Six exponentials Theorem – irrationality

Michel Waldschmidt

Let p, q, r be three multiplicatively independent positive rational numbers and u a positive real number such that the three numbers p^u, q^u, r^u are rational. Then u is also rational. We prove this result by introducing a parameter L and a square $L \times L$ matrix, the entries of which are functions $(p^{s_1}q^{s_2}r^{s_3})^{(t_0+t_1u)x}$. The determinant $\Delta(x)$ of this matrix vanishes at a real point $x \neq 0$ if and only if u is rational. From the hypotheses, it follows that $\Delta(1)$ is a rational number; one easily estimates a denominator of it. An upper bound for $|\Delta(1)|$ follows from the fact that the first $L(L-1)/2$ Taylor coefficients of $\Delta(x)$ at the origin vanish.

This text is mainly an english translation by the author of his paper published in French in the Revue de la Filière Mathématiques-RMS http://www.rms-math.com with the title *Le théorème des six exponentielles restreint à l'irrationalité*, RMS, avril 2021, 131ème année, N.3, 2020-2021, 26-33.

Michel Waldschmidt is a French mathematician, specialist of number theory, in particular Diophantine problems, which includes transcendental number theory. He is now emeritus professor at Sorbonne University.

Our goal is to give a complete elementary proof of the following result:

Theorem. *Let p, q, r be three positive rational numbers which are multiplicatively independent, namely, the only relation $p^aq^br^c = 1$ with integers a, b, c is for $a = b = c = 0$. Let u be a real number such that p^u, q^u and r^u are rational numbers. Then u is a rational number.*

Recall that for $x > 0$ and $u \in \mathbb{R}$, $x^u = \exp(u \log x)$.

This statement is a special case of the six exponentials Theorem, where the assumption that p, q, r and x^u are rational is replaced with the assumption that they are algebraic (and u may be a complex number). More information on this result from transcendental number theory is available in [KKT, Lan, Lau, R, W1, W2] for instance.

From the fundamental Theorem of arithmetic, it follows that any three distinct prime numbers are multiplicatively independent. One easily checks that if u is a rational number and p a prime number such that p^u is rational, then u is an integer. Examples with an irrational u and a prime number p with p^u an integer n are obtained with $u = (\log n)/(\log p)$. We do not know whether there exist an irrational u and two multiplicatively independent rational numbers p and q with p^u and q^u rational numbers: proving that there is no such example is the four exponentials Conjecture for irrationality, so far it is an open problem. Writing $p^u = r$ and $q^u = s$, we would get

$$u = \frac{\log r}{\log p} = \frac{\log s}{\log q}\cdot$$

The problem is to prove that a 2×2 matrix

$$\begin{pmatrix} \log p & \log q \\ \log r & \log s \end{pmatrix}$$

has a rank 2 when p, q, r, s are positive rational numbers with multiplicatively independent p, q and multiplicatively independent p, r.

A consequence of the Theorem is the following statement:

Corollary. *If u is a positive real number such that x^u is a rational number for each positive rational number x, then u is an integer.*

In his paper *Transcendental numbers* [H], Heini Halberstam quotes the following special case of the above corollary:

> *If u is a positive real number such that x^u is an integer for each positive integer x, then u is an integer.*

According to Halberstam: *This result appeared as a problem in the 1972 Putnam Prize competition, and not one of more than*

2000 university student competitors gave a solution; the solution, though not hard, could well elude even a professional mathematician for several hours (or days). The reference to Putnam is *32nd Putnam 1971 question A6* https://prase.cz/kalva/putnam/putn71.html. A proof of this special case, using the calculus of finite differences, is given in [H] — see also [W1, Chapter I Exercise 6, p. I-12 — I-13] and [KKT]. It might be interesting to find a similar proof of the above corollary.

Here is the idea of the proof of the Theorem. Given that the six numbers p, q, r, p^u, q^u and r^u are rational. Then the three functions of a real variable p^x, q^x and r^x take rational values at all points of the form $\xi_{\underline{t}} = t_0 + t_1 u$ with $\underline{t} = (t_0, t_1) \in \mathbb{Z}^2$. For $\underline{s} = (s_1, s_2, s_3) \in \mathbb{Z}^3$, the same is true for the function $f_{\underline{s}}(x) = (p^{s_1} q^{s_2} r^{s_3})^x$. Select a sufficiently large integer N (we will make this assumption explicit at the end of the proof). Set $S = N^2$, $T = N^3$, $L = N^6$, so that $L = S^3 = T^2$. The determinant [1]

$$\Delta = \det\Big(f_{\underline{s}}(\xi_{\underline{t}}) \Big)_{\substack{0 \le s_j < S \\ 0 \le t_i < T}}$$

is a rational number. Let D be a common denominator of p, q, r, p^u, q^u and r^u. Since $s_j \ge 0$ and $t_i \ge 0$ are integers, the numbers

$$D^{6ST} f_{\underline{s}}(\xi_{\underline{t}}) = (Dp)^{s_1 t_0} (Dq)^{s_2 t_0} (Dr)^{s_3 t_0} (Dp^u)^{s_1 t_1} (Dq^u)^{s_2 t_1} (Dr^u)^{s_3 t_1}$$

are integers, hence $D^{6LST}\Delta$ is a rational integer. We will produce an upper bound for $|\Delta|$, in particular, for sufficiently large N, we will check $|\Delta| < D^{-6LST}$, hence $\Delta = 0$. And we will show that the condition $\Delta = 0$ implies that u is rational.

Let us start by proving this last claim. The condition $\Delta = 0$ means that there are rational numbers $a_{\underline{s}}$, not all of which are zero, such that the function

$$F(x) = \sum_{s_1=0}^{S-1} \sum_{s_2=0}^{S-1} \sum_{s_3=0}^{S-1} a_{\underline{s}} f_{\underline{s}}(x)$$

satisfies

$$F(\xi_{\underline{t}}) = 0 \quad \text{for} \quad 0 \le t_0, t_1 < T. \tag{1}$$

[1] This determinant is well defined up to its sign, depending on the ordering of the $\underline{s}$ and of the $\underline{t}$.

Since p, q, r are multiplicatively independent, the three numbers $\log p, \log q, \log r$ are $\mathbb{Q}$–linearly independent. Using the next lemma for

$$\{w_1, \ldots, w_n\} = \{s_1 \log p + s_2 \log q + s_3 \log r \mid 0 \leq s_1, s_2, s_3 < S\}$$

with $n = L$, we deduce that the conditions (1) imply that the numbers $\xi_{\underline{t}}$ are not all distinct, hence u is a rational number.

Lemma 1. *Let $w_1, \ldots, w_n$ be pairwise distinct real numbers and $a_1, \ldots, a_n$ real numbers, not all of which are zero. Then the number of real zeroes of the function*

$$F(x) = a_1 \mathrm{e}^{w_1 x} + \cdots + a_n \mathrm{e}^{w_n x}$$

is $\leq n - 1$.

Proof. We use the following result, known as Rolle Theorem (1691)[2]: *if a real function of a real variable of class C^1 (continuously derivable) has at least m real zeroes, then its derivative has at least $m - 1$ zeroes.*

We prove Lemma 1 by induction on n. The statement is true for $n = 1$: the function $a_1 \mathrm{e}^{w_1 x}$ has no zero. Assume that the result holds for $n - 1$ for some $n \geq 2$. Assume also, without loss of generality, that $a_1, \ldots, a_{n-1}$ are not all zero. The derivative $G(x)$ of the function $\mathrm{e}^{-w_n x} F(x)$ can be written

$$G(x) = a_1(w_1 - w_n)\mathrm{e}^{(w_1 - w_n)x} + \cdots + a_{n-1}(w_{n-1} - w_n)\mathrm{e}^{(w_{n-1} - w_n)x}$$

with coefficients $a_1(w_1 - w_n), \ldots, a_{n-1}(w_{n-1} - w_n)$, not all of which are zero, while in the exponent $w_1 - w_n, \ldots, w_{n-1} - w_n$ are pairwise distinct. From the inductive hypothesis, we deduce that $G(x)$ has at most $n - 2$ zeroes. From Rolle Theorem it follows that $\mathrm{e}^{-w_n x} F(x)$, hence also $F(x)$, has at most $n - 1$ zeroes. □

It remains only to estimate $|\Delta|$ from above. The upper bound will not use arithmetic assumptions: it holds also when the numbers

[2] Already stated by Bhāskarācārya (Bhāskara II, 1114 - 1185).

p, q, r, p^u, q^u and r^u are not assumed to be rational, only real numbers.

We introduce the function

$$\Psi(x) = \det\Big(f_{\underline{s}}(\xi_{\underline{t}}x)\Big)_{\substack{0\le s_j<S\\ 0\le t_i<T}},$$

so that $\Delta = \Psi(1)$. We expand the determinant and write

$$\Psi(x) = \sum_{\sigma\in\mathfrak{S}_L} \epsilon(\sigma)\mathrm{e}^{w_\sigma x},$$

where $\mathfrak{S}_L$ is the set with $L!$ elements which are the bijective maps $\sigma : \underline{s} \to (t_{0,\sigma(\underline{s})}, t_{1,\sigma(\underline{s})})$ from the set of $\underline{s} = (s_1, s_2, s_3)$ $(0 \le s_j < S$, $j = 1, 2, 3)$ onto the set of $\underline{t} = (t_0, t_1)$, $(0 \le t_i < T$, $i = 1, 2)$, $\epsilon(\sigma)$ is the signature of σ (depending on the order which was chosen for the $\underline{s}$ and the $\underline{t}$), and, for $\sigma \in \mathfrak{S}_L$,

$$w_\sigma = \sum_{s_1=0}^{S-1}\sum_{s_2=0}^{S-1}\sum_{s_3=0}^{S-1}(s_1 \log p + s_2 \log q + s_3 \log r)(t_{0,\sigma(\underline{s})} + t_{1,\sigma(\underline{s})}u).$$

We will use the upper bound

$$|w_\sigma| \le LST(1 + u)\log(pqr). \tag{2}$$

We write the Taylor expansion at the origin of ψ:

$$\Psi(x) = \sum_{m\ge 0} \alpha_m x^m.$$

The next Lemma shows that

$$\alpha_0 = \alpha_1 = \cdots = \alpha_{M-1} = 0$$

with $M = L(L - 1)/2$.

Let us recall that an analytic function at 0 is the sum in a neighbourhood of 0 of a convergent series: this series is the Taylor expansion of the function at the origin.

Lemma 2. *Let $f_1, \ldots, f_L$ be analytic functions at 0 and $\xi_1, \ldots, \xi_L$ be complex numbers. The Taylor expansion at the origin of the function*

$$F(x) = \det\Big(f_\lambda(\xi_\mu x)\Big)_{1\le\lambda,\mu\le L},$$

say

$$F(x) = \sum_{m \geq 0} \alpha_m x^m,$$

satisfies

$$\alpha_0 = \alpha_1 = \cdots = \alpha_{M-1} = 0.$$

Proof. From the multilinearity of the determinant, it is sufficient to prove this lemma when each $f_\lambda(x)$ is a monomial x^{n_λ}. If the determinant

$$\det\Big((\xi_\mu x)^{n_\lambda}\Big)_{1 \leq \lambda, \mu \leq L} = x^{n_1+n_2+\cdots+n_L} \det\Big(\xi_\mu^{n_\lambda}\Big)_{1 \leq \lambda, \mu \leq L}$$

is not zero, then $n_1, \ldots, n_L$ are pairwise distinct, hence

$$n_1 + n_2 + \cdots + n_L \geq 0 + 1 + \cdots + (L-1) = M.$$

□

In order to prove the expected upper bound for $|\Delta|$, we introduce an auxiliary parameter $R > 1$; we will choose $R = \mathrm{e}$, the basis of the Napierian logarithms, but any constant > 1 would do.

Lemma 3. *Let $w_1, \ldots, w_J$, $a_1, \ldots, a_J$ be real numbers. If the Taylor expansion at the origin of the function*

$$F(x) = \sum_{j=1}^{J} a_j \mathrm{e}^{w_j x},$$

say

$$F(x) = \sum_{m \geq 0} \alpha_m x^m,$$

has

$$\alpha_0 = \alpha_1 = \cdots = \alpha_{M-1} = 0,$$

then

$$|F(1)| \leq R^{-M} \sum_{j=1}^{J} |a_j| \mathrm{e}^{|w_j| R}.$$

Proof. We have

$$F(x) = \sum_{j=1}^{J} a_j \sum_{m\geq 0} \frac{w_j^m}{m!} x^m = \sum_{m\geq 0} \sum_{j=1}^{J} a_j \frac{w_j^m}{m!} x^m,$$

hence

$$\alpha_m = \sum_{j=1}^{J} a_j \frac{w_j^m}{m!}$$

and

$$|\alpha_m| \leq \sum_{j=1}^{J} |a_j| \frac{|w_j|^m}{m!}.$$

Therefore

$$\begin{aligned} |F(1)| = \left| \sum_{m\geq M} \alpha_m \right| &\leq \sum_{m\geq M} |\alpha_m| \leq R^{-M} \sum_{m\geq M} |\alpha_m| R^m \\ &\leq R^{-M} \sum_{m\geq M} \sum_{j=1}^{J} |a_j| \frac{|w_j|^m}{m!} R^m \leq R^{-M} \sum_{j=1}^{J} |a_j| \mathrm{e}^{|w_j|R}. \end{aligned}$$

□

Thanks to Lemma 2, we can use the upper bound given by Lemma 3 for the function Ψ with $J = L!$ and $a_j \in \{-1, 1\}$; since $\Psi(1) = \Delta$, we deduce from (2):

$$|\Delta| \leq R^{-M} L! (pqr)^{LST(1+u)R}.$$

It remains to check

$$L!(pqr)^{LST(1+u)R} D^{6LST} < R^M \tag{3}$$

for sufficiently large N. Recall the choice of parameters

$$L = N^6, \quad S = N^2, \quad T = N^3, \quad M = \frac{1}{2} L(L-1).$$

One checks that the condition (3) is satisfied with $R = \mathrm{e}$ as soon as

$$N > 12 \log D + 2\mathrm{e}(1+u) \log(pqr) + 1.$$

Comments. Where does this determinant Δ comes from? There is a long history behind it. The transcendence proofs originate in the proof by Hermite of the transcendence of the number e; they have been developed since 1873 by many a mathematician, including Siegel, Lang and Ramachandra, who are at the origin of the six exponentials Theorem. The first occurence of this Theorem is in a paper by Alaoglu and Erdős [AE] on Ramanujan highly composite numbers, where they also study superabundant and colossaly abundant numbers. They asked Siegel whether it was true that the conditions that p^u and q^u are integers with p and q distinct primes imply that u is an integer. Siegel replied that he did not know how to prove such a result (which is still an open problem nowadays), but that he knew how to get the conclusion if one added r^u, like in the Theorem.

> [AE, p. 449] *This question leads to the following problem in Diophantine analysis. If p and q are different primes, is it true that p^x and q^x are both rational only if x is an integer?*

> [AE, p. 455] *It is very likely that q^x and p^x can not be rational at the same time except if x is an integer. At present we cannot show this. Professor Siegel has communicated to us the result that q^x, r^x and s^x cannot be simultaneously rational except if x is an integer*

The proofs by Lang and Ramachandra are given in [Lan] and [R]. These proofs involve auxiliary functions. To replace these functions with the so–called interpolation determinant Δ is an idea of M. Laurent [Lau, § 6.1]. There is already a similar determinant introduced by Cantor and Straus in their paper [CS] on a Theorem of Dobrowolski dealing with a question of Lehmer. Further references are given in [W1, W2].

The interested reader will compare this proof with the proof in [KKT].

Suggested Reading

[AE] L. Alaoglu & P. Erdös – "On highly composite and similar numbers", *Trans. Amer. Math. Soc.* 56 (1944), p. 448–469.
DOI http://dx.doi.org/10.2307/1990319.

[CS] D. C. Cantor & E. G. Straus – "On a conjecture of D. H. Lehmer", *Acta Arith.* 42 (1982/83), no. 1, p. 97–100, Correction, id. no. 3 p.327.
DOI http://dx.doi.org/10.4064/aa-42-1-97-100.

[H] H. Halberstam – "Transcendental numbers", *Math. Gaz.* 58 (1974), p. 276–284,
DOI https://www.jstor.org/stable/3616099.

[KKT] K.Senthil Kumar& Veekesh Kumar & R.Thangadurai, "On a Problem of Alaoglu and Erdős", *Resonance* (2018), 749–758.
https://www.ias.ac.in/article/fulltext/reso/023/07/0749-0758

[Lan] S. Lang – *Introduction to transcendental numbers*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966.

[Lau] M. Laurent – "Sur quelques résultats récents de transcendance", *Astérisque* (1991), no. 198-200, p. 209–230 (1992); Journées Arithmétiques, Luminy 1989.
https://smf.emath.fr/publications/sur-quelques-resultats-recents-de-transcendance.

[R] K. Ramachandra – "Contributions to the theory of transcendental numbers. I, II", *Acta Arith.* 14 (1967/68), 65-72 and 73–88.
DOI http://dx.doi.org/10.4064/aa-14-1-73-88.

[W1] M. Waldschmidt – *Linear independence of logarithms of algebraic numbers*, IMS Report, vol. 116, Institute of Mathematical Sciences, Madras, 1992, With an appendix by Michel Laurent.
https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/LIL.pdf.

[W2] — , *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften, vol. 326, Springer-Verlag, Berlin, 2000.
DOI http://dx.doi.org/10.1007/978-3-662-11569-5.

Address for correspondence

Michel Waldschmidt

Sorbonne Université, Faculté Sciences et Ingénierie

CNRS, Institut Mathématique de Jussieu Paris Rive Gauche, IMJ-PRG

F – 75005 Paris, France

E-mail: michel.waldschmidt@imj-prg.fr

URL: http://www.imj-prg.fr/~michel.waldschmidt