

# Improving Julia Robinson (conjecturally)

by Gunther Cornelissen (Utrecht) *and* Karim Zahidi (Antwerp)



## Julia Robinson's result (1949)



$\mathbb{Z}$  can be defined in  $\mathbb{Q}$   
by a *first-order formula*.

How close is it to being diophantine?

- First-order formula in  $\mathbb{Q}$  can always be put into **positive prenex form**:

$$(\forall x_1^{(1)} \dots \forall x_{f_1}^{(1)})(\exists y_1^{(1)} \dots \exists y_{e_1}^{(1)}) \dots (\forall x_1^{(N)} \dots \forall x_{f_N}^{(N)})(\exists y_1^{(N)} \dots \exists y_{e_N}^{(N)})(F(\mathbf{x}, \mathbf{y}) = 0),$$

with  $e_i > 0$  for  $i = 1, \dots, N - 1$  and  $f_i > 0$  for all  $i = 2, \dots, N$ ; where  $F$  is a polynomial in multi-variables  $\mathbf{x} = (x_1^{(1)}, \dots, x_{f_1}^{(1)}, \dots, x_1^{(N)}, \dots, x_{f_N}^{(N)})$  and  $\mathbf{y} = (y_1^{(1)}, \dots, y_{e_1}^{(1)}, \dots, y_1^{(N)}, \dots, y_{e_N}^{(N)})$ .

- A **diophantine** formula has  $N = 1, f_1 = 0$ .

## The positive arithmetical hierarchy $(\Sigma^+, \Pi^+)$

Let  $\Sigma_0^+ = \Pi_0^+$  denote the set of positive boolean combinations of atomic formulæ.

Define a formula  $\mathcal{F}$  inductively to be in  $\Sigma_n^+$  if it is of the form  $\exists \mathcal{G}$  with  $\mathcal{G} \in \Pi_{n-1}^+$ .

Define a formula  $\mathcal{F}$  inductively to be in  $\Pi_n^+$  if it is of the form  $\forall \mathcal{G}$  with  $\mathcal{G} \in \Sigma_{n-1}^+$ .

### Examples.

- $(\forall x, y)(\exists z)(x^{17} + y^3 = z^{2005})$  is  $\Pi_2^+$
- $(\exists x, y)(\forall z, t)(\exists u)(xyztu = 1)$  is  $\Sigma_3^+$

A formula in  $\Sigma_1^+$  is *diophantine*. For  $\mathbf{Z}$  or  $\mathbf{Q}$ , formulæ in  $\Sigma_0^+$  are equivalent to *atomic* formulæ.

By (syntax/semantics) abuse, we will from now on sometimes write that  $\mathcal{F} \in \Sigma_n^+$  if  $\mathcal{F}$  is equivalent to a formula in  $\Sigma_n^+$  in the given theory.

## Two measures of complexity

$$\mathcal{F} : (\forall x_1^{(1)} \dots \forall x_{f_1}^{(1)}) (\exists y_1^{(1)} \dots \exists y_{e_1}^{(1)}) \dots (\forall x_1^{(N)} \dots \forall x_{f_N}^{(N)}) (\exists y_1^{(N)} \dots \exists y_{e_N}^{(N)}) (F(\mathbf{x}, \mathbf{y}) = 0)$$

- The **number of quantifier changes** is

$$c(\mathcal{F}) := \begin{cases} 2N - 1 & \text{if } f_1 e_N \neq 0, \\ 2N - 2 & \text{if one of } f_1, e_N = 0 \\ 2N - 3 & \text{if } f_1 = e_N = 0. \end{cases}$$

In terms of the hierarchy, this means the following: if  $\mathcal{F} \in \Sigma_{n+1}^+ - \Pi_n^+$  or  $\mathcal{F} \in \Pi_{n+1}^+ - \Sigma_n^+$ , then  $c(\mathcal{F}) = n$ .

- The **total number of universal quantifiers**  $t$  is

$$t(\mathcal{F}) = f_1 + \dots + f_N.$$

## Complexity of models

- ▶ A **model** of  $\mathbf{Z}$  in  $\mathbf{Q}$  is a **definable** subset  $D$  of  $\mathbf{Q}^N$  and a bijection  $\iota : Z \rightarrow D \subseteq \mathbf{Q}^N$  such that the graphs of addition and multiplication are mapped to **definable** subsets of  $\mathbf{Q}^{3N}$ .
- ▶ Note: **diophantine model** has **diophantine** instead of **definable**.
- ▶ If  $\mathbf{Z}$  has a diophantine model in  $\mathbf{Q}$ , then  $\text{HTP}(\mathbf{Q})$  has a negative answer and Mazur's conjecture is wrong (CZ, 1999).

## Complexity of models

- ▶ A **model** of  $\mathbf{Z}$  in  $\mathbf{Q}$  is a **definable** subset  $D$  of  $\mathbf{Q}^N$  and a bijection  $\iota : Z \rightarrow D \subseteq \mathbf{Q}^N$  such that the graphs of addition and multiplication are mapped to **definable** subsets of  $\mathbf{Q}^{3N}$ .
- ▶ Models can be used to **translate formulæ** (true sentences  $\Rightarrow$  true sentences).

**Example.**  $(\exists x_1)(\forall x_2)(x_1^2 x_2 + x_2 = 0)$  in  $\mathbf{Z}$  in a 2-dimensional model  $D \subseteq \mathbf{Q}^2$  of  $\mathbf{Z}$  in  $\mathbf{Q}$  translates into

$$\begin{aligned}
 & (\exists y_1^1 y_1^2)(\forall y_2^1 y_2^2)(\exists u_1 u_2 v_1 v_2)[(y_1^1, y_1^2) \in D \wedge [(y_2^1, y_2^2) \in D \Rightarrow \\
 & [(y_1^1, y_1^2, y_1^1, y_1^2, u_1, u_2) \in \iota(\times) \wedge (y_2^1, y_2^2, u_1, u_2, v_1, v_2) \in \iota(\times) \wedge \\
 & (y_2^1, y_2^2, v_1, v_2, \iota(0)) \in \iota(+)]]]
 \end{aligned}$$

further replace membership of  $D$ ,  $\iota(+)$  and  $\iota(\times)$  by their first-order definitions. Note: “dummy variables”  $u_i, v_i$  to unravel nested occurrences of  $+$  and  $\times$ .

## Complexity of models

- ▶ A **model** of  $\mathbf{Z}$  in  $\mathbf{Q}$  is a **definable** subset  $D$  of  $\mathbf{Q}^N$  and a bijection  $\iota : Z \rightarrow D \subseteq \mathbf{Q}^N$  such that the graphs of addition and multiplication are mapped to **definable** subsets of  $\mathbf{Q}^{3N}$ .
- ▶ Can define  $t$ - and  $c$ -**complexity of a model** of  $\mathbf{Z}$  in  $\mathbf{Q}$  as the maximal  $t$ - or  $c$ - complexity of the formula defining  $D$  and the images of the graphs of  $+$  and  $\times$  (note: syntax/semantics abuse); and one can follow the complexity, e.g.

**Lemma.** *If  $(D, \iota)$  is a model of  $\mathbf{Z}$  in  $\mathbf{Q}$  with  $D$  and  $\iota(+)$  diophantine and  $t(\iota(\times)) \leq 1$ , then  $\Sigma_1^+$ -sentences are translated into  $\Sigma_3^+$ -sentences (so DMPR  $\Rightarrow \Sigma_3^+$ -theory of  $\mathbf{Q}$  is undecidable).*

## Three complexities

- ▶ **Lemma.** *The complexity of Julia Robinson's definition of  $\mathbf{Z}$  in  $\mathbf{Q}$  is  $\Pi_4^+$  with  $t(\mathcal{F}) = 8$  and  $c(\mathcal{F}) = 3$ ; hence it says that the  $\Sigma_5^+$ -theory of  $\mathbf{Q}$  is undecidable.*
- ▶ Let  $\phi(A, B, K)$  denote the formula  $(\exists X, Y, Z)(P_{A,B,K}^{X,Y,Z} = 0)$  with  $P_{A,B,K}^{X,Y,Z} = 2 + ABK^2 + BZ^2 - X^2 - AY^2$ . Then for  $N \in \mathbf{Q}$ , we have  $N \in \mathbf{Z} \iff \forall A, B \{ [\phi(A, B, 0) \wedge (\forall M)(\phi(A, B, M) \Rightarrow \phi(A, B, M+1))] \Rightarrow \phi(A, B, N) \}$

## Three complexities

- ▶ **Lemma.** *The complexity of Julia Robinson's definition of  $\mathbf{Z}$  in  $\mathbf{Q}$  is  $\Pi_4^+$  with  $t(\mathcal{F}) = 8$  and  $c(\mathcal{F}) = 3$ ; hence it says that the  $\Sigma_5^+$ -theory of  $\mathbf{Q}$  is undecidable.*
- ▶ **Observation.** *HTP( $\mathbf{Q}$ ) is equivalent to: the  $\Sigma_1^+$ -theory of  $\mathbf{Q}$  is undecidable.*

## Three complexities

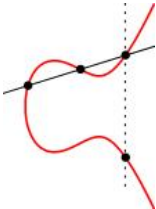
- ▶ **Lemma.** *The complexity of Julia Robinson's definition of  $\mathbf{Z}$  in  $\mathbf{Q}$  is  $\Pi_4^+$  with  $t(\mathcal{F}) = 8$  and  $c(\mathcal{F}) = 3$ ; hence it says that the  $\Sigma_5^+$ -theory of  $\mathbf{Q}$  is undecidable.*
- ▶ **Observation.** *HTP( $\mathbf{Q}$ ) is equivalent to: the  $\Sigma_1^+$ -theory of  $\mathbf{Q}$  is undecidable.*
- ▶ **Main Theorem (C-Zahidi, ArXiv:math.NT/0412473).** *If the following conjecture  $\mathbf{C}$  about elliptic curves is true, then  $\mathbf{Z}$  has a model in  $\mathbf{Q}$  with  $t$ - and  $c$ -complexity  $\leq 1$ ; and the  $\Sigma_3^+$ -theory of  $\mathbf{Q}$  is undecidable.*

## Diophantine models and elliptic curves

Typical (partial) diophantine model arises as follows: let  $E$  be an elliptic curve of rank one over  $\mathbf{Q}$  with torsion group of order  $\tau$ , then  $\tau \cdot E(\mathbf{Q})$  is a ( $\mathbf{R}$ -topologically dense) diophantine model of  $(\mathbf{Z}, +)$ .

For practical purposes:

- $E(\mathbf{Q}) = \{(x, y, 1) \in \mathbf{Q}^3 : y^2 = x^3 + ax^2 + bx + c\} \cup \{(0, 0, 0)\}$

-   $E(\mathbf{Q})$  is a group, where for three points  $P, Q, R$  we have

$$P + Q + R = (0, 0, 0) \iff P, Q, R \text{ collinear.}$$

and  $E(\mathbf{Q})$  is finitely generated (Mordell, 1920)

An elliptic curve:  $E : y^2 = x^3 + 12x^2 + 11x$

- $E(\mathbf{Q}) = \langle (0, 0), (1, 0) \rangle \times \langle P = (\frac{1}{4}, \frac{15}{8}) \rangle \cong (\mathbf{Z}/2)^2 \times \mathbf{Z}$
- $E(\mathbf{Q})$  has rank one and  $\tau = 4$ .
- Since  $(0, 0) \in E[2]$ , we can write

$$nP = (x_n, y_n) = \left( \left( \frac{A_n}{B_n} \right)^2, \frac{A_n C_n}{B_n^3} \right).$$

$$P = \left(\frac{1}{4}, \frac{15}{8}\right); \quad nP = \left( \left(\frac{A_n}{B_n}\right)^2, \frac{A_n C_n}{B_n^3} \right)$$

$$A_1 = 1$$

$$A_2 = 5 \cdot 7$$

$$A_3 = 19 \cdot 269$$

$$A_4 = 659 \cdot 1931$$

$$A_5 = 23042506969$$

$$A_6 = \underline{5 \cdot 7 \cdot 89 \cdot 4639 \cdot 4575913}$$

$$A_7 = 647873811 \cdot 19522768049$$

$$B_1 = 2$$

$$B_2 = \underline{2^2} \cdot 3$$

$$B_3 = \underline{2} \cdot 29 \cdot 41$$

$$B_4 = \underline{2^3 \cdot 3} \cdot 5 \cdot 7 \cdot 37 \cdot 53$$

$$B_5 = \underline{2} \cdot 11 \cdot 6571 \cdot 10949$$

$$B_6 = \underline{2^2 \cdot 3^2} \cdot 19 \cdot \underline{29 \cdot 41} \cdot 269 \cdot 467 \cdot 2521$$

$$B_7 = \underline{2} \cdot 31 \cdot 211 \cdot 1481 \cdot 8629 \cdot 184598671$$

$$C_1 = 3 \cdot 5$$

$$C_2 = -37 \cdot 53$$

$$C_3 = \underline{3^2 \cdot 5} \cdot 467 \cdot 2521$$

$$C_4 = -13 \cdot 160117 \cdot 5609521$$

$$C_5 = \underline{3 \cdot 5} \cdot 17 \cdot 67 \cdot 1601 \cdot 3019 \cdot 17417 \cdot 379513$$

$$C_6 = \underline{23 \cdot 37 \cdot 53} \cdot 59 \cdot 10531 \cdot 1131223 \cdot 7186853449441$$

$$C_7 = -\underline{3 \cdot 5} \cdot 353 \cdot 1483 \cdot 17609 \cdot 11748809 \cdot 281433601 \cdot 46333351129459$$

## Elliptic divisibility sequences

- ▶ The sequence  $\{B_n\}$  is an **e.d.s.**:

$$m|n \Rightarrow B_m|B_n$$

- ▶ The sequence  $\{C_n\}$  is an **odd e.d.s.**:

$$n/m \in 2\mathbf{Z} + 1 \Rightarrow C_m|C_n$$

# Elliptic divisibility sequences

- ▶ The sequence  $\{B_*\}$  is an **e.d.s.**:

$$m|n \Rightarrow B_m|B_n$$

- ▶ The sequence  $\{C_*\}$  is an **odd e.d.s.**:

$$n/m \in 2\mathbf{Z} + 1 \Rightarrow C_m|C_n$$

- ▶ For  $n \gg$ ,  $B_n$  (and  $C_n$ ) has a primitive divisor:

$$\exists p > 1; \quad p|B_n, \quad p \nmid B_i \text{ for } i < n$$

= **elliptic Zsigmondy's theorem**

(J. Silverman, 1988)



## C-odd-inertial elliptic Zsigmondy's "theorem"

**Conjecture C.** *There exists*

- *an elliptic curve  $y^2 = x^3 + ax^2 + bx$  ( $b$  squarefree) of rank one over  $\mathbf{Q}$ ; and a point  $P$  of infinite order and sufficiently large height on  $E(\mathbf{Q})$ ;*
- *a finite set  $D$  of integers, such that every element of the odd e.d.s.  $C_n$  associated to  $P$  on  $E$  has a primitive odd order divisor from the set  $R_D$ .*

**Definition.** The set  $R_D$  consists of all prime numbers  $p$  such that  $p$  cannot be written as  $x^2 - dy^2$  for  $x, y \in \mathbf{Z}$  and at least one  $d \in D$  (inert in at least one of  $\mathbf{Q}(\sqrt{d})$ ).

**Examples.**  $D = \{-1\}$ ;  $R_D = \{p = 3 \pmod{4}\} = \{3, 7, 11, \dots\}$ ;

$D = \{5\}$ ;  $R_D = \{p = \pm 3 \pmod{5}\} = \{2, 3, 7, \dots\}$ .

Example:  $y^2 = x^3 + 12x^2 + 11x$ ;  $P = (\frac{1}{4}, \frac{15}{8})$ ;  $D = \{5\}$

$$C_1 = 3 \cdot 5$$

$$C_2 = -37 \cdot 53$$

$$C_3 = 3^2 \cdot 5 \cdot 467 \cdot 2521$$

$$C_4 = -13 \cdot 160117 \cdot 5609521$$

$$C_5 = 3 \cdot 5 \cdot 17 \cdot 67 \cdot 1601 \cdot 3019 \cdot 17417 \cdot 379513$$

$$C_6 = 23 \cdot 37 \cdot 53 \cdot 59 \cdot 10531 \cdot 1131223 \cdot 7186853449441$$

$$C_7 = -3 \cdot 5 \cdot 353 \cdot 1483 \cdot 17609 \cdot 11748809 \cdot 281433601 \cdot 46333351129459$$

## Primitivity condition

Let  $\{X_n\}$  be an (odd) divisibility sequence. Let  $R$  denote a set of valuations. We say  $\{X_n\}$  is  **$R$ -primitive** if every term  $X_n$  has a primitive divisor from  $R$ , that is:

$$(\forall n)(\exists v \in R)[v(X_n) > 0 \text{ and } (\forall i < n)(v(X_i) = 0)].$$

We say  $\{X_n\}$  is  **$R$ -odd-primitive** if every term  $X_n$  has a primitive *odd order* divisor from  $R$ , that is:

$$(\forall n)(\exists v \in R)[v(X_n) \text{ is odd and } (\forall i < n)(v(X_i) = 0)].$$

We sometimes say  $v$  is  $R$ -(odd-)primitive for  $X_n$  if these formulæ holds for  $v$  and  $X_n$ .

**Lemma (“detecting divisibility”).** *Suppose that  $E$  and  $P$  are as in **C**. Assume that  $\{C_n\}$  is  $R$ -(odd-)primitive for some  $R$ . If  $v \in R$  is (odd-)primitive for  $C_m$  and  $v(C_n) > 0$  for some  $n$ , then  $m|n$  and  $n/m$  is odd.*

## Divisibility predicate

Let  $R$  denote a set of valuations. Denote by  $\mathcal{D}_R(x, y)$  the property

$$\mathcal{D}_R(x, y) : \forall v \in R : v(x) \text{ odd} \Rightarrow v(x) < v(y^2).$$

**Theorem (“expressing divisibility using  $\mathbf{Q}$ ”).** *Let  $E$  be an elliptic curve over  $\mathbf{Q}$  and  $P$  a point of infinite order on  $2E(\mathbf{Q})$  of sufficiently large height. Assume  $E$  has Weierstrass form  $y^2 = x^3 + ax^2 + bx$  (in particular, a rational 2-torsion point) with  $b$  squarefree. Assume the odd divisibility sequence  $\{C_*\}$  associated to  $P$  on  $E$  is  $R$ -odd-primitive. Then for any integers  $m, n \in \mathbf{Z}$ ,*

$$m|n \iff \mathcal{D}_R(y_m\sqrt{x_m}, y_n\sqrt{x_n}) \vee \mathcal{D}_R(y_m\sqrt{x_m}, y_{m+n}\sqrt{x_{m+n}})$$

## Diophantineness of divisibility predicate

(Pheidas 1999, Van Geel-Zahidi 2002, Van Geel-Demeyer 2004)

**Proposition (“Diophantineness for special  $R$ ”).** *For a non-square  $d$ , let  $R_d$  denote the set of valuations of  $\mathbf{Q}$  that are inert in  $\mathbf{Q}(\sqrt{d})$ . Then there is a (diophantine)  $\Sigma_1^+$ -formula equivalent to  $\mathcal{D}_{R_d}(x, y)$ , i.e.,  $t(\mathcal{D}_{R_d}) = 0$ .*

For any finite set  $D$  of fundamental discriminants, set  $R_D := \bigcup_{d \in D} R_d$ . Then  $\mathcal{D}_{R_D}$  is expressible by a  $\Sigma_1^+$ -formula. In particular, there are sets of primes  $R$  of arbitrary high Dirichlet density  $< 1$  for which  $\mathcal{D}_R$  is diophantine.

$\mathbf{C} \Rightarrow$  diophantine model of  $(\mathbf{Z}, +, |)$  in  $(\mathbf{Q}, +, \times)$

## Defining multiplication in $(\mathbf{Z}, +, |)$

**Lemma** *There exists a  $\Sigma_3^+$ -formula  $\mathcal{F}$  in  $(\mathbf{Z}, +, |, \neq)$  such that for integers  $m, n, k$ , we have  $k = m \cdot n \iff \mathcal{F}(m, n, k)$ .*

*Proof.*  $\iff$  squaring by  $\Pi_2^+$ .

$y = x^2$  if and only if

$$\begin{aligned} & (\forall t)(x|y \wedge x + 1|y + x \wedge x - 1|y - x \wedge \\ & ((x|t \wedge x + 1|t + x \wedge x - 1|t - x) \Rightarrow (y + x|t + x \wedge y - x|t - x))) \end{aligned}$$

Implications translate into non-divisibilities  $a \not| b$ , but means  $(a) \neq (a, b)$ , which is existential using  $\neq$ .

$$\mathbf{C} \Rightarrow \text{model of } (\mathbf{Z}, +, \times) \text{ in } (\mathbf{Q}, +, \times) \quad \square$$

## Conjecture(s)

**(Odd-)inertial  $C$ -elliptic Zsigmondy's conjecture.** *For every elliptic curve  $E$  in Weierstrass form such that  $(0, 0) \in E[2]$  and every rational point  $P$  of infinite order and sufficiently large height, the associated odd divisibility sequence  $\{C_*\}$  is  $R_D$ -(odd-)primitive for some  $D$ .*

**(Odd-)inertial elliptic Zsigmondy's conjecture.** *For every elliptic curve  $E$  in generalised Weierstrass form and every rational point  $P$  of infinite order and sufficiently large height, the associated elliptic divisibility sequence  $\{B_*\}$  is  $R_D$ -(odd)-primitive for some  $D$ .*

## Discussion: usual Zsigmondy

**Proposition ((C)-elliptic Zsigmondy's theorem).** *Let  $E$  be an elliptic curve over  $\mathbf{Q}$  and  $P$  a point of infinite order in  $E(\mathbf{Q})$  of sufficiently large height. Let  $R$  denote the set of all finite valuations of  $\mathbf{Q}$ . Then*

- (i)  $\{B_*\}$  is  $R$ -primitive.
- (ii) If  $(0, 0) \in E[2]$ , then  $\{C_*\}$  is  $R$ -primitive.
- (iii) If  $E$  has  $j$ -invariant  $j = 0$  or  $j = 1728$ , then the ABC-conjecture implies that  $\{B_*\}$  and  $\{C_*\}$  (for  $(0, 0) \in E[2]$ ) are  $R$ -odd-primitive.

Expectation: for any given  $K > 0$ , for any  $n > n_0(K)$ ,  $C_n$  has at least  $K$  primitive odd order divisors. Probability that one is in  $R_D$  is very high.

## Discussion: heuristics

(Landau-Serre) The probability that a given number  $x$  has all its prime factors outside  $R_D$  admits an asymptotic expansion

$$\log(x)^{-\delta} \left( \sum_{i=0}^N c_i \log(x)^{-i} + O(\log(x)^{-(N+1)}) \right)$$

with  $c_0 > 0$ , for any positive integer  $N$ , and  $\delta = 1 - 1/2^{|D|} > 0$ .

## Discussion: heuristics

►  $\mathbf{P}(\text{all factors } x \text{ outside } R_D) \sim \frac{1}{\log(x)^\delta}.$

## Discussion: heuristics

- ▶  $\mathbf{P}(\text{all factors } x \text{ outside } R_D) \sim \frac{1}{\log(x)^\delta}$ .
- ▶ For  $A_x = \{P \in E(\mathbf{Q}) - E(\mathbf{Z}[\frac{1}{R_D}]) : \hat{h}(P) \leq x\}$ ,  $\text{rk}(E(\mathbf{Q})) = r$ ,

$$|A_x| \approx \sum_{\substack{P \in E(\mathbf{Q}) \\ \hat{h}(P) \leq x}} \hat{h}(P)^{-\delta} \approx \sum_{\substack{\lambda \in \mathbf{Z}^r - \{0\} \\ \|\lambda\|^2 \leq x}} \|\lambda\|^{-2\delta} \approx \sum_{m=1}^{\sqrt{x}} m^{r-1} \cdot m^{-2\delta}.$$

## Discussion: heuristics

- ▶  $\mathbf{P}(\text{all factors } x \text{ outside } R_D) \sim \frac{1}{\log(x)^\delta}$ .
- ▶ For  $A_x = \{P \in E(\mathbf{Q}) - E(\mathbf{Z}[\frac{1}{R_D}]) : \hat{h}(P) \leq x\}$ ,  $\text{rk}(E(\mathbf{Q})) = r$ ,

$$|A_x| \approx \sum_{\substack{P \in E(\mathbf{Q}) \\ \hat{h}(P) \leq x}} \hat{h}(P)^{-\delta} \approx \sum_{\substack{\lambda \in \mathbf{Z}^r - \{0\} \\ \|\lambda\|^2 \leq x}} \|\lambda\|^{-2\delta} \approx \sum_{m=1}^{\sqrt{x}} m^{r-1} \cdot m^{-2\delta}.$$

- ▶  $A_\infty$  finite  $\iff \delta > r/2$ .

## Discussion: density version

- ▶ (Morgan Ward, 1948) With the correct choice of sign,  $B_*$  is periodic modulo any prime  $p$ .
- ▶ For  $P = (-2, 4)$  in  $E : y^2 = x^3 + 7x^2 + 2x$ , Jacobi symbols  $(\frac{5}{B_n}) = (\frac{B_n}{5})$  repeat  $(1, 1, -1, 0, -1, 1, 1, 0) \pmod{5}$ .
- ▶ **Proposition.** *Let  $\{B_*\}$  denote the elliptic divisibility sequence associated to  $(2, -4)$  on  $y^2 = x^3 + 7x^2 + 2x$ , and let  $D = \{5, 13, 29, 41, 53\}$ . Then the set*

$$\{s \text{ prime} : B_s \text{ has a primitive odd order divisor from } R_D\}$$

has Dirichlet density at least  $43/45 \geq 95.5\%$ .

## Further remarks about the conjecture

- Conjecture includes, e.g., finding the integral coprime solution to the equation (smooth Calabi-Yau surface):

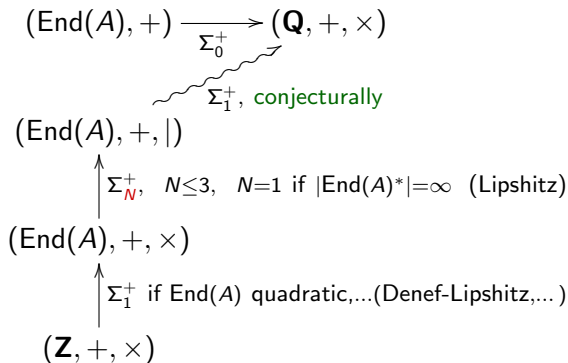
$$9(A^2 + B^2)(A^2 + 11B^2) = (X^2 - 5Y^2)^2.$$

- compare: e.d.s. vs. l.r.s.
- can make function field analogues; some weak results.

▶ [Jump to short conclusion](#)

## Overall philosophy / Conclusion

$A$  = an abelian variety over  $\mathbf{Q}$  of rank one over  $\text{End}(A)$ .  
 $\text{End}A \cong R$  a number ring.



## Overall philosophy / Conclusion

$A$ =elliptic curve of rank one, having  $\text{End}(A) = \mathbf{Z}$

$$\begin{array}{ccc}
 (\mathbf{Z}, +) & \xrightarrow{\Sigma_0^+} & (\mathbf{Q}, +, \times) \\
 & \nearrow \Sigma_1^+ & \\
 (\mathbf{Z}, +, |) & & \text{conjecturally: } C\text{-odd inertial Zsigmondy} \\
 \uparrow \Sigma_3^+ & & \\
 (\mathbf{Z}, +, \times) & & 
 \end{array}$$

## Overall philosophy / Conclusion

$A$  = Jacobian of curve  $y^2 + (x^3 + x^2 + x)y = x^4 + x^3 + 3x^2 - 2x + 1$   
 is abelian surface with real multiplication by  $R = \mathbf{Z}[\sqrt{2}]$  and  
 $R$ -rank one over  $\mathbf{Q}$ .

$$(\mathbf{Z}[\sqrt{2}], +) \xrightarrow{\Sigma_0^+} (\mathbf{Q}, +, \times)$$

$\Sigma_1^+$ , conjecturally; problem (!) what is the correct conjecture?

$$(\mathbf{Z}[\sqrt{2}], +, |)$$

$$\uparrow_{\Sigma_1^+} \quad (\text{Lipshitz})$$

$$(\mathbf{Z}[\sqrt{2}], +, \times)$$

$$\uparrow_{\Sigma_1^+} \quad (\text{Denef-Lipshitz})$$

$$(\mathbf{Z}, +, \times)$$

# Conclusion

- ▶ Quantitative theory of statements in number theory w.r.t. diophantineness (positive hierarchy, complexity measures)
- ▶ Can improve upon Julia Robinson (“ $c = 5$  to  $c = 3$ ”; “ $t = 8$  to  $t = 1$ ”), depending on deep (?) conjectures about elliptic curves
- ▶ Could improve further (“ $c = 3$  to  $c = 1$ ”; “ $t = 1$  to  $t = 0$ ” = HTP( $\mathbf{Q}$ )) conjecturally, *if* would know analogue of conjectures for abelian surfaces with real multiplication.

