MATH 568 ANALYTIC NUMBER THEORY I.
CHAPTER 21

21.1. **Uniform Distribution.** Given an $\alpha \in \mathbb{R}$ we define

$$\|\alpha\| = \min_{n \in \mathbb{Z}} |\alpha - n|$$

to be the distance of α from a nearest integer. Note that $\|\alpha\|$ is periodic with period 1, and satisfies the triangle inequality $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$.

The central theme in the previous chapter can be interpreted as the question of how small we can make the quantity $\|\alpha q\|$, measured in terms of the size of q, or alternatively, what is the size of $\min_{q \leq Q} \|\alpha q\|$ for large Q? One can look at various generalizations of this, and several of the multidimensional versions can be studied through the use of the geometry of numbers. One can also ask about the general distribution of αq. In other words, given β, how small can we make $\|\alpha q-\beta\|$? By Dirichlet's theorem, or the continued fraction algorithm, we know that for any given α there are integers c and s with $s>0$ such that $|\alpha-c/s|<s^{-2}$ and that if α is irrational, then there are arbitrarily large such s. Now let

$$b=\lfloor \beta s\rfloor$$

and choose q so that

$$cq\equiv b \pmod{s}, \quad 0<q\le s.$$

Then $(cq-b)/s\in\mathbb{Z}$ and so

$$\begin{aligned}\|\alpha q-\beta\| &= \|\alpha q-\beta-cq/s+b/s\|\\ &= \|(\alpha-c/s)q-(\beta s-\lfloor \beta s\rfloor)/s\|\\ &\le qs^{-2}+s^{-1}\\ &\le 2/s.\end{aligned}$$

Thus, at least when α is irrational, we can find q so that $\|\alpha q-\beta\|$ is arbitrarily small, i.e. the quantities $\alpha q-\beta$ are dense modulo 1.

It turns out that we can say something more precise than this, as when α is irrational we can show that the sequence $\|\alpha q\|$ is very regularly distributed. With this in mind we define the concept of uniform distribution modulo 1 as follows.

Definition The real sequence α_n is *uniformly distributed modulo* 1 when for every sub-interval $I = [a, b)$ of $[0, 1)$ with $b \geq a$ the limit

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ \alpha_n - \lfloor \alpha_n \rfloor \in I}}^{N} 1$$

exists and equals the length of I, $b - a$.

In particular, when α_n is uniformly distributed modulo 1, then for each real number β and each positive real number ε there are infinitely many n such that $\|\alpha_n - \beta\| < \varepsilon$.

The concept was first studied systematically in a seminal paper by Herman Weyl in 1916, and much of analytic number theory has benefited from the underlying ideas in this paper.

One useful observation that we can make imediately is that by taking $\beta_n = \alpha_n - \lfloor \alpha_n \rfloor$, it suffices to consider sequences whose members lie in $[0,1)$].

There are two general criteria for uniform distribution modulo 1, both stemming from Weyl.

Theorem 21.1 (First Criterion)**.** *Suppose that $0 \le \alpha_n < 1$. Then the sequence α_n is uniformly distributed modulo 1 if and only if for each function f Riemann integrable on $[0,1]$ we have*

$$\frac{1}{N}\sum_{n=1}^{N} f(\alpha_n) \to \int_0^1 f(\alpha)d\alpha \quad \text{as } N \to \infty, \tag{21.1}$$

Proof. First suppose that (21.1) holds. Let I be any interval $[a,b)$ and let f be the characteristic function of the interval. Then the left hand side of (21.1) is

$$\frac{1}{N}\sum_{\substack{n=1\\ \alpha_n-\lfloor\alpha_n\rfloor\in I}} 1$$

and the right hand side is $b-a$.

Second suppose that α_n is uniformly distributed modulo 1. Let f be any Riemann integrable function on $[0,1]$, so that, in particular, f is bounded on $[0,1]$. We can approximate arbitrarily closely to

$$\int_0^1 f(\alpha)d\alpha$$

by upper and lower sums. Thus for each $\varepsilon > 0$ there is a dissection

$$0 = a_0 < a_1 < \ldots < a_{M-1} < a_M = 1$$

of $[0,1]$ and step functions defined by

$$f^{\pm}(\alpha) = c_m^{\pm} \quad \alpha \in [a_{m-1}, a_m),$$
$$f^{\pm}(a_M) = c_M^{\pm},$$

where

$$c_m^{\pm} = \pm \sup_{[a_{m-1},a_m]} (\pm f(\alpha)),$$

such that

$$f^-(\alpha) \le f(\alpha) \le f^+(\alpha)$$

and

$$\int_0^1 \left| f^+(\alpha) - f^-(\alpha) \right| d\alpha < \varepsilon.$$

Since $\{\alpha_n\}$ is uniformly distributed modulo 1,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ \alpha_n \in [a_{m-1}, a_m)}}^{N} f^{\pm}(\alpha_n) = c_m^{\pm}(a_m - a_{m-1}).$$

Thus

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f^{\pm}(\alpha_n) = \sum_{m=1}^{M} c_m^{\pm}(a_m - a_{m-1})$$
$$= \int_0^1 f^{\pm}(\alpha) d\alpha.$$

Therefore

$$0 \leq \limsup_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \pm \big(f^{\pm}(\alpha_n) - f(\alpha_n) \big)$$
$$\leq \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \big(f^{+}(\alpha_n) - f^{-}(\alpha_n) \big) < \varepsilon.$$

Hence we have the chain of inequalities

$$\begin{aligned}
\int_0^1 f(\alpha)d\alpha - \varepsilon &\le \int_0^1 f^-(\alpha)d\alpha \\
&\le \liminf_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\alpha_n) \\
&\le \limsup_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\alpha_n) \\
&\le \int_0^1 f^+(\alpha)d\alpha \\
&\le \int_0^1 f(\alpha)d\alpha + \varepsilon.
\end{aligned}$$

This is true for every $\varepsilon > 0$, and so the integral, the lim sup and the lim inf are all equal. □

The above criterion is quite useful, but the following, second criterion, is much more so and has been the basis for a good deal of important work. Indeed the underlying idea is central to much of analytic number theory. There are also important repercussions in harmonic analysis, ergodic theory and dynamical systems.

Throughout we use the notation $e(\beta)$ to denote $\exp(2\pi i\beta)$.

Theorem 21.2 (The Weyl Criterion)**.** *Suppose that α_n is a real sequence. Then it is uniformly distributed modulo 1 if and only if for every $h \in \mathbb{Z}\backslash\{0\}$ we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(h\alpha_n) = 0. \tag{21.2}$$

Proof. The proof in one direction is immediate from the first criterion since

$$\int_0^1 e(h\alpha)d\alpha = 0$$

when $h \neq 0$. There are various ways of proving this in the opposite direction. One way is to observe that if (21.1) holds for continuous functions f on $[0, 1]$, then we can deduce the uniform distribution modulo 1 for the sequence α_n by taking for a given interval $I = [a, b)$ upper and lower continuous approximations $f^{\pm}$ to the characteristic function of I. For example we can take

$f^-(\alpha)$ to be 1 when $a+\varepsilon \le \alpha \le b-\varepsilon$, to be 0 when $\alpha \notin I$ and elsewhere take the obvious line segments which make f continuous and then f^- will minorise the characteristic function. This with a similar definition for a majorant shows that the upper and lower limits of $\frac{1}{N}\sum_{n=1,\ \alpha_n-\lfloor\alpha_n\rfloor\in I}^{N} 1$ as $N \to \infty$ differ from $b-a$ by at most ε, and letting $\varepsilon \to 0$ gives the desired conclusion. One then has to deduce (21.1) for continuous f from (21.2), and to do this one needs to know that the set of trigonometric polynomials $\sum_{h=-H}^{H} c_h e(h\alpha)$ is dense in the space of periodic continuous functions, and this in turn requires some knowledge of the basic elements of the theory of Fourier series.

A second line of approach is to use directly the Fourier series for the characteristic function $\chi_I(\alpha)$ of $I = [a,b)$, where $0 \le a \le b < 1$. Note that

$$\chi_I(\alpha) = s(\alpha-a) - s(\alpha-b) + b - a$$

where $s(\alpha) = \alpha - \lfloor\alpha\rfloor - \frac{1}{2} = \{\alpha\} - \frac{1}{2}$ is the function of Lemma 1 of Appendix D. This gives

$$\chi_I(\alpha) = b - a + \sum_{h=-H}^{H} \frac{e(-ha) - e(-hb)}{2\pi i h} e(h\alpha) + O\left(\min\{1, H^{-1}\|\alpha - a\|^{-1}\}\right) + O(\left(\min\{1, H^{-1}\|\alpha - b\|^{-1}\}\right) . \tag{21.3}$$

The error term here is a continuous function of α and can itself be expanded as a Fourier series (see Theorem 2 of the appendix), and this is absolutely convergent. In fact

$$\min\{1, H^{-1}\|\alpha\|^{-1}\} = \frac{2}{H}\log\frac{eH}{2} + \sum_{h=-\infty}^{\infty} c_h e(h\alpha)$$

with the c_h satisfying for $h \neq 0$,

$$c_h = \int_{1/H}^{1/2} \frac{e(h\alpha) - e(-h\alpha)}{H\alpha^2 2\pi i h} d\alpha$$

and so

$$c_h \ll \min\left\{\frac{1}{|h|}, \frac{H}{h^2}\right\}.$$

Now one sees that for $K \geq H$

$$\frac{1}{N}\sum_{n=1}^{N}\chi_I(\alpha_n) - (b-a)$$
$$\ll \sum_{0<|h|\leq K} \frac{|S_N(h)|}{|h|} + \frac{\log(2H)}{H} + \sum_{|h|>K} \frac{H}{h^2}$$
$$\ll \sum_{0<|h|\leq K} \frac{|S_N(h)|}{|h|} + \frac{\log(2K)}{\sqrt{K}}$$

where

$$S_N(h) = \frac{1}{N}\sum_{n=1}^{N} e(h\alpha_n).$$

The result follows from this - pick $\varepsilon > 0$. Then pick, say, $K = \varepsilon^{-3}$ and then take N large enough that for each h with $0 < |h| \leq K$ one has $|S(h)| < \varepsilon$. $\square$

Something interesting one can see in this proof is that the upper bound for

$$\frac{1}{N}\sum_{n=1}^{N}\chi_I(\alpha_n) - (b-a)$$

above is independent of I. Also one can extend the result by periodicity to $\mathbb{R}$. For example if $-1 < a < 0 \leq b < 1$ one can think of I as being $[0, b) \cup [1 + a, a)$ and apply the previous bound twice. Thus if we define the discrepancy D_N of $\{\alpha_n\}$ by

$$D_N(a, b) = \frac{1}{N} \sum_{\substack{n=1 \\ \alpha_n \in I \pmod 1}}^{N} 1 - (b - a) \tag{21.4}$$

and

$$\overline{D}_N = \sup_{a \leq b \leq a+1} |D_N(a, b)| \tag{21.5}$$

we have just shown that

$$\overline{D}_N \ll \sum_{0 < |h| \leq K} \frac{|S_N(h)|}{|h|} + \frac{\log(2K)}{\sqrt{K}}$$

21.2. **The Erdős-Turán Inequality.** This not sharp, and there is a sharper version of this known as the Erdős-Turán inequality. This is obtained by refining the above argument, by using the Féjer kernel

$$F_H(\alpha) = \frac{1}{H} \left| \sum_{h=1}^{H} e(h\alpha) \right|^2$$

directly rather than the general theory of Fourier series or by using Selberg's so called "magic functions".

Theorem 21.3 (Erdős-Turán, 1948). *Whenever α_n is a real sequence and $0 \le b \le 1$ we have*

$$\bar{D}_N(b) \ll \frac{1}{H} + \sum_{h=1}^{H} \left(\frac{1}{H} + \frac{|\sin(\pi h b)|}{h} \right) |S_N(h)| . \tag{21.6}$$

In particular

$$\bar{D}_N \le 120 \left(\frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h} |S_N(h)| \right) . \tag{21.7}$$

In practice, one does not use the Weyl criterion itself because in applications one usually needs a quantitative bound. Thus one requires something similar to the Erdős-Turán inequality, anyway. It is essentially best possible, but we now have very good values known in place of the implicit constant, in fact we know that

$$|D_N(a,b)| \leq \frac{1}{H+1} + 2\sum_{h=1}^{H}\left(\frac{1}{H+1} + \min\left(b-a, \frac{1}{\pi h}\right)\right)|S_N(h)|,$$

and this has been obtained via Selberg's *magic functions* and their allies (see R. C. Baker, *Diophantine Approximation*, Chapter 2, or H. L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series, Vol. 84, Chapter 1).

Before embarking on the proof of Theorem 21.1 we investigate some of the simple properties of the Féjer kernel.

1. $F_H(\alpha) \geq 0$.

2. By writing the modulus squared sum as the sum times its complex conjugate and collecting togher those terms which contribute to a general term $e(j\alpha)$ we see that we are simply counting the number of h_1, h_2 with $1 \leq h_i \leq H$ and $h_1 - h_2 = j$. By symmetry we may suppose the $j \geq 0$ and then the

number of pairs h_1, h_2 is the number of h_2 with $1 \le h_2 \le H - j$, i.e $H - j$. Thus it follows that

$$F_H(\alpha) = \frac{1}{H}\sum_{j=-H}^{H}(H-|j|)e(j\alpha) = \sum_{j=-H}^{H}\left(1 - \frac{|j|}{H}\right)e(j\alpha).$$

3. $\int_0^1 F_H(\alpha)d\alpha = 1$.

4. The sum $\sum_{h=1}^{H} e(h\alpha)$ is the sum of a geometric progression with common ratio $e(\alpha)$. Thus, when α is not an integer its sum is $(e((H+1)\alpha) - e(\alpha))/(e(\alpha) - 1)$. Thus

$$F_H(\alpha) = \frac{(\sin(\pi H\alpha))^2}{H(\sin(\pi\alpha))^2}.$$

21. We have $|\sin(\pi\alpha)| \ge 2\|\alpha\|$. Thus

$$F_H(\alpha) \le \frac{1}{4H\|\alpha\|^2}.$$

6. If $H\|\alpha\| \le \frac{1}{2}$, then $|\sin(\pi H\alpha)| \ge 2H\|\alpha||$, and $|\sin(\pi\alpha)| \le \pi\|\alpha\|$. Thus

$$F_H(\alpha) \ge \frac{4H}{\pi^2} \quad \left(\|\alpha\| \le \frac{1}{2H}\right).$$

Before proceeding with the proof of the Erdős-Turán inequality we establish a special case.

Lemma 21.4. *Suppose that a is any real number and H is a positive integer. Then*

$$\sum_{\substack{n=1 \\ \alpha_n \in [a, a+1/H) \pmod 1}}^{N} \frac{1}{N} \le \frac{\pi^2}{4H} + \frac{\pi^2}{2H} \sum_{h=1}^{H} |S_N(h)|.$$

Proof. By property 6 above, the expression

$$\frac{\pi^2}{4H} F_H\left(\alpha_n - a - \frac{1}{2H}\right)$$

is greater than or equal to 1 whenever α_n is counted in the sum on the left. Thus, by property 1 above the expression we wish to estimate is bounded by

$$\frac{\pi^2}{4H} \sum_{n=1}^{N} \frac{1}{N} F_H\left(\alpha_n - a - \frac{1}{2H}\right)$$

and by property 2 this is

$$\frac{\pi^2}{4H} + \frac{\pi^2}{4H} \sum_{\substack{h=-H \\ h \ne 0}}^{H} \left(1 - \frac{|h|}{H}\right) S_N(h) e\left(-ha - \frac{h}{2H}\right)$$

and the lemma follows from this. □

We now turn to the proof of the Erdős-Turán inequality, Theorem 21.4.

Proof. We begin by observing that we may suppose that $H > 16$, for the bound is trivial for $H \le 16$.

For general real a and b with $a \in \mathbb{R}$ and $0 \le b \le 1$, we estimate the expression

$$J = \int_0^1 D_N(a+\alpha, a+b+\alpha)F_H(\alpha)d\alpha$$

in two different ways. First we insert the definition of D_N and appeal to property 4. We integrate term by term. The expression $-b$ in D_N when integrated against F_H gives $-b$ by property 3. The remainder of D_N when integrated against the constant term 1 in F_H contributes b. Thus it remains to consider

$$\int_0^1 \sum_{\substack{n=1 \\ \alpha_n \in [a+\alpha, a+b+\alpha) \pmod 1}}^N \frac{1}{N} \sum_{\substack{j=-H \\ j\ne 0}}^H \left(1 - \frac{|j|}{H}\right) e(j\alpha)d\alpha.$$

Here the result of integrating term by term contributes

$$\sum_{n=1}^N \frac{1}{N} \sum_{\substack{j=-H \\ j\ne 0}}^H \left(1 - \frac{|j|}{H}\right) \frac{e(j(\alpha_n - b - a)) - e(j(\alpha_n - a))}{2\pi i j}$$

and so we may conclude that

$$|J| \le \sum_{h=1}^{H} \frac{2|\sin(\pi hb)|}{\pi h} |S_N(h)|. \qquad (21.8)$$

By property 3,

$$\int_0^1 D_N(a, a+b) F_H(\alpha) d\alpha = D_N(a, a+b).$$

Let

$$K = \int_0^1 \left(D_N(a+\alpha, a+b+\alpha) - D_N(a, a+b)\right) F_N(\alpha) d\alpha.$$

Then

$$D_N(a, a+b) = J - K. \qquad (21.9)$$

By property 5, the contribution to K from the α with $\frac{8}{H} \le \|\alpha\| \le \frac{1}{2}$ is bounded by

$$4\bar{D}_N(b) \int_{8/H}^{1/2} \frac{1}{4H\beta^2} d\beta \le \frac{1}{2} \bar{D}_N(b). \qquad (21.10)$$

It remains to consider the α with $\|\alpha\| \le \frac{8}{H}$ and by periodicity we may suppose that $|\alpha| \le \frac{8}{H}$. There are several different cases, but typically $D_N(a+\alpha, a+b+\alpha) - D_N(a, a+b)$ can be written as a difference such as

$D_N(a+b, a+b+\alpha) - D_N(a, a+\alpha)$ where the two terms correspond to two intervals of length $|\alpha|$. Thus for $c = a$, or $a+b$, or $a-|\alpha|$, or $a+b-|\alpha|$,

$$|D_N(a+\alpha, b+\alpha) - D_N(a,b)| \leq \sum_{\substack{n=1 \\ \alpha_n \in [c, c+|\alpha|) \pmod 1}}^{N} \frac{1}{N} + |\alpha|.$$

We can divide each of these intervals of length $|\alpha|$ in the sum on the right into at most 8 subintervals of length at most $1/H$ and by the lemma each one of these will contribute at most

$$\frac{\pi^2}{4H}\left(1 + 2\sum_{h=1}^{H} |S_N(h)|\right).$$

Thus

$$|D_N(a+\alpha, b+\alpha) - D_N(a,b)| \leq \frac{4\pi^2}{H}\left(1 + 2\sum_{h=1}^{H} |S_N(h)|\right) + \frac{8}{H}.$$

Having bounded this part of the integrand in K in this way we can then extend the interval of integration to a unit interval and appeal to property 3 once more. Thus, by (21.12),

$$|K| \le \frac{1}{2}\bar{D}_N(b)+\frac{4\pi^2}{H}\left(1+2\sum_{h=1}^{H}|S_N(h)|\right)+\frac{8}{H}.$$

Hence, by (21.10) and (21.11),

$$|D_N(a,a+b)| \le \frac{1}{2}\bar{D}_N(b)+\frac{4\pi^2+8}{H} + \sum_{h=1}^{H}\left(\frac{8\pi^2}{H}+\frac{2|\sin(\pi hb)|}{\pi h}|S_N(h)|\right).$$

This holds uniformly for all $a \in \mathbb{R}$ and so we can choose a so that $|D_N(a,b)|$ is arbitrarily close to $\bar{D}_N(b)$. Thus

$$\frac{1}{2}\bar{D}_N(b) \le \frac{4\pi^2+8}{H}+\sum_{h=1}^{H}\left(\frac{4\pi^2}{H}+\frac{2|\sin(\pi hb)|}{\pi h}|S_N(h)|\right).$$

□

21.3. **Polynomials.** We have already seen that when α is irrational the sequence $n\alpha - \lfloor n\alpha \rfloor$ is everywhere dense. Now we are in a position to give a simple proof that $n\alpha$ is uniformly distributed. It suffices to consider the sum

$$S_N(h) = \frac{1}{N}\sum_{n=1}^{N} e(hn\alpha)$$

when $h \neq 0$. This is the sum of a geometric progression, and since α is irrational, $h\alpha$ is never an integer. Thus

$$S_N(h) = \frac{e(h(N+1)\alpha) - e(h\alpha)}{N(e(h\alpha)-1)}$$

so that

$$|S_N(h)| \le \frac{1}{N|\sin(\pi h\alpha)|}$$

and plainly for each fixed $h \neq 0$ this tends to 0 as $N \to \infty$. Thus we have just established

Theorem 21.5. *Suppose that α is irrational. Then the sequence $n\alpha$ is uniformly distributed modulo* 1*.*

One can ask the same question with regard to the sequence $p(n)$ where $p(n)$ is a polynomial of degree $d \ge 1$. It is clear that if the only irrational coefficient is the constant term, then the polynomial cannot be uniformly distributed. On the other hand if $p(0) = 0$ and the polynomial is uniformly distributed, then so is $p(n)+\beta$ for any given β since the property is translation invariant. Thus we can concentrate on polynomials with $p(0) = 0$. When $d = 1$ the conclusion is immediate from Theorem 21.2. However, when $d \geq 2$ one immediately runs in to the problem that there is no longer any simple formula for the corresponding exponential sums $S_N(h)$. Weyl solved this difficulty with a simple device. This is based on the observation that for any fixed j the polynomial $p(n + j) - p(n)$ is a polynomial in n of degree $d-1$. More generally one can establish the following theorem.

Theorem 21.6 (van der Corput, 1931). *Suppose that α_n is a real sequence such that for each fixed non-zero integer j the sequence $\alpha_{n+j}-\alpha_n$ is uniformly distributed modulo 1. Then the sequence α_n is uniformly distributed modulo 1.*

Proof. Proof Suppose that $\sigma(n)$ is a sequence of complex numbers with $|\sigma(n)| \leq 1$, and let H denote a positive integer. Then

$$H\sum_{n=1}^{N}\sigma(n) = \sum_{m=1}^{N}\sum_{h=1}^{H}\sigma(n)$$

$$\int_0^1 \sum_{m=1}^{N+H} e(-m\beta)\sum_{n=1}^{N}\sum_{j=1}^{H}\sigma(n)e(n\beta+j\beta)d\beta$$

as can be seen readily by the observation that the integral picks out precisely those terms in the multiple sum for which $m = n+j$ and for any one pair n, j in the given ranges there is exactly one m which meets this requirement. We apply Schwarz's inequality to this.

Thus $\left|H\sum_{n=1}^{N}\sigma(n)\right|^2 \le$

$$\left(\int_0^1\left|\sum_{m=1}^{N+H} e(m\beta)\right|^2 d\beta\right)\times$$
$$\left(\int_0^1\left|\sum_{n=1}^{N}\sigma(n)e(n\beta)\sum_{j=1}^{H}e(j\beta)\right|^2 d\beta\right)$$

We have

$$\left|\sum_{j=1}^{H}e(j\beta)\right|^2 = \sum_{k=-H}^{H}(H-|k|)e(\beta k).$$

Replacing k by $-j$ gives

$$\left|H\sum_{n=1}^{N}\sigma(n)\right|^2 \le$$
$$(N+H)\sum_{j=-H}^{H}(H-|j|)\int_0^1\left|\sum_{n=1}^{N}\sigma(n)e(n\beta)\right|^2 e(-j\beta)d\beta$$

$$\left|H\sum_{n=1}^{N}\sigma(n)\right|^2 \le$$

$$(N+H)\sum_{j=-H}^{H}(H-|j|)\int_0^1\left|\sum_{n=1}^{N}\sigma(n)e(n\beta)\right|^2 e(-j\beta)d\beta$$

$$=(N+H)\sum_{j=-H}^{H}(H-|j|)\sum_{m=1}^{N}\sum_{\substack{n=1\\ n=m-j}}^{N}\sigma(m)\overline{\sigma}(n).$$

The terms with $j=0$ contribute at most

$$(N+H)H\sum_{n=1}^{N}|\sigma(n)|^2 \le (N+H)HN.$$

Thus

$$\left|\frac{1}{N}\sum_{n=1}^{N}\sigma(n)\right|^2 \le$$

$$\frac{1}{H}+\frac{1}{N}+2\left(\frac{1}{H}+\frac{1}{N}\right)\sum_{j=1}^{H}\left|\frac{1}{N}\sum_{n=1}^{N-j}\sigma(n+j)\bar{\sigma}(n)\right|.$$

For the terms with $j>0$ this is clear. For the terms with $j<0$ we replace j by $-j$ and interchange the letters m and j and observe that $\overline{\sigma(n)\overline{\sigma}(n+j)} = \sigma(n+j)\overline{\sigma}(n)$.

$$\left|\frac{1}{N}\sum_{n=1}^{N}\sigma(n)\right|^2 \leq$$

$$\frac{1}{H}+\frac{1}{N}+2\left(\frac{1}{H}+\frac{1}{N}\right)\sum_{j=1}^{H}\left|\frac{1}{N}\sum_{n=1}^{N-j}\sigma(n+j)\bar{\sigma}(n)\right|.$$

We now take $\sigma(n) = e(h\alpha_n)$. Since for each fixed j, $\alpha_{n+j} - \alpha$ is uniformly distributed modulo 1, for each fixed H the all the terms except the first have limit 0 as $N \to \infty$. Thus the limit superior of the left hand side as $N \to \infty$ is at most H^{-1}. But this holds for every positive integer H. Thus

$$\frac{1}{N}\sum_{n=1}^{N} e(h\alpha_n) \to 0 \text{ as } N \to \infty$$

and so by the Weyl criterion once more we have the desired conclusion. □

The technique utilised in the proof of the previous theorem is sometimes known as Weyl differencing, but van der Corput was the first to find a way of limiting the size of the difference parameter j.

The following theorem is an easy deduction from the previous two by induction on the degree.

Theorem 21.7. *Suppose that $p(n)$ is a polynomial of degree $d \geq 1$ with leading coefficient irrational. Then the sequence $p(n)$ $n = 1, 2 \ldots$ is uniformly distributed modulo 1.*

The conclusion also holds if any of the coefficients are irrational.

Theorem 21.8. *Suppose that $p(n)$ is a polynomial of degree $d \geq 1$ with any coefficient, except the constant term, irrational. Then the sequence $p(n)$ $n = 1, 2 \ldots$ is uniformly distributed modulo 1.*

Proof. Write the polynomial as $p(n) = \alpha_0 + \alpha_1 n + \cdots \alpha_d n^d$. Choose D maximal so that the coefficient of n^D is irrational and let $Q(n) = \sum_{k=D+1}^{d} a_k n^k$ and $R(n) = \sum_{k=0}^{D} a_k n^k$, so that $P(n) = R(n) + Q(n)$. Then the coefficients of Q are rational and the leading coefficient of R is irrational. Choose the natural number q so that $qQ(n)$ has rational coefficients and for any a with $0 \le a < 1$ consider $P(qn+a)$. Then $Q(qn+a)-Q(a)$ is an integer and $P(qn+a) \equiv R(qn+a)+Q(a) \pmod 1$. Moreover $R(qn+a)$ has an irrational leading coefficient so is uniformly distributed modulo 1. Hence so is $R(qn+a)+Q(a)$, whence so is $P(qn+a)$. Since this holds for every a it holds for $P(n)$. □

We can also use the Erdős-Turán Theorem to give quantitative bounds. The earliest of these is due to Vinogradov.

Theorem 21.9 (Vinogradov, 1927?)**.** *Suppose that α is irrational and β is any real number, and let ε be any positive number. Then there are infinitely many integers n such that*

$$\|\alpha n^2 + \beta\| < n^{\varepsilon - \frac{1}{2}}.$$

Before proceeding with the proof of Vinogradov's result we establish some useful lemmas. The first one is established by using ideas which we have already explored in exercises earlier in the term, but for completness I include the proof here. The condition on α that it can be approximated in this way is easily met in applications by an appeal to Dirichlet's theorem or the theory of continued fractions.

Lemma 21.10. *Suppose that a and q are integers with $q \geq 1$, $\gcd(a,q) = 1$ and $|\alpha - a/q| \leq q^{-2}$, and suppose that X and Y are real numbers with $X \geq 1$, $Y \geq 1$. Then*

$$\sum_{x \leq X} \min\left(Y, \|\alpha x\|^{-1}\right) \ll \left(\frac{XY}{q} + X + Y + q\right) \log(2q).$$

Proof. Proof The sum in question can be split up in to at most $Xq^{-1}+1$ sub sums in which the x, for some non-negative integer k, lies in the interval $kq < x \leq (k+1)q$. It suffices, therefore, to show that the contribution from such an interval is

$$\ll Y + q\log(2q).$$

Let $\beta = \alpha - a/q$. Then for such an x we have $x = kq + y$ with $1 \le y \le q$, and so

$$\begin{aligned}\alpha x &= ak + \frac{a}{q}y + \beta kq + \beta y\\ &= ak + \frac{ay + \lfloor \beta kq \rfloor}{q} + \frac{\beta kq - \lfloor \beta kq \rfloor}{q} + \beta y.\end{aligned}$$

The expression $ay + \lfloor \beta kq \rfloor$ runs through a complete set of residues modulo q as y does. Thus apart from those five choices of y for which this expression is 0, ± 1 or ± 2 modulo q we have

$$\|\alpha x\| \ge \frac{1}{3}\|(ay + \lfloor \beta kq \rfloor)/q\|.$$

Thus the contribution from the x in the interval under consideration is at most

$$5Y + \sum_{j=1}^{q-1} 3\|jq^{-1}\|^{-1} \ll Y + q\log(2q)$$

as required. □

We now use the above lemma to get a good quantitative bound for the average of the exponential sum which is relevant to Vinogradov's theorem.

Lemma 21.11. *Suppose that H an N are integers and that a and q are integers with $q \geq 1$, $\gcd(a, q) = 1$ and $|\alpha - a/q| \leq q^{-2}$. Then for each positive number ε we have*

$$\sum_{h=1}^{H} \left| \sum_{n=1}^{N} e(\alpha h n^2) \right| \ll \left(HNq^{-\frac{1}{2}} + HN^{\frac{1}{2}} + (Hq)^{\frac{1}{2}} \right) (HN)^{\varepsilon}.$$

Proof. Proof We use Weyl differencing in its classical form. We may certainly suppose that $q \leq HN^2$ for otherwise the conclusion is trivial.

Let S denote the expression we wish to estimate. Then, by Cauchy's inequality we have

$$|S|^2 \leq H \sum_{h=1}^{H} \left| \sum_{n=1}^{N} e(\alpha h n^2) \right|^2.$$

We square out the inner sum to obtain

$$\sum_{n=1}^{N} \sum_{m=1}^{N} e\left(\alpha h(m^2 - n^2)\right)$$

and put $m = n + j$. The sum over j has range $1 - n$ to $N - n$. Now we interchange the order of summation

$$\sum_{j=1-n}^{N-1} \sum_{n} e\left(\alpha h(2nj + j^2)\right)$$

where the inner summation is now over those n with $1 \le n \le N$ and $1 - j \le n \le N - j$. Now we have a geometric progression which we can sum. For $j = 0$ the inner sum is N, and when $j \ne 0$ it is bounded by $\min(N, \|2\alpha hj\|^{-1})$. Thus

$$|S|^2 \ll H^2N + H \sum_{h=1}^{H} \sum_{j=1}^{N} \min\left(N, \|2\alpha hj\|^{-1}\right).$$

By standard estimates for the divisor function the double sum here is

$$\ll (HN)^{\varepsilon} \sum_{k=1}^{2HN} \min\left(N, \|\alpha k\|^{-1}\right).$$

Hence, by the previous lemma

$$|S|^2 \ll H^2N + (HN)^{2\varepsilon} H \left(HN^2q^{-1} + HN + q\right)$$

amd the lemma follows □

Proof of Theorem 21.9. Let $\varepsilon > 0$ and apply Dirichlet's Theorem or the theory of continued fractions to obtain integers a and q

with $\gcd(a,q) = 1$, $q > q_0(\varepsilon)$ and $|\alpha - a/q| \le q^{-2}$. Now take $N = q$, $a = -\beta$, $b = N^{\varepsilon-\frac{1}{2}}$, let δ be a positive number, sufficiently small in terms of ϵ and put $H = n^{\frac{1}{2}-\delta}$. By (21.7) and (21.8) we find that

$$|D_N(a,b)| \ll H^{-1} + b\sum_{h=1}^{H}\left|\frac{1}{n}\sum_{n=1}^{N} e(\alpha h n^2)\right|$$

and by the last lemma this is

$$\begin{aligned}&\ll N^{\delta-\frac{1}{2}} + bHN^{-\frac{1}{2}}(HN)^{\frac{1}{4}\delta}\\ &\ll N^{\delta-\frac{1}{2}} + bN^{-\frac{1}{2}\delta}\end{aligned}$$

and this is small by comparison with b. □

There is a localised version of this due to Heilbronn.

Theorem 21.12 (Heilbronn, 1948)**.** *Let α be any real number and let ε be a positive real number. Then for every large natural number N we have*

$$\min_{1\le n\le N} \|\alpha n^2\| < N^{\epsilon-\frac{1}{2}}.$$

At first sight it would seem desirable ot extend this to the whole real line as in the previous theorem. However, by constructing certain irrational numbers α whose continued fraction convergents converge very rapidly one can ensure that the corresponding inequality really does occur very infrequently.

We require an extension of Lemma 21.3, which again utilises an idea seen earlier in an exercise.

Lemma 21.13. *Suppose that α is a real number, that ε is a positive real number and that a and q are integers with $q \ge 1$, $\gcd(a,q) = 1$ and $|\alpha - a/q| \le q^{-2}$. Let*

$$\Delta = (q + HN^2|\alpha q - a|)^{1/2}.$$

Then,

$$\sum_{h=1}^{H} \left| \sum_{n=1}^{N} e(\alpha h n^2) \right| \ll \left(\frac{HN}{\Delta} + HN^{\frac{1}{2}} + H^{\frac{1}{2}}\Delta \right) (HN)^{\varepsilon}.$$

Proof. Choose a, q as stated. When $HN^2|\alpha q - a| \le q$, then the conclusion is immediate from Lemma 21.3. Thus we may suppose that

$$HN^2|\alpha q - a| > q. \tag{21.11}$$

Let $Q = \left\lfloor 2|\alpha q - a|^{-1} \right\rfloor$. By Dirichlet's theorem there are b and r with $1 \le r \le Q$ and $|\alpha r - b| \le (Q+1)^{-1}$. Now either $b/r = a/q$, whence $\alpha = a/q = b/r$ which contradicts (21.13), or $1/(qr) \le |\alpha - a/q| + |\alpha - b/r|$ and the second term here does not exceed $(2r)^{-1}|\alpha q - a| \le 1/(2qr)$. Thus $\frac{1}{2}|\alpha q - a|^{-1} \le r \le Q$ Now we apply Lemma 21.3 with a, q replaced by b and r. Hence

$$\sum_{h=1}^{H} \left| \sum_{n=1}^{N} e(\alpha h n^2) \right| \ll \left(HNr^{-\frac{1}{2}} + HN^{\frac{1}{2}} + (Hr)^{\frac{1}{2}} \right) (HN)^{\varepsilon}$$

and the lemma follows once more. □

Proof. Proof of Theorem 21.6 Let δ denote a positive number which is small comapared with ε and put $H = N^{\frac{1}{2}-\delta}$. By Dirichlet's theorem we may choose a and q with $q \ge 1$, $\gcd(a, q) = 1$, $|\alpha - a/q| \le \frac{1}{qHN}$ and $q \le$

HN. Let $b = N^{\varepsilon-\frac{1}{2}}$. Then, by Lemma 21.4, the right hand side of (21.8) is

$$\ll \frac{1}{H}+bN^{\frac{1}{2}\delta}\left(\frac{H}{(q+HN^2|\alpha q-a|)^{\frac{1}{2}}}+HN^{-\frac{1}{2}}\right).$$

If $q+HN^2|\alpha q-q|>H^2N^{3\delta}$, then we are done. Suppose not. Then $q\le H^2N^{3\delta}$ and $|\alpha q-a|<HN^{-2+3\delta}$. Thus

$$\|\alpha q^2\|<H^3N^{2-6\delta}=N^{3\delta-\frac{1}{2}}$$

and we are done anyway! □

Zaharescu (1995?) has improved the exponents in Theorems 21.5 and 21.6 to $\frac{2}{3}$ and $\frac{4}{7}$ respectively.