ACTA ARITHMETICA
174.4 (2016)

Sets of recurrence as bases for the positive integers

by

Jakub Konieczny (Oxford)

Introduction. Let $p(n)$ be a real polynomial and let $\varepsilon(n) > 0$ be a slowly decaying function. We consider the sets

$$\mathcal{A} = \{n \in \mathbb{N} \mid \|p(n)\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon(n)\},$$

where $\|t\|_{\mathbb{R}/\mathbb{Z}} = \min_{n\in\mathbb{Z}} |t-n|$ denotes the distance to the nearest integer and $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Our particular concern will be the additive properties of such sets. Specifically, when is $\mathcal{A}$ a basis for $\mathbb{N}$ of a given finite order? That is, for which k, if any, is it true that the sumset

$$k\mathcal{A} = \mathcal{A} + \cdots + \mathcal{A} = \{n_1 + \cdots + n_k \mid n_i \in \mathcal{A}\}$$

contains all sufficiently large integers? We will also be interested in when $\mathcal{A}$ is an *almost* basis of order k, by which we mean that $k\mathcal{A}$ has asymptotic density 1. Here, the *asymptotic density* of a set $\mathcal{B}$ is defined as

$$\mathrm{d}(\mathcal{B}) = \lim_{n\to\infty} \frac{|\mathcal{B} \cap [n]|}{n},$$

provided that the limit exists. We use $[n]$ to denote the set $\{1, \ldots, n\}$.

We consider two types of behaviour of $\varepsilon(n)$: we either demand that $\varepsilon(n) \to 0$, or that $\varepsilon(n)$ is bounded pointwise by a suitably small constant ε_0 (in which case we may equally well assume that $\varepsilon(n) = \varepsilon_0$). This technical issue will appear at various points in the paper.

In the case when $\deg p = 1$, the problem is rather straightforward. We are then essentially dealing with Bohr sets, which are simple and well studied objects (see e.g. [8, Chapter 4.4]). We expect that the sets $k\mathcal{A}$ should not be significantly larger than $\mathcal{A}$, and hence that $\mathcal{A}$ should not be a basis of any order for sufficiently small ε.

2010 *Mathematics Subject Classification*: Primary 11J54; Secondary 11P99.
Key words and phrases: additive basis, set of recurrence, Nil-Bohr set, small fractional parts.
Received 30 March 2015; revised 23 December 2015.
Published online 12 July 2016.

DOI: 10.4064/aa8125-4-2016

It is an easy exercise to show that for any k the set

$$\mathcal{A} = \{n \in \mathbb{N} \mid \|\alpha n\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon(n)\}$$

is not a basis of order k provided that, say, $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and $\varepsilon(n) < 1/(3k)$ for all n. Indeed, this follows easily from the observation that $\|N\alpha\|_{\mathbb{R}/\mathbb{Z}} < 1/3$ for $N \in k\mathcal{A}$. Similarly, one can show that $\mathcal{A}$ defined above is not a basis of order k if $\varepsilon(n) \to 0$ as $n \to \infty$. We leave the details to the interested reader.

The problem is most interesting when $\deg p = 2$. One might expect $\mathcal{A}$ to behave roughly as a random set such that $n \in \mathcal{A}$ with probability $\varepsilon(n)$, and hence to be a basis of finite order if $\varepsilon(n)$ decays reasonably slowly. A particular case of this problem was considered by Erdős, who asked the following ([1]).

QUESTION 1. *Is the set* $\mathcal{A} = \{n \in \mathbb{N} \mid \|\sqrt{2}\, n^2\|_{\mathbb{R}/\mathbb{Z}} \leq 1/\log n\}$ *a basis of order* 2*?*

Somewhat unexpectedly, the answer to this question is negative. One can even produce an explicit sequence

$$N_i = \frac{(3+2\sqrt{2})^{2i+1} - (3-2\sqrt{2})^{2i+1}}{2\sqrt{2}}$$

such that $N_i \notin 2\mathcal{A}$ for all sufficiently large i.

Several other constructions of this type are possible, each leading to a sequence $N_i \notin 2\mathcal{A}$ with N_i growing exponentially with i. Hence, one may hope that the following weaker variant should have a positive answer. Recall that we call $\mathcal{A}$ an almost basis of order 2 if $\mathrm{d}(2\mathcal{A}) = 1$.

QUESTION 2. *Is the set* $\mathcal{A} = \{n \in \mathbb{N} \mid \|\sqrt{2}\, n^2\|_{\mathbb{R}/\mathbb{Z}} \leq 1/\log n\}$ *an almost basis of order* 2*?*

This is indeed the case. In fact, we can prove a stronger statement concerning the size of the complement $(2\mathcal{A})^c = \mathbb{N} \setminus 2\mathcal{A}$, namely $|[T] \setminus 2\mathcal{A}| \ll \log^C T$ as $T \to \infty$, where C is a constant.

Here and elsewhere, we use the Vinogradov notation $f \ll g$ or $f = O(g)$ to denote that $f \leq Cg$ for some constant C. When C depends on a parameter A, we write $f \ll_A g$ or $f = O_A(g)$. If $f = O(g)$ and $g = O(f)$, we write $f = \Theta(g)$.

In larger generality, we have the following collection of results.

THEOREM A. *Let* $\varepsilon(n)$ *be a slowly decaying function, let* $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ *and set*

$$\mathcal{A} = \{n \in \mathbb{N} \mid \|\alpha n^2\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon(n)\}.$$

Then:

([1]) Personal communication from Ben Green; no written reference could be located.

A1. *For any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\mathcal{A}$ is an almost basis of order 2 provided that $\varepsilon(n)$ decays slowly enough.*

A2. *For uncountably many exceptional values of α, $\mathcal{A}$ is a basis of order 2 provided that $\varepsilon(n)$ decays slowly enough.*

A3. *In particular, for any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\mathcal{A}$ is a basis of order 3 provided that $\varepsilon(n)$ decays slowly enough.*

A4. *However, for almost all α, $\mathcal{A}$ is not a basis of order 2 as long as $\varepsilon(n) \to 0$.*

Above, the phrase "provided that $\varepsilon(n)$ decays slowly enough" may be expanded into "there exists $\varepsilon_0(n) \to 0$ such that if $\varepsilon(n) \geq \varepsilon_0(n)$ for all n, then the statement holds", and "almost all" means "all except for a set of Lebesgue measure 0". We state the results in a more rigorous manner when we approach the proof.

We first address item **A4**, which was the original motivation for this research project. Because of **A2**, we cannot hope to obtain a result for all α, but we are able to cover a number of interesting cases, including Lebesgue almost all reals, as well as all quadratic surds. This is done in Section 1.

Items **A1** and **A2** are proved in Section 2. Our key idea is to translate information about the complement of $2\mathcal{A}$ into information about good rational appoximations of α. We are then able to use known equidistribution results as a black box, in order to show that if $(2\mathcal{A})^c$ had positive (upper asymptotic) density, then α would have too many good rational approximations. Item **A2** is proved by an explicit construction using continued fractions.

Item **A3** is an immediate consequence of **A1** (or, strictly speaking, the proof thereof). In fact, our argument implies that $2\mathcal{A} + \mathcal{B}$ contains all sufficiently large integers for any set $\mathcal{B}$ with at least two elements.

For polynomials p of degree ≥ 3, the situation becomes much simpler. The heuristic expectation that $\mathcal{A}$ should be a basis of order 2 is confirmed in this case, as long as we impose suitable genericity assumptions. Below we give a special case of our main result for polynomials of degree ≥ 3.

THEOREM B. *Let $d \geq 3$. Fix some slowly decaying function $\varepsilon(n)$, $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and set*

$$\mathcal{A} = \{n \in \mathbb{N} \mid \|\alpha n^d\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon(n)\}.$$

Then:

B1. *For almost all α, $\mathcal{A}$ is a basis of order 2 provided that $\varepsilon(n)$ decays slowly enough.*

B2. *Nevertheless, for uncountably many α, $\mathcal{A}$ is not a basis of order 2, even when $\varepsilon(n)$ is constant.*

In Section 3 we will establish a more general result in which the polynomial p varies in a linear family. The bulk of the difficulty lies in proving **B1**.

We rely on similar ideas to those for **A1**, and relate each element in the complement of $2\mathcal{A}$ to the lack of equidistribution of a certain polynomial sequence. Using a known result about distribution of polynomial sequences, we then connect lack of equidistribution with a system of approximate rational dependencies, which generically turn out not to be satisfiable.

For **B2**, it suffices to take α sufficiently well approximable by rationals, and we can construct such α explicitly.

1. Failure to be a basis of order 2. Our goal in this section is to prove that the sets

$$\mathcal{A}_\varepsilon^\alpha := \{n \in \mathbb{N} \mid \|\alpha n^2\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon(n)\} \tag{1.1}$$

are "usually" not bases of order 2, even when $\varepsilon(n) = \varepsilon_0$ is constant.

THEOREM (**A4**, reiterated). *There exists a set $Z \subset \mathbb{R}$ of Lebesgue measure 0 such that for any $\alpha \in \mathbb{R} \setminus Z$ and any $\varepsilon(n) \to 0$, the set $\mathcal{A}_\varepsilon^\alpha$ defined in* (1.1) *is not a basis of order 2. The same is true for $\alpha \in \mathbb{Q}[\sqrt{d}] \setminus \mathbb{Q}$, for any $d \in \mathbb{N}$.*

This result is somewhat surprising, because a random (unstructured) set of similar size should be a basis of order 2. In fact, if $\mathcal{A} \subset \mathbb{N}$ is constructed randomly with

$$\mathbb{P}(n \in \mathcal{A}) = \varepsilon,$$

independently for each n, then with high probability $2\mathcal{A}$ contains all integers larger than roughly $(1/\varepsilon^2)\log(1/\varepsilon)$.

We will prove a variety of partial results, with different restrictions on α and $\varepsilon(n)$, not all of which are included in Theorem **A4** as stated above. For α, we separately address the "structured" case when α is a quadratic surd or, more generally, is badly approximable, and the "generic" case when α is selected from a suitable set of full measure. For $\varepsilon(n)$, we assume that either $\varepsilon(n) \to 0$ as $n \to \infty$, or $\varepsilon(n) \le \varepsilon_0(\alpha)$ is bounded by a constant which is allowed to depend on α.

1.1. General strategy. We begin by introducing a somewhat technical tool which will allow us to detect large integers N in the complement of $2\mathcal{A}_\varepsilon^\alpha$. Importantly, we are able to reduce the task of proving that $N \notin 2\mathcal{A}_\varepsilon^\alpha$ to the task of verifying a simple Diophantine inequality.

The basic idea is quite simple. Suppose that we allowed α to take rational values, and take for instance $\alpha = 1/2$. Assuming that $\varepsilon(n) < 1/2$ for all n, the set $\mathcal{A}_\varepsilon^\alpha$ is far from being a basis of order 2. Indeed, we then have $\mathcal{A}_\varepsilon^\alpha = 2\mathbb{N}$, which is not a basis of any order.

The following lemma makes this observation quantitative. We will use it multiple times.

LEMMA 1.1. *Suppose that for an odd integer N, there are integers k, m, with k even and m odd, and a real parameter $\delta > 0$, such that*

$$\left\| N\alpha - \frac{m}{k} \right\|_{\mathbb{R}/\mathbb{Z}} < \frac{1-\delta}{kN}. \tag{1.2}$$

Then $N \notin 2\mathcal{A}_\varepsilon^\alpha$ for any pointwise bounded $\varepsilon(n) \le \varepsilon_0$, where $\varepsilon_0 = \delta/(2k)$.

Proof. Take γ with $|\gamma| < 1 - \delta$ so that

$$N\alpha \equiv \frac{m}{k} + \frac{\gamma}{kN} \pmod 1.$$

Consider any decomposition $N = n_1 + n_2$ with $n_1, n_2 \in \mathbb{N}$. Then

$$\begin{aligned} \|n_1^2\alpha - n_2^2\alpha\|_{\mathbb{R}/\mathbb{Z}} &= \|(n_1 - n_2)N\alpha\|_{\mathbb{R}/\mathbb{Z}} \\ &= \left\| \frac{(n_1 - n_2)m}{k} + \frac{n_1 - n_2}{N}\frac{\gamma}{k} \right\|_{\mathbb{R}/\mathbb{Z}} \ge \frac{1}{k} - \frac{|\gamma|}{k} > \frac{\delta}{k} = 2\varepsilon_0. \end{aligned}$$

It follows that $n_1^2\alpha$ and $n_2^2\alpha$ cannot both lie in $(-\varepsilon_0, \varepsilon_0)$ modulo 1. Hence at least one of n_1, n_2 fails to belong to $\mathcal{A}_\varepsilon^\alpha$ and so $N \notin 2\mathcal{A}_\varepsilon^\alpha$. ∎

Our next result is in similar spirit, with the difference that instead of the pointwise bound $\varepsilon(n) \le \varepsilon_0$, we work with the condition $\varepsilon(n) \to 0$.

REMARK. It might seem that a set $\mathcal{A}_\varepsilon^\alpha$ with $\varepsilon(n) \to 0$ must necessarily be "smaller" than one with $\varepsilon(n) = \varepsilon_0$, and hence that Lemma 1.2 below is strictly weaker than Lemma 1.1. However, we wish to emphasise that for variable $\varepsilon(n)$ we allow the value $\varepsilon(n)$ to be large when n is small.

Because we expect the complement of $2\mathcal{A}_\varepsilon^\alpha$ to have density 0, we cannot rule out a priori that small values of n play a role. In fact, for any $\varepsilon_0 > 0$, one can construct $\varepsilon(n) \to \varepsilon_0$ such that $\mathcal{A}_\varepsilon^\alpha$ is a basis of order 2, simply by exploiting the fact that $\mathcal{A}_{\varepsilon_0}^\alpha$ is syndetic. Hence, it is not the case that small values of n can be altogether ignored.

Here and elsewhere, by a slight abuse of notation, we write $\mathcal{A}_{\varepsilon_0}^\alpha$, allowing the symbol ε_0 to also denote the constant function $n \mapsto \varepsilon_0$.

LEMMA 1.2. *Let $\varepsilon(n) \to 0$, and let $(N_i)_{i=1}^\infty$ be an increasing sequence of odd integers. Suppose that for each i,*

$$N_i\alpha = \frac{m_i}{k} + \frac{\gamma_i}{kN_i},$$

where m_i, k are integers, k is even and m_i is odd. Assume further that γ with $|\gamma| < 1$ is an accumulation point of γ_i. Then $N_i \notin 2\mathcal{A}_\varepsilon^\alpha$ for infinitely many i, unless $\gamma + kn^2\alpha \in \mathbb{Z}$ for some integer n.

Proof. Passing to a subsequence, we may assume that $\gamma_i \to \gamma$ as $i \to \infty$.

Let ε_0 be such that $(1 - |\gamma|)/k > 2\varepsilon_0 > 0$. Then from Proposition 1.1 it follows that $N_i \notin 2\mathcal{A}_{\varepsilon_0}^\alpha$ for sufficiently large i. Hence, if $N_i \in 2\mathcal{A}_\varepsilon^\alpha$ for some i, then N_i can be represented as $n_1 + n_2$ with $n_1 \in \mathcal{A}_\varepsilon^\alpha \setminus \mathcal{A}_{\varepsilon_0}^\alpha$ and

$n_2 \in \mathcal{A}_\varepsilon^\alpha$. Note that the set $\mathcal{A}_\varepsilon^\alpha \setminus \mathcal{A}_{\varepsilon_0}^\alpha$ is finite, so passing to a subsequence again we may assume that there exists a single n_1 such that for each i we have $n_{2,i} := N_i - n_1 \in \mathcal{A}_\varepsilon^\alpha$.

Directly from the membership condition for $\mathcal{A}_\varepsilon^\alpha$, we now find

$$\varepsilon(n_{2,i}) > \left\| (N_i - 2n_1)\left(\frac{m_i}{k} + \frac{\gamma_i}{kN_i}\right) + n_1^2\alpha \right\|_{\mathbb{R}/\mathbb{Z}}.$$

We have $\varepsilon(n_{2,i}) \to 0$ and

$$\frac{N_i - 2n_1}{N_i}\,\frac{\gamma_i}{k} \to \frac{\gamma}{k} \quad \text{as } i \to \infty.$$

It follows that

$$\left\| \frac{m_i'}{k} + \frac{\gamma}{k} + n_1^2\alpha \right\|_{\mathbb{R}/\mathbb{Z}} \to 0,$$

where $m_i' := (N - 2n_1)m_i \bmod k$. Note that m_i' is odd and takes only finitely many values. Restricting to a subsequence, we may assume that $m_i' = m'$ is constant. Now, the expression in the limit above is independent of i, and hence

$$\left\| \frac{m'}{k} + \frac{\gamma}{k} + n_1^2\alpha \right\|_{\mathbb{R}/\mathbb{Z}} = 0.$$

In particular, $k(\gamma/k + n_1^2\alpha) \in \mathbb{Z}$, contradicting the irrationality assumption. ∎

1.2. Quadratic irrationals. We will now prove Theorem **A4** in the special case when $\alpha = \sqrt{2}$. The argument generalises to $\alpha \in \mathbb{Q}[\sqrt{d}] \setminus \mathbb{Q}$ without any new ideas. This case is already representative for some of our methods. Our immediate goal is the following result.

PROPOSITION 1.3. *Let $\varepsilon_1 := \frac{1}{4}\big(1 - \frac{1}{4\sqrt{2}}\big)$. Suppose that either $\varepsilon(n) \le \varepsilon_0 < \varepsilon_1$ or $\varepsilon(n) \to 0$. Then $\mathcal{A}_\varepsilon^{\sqrt{2}}$ is not a basis of order 2. When $\varepsilon(n)$ is pointwise bounded, we additionally have the quantitative bound*

$$|[T] \setminus 2\mathcal{A}_\varepsilon^{\sqrt{2}}| \gg \log T,$$

where the implicit constant depends at most on $\varepsilon_0, \varepsilon_1$.

Proof. Any positive integer solution (x, y) to the Pell equation

$$X^2 - 2Y^2 = 1 \tag{1.3}$$

gives rise to the rational approximation x/y of α with $\frac{x}{y} - \sqrt{2} = \frac{1}{y(x+\sqrt{2}y)}$.

The fundamental solution to (1.3) is $(x, y) = (3, 2)$. If we let $\phi := 3 + 2\sqrt{2}$ and $\hat{\phi} := 3 - 2\sqrt{2}$, and define integer sequences a_i, b_i by $\phi^i = a_i + b_i\sqrt{2}$, then all solutions to (1.3) are of the form $(x, y) = (a_i, b_i)$. We note that

a_i, b_i have explicit formulas:

$$a_i = \frac{\phi^i + \hat{\phi}^i}{2}, \quad b_i = \frac{\phi^i - \hat{\phi}^i}{2\sqrt{2}}, \tag{1.4}$$

as well as recursive relations:

$$a_{i+2} = 6a_{i+1} - a_i, \quad a_0 = 1,\ a_1 = 3,$$
$$b_{i+2} = 6b_{i+1} - b_i, \quad b_0 = 0,\ b_1 = 2.$$

It will be convenient to take $N_i = b_i/2$. Each N_i is an integer, and if i is odd, then N_i is odd. We may write

$$N_i\sqrt{2} = \frac{a_i}{2} + \frac{\gamma_i}{2N_i}, \quad \text{where} \quad \gamma_i = \hat{\phi}^i N_i = \frac{-1}{4\sqrt{2}} + O\left(\frac{1}{N_i^2}\right). \tag{1.5}$$

To prove the statement in the case $\varepsilon(n) \le \varepsilon_0 < \varepsilon_1$, we apply Lemma 1.1 to N_i, assuming that i is large enough and odd. It follows that $N_i \notin 2\mathcal{A}_\varepsilon^{\sqrt{2}}$, and hence $\mathcal{A}_\varepsilon^{\sqrt{2}}$ is not a basis of order 2. The quantitative estimate follows from the fact that $N_i = \Theta(\phi^i)$, and for any T there are $\Theta(\log T)$ values of i with $N_i < T$.

In the case $\varepsilon(n) \to 0$, we similarly apply Lemma 1.2 to the sequence N_i restricted to odd i, with $\gamma = -1/(4\sqrt{2})$. The claim follows unless there exists n such that $\gamma + 2n^2\sqrt{2} \in \mathbb{Z}$. Since $\sqrt{2}$ is irrational, that would imply $2n^2 = 1/8$, which is absurd. ∎

The result for general quadratic irrational $\alpha \in \mathbb{Q}[\sqrt{d}]$ can be obtained with essentially the same argument.

Proposition 1.4. *For any $\alpha \in \mathbb{Q}[\sqrt{d}] \setminus \mathbb{Q}$ there exists $\varepsilon_1 = \varepsilon_1(\alpha)$ such that the following is true. Suppose that either $\varepsilon(n) \le \varepsilon_0 < \varepsilon_1$ or $\varepsilon(n) \to 0$. Then $\mathcal{A}_\varepsilon^\alpha$ is not a basis of order 2.*

Proof. We may write $\alpha = (a + b\sqrt{d})/c$, where a, b, c are integers. Let $\phi = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ be a unit, and let $\mu := \nu_2(y)$, the largest power of 2 dividing y. Replacing ϕ by ϕ^{2^n} for large n, we may assume that μ is sufficiently large, or more concretely $\mu > \nu_2(b)$ and $2^\mu > bc$.

As before, we consider the integer valued sequences

$$a_i = \frac{\alpha\phi^i - \hat{\alpha}\hat{\phi}^i}{2\sqrt{d}}c, \quad b_i = \frac{\phi^i - \hat{\phi}^i}{2\sqrt{d}}c. \tag{1.6}$$

Using $\mu > \nu_2(b)$ and $\nu_2(x) = 0$, we obtain

$$\nu_2(a_1) = \nu_2(ay + bx) = \nu_2(b), \quad \nu_2(b_1) = \nu_2(cy) = \nu_2(c) + \mu. \tag{1.7}$$

Because the sequences a_i and b_i are periodic modulo any power of 2, there exists some L such that for all $i \equiv 1 \pmod{L}$ we have $\nu_2(a_i) = \nu_2(a_1)$

and $\nu_2(b_i) = \nu_2(b_1)$. For any such i we define

$$N_i := \frac{b_i}{2^{\nu_2(c)+\mu}}, \quad m_i := \frac{a_i}{2^{\nu_2(b)}}, \quad k := 2^{\nu_2(c)-\nu_2(b)+\mu}. \tag{1.8}$$

It is straightforward, if mundane, to check that these quantities are integers, and that

$$N_i\alpha = \frac{m_i}{k} + \frac{\gamma_i}{kN_i},$$

where $\gcd(m_i, k) = 1$ and γ_i are given by

$$\gamma_i = \frac{b\hat{\phi}^i}{2^{\mu+\nu_2(c)}} = \frac{\pm bc}{2^{\mu+\nu_2(bc)+1}\sqrt{d}} + o(1).$$

Here, $o(1)$ denotes an error term which goes to 0 as $i \to \infty$. The choice of μ guarantees that $|\gamma_i| < 1/2$ for large i. In the case $\varepsilon(n) \le \varepsilon_0$, it follows from Lemma 1.1 that $N_i \notin 2\mathcal{A}_\varepsilon^\alpha$ provided that $\varepsilon_1 \le 1/(4k)$.

To deal with the case $\varepsilon(n) \to 0$, we notice that

$$\gamma_i \to \gamma := \frac{\pm bc\sqrt{d}}{2^{\mu+\nu_2(bc)+1}d}.$$

By Lemma 1.2, we have $N_i \notin 2\mathcal{A}_\varepsilon^\alpha$ for sufficiently large i unless $\gamma + kn^2\alpha \in \mathbb{Z}$ for some n. However, the latter would imply $k2^{\mu+\nu_2(bc)+1}d \mid bc^2$, which is impossible, since

$$\nu_2(k2^{\mu+\nu_2(bc)+1}d) \ge \mu + \nu_2(bc) + 1 > \nu_2(bc^2). \ \blacksquare$$

1.3. Badly approximable reals. We now turn to the proof of a variant of Theorem **A4** for badly approximable α.

We say that α is *badly approximable* if for any p, q we have

$$\left|\alpha - \frac{p}{q}\right| \ge \frac{c(\alpha)}{q^2},$$

where $c(\alpha) > 0$ is a constant depending only on α. The most well known examples of such numbers are quadratic irrationals.

This is a more general situation than $\alpha \in \mathbb{Q}[\sqrt{d}]$, but still rather specific. In particular, almost all α are *not* badly approximable. However, badly approximable α provide a non-trivial and fairly explicit class of examples where the conclusion of Theorem **A4** holds (as opposed to an "almost surely" type of statement).

A useful characterisation of badly approximable reals is that these are precisely the ones whose continued fraction expansion has bounded entries (see Appendix, Fact A.16). A specific class of badly approximable real numbers which has attracted some attention are those whose entries are produced by finite automata. For instance, it has been shown that such numbers are transcendental unless their continued fraction expansion is periodic (see [1]).

The main result in this section shows that the sets $\mathcal{A}_\varepsilon^\alpha$ are not bases of order 2 for badly approximable α and sufficiently small ε.

PROPOSITION 1.5. *If α is badly approximable then there is $\varepsilon_1 = \varepsilon_1(\alpha)$ such that if $\varepsilon(n) \le \varepsilon_0 < \varepsilon_1$ then $\mathcal{A}_\varepsilon^\alpha$ is not a basis of order 2. Moreover, $|[T] \setminus 2\mathcal{A}_\varepsilon^\alpha| \gg \log T$, where the implicit constant depends only on α.*

We will make extensive use of the continued fraction expansion of 2α. The crucial role played by the continued fraction expansion explains why we were able to give rather elementary proofs for $\alpha = \sqrt{2}$ and $\alpha \in \mathbb{Q}[\sqrt{d}]$, whose expansion is particularly simple.

Continued fractions are a classical topic, and we assume some familiarity with the basic notions and theorems. For an accessible introduction, see e.g. [5], or the more analytic approach in [6]. For the perspective inspired by measurable dynamics, see [2, Chpt. 3]. In the Appendix, we provide a complete list of properties used. Here, we just review several basic properties and introduce notation, which we will also use in subsequent sections. We will write

$$2\alpha = [a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} \tag{1.9}$$

and a_i will denote the coefficients of 2α throughout this section (note that for technical reasons we consider 2α rather than α). By obvious translation invariance, we may assume that $a_0 = 0$. We also use the partial approximations

$$\frac{p_i}{q_i} = [0; a_1, a_2, \dots, a_i] = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\cdots}{a_i}}}. \tag{1.10}$$

These are essentially the best possible rational approximations of α (see A.15), and we have the error term of the form

$$2\alpha = \frac{p_i}{q_i} + \frac{\delta_i}{q_i^2}, \tag{1.11}$$

where δ_i can be explicitly described by

$$|\delta_i| = q_i^2 \left(\frac{1}{q_i q_{i+1}} - \frac{1}{q_{i+1} q_{i+2}} + \frac{1}{q_{i+2} q_{i+3}} - \cdots \right). \tag{1.12}$$

In particular, $|\delta_i| < q_i/q_{i+1} < 1/a_{i+1} \le 1$.

Proof of Proposition 1.5. Because α is badly approximable, so is 2α, and by A.17 the coefficients a_i are bounded, say $a_i \le a_{\max}$. Let κ be large enough that $2^\kappa \nmid a_i$ for all i.

We claim that among any four consecutive indices $\{j, j+1, j+2, j+3\}$ we can find an index i such that p_i is odd and $\nu_2(q_i) < \kappa$, where as usual $\nu_2(q_i)$ is the largest power of 2 dividing q_i.

For each i we have (e.g. by A.3) $\gcd(p_i, p_{i+1}) = \gcd(q_i, q_{i+1}) = 1$, and in particular neither p_i, p_{i+1} nor q_i, q_{i+1} can both be even. If for some $j \le i \le j+2$ both p_i and p_{i+1} are odd then either q_i or q_{i+1} is odd, and the claim holds. Otherwise, since p_i, p_{i+1} can never both be even, the parity of p_i alternates. It follows that for one of $i \in \{j, j+1\}$, both p_i, p_{i+2} are odd, while p_{i+1} is even. Then $q_{i+2} - q_i = a_{i+2}q_{i+1}$ is not divisible by 2^κ, so one of q_{i+2}, q_i is not divisible by 2^κ. Either i or $i+2$ is the sought index.

Suppose now that i is an index such that p_i is odd and $\nu_2(q_i) < \kappa$, whose existence we have just proved. Take

$$N_i := \frac{q_i}{k_i/2}, \qquad k_i := 2^{\nu_2(q_i)+1}. \tag{1.13}$$

(The definition makes sense for arbitrary i, but we only apply it to i as above.)

Note that k_i is guaranteed to be an even integer, and N_i an odd integer. More precisely, $k_i \le 2^\kappa$ is a power of 2. It is slightly inconvenient that the N_i do not need to be distinct for distinct i, but this will not lead to problems since the N_i take any given value at most κ times.

Finally, we introduce $\gamma_i := 2\delta_i/k_i$, so that

$$N_i\alpha = \frac{p_i}{k_i} + \frac{\gamma_i}{k_iN_i}.$$

Note that

$$|\gamma_i| \le |\delta_i| \le \frac{q_i}{q_{i+1}} = \frac{q_i}{q_i + q_{i-1}} \le 1 - \frac{1}{1+a_{\max}} < 1.$$

We are now in a position to apply Lemma 1.1 (with $\delta = 1/(1+a_{\max})$). It follows that for $\varepsilon_0 < 1/(2^{\kappa+1}(1+a_{\max}))$, if $\varepsilon(n) \le \varepsilon_0$ for all n, then $N_i \notin 2\mathcal{A}_\varepsilon^\alpha$ for all i as described above. In particular, the complement of $2\mathcal{A}_\varepsilon^\alpha$ is infinite, proving the first part of the proposition.

For the quantitative bound, we begin by noticing that $\log N_i = \Theta(i)$. Hence, given T, we have $N_i \in [T]$ for $i \le i_0(T)$, with $i_0(T) = \Theta(\log T)$. For any four consecutive values of i, sufficiently large, for at least one of them we have $N_i \notin 2\mathcal{A}_\varepsilon^\alpha$. Thus,

$$|[T] \setminus 2\mathcal{A}_\varepsilon^\alpha| \gg \frac{i_0(T)}{4\kappa} \gg \log T. \ \blacksquare$$

Remark. In the above result we deal exclusively with pointwise bounded $\varepsilon(n)$. As noted earlier, it does not quite follow that an analogous claim holds when $\varepsilon(n) \to 0$, since large values of $\varepsilon(n)$ for small n can lead to problems. The main difficulty which stops us from extending our results is establishing

the irrationality condition in Lemma 1.2. This can be done for specific values of α, but we do not give a general result.

REMARK. We believe that our methods should extend to numbers such as

$$e^{1/n} = [1; n-1, 1, 1, 3n-1, 1, 1, 5n-1, 1, \dots],$$
$$\tanh(1/n) = [0; n, 3n, 5n, 7n, \dots],$$

whose continued fraction expansions are well understood (see [6, Chpt. II]). It is straightforward to adapt our argument to these situations, and the only reason we do not pursue this further is that we doubt if any of those results would be of much interest.

1.4. Generic reals. Finally, we consider "generic" values of α. We prove a version of A4 which is valid for α outside a set of measure 0. Conveniently, in this case we can make the dependence on ε rather explicit.

PROPOSITION 1.6. *For all $\alpha \in \mathbb{R}$ off a set of measure 0, the set $\mathcal{A}_\varepsilon^\alpha$ fails to be a basis of order 2 if either $\varepsilon(n) \le \varepsilon_0 < 1/4$ for all n, or $\varepsilon(n) \to 0$.*

We retain the definitions and conventions from the previous section. Namely, we assume that $2\alpha \in (0,1)$ has expansion $2\alpha = [0; a_1, a_2, \dots]$ and $p_i/q_i = [0; a_1, a_2, \dots, a_i]$ are the convergents.

The following description of the continued fraction expansion comes as no surprise. It can be construed as a continued fractions analogue of the fact that almost all numbers are normal.

PROPOSITION 1.7. *There exists a set Z of zero measure such that the following is true for $\alpha \notin Z$. Let $b = (b_i)_{i=1}^l \in \mathbb{N}^l$ be a finite string of integers. Let J be the set of indices where b occurs in the expansion $(a_i)_{i=1}^\infty$, i.e. the set of those $j \in \mathbb{N}$ for which $a_{j+t} = b_t$ for all $t \in [l]$. Then the asymptotic density $\mathrm{d}(J) = \lim_{n\to\infty} \frac{1}{n}|J \cap [n]|$ of the set J exists and is positive.*

Proof. Let $T\colon [0,1] \to [0,1]$ be the continued fraction map $T(x) = \{1/x\}$, where $\{\cdot\}$ denotes the fractional part, and let μ be the Gauss measure on $[0,1]$,

$$\mu(E) = \frac{1}{\log 2} \int_E \frac{dx}{x+1}.$$

It is known that $([0,1], T, \mathcal{B}, \mu)$ is an ergodic measure preserving system, and that T acts on continued fraction expansions as a shift: $T([0; c_1, c_2, \dots]) = [0; c_2, c_3, \dots]$ (for details, see [2, Chpt. 3], and Appendix A).

Define $B \subset [0,1]$ to be the set of those $\beta \in [0,1]$ whose expansion is of the form $\beta = [0; b_1, \dots, b_l, *, *, \dots]$. In simpler terms, B is an interval with endpoints $[0; b_1, \dots, b_l]$ and $[0; b_1, \dots, b_l + 1]$. Clearly, $\mu(B) > 0$.

By the pointwise ergodic theorem, for all α off a set of zero measure we have

$$\mathrm{d}(J) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} 1_B(T^n(2\alpha)) = \int 1_B \, d\mu = \mu(B). \ \blacksquare$$

Proof of Proposition 1.6, case $\varepsilon(n) \le \varepsilon_0 < 1/4$. Let A be a large, odd integer, to be specified in the course of the proof. For almost all choices of α, the sequence (A, A, A) appears infinitely often in $(a_i)_{i=1}^{\infty}$, i.e. there exists an infinite set J such that for each $j \in J$ we have $a_{j+1} = a_{j+2} = a_{j+3} = A$.

We claim that for each $j \in J$ we can find $i = i(j) \in \{j, j+1, j+2\}$ such that p_i, q_i are both odd.

If p_j, q_j are odd, we are done. Else, because $\gcd(p_j, q_j) = 1$, precisely one of the two, say p_j, is even. If p_{j+1}, q_{j+1} are both odd, we are done. Otherwise, q_{j+1} is odd, because p_j, p_{j+1} cannot both be even. We have the recursive relation $p_{j+2} = a_{j+2}p_{j+1} + p_j = Ap_{j+1} + p_j$, so p_{j+2} is odd. By a similar argument, q_{j+2} is odd, so we are done.

For any $j \in J$, take $N_j = q_{i(j)}$ and $\gamma_j = \delta_{i(j)}$. By construction, N_j is odd and we have

$$N_j\alpha = \frac{p_{i(j)}}{2} + \frac{\gamma_j}{2N_j}.$$

We are now in a position to apply Lemma 1.1. It follows that $N_j \notin \mathcal{A}_\varepsilon^\alpha$ provided that $\varepsilon(n) \le \varepsilon_1$ for all n, where $\varepsilon_1 < \frac{1}{4} - \frac{1}{4}|\gamma_j|$ for all j. We know that $|\gamma_j| < 1/a_{i(j)+1} = 1/A$, so it will suffice to ensure that $\varepsilon_0 < 1/4 - 1/(4A)$, which can be accomplished by choosing A sufficiently large. $\blacksquare$

We will next deal with the situation when $\varepsilon(n) \to 0$. Surprisingly, this is more difficult, because care is needed to ensure that the irrationality condition in Lemma 1.2 is satisfied.

We need a preliminary lemma about estimation of the error term δ_i based on the knowledge of a limited number of continued fraction coefficients. Recall that δ_i is related to α by $2\alpha = p_i/q_i + \delta_i/q_i^2$.

LEMMA 1.8. *Let l be a positive integer. Then there exists a function $\tilde{\delta}_l \colon \mathbb{N}_{\ge 1}^{2l+1} \to \mathbb{R}$ such that for any $n > l$ we have*

$$|\delta_n - (-1)^n \tilde{\delta}_l((a_i)_{i=n-l}^{n+l})| \ll 2^{-l/2}, \tag{1.14}$$

where the implicit constant is absolute.

Proof. Recall that $\delta_n = q_n^2(2\alpha - p_n/q_n)$. Using standard facts about continued fractions, setting $\rho_n = [a_n; a_{n+1}, \dots]$ we may write

$$\delta_n = q_n^2\left(\frac{p_{n-1}\rho_n + p_{n-2}}{q_{n-1}\rho_n + q_{n-2}} - \frac{p_{n-1}a_n + p_{n-2}}{q_{n-1}a_n + q_{n-2}}\right)$$
$$= \frac{(-1)^n(q_{n-1}a_n + q_{n-2})^2(\rho_n - a_n)}{(q_{n-1}a_n + q_{n-2})(q_{n-1}\rho_n + q_{n-2})}.$$

Recalling that $q_{n-2}/q_{n-1} = [0; a_{n-1}, a_{n-2}, \dots] := \lambda_n$ we may simplify the above formula to

$$\delta_n = (-1)^n(\rho_n - a_n)\frac{a_n + \lambda_n}{\rho_n + \lambda_n}.$$

Setting $\tilde{\rho} = \tilde{\rho}((a_i)_{i=n-l}^{n+l}) := [a_n; a_{n+1}, \dots, a_{n+l}]$ and $\tilde{\lambda} = \tilde{\lambda}((a_i)_{i=n-l}^{n+l}) := [0; a_{n-1}, a_{n-2}, \dots, a_{n-l}]$ we have $\rho_n = \tilde{\rho} + O(2^{-n/2})$ and $\lambda_n = \tilde{\rho} + O(2^{-n/2})$. It remains to define

$$\tilde{\delta}_l = \tilde{\delta}_l((a_i)_{i=n-l}^{n+l}) := (-1)^n(\tilde{\rho} - a_n)\frac{a_n + \tilde{\lambda}}{\tilde{\rho} + \tilde{\lambda}}. \blacksquare$$

Proof of Proposition 1.6, case $\varepsilon(n) \to 0$. Using Proposition 1.7, for almost all choices of α, we may find arbitrarily long strings of 1's in the expansion $(a_i)_{i=1}^{\infty}$. More precisely, there exists an infinite set J and a sequence $l(j)$, $j \in J$, with $l(j) \to \infty$ as $J \ni j \to \infty$, such that $a_{j+t} = 1$ for all $j \in J$ and $|t| \le l(j)$.

Repeating the argument from the proof in the pointwise bounded case, we find for each $j \in J$ an index $i = i(j) \in \{j, j+1, j+2\}$ such that p_i, q_i are both odd. Without loss of generality we may assume that $i(j) = j$, i.e. p_j, q_j are both odd for $j \in J$.

Set $N_j := q_j$ and $\gamma_j := \delta_j$, so that

$$N_j\alpha \equiv \frac{p_{i(j)}}{2} + \frac{\gamma_j}{2N_j} \pmod 1.$$

Applying Lemma 1.2, we conclude that either $N_j \notin \mathcal{A}_\varepsilon^\alpha$ for infinitely many j, or for each limit point γ of γ_j there exists n such that $\gamma + 2n^2\alpha \in \mathbb{Z}$.

Passing to a subsequence, we may assume that γ_j converges. Using Lemma 1.8 we can identify $\gamma := \lim_{j\to\infty} \gamma_j$:

$$\gamma = \pm\frac{1}{\varphi} \cdot \frac{1 + \frac{1}{\varphi}}{\varphi + \frac{1}{\varphi}} = \pm\frac{1}{\sqrt{5}},$$

where $\varphi = (1 + \sqrt{5})/2 = [1; 1, 1, \dots]$.

There are two cases to consider, depending on whether or not α and γ are affinely independent over $\mathbb{Z}$. If they are, then we are done by Lemma 1.2. Otherwise, $\alpha \in \mathbb{Q}[\sqrt{5}]$. However, we can exclude this case, since $\mathbb{Q}[\sqrt{5}]$ has measure 0 (alternatively, we can apply Proposition 1.3). $\blacksquare$

REMARK 1.9. It is tempting to try to repeat the argument for $\varepsilon(n) \le \varepsilon_0$ in the case $\varepsilon(n) \to 0$. Arguing along these lines, one can find a sequence of

odd integers N_j such that $N_j\alpha \equiv p_{i(j)}/2 + \gamma_j/(2N_j) \pmod 1$ with $p_{i(j)}$ odd and $\gamma_j \to 0$. Lemma 1.2 would be applicable with $\gamma = 0$. We may conclude (inspecting the proof of Lemma 1.2) that for sufficiently large j, the only possible representation of N_j as a member of $2\mathcal{A}_\varepsilon^\alpha$ is $N_j = N_j + 0$. However, $0 \in \mathcal{A}_\varepsilon^\alpha$, and we cannot exclude the possibility that $N_j \in \mathcal{A}_\varepsilon^\alpha$, hence the need for a more involved argument.

2. Largeness and equidistribution. In Section 1 we have seen that usually the sets $\mathcal{A}_\alpha^\varepsilon$ (as defined in 1.1) are not bases of order 2. Our goal in this section is to show that the sets $2\mathcal{A}_\alpha^\varepsilon$ nevertheless tend to be quite sizeable. For the convenience of the reader we recall the statements of our main theorem, given in the introduction. Our first result deals with density, and applies in a fairly general situation.

THEOREM (**A1**, reiterated). *Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$. Then there exists a decreasing sequence $\varepsilon_\alpha(n) \to 0$ such that $\mathcal{A}_\varepsilon^\alpha$ is an almost basis of order 2 provided that $\varepsilon(n) \geq \varepsilon_\alpha(n)$ for all n.*

We will also prove a more surprising result, which shows that results from Section 1 cannot be generalised to all α.

THEOREM (**A2**, reiterated). *There exists an uncountable set $E \subset \mathbb{R}$ such that for any $\alpha \in E$, there exists a decreasing sequence $\varepsilon_\alpha(n) \to 0$ such that $\mathcal{A}_\varepsilon^\alpha$ is a basis of order 2 provided that $\varepsilon(n) \geq \varepsilon_\alpha(n)$ for all n.*

As the reader will have noticed, because of the monotonicity of the family $\mathcal{A}_\varepsilon^\alpha$ with respect to ε, it is no loss of generality to assume in both theorems that $\varepsilon(n) = \varepsilon_\alpha(n)$ for all n.

2.1. Equidistribution and quantitative rationality. In Section 1, specifically in Lemmas 1.1 and 1.2, we have identified a class of obstructions to $\mathcal{A}_\varepsilon^\alpha$ being a basis of order 2. Namely, we found sufficient conditions for a large integer N to fail to belong to $2\mathcal{A}_\varepsilon^\alpha$.

Here, our first goal is to prove that these obstructions are essentially the only possible ones. We obtain two subtly different results, which can be construed as partial converses to Lemmas 1.1 and 1.2. Because $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ is always at most $1/2$, we implicitly assume that $\varepsilon_0 \leq 1/2$ in what follows.

LEMMA 2.1. *There exists a constant C such that the following is true. Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, let $\varepsilon(n) \geq \varepsilon_0$ for all n, and suppose that $N \notin 2\mathcal{A}_\varepsilon^\alpha$. Then there exists $0 < k \leq 1/\varepsilon_0^C$ such that*

$$\|kN\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{N\varepsilon_0^C}. \tag{2.1}$$

LEMMA 2.2. *Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ and $\varepsilon_1 > 0$. For any $\varepsilon_0 > \varepsilon_1$ there exists $N_0 = N_0(\alpha, \varepsilon_1, \varepsilon_0)$ such that following is true for $N \geq N_0$. Suppose that*

$\varepsilon(n) \geq \varepsilon_0$ for all n and $N \notin 2\mathcal{A}_\varepsilon^\alpha$. Then N is odd and there exist $m, k \in \mathbb{N}$ and $\gamma \in \mathbb{R}$ such that $2 \mid k$, $\gcd(m,k) = 1$, and

$$N\alpha = \frac{m}{k} + \frac{\gamma}{kN}, \qquad \frac{1-|\gamma|}{2k} > \varepsilon_1. \tag{2.2}$$

We pause to describe the difference between these two results. Both state that if $N \notin 2\mathcal{A}_\varepsilon^\alpha$, then $N\alpha$ is well approximated by a rational with small denominator. In Lemma 2.1, the quality of approximation is worse, but no additional assumptions are imposed on N. On the other hand, in Lemma 2.2 we obtain detailed information, but we need to restrict to sufficiently large N. In particular, Lemma (2.1) is non-vacuous in the regime $\varepsilon \sim 1/N^\delta$ with δ sufficiently small.

The first step in order to prove Lemmas 2.1 and 2.2 is to reduce the problem of representing N as an element of $2\mathcal{A}_\varepsilon^\alpha$ to an equidistribution statement about an orbit on the torus.

Observation. *Fix α, let $\varepsilon(n) = \varepsilon_0$ be constant, and let $N \in \mathbb{N}$. Then $N \in 2\mathcal{A}_\varepsilon^\alpha$ if and only if the quadratic orbit*

$$x_n := \left(n^2\alpha, (N-n)^2\alpha\right) \in \mathbb{T}^2$$

enters the set $(-\varepsilon_0, \varepsilon_0)^2 \subset \mathbb{T}^2$ at some time up to N, i.e. there exists $0 < n \leq N$ such that $x_n \in (-\varepsilon_0, \varepsilon_0)^2$.

For a sequence $(x_n)_{n=1}^\infty \in X$ of points in a compact metric space endowed with a probability measure μ, we shall say, following e.g. [3], that x_n is (δ, N)-*equidistributed* if for each $f \in \mathrm{Lip}(X;\mathbb{R})$ we have

$$\left| \mathbb{E}_{n \leq N} f(x_n) - \int\limits_X f \, d\mu \right| \leq \delta \|f\|_{\mathrm{Lip}}.$$

Here,

$$\|f\|_{\mathrm{Lip}} = \sup_{x,y \in X} \frac{|f(x) - f(y)|}{d_X(x,y)},$$

and $\mathrm{Lip}(X;\mathbb{R}) \subset \mathcal{C}(X;\mathbb{R})$ denotes the space of those f with $\|f\|_{\mathrm{Lip}} < \infty$.

Although we are ultimately interested in density, equidistribution turns out to be easier to work with. Of course, not every dense sequence is equidistributed. However, equidistribution implies density, if we allow for a slight change in the parameters. The following observation is elementary.

Observation. *Suppose that X is a d-dimensional compact smooth manifold equipped with a Riemannian metric and with a measure μ arising from a volume form. Then there exists a constant $c > 0$ such that the following is true. Let $\delta > 0$, and suppose that a sequence x_n is $(c\delta^d, N)$-equidistributed. Then for any $x \in X$, there exists n such that $d_X(x, x_n) < \delta$.*

It is a classical result of Weyl that lack of equidistribution of a polynomial orbit on the torus can always be explained by a rational obstruction. We have the following classical theorem (see [2, Thm. 1.4]).

THEOREM 2.3 (Weyl equidistribution). *For any d there exist a family of constants $N_0(p,\delta)$ such that the following is true. Let $p(n) = (p_i(n))_{i=1}^d$ be a polynomial sequence in $\mathbb{T}^d$. Suppose that $p(n)$ is not (δ, N)-equidistributed. Then either $N < N_0(p,\delta)$, or there exists $k \in \mathbb{Z}^d \setminus \{0\}$ such that if $\sum_i k_i p_i = \sum_j \alpha_j n^j$, then $\alpha_j \in \mathbb{Z}$ for all j.*

We will need a quantitative version of the above theorem. The following result is a special case of [3, Theorem 1.16].

THEOREM 2.4. *For any d, r there exists a constant C such that the following is true. Let $p(n) = (p_i(n))_{i=1}^d$ be a polynomial sequence in $\mathbb{T}^d$ with $\deg p = r$. Suppose that $p(n)$ is not (δ, N)-equidistributed. Then there exists $k \in \mathbb{Z}^d \setminus \{0\}$ such that $k_i \ll 1/\delta^C$ and if we write $\sum_i k_i p_i = \sum_j \alpha_j n^j$ then $\|\alpha_j\|_{\mathbb{R}/\mathbb{Z}} \ll 1/(N^j \delta^C)$.*

We are now ready to prove the main results in this section.

Proof of Lemma 2.1. Since $N \notin 2\mathcal{A}_\varepsilon^\alpha$, the orbit $(n^2\alpha, (N-n)^2\alpha)$ misses $(-\varepsilon_0, \varepsilon_0)^2$ up to time N. It follows that $(n^2\alpha, 2Nn\alpha)$ fails to be $(c\varepsilon_0^2, N)$-equidistributed with $c > 0$.

By the characterisation of equidistribution in Theorem 2.4, it follows that there is a universal constant C such that we can find k_1, k_2 with $|k_i| \ll 1/\varepsilon_0^C$, $(k_1, k_2) \neq (0,0)$, such that

$$\|k_1\alpha\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{1}{N^2\varepsilon_0^C} \quad \text{and} \quad \|k_2 N\alpha\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{1}{N\varepsilon_0^C}.$$

Hence, for $i = 1, 2$ we have $\|k_i N\alpha\|_{\mathbb{R}/\mathbb{Z}} \ll 1/(N\varepsilon_0^C)$, and since the k_i cannot both be 0, the claim follows. ∎

Proof of Lemma 2.2. It follows from Lemma 2.1 that there exists $K = O_{\varepsilon_0}(1)$ such that $\|kN\alpha\|_{\mathbb{R}/\mathbb{Z}} = O_{\varepsilon_0}(1/N)$ for some $k \in [K]$. Possibly replacing k with one of its divisors, we can therefore write

$$N\alpha = \frac{m}{k} + \frac{\gamma}{kN},$$

where $\gcd(m,k) = 1$, $|\gamma| \leq G$ and $G = O_{\varepsilon_0}(1)$ is a constant.

Let $\delta > 0$ be a small number to be determined later and let $M = M(\delta, \alpha)$ be such that $(n^2\alpha \bmod 1)$ intersects any interval of length δ as n ranges over any progression $P = n_0 + l[M']$ with length $M' \geq M$ and step $l \leq K$. We know that such an M exists, for instance by Theorem 2.4.

Note that for any $n \in \mathbb{N}$ we have

$$(n^2\alpha, (N-n)^2\alpha) = \left(n^2\alpha, n^2\alpha + \frac{(N-2n)m}{k} + \frac{N-2n}{N}\,\frac{\gamma}{k}\right).$$

Thus, the values $n^2\alpha \bmod 1$ and $(N-n)^2\alpha \bmod 1$ depend only on $n^2\alpha \bmod 1$, $N-2n \bmod k$ and $(N-2n)/N$. If k is even, then for any choice of n, $N-2n \bmod k$ has the same parity as N, and obviously $(N-2n)/N \in [-1,1]$. These turn out to be essentially the only restrictions.

OBSERVATION 2.5. *Let $\tau \in \mathbb{T}$, $b \in [k]$, $x \in [-1,1]$, and if k is even, assume additionally that $b \equiv N \pmod 2$. Then there exists some $n \in [N]$ such that $\|n^2\alpha - \tau\|_{\mathbb{R}/\mathbb{Z}} \le \delta$, $(N-2n)m \bmod k = b$ and*

$$\left|\frac{N-2n}{N} - x\right| \le \frac{2KM}{N} \quad \text{provided that } N > 2KM.$$

Proof. We can pick n_0 such that

$$\left|\frac{N-2n_0}{N} - x\right| \le \frac{2}{N}.$$

Next, we can pick n_1 with $|n_0 - n_1| \le k$ such that $(N-2n_1)m \equiv b \pmod k$ and

$$\left|\frac{N-2n_1}{N} - x\right| \le \frac{2K}{N}.$$

Let $P = n_2 + k[M]$ be a progression of length M, step k, containing n_1, and contained in $[N]$. For $n \in P$ we have

$$\left|\frac{N-2n}{N} - x\right| \le \frac{2KM}{N}$$

and $(N-2n)m \equiv b \pmod k$. For at least one of these values, we have $\|n^2\alpha - \tau\|_{\mathbb{R}/\mathbb{Z}} \le \delta$. ∎

If N is even or k is odd, then taking $\tau = 0$, $b = 0$, $x = 0$ and setting $\delta = \varepsilon_0/2$ we find some $n \in [N]$ such that $\|n^2\alpha\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon_0/2$ and $\|(N-n)^2\alpha\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon_0/2 + 2MKG/N$, unless $N \le 2KM$. Since $N \notin 2\mathcal{A}_\varepsilon^\alpha$, this situation is only possible if $N \ll MKG/\varepsilon_0$. Hence, we may assume that N is odd and k is even.

If $|\gamma| \ge 1$, then taking $\tau = 0$, $b = 1$, $x = 1/\gamma$, $\delta = \varepsilon_0/2$ we again find some $n \in [N]$ such that $\|n^2\alpha\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon_0/2$ and $\|(N-n)^2\alpha\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon_0/2 + 2MKG/N$, which leads to a contradiction, unless $N \ll MKG/\varepsilon_0$. Hence, we may assume this is not the case.

Finally, take $b = 1$, $x = -\operatorname{sgn}\gamma$ and $\tau = -\frac{1}{2k}(1-|\gamma|)$ and $\delta = (\varepsilon_0 - \varepsilon_1)/2$. Then for some $n \in [N]$ we have (assuming $N \ge KM$)

$$\begin{aligned}\varepsilon_0 &\le \max(\|n^2\alpha\|_{\mathbb{R}/\mathbb{Z}}, \|(N-n)^2\alpha\|_{\mathbb{R}/\mathbb{Z}}) \\ &\le \frac{1-|\gamma|}{2k} + \frac{\varepsilon_0 - \varepsilon_1}{2} + 2\frac{MKG}{N}.\end{aligned}$$

If $(1-|\gamma|)/(2k) \le \varepsilon_1$, then the above implies that $N \ll MKG/(\varepsilon_0 - \varepsilon_1)$. Otherwise, the decomposition $N\alpha = m/k + \gamma/(kN)$ obtained earlier satisfies

the condition $(1-|\gamma|)/(2k) > \varepsilon_1$, and we find that k is even and N is odd from previous considerations. ∎

2.2. Almost bases of order 2. With tools introduced in 2.1, we are ready to prove the first of the two main results of this section, of which Theorem **A1** is a special case.

To formulate the theorem, we need an additional piece of notation. For real α, the *irrationality measure* of α, denoted $\mu(\alpha)$, is the smallest μ such that for any $\delta > 0$ we have

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^{\mu+\delta}}$$

for any p, q with $\alpha \neq p/q$, where $c = c(\alpha, \delta, \mu) > 0$ is a constant independent of p and q. If no such μ exists, then $\mu(\alpha) = \infty$. We also recall that α is said to be *badly approximable* if $|\alpha - p/q| \geq c/q^2$ for any integers p, q, where $c = c(\alpha) > 0$.

For $\alpha \in \mathbb{Q}$ we have (somewhat artificially) $\mu(\alpha) = 1$, and $\mu(\alpha) \geq 2$ for any other α. For almost all α (with respect to Lebesgue measure), we have $\mu(\alpha) = 2$. Specifically, this holds for algebraic numbers, which is a celebrated result due to Roth [7].

THEOREM 2.6. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then there exists a decreasing sequence $\varepsilon_\alpha(n) \to 0$ such that for any ε with $\varepsilon(n) \geq \varepsilon_\alpha(n)$ for all n, the set $\mathcal{A}_\varepsilon^\alpha$ is an almost basis of order 2.*

Moreover, if $\mu(\alpha) < \infty$, then the assumption $\varepsilon(n) \geq \varepsilon_\alpha(n)$ can be replaced with $\log(1/\varepsilon(n))/\log n \to 0$. In this case, we additionally have

$$|[T] \setminus 2\mathcal{A}_\varepsilon^\alpha| \ll T^{1-c},$$

where the constant $c > 0$ depends only on α.

Finally, if α is badly approximable, and $\varepsilon(n) \geq \varepsilon_0 > 0$ for all n, we have a sharper estimate

$$|[T] \setminus 2\mathcal{A}_\varepsilon^\alpha| \ll \log T,$$

where the implicit constant depends only on α and ε_0.

We begin by proving a technical proposition which describes local sparsity of the complement of $2\mathcal{A}_\varepsilon^\alpha$. We wish to point out that this is a slightly stronger type of statement than Theorem 2.6, since even sets with extremely slow asymptotic growth can contain many consecutive elements.

PROPOSITION 2.7. *There exists a constant C such that the following is true. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and suppose that $\varepsilon(n) \geq \varepsilon_0 > 0$. Suppose that $N, N' \notin 2\mathcal{A}_\varepsilon^\alpha$ and $N' > N$. Then:*

(1) *If α is badly approximable, then $N' - N \gg N\varepsilon_0^C$.*
(2) *If $\mu(\alpha) < \infty$ and $\tau > \frac{\mu(\alpha)-2}{\mu(\alpha)-1}$, then $N' - N \gg_\tau N^{1-\tau}\varepsilon_0^C$.*
(3) *If $\mu(\alpha) = \infty$ then $N' - N \gg \varepsilon_0^C \omega(N\varepsilon_0^C)$, where $\omega(t) \to \infty$ as $t \to \infty$.*

Proof. Since $N, N' \notin 2\mathcal{A}_\varepsilon^\alpha$, it follows from Lemma 2.1 that there are $k, k' \le 1/\varepsilon_0^C$ such that $\|kN\alpha\|_{\mathbb{R}/\mathbb{Z}}, \|k'N'\alpha\|_{\mathbb{R}/\mathbb{Z}} \le 1/(N\varepsilon_0^C)$, where C is a universal constant.

Let $Q_0(\delta)$ denote the least positive integer such that $\|Q_0(\delta)\alpha\|_{\mathbb{R}/\mathbb{Z}} \le \delta$. For any irrational α we have $Q_0(\delta) \to \infty$ as $\delta \to 0$. Moreover, if $\mu > \mu(\alpha)$ and $1/(1-\tau) = \mu - 1$ (resp. if $\mu = 2$, and $\tau = 0$ if α is badly approximable), then $Q_0(\delta) \gg 1/\delta^{1-\tau}$.

Let $L := N - N'$ and $m := kk' \le 1/\varepsilon_0^{2C}$. We have

$$\|mL\alpha\|_{\mathbb{R}/\mathbb{Z}} \le k\|k'N'\alpha\|_{\mathbb{R}/\mathbb{Z}} + k'\|kN\alpha\|_{\mathbb{R}/\mathbb{Z}} \le \frac{2}{N\varepsilon_0^{2C}},$$

and as a consequence

$$\frac{L}{\varepsilon_0^{2C}} \ge Q_0\left(\frac{2}{N\varepsilon_0^{2C}}\right) \gg (N\varepsilon_0^{2C})^{1-\tau}.$$

In each case, this easily leads to the sought bound. ∎

Proof of Theorem 2.6. We may assume that $\varepsilon(2n) \ge \frac{1}{2}\varepsilon(n)$, and that $\varepsilon(n)$ is non-increasing. Set $\mathcal{N} := \mathbb{N} \setminus 2\mathcal{A}_\varepsilon^\alpha$ and enumerate $\mathcal{N} = \{N_i\}_{i=1}^\infty$ so that $N_{i+1} > N_i$.

Our first aim is to show that the sequence N_i increases rapidly enough. Take any i. If $N_{i+1} \ge 2N_i$, then we have a sufficiently good lower bound for N_{i+1}, so suppose that this is not the case. Since $N_{i+1}, N_i \notin 2\mathcal{A}_{\varepsilon(N_{i+1})}^\alpha$, we may apply Proposition 2.7 to conclude that

$$N_{i+1} - N_i \gg \begin{cases} N_i\varepsilon(N_i)^C & \text{if } \alpha \text{ b. approx., with } C > 0, \\ N_i^c\varepsilon(N_i)^C & \text{if } \mu(\alpha) < \infty, \text{ with } C, c > 0, \\ \varepsilon(N_i)^C\omega(N_i\varepsilon(N_i)^C) & \text{else, with } \omega(t) \to \infty,\ C > 0. \end{cases} \tag{2.3}$$

In the general case, we have $N_{i+1} - N_i \to \infty$ as $i \to \infty$ provided that $\varepsilon(n)^C\omega(n\varepsilon(n)^C) \to 0$ as $n \to \infty$. The latter condition is satisfied for $\varepsilon(n)$ constant, and hence also for some slowly decaying $\varepsilon_\alpha(n) \to 0$. Lack of control on ω makes it impossible to say anything more explicit about ε_α.

In the case when $\mu(\alpha) < \infty$, assume that $\varepsilon(n) \gg 1/N^\delta$, where δ is small enough. We have $N_{i+1} \gg N_i + c_2N_i^{c_1}$ with $c_1, c_2 > 0$. A simple inductive argument shows that in this case $N_i \gg i^{1+c}$ for some $c > 0$. Hence, $|[T] \cap \mathcal{N}| \ll T^{1/(1+c)}$, proving the sought bound.

When α is badly approximable and $\varepsilon(n) \ge \varepsilon_0$, we have $N_{i+1} \gg N_i(1+\varepsilon_0^C)$ with some constant C. It follows by a simple inductive argument that $\log N_i \gg \log i$. In particular, $|[T] \cap \mathcal{N}| \ll \log T$. ∎

Remark. Essentially the same argument leads to a result in higher dimensions. More precisely, if $\alpha \in \mathbb{R}^r$ and we define

$$\mathcal{A} = \{n \in \mathbb{N} \mid \|n^2\alpha_i\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon \text{ for } i = 1, \dots, r\},$$

where $\varepsilon > 0$ is constant, then one can show that $2\mathcal{A}$ has density 1 provided that $k \cdot \alpha = \sum_i k_i \alpha_i$ is irrational for all $k \in \mathbb{Z}^r \setminus \{0\}$.

2.3. Exceptional values of α. We have seen in Section 1 that the sets $\mathcal{A}_\varepsilon^\alpha$ tend not to be bases of order 2. The main result of this section shows that such statements do not generalise to *all* values of α: we can find values of α such that $\mathcal{A}_\varepsilon^\alpha$ is a basis of order 2 as soon as $\varepsilon(n) \geq \varepsilon_0 > 0$.

For such values of α we also find that $\mathcal{A}_\varepsilon^\alpha$ is a basis of order 2 for some $\varepsilon(n) \to 0$. However, we have little control over the rate of convergence, so we do not pursue this issue further.

Our approach amounts to carefully preventing the conditions (2.2) in Lemma 2.2 from being satisfied. The crucial step is establishing some control over all good approximations of α.

Throughout this section, we work with $\alpha \in (0,1) \setminus \mathbb{Q}$, and we let a_i denote the digits in the continued fraction expansion of α:

$$\alpha = [a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} \tag{2.4}$$

(note the difference with usage in Section 1), and p_i/q_i denote the rational approximations of α arising from the truncated continued fractions: $p_i/q_i = [a_0; a_1, \dots, a_i]$.

Recall that $\nu_p(a)$ denotes the largest power of the prime p dividing a. We will be interested in α satisfying the following conditions:

$$\nu_2(q_i) \to \infty \quad \text{as } i \to \infty \text{ through even numbers,} \tag{2.5}$$

$$\nu_p(q_i) \to \infty \quad \text{as } i \to \infty \text{ through odd numbers, for } p \text{ odd prime.} \tag{2.6}$$

We observe that if the a_i obey (2.5), (2.6), then they also obey

$$\nu_2(a_i) \to \infty \quad \text{as } i \to \infty \text{ through even numbers,} \tag{2.7}$$

$$\nu_p(a_i) \to \infty \quad \text{as } i \to \infty \text{ through odd numbers, for } p \text{ odd prime.} \tag{2.8}$$

This is an easy consequence of the facts that $a_i = \frac{q_i - q_{i-2}}{q_{i-1}}$ (Fact A.2) and $\gcd(q_i, q_{i-1}) = 1$ (Fact A.3).

The following observation ensures that our considerations are not vacuous. It is not difficult, but the proof is slightly mundane.

Observation 2.8. *There exist uncountably many α such that the conditions* (2.5) *and* (2.6) (*and hence also* (2.7) *and* (2.8)) *are satisfied. Moreover, for any $h_i \in \mathbb{N}$ with $h_i \to \infty$ as $i \to \infty$, we can additionally require that $a_i \leq h_i$ for all i.*

Proof. Let p be a prime and $k_i^{(p)}$ a sequence of integers with $k_i^{(p)} \to \infty$. We will construct a sequence $a_i^{(p)}$ such that $a_i^{(p)} \leq p^{k_i^{(p)}}$ and an associated

sequence $q_i^{(p)}$ (related to $a_i^{(p)}$ by $r_i^{(p)}/q_i^{(p)} = [a_0^{(p)}; a_1^{(p)}, \dots, a_i^{(p)}]$ for some $r_i^{(p)}$) in such a way that $\nu_p(q_i^{(p)}) \ge k_i^{(p)}$ for sufficiently large i. Once this is done, we choose sequences $k_i^{(p)}$ with $k_i^{(p)} \to \infty$ such that $\prod_p p^{k_i^{(p)}} \le h_i$, and define $a_i \le \prod_p p^{k_i^{(p)}}$ by requiring that $a_i \equiv a_i^{(p)} \pmod{p^{k_i^{(p)}}}$. It is clear that the sequence a_i thus defined satisfies (2.5) and (2.6).

To construct $a_i^{(p)}$ we proceed by induction. We only consider the case $p \ne 2$; the case $p = 2$ is fully analogous. We may take arbitrary values $a_i^{(p)}$ for a number of small values of i. In particular, in the construction we may assume that i is large enough that $k_i^{(p)} \ge 1$. Suppose that $a_1^{(p)}, \dots, a_i^{(p)}$ have been constructed for some $i \equiv 1 \pmod 2$. Since at most one of $q_i^{(p)}, q_{i+1}^{(p)}$ is divisible by p, we can choose $a_{i+1}^{(p)} \le p \le p^{k_{i+1}^{(p)}}$ so that $q_{i+1}^{(p)} = a_{i+1}^{(p)} q_i^{(p)} + q_{i-1}^{(p)} \not\equiv 0 \pmod p$. Next, since $p \nmid q_{i+1}^{(p)}$, we may choose $a_{i+2}^{(p)} \le p^{k_{i+2}^{(p)}}$ so that $q_{i+2}^{(p)} = a_{i+2}^{(p)} q_{i+1}^{(p)} + q_i^{(p)} \equiv 0 \pmod{p^{k_{i+2}^{(p)}}}$. This finishes the inductive step. It follows from the construction that $\nu_p(q_i) \ge p^{k_i^{(p)}}$ for all but finitely many i, so the sequence satisfies the required conditions.

To show that the number of possible choices of α is uncountable, we notice that different choices of the sequences $k_i^{(p)}$ produce different α. Since there are uncountably many choices for $k_i^{(p)}$, there are also uncountably many choices of α. ∎

Theorem **A2** is an immediate consequence of the following slightly more technical result, paired with Observation 2.8.

PROPOSITION 2.9. *Suppose that for some α, the conditions* (2.5)–(2.8) *are satisfied, and* $(\log a_i)/i \to 0$. *Then $\mathcal{A}_\varepsilon^\alpha$ is a base of order* 2 *provided that $\varepsilon(n) \ge \varepsilon_0 > 0$ for all n.*

Proof. For a contradiction, suppose that there is some $\varepsilon_0 > 0$ such that $\mathcal{A}_{\varepsilon_0}^\alpha$ is not a base of order 2.

By Lemma 2.2, for infinitely many odd N there exist k, m, γ with k even and $\gcd(m, k) = 1$ such that

$$N\alpha = \frac{m}{k} + \frac{\gamma}{kN}, \qquad \frac{1}{2k}(1 - |\gamma|) > \frac{\varepsilon_0}{2}.$$

Because k is automatically bounded by $k \le 1/\varepsilon_0$, we may assume that k does not depend on N. Moreover, we may assume that m and N are coprime, because a similar relation is satisfied for $N' = N/\gcd(N, m)$, $m' = m/\gcd(N, m)$ and $\gamma' = \gamma/\gcd(N, m)^2$.

We fix N, but we reserve the right to assume that N is sufficiently large in terms of ε_0 and k, and take m, γ as above. Set $q = kN$ and $p = m$, and let i be the largest index such that p/q lies between α and p_i/q_i, where $q := kN$.

We will assume that i is odd so that $\alpha < p_{i+2}/q_{i+2} < p/q \le p_i/q_i$. The other case, when $\alpha > p_{i+2}/q_{i+2} > p/q \ge p_i/q_i$, is fully analogous.

The case $p/q = p_i/q_i$ is particularly simple. Because k is even, $q_i = q = kN$ is even, and in particular i is even (because of assumption (2.5)). Since N is odd, $\nu_2(q_i) = \nu_2(k)$ is bounded. However, this contradicts (2.5) provided that N (and hence i) is sufficiently large. Hence, we may assume that $p/q < p_i/q_i$.

We now deal with the general p/q. We can write

$$\frac{p}{q} = \frac{ap_{i+1} + bp_i}{aq_{i+1} + bq_i}$$

for some coprime $a, b \in \mathbb{N}$, simply because $p_{i+1}/q_{i+1} < p/q < p_i/q_i$. A straightforward computation using A.3 shows that

$$\frac{p}{q} - \frac{p_{i+2}}{q_{i+2}} = \frac{(a_{i+2}b - a)(p_{i+1}q_i - p_iq_{i+2})}{qq_{i+2}} = \frac{\Delta}{qq_{i+2}},$$

where $\Delta := a_{i+2}b - a \ge 1$. It follows that

$$\frac{k|\gamma|}{q^2} = \frac{|\gamma|}{kN^2} = \left|\frac{p}{q} - \alpha\right| > \left|\frac{p}{q} - \frac{p_{i+2}}{q_{i+2}}\right| = \frac{\Delta}{qq_{i+2}}.$$

Thus,

$$\gamma \ge \frac{\Delta}{k}\,\frac{q}{q_{i+2}} = \frac{\Delta}{k}\left(b - \frac{\Delta}{q_{i+2}}\right). \tag{2.9}$$

To have some rather crude control on the size of Δ, we note that $q \ge q_i$ (see A.15), so

$$1 \ge |\gamma| \ge \frac{\Delta}{k}\,\frac{q}{q_{i+2}} \ge \frac{\Delta}{4ka_{i+2}a_{i+1}},$$

which leads to $\Delta \le 4ka_{i+2}a_{i+1} \ll (1 + 1/10)^i$. On the other hand, because of A.2 we have $q_i \gg \sqrt{2}^{\,i}$, so if N (and hence also i) is sufficiently large, then $\Delta/q_{i+2} < \varepsilon_0$. Combining this with the previous bounds, we find that

$$1 - 2k\varepsilon_0 \ge |\gamma| > \frac{\Delta}{k}(b - \varepsilon_0),$$

which in particular implies that $1 > \Delta b/k$ provided that ε_0 is small enough.

Let us write $k = k_0k_1$ as a product of a power of 2 and an odd integer. Recall that $k_0k_1 = \frac{q}{N} \mid aq_{i+1} + bq_i$. Assuming that N (and hence i) is sufficiently large, and possibly exchanging the order of k_0, k_1, we conclude from (2.5) and (2.6) that $k_0 \mid q_i$, $\gcd(k_0, q_{i+1}) = 1$ and $k_1 \mid q_{i+1}$, $\gcd(k_1, q_i) = 1$. The divisibility condition $k_0 \mid aq_{i+1} + bq_i$ reduces to $k_0 \mid a$, and likewise $k_1 \mid aq_{i+1} + bq_i$ reduces to $k_1 \mid b$.

Clearly, $k_1 \mid b$ implies that $b \ge k_1$. From $k_0 \mid a$, we have $k_0 \mid \Delta = a_{i+2}b - a$ because of (2.7) and (2.8). Consequently, $\Delta \ge k_0$. Thus, $\Delta b \ge k_0k_1 = k > \Delta b$. This contradiction finishes the proof. ∎

3. Higher degrees. In this section we deal with the sets

$$\mathcal{A}_\varepsilon^p := \{n \in \mathbb{N} \mid \|p(n)\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon(n)\}, \tag{3.1}$$

where $p : \mathbb{Z} \to \mathbb{R}$ is a polynomial, generally of degree higher than 2, and $\varepsilon(n)$ is a slowly decaying function. Our main goal is to prove a generalisation of Theorem **B1**.

THEOREM (**B1**, reiterated). *There exists a set $Z \subset \mathbb{R}$ of measure 0 such that for any $\varepsilon(n) > 0$ with $\log(1/\varepsilon(n))/\log n \to 0$ and any $\alpha \in \mathbb{R} \setminus Z$, the set $\mathcal{A}_\varepsilon^p$ defined in (3.1) with $p(n) = \alpha n^d$ is a basis of order 2.*

Note that the limit restriction is just another way of saying that $\varepsilon(n) = n^{-o(1)}$. In particular, any function of the form $\varepsilon(n) = \log^{-C} n$ will be suitable.

We will also give a simple argument for **B2**.

THEOREM (**B2**, reiterated). *There exists a closed uncountable set $E \subset \mathbb{R}$ and a constant $\varepsilon_0 > 0$ such that for any ε with $\varepsilon(n) \le \varepsilon_0$ and any $\alpha \in E$, the set $\mathcal{A}_\varepsilon^p$ defined in (3.1) is not a basis of order 2.*

3.1. Bases of order 2. In degree at least 3, the generic behaviour is that $\mathcal{A}_\varepsilon^p$ is a basis of order 2. We can prove a result for p varying over an affine subspace $\mathcal{P}$ of the $\mathbb{R}$-vector space $\mathbb{R}[x]$. For brevity, we refer to such $\mathcal{P}$ as an *affine* family of polynomials. Note that $\mathcal{P}$ has a canonical Haar measure (defined up to a constant factor), and hence we have a notion of zero measure sets.

THEOREM 3.1. *Let $\mathcal{P} \subset \mathbb{R}[x]$ be an affine family of polynomials, and let $\varepsilon(n) > 0$ be such that $\log(1/\varepsilon(n))/\log n \to 0$. Then at least of the following holds:*

(1) *For all $p \in \mathcal{P}$ we have $\deg p \le 2$.*
(2) *There is $p \in \mathcal{P}$ such that $\deg p > \deg(p - q)$ for all $q \in \mathcal{P}$.*
(3) *For all $p \in \mathcal{P}$ off a set of measure 0, the set $\mathcal{A}_\varepsilon^p$ is a basis of order 2.*

*Proof of Theorem **B1** assuming Theorem 3.1.* Apply Theorem 3.1 to the linear family of polynomials $\mathcal{P} = \{\alpha x^d \mid \alpha \in \mathbb{R}\}$ with $d \ge 3$. It is clear that neither (1) nor (2) holds for $\mathcal{P}$. Hence, we have (3), which is precisely the claim of **B1**. ∎

Perhaps a more useful restatement of the above theorem is that if $\mathcal{P}$ is an affine family of polynomials not satisfying (1) or (2), then $\mathcal{P}$ must satisfy (3). We clearly need to include (1), because the behaviour for polynomials of degree 2 is different. Condition (2) is meant to exclude the possibility that the behaviour of $\mathcal{A}_\varepsilon^p$ is controlled by a highest degree term which is constant in p.

In the above theorem, we cannot replace "almost all $p \in \mathcal{P}$" with "all $p \in \mathcal{P}$", because $\mathcal{A}_\varepsilon^p$ need not be a basis of order 2, for example when p is

rational. We also believe there exist $p \in \mathbb{R}[x]$ with $\deg p \geq 3$ and highly irrational leading coefficients such that $\mathcal{A}_\varepsilon^p$ is not a basis of order 2.

To prove Theorem 3.1, we need a simple geometric lemma.

LEMMA 3.2. *Let $\mathcal{P}$ be an affine space equipped with a volume form. Let $\alpha, \beta \colon \mathcal{P} \to \mathbb{R}$ be affine forms, let $B \subset \mathcal{P}$ be an open convex set, and let $k, l \in \mathbb{Z}$ be such that $k\alpha + l\beta$ is non-constant. Then there exists $r_0 = r_0(\alpha, \beta, B)$ such that for $r \geq r_0$ and arbitrary $\delta > 0$ we have*

$$\mathbb{P}_{v \in rB}\big(\|k\alpha(v) + l\beta(v)\|_{\mathbb{R}/\mathbb{Z}} \leq \delta\big) = 2\delta(1 + o(1)) \tag{3.2}$$

as $r \to \infty$, where the error term is bounded uniformly in δ and k, l (but may depend on α, β and B).

Proof. If α and β are affinely dependent, then the problem becomes simpler, and can be solved by an argument similar to the one presented below. Let us suppose that α, β are not affinely dependent.

It is easy to construct a parallelepiped K such that $(\alpha(v), \beta(v))$ are uniformly distributed in $\mathbb{T}^2$ for $v \in K$. Then

$$\mathbb{P}_{v \in K}\big(\|k\alpha(v) + l\beta(v)\|_{\mathbb{R}/\mathbb{Z}} \leq \delta\big) = 2\delta.$$

It is elementary that for each r, there exist collections $C_+(r)$, $C_-(r)$ of such parallelepipeds with $C_+(r) \supset rB \supset C_-(r)$ and $\mathrm{vol}(C_\pm(r))/\mathrm{vol}(rB) \to 1$ as $r \to \infty$. The proof now follows by a sandwiching argument. ∎

Proof of Theorem 3.1. We shall assume that neither (1) nor (2) holds, and derive (3). We may assume that $\varepsilon(n) \gg 1/n^\delta$, where δ is a small positive constant yet to be determined, and that $\varepsilon(n)$ is decreasing.

Given $p \in \mathcal{P}$, we define $\mathcal{N}^{(p)}$ to be the set of N such that $N \notin 2\mathcal{A}^p_{\varepsilon(N)}$. Since $\mathcal{N}^{(p)} \supset \mathbb{N} \setminus 2\mathcal{A}^p_\varepsilon$, it will suffice to show that $\mathcal{N}^{(p)}$ is almost surely finite. For this, it is enough to prove that $\mathbb{E}_{p \in rB} |\mathcal{N}^{(p)}| < \infty$, where $B \subset \mathcal{P}$ denotes the unit ball with respect to some norm on $\mathcal{P}$.

Take any $N \in \mathcal{N}^{(p)}$. Following the argument in Lemma 2.1, the orbit $(p(n), p(N-n))$ is not $1/\varepsilon(N)^{O(1)}$-equidistributed for $n \in [N]$. Hence, by Theorem 2.4, there exist $(k, l) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that

$$\|kp(n) + lp(N-n)\|_{\ell^\infty[N]} \ll \frac{1}{\varepsilon(N)^{O(1)}} \ll N^{O(\delta)}, \quad |k|, |l| \ll N^{O(\delta)}, \tag{3.3}$$

where $\|\sum_i \alpha_i n^i\|_{\ell^\infty[N]} := \max_i N^i \|\alpha_i\|_{\mathbb{R}/\mathbb{Z}}$.

Given k, l and p, let $\mathcal{N}^{(p)}_{k,l}$ denote the set of all N satisfying (3.3) (for some choice of the implicit constants). We have

$$\mathcal{N}^{(p)} \subset \bigcup_{(k,l) \neq (0,0)} \mathcal{N}^{(p)}_{k,l}.$$

We will allow for a certain finite set $\mathcal{N}_* \subset \mathbb{N}$ of N which may belong to particularly many sets $\mathcal{N}_{k,l}^{(p)}$. It will suffice if (for a suitable choice of $\mathcal{N}_*$) we prove the bound

$$\sum_{(k,l)\neq(0,0)} \mathbb{E}_{p\in rB} \, |\mathcal{N}_{k,l}^{(p)} \setminus \mathcal{N}_*| < \infty. \tag{3.4}$$

We can write $p(x) = \sum_{i=0}^{d} \alpha_i^{(p)} x^i$, where $\alpha_i^{(p)}$ are affine functions of p. Because conditions (2) and (3) do not hold, $\alpha_d^{(p)}$ is not a constant function of p, and $d \geq 3$.

A straightforward manipulation of (3.3) shows that if $N \in \mathcal{N}_{k,l}^{(p)}$ then

$$\|k\alpha_d^{(p)} + (-1)^d l\alpha_d^{(p)}\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{1}{N^{d-O(\delta)}}, \tag{3.5}$$

$$\|k\alpha_{d-1}^{(p)} - (-1)^d l\alpha_{d-1}^{(p)} - (-1)^d l\alpha_d^{(p)} N\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{1}{N^{d-1-O(\delta)}}. \tag{3.6}$$

If $k + (-1)^d l \neq 0$ then the first bound (3.5) together with Lemma 3.2 implies for $r \geq r_0 = r_0(\alpha_d, \alpha_{d-1}, B)$ that

$$\mathbb{P}_{p\in rB}(N \in \mathcal{N}_{k,l}^{(p)}) \ll \frac{1}{N^{d-O(\delta)}}. \tag{3.7}$$

Else, if $k + (-1)^d l = 0$, then likewise the second bound (3.6) together with Lemma 3.2 implies for $r \geq r_0$ that

$$\mathbb{P}_{p\in rB}(N \in \mathcal{N}_{k,l}^{(p)}) \ll \frac{1}{N^{d-1-O(\delta)}}, \tag{3.8}$$

unless $2\alpha_{d-1}^{(p)} + N\alpha_d^{(p)}$ is constant in p. The latter condition can only hold for a single value of N, independent of k and l. Letting $\mathcal{N}_*$ consist of this specific N (or $\mathcal{N}_* = \emptyset$ if no such N exists), we conclude that for any N we have the bound

$$\mathbb{P}_{p\in rB}(N \in \mathcal{N}_{k,l}^{(p)} \setminus \mathcal{N}_*) \ll \frac{1}{N^{d-1-O(\delta)}}. \tag{3.9}$$

Because for $N \in \mathcal{N}_{k,l}^{(p)}$ we have $|k|, |l| \ll N^{O(\delta)}$, at the cost of worsening implicit constants, we may rewrite (3.8) as

$$\mathbb{P}_{p\in rB}(N \in \mathcal{N}_{k,l}^{(p)} \setminus \mathcal{N}_*) \ll \frac{1}{(k^4+l^4)N^{d-1-O(\delta)}}. \tag{3.10}$$

Taking δ sufficiently small, we can now derive

$$\sum_{k,l} \mathbb{E}_{p\in rB} \, |\mathcal{N}_{k,l}^{p} \setminus \mathcal{N}_*| \ll \sum_{k,l} \frac{1}{k^4+l^4} \sum_{N} \frac{1}{N^{1.1}} < \infty. \tag{3.11}$$

This finishes the proof. ∎

REMARK. The same ideas can be applied to higher dimensions. One then defines

$$\mathcal{A}_\varepsilon^p := \{n \in \mathbb{N} \mid \|p_i(n)\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon(n),\ i \in [r]\}$$

for a polynomial map $p(n) = (p_i(n))_{i=1}^r$. For $\varepsilon(n) \ge \varepsilon_0 > 0$, these sets will generically be bases of order 2.

Because the general version of the equidistribution Theorem 2.4 holds for general nilmanifolds, similar arguments can be applied to "generic" Nil-Bohr sets (see [3] and [4] for relevant definitions).

3.2. Non-bases of order 2. We close this section by considering situations when the sets $\mathcal{A}_\varepsilon^p$ fail to be bases of order 2. We show that for higher degrees of polynomials, it is still possible for $\mathcal{A}_\varepsilon^p$ to fail to be a basis of order 2. For concreteness, we work with the polynomials of the specific form $p(n) = \alpha n^d$.

*Proof of Theorem **B2**.* Take any $\varepsilon_0 < 1/4$, and let d be fixed. We first claim, in analogy to Lemma 1.2, that there is some $N_0 = N_0(d, \varepsilon_0)$ such that if $N > N_0$ is odd and $\varepsilon(n) \le \varepsilon_0$ for all n, and if N and α satisfy

$$\left\| N\alpha - \frac{1}{2} \right\|_{\mathbb{R}/\mathbb{Z}} \le \frac{1}{N^d},$$

then $N \notin 2\mathcal{A}_\varepsilon^p$. Indeed, if $n_1, n_2 \in [N]$ are such that $n_1 + n_2 = N$ then

$$\|n_1^d\alpha - (-1)^d n_2^d \alpha\|_{\mathbb{R}/\mathbb{Z}} = \left\| \sum_{j=0}^{d-1} (-1)^j n_1^{d-1-j} n_2^j N\alpha \right\| = \frac{1}{2} + O\left(\frac{1}{N}\right),$$

where the implicit constant in the error term depends only on d. Thus it is impossible that $n_1, n_2 \in \mathcal{A}_\varepsilon^p$ if $\varepsilon(n) \le \varepsilon_0 < 1/4$ and N is sufficiently large.

Let N_i be a rapidly increasing sequence of odd integers, and set

$$\Gamma := \bigcap_{i \in \mathbb{N}} \Gamma_i, \quad \Gamma_i := \left\{ \alpha \in \mathbb{T} \;\middle|\; \|N_i\alpha - 1/2\|_{\mathbb{R}/\mathbb{Z}} \le \frac{1}{N_i^d} \right\}.$$

For any $\alpha \in \Gamma$, by the above observation we have $N_i \notin 2\mathcal{A}_\varepsilon^p$ for all but finitely many i.

Note that for each i, Γ_i is a union of N_i closed intervals of length $2/N_i^{d+1}$ each, equally spaced in $\mathbb{T}$. Assuming N_i are increasing rapidly enough, each set $\bigcap_{j<i} \Gamma_j$ is a union of closed intervals, and each of these intervals intersects at least two different intervals in Γ_i.

It now follows easily that Γ contains a homeomorphic copy of the Cantor set, and hence is uncountable. The set E in B2 can be taken to be $\Gamma + \mathbb{Z}$. ∎

A. Appendix: Continued fractions. In this appendix we recall some fairly standard facts concerning continued fractions. Because the results are standard, we do not provide proofs, merely references.

A.1. Basic definitions. A continued fraction is an expression of the form

$$[a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}},$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i > 0$. This can be either finite or infinite; we focus mostly on the infinite case.

A standard way to make sense of infinite fractions of this form is to consider consecutive finite approximations, which we typically denote as $\frac{p_n}{q_n}$, given by

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

In particular, $p_0 = a_0,\ q_0 = 1$. It is also convenient to define $p_{-1} = 1$ and $q_{-1} = 0$.

We list some basic properties of the partial approximations. Throughout, a_i denote integers, and p_i, q_i are defined as above. Perhaps the most fundamental fact that we shall use is the following.

FACT A.1 ([5, Thm. 5]). *We have the relation*

$$[a_0, a_1, \dots, a_n, x] = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}.$$

It is not difficult to derive the following consequences.

FACT A.2 ([5, Thms. 1, 12]). *The sequences p_n, q_n are given recursively by*

$$p_{n+2} = a_{n+2}p_{n+1} + p_n, \quad p_{-1} = 1,\ p_0 = a_0,$$
$$q_{n+2} = a_{n+2}q_{n+1} + q_n, \quad q_{-1} = 0,\ q_0 = 1.$$

In particular, $p_{n+m} \geq 2^{(m-1)/2}p_n$ and $q_{n+m} \geq 2^{(m-1)/2}q_n$ for each n, m.

FACT A.3 ([5, Thm. 2]). *We have*

$$q_n p_{n+1} - q_{n+1}p_n = (-1)^n, \quad \textit{or equivalently} \quad \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n+1}}.$$

The sequence p_n/q_n converges rather rapidly. We shall denote

$$\alpha := \lim_{n\to\infty} \frac{p_n}{q_n} = [a_0; a_1, a_2, \dots].$$

and refer to a_i as the *continued fraction expansion* of α.

FACT A.4 ([5, Thm. 9]). *The speed of convergence in* $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$ *is described by*

$$\alpha - \frac{p_n}{q_n} = \sum_{i=n}^{\infty} \frac{(-1)^i}{q_i q_{i+1}},$$

and in particular

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{a_{n+1} q_n^2}.$$

As a consequence, it is always easy to compare two continued fraction approximations.

FACT A.5 ([5, Thm. 4]). *We have the ordering*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \alpha < \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

It is often useful to have a good understanding of the ratio q_{n+1}/q_n. Fortunately, this quantity has a simple description.

FACT A.6 ([5, Thm. 6]). *We have* $q_{n+1}/q_n = [a_{n+1}; a_n, \dots, a_1]$.

A.2. Ergodic perspective. Every irrational number has precisely one (infinite) continued fraction expansion. (A similar statement is true for rational numbers, but one needs to be careful with uniqueness.) More precisely, we have the following fact.

FACT A.7 ([2, Lem. 3.4]). *The map* $\mathbb{Z}\times\mathbb{N}_{\geq 1}^{\mathbb{N}} \ni (a_0, a_1, \dots) \mapsto [a_0; a_1, a_2, \dots] \in \mathbb{R}\setminus\mathbb{Q}$ *is a bijection. Likewise,* $\mathbb{N}_{\geq 1}^{\mathbb{N}} \ni (a_1, \dots) \mapsto [0; a_1, a_2, \dots,] \in [0,1]\setminus\mathbb{Q}$ *is a bijection.*

DEFINITION A.8 (Continued fraction transformation). Define the transformation $T\colon [0,1]\setminus\mathbb{Q} \to [0,1]\setminus\mathbb{Q}$ by $T\alpha = \{1/\alpha\}$, where $\{x\}$ denotes the fractional part of x. (One may extend the definition to $\mathbb{Q}$ by setting $T\alpha = 0$ for $x \in \mathbb{Q}$ if one wishes to have a map $T\colon [0,1] \to [0,1]$.)

Define the measure μ on $[0,1]$ by

$$\mu(A) = \frac{1}{\log 2} \int_A \frac{dx}{x+1} \quad \text{for } A \in \mathcal{B}([0,1]),$$

where $\mathcal{B}([0,1])$ denotes the Borel σ-algebra.

We refer to the transformation T as the *continued fraction transformation* and to μ as the *Gauss measure*.

FACT A.9 ([2, Chpt. 3]). *The transformation* T *acts on* $\mathbb{N}^{\mathbb{N}}$ *by a shift:*

$$T([0; a_1, a_2, \dots]) = T([0; a_2, a_3, \dots]).$$

FACT A.10 ([2, Chpt. 3]). *The measure* μ *is equivalent to the Lebesgue measure. The transformation* T *is measurable and piecewise continuous.*

FACT A.11 ([2, Chpt. 3]). *The transformation T is μ-invariant, in the sense that for each $A \in \mathcal{B}([0,1])$ we have $\mu(T^{-1}(A)) = \mu(A)$.*

Thus, $([0,1], T, \mathcal{B}([0,1]), \mu)$ is a measure preserving system (for introduction to measure preserving systems, see e.g. [2, Chpt. 1]).

FACT A.12 ([2, Thm. 3.7]). *The measure preserving system $([0,1], T, \mathcal{B}([0,1]), \mu)$ is ergodic.*

A.3. Good rational approximations. Essentially all good rational approximations of a number $\alpha = [a_0; a_1, a_2, \dots]$ come from continued fractions.

FACT A.13 (Legendre, [5, Thm. 4]). *If*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

for some p/q, then there exists some i with $p/q = p_i/q_i$.

For context, we also mention a result which we do not use, even implicitly.

FACT A.14 (Hurwitz). *For every α there are p, q such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\, q^2}.$$

Call a fraction p/q a *best rational approximation* (of the second kind, in the terminology of [5]) of α if $|q\alpha - p| < |q'\alpha - p'|$ for any $p'/q' \neq p/q$ with $q' \leq q$.

FACT A.15 ([5, Thms. 16, 17]). *If p/q is a best rational approximation of α, then there exists some i with $p/q = p_i/q_i$. Conversely, if $i \geq 1$ then p_i/q_i is a best rational approximation of α. In particular, if $|\alpha - p/q| \leq |\alpha - p_i/q_i|$ then $q \geq q_i$.*

See also [5, Chpt. 6] for different notions of best rational approximation and more similar results.

Badly approximable numbers can be characterised in terms of their continued fraction expansion. Recall that α is badly approximable precisely when $|\alpha - p/q| \gg 1/q^2$ for all p/q.

FACT A.16 ([2, Prop. 3.10]). *The number α is badly approximable if and only if the sequence $(a_i)_{i=1}^{\infty}$ is bounded.*

A particularly important class of badly approximable numbers are the quadratic irrationals.

FACT A.17 ([5, Thm. 28]). *The expansion $(a_i)_{i=1}^{\infty}$ of α is eventually periodic if and only if α is a quadratic irrational.*

In particular, if α is quadratic irrational then α is badly approximable.

Acknowledgements. The author wishes to thank Ben Green for introducing him to the problem and for much helpful advice and corrections to the manuscript. The author is also indebted to Bryna Kra for comments on possible further directions. Finally, thanks go to Sean Eberhard, Frederick Manners, Przemysław Mazur and Rudi Mrazović for many informal discussions.

References

[1] Y. Bugeaud, *Automatic continued fractions are transcendental or quadratic*, Ann. Sci. École Norm. Sup. (4) 46 (2013), 1005–1022.

[2] M. Einsiedler and T. Ward, *Ergodic Theory with a View Towards Number Theory*, Grad. Texts in Math. 259, Springer London, London, 2011.

[3] B. Green and T. Tao, *The quantitative behaviour of polynomial orbits on nilmanifolds*, Ann. of Math. (2) 175 (2012), 465–540.

[4] B. Host and B. Kra, *Nil-Bohr sets of integers*, Ergodic Theory Dynam. Systems 31 (2011), 113–142.

[5] A. Y. Khinchin, *Continued Fractions*, Dover Publ., Mineola, NY, 1997.

[6] A. N. Khovanskii, *The Application of Continued Fractions and Their Generalizations to Problems in Approximation Theory*, Noordhoff, Groningen, 1963.

[7] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20; Corrigendum, 168.

[8] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, 2006.

Jakub Konieczny
Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road, Oxford, OX2 6GG, U.K.
E-mail: jakub.konieczny@gmail.com