

Elliptic divisibility sequences and undecidable problems about rational points

by Gunther Cornelissen *and* Karim Zahidi

Abstract. Julia Robinson has given a first-order definition of the rational integers \mathbf{Z} in the rational numbers \mathbf{Q} by a formula $(\forall\exists\forall\exists)(F = 0)$ where the \forall -quantifiers run over a total of 8 variables, and where F is a polynomial. This implies that the Σ_5 -theory of \mathbf{Q} is undecidable. We prove that a conjecture about elliptic curves provides an interpretation of \mathbf{Z} in \mathbf{Q} with quantifier complexity $\forall\exists$, involving only one universally quantified variable. This improves the complexity of defining \mathbf{Z} in \mathbf{Q} in two ways, and implies that the Σ_3 -theory, and even the Π_2 -theory, of \mathbf{Q} is undecidable (recall that Hilbert's Tenth Problem for \mathbf{Q} is the question whether the Σ_1 -theory of \mathbf{Q} is undecidable).

In short, granting the conjecture, there is a one-parameter family of hypersurfaces over \mathbf{Q} for which one cannot decide whether or not they all have a rational point.

The conjecture is related to properties of elliptic divisibility sequences on an elliptic curve and its image under rational 2-descent, namely existence of primitive divisors in suitable residue classes, and we discuss how to prove weaker-in-density versions of the conjecture and present some heuristics.

Introduction.

This paper addresses a mixture of number theory and logic, and we will use this introduction to give an informal preview directed at both communities. The central two questions can be phrased as follows: “What is more difficult: to decide of an arbitrary polynomial equation with integer

coefficients whether it has an integer solution, or whether it has a rational solution?"; and: "What is a hard problem about rational points?" If one makes these vague questions mathematically more precise, "decide" should mean the existence of an algorithm on a Turing Machine (which in practice is equivalent to any notion of "computable" via Church's Thesis). Call Hilbert's Tenth Problem $\text{HTP}(R)$ for a subring R of the rational number \mathbf{Q} the question whether one can decide if an arbitrary polynomial equation with integer coefficients has a solution in R . The classical result of Davis, Matijasevich, Putnam and Robinson ([10], [21], [22]) shows that $\text{HTP}(\mathbf{Z})$, for \mathbf{Z} the ring of integers, has a negative answer. The answer to $\text{HTP}(\mathbf{Q})$, however, is not known. But a more general problem has been settled by Julia Robinson in 1949 ([25]). She showed that \mathbf{Z} is definable in \mathbf{Q} by a first-order formula. This implies that the full first order theory of \mathbf{Q} is undecidable, i.e., that one cannot decide (in the above sense) the truth of an arbitrary first-order sentence in \mathbf{Q} built from the symbols $(0, 1, +, \times, =)$. One should think of such a sentence as a "algorithmically hard" number theoretical statement

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

where F is a polynomial over \mathbf{Z} in multi-variables $\mathbf{x} = (x_1^{(1)}, \dots, x_{f_N}^{(N)})$ and $\mathbf{y} = (y_1^{(1)}, \dots, y_{e_N}^{(N)})$. Note: any formula over \mathbf{Q} can be put into this form, which we call *positive prenex* form (cf. lemma 1.2). Examples of such statements: if there are only existential quantifiers ($N = 1, f_1 = 0$), such a formula says that a certain diophantine equation has a solution; a formula with $N = 1$ says that a family of diophantine equations has a solution in \mathbf{y} for all values of the parameters \mathbf{x} , etc.

Related to our first question, Robinson's result expresses in some sense that testing the truth of such sentences in \mathbf{Q} or in \mathbf{Z} is "equally hard". $\text{HTP}(\mathbf{Q})$ is the particular case where one only wants to decide the truth of formulæ with $N = 1$ and $f_1 = 0$ (with $e_1 = m$ arbitrary): $(\exists y_1 \dots y_m) : F(y_1, \dots, y_m) = 0$. We now recast the original question above in the following way: how "complex" does a formula in \mathbf{Q} have to be, in order to be undecidable? Phrased more dramatically: what is the easiest *hard* problem about rational points? Since we want to indicate how far a formula is from being "diophantine" (i.e., in positive prenex form with $N = 1$), in 1.5—1.8 we look at the following two measures of complexity. First, we define the *positive arithmetical hierarchy* (Σ^+, Π^+) as follows: we let $\Sigma_0^+ = \Pi_0^+$ denote the set of *atomic* formulæ (= "polynomials"). Define a formula \mathcal{F} inductively to be in Σ_n^+ (resp. Π_n^+) if it is of the form $\exists \mathcal{G}$ (resp. $\forall \mathcal{G}$) with

$\mathcal{G} \in \Pi_{n-1}^+$ (resp. $\mathcal{G} \in \Sigma_{n-1}^+$). The place in the hierarchy of a formula counts its number of *quantifier changes*. Secondly, we introduce the *total number of universal quantifiers* of a formula as above to be $f_1 + \cdots + f_N$.

An analysis shows that a positive prenex form of Julia Robinson’s original formula defining \mathbf{Z} in \mathbf{Q} is a Π_4^+ -formula (see 1.10), and we can conclude from this that the Σ_5^+ -theory of \mathbf{Q} (= theory of all Σ_5^+ -sentences that are true in \mathbf{Q}) is undecidable. $\text{HTP}(\mathbf{Q})$ is the question whether the Σ_1^+ -theory is undecidable. Also, that formula, in positive prenex form, has 8 universal quantifiers. This should be considered at the verge of human mathematical understanding — one is compelled to quote Hartley Rogers, Jr.: “The human mind seems limited in its ability to understand and visualize beyond four or five alternations of quantifier.” ([26], p. 322).

So how can we, in any way, improve upon this complexity? We propose to use elliptic curves and give a conjectural improvement. First of all, we recall the concept of a *model*¹ of \mathbf{Z} in \mathbf{Q} (cf. 1.11) and study how the complexity of formulæ changes under interpretation via certain models (1.14–1.22). We then recall (in Section 2) how elliptic curves over \mathbf{Q} provide natural models of $(\mathbf{Z}, +)$ in \mathbf{Q} . We follow a suggestion of Pheidas ([23]) that it is natural to use such models to try to define “divisibility” of integers within \mathbf{Q} ; this is very much inspired by the function field case. For this, we have to introduce a variant of the old concept of “elliptic divisibility sequence” (apparently due to Lucas and studied by M. Ward, cf. [35]). Assume that E is an elliptic curve over \mathbf{Q} with $(0, 0)$ as 2-torsion point and Weierstrass equation $y^2 = x^3 + ax^2 + bx$ with b squarefree, and that P is a point of infinite order of sufficiently large height on E . Then for even n , we can write

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

for coprime integers A_n, B_n, C_n , and $\{C_*\}$ forms an *odd divisibility sequence* in the sense that C_n divides C_{tn} precisely for odd t (2.12). Our first main theorem uses two further notions. Let R denote a set of primes. We agree to identify primes p with normalized non-archimedean valuations $v = v_p$, such that $v(p) = 1$ and $v(ab) = v(a) + v(b)$ (please mind: this is a logarithm of what has been called a valuation elsewhere). We say that $\{C_*\}$ is R -(odd-)primitive if any C_n has an (odd order) primitive divisor from R , i.e., there is a valuation $v \in R$ such that $v(C_n)$ is non-zero (odd) but $v(C_i) = 0$ for all

¹The words “model” and “interpretation” seem to have acquired a non-standard meaning in connection with HTP. The precise meaning will be explained in the text.

$i < n$. Secondly, for two rational numbers x and y , we denote by \mathcal{D}_R the R -divisibility predicate: $(\forall v \in R)(v(x) \text{ odd} \Rightarrow v(x) < v(y^2))$. Theorem 3.5 then says that *if in the above setup, $\{C_*\}$ is R -odd-primitive, then for any integers $m, n \in \mathbf{Z}$,*

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

This is our attempt at defining integer divisibility in the rational numbers.

The relevant question becomes: can we find R for which \mathcal{D}_R is equivalent to a formula in Σ_1^+ (whence irrelevant from our point of view of complexity) and for which $\{C_*\}$ is R -primitive? The elliptic Zsigmondy's theorem, transferred to C , says that R -primitivity holds for R equal to the set of all primes, but we don't know whether \mathcal{D}_R is Σ_1^+ for that R . On the other hand, a theorem of Van Geel and Demeyer (based on previous work of Pheidas and Van Geel/Zahidi) states that \mathcal{D}_R is diophantine for $R = R_D$ the set of primes inert in one of finitely many quadratic number fields of discriminants $D = \{d_1, \dots, d_r\}$, and hence for R of arbitrary high Dirichlet density $\neq 1$, see 3.15. So our natural conjecture (3.16) becomes an *inertial elliptic Zsigmondy's theorem: there exists E, P and D as above such that $\{C_*\}$ is R_D -odd-primitive.*

We can show that multiplication is definable in $(\mathbf{Z}, +, |, 0, \neq)$ by a Σ_3^+ -formula only involving one universal quantifier (4.1), and that our model allows us to get rid of “0” and “ \neq ”. Collecting these facts, we arrive at our second main theorem: *the conjecture implies that integer arithmetic $(\mathbf{Z}, +, \times)$ is interpretable by a Σ_3^+ -formula in the rationals \mathbf{Q} , using only one universal quantifier; and that the Σ_3^+ -theory of \mathbf{Q} is undecidable.* This (conjecturally) improves the complexity of Robinson's definition in two ways. In section 5, we adapt the construction to show that *the conjecture even implies that the Π_2^+ -theory (and even the set of formulæ with only one universal quantifier) is undecidable;* but note that this is *not* proven by constructing a model of \mathbf{Z} in \mathbf{Q} that has complexity Π_2^+ . The geometrical meaning of this statement is that there is a one-parameter family of hypersurfaces over \mathbf{Q} for which one cannot decide whether or not they all have a rational point.

It is difficult to verify the conjecture numerically since it involves hard prime factorisations. However, note that the philosophy of encoding the integer n by the point nP on an elliptic curve is advantageous from the point of view of divisibility for two reasons: the “powerful” part of the coordinates of nP is very small (in the sense that the height of the “powerless” part of nP is of the same order as the height of nP), and C_n tends to have many more prime factors than n . These remarks can be turned into heuristics

that support the conjecture (see section 6). The conjecture incorporates statements about solutions in coprime integers of such Calabi-Yau surfaces as

$$(A^2 + B^2)(A^2 + 11B^2) = 3^2 \cdot 5^2 \cdot (X^2 - 5Y^2)^2,$$

which becomes the “One Equation to Rule Them All” of the Π_2 -theory of \mathbf{Q} (like Martin Davis’s for the Σ_1 -theory of \mathbf{Z} ; but that equation heuristically behaved the wrong way, cf. [29]).

Finally, we use the periodicity of elliptic divisibility sequences to prove in Section 7 that if $\{B_*\}$ is the elliptic divisibility sequence associated to $(2, -4)$ on $y^2 = x^3 + 7x^2 + 2x$, then any B_{s^e} for s a prime number $\equiv \pm 3 \pmod{8}$ has a primitive odd order divisor from R_5 , and for $D = \{5, 13, 29, 41, 53\}$, the set $\{s \text{ prime} : B_s \text{ has a primitive odd order divisor from } R_D\}$ has Dirichlet density at least 95.5%.

Remarks. (i) Beltjukov studied the theory of $(\mathbf{Z}, +, |)$ ([2]) and Lipshitz ([17], [18], [19]) has studied divisibility structures of the form $(\mathcal{O}, +, |)$ for \mathcal{O} the ring of integers in a number field K , including (independently) the usual integers, and obtained exact results on which of these theories are (un)decidable. He showed in particular that multiplication is definable in the Σ_1^+ -theory of such a structure and that it contains a diophantine model of \mathbf{Z} , precisely if \mathcal{O} has infinitely many units. Thus, if K is not equal to \mathbf{Q} or an imaginary quadratic number field and A is an abelian variety with multiplication by \mathcal{O} , then an imitation of the above theory for A would lead to a Σ_1^+ -definition of \mathbf{Z} in \mathbf{Q} and hence a negative answer to Hilbert’s Tenth Problem for \mathbf{Q} . This can already occur for A the Jacobian of a genus two curve with real multiplication: to give an example from [14], the curve

$$\mathcal{C} : y^2 + (x^3 + x^2 + x)y = x^4 + x^3 + 3x^2 - 2x + 1$$

(the modular curve $X_0(85)$ modulo an Atkin-Lehner involution) has a Jacobian of rank two over \mathbf{Q} , and real multiplication by $\mathbf{Z}[\sqrt{2}]$ defined over \mathbf{Q} . The rôle of the “ x -coordinate” on the elliptic curve should be played by the associated Kummer surface. There are, however, many obstacles to make such a generalisation work, even assuming certain arithmetical conjectures.

A generalisation of the above to elliptic curves with complex multiplication, however, should be unproblematic.

(ii) In another direction, Poonen ([24]) has shown that there exists a set S of primes of Dirichlet density one such that \mathbf{Z} is definable by a diophantine formula in $\mathbf{Z}[\frac{1}{S}]$.

(iii) This paper supersedes the first author’s year 2000 manuscripts [8] about the topic.

(iv) Number theorists can take the following direct path to the relevant conjecture: Sections 2.4-2.14 (divisibility sequences), 3.1, 3.7 ((weak) R -primitivity), 3.16 (main conjecture) and Sections 6 and 7 (discussion of the conjecture).

Acknowledgements. It is a pleasure to thank Thanases Pheidas for his help. The first author thanks Graham Everest for making him reconsider this material during an inspiring visit to UEA in 2004, and for many suggestions. Some of the heuristical arguments in section 6.4 were shown to us by Bjorn Poonen at Oberwolfach in 2003, and some of the references in that section were kindly provided by Pieter Moree. Marco Streng suggested some important improvements in section 2.

1. Models and their complexity.

1.1 Positive prenex-form. Julia Robinson proved in 1949 that the set of rational integers \mathbf{Z} is definable in the rational numbers \mathbf{Q} ([25]) by a first-order formula. It is still an open problem whether \mathbf{Z} can be defined in \mathbf{Q} by a positive-existential formula (and consequently, the positive-existential theory of \mathbf{Q} is undecidable). It should therefore be interesting to study the question of how complicated the definition of \mathbf{Z} is in terms of number of universal quantifiers used, or number of quantifier changes. We thus propose to study the complexity of defining the integers in the rational numbers. To formulate the problem very precisely, we need to make the following convention: a formula \mathcal{F} in the first-order theory of $(\mathbf{Z}, +, \times, 0, 1, =)$ or $(\mathbf{Q}, +, \times, 0, 1, =)$ will be written in the following normal 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 $\mathbf{y} = (y_1^{(1)}, \dots, y_{e_1}^{(1)}, \dots, y_1^{(N)}, \dots, y_{e_N}^{(N)})$. We will call such a formula a $((f_1, e_1), \dots, (f_N, e_N))$ -formula and call this form the *positive prenex* form. Note that the formula is not only in “prenex”-form (in which the quantifiers are followed by a quantifier-free formula that can be any boolean combination of atomic formulæ; see, e.g. [6], p. 157), but that we let the quantifiers be followed by a single atomic formula, viz. an equation. That this is possible is specific to certain languages. We don’t want to allow negations in

the quantifier-free part, because we are interested in measuring “closeness” to a *positive existential* (= diophantine) formula. It is indeed possible to transform any formula into such positive prenex normal form; this is well known but we include a proof for completeness.

1.2 Lemma. *let $R \subseteq \mathbf{Q}$ be a ring. Any first-order formula in the ring language $(R, +, \times, 0, 1, =)$ of R can be written in normal form.*

Proof. The following logical connectives can occur: $\Rightarrow, \neg, \vee, \wedge$. Here is an algorithm that eliminates their occurrences. Replace $A \Rightarrow B$ by $\neg A \vee B$. Pull negations from left to right through a formula (changing quantifiers and connectives accordingly). Put all the quantifiers on the left (possibly changing names of variables).

Lagrange’s four-squares theorem states that any integer $n \geq 0$ is a sum of four squares. Therefore, for $x \in R$ we have

$$x > 0 \iff (\exists a, b, c, d, e, f, g, h)((e^2 + f^2 + g^2 + h^2)(x+1) = a^2 + b^2 + c^2 + d^2).$$

Furthermore, $n \neq 0 \iff (n > 0) \vee (n < 0)$. Use this to replace, for a polynomial P , the formula $P \neq 0$ by a formula only involving equality signs.

For polynomials P and Q , replace $(P = 0) \vee (Q = 0)$ by $PQ = 0$, and $(P = 0) \wedge (Q = 0)$ by $P^2 + Q^2 = 0$. The final result of all these replacements is the above normal form. \square

1.3 Remark. Depending on R , one can sometimes improve upon the number of existential quantifiers used to translate $P \neq 0$. For example, if $R = \mathbf{Q}$, then $P \neq 0 \iff (\exists Q)(PQ = 1)$.

1.4 Remark. The polynomial F in the general positive prenex form might still depend on unquantified variables (also called free variables) which are omitted in our notation; this will cause no confusion. If no free variables occur we call the formula a *sentence*. A sentence has a precise truth-value, whereas this is not the case for a formula with free variables. However if we give these free variables a specific value then we obtain a sentence with a specific truth value. The set of all specifications of the free variables for which the corresponding sentence is true, is *the set defined by the formula*.

1.5 Measures of complexity. As explained in the introduction, we do not care too much about the number of existential quantifiers, but want to have as few universal quantifiers as possible in our formulæ. A first measure of such complexity of a formula is its *total number of universal quantifiers* (t -complexity)

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

A second measure of complexity is the place of the formula in the (positive) arithmetical hierarchy, that we will now introduce.

1.6 The positive arithmetical hierarchy. One usually defines the (arithmetical) hierarchy (Σ, Π) of a language as follows (compare [3], p. 117). Let $\Sigma_0 = \Pi_0$ denote the set of quantifier-free formulæ. Define a formula \mathcal{F} inductively to be in Σ_n (resp. Π_n) if it is of the form $\exists \mathcal{G}$ (resp. $\forall \mathcal{G}$) with $\mathcal{G} \in \Pi_{n-1}$ (resp. $\mathcal{G} \in \Sigma_{n-1}$).

In accordance with our use of a normal form which is positive prenex, we define the *positive arithmetical hierarchy* (Σ^+, Π^+) as follows: we let $\Sigma_0^+ = \Pi_0^+$ denote the set of positive boolean combinations of atomic formulæ. Define a formula \mathcal{F} inductively to be in Σ_n^+ (resp. Π_n^+) if it is of the form $\exists \mathcal{G}$ (resp. $\forall \mathcal{G}$) with $\mathcal{G} \in \Pi_{n-1}^+$ (resp. $\mathcal{G} \in \Sigma_{n-1}^+$).

A formula in Σ_1 is called *existential*, in Π_1 *universal*, in Σ_1^+ *positive existential* or *diophantine*.

The *number of quantifier changes* c (c -complexity) can be defined by

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

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 $c(\mathcal{F}) = n$.

For a ring language as in 1.2, formulæ in Σ_0^+ are equivalent to *atomic* formulæ by 1.2. Furthermore, as non-equalities are existential, any Σ_{2n+1} -formula is equivalent to a Σ_{2n+1}^+ -formula and any Π_{2n} -formula is equivalent to a Π_{2n}^+ -formula.

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

1.7 Remark. (i) For $(\mathbf{N}, +, \times, 0, 1)$, a polynomial bijection $\mathbf{N}^2 \rightarrow \mathbf{N}$ as in Martin Davis ([10], pp. 236-237) can be used to show that any formula is equivalent to a formula in positive prenex form with $f_1 = \dots = f_N = 1$. For $(\mathbf{Z}, +, \times, 0, 1)$, the same conclusion $f_1 = \dots = f_N = 1$ holds by the method of diophantine storing. The analogous statement is not known for \mathbf{Q} , but would follow from the ABC-hypothesis, see [7].

(ii) In the course of the proof of the main theorem, we will also have to use other languages than the usual ring language, and the reader should be cautioned that the positive and the usual hierarchy can be quite different in such a case (up to equivalence of formulæ in that language): there might

be quantifier-free formulæ that are not equivalent to an atomic formula. Example: $(a = b) \wedge (c = d)$ in $(\mathbf{Z}, +, 0, 1, =)$.

1.8 Remark. A formula \mathcal{F} could be equivalent (in a given theory) to a formula \mathcal{G} whose complexity is different. In practice, it is often possible to reduce the number of universal quantifiers in a formula by using fewer variables, and we will sometimes do so. For example if \mathcal{F} and \mathcal{G} are formulæ with disjoint sets of variables, then $(\forall X, Y)(\mathcal{F}(X) \wedge \mathcal{G}(Y))$ is equivalent to $(\forall X)(\mathcal{F}(X) \wedge \mathcal{G}(X))$.

1.9 Robinson's definition. Julia Robinson's definition of the integers is the following: 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 $N \in \mathbf{Z} \iff \mathcal{R}(N)$ with

$$\mathcal{R}(N) : \forall A, B \{ [\phi(A, B, 0) \wedge (\forall M)(\phi(A, B, M) \Rightarrow \phi(A, B, M + 1))] \Rightarrow \phi(A, B, N) \}$$

We will now analyse the diophantine complexity of this formula:

1.10 Lemma. *The formula \mathcal{R} is equivalent to a Π_4^+ - $((5, 4), (3, 1))$ -formula \mathcal{F} with $t(\mathcal{F}) = 8$ and $c(\mathcal{F}) = 3$.*

Proof. We use the algorithm from the proof of Lemma 1.2. Thus, we replace the implications to get

$$(\forall A, B) \{ \neg [\phi(A, B, 0) \wedge (\forall M)(\neg \phi(A, B, M) \vee \phi(A, B, M + 1))] \vee \phi(A, B, N) \}.$$

We pull through the negations

$$(\forall A, B) \{ [\neg \phi(A, B, 0) \vee (\exists M)(\phi(A, B, M) \wedge \neg \phi(A, B, M + 1))] \vee \phi(A, B, N) \}.$$

Now plug in the $(0, 3)$ -formula $\phi(A, B, *)$

$$\begin{aligned} & (\forall A, B, X, Y, Z)(\exists M, X', Y', Z')(\forall X'', Y'', Z'')(\exists X''', Y''', Z''') \\ & [P_{A,B,0}^{X,Y,Z} \neq 0 \vee (P_{A,B,M}^{X',Y',Z'} = 0 \wedge P_{A,B,M+1}^{X'',Y'',Z''} \neq 0) \vee P_{A,B,N}^{X''',Y''',Z'''} = 0] \end{aligned}$$

In \mathbf{Q} , we can replace an inequality by an equality at the cost of introducing one existential quantifier (1.3). We can use the same variable for both inequalities in the above formula, since it is a disjunction of inequalities. We can simplify the arising formula further by using the same name for X' and X''' , Y' and Y''' and Z' and Z''' . to arrive at a $((5, 4), (3, 1))$ -formula.

□

1.11 (Diophantine) models. Our (conjectural) improvement of this formula will not depend on a definition of \mathbf{Z} as a *subset* of \mathbf{Q} , but rather on the existence of a model of \mathbf{Z} over \mathbf{Q} . We therefore give a general definition first (in a certain model theoretic parlance, this just means an interpretation of the first theory in the second model):

1.12 Definition. Let (M, L, ϕ) be a triple consisting of a set M and a finite collection $L = \{r_i\}$ of subsets of cartesian powers of M (called “relations” or “constants”), where ϕ is an *interpretation* of L in M (which we will often leave out of the notation). If $(N, L' = \{s_i\}, \phi')$ is another such triple, M is said to have a *model* (D, ι) in N if there is a bijection $\iota : M \rightarrow D$ between M and a definable subset D of some cartesian power N^d of N , such that the induced inclusions of $\iota(r_i)$ in the appropriate cartesian power of N are definable subsets. We call d the *dimension* of the model. By slight abuse, we will sometimes omit ι from notations.

1.13 Examples. From now on, we will write \mathbf{Z} and \mathbf{Q} for (\mathbf{Z}, L) and (\mathbf{Q}, L) with $L = (0, 1, +, \times, =)$ the standard language of rings. By further abuse of notation, we will often leave out the constants “0”, “1” and equality “=” from a language on a ring. A model of \mathbf{Z} in \mathbf{Q} is a countable definable subset of D , such that under a bijection $\iota : \mathbf{Z} \rightarrow D$, the induced images of the graphs of addition and multiplication are definable subsets D_+ and D_\times of \mathbf{Q}^3 . The result of Julia Robinson shows that one can take $D = \mathbf{Z}$ and $\iota = \text{id}$, leading to a one-dimensional model. If G is an affine algebraic group over \mathbf{Q} , then embedding G in some affine space of dimension d gives a d -dimensional model of $(G(\mathbf{Q}), +_G)$ in $(\mathbf{Q}, +, \times)$. If $G(\mathbf{Q}) = \mathbf{Z}$, one thus has a model of $(\mathbf{Z}, +)$ in \mathbf{Q} (but lacking multiplication).

One can measure the complexity of a model by the complexity of the formulæ that define the embeddings of the relations. Thus,

1.14 Definition. For S a definable subset of a cartesian power of N , write $t(S) \leq n$ (or $c(S) \leq n$) if there exists a formula \mathcal{F} defining S with $n = t(\mathcal{F})$ (or $n = c(\mathcal{F})$).

We say that the *t-complexity* $t(D)$ of a model (D, ι) of (M, L) in (N, L') satisfies $t(D) \leq n$ if

$$\max\{t(\iota(D)), t(\iota(r_i))\} \leq n,$$

and similarly for the *c-complexity* or position in the hierarchy. D is called a *diophantine model* of M in N if $t(D) = 0$.

1.15 Remark. This definition involves only upper bounds for the complexity of a definable set, since S could be definable by several equivalent

formulae having different complexity, cf. 1.8. In general, it seems quite hard to prove that a set *cannot* be defined by a less complex formula.

1.16 Examples (continued). The complexity of Julia Robinson’s model is as in Lemma 1.10. The t -complexity of embedding $(G(\mathbf{Q}), +_G)$ in \mathbf{Q} (for G an affine algebraic group) is zero, since $G(\mathbf{Q})$ is the solution set to the ideal of equations that defines G in affine space, and addition is defined by an algebraic formula that involves the coordinates in that affine space (note that a different formula might be needed for distinct cases, such as doubling of points, but this distinction is made by a formula only involving inequalities and case distinctions, that are equivalent to a formula only involving existential quantifiers).

1.17 Remark. If \mathbf{Z} admits a diophantine model in \mathbf{Q} , then there exists a variety V over \mathbf{Q} such that the real topological closure of the set of rational points $V(\mathbf{Q})$ in the set of real points $V(\mathbf{R})$ has infinitely many connected components. This contradicts a conjecture of Mazur, cf. [9].

1.18 Translation of formulae. One can use a model of M in N to translate formulae in M to formulae in N , such that true sentences in M are precisely translated into true sentences in N . Given a formula \mathcal{F} in M , one replaces every occurrence of a variable x by the N -definition of “ $x \in D$ ”, and every occurrence of a relation $r(\mathbf{x})$ by the N -definition of r . One thus gets a formula which we denote by $\iota(\mathcal{F})$.

1.19 Example. Consider the formula $\mathcal{F} : (\exists x_1)(\forall x_2)(x_1^2 x_2 + x_2 = 0)$ in \mathbf{Z} . Suppose one is given a 2-dimensional model $D \subseteq \mathbf{Q}^2$ of \mathbf{Z} in \mathbf{Q} . Then this formula translates into

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

where one should now further replace membership of D , $\iota(+)$ and $\iota(\times)$ by their first-order definitions. Note the introduction of the “dummy variables” u_i, v_i to unravel nested occurrences of addition and multiplication.

If one applies positive prenex simplification to remove implications and negations, one can keep track of the complexity of the translation. One can ask how the complexity of a formula changes under translation. We will only consider the following case:

1.20 Proposition. Let (D, ι) be a d -dimensional model of \mathbf{Z} in \mathbf{Q} and assume that membership of D is atomic and of $\iota(+)$ is Σ_1^+ . In the following

table, the second and third column list the positive hierarchical status of the formula $\iota(\mathcal{F})$ as a function of the status of $\iota(x)$ and \mathcal{F} as it is indicated in the first column and top row:

$\mathcal{F} \in$	$\iota(x) \in \Sigma_s^+ \Rightarrow \iota(\mathcal{F}) \in$	$\iota(x) \in \Pi_s^+ \Rightarrow \iota(\mathcal{F}) \in$
Σ_{2n}^+	Σ_{2n+s}^+	Σ_{2n+s+1}^+
Σ_{2n+1}^+	Σ_{2n+s}^+	Σ_{2n+s+1}^+
$\Pi_{2n}^+ (n > 0)$	Π_{2n+s-1}^+	Π_{2n+s}^+
Π_{2n+1}^+	Π_{2n+s+1}^+	Π_{2n+s+2}^+

(note: inclusion of a formula in a class of the hierarchy means that the formula is equivalent to a formula in that class). Furthermore, in all cases we have

$$t(\iota(\mathcal{F})) \leq t(\iota(x)) + dt(\mathcal{F}).$$

Proof. The proof is a matter of non-trivial book-keeping. We use the following notation: let $\Delta_n^+ = \Sigma_n^+ \cup \Pi_n^+$. We need to establish the following fact, that will be used implicitly in the sequel:

1.20.1 Lemma. *Let \mathcal{F}_1 be a Σ_n^+ -formula (respectively a Π_n^+ -formula) and suppose that $\{\mathcal{F}_2, \dots, \mathcal{F}_q\}$ is a finite collection of formulæ such that each \mathcal{F}_i is either a Σ_n^+ -formula (respectively a Π_n^+ -formula) or a Δ_m^+ -formula, for some $m < n$. Then*

$$\mathcal{F} = \mathcal{F}_1 \wedge \dots \wedge \mathcal{F}_q \text{ and } \mathcal{F}' = \mathcal{F}_1 \vee \dots \vee \mathcal{F}_q$$

are Σ_n^+ -formulæ (respectively Π_n^+ -formulæ).

Suppose further that \mathcal{F}_i is a $((f_{ik_i}, e_{ik_i}), \dots, (f_{i1}, e_{i1}))$ -formula; then:

$$t(\mathcal{F}) \leq \sum_{j=1}^{k_1} \max\{f_{1j}, \dots, f_{qj}\} \quad \text{and} \quad t(\mathcal{F}') \leq t(\mathcal{F}_1) + \dots + t(\mathcal{F}_q) = \sum_{i=1}^q \sum_{j=1}^{k_i} f_{ij}.$$

We prove the result for \mathcal{F}_1 a Π_n^+ statement – the other cases are similar. Without loss of generality, we may assume that each formula \mathcal{F}_i is a Π_n^+ -formula (indeed, we can add quantifiers whose variables are those variables that do not appear freely in \mathcal{F}_i ; for each new variable x introduced in this way add the equation “ $x = x$ ”). For $n = 0$ the statement is trivial. For $n = 1$ the result is also clear, since for any formulæ \mathcal{C} , \mathcal{D} , $(\forall x)(\mathcal{C}(x)) \wedge (\forall y)(\mathcal{D}(y))$

is equivalent to $(\forall x)(\mathcal{C}(x) \wedge \mathcal{D}(x))$. So, suppose each of the \mathcal{F}_i is a Π_{n+1}^+ -formula with $n > 0$, i.e., each \mathcal{F}_i is of the form

$$(\forall x_1, \dots, x_{f_{i1}})(\exists y_1, \dots, y_{m_i})(\mathcal{G}_i(x_1, \dots, x_n, y_1, \dots, y_f))$$

with $\mathcal{G}_i \in \Pi_{n-1}^+$. Let $m = m_1 + \dots + m_q$ and $f = \max_i f_{i1}$. Since for any formulæ \mathcal{C}, \mathcal{D} , $(\forall x)(\mathcal{C}(x)) \wedge (\forall y)(\mathcal{D}(y))$ is equivalent to $(\forall x)(\mathcal{C}(x) \wedge \mathcal{D}(x))$, and $(\exists x)(\mathcal{C}(x)) \wedge (\exists y)(\mathcal{D}(y))$ is equivalent to $(\exists x, y)(\mathcal{C}(x) \wedge \mathcal{D}(y))$, the formula \mathcal{F} is equivalent to

$$(\forall x_1, \dots, x_f)(\exists y_1, \dots, y_m)(\mathcal{G}_1 \wedge \dots \wedge \mathcal{G}_q) .$$

By induction, the formula $\mathcal{G} = \mathcal{G}_1 \wedge \dots \wedge \mathcal{G}_q$ is Π_{n-1}^+ , hence \mathcal{F} is a Π_{n+1}^+ -formula. We have $t(\mathcal{F}) = f + t(\mathcal{G})$, and hence by induction $t(\mathcal{F}) = \max_i f_{i1} + \sum_{j=2}^k \max_i f_{ij}$, which proves the result (note that the extra quantifiers which we may have added to make all formulæ Π_n^+ do not affect the statement). The statement concerning a disjunction of Π_n^+ -formulæ can be proven similarly, by noting that for formulæ \mathcal{C}, \mathcal{D} , $(\forall x)(\mathcal{C}(x)) \vee (\forall y)(\mathcal{D}(y))$ is equivalent to $(\forall x, y)(\mathcal{C}(x) \vee \mathcal{D}(y))$, and $(\exists x)(\mathcal{C}(x)) \vee (\exists y)(\mathcal{D}(y))$ is equivalent to $(\exists x)(\mathcal{C}(x) \vee \mathcal{D}(x))$. This proves the lemma. \square

The proof of 1.20 is by induction, jumping down by 2 in the hierarchy (and thus induction starts at the two lowest levels of the hierarchy):

(a) Let $\iota(\times) \in \Sigma_s^+$. Suppose first that $\mathcal{F} \in \Sigma_0^+$, i.e.,

$$\mathcal{F} : F(x_1, \dots, x_n) = 0$$

for some integral polynomial. Then there exists a set $\Lambda = \{1, \dots, \ell\}$, with $\ell \geq n$, subsets $I, J \subset \Lambda^3$ and natural numbers $s, r \in \Lambda$ such that the translation $\iota(\mathcal{F})$ is of the form:

$$\begin{aligned} & (\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge (\exists \mathbf{u}_1, \dots, \mathbf{u}_\ell) \\ & (\mathbf{u}_1 = \mathbf{x}_1 \wedge \dots \wedge \mathbf{u}_n = \mathbf{x}_n \bigwedge_{\bar{i} \in I} (\mathbf{u}_{i_1}, \mathbf{u}_{i_2}, \mathbf{u}_{i_3}) \in \iota(+)) \\ & \bigwedge_{\bar{j} \in J} (\mathbf{u}_{j_1}, \mathbf{u}_{j_2}, \mathbf{u}_{j_3}) \in \iota(\times) \wedge (\mathbf{u}_r, \mathbf{u}_r, \iota(0)) \in \iota(+)) , \end{aligned}$$

where $\bar{i} = (i_1, i_2, i_3)$ and $\bar{j} = (j_1, j_2, j_3)$ are multi-indices and boldface variables are variables ranging over \mathbf{Q}^d . The conjunction

$$\bigwedge_{\bar{i} \in I} (\mathbf{u}_{i_1}, \mathbf{u}_{i_2}, \mathbf{u}_{i_3}) \in \iota(+)) \bigwedge_{\bar{j} \in J} (\mathbf{u}_{j_1}, \mathbf{u}_{j_2}, \mathbf{u}_{j_3}) \in \iota(\times) \wedge (\mathbf{u}_r, \mathbf{u}_r, \iota(0)) \in \iota(+))$$

is a conjunction of Σ_1^+ -formulæ and Σ_s^+ -formulæ, and hence is itself a Σ_s^+ -formula. Hence, the formula $\iota(\mathcal{F})$ is a conjunction of a Σ_s^+ -formula and a Σ_0^+ -formula, hence is a Σ_s^+ -formula. Furthermore, $t(\iota(\mathcal{F})) = t(\iota(\times))$.

If $\mathcal{F} \in \Sigma_1^+$, then $\iota(\mathcal{F}) \in \Sigma_s^+$. Indeed, write $\mathcal{F} = (\exists x_1, \dots, x_n)\mathcal{G}(x_1, \dots, x_n)$ for some quantifier-free formula \mathcal{G} . The translation $\iota(\mathcal{F})$ is then given by:

$$(\exists \mathbf{x}_1, \dots, \mathbf{x}_n)(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D \wedge \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n)),$$

and the result is clear since membership of D is atomic.

We proceed by induction. Suppose that \mathcal{F} is Σ_{n+1}^+ , i.e. there exists a Σ_{n-1}^+ -formula \mathcal{G} such that

$$\mathcal{F} : (\exists x_1, \dots, x_n)(\forall y_1, \dots, y_m)(\mathcal{G}(x_1, \dots, x_n, y_1, \dots, y_m)).$$

The translation $\iota(\mathcal{F})$ then becomes:

$$\begin{aligned} & (\exists \mathbf{x}_1, \dots, \mathbf{x}_n)(\forall \mathbf{y}_1, \dots, \mathbf{y}_m)[(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge \\ & \wedge ((\mathbf{y}_m \in D \wedge \dots \wedge \mathbf{y}_m \in D) \Rightarrow \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m))] \end{aligned}$$

which is equivalent to:

$$\begin{aligned} & (\exists \mathbf{x}_1, \dots, \mathbf{x}_n)(\forall \mathbf{y}_1, \dots, \mathbf{y}_m)[(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge \\ & \wedge (\mathbf{y}_1 \notin D \vee \dots \vee \mathbf{y}_m \vee \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m))] \end{aligned}$$

Since subformulæ of the form $\mathbf{y} \notin D$ are negations of atomic formulæ in the language of \mathbf{Q} , they are equivalent to a formula in Σ_1^+ and, by induction $\iota(\mathcal{G}) \in \Sigma_{n-1+s}^+$ ($n+1$ even) or Σ_{n-2+s}^+ ($n+1$ odd), it follows that the subformula

$$(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge (\mathbf{y}_1 \notin D \vee \dots \vee \mathbf{y}_m \vee \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m))$$

is Σ_{n-1+s}^+ ($n+1$ even) or Σ_{n+s}^+ ($n+1$ odd). Hence $\iota(\mathcal{F})$ is Σ_{n+1+s}^+ ($n+1$ even) or Σ_{n+s}^+ ($n+1$ odd). Furthermore, $t(\iota(\mathcal{F})) = dm + t(\iota(\mathcal{G}))$, from which we find by iteration that $t(\iota(\mathcal{F})) = dt(\mathcal{F}) + t(\iota(\times))$.

If \mathcal{F} is a Π_n^+ -formula, the result can be proven in a similar way – but one has to start the induction at $n=1$ and $n=2$.

(b) Assume $\iota(\times) \in \Pi_s^+$. If \mathcal{F} is a Σ_0^+ -formula we get the same translation as in (a). The subformula

$$\bigwedge_{\bar{i} \in I} (\mathbf{u}_{i_1}, \mathbf{u}_{i_2}, \mathbf{u}_{i_3}) \in \iota(+)$$

$$\bigwedge_{\bar{j} \in J} (\mathbf{u}_{j_1}, \mathbf{u}_{j_2}, \mathbf{u}_{j_3}) \in \iota(\times) \wedge (\mathbf{u}_r, \mathbf{u}_r, \iota(0)) \in \iota(+)$$

is a conjunction of Σ_1^+ -formulæ and Π_s^+ -formulæ, and hence is itself a Π_s^+ -formula. The translation of $\iota(\mathcal{F})$ is then of the form:

$$(\exists \mathbf{u}_1, \dots, \mathbf{u}_l) \mathcal{G}$$

where \mathcal{G} is Π_s^+ , hence $\iota(\mathcal{F})$ is Σ_{s+1}^+ .

If \mathcal{F} is a Σ_1^+ -formula, then $\mathcal{F} = (\exists x_1, \dots, x_n) \mathcal{G}(x_1, \dots, x_n)$ for some quantifier-free formula \mathcal{G} . The translation $\iota(\mathcal{F})$ is then given by:

$$(\exists \mathbf{x}_1, \dots, \mathbf{x}_n) (\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D \wedge \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n)) .$$

Since $\iota(\mathcal{G})$ is Σ_{s+1}^+ and membership of D is atomic, the quantifier-free part of this formula is Σ_{s+1}^+ . Hence $\iota(\mathcal{F})$ is Σ_{s+1}^+ .

We proceed by induction. Let \mathcal{F} be a Σ_{n+1}^+ -formula, i.e.

$$\mathcal{F} = (\exists x_1, \dots, x_n) (\forall y_1, \dots, y_m) (\mathcal{G}(x_1, \dots, x_n, y_1, \dots, y_m))$$

for some $\mathcal{G} \in \Sigma_{n-1}^+$. The translation $\iota(\mathcal{F})$ then becomes:

$$\begin{aligned} & (\exists \mathbf{x}_1, \dots, \mathbf{x}_n) (\forall \mathbf{y}_1, \dots, \mathbf{y}_m) [(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge \\ & \wedge ((\mathbf{y}_m \in D \wedge \dots \wedge \mathbf{y}_1 \in D) \Rightarrow \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m))] \end{aligned}$$

which is equivalent to:

$$\begin{aligned} & (\exists \mathbf{x}_1, \dots, \mathbf{x}_n) (\forall \mathbf{y}_1, \dots, \mathbf{y}_m) [(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge \\ & \wedge (\mathbf{y}_1 \notin D \vee \dots \vee \mathbf{y}_m \vee \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m))] . \end{aligned}$$

By induction $\iota(\mathcal{G})$ is a Σ_{n+s}^+ -formula (if $n+1$ is even) or Σ_{n+s-1}^+ -formula (if $n+1$ is odd), hence

$$(\mathbf{x}_1 \in D \wedge \dots \wedge \mathbf{x}_n \in D) \wedge (\mathbf{y}_1 \notin D \vee \dots \vee \mathbf{y}_m \vee \iota(\mathcal{G})(\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_m))$$

is Σ_{n+s}^+ or Σ_{n+s-1}^+ . From which it easily follows that $\iota(\mathcal{F})$ is Σ_{n+s+2}^+ ($n+1$ even) or Σ_{n+s+1}^+ ($n+1$ odd).

If \mathcal{F} is a Π_n^+ -formula, the result can be proved in a similar way (but starting the induction at $n=1$ and $n=2$). \square

1.21 Remark. If membership of D is positive-existential, then one can slightly alter the model (D, ι) to another (D', ι') in which membership of D' is quantifier-free, and hence for this altered model the theorem is true.

1.22 Corollary. *If (D, ι) is a model of \mathbf{Z} in \mathbf{Q} that has D defined by an atomic (Σ_0^+) -formula, $\iota(+)$ diophantine (Σ_1^+) and $t(\iota(\times)) \leq 1$, then the Σ_3^+ -theory of \mathbf{Q} is undecidable.*

Proof. Davis, Matijasevich, Putnam and Robinson (cf. [10]) have shown that the Σ_1^+ -theory of \mathbf{Z} is undecidable, but the proposition implies that any Σ_1^+ -sentence is translated into a Σ_3^+ -sentence over \mathbf{Q} using ι . Indeed, $\iota(\times)$ is Π_2^+ , Σ_2^+ or Σ_3^+ , and in each of these cases, a Σ_1^+ -sentence translates to a Σ_3^+ , Σ_2^+ and Σ_3^+ -sentence, respectively. \square

2. Preliminaries on elliptic divisibility sequences

2.1 Elliptic curve model of $(\mathbf{Z}, +)$. Let E denote an elliptic curve of rank one over \mathbf{Q} . Thus, as a group, $E(\mathbf{Q}) = \mathbf{Z} \oplus \mathcal{T}$ for a finite group \mathcal{T} of cardinality τ . Let P be a point of infinite order on E . Choose a plane model $f(x, y) = 0$ for E .

2.2 Lemma. (i) *In the above coordinates (x, y) , for any r , the set $T_{r\tau} = \langle r\tau P \rangle = \{nr\tau P : n \in \mathbf{Z}\}$ is diophantine over \mathbf{Q} .*

(ii) *Consider $D_r := \{(x, y, 1) : (x, y) \in T_{r\tau}\} \cup \{(0, 1, 0)\}$. Consider $\mathbf{0} := (0, 1, 0)$ as a symbol for the neutral element of E . If $+$ denotes the addition on E , then (D_r, ι) is a three-dimensional diophantine model of $(\mathbf{Z}, +)$ over \mathbf{Q} (where $\iota(0) = \mathbf{0}$ and $\iota(n) = (x(n\tau r P), y(n\tau r P), 1)$). Furthermore, membership of D_r (“ $(x, y, z) \in D_r$ ”) can be expressed by an atomic formula.*

(iii) *The relations “0” and “ \neq ” in $(\mathbf{Z}, +)$ are diophantine over \mathbf{Q} via (D_r, ι) .*

Proof. (i) Let Q be a generator for the free part of E . Then there exists an integer N such that $P = NQ$. Then

$$T_{r\tau} = \{R \in E(\mathbf{Q}) : (\exists S \in E(\mathbf{Q}))(R = Nr\tau S)\}.$$

The statement that “ $R \in E(\mathbf{Q})$ ” is a quantifier-free formula in \mathbf{Q} . The statement that $R = Nr\tau S$ (for fixed integers N, r) is too. Hence T_r is diophantine over \mathbf{Q} .

(ii) The map ι is a bijection since we have killed the torsion subgroup of $E(\mathbf{Q})$ by multiplying by τ . The addition formulæ on E can be written down in terms of coordinates on the chosen model. They will involve a choice distinction (e.g., doubling a point is different from adding two distinct points that are not opposite), but these choices are written by a formula involving inequalities and connectives, which translates into normal form only involving existential quantifiers. Hence addition is given by a diophantine formula. The statement about membership is immediate.

(iii) $\iota(0) = (0, 1, 0)$ is obviously atomic. Since we are in a group, to define “ $a \neq b$ ” in a diophantine way, it suffices to define “ $n \neq 0$ ”, and this is clearly equivalent to $\iota(n) \in T_{r\tau}$, which is diophantine. \square

2.3 Remark. Note that if E is an elliptic curve of rank one over \mathbf{Q} , there is an algorithm to compute the torsion subgroup, and if a point P of infinite order is known, then one can find N and Q algorithmically by going through the (finite) list of points R of height smaller than P and checking whether $mR = P$ for the appropriate finite list of integers m .

2.4 An “odd” divisibility sequence. Let E be an elliptic curve over \mathbf{Q} of non-zero rank over \mathbf{Q} . Let P be a point of infinite order on E . We want to study arithmetical properties of the numerator and denominator of the coordinates of multiples of P . Choose a plane Weierstrass model for E :

$$y^2 = x^3 + ax^2 + bx + c,$$

with a, b, c integers. We can write

$$nP = (x_n, y_n) = \left(\frac{a_n}{B_n^2}, \frac{c_n}{B_n^3} \right),$$

with a_n, B_n and c_n, B_n pairs of coprime integers (with B_n and c_n defined up to sign).

2.5 Notation. We write (a, b) to denote any greatest common divisor of integers a and b (hence this symbol doesn’t have a well-defined sign).

2.6 Lemma. (i) *If v is a valuation for which $v(B_n) > 0$ then for any integer t , $v(B_{tn}) = v(B_n) + v(t)$.*

(ii) *$\{B_n\}$ is a divisibility sequence, i.e., if $m|n$, then B_m divides B_n .*

(iii) *$\{B_n\}$ is a strong divisibility sequence, i.e., $(B_m, B_n) = B_{(m,n)}$.*

Proof. (i) For $v \neq v_2$, the claim follows from looking at the formal group law associated to $E(\mathbf{Q}_p)$, cf. [4] - but some care should be taken with this reference, cf. the remark below. The following considerations hold regardless of the fact whether E is in global minimal form or not, as long as the coefficients are integral.

Let $v = v_p$. Let \hat{E} denote the formal group of E . If E_1 denotes the kernel of reduction modulo p , then $E_1 \rightarrow \hat{E}(p\mathbf{Z}) : P = (x, y) \mapsto z(P) := -\frac{x}{y}$ is an isomorphism such that $v(z) = -\frac{1}{2}v(x)$. Theorem IV.6.4(b) from [31] says that if $r > 1/(p-1)$, then the formal logarithm induces an isomorphism $\hat{E}(p^r\mathbf{Z}) \cong p^r\mathbf{Z}$.

Note that for rational primes, $1/(p-1) < 1$ unless $p = 2$. Hence if $p \neq 2$ or $v(z(P)) > 1$, the isomorphism $\hat{E}(p^r\mathbf{Z}) \cong p^r\mathbf{Z}$ holds for $r = v(z(P))$ and since it is true for any larger r , the map preserves valuations. Hence $v(z(nP)) = v(n) + v(z(P))$. This implies the claim since $z(nP) = -\frac{a_n B_n}{c_n}$ and a_n and c_n are coprime to B_n .

We are only left to consider the case $v = v_2$ and $v_2(z(P)) = 1$. Assume $v_2(x) < 0$. The duplication formula gives

$$x_2 = \frac{x}{4} \cdot \frac{1 - 2bx^{-2} - 8cx^{-3} + (b^2 - 4ac)x^{-4}}{1 + ax^{-1} + bx^{-2} + cx^{-3}},$$

The second factor in this product has valuation zero, and hence we get $v(x_2) = v(x) - 4$, and this implies the result for $t = 2$. It follows by induction for $t = 2^\ell$ for some ℓ , and then, using the first part of the proof, for general $t = 2^\ell \cdot t'$ with t' odd.

(ii) follows immediately from (i).

For (iii), we only need to prove that (B_m, B_n) divides B_d for $d = (m, n)$. Choose integers x, y such that $xm + yn = d$. Then part (i) implies that $v(B_{xm}) \geq v(B_m) \geq v(B_d)$ and $v(B_{yn}) \geq v(B_n) \geq v(B_d)$. Therefore $dP = xmP + ynP$ belongs to the group of points $P = (x, y)$ with $v(x) \leq -2r$ (including the zero element of E) — this is a group, since under the isomorphism $E_1 \mapsto \hat{E}(p\mathbf{Z})$ it corresponds to the subgroup $\hat{E}(p^r\mathbf{Z})$. Hence $v(x_d) \geq -2r$, so $v(B_d) \leq r$. \square

2.7 Remark. As Marco Streng notes, the claim in [4] that $v(B_{tn}) = v(B_n) + v(t)$ also holds for the long Weierstrass form and for number fields is wrong; a counterexample is given by $P = (-\frac{1}{4}, \frac{7}{8})$ on $y^2 + xy = x^3 + x^2 - 2x$, for which $v_2(B_2) = 3$ but $v_2(B_1) + v_2(2) = 2$. Over an arbitrary number field, it might go wrong for a larger number of (too ramified) valuations.

In proofs to follow, we will rely on properties of division polynomials ϕ_n, ψ_n, ω_n (e.g., [31] III.3.7 for standard Weierstrass form and [1] for the general case). The sequence $\{\psi_n\}$ has been termed an *elliptic divisibility sequence* by Morgan Ward ([35]). This recourse to the literature is strictly speaking not necessary in this section (but we will need it in the final part of the paper), since all properties can be checked by direct, but sometimes tedious, computation using the addition formulæ on E . Instead, we will use the following

2.8 Substitution principle. *Let $f \in \mathbf{C}[x_1, y_1, z_1, \dots, x_r, y_r, z_r]$ be a homogeneous polynomial w.r.t. the weights $\text{wt}(x_i) = 2i^2$, $\text{wt}(y_i) = i^2$ and $\text{wt}(z_i) = 3i^2$. Suppose $f(\phi_1, \psi_1, \omega_1, \dots, \phi_r, \psi_r, \omega_r) = 0$. Then for any point $P \in E(\mathbf{Q})$ that is non-singular modulo all primes, we have*

$$f(a_1, B_1, c_1, \dots, a_r, B_r, c_r) = 0,$$

if we choose the signs of a_i, B_i, c_i such that they agree with those of the classical division polynomials.

Proof. The trick is dehomogenization w.r.t. the denominator of x_1 . As Mohamed Ayad has notes by direct computation in [1] (bottom of page 306), for any n we can write

$$x_n = \frac{b_1^{2n^2} \phi_n}{b_1^2 ((b_1^{n^2-1} \psi_n)^2)}, y_n = \frac{b_1^{3n^2} \omega_n}{b_1^3 (b_1^{n^2-1} \psi_n)^3},$$

where numerators and denominators in these fractions are *integers*; that there is no cancellation of factors of b_1 in this representation; and that the common divisors of $b_1^{2n^2} \phi_n$ and $b_1^{n^2-1} \psi_n$ (and $b_1^{3n^2} \omega_n$ and $b_1^{n^2-1} \psi_n$) are the primes p for which P is singular modulo p . Therefore, if P is non-singular modulo all primes, we find $a_n = b_1^{2n^2} \phi_n$, $B_n = b_1^{n^2} \psi_n$ and $c_n = b_1^{3n^2} \omega_n$, and the result follows. \square

Now let E be an elliptic curve of rank one over E with a rational two-torsion point. By translation, we can assume that $(0,0)$ is a two-torsion point on E . Then E has a Weierstrass equation $y^2 = x^3 + ax^2 + bx$.

2.9 Lemma/Definition. *Let E be in Weierstrass form $y^2 = x^3 + ax^2 + bx$, having $(0,0)$ as rational 2-torsion point. Let P be a point of infinite order in $2E(\mathbf{Q})$ (i.e., divisible by 2 in $E(\mathbf{Q})$) that is non-singular modulo all primes. Then we can write*

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

for integers A_n, B_n and C_n (defined up to sign) with $(A_n, B_n) = 1$ and $(B_n, C_n) = 1$. Then:

- (i) The greatest common divisor of A_n and C_n divides the coefficient b of the Weierstrass model, and the order of b at any common divisor of A_n and C_n is at least 2; in particular, if b is squarefree, then $(A_n, C_n) = 1$;
- (ii) We have $B_{2n} = 2A_n B_n C_n$ up to sign; in particular, A_n divides B_{2n} .

Proof. Let $P = 2Q$ with $Q \in E(\mathbf{Q})$. We have $\phi_2 = (\phi_1 - b)^2$, so applying the substitution principle to this equation and the point nQ , we find that x_n is a rational square and hence A_n is well-defined up to sign. Substituting the point nP into the equation of E gives that $c_n^2 = A_n^2 (A_n^4 + aA_n^2 B_n^2 + bB_n^4)$, so A_n divides c_n and the definition of C_n makes sense. Then $C_n^2 = A_n^4 + aA_n^2 B_n^2 + bB_n^4$, and the gcd of C_n and A_n divides bB_n^4 , hence b since B_n and A_n are coprime; if $v((C_n, A_n)) > 0$, then we see immediately from this formula that $v(b) \geq 2$. This proves (i).

(ii) This follows from the substitution principle via the identity of division polynomials $\psi_2 = 2\psi_1\omega_1$ applied to nQ . \square

2.10 Remark. The numbers A_n , B_n and C_n (and the symbol $\sqrt{x_n}$ occasionally to be used) are only defined up to sign, but that sign will play no rôle in the formulæ under consideration (such as (ii) above), so we will not mention this issue anymore, except in the final section of this paper.

In subsequent considerations, we will also need to study the divisibility properties of the sequences $\{A_*\}$ and $\{C_*\}$. It turns out that divisibility between their m - and n -th term is only assured if n is an *odd* multiple of m .

2.11 Definition. We call a sequence of integers $\{X_*\}$ an *odd divisibility sequence* if X_n divides X_{nt} as soon as t is odd. We call $\{C_*\}$ as defined by the previous lemma *the odd divisibility sequence associated to (E, P)* .

That the previous definition makes sense is the contents of the following lemma:

2.12 Lemma. *Assume (E, P) and (A_*, B_*, C_*) are as in Lemma 2.9, with b and $a^2 - 4b$ squarefree. Then:*

- (i) $\{A_*B_*\}$ is a strong divisibility sequence.
- (ii) $\{A_*\}$ and $\{C_*\}$ are odd divisibility sequences.
- (iii) If t is odd and $v(A_n) > 0$, then $v(A_{nt}) = v(A_n) + v(t)$; but if t is even, then $(A_n, A_{nt}) = 1$ for all n . Identical statements hold with A_* replaced by C_* .

Proof. Recall that we have a morphism of 2-descent (cf. [31], X.4.9) given by the rational map:

$$\delta' : E \rightarrow E' : (X, Y) \mapsto \left(\frac{Y^2}{X^2}, \frac{Y(X^2 - a^2 + 4b)}{X^2} \right)$$

with $E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$.

- (i) Suppose $Q = nP$ maps via δ' to Q' . Then $x(Q') = \left(\frac{y(Q)}{x(Q)}\right)^2$, so

$$\sqrt{x(Q')} = \frac{A'_n}{B'_n} = \frac{C_n}{B_n A_n}$$

is a coprime representation (since b is squarefree), and we find that $\{A_*B_*\}$ is a strong divisibility sequence, as in Lemma 2.6, (as it is equal to the “ B' ”-sequence $\{B'_*\}$ associated to $(E', \delta'(P))$).

(ii) Let us now prove that $\{A_*\}$ is an odd divisibility sequence. Suppose $v(A_n) > 0$. Then $v(B_n) = 0$ by coprimeness of the representation. Now $v(A_n B_n) \geq v(A_n) > 0$, and since $B'_n = 2A_n B_n$, the formal group law on E' (2.6) implies that $v(B'_{tn}) = v(B'_n) + v(t)$, so we find

$$(2.12.1) \quad v(A_{tn}) + v(B_{tn}) = v(A_n) + v(t).$$

If $v(B_{tn}) = 0$, we indeed find that $v(A_{tn}) \geq v(A_n)$. If on the other hand, $v(B_{tn}) = 0$, then since A_{tn} and B_{tn} are coprime, we find that $v(A_{tn}) = 0$, and hence $v(B_{tn}) = v(A_n) + v(t)$. Now A_n divides B_{2n} (2.9 (ii)), so we have that $(B_{tn}, B_{2n}) = B_{(tn, 2n)} = B_{n(t, 2)}$ is divisible by a valuation v which doesn't divide B_n ; hence $(t, 2) \neq 1$ and t is even; which we have excluded.

That $\{C_*\}$ is an odd divisibility sequence is immediate, since $C_n = A'_n$ for the image sequence under δ' (with $a^2 - 4b$ squarefree), and we have just shown that $\{A'_*\}$ is an odd divisibility sequence.

(iii) This is implicit in the proof of (ii), noting again that A_{tn} and B_{tn} are coprime in (2.12.1). \square

2.13 Remark. Here is a quick proof that $\{A_*\}$ and $\{C_*\}$ are odd divisibility sequences: if an integer d divides A_n or C_n , then $nP \in E[2](\mathbf{Z}/d)$, so for odd t , $tnP = nP \in E[2](\mathbf{Z}/d)$.

2.14 Example. The elliptic curve $E : y^2 = x^3 + 12x^2 + 11x = x(x+1)(x+11)$ is of rank one over \mathbf{Q} , and $P = (1/4, 15/8)$ is of infinite order. The torsion subgroup of $E(\mathbf{Q})$ is $\mathbf{Z}/2 \times \mathbf{Z}/2$, generated by $(-1, 0)$ and $(0, 0)$. We computed the prime factorisations of A_n, B_n and C_n for $n \leq 8$:

$$\begin{aligned}
A_1 &= 1 \\
A_2 &= 5 \cdot 7 \\
A_3 &= 19 \cdot 269 \\
A_4 &= 659 \cdot 1931 \\
A_5 &= 23042506969 \\
A_6 &= \underline{5 \cdot 7} \cdot 89 \cdot 4639 \cdot 4575913 \\
A_7 &= 647873811 \cdot 19522768049 \\
A_8 &= 1321 \cdot 6637 \cdot 1356037 \cdot 6591431535431 \\
B_1 &= 2 \\
B_2 &= \underline{2^2} \cdot 3 \\
B_3 &= \underline{2} \cdot 29 \cdot 41 \\
B_4 &= \underline{2^3} \cdot \underline{3} \cdot 5 \cdot 7 \cdot 37 \cdot 53 \\
B_5 &= \underline{2} \cdot 11 \cdot 6571 \cdot 10949 \\
B_6 &= \underline{2^2} \cdot \underline{3^2} \cdot 19 \cdot \underline{29} \cdot \underline{41} \cdot 269 \cdot 467 \cdot 2521 \\
B_7 &= \underline{2} \cdot 31 \cdot 211 \cdot 1481 \cdot 8629 \cdot 184598671 \\
B_8 &= \underline{2^4} \cdot \underline{3^1} \cdot \underline{5} \cdot \underline{7} \cdot 13 \cdot \underline{37} \cdot \underline{53} \cdot 659 \cdot 1931 \cdot 160117 \cdot 5609521 \\
C_1 &= 3 \cdot 5 \\
C_2 &= -37 \cdot 53 \\
C_3 &= \underline{3^2} \cdot \underline{5} \cdot 467 \cdot 2521 \\
C_4 &= -13 \cdot 160117 \cdot 5609521 \\
C_5 &= \underline{3} \cdot \underline{5} \cdot 17 \cdot 67 \cdot 1601 \cdot 3019 \cdot 17417 \cdot 379513 \\
C_6 &= 23 \cdot \underline{37} \cdot \underline{53} \cdot 59 \cdot 10531 \cdot 1131223 \cdot 7186853449441 \\
C_7 &= -\underline{3} \cdot \underline{5} \cdot 353 \cdot 1483 \cdot 17609 \cdot 11748809 \cdot 281433601 \cdot 46333351129459 \\
C_8 &= 5303 \cdot 108739 \cdot 1830931 \cdot 170749043903 \cdot 92397921271034416798380481
\end{aligned}$$

Note that although $b = 11$ is squarefree in the example, $a^2 - 4b = 100$ is not. This means something might go wrong with the valuation formula for C_* upon multiplication by 2 or 5, and indeed, $v_5(C_5) \neq v_5(C_1) + v_5(5)$.

The examples illustrate all the (non-)divisibility-properties mentioned before, but also some other apparent features that will be discussed later on: whereas the indices have one prime factor on average, the numbers themselves have three primitive factors on average. It is expected that for any given $k > 0$, all terms in the sequence from a certain moment on will have at least k primitive factors. In the above tables, we have underlined the “non-primitive” part, i.e., the prime factors that occur earlier on the list.

Observation. *All divisors of A_n and B_n for odd n are $\equiv \pm 1 \pmod{5}$.*

Proof (for B_* , as shown to us by Karl Rubin). 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

On the other hand, all C_n seem to have primitive prime divisors of odd order $\equiv \pm 2 \pmod{5}$, i.e., inert in $\mathbf{Q}(\sqrt{5})$, but we have no general proof of that.

3. Elliptic divisibility sequences and models of $(\mathbf{Z}, +, |)$

3.1 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 .

3.2 Lemma. *Suppose that E and P are as in lemma 2.9. 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.*

Proof. It suffices to prove this for the A -sequence, since the descent morphism δ' transfers $\{C_*\}$ into $\{A_*\}$ (proof of Lemma 2.12). Now since $\{A_*B_*\}$ is a strong divisibility sequence (2.12), we have

$$(A_mB_m, A_nB_n) = A_{(m,n)}B_{(m,n)}.$$

Since we assume $v(A_m) > 0$ and $v(A_n) > 0$, we have $v(B_m) = v(B_n) = 0$ by coprimeness assumptions; and $v((A_{(m,n)}B_{(m,n)})) > 0$ by the above formula. Suppose first that $v(A_{(m,n)}) > 0$. Since $(m, n) \leq m$, the R -primitivity of v for A_m implies that $(m, n) = m$. This means that $m|n$. By 2.12 (iii), we find that n/m is odd.

On the other hand, if $v(B_{(m,n)}) > 0$, since $\{B_*\}$ is a divisibility sequence and $(m, n)|m$, we have $v(B_m) > 0$, contrary to the assumption. \square

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

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

3.4 Remark. This predicate says that odd order “zeros” of x are zeros of at least half that order of y , and that odd order “poles” of x are at most poles of y of half that order. Note that it seems at this point maybe more natural to have a definition in which the condition $v(x) < v(y^2)$ is replaced by $v(x) < v(y)$, but for future applications, we will need it as it stands.

3.5 Theorem. *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 and $a^2 - 4b$ squarefree. Assume the odd divisibility sequence $\{C_*\}$ associated to P on E is R -odd-primitive. Then for any integers $m, n \in \mathbf{Z}$,*

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

Proof. Replacing P by a suitable multiple, we can assume P is non-singular modulo all primes. Indeed, for any prime p , consider the group $E(\mathbf{Q}_p)$ and the subgroup $E_0(\mathbf{Q}_p)$ of points that reduce to non-singular points modulo p . Then $E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)$ is finite and non-zero for only finitely many p (actually, by a theorem of Kodaira and Néron, of order bounded uniformly in p by 4 times the least common multiple of the exponents in the minimal discriminant of E , cf. [31] VII.6.1). Note that the R -odd-primitivity condition is unaffected by this replacement of P by a multiple. By 2.12, $\{C_*\}$ is an odd divisibility sequence.

It follows from the definition of C_n that

$$(3.5.1) \quad C_N = \pm y_N \sqrt{x_N} \left(\frac{B_N^2}{A_N} \right)^2.$$

We claim that our assumption that b is squarefree implies the following:

3.5.2 Claim. *If $v(C_N) \neq 0$, then $v(C_N) = v(y_N \sqrt{x_N})$.*

Proof of the claim. By the above formula we should prove $v(B_N^2/A_N) = 0$. Now B_N and C_N are coprime by definition, and by 2.9 (i) and since b is squarefree, we find that A_N and C_N are also coprime.

Proof of \Rightarrow . Assume $m|n$. Then either n/m or $(n+m)/m$ is odd. Then lemma 2.12 implies that $C_m|C_n$ or $C_m|C_{m+n}$. We will agree from now on to write n but mean either n or $m+n$, and assume that n/m is odd.

Pick a valuation v in R and suppose that $v(y_m \sqrt{x_m})$ is odd. From formula (3.5.1), we see that $v(C_m)$ has to be odd. Since n/m is odd, lemma 2.12 implies that $v(C_n) \geq v(C_m) > 0$. By (3.5.2), we find $v(y_n \sqrt{x_n}) \geq v(y_m \sqrt{x_m}) > 0$ and this implies $\mathcal{D}_R(y_m \sqrt{x_m}, y_n \sqrt{x_n})$.

Proof of \Leftarrow . Choose a valuation v that belongs to an odd order primitive divisor of C_m from R . Then claim (3.5.2) implies that $v(y_m \sqrt{x_m})$ is positive and odd. The assumption means that $2v(y_n \sqrt{x_n}) > v(y_m \sqrt{x_m}) > 0$ (or similarly with n replaced by $m+n$). Formula (3.5.1) implies that one of the following two cases has to occur: $v(C_n) > 0$ or $v(A_n) > 0$. In the first case, since v is primitive for C_m , we find that $m|n$ from Lemma 3.2. In the second case, note that A_n divides B_{2n} (2.9(ii)), so B_{2n} and C_m have a common divisor v . We will prove that v is a primitive divisor of B_{2m} . Since $v(B_{2n}) > 0$, we will find from this that $m|n$.

By 2.9 (ii), we have an identity

$$(3.5.3) \quad C_m = \frac{B_{2m}}{2A_m B_m}.$$

Should $v(B_m) > 0$, then $v(B_{2m}) = v(B_m) + v(2)$, and hence (as A_m and B_m are coprime) $v(C_m) = 0$, a contradiction. Hence

$$(3.5.4) \quad v(B_m) = 0 \text{ and } v(B_{2m}) > v(2A_m).$$

Since v is primitive for C_m , we have $v(C_i) = 0$ if $i|m$, $i < m$. Recall $v(B_m) = 0$, and since $\{B_*\}$ is a divisibility sequence, $v(B_i) = 0$ for all i as before. Hence for such i , we find from (3.5.3):

$$(3.5.5) \quad i|m, i < m \Rightarrow v(B_{2i}) = v(2A_i).$$

Suppose that m/i is odd. Since $\{A_*\}$ forms an odd divisibility sequence (by 2.12), should $v(A_i) > 0$, then $v(A_m) > 0$. But since we assume b squarefree, A_m and C_m are coprime, so we cannot have $v(A_m) > 0$ and $v(C_m) > 0$. Hence $v(A_i) = 0$ for all v and so by (3.5.5), $v(B_{2i}) = 0$ for all $i|m$, unless $v = v_2$. For $v = v_2$, we find instead that $v(B_{2i}) = v(2A_i) = 1$, and hence $v(B_{2m}) = v(B_{\frac{m}{2} \cdot 2i}) = v(B_{2i}) = 1$ by the formal group law, since m/i is odd. But since $v(C_m) > 0$, we have $v(B_{2m}) > 1$ from (3.5.3). This is a contradiction.

For the general case (m/i not odd), write $m/i = 2^l \cdot k$ with k odd. We conclude from the previous reasoning that $v(B_{2^{l+1}i}) = 0$, but since $\{B_*\}$ forms a divisibility sequence, we find from this that also $v(B_{2i}) = 0$.

Recall that $v(B_m) = 0$ and hence $v(B_i) = 0$ for all $i|m$. We conclude from this and $v(B_{2i}) = 0$ that v is also primitive for B_{2m} . But remember we had $v(B_{2n}) > 0$. Hence $2m|2n$. \square

3.6 Remarks. (i) It might be possible to remove the assumption that b or $a^2 - 4b$ be squarefree, but then (3.5.2) changes.

(ii) We work with $\{C_*\}$ because C_n is an algebraic function of the coordinates of nP “up to squares” (3.5.1). It has been suggested in the past that $m|n$ is equivalent to $\mathcal{D}_R(\sqrt{x_m}, \sqrt{x_n})$, but this is wrong in two ways: if n/m is even, then “zeros” of x_m are not zeros of x_n ; and in general, “poles” of x_m are “poles” of x_n of larger order (in particular, if n/m is divisible by that pole). In case of an isotrivial elliptic curve over a rational function field, this problem doesn’t occur ([23], esp. 2.2), since the order stays equal.

Not to obscure the proof too much, we have not included the following stronger statement in the original statement of the theorem:

3.7 Proposition/Definition. *The conclusion of the above theorem 3.5 still holds if one replaces the R -odd-primitivity condition of $\{C_*\}$ by the following weaker condition:*

(“**weak** R -odd-primitivity condition”) *All terms $C_{2^a p^b}$ for a, b positive integers and p any odd prime have a primitive odd order divisor from R .*

Proof. The only part of the proof that changes is the proof of \Leftarrow . Set $a = v_2(m)$. If p is an odd prime such that $v_p(m) = b > 0$, choose a primitive odd divisor v for $C_{2^a p^b}$ from R based on the assumption. Since $m/2^a p^b$ is odd, lemma 2.12 implies that $v(C_m)$ is odd, so the assumption of the theorem assures us that $v(C_n) > 0$. We can then proceed as before with m

replaced by $2^a p^b$ to conclude $2^a p^b | n$. Since this holds for any odd p , we find $m | n$. \square

We now suggest the following conjecture about the sequences $\{C_*\}$:

3.8 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 and $a^2 - 4b$ squarefree;*

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

(c) *a set R of prime numbers such that \mathcal{D}_R is diophantine over \mathbf{Q} ; and such that $\{C_*\}$ is (weakly) R -odd-primitive.*

3.9 Theorem. *Assume Conjecture 3.8. Then $(\mathbf{Z}, +, |)$ has a three-dimensional diophantine model in \mathbf{Q} .*

Proof. Immediate from 2.2, 3.5 and 3.7, observing that $a = \pm y_n \sqrt{x_n}$ for $(x_n, y_n) \in T_r$ is diophantine over \mathbf{Q} . \square

3.10 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.*

Proof. The crucial statement is Siegel's theorem on integral points on an elliptic curve (cf. [31], IX 3.3), which implies that A_n and B_n are both of order of magnitude the height of nP .

For B_* , (i) is the usual elliptic Zsigmondy's theorem, first proven by Silverman in [32], Lemma 9. The same proof works for the sequence $\{A_*\}$; we include a variation of the proof for completeness.

Suppose that A_n doesn't have a primitive divisor. We will show that n is absolutely bounded, so changing P to some multiple, we get the result. We claim that there exists a set W of distinct divisors d of n with all $d > 1$ such that

$$A_n | n \prod_{d \in W} A_{\frac{n}{d}}.$$

We can then finish the proof as follows: We get

$$\log |A_n| \leq \log n + \sum_{d \in W} \log |A_{\frac{n}{d}}|.$$

Let m denote the canonical height of P . Classical height estimates give $\log |A_{\frac{n}{d}}| \leq (\frac{n}{d})^2 m + O(1)$. They combine with Siegel's theorem (“ $|A_n|$ and $|B_n|$ are of the same size”) to give for any $\varepsilon > 0$, $(1 - \varepsilon)n^2 m \leq \log |A_n|$. Since

$$\sum_{d \in W} \frac{1}{d^2} < \zeta(2) - 1 \text{ (recall: } d > 1 \text{ for } d \in W),$$

we find after insertion of these estimates into the above formula:

$$(2 - \varepsilon - \zeta(2))mn^2 \leq \log(n) + O(1),$$

and this bounds n absolutely.

For the proof of the claim: by assumption, any prime p dividing A_n divides A_m for some $m < n$. Then also $p|A_{(m,n)}$ (as in the proof of 3.2), so we can assume $m|n$ and n/m odd. Hence $v_p(A_n) = v_p(A_m) + v_p(n/m)$ (2.12 (iii)). Run through all p in this way, and pick such an m for each p . If $v_p(A_n) = v_p(A_m)$, then let $d := n/m \in W$. Then $v_p(A_n) = v_p(A_{\frac{n}{d}})$. If, on the other hand, $v_p(A_n) > v_p(A_m)$, then we must have $p|\frac{n}{m}$. In this case, set $d := p \in W$. Then $v_p(A_n) = v_p(A_{\frac{n}{d}}) + 1$. Indeed, we only have to prove that $v_p(A_{\frac{n}{d}}) > 0$ since we get the implication by the formal group law formula as p is odd. Now since $v_p(A_m) > 0$ and n/mp is an odd integer, the same formula implies that $v_p(A_{\frac{n}{p}}) = v_p(A_m) + v_p(\frac{n}{mp}) > 0$, and we are done.

To finish the proof of the proposition, the statement is true for C_* , since it is the A_* -sequence of the isogenous curve E' (as observed before). We note that (iii) for $\{B_*\}$ is Lemma 13 in [32], and a similar argument works for $\{C_*\}$. \square

3.11 Remarks. (i) We don't know whether \mathcal{D}_R for R the full set of valuations is diophantine over \mathbf{Q} . This would be quite a strong statement. For example, if we write a rational number x as $x = x_0 \cdot x_1^2$ with for any $v \in R$ such that $v(x_0) \neq 0$, one has $v(x_0)$ odd and $v(x_1) = 0$, then $\mathcal{D}_R(x^{-1}, 1)$ expresses that x_0 is an integer.

(ii) Using elliptic Zsigmondy and a proof similar to (but easier than) that of theorem 3.5, one can prove that $m|n \iff B_m|B_n \iff \text{rad}(B_m)|B_n$. However, we don't know that the formula $\mathcal{F}(x, y) : (\forall v)(v(x) < 0 \implies v(y) < 0)$ is equivalent to a diophantine formula $\mathcal{D}'(x, y)$ in \mathbf{Q} . If so, then $\mathcal{D}'(x_m, x_n)$ would be a diophantine definition of $m|n$ in \mathbf{Q} . But then again, “ $\mathcal{D}'(x, 1)$ ” would be a diophantine definition of \mathbf{Z} in \mathbf{Q} .

3.12 A diophantine predicate. We will now investigate in how far one can construct sets R for which \mathcal{D}_R is diophantine over \mathbf{Q} . In [23], Pheidas has produced a diophantine definition over \mathbf{Q} that says of two rational

numbers x and y that for any prime $p = 3 \pmod 4$, we have $v_p(x) > v_p(y^2)$ (and some extra conditions). This was consequently extended to all primes inert in a given quadratic extension of \mathbf{Q} by Van Geel and Zahidi at Oberwolfach ([34]), but still involving extra conditions. Finally, Demeyer and Van Geel have proven the following (for an arbitrary extension of global fields, but we only state it for \mathbf{Q}):

3.13 Proposition. ([11]) *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., $t(\mathcal{D}_{R_d}) = 0$.*

3.14 Remarks. The proof involves the theory of quadratic forms and is very close in spirit to the proof of Pheidias, which in its turn is an attempt to analyse Julia Robinson's definition \mathcal{R} from the following perspective: \mathcal{R} is essentially a conjunction over all valuations v of a predicate that says that a rational number x is v -integral. The latter is expressed by the isotropy of a quaternary quadratic form that depends on x and v . Pheidias' analysis says that one can discard this conjunction over an infinite set of primes (but not all). It would be interesting to see whether \mathcal{D}_R is diophantine for other sets of primes R that are inert in not necessarily quadratic extensions of \mathbf{Q} . Note that one can define $v(x) \geq 0$ for all v not completely split in a cyclic extension of \mathbf{Q} of degree q (with finitely many exceptions on v), but for $x \in \mathbf{Z}[T^{-1}]$ where T is the complement of finitely many primes, instead of $x \in \mathbf{Q}$ (Shlapentokh [30], 4.4.6).

3.15 Corollary. *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.

Proof. The first claim is automatic, since a finite disjunction of Σ_1^+ -formulae is equivalent to a Σ_1^+ -formula. For the second statement, choose all $\mathbf{Q}(\sqrt{d})$ for $d \in D$ linearly disjoint, then R_D is the complement of the set of primes that split completely in the compositum L of all $\mathbf{Q}(\sqrt{d})$ for $d \in D$, and this complement has Dirichlet density $1/|L| = 1/2^{|D|}$ (by Chebotarev's or weaker density theorems), which can be made arbitrary small $\neq 0$ by increasing $|D|$. \square

Based on this information, we change our conjecture to the following, the plausibility of which will be discussed in another section, and that will be used here as input for our main theorem.

3.16 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.

As before, we get:

3.17 Theorem. *Assume Conjecture 3.16. Then $(\mathbf{Z}, +, |)$ has a diophantine model in \mathbf{Q} . \square*

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

4.1 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. The first part of the proof is very similar to that of Lipshitz for \mathbf{N} in [20]. To define multiplication by a Σ_3^+ -formula, it suffices to define squaring by a Π_2^+ -formula, since $x = mn \iff 2x = (m+n)^2 - m^2 - n^2$ (translating this as $(\exists u, v, w, s)(x + x + u + v = w \wedge u = m^2 \wedge v = n^2 \wedge w = s^2 \wedge s = m + n)$).

We first claim that $y = x^2$ if and only if $(\forall t)(\phi(x, y, t))$, where ϕ is the formula

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

Indeed, the first three divisibilities imply $y = ux$ with $u \in \mathbf{Z}$ and $|x + 1| \leq |u + 1|$ and $|x - 1| \leq |u - 1|$. Taking $t = x^2$, the divisibilities following the implication sign imply $|x + 1| \geq |u + 1|$ and $|x - 1| \geq |u - 1|$. Hence $x + 1 = \pm(u + 1)$ and $x - 1 = \pm(u - 1)$. If in either of the two equalities, the equality holds with a positive sign we get that $u = x$ and hence $y = x^2$. The case $x - 1 = -u + 1$ and $x + 1 = -u - 1$ leads to a contradiction. The other direction is easy.

Rewriting the formula ϕ as an atomic formula using the recipe from Lemma 1.2, we see that the replacement of the implication in ϕ by disjunction introduces (non-positive) expressions of the form “ a does not divide b ”. We will now show how to replace this by a positive existential statement in $(\mathbf{Z}, +, |, \neq)$.

Observe that g is a greatest common divisor of a and b in \mathbf{Z} (notation: $(g) = (a, b)$) if and only if

$$(4.1.1) \quad g|a \wedge g|b \wedge (\exists x, y)(a|x \wedge b|y \wedge g = x + y).$$

Indeed, the first two divisibilities imply an inclusion of ideals $(a, b) \subseteq (g)$, and the existential statement implies that $g \in (a, b)$.

Now a doesn't divide b if and only if $(a) \neq (a, b)$, and this can be rewritten as

$$(\exists g, g')((g) = (a, b) \wedge g + g' = 0 \wedge a \neq g \wedge a \neq g'),$$

which is a positive existential formula in $(\mathbf{Z}, +, |, \neq)$, after substitution of (4.1.1). \square

4.2 Theorem. *Assume Conjecture 3.8 or 3.16. Then \mathbf{Z} has a model D in \mathbf{Q} with complexity $t(D) \leq 1$, $c(D) \leq 1$; and the Σ_3^+ -theory (= Σ_3 -theory) of \mathbf{Q} is undecidable.*

Proof. Picking an elliptic curve as in one of the conjectures, we find a three-dimensional diophantine model of $(\mathbf{Z}, +, |)$ in $(\mathbf{Q}, +, \times)$ as in Theorem 3.9 or 3.17. Now observe that 0 is also definable in the model by an atomic formula, and that $n \neq 0$ is also definable in the model by an existential formula, cf. Lemma 2.2. Hence each of the conjectures actually imply that $(\mathbf{Z}, +, |, 0, \neq)$ is definable in \mathbf{Q} .

Now \times is defined by a Σ_3^+ -formula in $(\mathbf{Z}, +, |, \neq)$ with only one universal quantifier; in particular, $t(\iota(\times)) \leq 1$ and $c(\iota(\times)) \leq 1$ for the induced model D of \mathbf{Z} in \mathbf{Q} . By 1.22, we conclude that $t(D) \leq 1$, $c(D) \leq 1$ and that the Σ_3^+ -theory of \mathbf{Q} is undecidable. \square

4.3 Remark. The trick of replacing non-divisibilities by existential sentences in the lemma (communicated to us by Pheidias) is crucial. The negation of a diophantine formula expressing divisibility (as it comes out of our conjecture) is a universal formula that leads to a model of the same complexity as Julia Robinson's.

5. Conditional undecidability of the Π_2^+ -theory of \mathbf{Q}

Theorem 4.2 is our main result about the complexity of a model of \mathbf{Z} in \mathbf{Q} . Although the model given there is Σ_3^+ , we can slightly alter the method to (conditionally) prove the existence of undecidable formulæ in \mathbf{Q} of complexity Π_2^+ .

5.1 Lemma. *The Π_2^+ -theory of $(\mathbf{Z}, +, |)$ is undecidable.*

Proof. The proof is entirely analogous to that for \mathbf{N} by Lipshitz in [20]. By Lemma 4.1, we know that squaring is definable in $(\mathbf{Z}, +, |)$ by a Π_2^+ -formula. The proof of 4.1 actually shows that if one allows negated divisibilities, the defining formula can be taken to be a Π_1 -formula. It is easily seen that the Σ_1^+ -theory of the structure $(\mathbf{Z}, +, x \rightarrow x^2)$ is undecidable (since multiplication is existentially definable). We obtain that the Σ_2 -theory of $(\mathbf{Z}, +, |)$ is undecidable. Since the negation of a Σ_2 -formula is a Π_2 -formula, we obtain that the Π_2 -theory of $(\mathbf{Z}, +, |)$ is undecidable. This means that sentences of the form:

$$\forall \mathbf{x} \exists \mathbf{y} \phi(\mathbf{x}, \mathbf{y})$$

(with ϕ quantifier free) are undecidable. However ϕ may still contain negated divisibilities and inequations. These can be eliminated as in the proof of 4.1 at the expense of introducing extra existential quantifiers. Thus, any Π_2 -sentence is equivalent to a Π_2^+ -sentence and hence the Π_2^+ -theory of $(\mathbf{Z}, +, |)$ is undecidable. \square

We now need the following extension of Lemma 1.20:

5.2 Proposition. *Let (D, ι) be a diophantine model of $(\mathbf{Z}, +, |)$ in $(\mathbf{Q}, +, \times)$, such that membership of D is quantifier-free. In the following table, the second column lists the positive hierarchical status of the formula $\iota(\mathcal{F})$ as a function of the status of \mathcal{F} :*

\mathcal{F}	$\iota(\mathcal{F})$
Σ_{2n}^+	Σ_{2n+1}^+
Σ_{2n+1}^+	Σ_{2n+1}^+
$\Pi_{2n}^+ (n > 0)$	Π_{2n}^+
Π_{2n+1}^+	Π_{2n+2}^+

(note: inclusion of a formula in a class of the hierarchy means that the formula is equivalent to a formula in that class).

Proof. The proof is completely analogous to the proof 1.20. \square

5.3 Theorem. *Assume Conjecture 3.8 or 3.16. Then the Π_2^+ -theory of \mathbf{Q} is undecidable. Furthermore the subset of sentences of Π_2^+ with t -complexity 1 is already undecidable.*

Proof. Follows immediately from 3.9, 3.17, 5.1 and 5.2. \square

6. Discussion of the conjecture

6.1 Different versions of the conjecture. Our conjecture is merely about the existence of *one* elliptic curve, but one can of course also investigate whether the conjecture might be true for any elliptic curve E with a point of infinite order on it. The conjecture then becomes a kind of elliptic Zsigmondy conjecture with odd order and inertial conditions. It then seems natural to also look at the conjecture for $\{B_*\}$ instead of $\{C_*\}$, although we don't know of a direct application to logic. We now first list these variants of the conjecture in a more precise way:

6.2 (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 (weakly) R_D -(odd-)primitive for some D .*

6.3 (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 (weakly) R_D -(odd-)primitive for some D .*

It is hard to falsify these conjectures, because if one finds a multiple of a given point P for which the divisibility sequences under consideration has no primitive odd order divisor from a given R_D , one simply takes a multiple of P or enlarges the set of discriminants. But if the height of P becomes too large, one can no longer factor B_n or C_n in reasonable time with existing algorithms, and if the height of P is too small, then B_n or C_n could be non-typical (e.g., prime) for small n (similar problems occur in [12]). We will therefore refrain from presenting extensive numerical computation, but rather present some heuristics and remarks below, and a density version of the conjecture in the next section.

6.4 Heuristic arguments.

We start from the following observation:

(6.4.1) (Landau-Serre [27] 2.8) *Let M be a multiplicative set of positive non-zero integers (i.e., $xy \in M \iff x \in M \vee y \in M$), and assume that the set of prime numbers in M is Frobenian with density $\delta > 0$ (i.e., every sufficiently large prime p belongs to M exactly if its Frobenius morphism belongs to a fixed subset H of the Galois group G of some fixed number field with H stable under conjugation by G and $\delta = |H|/|G|$). Then the probability that a given number x belongs to the complement of M 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 .

We can now “prove” heuristically:

(6.4.2) *Let E be an elliptic curve over \mathbf{Q} . Then set $A = E(\mathbf{Q}) - E(\mathbf{Z}[\frac{1}{R_D}])$ of points whose denominators are only divisible by primes outside R_D is heuristically finite if $|D|$ is large enough.*

Let M denote the set of integers having at least one factor from R_D . Then M is multiplicative, and a prime p belongs to M exactly if p is not completely split in the compositum $L = \mathbf{Q}(\sqrt{d_1}, \dots, \sqrt{d_N})$, where $D = \{d_1, \dots, d_N\}$. This is the same as saying that the Frobenius element of p belongs to $H = \text{Gal}(L/\mathbf{Q}) - \{1\}$. Note that H is stable under conjugation, and that $\delta := |G|/|H| = 1 - 1/2^N > 0$.

We approximate the probability that a number is outside M by the first order term in (6.4.1) — in the considerations below, any finite order truncation actually gives the same result. We consider the set

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

We find for large x ,

$$|A_x| \approx \sum_{\substack{P \in E(\mathbf{Q}) \\ \hat{h}(P) \leq x}} \hat{h}(P)^{-\delta}.$$

We now pick a basis $\{P_i\}_{i=1}^r$ for the free part of $E(\mathbf{Q})$ and write any $P \in E(\mathbf{Q})$ as $\sum \lambda_i P_i + T$ with $\lambda_i \in \mathbf{Z}$ and $T \in E(\mathbf{Q})_{\text{tor}}$. Then $\hat{h}(P) \approx \|\lambda\|^2 \cdot \log c$ for some constant c , and the above sum becomes

$$|A_x| \approx \sum_{\substack{\lambda \in \mathbf{Z}^r - \{0\} \\ \|\lambda\|^2 \leq x}} \|\lambda\|^{-2\delta}.$$

We group terms with $\|\lambda\| = m$ for a fixed integer m :

$$|A_x| \approx \sum_{m=1}^{\sqrt{x}} m^{r-1} \cdot m^{-2\delta}.$$

We let $x \rightarrow \infty$, and find that A is finite if this sum converges, which happens exactly for $2\delta - r + 1 > 1$, i.e., $\delta > r/2$. This can be attained for N sufficiently large. \square

With $r = 1$, this implies that B_n doesn't have a divisor in R_D only for finitely many n as soon as $|D| \geq 2$. Applying it to the isogenous curve E' , it implies the same for $\{A_*\}$ and hence $\{C_*\}$.

Actually, the primitive part of B_n is of size at least $\hat{h}(P)^{0.6 \cdot n^2}$ (cf. Silverman [32], Lemma 9 for an estimate $\hat{h}(P)^{n^2/3}$ and [33] for a proof with a factor 0.6, using elliptic transcendence theory). We can apply the same argument to the primitive part of B_n . Furthermore, taking the ABC -conjecture for granted, if E has j -invariant 0 or 1728, then we even know that the squarefree primitive part of B_n is of the same order (Lemma 13 in loc. cit.), and this gives a heuristical proof of R_D -odd-primitivity for $|D| \geq 2$ on such curves.

(6.4.3) One might note the following about the error term in (6.4.1): Shanks [28] analysed (6.4.1) in case M is the complement of the set of sums of two squares (cf. Ramanujan's first letter to Hardy) and noted that the first two terms give an accuracy of only 0.005 at $x = 10^7$.

(6.4.4) Note further that for E having a rational 2-torsion point, B_n can be prime only finitely often, as follows from [13] (since it arises as image sequence under an isogeny). It is actually conjectured (see loc. cit.) that B_n can only be prime for $n \leq K$ and some constant K independent of E and P ; this is related to the elliptic Lehmer problem. It is reasonable to expect that B_n has m distinct odd order primitive prime factors as soon as $n \geq K$ for some constant K only depending on P and E and m (and maybe even only m). Granting that the (many) prime factors of B_n are equidistributed over residue classes, the probability that at least one of the them is inert in a given $\mathbf{Q}(\sqrt{d})$ is very high.

6.5 Further remarks. (i) One can wonder whether the property of being R_D -primitive is very sensitive to the choice of D , so ask whether it is true that *for every elliptic curve E (respectively, such that $(0, 0) \in E[2]$) and every non-empty set D of discriminants, for every rational point P of infinite order and sufficiently large height, B_n (respectively C_n) satisfies the R_D -primitivity condition.* There is some evidence that the R_D -primitive part doesn't behave the same for all D . For example, if E has complex multiplication by some $d \in D$, there appear to be "more" split primes. This is explained by a Zsigmondy's theorem for an interpolation of the usual elliptic divisibility sequence by a sequence indexed by all endomorphisms of

the curve, see Streng [33]. Another example is Rubin’s proof in 2.14.

(ii) It is interesting to observe that the multiplicative group (disguised as the Fibonacci sequence) played an essential rôle in the original proof of HTP(\mathbf{Z}). However, the analogue of our conjectures for linear recurrent sequences or the multiplicative group, i.e., an “inertial classical Zsigmondy’s theorem”, is almost certainly false. Let us reason heuristically for the sequence $\{a^n - 1\}_{n \geq 1}$ for fixed a . The probability that $a^n - 1$ is divisible only by primes outside R_D is $[\log(a^n - 1)]^{-\delta}$ with $\delta = 1 - 1/2^{|D|}$ (cf. (6.4.1)), so the number of $n \leq x$ for which this holds is approximately

$$\sum_{n \leq x} \log[(a^n - 1)]^{-\delta} \approx \sum_{n \leq x} n^{-\delta}$$

which diverges if $x \rightarrow \infty$ for all δ . Also, a general term of such a sequence (if a is not composite) can be prime infinitely often. This is why we really need elliptic curves.

(iii) It is easy to formulate an analogue of the above conjecture for elliptic curves over global function fields. Especially in the case of an isotrivial curve (e.g., the “Manin-Denef curve” $f(t)y^2 = f(x)$), some information can be found in the literature, cf. [23].

Another function field analogue of 6.3 is the following: let ϕ be a rank-2 $\mathbf{F}_q[T]$ -Drinfeld module over $\mathbf{F}_q(T)$ (see, e.g. [15]). If $x \in \mathbf{F}_q[T]$ is a polynomial of sufficiently large degree with $\phi_a(x) \neq 0$ for all $a \in \mathbf{F}_q[T]$, then for all polynomials n , $\phi_n(x)$ is divisible by an irreducible polynomial \wp coprime to $\phi_m(x)$ for all m of degree $\deg(m) < \deg(n)$, such that \wp is inert in at least one of $\mathbf{F}(T)(\sqrt{d})$ for d in a finite set of polynomials. A Drinfeld module analogue of Zsigmondy’s theorem was proven by Hsia ([16]).

(iv) The weaker statement that every C_n/C_1 has an odd order divisor from R_d , but not necessarily primitive, is equivalent to the fact that each of the “fibrations in conics over E ”

$$C/C_1 = f(X, Y) \wedge C^2 = A^4 + aA^2B^2 + bB^4$$

has only finitely many rational (\mathbf{P}^1 -)fibres over E , where f runs over the classes of binary quadratic forms of the correct discriminant. For example, since $\mathbf{Q}(\sqrt{5})$ has class number one, related to example 2.14 is the diophantine equation

$$(A^2 + B^2)(A^2 + 11B^2) = 3^2 \cdot 5^2 \cdot (X^2 - 5Y^2)^2,$$

a smooth projective K3-surface whose rational points should be found. One is reminded of the trouble deciding whether or not Martin Davis’s equa-

tion has finitely many solutions (cf. Shanks and Wagstaff [29], again using Landau-Serre type estimates).

(v) In conjecture 6.3, one can move the point P to $(0, 0)$ by a rational change of coordinates. Then the conjecture becomes purely a statement about the division points on E , as we then have

$$B_n^2 = \pm n^2 \prod_{Q \in E[n]} x(Q).$$

(vi) If E has complex multiplication, then one has a divisibility sequence $\{B_\alpha\}$ associated to any $\alpha \in \text{End}(E)$ (cf. [5]). A similar theory with similar conjectures can be worked out. For the analogue of Zsigmondy's theorem, see [33].

7. A density version of the conjecture.

7.1 Periodicity technique. There is a principle of periodicity of elliptic divisibility sequences that can be used to prove density versions of the conjectures. Here is an example for Conjecture 6.3: the point $P = (-2, 4)$ is non-singular modulo all primes and of infinite order on the curve $E : y^2 = x^3 + 7x^2 + 2x$. The sequence $\{B_*\}$ for P starts as $(1, 2^2, 3 \cdot 11, 2^3 \cdot 5^2, \dots)$ up to signs.

7.2 Definition. The rank of apparition $\rho_p = \rho_p(X_*)$ of a prime p in a sequence $\{X_*\}$ is the smallest n for which $p|X_n$.

7.3 Periodicity (Morgan Ward [35], section III). Assume that the sign of B_n is chosen so that $B_n = \psi_n(P)$ for the classical division polynomial ψ_n . Assume $p > 3$ has rank of apparition $\rho_p > 3$ in $\{B_*\}$. Then that sequence is periodic with period π_p given by

$$\pi_p = \rho_p \cdot 2^{a_p} \cdot \tau_p,$$

where τ_p is the least common multiple of the (multiplicative) orders ϵ and κ of B_{ρ_p-1} and B_{ρ_p-2}/B_2 modulo p , respectively; and where $a_p = 1$ if both ϵ and κ are odd, $a_p = -1$ if both ϵ and κ are divisible by the same power of 2, and $a_p = 0$ otherwise.

We now look at the behaviour of the Jacobi symbol of B_* modulo a given prime p . To avoid sign problems, we choose $p = 1 \pmod{4}$. For example, our sequence is periodic modulo 5 with period 8. Hence the sequence of Jacobi symbols $(\frac{5}{B_n}) = (\frac{B_n}{5})$ (by quadratic reciprocity) is periodic with the same

period, and its repeats

$$(1, 1, -1, 0, -1, 1, 1, 0) \pmod{5}.$$

This implies that $\left(\frac{5}{B_n}\right) = -1$ whenever $n = \pm 3 \pmod{8}$, so all B_s for s a prime congruent to $\pm 3 \pmod{8}$ have a primitive odd order divisor in R_5 .

In this case, one can do a little better. Assume $n = s^e$ is a power of a prime $s = \pm 3 \pmod{8}$. Then for e even, $s^e = 1 \pmod{8}$ and $s^{e-1} = \pm 3 \pmod{8}$, whereas for e odd, we have $s^e = \pm 3 \pmod{8}$ and $s^{e-1} = 1 \pmod{8}$. From periodicity, we see that in any case the Jacobi symbol of $B_{s^e}/B_{s^{e-1}}$ is -1 , so the number is divisible by an odd order divisor in R_5 . We conclude:

7.4 Proposition. *If $\{B_*\}$ is the elliptic divisibility sequence associated to $(2, -4)$ on $y^2 = x^3 + 7x^2 + 2x$, then any B_{s^e} for s a prime number $= \pm 3 \pmod{8}$ has a primitive odd order divisor from R_5 . In particular, the set $\{s \text{ prime} : B_s \text{ has a primitive odd order divisor from } R_5\}$ has Dirichlet density at least $2/\varphi(8) = 1/2$. \square*

One can go on and create a race between inertial conditions in different $\mathbf{Q}(\sqrt{p})$ and the period of $\{B_*\}$ modulo p . We do this for the first few $p = 1 \pmod{5}$ and the above curve and point (leaving out the easy computations). For $p = 13$, the sequence has period 36 and for $s = \pm 5, 7, 11, 13 \pmod{36}$, $\left(\frac{B_s}{13}\right) = -1$. For $p = 17$, all Kronecker symbols are positive. For $p = 29$, the period is 38, and $s = \pm 9, 11, 15 \pmod{38}$ give a negative Kronecker symbol. For $p = 37$, no new residue classes occur. For $p = 41$, the period is 42, and $s = \pm 13, 17 \pmod{42}$ have negative Kronecker symbol. For 53, the period is 66 and $s = \pm 5, 7, 25, 29 \pmod{66}$ have negative Kronecker symbol. An easy density computation gives:

7.5 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 $43/45 \geq 95.5\%$. \square

7.6 Remark. It is an interesting question whether, given any elliptic divisibility sequence B_* , and $\varepsilon > 0$, one can choose a set D such that

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

has density at least $1 - \varepsilon$.

References

- [1] Mohamed Ayad. Points S -entiers des courbes elliptiques. *Manuscripta Math.*, 76(3-4):305–324, 1992.
- [2] A.P. Bel'tjukov, Decidability of the universal theory of natural numbers with addition and divisibility. Studies in constructive mathematics and mathematical logic, VII. Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 60:15–28, 1976.
- [3] C. C. Chang and H. J. Keisler. *Model theory*. North-Holland Publishing Co., Amsterdam, 1973. Studies in Logic and the Foundations of Mathematics, Vol. 73.
- [4] J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. *Manuscripta Math.*, 97(3):319–328, 1998.
- [5] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7(4):385–434, 1986.
- [6] René Cori and Daniel Lascar. *Mathematical logic, Part I*. Oxford University Press, Oxford, 2000.
- [7] Gunther Cornelissen. Stockage diophantien et hypothèse abc généralisée. *C. R. Acad. Sci. Paris*, 328(Ser.I), 3–8, 1999.
- [8] Gunther Cornelissen. Elliptic curves and rational diophantine models of integer divisibility; Elliptic curves and divisibility. Unpublished manuscripts, 2000.
- [9] Gunther Cornelissen and Karim Zahidi. Topology of Diophantine sets: remarks on Mazur's conjectures. In *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, volume 270 of *Contemp. Math.*, pages 253–260. Amer. Math. Soc., Providence, RI, 2000.
- [10] Martin Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80:233–269, 1973.
- [11] Jeroen Demeyer and Jan Van Geel. An existential divisibility lemma for global fields. *Monatsh. Math.*, 147:293–308, 2006.
- [12] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.*, 4:1–13 (electronic), 2001.
- [13] Graham Everest, Victor Miller, and Nelson Stephens. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.*, 132(4):955–963, 2004.
- [14] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell. Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. *Math. Comp.*, 70(236):1675–1697 (electronic), 2001.
- [15] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebn. der Math. und ihrer Grenzgeb. (3)*. Springer-Verlag, Berlin, 1996.
- [16] L.-C. Hsia. On the reduction of a non-torsion point of a Drinfeld module, preprint (2002).
- [17] Leonard Lipshitz. Undecidable existential problems for addition and divisibility in algebraic number rings. II. *Proc. Amer. Math. Soc.*, 64(1):122–128, 1977.
- [18] Leonard Lipshitz. The Diophantine problem for addition and divisibility. *Trans. Amer. Math. Soc.*, 235:271–283, 1978.

- [19] Leonard Lipshitz. Undecidable existential problems for addition and divisibility in algebraic number rings. *Trans. Amer. Math. Soc.*, 241:121–128, 1978.
- [20] Leonard Lipshitz. Some remarks on the Diophantine problem for addition and divisibility. Proceedings of the Model Theory Meeting (Brussels/Mons, 1980). *Bull. Soc. Math. Belg. Sér. B* 33:41–52, 1981.
- [21] Yuri V. Matiyasevic. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk S.S.S.R.* 191:279–282, 1970.
- [22] Yuri V. Matiyasevich. Hilbert’s tenth problem. Foundations of Computing Series. MIT Press, Cambridge, MA, 1993.
- [23] Thanases Pheidas. An effort to prove that the existential theory of \mathbf{Q} is undecidable. In *Hilbert’s tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, volume 270 of *Contemp. Math.*, pages 237–252. Amer. Math. Soc., Providence, RI, 2000.
- [24] Bjorn Poonen. Hilbert’s tenth problem and Mazur’s conjecture for large subrings of \mathbf{Q} . *J. Amer. Math. Soc.*, 16(4):981–990, 2003.
- [25] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949.
- [26] Hartley Roger, Jr. Theory of Recursive Functions and Effective Computability. McGraw-Hill, 1967.
- [27] Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. *Enseignement Math. (2)*, 22(3-4):227–260, 1976.
- [28] Daniel Shanks. The second-order term in the asymptotic expansion of $B(x)$. *Math. Comp.*, 18:75–86, 1964.
- [29] Daniel Shanks and Samuel S. Wagstaff, Jr. 48 more solutions of Martin Davis’s quaternary quartic equation. *Math. Comp.*, 64:1717–1731, 1995.
- [30] Alexandra Shlapentokh. *Hilbert’s Tenth Problem: Diophantine Classes and Other Extensions to Global Fields*. Cambridge University Press, to appear.
- [31] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
- [32] Joseph H. Silverman. Wieferich’s criterion and the abc -conjecture. *J. Number Theory*, 30(2):226–237, 1988.
- [33] M. Streng. Elliptic divisibility sequences with complex multiplication. Master’s thesis, Utrecht University, 2006.
- [34] Jan Van Geel and Karim Zahidi. Quadratic forms and divisibility. In: Mathematisches Forschungsinstitut Oberwolfach Report nr. 3/2003 Mini-Workshop “Hilbert’s 10th Problem, Mazur’s conjecture and divisibility sequences”, p. 4, 2003.
- [35] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

Mathematisch Instituut, Universiteit Utrecht, Postbus 80010, 3508 TA Utrecht, Nederland
 Email: cornelissen@math.uu.nl

Departement Wiskunde, Statistiek en Actuarieat, Universiteit Antwerpen, Prinsstraat 13,
 2000 Antwerpen, België
 Email: zahidi@logique.jussieu.fr