

UNDECIDABLE PROBLEMS ABOUT RATIONAL POINTS AND CONJECTURES ABOUT ELLIPTIC CURVES

by Gunther Cornelissen (Utrecht)
joint work with Karim Zahidi (Antwerpen)



KURT GÖDEL'S 193? MANUSCRIPT ON UNDECIDABLE DIOPHANTINE PROPOSITIONS

Let a polynomial F in $m+n$ variables $a_1, \dots, a_m, x_1, \dots, x_n$ and with integer coefficients be given [...] and now let's ask the question: Has the given diophantine equation $F(a_1, \dots, a_m, x_1, \dots, x_n) = 0$ solutions for arbitrary integer values of the parameters a_i ? [...]

Let us denote the class of [...] propositions by which [these problems] are expressed by A , then it can be shown that already the class A of propositions cannot be completely formalised. That means two things:



KURT GÖDEL'S 193? MANUSCRIPT [II]

1. There exist no mechanical procedure for deciding every proposition of the class A .
2. In every formal theory which allows [[one]] to formulate all propositions of the class A there exists an undecidable proposition of class A , i.e., there exists a polynomial with integer coefficients and with the variables divided into two groups, the parameters and unknowns, and it is impossible to decide in the given formalism whether or not this particular diophantine equation has solutions for arbitrary values of the parameters. [...]



KURT GÖDEL'S 193? MANUSCRIPT [III]

When I first published my paper about undecidable propositions the result could not be pronounced in this generality, because for the notions of mechanical procedure and of formal system no mathematically satisfactory definition had been given at that time. This gap has since been filled by Herbrand, Church and Turing.



THEOREM (GÖDEL)

The Π_2^+ -theory of $(\mathbf{Z}, +, \times, 0, 1)$ is undecidable. There is an undecidable sentence with 6 universal quantifiers.

Π_2^+ is our way of saying “of class A”.



KURT GÖDEL'S 1951 GIBBS LECTURE

“SOME BASIC THEOREMS ON THE FOUNDATIONS OF MATHEMATICS AND THEIR IMPLICATIONS”

What is the meaning of such a result for philosophy of the mind? It is very hard to draw the conclusion that the “mind” is not a Turing machine. Gödel has a subtle viewpoint.



KURT GÖDEL'S 1951 GIBBS LECTURE

SO the following disjunctive conclusion is inevitable: Either mathematics is incompletable in this sense, that its evident axioms can never be comprised in a finite rule, that is to say, the human mind (even within the realm of pure mathematics) infinitely surpasses the powers of any finite machine, or else there exist absolutely unsolvable diophantine problems [[of class *A*, where “absolutely” means that they would be undecidable, not just within some particular axiomatic system, but by any mathematical proof the human mind can conceive]] (where the case that both terms of the disjunction are true is not excluded) [...] This fact is entirely independent of the special standpoint taken toward the foundations of mathematics.

critical point (e.g., George Boolos's comments): what is “mind”; can be circumvented using “if there exists a Turing machine that simulates the output of the human mind”.



HILBERT'S 1930 RADIO ADDRESS

“NATURERKENNEN UND LOGIK”

Hilbert counters Emil DuBois-Reymond, e.g., “Über die Grenzen des Naturerkennens” (1872).

Wir dürfen nicht denen glauben, die heute mit philosophischer Miene und überlegenem Tone den Kulturuntergang prophezeien und sich in dem Ignorabimus gefallen. Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiße im Gegenteil unsere Losung: Wir müssen wissen, Wir werden wissen.

We must not believe those, who today with philosophical bearing and deliberative tone prophesy the fall of culture and accept the ignorabimus. For us there is no ignorabimus, and in my opinion none whatever in natural science. In opposition to the foolish ignorabimus I offer our motto: We must know, we will know.

RADIO SOUND

“According to Wang, Gödel believed that Hilbert was right to reject the second alternative”
(Boolos)

Universiteit Utrecht



HILBERT'S TENTH PROBLEM

Entscheidung der Lösbarkeit einer diophantischen Gleichung.

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Determination of the solvability of a Diophantine equation.

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

David Hilbert, 2nd ICM (Paris, 1900)



THE POSITIVE ARITHMETICAL HIERARCHY (Σ^+ , Π^+)

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

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

Hilbert's Tenth Problem: is any Σ_1^+ -sentence over \mathbf{Z} decidable?

Examples.

- $(\exists x, y, z)(x^2 + y^2 = z^2)$ is Σ_1^+
- $(\forall x, y)(\exists z)(x^{22} + y^3 = z^{2006})$ is Π_2^+
- $(\exists x, y)(\forall z, t)(\exists u)(xyztu = 1)$ is Σ_3^+

A formula in Σ_1^+ is *diophantine*. For \mathbf{Z} or \mathbf{Q} , formulae in Σ_0^+ are equivalent to *atomic* formulae.



TWO MEASURES OF COMPLEXITY

Fact: a first-order formula in \mathbf{Z}, \mathbf{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 $\mathbf{y} = (y_1^{(1)}, \dots, y_{e_1}^{(1)}, \dots, y_1^{(N)}, \dots, y_{e_N}^{(N)})$.

- ▶ c -complexity = **Number of quantifier changes**: position in the hierarchy
- ▶ t -complexity = The **total number of universal quantifiers**



**THEOREM (DAVIS, MATIJASEVICH, PUTNAM, ROBINSON,
1950—1970)**

The Σ_1^+ -theory of $(\mathbf{Z}, +, \times, 0, 1)$ is undecidable. There is an undecidable sentence with 0 universal quantifiers. Hilbert's Tenth Problem has a negative answer.



NOT ONLY AN UNDECIDABILITY STATEMENT

THEOREM (DAVIS, MATIJASEVICH, PUTNAM, ROBINSON)

Diophantine sets are the same as recursively enumerable sets.

A set of integers is

- ▶ **diophantine** if it is the set of integer parameters t for which a diophantine equation $f(x_1, \dots, x_n, t) = 0$ has a solution in integers x_1, \dots, x_n (= projection of the set of integral points on a variety).
- ▶ **recursively enumerable** if there is a computer program that can list it.

Negative answer to HTP follows: there is a r.e. set S that is not recursive (i.e., of which membership is not Turing decidable); S comes e.g., out of the Halting Problem, setting $S = \{2^p 3^x\}$ for p a program that halts on x .



RELEVANCE FOR “GENERAL MATHEMATICS”

Many general mathematical problems can be reduced to deciding whether or not a diophantine equation has a solution.

The trick: whenever a problem can be formalized in a suitable way, the question of its provability is equivalent to that of its Gödel number belonging to the r.e. set of provable formulæ, which is equivalent to deciding a diophantine equation by DMPR.

- ▶ Fermat's Last Theorem
- ▶ Riemann Hypothesis



RELEVANCE FOR “GENERAL MATHEMATICS” (II)

Suitable classes of general mathematical problems can be shown to be undecidable.

- ▶ There are real numbers that cannot be bit-computed to arbitrary precision. Example: if $\{d_n\}$ is an enumeration of all diophantine equations,

$$\sum_{n \in S} 4^{-n}, \quad S = \{n : d_n \text{ has a solution}\}$$

- ▶ There exists a game with two players, such that the second one always has a winning strategy, whatever move the first one makes, but the second player can never compute that strategy.
- ▶ One cannot decide of a function in the closure under composition of $\{\text{id}, +, \cdot, -, /, \sin\}$ whether or not its integral over the real line converges.



OPEN PROBLEM: HILBERT'S TENTH PROBLEM FOR \mathbb{Q}

- ▶ “Is there an algorithm to determine whether an arbitrary diophantine equation has a solution in **rational numbers**?”



OPEN PROBLEM: HILBERT'S TENTH PROBLEM FOR \mathbf{Q}

- ▶ “Is there an algorithm to determine whether an arbitrary diophantine equation has a solution in **rational numbers**?”
- ▶ Idea: if \mathbf{Z} is a **diophantine subset** of \mathbf{Q} , i.e., there exists a polynomial f such that

$$t \in \mathbf{Q} : t \in \mathbf{Z} \iff (\exists \mathbf{x} \in \mathbf{Q})(f(\mathbf{x}, t) = 0),$$

then we are done (HTP(\mathbf{Q}) has been answered negatively).

If we have an algorithm over \mathbf{Q} , the following is an algorithm over \mathbf{Z} : if $F(\mathbf{y})$ is any polynomial, decide whether

$$F(\mathbf{y})^2 + f(\mathbf{x}_1, y_1)^2 + \cdots + f(\mathbf{x}_n, y_n)^2 = 0$$

has a solution over \mathbf{Q} .



MAZUR'S CONJECTURE

CONJECTURE (BARRY MAZUR, 1990's)

For any variety V/\mathbf{Q} (= system of polynomial equations with coefficients from \mathbf{Q}), the real topological closure of the set $V(\mathbf{Q})$ of rational points (= rational solutions to the equations) in the set $V(\mathbf{R})$ of real points, has only finitely many components.

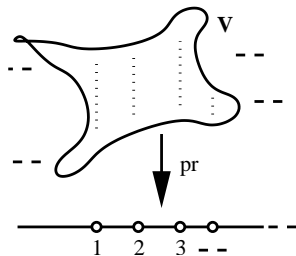


MAZUR'S CONJECTURE

CONJECTURE (BARRY MAZUR, 1990's)

For any variety V/\mathbf{Q} (= system of polynomial equations with coefficients from \mathbf{Q}), the real topological closure of the set $V(\mathbf{Q})$ of rational points (= rational solutions to the equations) in the set $V(\mathbf{R})$ of real points, has only finitely many components.

If this conjecture is true, \mathbf{Z} cannot be a diophantine subset of \mathbf{Q} .



If $(\exists \mathbf{x})(f(\mathbf{x}, t) = 0)$ defines \mathbf{Z} in \mathbf{Q} , then if V is the zero locus of f ,

$$V(\mathbf{Q}) = \text{pr}_t^{-1}(\mathbf{Z}),$$

and \mathbf{Z} is discrete in \mathbf{Q} .



DIOPHANTINE MODEL

Variation: if \mathbf{Z} has a **diophantine model** in \mathbf{Q} , then $\text{HTP}(\mathbf{Q})$ has a negative answer.

A **diophantine** subset D of \mathbf{Q}^N is a **diophantine model of \mathbf{Z}** if there is a bijection $\iota : \mathbf{Z} \rightarrow D$ that maps the graphs of addition and multiplication on \mathbf{Z} to **diophantine** subsets of \mathbf{Q}^{3N} .



DIOPHANTINE MODELS AND MAZUR'S CONJECTURE

THEOREM (C-ZAHIDI, 1999)

if \mathbf{Z} has a *diophantine model* in \mathbf{Q} , then Mazur's conjecture is wrong.

- ▶ Typical case: $n \in \mathbf{Z} \rightsquigarrow d_n \in D$ is dense in the unit interval $[0, 1]$.
- ▶ The infinite set

$$\tilde{\mathbf{Z}} = \{n \in \mathbf{Z} \mid \frac{1}{2j+1} \leq d_n \leq \frac{1}{2j} \text{ for some } j \in \mathbf{Z}_{>0}\}$$

is recursively enumerable.

- ▶ By DMPR, $\tilde{\mathbf{Z}}$ is diophantine in \mathbf{Z} . The corresponding set

$$\tilde{D} = \{d_n \mid n \in \tilde{\mathbf{Z}}\}.$$

is diophantine in D , and hence in \mathbf{Q} . So there exists a variety \tilde{V} over \mathbf{Q} whose \mathbf{Q} -rational points map to \tilde{D} . The real closure of \tilde{D} has infinitely many connected components by construction. Hence the same holds for $\tilde{V}(\mathbf{Q})$.



INTERMEZZO:

EXISTENCE OF SOLUTIONS VS. FINDING SOLUTIONS

- ▶ Ex-problem: does there exist a solution or not?
- ▶ Fin-problem: is the solution set finite or not?
- ▶ Sol-problem: if the solution set is finite, find all solutions

DMR conjecture that Fin-problem(\mathbf{Z}) is undecidable, even assuming Ex-problem(\mathbf{Z}) is decidable (by an oracle).

THEOREM (MINHYONG KIM, 2003)

Sol-problem(\mathbf{Q}) is decidable, if Ex-problem(\mathbf{Q}) is decidable (e.g., by an oracle) for polynomial equations $F(X, Y) = 0$ in two variables X, Y .



JULIA ROBINSON'S 1949

“DEFINABILITY AND DECISION PROBLEMS IN ARITHMETIC”

THEOREM (JULIA ROBINSON)

\mathbf{Z} can be defined in \mathbf{Q} by a Π_4^+ -formula involving 8 universal quantifiers. Hence the Σ_5^+ -theory of $(\mathbf{Q}, +, \times, 0, 1)$ is undecidable. There is an undecidable sentence with 8 universal quantifiers.



HARTLEY ROGERS JR.,

“THEORY OF RECURSIVE FUNCTIONS AND EFFECTIVE
COMPUTABILITY”

The human mind seems limited in its ability
to understand and visualise beyond four or five alterations of quantifier.



THEOREM (BJORN POONEN, TWO WEEKS AGO)

\mathbf{Z} can be defined in \mathbf{Q} by a Π_2^+ -formula involving 2 universal quantifiers. Hence the Σ_3^+ -theory of $(\mathbf{Q}, +, \times, 0, 1)$ is undecidable. There is an undecidable sentence with 2 universal quantifiers.



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} .



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 .
- Models can be used to translate formulæ, and one can follow the complexity, e.g.

Lemma. *If (D, ι) is a model of \mathbf{Z} in \mathbf{Q} with D and $\iota(+)$ diophantine and $t(\iota(\times)) \leq 1$, then Σ_1^+ -sentences are translated into sentences equivalent to Σ_3^+ -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

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

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 . **Universiteit Utrecht**



THEOREM (C—ZAHIDI, 2004, TO APPEAR IN CRELLE'S, ARXIV: MATH.NT/0412473)

Conjecture (E) implies the following.

\mathbf{Z} has a Π_2^+ -model over \mathbf{Q} involving one universal quantifier.

The Σ_3^+ -theory of $(\mathbf{Q}, +, \times, 0, 1)$ is undecidable. The Π_2^+ -theory of $(\mathbf{Q}, +, \times, 0, 1)$ is undecidable. There is an undecidable sentence with one universal quantifier.

CONJECTURE

The following exist:

(a) *an elliptic curve over \mathbf{Q} , such that E has Weierstrass form*

$y^2 = x^3 + ax^2 + bx$ (in particular, a rational 2-torsion point) with b squarefree;

(b) *a point P of infinite order on E with associated odd divisibility sequence $\{C_*\}$;*

(c) *a finite set D of quadratic discriminants such that $\{C_*\}$ is (weakly) R_D -odd-primitive.*



	Gödel	DMPR	JR	Poonen	C-Zahidi (conj)	H10(Q) (?)
undec. sentence	$\Pi_2^+(\mathbf{Z})$	$\Sigma_1^+(\mathbf{Z})$	$\Sigma_5^+(\mathbf{Q})$	$\Sigma_3^+(\mathbf{Q})$	$\Pi_2^+(\mathbf{Q})$	$\Sigma_1^+(\mathbf{Q})$ (?)
def. of Z in Q	—	—	Π_4^+	Π_2^+	Π_2^+	Σ_1^+ (?)
# univ. quant.	6	0	8	2	1	0 (?)

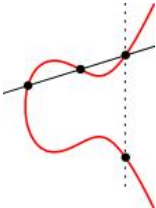


DIOPHANTINE MODELS AND ELLIPTIC CURVES

Typical (partial) diophantine model arises as follows: let E be an elliptic curve of rank one over \mathbf{Q} with torsion group of order τ , 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 torsion group of order 4.
- We can write

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



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

$$B_1 = 2$$

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

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

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

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

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

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

$$B_8 = \underline{2^4 \cdot 3^1 \cdot 5 \cdot 7} \cdot 13 \cdot \underline{37 \cdot 53} \cdot 659 \cdot 1931 \cdot 160117 \cdot 5609521$$

$$C_1 = 3 \cdot 5$$

$$C_2 = -37 \cdot 53$$

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

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

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

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

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

$$C_8 = 5303 \cdot 108739 \cdot 1830931 \cdot 170749043903 \cdot 92397921271034416798380481$$



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.**:

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



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.**:

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

- ▶ For $n \gg 1$, B_n (and C_n) has a primitive divisor:

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

= **elliptic Zsigmondy's theorem**

(J. Silverman, 1988)



C-ODD-INERTIAL ELLIPTIC ZSIGMONDY'S "THEOREM"

Conjecture. *There exists*

- *an elliptic curve of rank one over \mathbf{Q} ;*
- *a point P of infinite order 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 inert in at least one of the quadratic fields $\mathbf{Q}(\sqrt{d})$, $d \in D$. In case all d have class number one, this is equivalent to p not being of the form $x^2 - dy^2$ for $x, y \in \mathbf{Z}$ and at least one $d \in D$.

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

$$C_1 = 3 \cdot 5$$

$$C_2 = -37 \cdot 53$$

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

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

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

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

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

$$C_8 = 5303 \cdot 108739 \cdot 1830931 \cdot 170749043903 \cdot 92397921271034416798380481$$



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 before. 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 $2E(\mathbf{Q})$. 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, possibly replacing P by a multiple, 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) Σ_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 Σ_1^+ -formula. In particular, there are sets of primes R of arbitrary high Dirichlet density < 1 for which \mathcal{D}_R is diophantine.

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



DEFINING MULTIPLICATION IN $(\mathbf{Z}, +, |)$

Lemma There exists a Σ_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 Π_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 .

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

- ▶ $\mathbf{P}(\text{all factors of } N \text{ outside } R_D) \sim \frac{1}{\log(N)^\delta}$.



DISCUSSION: HEURISTICS

- ▶ $\mathbf{P}(\text{all factors of } N \text{ outside } R_D) \sim \frac{1}{\log(N)^\delta}$.
- ▶ Assume $\text{rk}(E(\mathbf{Q})) = r$. Set

$$A_x = \{P \in E(\mathbf{Q}) - E(\mathbf{Z}[\frac{1}{R_D}]) : \hat{h}(P) \leq x\}$$

Then

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



DISCUSSION: HEURISTICS

- ▶ $\mathbf{P}(\text{all factors of } N \text{ outside } R_D) \sim \frac{1}{\log(N)^\delta}$.
- ▶ Assume $\text{rk}(E(\mathbf{Q})) = r$. Set

$$A_x = \{P \in E(\mathbf{Q}) - E(\mathbf{Z}[\frac{1}{R_D}]) : \hat{h}(P) \leq x\}$$

Then

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

- ▶ A_∞ finite $\iff \delta > r/2$. For $r = 1$, $|D| > 1$ suffices.



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.
- various people (Jonathan Reynolds, Karl Rubin, Marco Streng) have observed that in examples, one can show the existence of primitive **split** divisors.
- Marco Streng has proven Zsigmondy for complex multiplication e.d.s.



RUBIN'S PROOF

PROPOSITION

On the example curve above, all divisors of B_n for odd n are $\equiv \pm 1 \pmod{5}$.

PROOF. Suppose l is a prime with $l|B_n$, i.e., $nP = 0 \pmod{l}$. Since n is odd, $P = 2Q \pmod{l}$ for $Q = (n+1)/2 \cdot P$. Then $x = x(Q)$ satisfies the equation $(x^2 - 8x + 11)(x^2 + 7x + 11) = 0 \pmod{l}$. Since both factors of this equation have discriminant 5 up to squares, there is a solution mod l precisely if 5 is a square modulo l . \square



**PROPOSITION (MARCO STRENG, 2006,
WWW.MATH.LEIDENUNIV.NL/~STRENG)**

Let E denote an elliptic curve over \mathbf{Q} with complex multiplication by an imaginary quadratic order \mathcal{O} . For all but finitely many integers n that are coprime to the index of \mathcal{O} in the maximal order A , B_n has at least as many primitive prime divisors that split in A as n has divisors that split in A .

