Lecture 4. The method of van der Corput. Diophantine approximation

M. Klazar

March 15, 2024

I continue my survey of G. Tenenbaum's book [13]. In the fourth lecture we cover the last two chapters of part I on elementary methods, Chapter I.6. *The method of van der Corput* and Chapter I.7. *Diophantine approximation*, up to page 169.

Chapter I.6. The method of van der Corput

In Lecture 1 we encountered estimates of sums with the form $\sum_{a<n\le b} f(n)$ where $f\colon [a,b] \to \mathbb{R}$ and $a < b$ are in $\mathbb{R}$. The method of van der Corput concerns with estimates of the related sums in which $f\colon [a,b] \to S$ where $S = \{z \in \mathbb{C} \mid |z| = 1\}$ is the complex unit circle. It is customary to write them as

$$\sum_{a<n\le b} \mathrm{e}\big(g(n)\big)$$

where $g\colon [a,b] \to \mathbb{R}$ and $\mathrm{e}(t) = \exp(2\pi i t)$, $t \in \mathbb{R}$. *Johannes van der Corput (1890–1975)* was a Dutch mathematician.

For the next Theorem 6.1 in [13], so called Poisson summation formula, one can think of $L^1(\mathbb{R})$ as of the class of functions $f\colon \mathbb{R} \to \mathbb{R}$ that are Riemann-integrable on every interval $[-n,n]$, $n \in \mathbb{N}$, and are such that for some constant $c > 0$ and every $n \in \mathbb{N}$,

$$\int_{-n}^{n} |f| \,\mathrm{d}t \le c\,.$$

For any $f \in L^1(\mathbb{R})$ its Fourier transform is

$$\widehat{f}(\vartheta) = \int_{-\infty}^{+\infty} f(t) \exp(-2\pi i \vartheta t) \,\mathrm{d}t\,.$$

Functions of bounded variation were defined in the first lecture.

Theorem 1 *Let $f \in L^1(\mathbb{R})$. Suppose that the next series converges for every t and that the 1-periodic function*

$$\varphi(t) = \sum_{n\in\mathbb{Z}} f(n+t)$$

is continuous at 0 *and has on* $[0,1]$ *bounded variation. Then the identity*

$$\lim_{N\to\infty}\sum_{|\nu|\le N}\widehat{f}(\nu)=\varphi(0)=\sum_{n\in\mathbb{Z}}f(n)$$

holds.

The following are Theorems 6.2 and 6.3 in [13]; recall that $\mathrm{e}(t)=\exp(2\pi i t)$, $t\in\mathbb{R}$.

Theorem 2 *Let $a<b$ be in $\mathbb{R}$, $f\in\mathcal{C}^1((a,b))$, f' be monotonic and of constant sign on (a,b) and let $m=\inf_{a<t<b}|f'(t)|>0$. Then*

$$\left|\int_a^b \mathrm{e}\big(f(t)\big)\,\mathrm{d}t\right|\le\frac{1}{\pi m}\,.$$

Theorem 3 *Let $a<b$ be in $\mathbb{R}$, $f\in\mathcal{C}^2((a,b))$, f'' be of constant sign on (a,b) and let $r=\inf_{a<t<b}|f''(t)|>0$. Then*

$$\left|\int_a^b \mathrm{e}\big(f(t)\big)\,\mathrm{d}t\right|\le\frac{4}{\sqrt{\pi r}}\,.$$

The following is Theorem 6.4 in [13].

Theorem 4 *Let $a<b$ be in $\mathbb{R}$, $f\in\mathcal{C}^1([a,b])$, f' be monotonic on (a,b) and let $\alpha=\inf_{a<t<b}f'(t)$ and $\beta=\sup_{a<t<b}f'(t)$. Then for every $\varepsilon>0$,*

$$\sum_{a<n\le b}\mathrm{e}\big(f(n)\big)=\sum_{\alpha-\varepsilon<\nu<\beta+\varepsilon}\int_a^b \mathrm{e}\big(f(t)-\nu t\big)\,\mathrm{d}t+O_\varepsilon\big(\log(\beta-\alpha+2)\big)\,.$$

The following are Theorem 6.5 (van der Corput's inequality), Lemma 6.6 (Kusmin–Landau) and Theorem 6.7 (Kusmin–Landau inequality) in [13].

Theorem 5 *Let $a<b$ be in $\mathbb{R}$, $f\in\mathcal{C}^2((a,b))$ and let $\lambda=\lambda(a,b)>0$ be a constant such that $\lambda\ll|f''|\ll\lambda$ on (a,b). Then*

$$\sum_{a<n\le b}\mathrm{e}\big(f(n)\big)\ll(b-a+1)\lambda^{1/2}+\lambda^{-1/2}\,.$$

Lemma 6 *Let $x_1,\ \ldots,\ x_N$ be $N\in\mathbb{N}$ real numbers such that $\vartheta\le x_2-x_1\le\cdots\le x_N-x_{N-1}\le 1-\vartheta$ for some $\vartheta\in(0,\frac{1}{2})$. Then*

$$\left|\sum_{n=1}^{N}\mathrm{e}\big(x_n\big)\right|\le\cot(\pi\vartheta/2)\le 2/(\pi\vartheta)\,.$$

In the next theorem, $\|\cdots\|$ denotes distance to the nearest integer.

Theorem 7 *Suppose that $I \subset \mathbb{R}$ is a bounded interval, $f \in \mathcal{C}^1(I)$, f' is monotonic on I and $\|f'\| \ge \lambda > 0$ on I. Then*

$$\Big|\sum_{n\in I} \mathrm{e}\big(f(n)\big)\Big| \le \frac{2}{\pi\lambda}\,.$$

The following are Lemma 6.8 (Weyl–van der Corput), Theorem 6.9 and Theorem 6.10 (van der Corput) in [13]; $[N] = \{1, 2, \ldots, N\}$.

Lemma 8 *If $N, Q \in \mathbb{N}$ and $z_1, \ldots, z_N$ are in $\mathbb{C}$ then*

$$\Big|\sum_{n=1}^{N} z_n\Big|^2 \le \big(1 + (N-1)/Q\big) \sum_{\substack{q\in\mathbb{Z}\\ |q|<Q}} (1 - |q|/Q) \sum_{n, n+q\in[N]} z_{n+q}\overline{z_n}\,.$$

Theorem 9 *Let $a, b \in \mathbb{Z}$, $b - a = N \in \mathbb{N}$, $I = (a, b]$, $f \in \mathcal{C}^3(I)$ and let $\lambda = \lambda(I) > 0$ be a constants such that $\lambda \ll |f'''| \ll \lambda$ on I. Then*

$$\sum_{n\in I} \mathrm{e}\big(f(n)\big) \ll N\lambda^{1/6} + N^{1/2}\lambda^{-1/6}\,.$$

Theorem 10 *Let $N, R \in \mathbb{N}$, $R \ge 2$, $I \subset [N+1, 2N]$ be a real interval, let $f \in \mathcal{C}^R(I)$ and let $F = F(I) > 0$ be a constant such that for every $r \in [R]$, $FN^{-r} \ll |f^{(r)}| \ll FN^{-r}$ on I. Then, with $u = \frac{1}{2^R-2}$ and $v = \frac{R}{2^R-2}$,*

$$\sum_{n\in I} \mathrm{e}\big(f(n)\big) \ll N\big(N^u F^{-v} + F^{-1}\big)\,.$$

The next Theorem 6.11 (Voronoï, 1903) in [13] is due to G. Voronoï in [14] in 1903; $\tau(n)$ means the number of divisors of $n \in \mathbb{N}$.

Theorem 11 *For $x \ge 2$,*

$$\sum_{n\le x} \tau(n) = x\log x + (2\gamma - 1)x + O\big(x^{1/3}\log x\big)\,.$$

This is a strengthening of the 1849 result of P. Dirichlet (Theorem 2 in Lecture 2). *Georgy F. Voronoy (1868–1908)* was a Russian-Ukrainian mathematician, see [12] for more information on his life. In 1922 in [2], J. van der Corput bounded the error more strongly as

$$O_\varepsilon\big(x^{\varepsilon+33/100}\big)\,.$$

The last four results in Chapter I.6 in [13], Definition 6.12, Theorem 6.13 (Weyl's criterion, 1916) — see [15], Proposition 6.14 and Theorem 6.15 (Erdős–Turán, 1948; Rivat–Tenenbaum, 2005) — see [4] and [9], concern equidistribution modulo 1.

Definition 12 *A sequence* $(u_n) \subset \mathbb{R}$ *(*$n \in \mathbb{N}$*) is equidistributed modulo* 1 *if for any real* $\alpha, \beta \in [0,1)$ *with* $\alpha \le \beta$ *we have for* $N \to \infty$ *that*

$$\big|\{n \in [N] \mid \alpha \le \{u_n\} \le \beta\}\big| = (\beta - \alpha)N + o(N)\,.$$

Here $[N] = \{1, 2, \ldots, N\}$ and $\{\cdots\}$ is the fractional part function.

Theorem 13 *A sequence* $(u_n) \subset \mathbb{R}$ *is equidistributed modulo* 1 *iff one the two following equivalent conditions holds.*

1. *For any function* f *that is Riemann-integrable on* $[0,1]$*,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{u_n\}) = \int_0^1 f(x)\,\mathrm{d}x\,.$$

2. *For any nonzero* $h \in \mathbb{Z}$*,*

$$\lim_{N\to\infty} \underbrace{\frac{1}{N} \sum_{n=1}^{N} \mathrm{e}\big(hu_n\big)}_{\sigma_N(h)} = 0\,.$$

For the next proposition and theorem we also define, for $N \in \mathbb{N}$ and a sequence $(u_n) \subset \mathbb{R}$, the *discrepancy* D_N to be

$$D_N = D_N((u_n)) = \sup_I \big|\,|\{n \in [N] \mid \{u_n\} \in I\}| - |I| \cdot N\,\big|/N\,,$$

where T runs through all subintervals $I \subset [0,1)$. Equidistribution of (u_n) modulo 1 is equivalent with $\lim D_N = 0$.

Proposition 14 *For any nonzero* $h \in \mathbb{Z}$*,* $\sigma_N(h) \le 4|h|D_N$*.*

Theorem 15 *For any* $H \in \mathbb{N}$*,*

$$D_n \le \frac{1}{H+1} + \frac{2}{3} \sum_{h=1}^{H} \frac{|\sigma_N(h)|}{H}\,.$$

Chapter I.7. Diophantine approximation

The following are Theorem 7.1 (Dirichlet) and Corollary 7.2 in [13]; $\|\vartheta\| = \min(\{\vartheta - \lfloor\vartheta\rfloor, \lceil\vartheta\rceil - \vartheta\})$ is the distance of $\vartheta \in \mathbb{R}$ to the nearest integer.

Theorem 16 *Let* $\vartheta \in \mathbb{R}$*. For every* $Q \in \mathbb{N}$*,*

$$\min_{1 \le q \le Q} \|q\vartheta\| \le \frac{1}{Q+1}\,.$$

Corollary 17 *Let $\vartheta \in \mathbb{R}$ and let q run in $\mathbb{N}$. The following three assertions are equivalent:* (i) $\vartheta \in \mathbb{Q}$, (ii) $\exists\, c = c(\vartheta) > 0$ *s. t.* $\|q\vartheta\| > 0 \Rightarrow \|q\vartheta\| \geq c$ *and* (iii) *the double inequality* $0 < q\|q\vartheta\| < 1$ *has only finitely many solutions* q.

By [11] (from this, by now shabby, booklet this author learned Diophantine approximation in 1980's) the previous theorem is due to P. L. Dirichlet in [3] in 1842.

The following are Theorem 7.3 (Liouville) and Corollary 7.4 in [13]. Recall that $z \in \mathbb{C}$ is called algebraic if $p(z) = 0$ for some nonzero polynomial $p \in \mathbb{Q}[x]$, and that else z is called transcendental.

Theorem 18 *Let $\vartheta \in \mathbb{R}$ be algebraic with degree $d \geq 1$. Then there is a constant $c = c(\vartheta) > 0$ such that for every $q \in \mathbb{N}$,*

$$\|q\vartheta\| \neq 0 \Rightarrow \|q\vartheta\| > c/q^{d-1}\,.$$

Corollary 19 *For any integer $a > 1$ the number*

$$\vartheta := \sum_{k \geq 0} a^{-k!}$$

is transcendental.

By [11] the last theorem is due to J. Liouville in [7] in 1844.

The following is Proposition 7.5 in [13];

$$D^{+}(\vartheta) := \{q \geq 2 \mid \|q\vartheta\| < \min_{1 \leq m < q} \|m\vartheta\|\}$$

are record holders in the discipline of Diophantine approximation of ϑ.

Proposition 20 $D^{+}(\vartheta)$ *is finite* $\iff$ $\vartheta \in \mathbb{Q}$.

The following is Definition 7.6 in [13]. Let $\{\vartheta\} = \vartheta - \lfloor \vartheta \rfloor \in [0, 1)$ be the fractional part of $\vartheta \in \mathbb{R}$. We set $z(\vartheta) = 0$ if $\{\vartheta\} \leq \frac{1}{2}$, and $z(\vartheta) = 1$ else.

Definition 21 *For $\vartheta \in \mathbb{R}$, the finite or infinite sequence*

$$D'(\vartheta) = (q_j)_{j > z(\vartheta)} = (q_j(\vartheta))_{j > z(\vartheta)}$$

is the increasing ordering of $D^{+}(\vartheta)$. The sequence $D(\vartheta)$ arises from $D'(\vartheta)$ by prefixing it $q_0 = 1$ if $z(\vartheta) = 0$, and $q_0 = q_1 = 1$ if $z(\vartheta) = 1$.

The following is Proposition 7.7 in [13].

Proposition 22 *Any sequence $D'(\vartheta)$ strictly increases. If $k > z(\vartheta)$ and if $\|q_k\vartheta\| \neq 0$ then k is not the last index in $D'(\vartheta)$ and $\|q_k\vartheta\| \leq 1/q_{k+1}$.*

The following is Definition 7.8 in [13].

Definition 23 *For $\vartheta \in \mathbb{R}$ and $k > z(\vartheta)$ we denote by p_k the integer closest to $q_k\vartheta$. The sequence $(p_k/q_k)_{k\geq 0}$ is called the sequence of convergents of ϑ.*

The following are Proposition 7.9, Lemma 7.10, Theorem 7.11 and Corollary 7.12 in [13]; we set $\vartheta_k = q_k\vartheta - p_k$.

Proposition 24 *If $\vartheta \in \mathbb{Q}$ then $\vartheta = p_k/q_k$ where k is the last index in $D(\vartheta)$. If $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$ then $\lim_{k\to\infty} p_k/q_k = \vartheta$.*

Lemma 25 *For any $\vartheta \in \mathbb{R}$ and any k, if ϑ_k and ϑ_{k+1} are nonzero then they have opposite signs.*

Theorem 26 *Let $\vartheta \in \mathbb{R}$. If $1 \leq k < |D(\vartheta)|$ then*

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k \,.$$

Corollary 27 *The convergents are in lowest terms: we have $(p_k, q_k) = 1$ for all $k \geq 0$.*

The following are Theorem 7.13, Definition 7.14, Theorem 7.15, Proposition 7.16 and Theorem 7.17 in [13]; ϑ_k is defined above.

Theorem 28 *Let $\vartheta \in \mathbb{R}$, $(p_{-2}, q_{-2}) = (0, 1)$, $(p_{-1}, q_{-1}) = (1, 0)$ and $a_k = \lfloor -\vartheta_{k-2}/\vartheta_{k-1} \rfloor$ for $k \in \mathbb{N}_0$. Then for $k \in \mathbb{N}_0$ (assuming $\vartheta_{k-1} \neq 0$),*

$$p_k = a_k p_{k-1} + p_{k-2} \quad \text{and} \quad q_k = a_k q_{k-1} + q_{k-2} \,.$$

Definition 29 *The numbers a_k in the previous theorem are called incomplete quotients (of the continued fraction expansion of ϑ). The numbers $\alpha_k = -\frac{\vartheta_{k-2}}{\vartheta_{k-1}}$ are called complete quotients (...).*

Theorem 30 *Let $\vartheta \in \mathbb{R}$. We have $\alpha_0 = \vartheta$ and $\alpha_{k+1} = 1/\{\alpha_k\}$ for $k \in \mathbb{N}_0$. For $k < |D(\vartheta)|$,*

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}} =: [a_0,\, a_1,\, \ldots,\, a_k] \,.$$

Proposition 31 *Let $k \in \mathbb{N}_0$, $a_0 \in \mathbb{R}$, $a_1, \ldots, a_{k-1} > 0$ and $x > 0$ be real. Then*

$$[a_0,\, a_1,\, \ldots,\, a_{k-1},\, x] = \frac{x p_{k-1} + p_{k-2}}{x q_{k-1} + q_{k-2}}$$

where $(p_{-2}, q_{-2}) = (0, 1)$, $(p_{-1}, q_{-1}) = (1, 0)$ and for $k \in \mathbb{N}_0$ the pairs (p_k, q_k) follow the recurrence in Theorem 28.

Theorem 32 *Let $r/s \in \mathbb{Q}$ with $s \in \mathbb{N}$ be nonzero and in lowest terms. Then*

$$\frac{r}{s} = [a_0, \ldots, a_N]$$

where $r = a_0 s + r_1$, $s = a_1 r_1 + r_2$, $\ldots$, $r_{N-2} = a_{N-1} r_{N-1} + r_N$, $r_{N-1} = a_N r_N$ are divisions with remainders, i.e., $0 \le r_1 < s$, $0 \le r_2 < r_1$, $\ldots$, $0 \le r_N < r_{N-1}$.

The following are Proposition 7.18 and Theorems 7.19–7.21 in [13].

Proposition 33 *Let $\vartheta \in \mathbb{R}$. For $k < |D(\vartheta)|$,*

$$[a_0, a_1, \ldots, a_k] = a_0 + \sum_{j=0}^{k-1} \frac{(-1)^j}{q_j q_{j+1}} .$$

Theorem 34 *With the convention that $a_k \ge 2$ when $\vartheta \in \mathbb{Q}$ and $k = |D(\vartheta)| - 1$, the continued fraction expansion is unique, i.e., for each real ϑ the integers a_j, $0 \le j \le k$, are uniquely determined by the formula in Theorem 30.*

Furthermore, for any (infinite) sequence $(a_n) \subset \mathbb{Z}$ $(n = 0, 1, \ldots)$ such that $a_j \ge 1$ for $j \ge 1$, the sequence

$$\big([a_0, a_1, \ldots, a_k]\big), \ k = 0, 1, \ldots ,$$

converges.

Theorem 35 *Let (F_k) $(k = 0, 1, \ldots)$ be the Fibonacci sequence. For all $\vartheta \in \mathbb{R}$ and $k \in \mathbb{N}$,*

$$q_k \ge F_k = \frac{1}{\sqrt{5}}\big(\varphi^k - (-1)^k/\varphi^k\big) ,$$

with equality when $\vartheta = \varphi = (1 + \sqrt{5})/2$.

Theorem 36 *Let $\vartheta \in \mathbb{R}$ and $k \in \mathbb{N}_0$. If $\|q_k \vartheta\| \ne 0$ then*

$$\vartheta - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\alpha_{k+1} q_k + q_{k-1})}.$$

In particular,

$$\frac{1}{q_k(q_{k+1} + q_k)} < \left|\vartheta - \frac{p_k}{q_k}\right| \le \frac{1}{q_k q_{k+1}} .$$

The following are Corollary 7.22, Theorem 7.23 (Lagrange's criterion), Corollary 7.24 and Theorem 7.25 (Girard–Fermat) in [13].

Corollary 37 *If $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$ then*

$$\frac{1}{2 + \limsup_{k\to\infty} a_k} \le \liminf_{q\to\infty} q\|q\vartheta\| \le \frac{1}{\limsup_{k\to\infty} a_k} .$$

Theorem 38 *Let $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$. Then p/q is a convergent of ϑ iff there exist integers $p' < p$, $q' < q$ and a real number $\alpha > 1$ such that $qp' - pq' = \pm 1$ and*

$$\vartheta = \frac{\alpha p + p'}{\alpha q + q'} .$$

Corollary 39 *For any irrational $\vartheta \in \mathbb{R}$ if $|\vartheta - p/q| < 1/(2q^2)$ then p/q is a convergent of ϑ.*

Theorem 40 *Let p be a prime congruent to 1 modulo 4. Then there exist integers r and s such that $p = r^2 + s^2$.*

Finally, the following are Definition 7.26 and Theorems 7.27 and 7.28 in [13].

Definition 41 *We say that $\vartheta, \vartheta' \in \mathbb{R} \setminus \mathbb{Q}$ are equivalent if for some $m, n \in \mathbb{N}_0$,*

$$\vartheta = [a_0, \dots, a_m, c_0, c_1, \dots] \text{ and } \vartheta' = [b_0, \dots, b_n, c_0, c_1, \dots] .$$

Theorem 42 *Two numbers $\vartheta, \vartheta' \in \mathbb{R} \setminus \mathbb{Q}$ are equivalent iff*

$$\vartheta' = \frac{a\vartheta + b}{c\vartheta + d}$$

for some integers $a, \dots, d$ with $ad - bc = \pm 1$.

Theorem 43 *A number $\vartheta \in \mathbb{R}$ is a quadratic irrationality iff its continued fraction (expansion) is ultimately periodic.*

By [11, p. 26], implication $\Leftarrow$ was proven by L. Euler in [5] in 1737, and the opposite implication is due to J. L. Lagrange in [6] in 1770.

References

[1] J. G. van der Corput, Zahlentheoretische Abschätzungen, *Math. Ann.* **8?** (1921), 53–79

[2] J. G. van der Corput, Verschärferung der Abschätzung beim Teilproblem, *Math. Ann.* **87** (1922), 39–65

[3] L. G. P. Dirichlet, Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen, *S. B. Preuss. Akad. Wiss.* (1842), 93–95

[4] P. Erdős and P. Turán, On a problem in the theory of uniform distribution I, II, *Indag. Math* **10** (1948), 370–378, 406–413

[5] L. Euler, De fractionibus continuis, *Comentarii Acad. Sci. Imperiali Petropoloitanae* **9** (1737)

[6] J. L. Lagrange, Addition au memoire la resolution des equations numeriques, *Mem. Berl.* **24** (1770)

[7] J. Liouville, Sur des classes très-étendues de quantités dont la irrationelles algébriques, *C. R. Acad. Sci. Paris* **18** (1844), 883–885 & 910–911

[8] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge University Press, Cambridge, UK 2007

[9] J. Rivat and G. Tenenbaum, Constantes d'Erdős–Turán, *The Ramanujan J.* **9** (2005), 111–121

[10] W. M. Schmidt, *Diophantine Approximation*, Springer-Verlag, Berlin 1980

[11] V. Shmidt, *Diofantovy priblizheniya*, Mir, Moskva 1983 (translation of [10] by V. G. Chirsky, revised by A. B. Shidlovsky)

[12] H. Syta and Rien van de Weygaert, Life and Times of Georgy Voronoi, arXiv:0912.3269, 2009, 30 pp.

[13] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, AMS, Providence, RI 2015 (Third Edition)

[14] G. Voronoï, Sur un problème de calcul des fonctions asymptotiques, *J. reine angew. Math.* **126** (1903), 241–282

[15] H. Weyl, Über die Gleichverteilung von Zahlen mod. Eins, *Math. Ann.* **77** (1916), 313–404