite?

Yes.

### Theorem (Northcott 1950)

Let  $f: \mathbb{Q} \to \mathbb{Q}$  be an polynomial of degree  $\geq 2$  with coefficients on  $\mathbb{Q}$ . Then f has only finitely many preperiodic points in  $\mathbb{Q}$ .

• Are the sets  $Per(f, \mathbb{Q})$  and  $PrePer(f, \mathbb{Q})$  finite?

Yes.

#### Theorem (Northcott 1950)

Let  $f: \mathbb{Q} \to \mathbb{Q}$  be an polynomial of degree  $\geq 2$  with coefficients on  $\mathbb{Q}$ . Then f has only finitely many preperiodic points in  $\mathbb{Q}$ .

- How large is the set  $PrePer(f, \mathbb{Q})$ ?
- Can you give an explicit bound?
- How is the bound depending on f?

#### Uniform Boundedness Conjecture:

Consider f(x) = (x-1)(x-2)(x-3)...(x-d) + x. Can you see that f has at least d periodic points?

### Uniform Boundedness Conjecture:

Consider f(x) = (x-1)(x-2)(x-3)...(x-d) + x. Can you see that f has at least d periodic points?

- $1 \circlearrowleft$
- 2 🔿
  - ÷
- $d \circlearrowleft$

### Uniform Boundedness Conjecture:

Consider f(x) = (x-1)(x-2)(x-3)...(x-d) + x. Can you see that f has at least d periodic points?

- 1 🔿
- 2 🔿
  - :
- d ♂

#### Conjecture (Uniform Boundedness Conjecture - Morton–Silverman 1994)

Let  $f: \mathbb{Q} \to \mathbb{Q}$  be a polynomial of degree  $d \geq 2$  with coefficients in  $\mathbb{Q}$ . Then there exists a bound B = B(d) such that

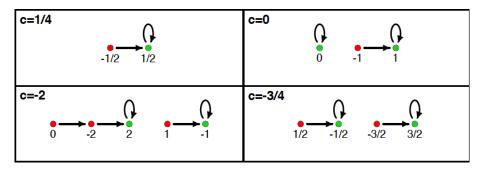
$$|\mathsf{PrePer}(\phi,\mathbb{Q})| \leq B.$$

↓□▶ ↓□▶ ↓□▶ ↓□▶ ↓□ ♥ ♀○

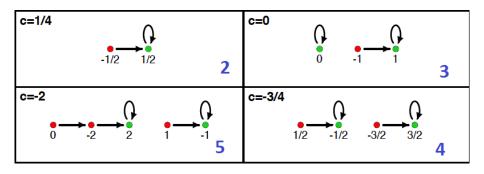
#### Quadratic functions:

Lets study quadratic Polynomials.

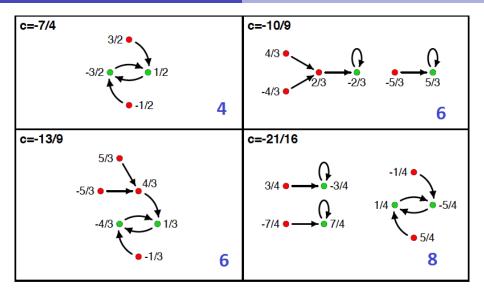
Even more, assume  $f_c(x) = x^2 + c$  with  $c \in \mathbb{Q}$ .



Diagrams of purely preperiodic points (red) and periodic points (green) of  $f_c(z) = z^2 + c$  in  $\mathbb{Q}$ .



Diagrams of purely preperiodic points (red) and periodic points (green) of  $f_c(z) = z^2 + c$  in  $\mathbb{Q}$ .



Diagrams of purely preperiodic points (red) and periodic points (green) of  $f_c(z) = z^2 + c$  in  $\mathbb{Q}$ .

Sebastian Troncoso Arithmetic Dynamics

15 / 31

#### Conjecture:

Let f be a quadratic polynomial of the form  $f_c(z)=z^2+c$  with  $c\in\mathbb{Q}$ . Then

$$|PrePer(f_c, \mathbb{Q})| \leq 8$$

#### **Conjecture:** Question:

Let f be a quadratic polynomial of the form  $f_c(z) = z^2 + c$  with  $c \in \mathbb{Q}$ . Then

$$|PrePer(f_c, \mathbb{Q})| \leq 8$$

#### Conjecture: Question:

Let f be a quadratic polynomial of the form  $f_c(z) = z^2 + c$  with  $c \in \mathbb{Q}$ . Then

$$|PrePer(f_c, \mathbb{Q})| \leq 8$$

# **USE SAGE**

#### Poonen's Conjecture

#### Conjecture (Poonen's Conjecture 1998)

Let  $f:\mathbb{Q}\to\mathbb{Q}$  be a quadratic polynomial with coefficients in  $\mathbb{Q}$ . Then

 $|\mathsf{PrePer}(\phi, \mathbb{Q})| \leq 8.$ 

If  $f = x^2 + d$  then B. Hutz and P. Ingram have shown that Poonen's conjecture holds when the numerator and denominator of d don't exceed  $10^8$ .

#### PART II:

- Extra hypothesis: Good/Bad Reduction.
- Results

Let  $\mathfrak{p}$  be a prime number in  $\mathbb{Z}$  and  $f(x) = \frac{a_d}{b_d} x^d + \ldots + \frac{a_1}{b_1} x + \frac{a_0}{b_0}$  be a polynomial with coefficients in  $\mathbb{Q}$ .

Let  $\mathfrak p$  be a prime number in  $\mathbb Z$  and  $f(x)=\frac{a_d}{b_d}x^d+\ldots+\frac{a_1}{b_1}x+\frac{a_0}{b_0}$  be a polynomial with coefficients in  $\mathbb Q$ .

• We say that f has **good reduction** at  $\mathfrak{p}$  if  $\mathfrak{p} \nmid a_d$  and  $\mathfrak{p} \nmid b_d$ .

Sebastian Troncoso

Let  $\mathfrak p$  be a prime number in  $\mathbb Z$  and  $f(x)=\frac{a_d}{b_d}x^d+\ldots+\frac{a_1}{b_1}x+\frac{a_0}{b_0}$  be a polynomial with coefficients in  $\mathbb Q$ .

- We say that f has **good reduction** at  $\mathfrak{p}$  if  $\mathfrak{p} \nmid a_d$  and  $\mathfrak{p} \nmid b_d$ .
- Otherwise, we say that f has **bad reduction** at  $\mathfrak{p}$ .



Let  $\mathfrak p$  be a prime number in  $\mathbb Z$  and  $f(x)=\frac{a_d}{b_d}x^d+\ldots+\frac{a_1}{b_1}x+\frac{a_0}{b_0}$  be a polynomial with coefficients in  $\mathbb Q$ .

- We say that f has **good reduction** at  $\mathfrak{p}$  if  $\mathfrak{p} \nmid a_d$  and  $\mathfrak{p} \nmid b_d$ .
- Otherwise, we say that f has **bad reduction** at  $\mathfrak{p}$ .

#### **Definition**

Let S be a finite set of primes of  $\mathbb{Z}$  and f a polynomial of degree d with coefficients in  $\mathbb{Q}$ . We say that f has **good reduction outside** S if f has good reduction at  $\mathfrak{p}$  for every  $\mathfrak{p} \notin S$ .

40140101010

• Consider  $f(x) = 15x^3 + 5x - 4$ . Can you find the primes of bad reduction?



Consider f(x) = 15x<sup>3</sup> + 5x - 4.
 Can you find the primes of bad reduction?
 Yes, 3 and 5 are primes of bad reduction for f.

If we set  $S = \{3, 5\}$  then f has good reduction outside S.

Consider f(x) = 15x<sup>3</sup> + 5x - 4.
 Can you find the primes of bad reduction?
 Yes, 3 and 5 are primes of bad reduction for f.

If we set  $S = \{3, 5\}$  then f has good reduction outside S.

② Consider  $f(x) = x^7 + 2x - 2$ . Can you find the primes of bad reduction?

Consider f(x) = 15x<sup>3</sup> + 5x - 4.
 Can you find the primes of bad reduction?
 Yes, 3 and 5 are primes of bad reduction for f.

If we set  $S = \{3, 5\}$  then f has good reduction outside S.

2 Consider  $f(x) = x^7 + 2x - 2$ . Can you find the primes of bad reduction?

If we set  $S = \emptyset$  then f has good reduction outside S.

• Consider  $f(x) = 15x^3 + 5x - 4$ . Can you find the primes of bad reduction? **Yes**, 3 and 5 are primes of bad reduction for f.

If we set  $S = \{3, 5\}$  then f has good reduction outside S.

Consider f(x) = x<sup>7</sup> + 2x - 2.
 Can you find the primes of bad reduction?
 No.

If we set  $S = \emptyset$  then f has good reduction outside S.

If we allow the number of primes of bad reduction as a parameter, much more is known for the cardinality of the set of preperiodic points.

Sebastian Troncoso Arithmetic Dynamics January 30, 2018. 21 / 31

#### **Theorem**

Let  $f:\mathbb{Q}\to\mathbb{Q}$  be a polynomial of degree  $d\geq 2$  with coefficients in  $\mathbb{Q}$ . Suppose f has good reduction outside a finite set of primes S and denote s=|S|. Then

#### **Theorem**

Let  $f:\mathbb{Q}\to\mathbb{Q}$  be a polynomial of degree  $d\geq 2$  with coefficients in  $\mathbb{Q}$ . Suppose f has good reduction outside a finite set of primes S and denote s=|S|. Then

•  $|PrePer(f, \mathbb{Q})| \le d^{2^{16s}(s \log(s))}$ J.K. Canci and L. Paladino (2015).

#### **Theorem**

Let  $f:\mathbb{Q}\to\mathbb{Q}$  be a polynomial of degree  $d\geq 2$  with coefficients in  $\mathbb{Q}$ . Suppose f has good reduction outside a finite set of primes S and denote s=|S|. Then

- $|PrePer(f, \mathbb{Q})| \le d^{2^{16s}(s \log(s))}$ J.K. Canci and L. Paladino (2015).
- $|\mathit{PrePer}(f,\mathbb{Q})| \leq 5\left(2^{16sd^3}\right) + 3$ S. Troncoso (2017).

#### **Theorem**

Let  $f:\mathbb{Q}\to\mathbb{Q}$  be a polynomial of degree  $d\geq 2$  with coefficients in  $\mathbb{Q}$ . Suppose f has good reduction outside a finite set of primes S and denote s=|S|. Then

- $|PrePer(f, \mathbb{Q})| \le d^{2^{16s}(s \log(s))}$ J.K. Canci and L. Paladino (2015).
- $|PrePer(f, \mathbb{Q})| \le 5\left(2^{16sd^3}\right) + 3$ S. Troncoso (2017).
- $|PrePer(f, \mathbb{Q})| \le \alpha d^2 + \beta d + \gamma$  where  $\alpha$ ,  $\beta$  and  $\gamma$  are roughly  $2^{78s}$ .

  J.K. Canci, S. Troncoso and S. Vishkautsan (submitted).

The previous theorem use some important results like:

• Riemann-Hurwitz formula

- Riemann-Hurwitz formula
- Baker's Theorem on existence of periodic points

- Riemann-Hurwitz formula
- Baker's Theorem on existence of periodic points
- Kisaka's analysis on Baker's Theorem

- Riemann-Hurwitz formula
- Baker's Theorem on existence of periodic points
- Kisaka's analysis on Baker's Theorem
- Logarithmic *p*-adic chordal distance.

- Riemann-Hurwitz formula
- Baker's Theorem on existence of periodic points
- Kisaka's analysis on Baker's Theorem
- Logarithmic p-adic chordal distance.
- Study the distance between periodic and purely preperiodic points.

- Riemann-Hurwitz formula
- Baker's Theorem on existence of periodic points
- Kisaka's analysis on Baker's Theorem
- Logarithmic p-adic chordal distance.
- Study the distance between periodic and purely preperiodic points.
- Number of solution of the *S*-unit equation.

# More general setting



### More general setting

$$\mathbb{Q} \Longrightarrow \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$$

#### More general setting

$$\mathbb{Q} \Longrightarrow \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\} \Longrightarrow \mathbb{P}^1(K)$$

where K is a number field *i.e* a finite field extension of  $\mathbb{Q}$ .

#### More general setting

$$\mathbb{Q} \Longrightarrow \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\} \Longrightarrow \mathbb{P}^1(K)$$

where K is a number field *i.e* a finite field extension of  $\mathbb{Q}$ .

 $f(x) = a_d x^d \dots + a_1 x + a_0$  a polynomial with coefficients in  $\mathbb{Q}$ .

#### More general setting

$$\mathbb{Q} \Longrightarrow \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\} \Longrightarrow \mathbb{P}^1(K)$$

where K is a number field *i.e* a finite field extension of  $\mathbb{Q}$ .

$$f(x) = a_d x^d \dots + a_1 x + a_0$$
 a polynomial with coefficients in  $\mathbb{Q}$ .  $\Downarrow$ 

 $\phi(x) = \frac{p(x)}{q(x)}$  where f and g are polynomials with coefficients in  $\mathbb{Q}$ .

#### More general setting

$$\mathbb{Q} \Longrightarrow \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\} \Longrightarrow \mathbb{P}^1(K)$$

where K is a number field *i.e* a finite field extension of  $\mathbb{Q}$ .

$$f(x) = a_d x^d \dots + a_1 x + a_0$$
 a polynomial with coefficients in  $\mathbb{Q}$ .  $\Downarrow$ 

$$\phi(x) = \frac{p(x)}{q(x)}$$
 where  $f$  and  $g$  are polynomials with coefficients in  $\mathbb{Q}$ .

$$\phi(x) = \frac{p(x)}{q(x)}$$
 where f and g are polynomials with coefficients in K.

#### PART III:

- Current Research
- Projects

#### Current project

# Arithmetic dynamics in higher dimension

#### Notation of preperiodic hypersurfaces

Let  $\phi$  be a function (polynomial in several variables) and H an irreducible hypersurface.

#### Notation of preperiodic hypersurfaces

Let  $\phi$  be a function (polynomial in several variables) and H an irreducible hypersurface.

**Periodic hypersurface**:  $\phi^n(H) = H$  for some  $n \ge 1$ .

**Preperiodic hypersurface**:  $\exists m \geq 0$  such that  $\phi^m(H)$  The set of preperiodic hypersurface is denoted by  $HPrePer(\phi, \mathbb{Q})$ . The set of preperiodic hypersurface of degree e is denoted by  $HPrePer(\phi, \mathbb{Q}, e)$ .

• Is the set  $HPrePer(\phi, \mathbb{Q})$  finite?

• Is the set  $HPrePer(\phi, \mathbb{Q})$  finite?

No.

• Is the set  $HPrePer(\phi, \mathbb{Q})$  finite?

No.

• Is the set  $HPrePer(\phi, \mathbb{Q}, e)$  finite?

• Is the set  $HPrePer(\phi, \mathbb{Q})$  finite?

No.

• Is the set  $HPrePer(\phi, \mathbb{Q}, e)$  finite?

Yes.

• Is the set  $HPrePer(\phi, \mathbb{Q})$  finite?

No.

• Is the set  $HPrePer(\phi, \mathbb{Q}, e)$  finite?

Yes.

#### Theorem (B. Hutz 2016)

Let  $\phi$  be a function. Then there are only finitely many preperiodic hypersurfaces of degree e.

#### Project 1: Data base of preperiodic hypersurfaces

Use Sage to provide examples of preperiodic hypersurfaces.

#### Project 1: Data base of preperiodic hypersurfaces

- Use Sage to provide examples of preperiodic hypersurfaces.
- The goal is to state "Uniform Boundedness Conjecture" and provide evidence for such a conjecture.

Let S be a finite set of primes of  $\mathbb{Z}$  and  $\mathbb{Z}_S^*$  be the group of S-units *i.e.*  $\mathbb{Z}_S^*$  is the set of fraction of the form  $\frac{a}{b}$  where a and b are not divisible by primes not in S.

Let S be a finite set of primes of  $\mathbb{Z}$  and  $\mathbb{Z}_S^*$  be the group of S-units *i.e.*  $\mathbb{Z}_S^*$  is the set of fraction of the form  $\frac{a}{b}$  where a and b are not divisible by primes not in S.

A linear relation of the form

$$u + v = 1$$

where  $(u, v) \in (\mathbb{Z}_S^*)^2$  is called a *S*-unit equation.

Let S be a finite set of primes of  $\mathbb{Z}$  and  $\mathbb{Z}_S^*$  be the group of S-units *i.e.*  $\mathbb{Z}_S^*$  is the set of fraction of the form  $\frac{a}{b}$  where a and b are not divisible by primes not in S.

A linear relation of the form

$$u + v = 1$$

where  $(u, v) \in (\mathbb{Z}_S^*)^2$  is called a *S*-unit equation.

 Beukers and Schlickewei give an explicit bound for the number of solution of a S-unit equation.

Let S be a finite set of primes of  $\mathbb{Z}$  and  $\mathbb{Z}_S^*$  be the group of S-units *i.e.*  $\mathbb{Z}_S^*$  is the set of fraction of the form  $\frac{a}{b}$  where a and b are not divisible by primes not in S.

A linear relation of the form

$$u + v = 1$$

where  $(u, v) \in (\mathbb{Z}_S^*)^2$  is called a *S*-unit equation.

- Beukers and Schlickewei give an explicit bound for the number of solution of a S-unit equation.
- An interesting project will be to understand application in mathematics of Beukers and Schlickewei's result.

# THANK YOU