

April 12 - 23, 2021: Hanoi (Vietnam) (online)
 CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers

Michel Waldschmidt

EXERCISES

Exercise 1. Let $b \geq 2$ be an integer, $(a_n)_{n \geq 0}$ be a bounded sequence of rational integers and $(u_n)_{n \geq 0}$ an increasing sequence of positive integers. Assume that the set $\{n \geq 0 \mid a_n \neq 0\}$ is infinite. Define

$$\vartheta := \sum_{n \geq 0} a_n b^{-u_n}.$$

(a) Assume

$$\limsup_{n \rightarrow \infty} (u_{n+1} - u_n) = \infty.$$

Show that ϑ is irrational.

(b) Assume

$$\limsup_{n \rightarrow \infty} (u_{n+1} - 2u_n) = \infty.$$

Show that ϑ is not a quadratic number.

(c) Assume

$$\limsup_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} > 1.$$

Show that ϑ is transcendental.

(d) Assume

$$\limsup_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} = +\infty.$$

Show that ϑ is a Liouville number.

Exercise 2. Consider the following numbers:

$$S_1 := \sum_{n=1}^{\infty} \frac{1}{n(n+1)}, \quad S_2 := \sum_{n=2}^{\infty} \frac{1}{n^2-1},$$

$$S_3 := \sum_{n=1}^{\infty} \frac{1}{(2n+1)(2n+2)},$$

$$S_4 := \sum_{n \geq 0} \left(\frac{1}{4n+1} - \frac{3}{4n+2} + \frac{1}{4n+3} + \frac{1}{4n+4} \right).$$

Are they rational, algebraic irrational or transcendental?

Exercise 3. Conjecture 2 p. 213 of the Introduction to Chapters X and XI in Lang [ECDA]¹ is the following:

For any $\epsilon > 0$, there exists a constant $C(\epsilon) > 0$ such that, for any nonzero rational integers $a_1, \dots, a_n, b_1, \dots, b_n$ with $a_1^{b_1} \cdots a_n^{b_n} \neq 1$, we have

$$\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right| \geq \frac{C(\epsilon)^n B}{(B_1 \cdots B_n A_1 \cdots A_n)^{1+\epsilon}},$$

where $A_i = \max\{1, |a_i|\}$, $B_i = \max\{1, |b_i|\}$ ($1 \leq i \leq n$) and $B = \max\{B_1, \dots, B_n\}$.

(a) Assuming this conjecture, deduce the following result :

Let $\epsilon > 0$. There exists a constant $C(\epsilon) > 0$ such that for x, y, p, q positive integers satisfying $x^p \neq y^q$, we have

$$|x^p - y^q| > C(\epsilon) \max\{x^p, y^q\}^{1 - \frac{1}{p} - \frac{1}{q} - \epsilon}.$$

(b) Deduce the same estimate (a) from the *abc* Conjecture:

Let $\epsilon > 0$. There exists a constant $\kappa(\epsilon) > 0$ with the following property. Let a, b, c be three positive relatively prime integers satisfying $a + b = c$. Then

$$c < \kappa(\epsilon) \text{Rad}(abc)^{1+\epsilon}.$$

Here, for a positive integer n , the *radical* of n is defined as

$$\text{Rad}(n) = \prod_{p|n} p$$

where the product is over the prime numbers p dividing n .

(c) Let

$$(u_n)_{n \geq 0} = 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, \dots$$

be the sequence² of perfect powers a^b with $a \geq 1$ and $b \geq 2$. Deduce from (a) Pillai's Conjecture: $u_{n+1} - u_n \rightarrow \infty$ as $n \rightarrow \infty$.

Check that Pillai's Conjecture is equivalent to the following statement: for any $k \geq 1$, the equation $x^p - y^q = k$ has only finitely many solutions in positive integers x, y, p, q satisfying $p \geq 2, q \geq 2$.

¹[ECDA] S. LANG, *Elliptic curves: Diophantine analysis*. Grundlehren der Math. Wiss. **231**, Springer-Verlag (1978).

²<http://oeis.org/A001597>

Exercise 4. Show that the only solutions of the equation $2^a + 3^b = 5^c$ in nonnegative integers a, b and c are given by

$$2 + 3 = 5, \quad 2^2 + 1 = 5, \quad 2^4 + 3^2 = 5^2.$$

Remark. *Such equations occur in the theory of finite groups³. This exercise shows that elementary methods sometimes yield very precise results, but only in very specific special cases, using ad hoc arguments; while methods from Diophantine approximation give much more general statements, in a systematic way⁴ - however it is often necessary to complete the results arising from Diophantine approximation with numerical computations.*

Exercise 5. Recall that \mathcal{L} denotes the \mathbb{Q} -vector subspace of \mathbb{C} of all logarithms of all nonzero algebraic numbers:

$$\mathcal{L} = \{\lambda \in \mathbb{C} \mid e^\lambda \in \overline{\mathbb{Q}}\}.$$

(a) The *homogeneous* version of Baker's Theorem on the linear independence of logarithms of algebraic numbers is the following statement:

Let $\lambda_1, \dots, \lambda_n$ be \mathbb{Q} -linearly independent elements of \mathcal{L} . Then $\lambda_1, \dots, \lambda_n$ be $\overline{\mathbb{Q}}$ -linearly independent.

Prove that this theorem is equivalent to the following statement.

Let n be a positive integer and V a vector subspace of \mathbb{C}^n which is rational over $\overline{\mathbb{Q}}$. Then

$$V \cap \mathcal{L}^n = \bigcup_{E \subset V} E \cap \mathcal{L}^n,$$

where E ranges over the vector subspaces of \mathbb{C}^n which are rational over \mathbb{Q} and contained in V .

Recall⁵ that for a subfield K of \mathbb{C} , a vector subspace of \mathbb{C}^n is *rational* over K if it has a basis of elements of K^n ; this is equivalent to saying that it is an intersection of kernels of linear forms with coefficients in K .

(b) The Conjecture on algebraic independence of logarithms of algebraic numbers is the following statement:

³J.L.Brenner & L.L.Foster, *Exponential Diophantine equations*, Pacific J. Math. **101** (1982), 263–301.

⁴D.Z.Mo & R.Tijdeman, *Exponential Diophantine equations with four terms*, Indag. Math. (N.S.) **3** (1992), 47–57.

⁵Exercise 1.4 of [GL326]

M. Waldschmidt *Diophantine approximation on linear algebraic groups*. Grundlehren der Mathematischen Wissenschaften. **326**. Springer, 2000.

<http://dx.doi.org/10.1007/978-3-662-11569-5>

Let $\lambda_1, \dots, \lambda_n$ be \mathbb{Q} -linearly independent elements of \mathcal{L} . Let $P \in \mathbb{Q}[X_1, \dots, X_n]$ be a nonzero polynomial with rational coefficients. Then $P(\lambda_1, \dots, \lambda_n) \neq 0$.

Prove that this conjecture is equivalent to the following conjecture (D. Roy):

For any algebraic subvariety \mathfrak{V} of \mathbb{C}^n defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers,

$$\mathfrak{V} \cap \mathcal{L}^n = \bigcup_{E \subset \mathfrak{V}} E \cap \mathcal{L}^n,$$

where E ranges over the set of vector subspaces of \mathbb{C}^n , rational over \mathbb{Q} , which are contained in \mathfrak{V} .

(c) List the vector subspaces of \mathbb{C}^4 contained in the hypersurface

$$X_1X_4 - X_2X_3 = 0.$$

Which are the ones rational over \mathbb{Q} ?

(d) Recall the *Four Exponentials Conjectures*:

Let x_1, x_2 , be two complex numbers which are linearly independent over \mathbb{Q} . Let y_1, y_2 , be two complex numbers which are linearly independent over \mathbb{Q} . Then one at least of the four numbers

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_2y_1}, e^{x_2y_2}$$

is transcendental.

Deduce the Four Exponentials Conjecture from the Conjecture on algebraic independence of logarithms of algebraic numbers.

Exercise 6. (a) Assuming Schanuel's Conjecture, what is the transcendence degree of the field generated over \mathbb{Q} by the following 31 numbers?

$$e, \pi, e\pi, e + \pi, e^\pi, \pi^e, e^i, \pi^i, e^e, \pi^\pi, e + e^\pi, \pi + e^\pi, \pi e^\pi, e^{\pi^2}, e^{e^e}, \pi^{\pi^\pi},$$

$$e^{\sqrt{2}}, 2^{\sqrt{2}}, 2^\pi, 2^e, e^\pi 2^{\sqrt{3}}, 2^{2^{\sqrt{2}}}, e^{\sqrt{5}} + ie^{\sqrt{7}}, \frac{1}{\pi} \log 3,$$

$$\pi \log 5, \pi + \log 5, 2^{\log 2}, 7^{\log 3}, (\log 2)^{\sqrt{2}}, 2^{\sqrt{2}} 3^{\sqrt{3}}, \log \log 3.$$

(b) Among these 31 numbers, which ones are known to be transcendental?

April 12 - 23, 2021: Hanoi (Vietnam) (online)
 CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers

Michel Waldschmidt

SOLUTIONS OF THE EXERCISES

Solution to Exercise 1.

Any subsequence of a sequence $(u_n)_{n \geq 0}$ satisfying one of the conditions (a) to (d) satisfies the same condition. Hence there is no loss of generality to assume $a_n \neq 0$ for all $n \geq 0$.

Since the sequence u_n is increasing, we have $u_{n+1} \geq u_n + 1$ for all $n \geq 0$, hence $u_{n+k} \geq u_n + k$ for all $n \geq 0$ and $k \geq 0$. Set $A = \max_{n \geq 0} |a_n|$. For $N \geq 1$, set

$$q_N = b^{u_{N-1}} \text{ and } p_N = \sum_{n=0}^{N-1} a_n b^{u_{N-1}-u_n}.$$

We have

$$\left| \sum_{n \geq N+1} a_n b^{-u_n} \right| \leq A \sum_{k \geq 0} b^{-u_{N+k+1}} \leq A \sum_{k \geq 1} b^{-u_{N+1}-k} \leq A b^{-u_{N+1}}.$$

Assume N is sufficiently large, so that

$$b^{u_{N+1}-u_N} > A.$$

Then

$$\left| \sum_{n \geq N+1} a_n b^{-u_n} \right| < \frac{1}{b^{u_N}} \leq \frac{|a_N|}{b^{u_N}},$$

hence

$$\left| \vartheta - \frac{p_N}{q_N} - a_N b^{-u_N} \right| < |a_N| b^{-u_N},$$

which ensures

$$\vartheta \neq \frac{p_N}{q_N}.$$

Also we have

$$0 < \left| \vartheta - \frac{p_N}{q_N} \right| \leq \frac{|a_N|}{b^{u_N}} + \left| \sum_{n \geq N+1} \frac{a_n}{b^{u_n}} \right| < \frac{A+1}{b^{u_N}}.$$

(a) Assume

$$\limsup_{n \rightarrow \infty} (u_{n+1} - u_n) = \infty.$$

We write $b^{u_N} = q_N b^{u_N - u_{N-1}}$. Let $\epsilon > 0$. There exists N satisfying

$$b^{u_N - u_{N-1}} > \frac{A+1}{\epsilon}.$$

From

$$\frac{A+1}{b^{u_N}} < \frac{\epsilon}{b^{u_{N-1}}},$$

we deduce

$$0 < \left| \vartheta - \frac{p_N}{q_N} \right| < \frac{\epsilon}{q_N},$$

which implies that ϑ is irrational.

(b) Assume

$$\limsup_{n \rightarrow \infty} (u_{n+1} - 2u_n) = \infty.$$

We write $b^{u_N} = q_N^2 b^{u_N - 2u_{N-1}}$. Let $\epsilon > 0$. There exists N satisfying

$$b^{u_N - 2u_{N-1}} > \frac{A+1}{\epsilon}.$$

We have

$$\frac{A+1}{b^{u_N}} < \frac{\epsilon}{b^{2u_{N-1}}},$$

hence

$$0 < \left| \vartheta - \frac{p_N}{q_N} \right| < \frac{\epsilon}{q_N^2},$$

which implies that ϑ is not a quadratic number.

(c1) Assume

$$\limsup_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} > 2.$$

We write $b^{u_N} = q_N^{u_N/u_{N-1}}$. There exist $\eta > 2$ and infinitely many N such that $u_N > \eta u_{N-1}$. From

$$0 < \left| \vartheta - \frac{p_N}{q_N} \right| < \frac{2A}{q_N^{u_N/u_{N-1}}} < \frac{2A}{q_N^\eta},$$

using the Thue–Siegel–Roth Theorem, we deduce that ϑ is transcendental.

(c2) Assume

$$\limsup_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} > 1.$$

We write $b^{u_N} = q_N^{u_N/u_{N-1}}$. There exist $\eta > 1$ and infinitely many N such that $u_N > \eta u_{N-1}$. From

$$0 < \left| \vartheta - \frac{p_N}{q_N} \right| < \frac{2A}{q_N^{u_N/u_{N-1}}} < \frac{2A}{q_N^\eta},$$

using Ridout's Theorem, we deduce that ϑ is transcendental.

(d) In the same way, if

$$\limsup_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} = \infty,$$

then for any $\kappa > 0$ there exists N such that $u_N > \kappa u_{N-1}$, hence

$$0 < \left| \vartheta - \frac{p_N}{q_N} \right| < \frac{2A}{q_N^\kappa},$$

and ϑ is a Liouville number. □

Examples

For the sequence $u_n = \lfloor x^n \rfloor$ with $x > 1$, we have $\lim_{n \rightarrow \infty} (u_{n+1} - u_n) = \infty$.

For the sequence $u_n = \lfloor x^n \rfloor$ with $x > 2$, we have $\lim_{n \rightarrow \infty} (u_{n+1} - 2u_n) = \infty$.

For the sequence $u_n = \lfloor 2^{x^n} \rfloor$ with $x > 1$, we have $\lim_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} > 2$.

For the sequence $u_n = \lfloor x^{n!} \rfloor$ with $x > 1$, we have $\lim_{n \rightarrow \infty} \frac{u_{n+1}}{u_n} = \infty$.

Of course, each of the three last lower bounds implies the one above.

Solution to Exercise 2.

The answer is that S_1 and S_2 are rational (telescoping series), S_4 is also rational, while S_3 is transcendental.

1. For $n \geq 1$,

$$\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}.$$

Hence

$$S_1 = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \dots = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \left(\frac{1}{4} - \frac{1}{5}\right) + \dots = 1.$$

2. For $n \geq 2$,

$$\frac{1}{n^2 - 1} = \frac{1}{2} \left(\frac{1}{n-1} - \frac{1}{n+1} \right).$$

Hence

$$2S_2 = \frac{2}{3} + \frac{2}{8} + \frac{2}{15} + \dots + \frac{2}{n^2 - 1} + \dots = \left(1 - \frac{1}{3}\right) + \left(\frac{1}{2} - \frac{1}{4}\right) + \left(\frac{1}{3} - \frac{1}{5}\right) + \left(\frac{1}{4} - \frac{1}{6}\right) + \dots = 1 + \frac{1}{2}.$$

Hence $S_2 = \frac{3}{4}$.

3. For $n \geq 0$,

$$\frac{1}{(2n+1)(2n+2)} = \frac{1}{2n+1} - \frac{1}{2n+2}.$$

Hence

$$\frac{1}{2} + S_3 = \frac{1}{1 \cdot 2} + \frac{1}{3 \cdot 4} + \frac{1}{5 \cdot 6} + \frac{1}{7 \cdot 8} + \dots = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \dots = \log 2$$

$$\text{and } S_3 = \log 2 - \frac{1}{2}.$$

4. Using, for $|z| < 1$, the principal value of the logarithm

$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \frac{z^4}{4} + \dots + \frac{z^{4n+1}}{4n+1} - \frac{z^{4n+2}}{4n+2} + \frac{z^{4n+3}}{4n+3} - \frac{z^{4n+4}}{4n+4} + \dots,$$

we deduce

$$\log(1+z^2) = z^2 - \frac{z^4}{2} + \dots - \frac{z^{4n+2}}{2n+1} + \frac{z^{4n+4}}{2n+2} + \dots$$

Hence, for $|z| < 1$,

$$\sum_{n \geq 0} \left(\frac{z^{4n+1}}{4n+1} - \frac{3z^{4n+2}}{4n+2} + \frac{z^{4n+3}}{4n+3} + \frac{z^{4n+4}}{4n+4} \right) = \log(1+z) - \log(1+z^2).$$

The left hand side and the right hand side has a limit for $z \rightarrow 1$, and this limit is the same (set $z = 1 - \varepsilon$ with $\varepsilon \rightarrow 0$); hence $S_4 = 0$.

□

Remark A consequence of Baker's Theorem on the linear independence, over the field $\overline{\mathbb{Q}}$ of algebraic numbers, of \mathbb{Q} -linearly independent logarithms of algebraic numbers, is the following:

Let $Q \in \mathbb{Q}[X]$ be a polynomial with only simple zeroes, with all its zeroes in the interval $[-1, 0)$. Let P be a polynomial with algebraic coefficients of degree $\geq \deg P + 2$. Then the number

$$\sum_{n \geq 0} \frac{P(n)}{Q(n)}$$

is either zero or transcendental.

The proof ⁶ uses some result of Lehmer ⁷. The example

$$\sum_{n=0}^{\infty} \frac{1}{(n+1)(2n+1)(4n+1)} = \frac{\pi}{3}$$

is given by Lehmer.

⁶Adhikari, S. D. & Saradha, N. & Shorey, T. N. & Tijdeman, R. *Transcendental infinite sums*. Indag. Math. (N.S.) **12** (2001), no. 1, 1–14.

⁷Lehmer, D.H. *Euler constants for arithmetical progressions*. Acta Arith. **27**, 125–142 (1975)

Solution to Exercise 3.

In this solution we use the same letter ϵ , where a formal proof should involve $\epsilon/2, \epsilon/4, \dots$; also the $C(\epsilon)$ should have different indices.

Remark: since $a_i \neq 0$ and $b_i \neq 0$ we have $A_i = |a_i|$ and $B_i = |b_i|$, no need to introduce $\max\{1, \cdot\}$.

Let $\epsilon > 0$ and let x, y, p, q be positive integers satisfying $x^p \neq y^q$. By symmetry we may assume $x^p > y^q$. We may also assume

$$x^p - y^q < \frac{1}{2}x^p$$

and

$$pq > p + q,$$

otherwise the lower bound is obvious.

(a) The Conjecture in [ECDA] with $n = 2$, $a_1 = x$, $a_2 = y$, $b_1 = -p$, $b_2 = q$, $A_1 = x$, $A_2 = y$, $B_1 = p$, $B_2 = q$, $B = \max\{p, q\}$ implies

$$|x^{-p}y^q - 1| \geq \frac{C(\epsilon)^2 B}{(B_1 B_2 A_1 A_2)^{1+\epsilon}}.$$

We have

$$p \log 2 \leq p \log x, \quad q \log 2 \leq q \log y \leq p \log x, \quad B \leq \frac{p \log x}{\log 2} = \frac{\log(x^p)}{\log 2} \leq (x^p)^\epsilon,$$

$$\frac{(B_1 B_2)^{1+\epsilon}}{B} \leq B^{1+\epsilon} \leq (x^p)^\epsilon$$

and $A_2 \leq x^{\frac{p}{q}}$. Hence

$$\frac{(B_1 B_2 A_1 A_2)^{1+\epsilon}}{B} \leq x^{1+\frac{p}{q}+p\epsilon}$$

and therefore

$$x^p - y^q = x^p |x^{-p}y^q - 1| \geq x^p C(\epsilon) x^{-1-\frac{p}{q}-p\epsilon} \geq C(\epsilon) (x^p)^{1-\frac{1}{p}-\frac{1}{q}-\epsilon}.$$

(b) Let $k = x^p - y^q$. Write $x^p = y^q + k$ and let $a = y^q$, $b = k$, $c = x^p$. The radical $R(abc)$ satisfies $R \leq xyk$. The abc Conjecture yields

$$x^p < \kappa(\epsilon) (xyk)^{1+\epsilon}$$

with $xy \leq (x^p)^{\frac{1}{p}+\frac{1}{q}}$. Hence

$$k \geq C(\epsilon) \frac{1}{xy} (x^p)^{1-\epsilon} \geq C(\epsilon) (x^p)^{1-\frac{1}{p}-\frac{1}{q}-\epsilon}.$$

(c) Let $k \geq 1$. Assume x, y, p, q are positive integers with $p \geq 2$, $q \geq 2$ and $x^p - y^q = k$. If $pq > p + q$, then $1 - \frac{1}{p} - \frac{1}{q} \geq \frac{1}{6}$. From

$$x^p - y^q \geq C(\epsilon) (x^p)^{1-\frac{1}{p}-\frac{1}{q}-\epsilon}$$

we deduce

$$y^q < x^p \leq C(\epsilon)k^{6+\epsilon}.$$

Finally if $p = q = 2$ then

$$k = x^2 - y^2 \geq x^2 - (x-1)^2 = 2x - 1$$

and

$$y^2 < x^2 \leq \frac{1}{4}(k+1)^2.$$

A sequence $(v_n)_{n \geq 0}$ of positive real numbers tends to infinity if and only if for each $K > 0$ the set of $n \geq 0$ such that $v_n \leq K$ is finite. Hence a sequence $(v_n)_{n \geq 0}$ of positive integers tends to infinity if and only if for each $k > 0$ the set of $n \geq 0$ such that $v_n = k$ is finite. We apply this remark to the sequence $v_n = u_{n+1} - u_n$ where $(u_n)_{n \geq 0}$ is the sequence of perfect powers. \square

Solution to Exercise 4.

Let a, b, c satisfy $2^a + 3^b = 5^c$. We may assume $c \geq 3$ since for $c = 0, 1, 2$ the solutions are only the obvious ones. Looking at the parity we deduce $a \geq 1$.

From now on we assume $a \geq 1, c \geq 3$.

(a) Consider the special case $a = 1$:

$$2 + 3^b = 5^c$$

with $b \geq 2$. Since $\varphi(9) = 6$, we consider the powers of 5 modulo 9 with the exponents modulo 6:

$c \pmod 6$	0	1	2	3	4	5
$5^c \pmod 9$	1	5	7	8	4	2

From $5^c \equiv 2 \pmod 9$, we deduce $c \equiv 5 \pmod 6$. We also have $\varphi(7) = 6$. We consider the powers modulo 7 with the exponents modulo 6:

$\pmod 6$	0	1	2	3	4	5
$5^c \pmod 7$	1	5	4	6	2	3
$3^b \pmod 7$	1	3	2	6	4	5

From $c \equiv 5 \pmod 6$ we deduce $5^c \equiv 3 \pmod 7$, hence $3^b \equiv 1 \pmod 7$, and consequently $b \equiv 0 \pmod 6$. On the other hand $3^b = 5^c - 2 \equiv 3 \pmod 4$, hence b is odd, a contradiction.

From now on, we assume $a \geq 2$.

(b) Consider the special case $b = 0$:

$$2^a + 1 = 5^c.$$

From $c \geq 3$ we deduce $a \geq 7$. From $2^a \equiv -1 \pmod 5$ we deduce $a \equiv 2 \pmod 4$. Hence a has an odd prime divisor p . We write $a = kp$ with k even > 0 , and

$$5^c = (2^k + 1)(2^{k(p-1)} - 2^{k(p-2)} + \dots - 2^k + 1).$$

Hence $2^k + 1$ is a power of 5. If $k \geq 3$, then $2^k \equiv -1 \pmod{25}$, hence

$$2^{k(p-1)} - 2^{k(p-2)} + \cdots - 2^k + 1 \equiv p \pmod{25}.$$

This yields $p \equiv 0 \pmod{25}$ which is a contradiction with the fact that p is a prime number. If $k \leq 2$, then $k = 2$, the same argument shows $p \equiv 0 \pmod{5}$, hence $p = 5$, $a = 10$; but $2^{10} + 1 = 1025$ is not a power of 5.

From now on, we assume $b \geq 1$.

(c) Consider the special case $a = 3$:

$$8 + 3^b = 5^c.$$

From $c \geq 3$ we deduce $b \geq 5$. The above table for 5^c modulo 9 shows that $c \equiv 3 \pmod{6}$. Write $c = 6\gamma + 3$:

$$3^b = 5^{6\gamma+3} - 8 = (5^{2\gamma+1} - 2)(5^{4\gamma+2} - 2 \cdot 5^{2\gamma+1} + 4),$$

which gives $5^{2\gamma+1} \equiv 2 \pmod{9}$. Hence

$$5^{4\gamma+2} - 2 \cdot 5^{2\gamma+1} + 4 \equiv 4 \pmod{9};$$

this shows that the left hand side is not a power of 3.

(d) Assume a is odd ≥ 5 . We have

$$2^a \equiv \begin{cases} 2 \pmod{5} & \text{if } a \equiv 1 \pmod{4} \\ 3 \pmod{5} & \text{if } a \equiv 3 \pmod{4}. \end{cases}$$

From $2^a + 3^b \equiv 0 \pmod{5}$ we deduce that b is also odd. Both 3 and 5 have order 8 modulo 32. We consider the 3^b and 5^c modulo 32 with the exponent modulo 8 and b odd:

$b \pmod{8}$	1	3	5	7
$3^b \pmod{32}$	3	27	19	11

and

$c \pmod{8}$	0	1	2	3	4	5	6	7
$5^c \pmod{32}$	1	5	25	29	17	21	9	13

It follows that the congruence $3^b \equiv 5^c \pmod{32}$ has no solution with b odd.

(e) The only remaining case is a is even, $a = 2\alpha$. Recall $b \geq 1$ and $a \geq 2$. From $5^c \equiv 4^\alpha \equiv 1 \pmod{3}$ we deduce that c is also even, $c = 2\gamma$. Write

$$(5^\gamma - 2^\alpha)(5^\gamma + 2^\alpha) = 3^b.$$

From $5^\gamma + 2^\alpha \equiv 0 \pmod{3}$ we deduce that α and γ have opposite parity. This implies that $5^\gamma - 2^\alpha$ is not a multiple of 3, hence $5^\gamma - 2^\alpha = 1$ and $5^\gamma + 2^\alpha = 3^b$. Eliminating 5^γ yields

$$2^{\alpha+1} + 1 = 3^b,$$

which shows that α is even, hence ≥ 2 , while γ is odd. From $5^\gamma \equiv 5 \pmod{8}$ and $3^b \equiv 1 \pmod{8}$, it follows that there is no nontrivial solution with a even. \square

Solution to Exercise 5.

(a) We first deduce the homogeneous version of Baker's Theorem from the statement in (a). Let $\underline{\lambda} = (\lambda_1, \dots, \lambda_n)$ be an elements of \mathcal{L}^n with $\lambda_1, \dots, \lambda_n$ linearly dependent over $\overline{\mathbb{Q}}$:

$$\beta_1 \lambda_1 + \dots + \beta_n \lambda_n = 0$$

with $(\beta_1, \dots, \beta_n) \in \overline{\mathbb{Q}}^n \setminus \{0\}$. Let V be the hyperplane of \mathbb{C}^n of equation

$$\beta_1 z_1 + \dots + \beta_n z_n = 0.$$

Since $\underline{\lambda} \in V$ and V is rational over $\overline{\mathbb{Q}}$, the statement in (a) claims that there exists a vector subspace E of \mathbb{C}^n , contained in V (hence $\neq \mathbb{C}^n$), rational over \mathbb{Q} , such that $\underline{\lambda} \in E$. From $E \neq \mathbb{C}^n$ it follows that $\lambda_1, \dots, \lambda_n$ are linearly dependent over \mathbb{Q} .

Conversely, assume the homogeneous version of Baker's Theorem. Let V be a subspace of \mathbb{C}^n rational over $\overline{\mathbb{Q}}$. The inclusion

$$V \cap \mathcal{L}^n \supset \bigcup_{E \subset V} E \cap \mathcal{L}^n$$

is trivial. Let $\underline{\lambda} = (\lambda_1, \dots, \lambda_n) \in V \cap \mathcal{L}^n$. Let μ_1, \dots, μ_r be a basis of the \mathbb{Q} -vector space spanned by the numbers $\lambda_1, \dots, \lambda_n$; write

$$\lambda_i = \sum_{j=1}^r b_{ij} \mu_j \quad (i = 1, \dots, n).$$

Define, for $1 \leq j \leq r$,

$$\underline{b}_j = (b_{1j}, \dots, b_{nj}) \in \mathbb{Q}^n.$$

Let E be the vector subspace of \mathbb{C}^n spanned by $\underline{b}_1, \dots, \underline{b}_r$. From its definition, E is rational over \mathbb{Q} . Also from

$$\underline{\lambda} = \sum_{j=1}^r \mu_j \underline{b}_j$$

we deduce $\underline{\lambda} \in E \cap \mathcal{L}^n$.

By assumption V is the intersection of hyperplanes of \mathbb{C}^n which are rational over $\overline{\mathbb{Q}}$. Let H be such a hyperplane and

$$\beta_1 z_1 + \dots + \beta_n z_n = 0$$

an equation of H , where $(\beta_1, \dots, \beta_n) \in \overline{\mathbb{Q}}^n \setminus \{0\}$. Since $\underline{\lambda} \in V \subset H$, we have

$$\sum_{i=1}^n \beta_i \lambda_i = 0,$$

that is

$$\sum_{i=1}^n \sum_{j=1}^r \beta_i b_{ij} \mu_j = 0.$$

According to the homogeneous version of Baker's Theorem, the numbers μ_1, \dots, μ_r are $\overline{\mathbb{Q}}$ -linearly independent. Hence

$$\sum_{i=1}^n \beta_i b_{ij} = 0 \text{ for } j = 1, \dots, r,$$

which means that $\underline{b}_j \in H$ for $j = 1, \dots, r$, hence $E \subset H$. This is true for all hyperplanes H of \mathbb{C}^n which are rational over $\overline{\mathbb{Q}}$ and contain V , hence $E \subset V$.

(b) We first deduce the conjecture on algebraic independence of logarithms from Roy's Conjecture. Let $\underline{\lambda} = (\lambda_1, \dots, \lambda_n)$ be an elements of \mathcal{L}^n with $\lambda_1, \dots, \lambda_n$ algebraically dependent. Let $P \in \overline{\mathbb{Q}}[X_1, \dots, X_n] \setminus \{0\}$ be such that $P(\lambda_1, \dots, \lambda_n) = 0$. Let \mathfrak{V} be the hypersurface of \mathbb{C}^n of equation $P(z_1, \dots, z_n) = 0$. Since $\underline{\lambda} \in \mathfrak{V}$, Roy's Conjecture claims that there exists a vector subspace E of \mathbb{C}^n , contained in \mathfrak{V} (hence $\neq \mathbb{C}^n$), rational over \mathbb{Q} , such that $\underline{\lambda} \in E$. From $E \neq \mathbb{C}^n$ it follows that $\lambda_1, \dots, \lambda_n$ are linearly dependent over \mathbb{Q} .

Conversely, assume the conjecture on algebraic independence of logarithms. Let \mathfrak{V} be an algebraic subvariety of \mathbb{C}^n defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers. The inclusion

$$\mathfrak{V} \cap \mathcal{L}^n \supset \bigcup_{E \subset \mathfrak{V}} E \cap \mathcal{L}^n,$$

where E ranges over the set of vector subspaces of \mathbb{C}^n , rational over \mathbb{Q} , which are contained in \mathfrak{V} , is trivial.

Let $\underline{\lambda} = (\lambda_1, \dots, \lambda_n) \in \mathfrak{V} \cap \mathcal{L}^n$. As for part (a), we write

$$\underline{\lambda} = \sum_{j=1}^r \mu_j \underline{b}_j$$

with μ_1, \dots, μ_r linearly independent over \mathbb{Q} in \mathcal{L} and

$$\underline{b}_j = (b_{1j}, \dots, b_{nj}) \in \mathbb{Q}^n \quad 1 \leq j \leq r;$$

we also denote by E be the vector subspace of \mathbb{C}^n spanned by $\underline{b}_1, \dots, \underline{b}_r$, so that E is rational over \mathbb{Q} and $\underline{\lambda} \in E \cap \mathcal{L}^n$.

By assumption \mathfrak{V} is the intersection of hypersurfaces of \mathbb{C}^n which are rational over $\overline{\mathbb{Q}}$. Let H be such a hypersurface and

$$P(z_1, \dots, z_n) = 0$$

an equation of H , where $P \in \overline{\mathbb{Q}}[X_1, \dots, X_n] \setminus \{0\}$. Since $\underline{\lambda} \in \mathfrak{V} \subset H$, we have

$$P(\lambda_1, \dots, \lambda_n) = 0,$$

that is

$$P \left(\sum_{j=1}^r b_{1j} \mu_j, \dots, \sum_{j=1}^r b_{nj} \mu_j \right) = 0.$$

According to the conjecture on algebraic independence of logarithms, the numbers μ_1, \dots, μ_r are algebraically independent. Hence

$$P \left(\sum_{j=1}^r b_{1j} t_j, \dots, \sum_{j=1}^r b_{nj} t_j \right) = 0$$

for all $(t_1, \dots, t_r) \in \mathbb{C}^r$, which means

$$E = \mathbb{C}\underline{b}_1 + \dots + \mathbb{C}\underline{b}_r \subset H.$$

This is true for all hypersurfaces H of \mathbb{C}^n which are rational over $\overline{\mathbb{Q}}$ and contain \mathfrak{A} , hence $E \subset \mathfrak{A}$.

(c) Let Z be the hypersurface in \mathbb{C}^4 defined by the polynomial $X_1 X_4 - X_2 X_3$. Since this polynomial is homogeneous, for any $\underline{a} = (a_1, a_2, a_3, a_4) \in Z \setminus \{0\}$, the line $\mathbb{C}\underline{a}$ is contained in Z . Vector subspaces of dimension 2 (planes) of \mathbb{C}^4 contained in Z are the following: for $u := (h : k) \in \mathbb{P}^1(\mathbb{C})$,

$$V_u = \{(x_1, x_2, x_3, x_4) \mid hx_1 = kx_3, hx_2 = kx_4\},$$

$$W_u = \{(x_1, x_2, x_3, x_4) \mid hx_1 = kx_2, hx_3 = kx_4\}.$$

Let us show that $\{0\}$, the lines $\mathbb{C}\underline{a}$ with $\underline{a} \in Z$ and the planes V_u and W_u with $u \in \mathbb{P}^1(\mathbb{C})$ give a complete list of the vector subspaces of \mathbb{C}^4 contained in Z . Those which are rational over \mathbb{Q} are $\{0\}$, the lines $\mathbb{C}\underline{a}$ with $\underline{a} \in \mathbb{Q}^4 \cap Z$ and the planes V_u and W_u , with $u := (h : k) \in \mathbb{P}^1(\mathbb{Q})$.

Let E be \mathbb{C} -vector subspace of \mathbb{C}^4 contained in Z . Let $\underline{a} = (a_1, a_2, a_3, a_4)$ and $\underline{b} = (b_1, b_2, b_3, b_4)$ be two elements $\neq 0$ in E . For x and y in \mathbb{C} , the point $x\underline{a} + y\underline{b} = (xa_1 + yb_1, xa_2 + yb_2, xa_3 + yb_3, xa_4 + yb_4)$ belongs to E , hence to Z :

$$(xa_1 + yb_1)(xa_4 + yb_4) = (xa_2 + yb_2)(xa_3 + yb_3).$$

This amounts to

$$a_1 a_4 = a_2 a_3, \quad b_1 b_4 = b_2 b_3, \quad a_1 b_4 + a_4 b_1 = a_2 b_3 + a_3 b_2.$$

We eliminate a_4 and b_4 by multiplying the third equation by $a_1 b_1$:

$$a_1^2 b_1 b_4 + a_1 a_4 b_1^2 = a_1 a_2 b_1 b_3 + a_1 a_3 b_1 b_2,$$

which yields

$$a_1^2 b_2 b_3 + a_2 a_3 b_1^2 = a_1 a_2 b_1 b_3 + a_1 a_3 b_1 b_2,$$

or

$$(a_1 b_3 - a_3 b_1)(a_1 b_2 - a_2 b_1) = 0.$$

Therefore one at least of the two numbers $a_1 b_3 - a_3 b_1$, $a_1 b_2 - a_2 b_1$ vanishes. We consider several cases.

- Assume $a_1 = a_2 = 0$ for all $\underline{a} \in E$. Then $E \subset V_{(1:0)}$.
- Assume $a_1 = a_3 = 0$ for all $\underline{a} \in E$. Then $E \subset W_{(1:0)}$.

- Otherwise, there exists $\underline{b} \in E$ and $\underline{c} \in E$ with $(b_1, b_2) \neq (0, 0)$ and $(c_1, c_3) \neq (0, 0)$. Then one at least of \underline{b} , \underline{c} , $\underline{b} + \underline{c}$, say \underline{a} , has $(a_1, a_2) \neq (0, 0)$ and $(a_1, a_3) \neq (0, 0)$. We fix such an a .
- Assume $a_1 b_3 - a_3 b_1 = 0$ for all $\underline{b} \in E$. If $b_1 = b_3 = 0$, then the equation $a_1 b_4 + a_4 b_1 = a_2 b_3 + a_3 b_2$ becomes $a_1 b_4 = a_3 b_2$. This relation is also true if $b_2 = b_4 = 0$. If $(b_1, b_3) \neq (0, 0)$ and $(b_2, b_4) \neq (0, 0)$, then we have $(a_1 : a_3) = (b_1 : b_3) = (b_2 : b_4)$. In all cases we deduce

$$a_3 b_1 = a_1 b_3 \text{ and } a_3 b_2 = a_1 b_4$$

for all $\underline{b} \in E$, which means $E \subset V_{(a_3 : a_1)}$.

- Assume there exists $\underline{b} \in E$ such that $a_1 b_3 - a_3 b_1 \neq 0$. Hence $a_1 b_2 - a_2 b_1 = 0$. Let $\underline{c} \in E$. Since $\underline{b} + \underline{c} \in E$, one at least of the two numbers $a_1(b_3 + c_3) - a_3(b_1 + c_1)$, $a_1(b_2 + c_2) - a_2(b_1 + c_1)$ vanishes. If $a_1(b_3 + c_3) - a_3(b_1 + c_1) = 0$, from $a_1 b_3 - a_3 b_1 \neq 0$ we deduce $a_1 c_3 - a_3 c_1 \neq 0$, hence $a_1 c_2 = a_2 c_1$. If $a_1(b_2 + c_2) - a_2(b_1 + c_1) = 0$, then again $a_1 c_2 = a_2 c_1$. Therefore $a_1 c_2 = a_2 c_1$ for all $\underline{c} \in E$. In the same way as in the previous case, we deduce that for all $\underline{c} \in E$ we have

$$a_2 c_1 = a_1 c_2 \text{ and } a_2 c_3 = a_1 c_4$$

for all $\underline{c} \in E$, which means $E \subset W_{(a_2 : a_1)}$.

(d) Let

$$\begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}$$

be a 2×2 matrix with entries in \mathcal{L} and zero determinant. According to (b), the Conjecture on algebraic independence of logarithms of algebraic numbers implies that the point $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ belongs to a vector subspace of \mathbb{C}^4 rational over \mathbb{Q} contained in the hypersurface Z in \mathbb{C}^4 defined by the polynomial $X_1 X_4 - X_2 X_3$. From (c) we deduce that there exists $(h, k) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$ with either

$$h\lambda_1 = k\lambda_3, \quad h\lambda_2 = k\lambda_4$$

or

$$h\lambda_1 = k\lambda_2, \quad h\lambda_3 = k\lambda_4.$$

In the first case the rows of the matrix are linearly dependent over \mathbb{Q} , in the second case the columns of the matrix are linearly dependent over \mathbb{Q} .

Reference: [GL326] Exercices 1.5 and 1.8; also § 11.5 p.397 □

Solution to Exercise 6.

(a) There are 6 obvious algebraic dependence relations among these 31 numbers: we can remove the numbers

$$e\pi, e + \pi, e + e^\pi, \pi + e^\pi, \pi e^\pi, \pi + \log 5.$$

Let us deduce from Schanuel's Conjecture that the transcendence degree is 25 by showing that this conjecture implies the algebraic independence of the following 30 numbers:

$$\begin{aligned} & \log 2, \log 3, \log 5, \log 7, e^{\sqrt{2}}, e^{\sqrt{5}}, e^{\sqrt{7}}, \log \log 2, \log \log 3, e, \pi, e^\pi, \log \pi, \\ & \pi^e, e^i, \pi^i, e^e, \pi^\pi, e^{\pi^2}, e^{e^e}, \pi^{\pi^\pi}, 2^{\sqrt{2}}, 2^{\sqrt{3}}, 3^{\sqrt{3}}, 2^\pi, 2^e, \\ & 2^{2^{\sqrt{2}}}, 2^{\log 2}, 7^{\log 3}, (\log 2)^{\sqrt{2}}. \end{aligned}$$

We use Schanuel's Conjecture several times. It is easier to explain the proof by proceeding backwards. We want to prove (subject to Schanuel's Conjecture) that a field has transcendence degree 30. We introduce 30 numbers, x_1, \dots, x_{30} so that for $n = 1, \dots, 30$, exactly one of x_n, e^{x_n} is not in the field $\mathbb{Q}(x_1, \dots, x_{n-1}, e^{x_1}, \dots, e^{x_{n-1}})$. From Schanuel's Conjecture, the fact that the field $\mathbb{Q}(x_1, \dots, x_{30}, e^{x_1}, \dots, e^{x_{30}})$ will follow from Schanuel's Conjecture, provided that we prove the linear independence of these 30 numbers, x_1, \dots, x_{30} . This will be the next step.

Here are x_1, \dots, x_{30} and their exponentials:

$$\begin{array}{cccccccc} \log 2 & \log 3 & \log 5 & \log 7 & \sqrt{2} & \sqrt{5} & \sqrt{7} & \log \log 2 & \log \log 3 \\ 2 & 3 & 5 & 7 & e^{\sqrt{2}} & e^{\sqrt{5}} & e^{\sqrt{7}} & \log 2 & \log 3 \\ \\ 1 & i\pi & \pi & \log \pi & e \log \pi & i & i \log \pi & e & \pi \log \pi & \pi^2 \\ e & -1, & e^\pi & \pi & \pi^e & e^i & \pi^i & e^e & \pi^\pi & e^{\pi^2} \\ \\ e^e & \pi^\pi \log \pi & \sqrt{2} \log 2 & \sqrt{3} \log 2 & \sqrt{3} \log 3 & \pi \log 2 & e \log 2 \\ e^{e^e} & \pi^{\pi^\pi} & 2^{\sqrt{2}} & 2^{\sqrt{3}} & 3^{\sqrt{3}} & 2^\pi & 2^e \\ \\ 2^{\sqrt{2}} \log 2 & (\log 2)^2 & (\log 3)(\log 7) & \sqrt{2} \log \log 2 \\ 2^{2^{\sqrt{2}}} & 2^{\log 2} & 7^{\log 3} & (\log 2)^{\sqrt{2}}. \end{array}$$

So it remains to deduce from Schanuel's Conjecture that the 30 numbers x_1, \dots, x_{30} are linearly independent over \mathbb{Q} . A linear combination with integer coefficients among x_1, \dots, x_{30} is a polynomial in the following 12 numbers:

$$\log 2, \log 3, \log 5, \log 7, \log \log 2, \log \log 3, e, \pi, \log \pi, e^e, \pi^\pi, 2^{\sqrt{2}}.$$

The algebraic independence of these 12 numbers follows from Schanuel's Conjecture by means of the same strategy, involving a new set of numbers x_1, \dots, x_{12} , given as follows with their exponentials

$$\begin{array}{cccccc} \log 2 & \log 3 & \log 5 & \log 7 & \log \log 2 & \log \log 3 \\ 1 & 3 & 5 & 7 & \log 2 & \log 3 \\ \\ \sqrt{2} \log 2 & 1 & i\pi & \log \pi & e & \pi \log \pi \\ 2^{\sqrt{2}} & e & -1 & \pi & e^e & \pi^\pi. \end{array}$$

For the proof that Schanuel's Conjecture implies the linear independence of the 12 x_i 's in the second set, we modify slightly the strategy: a linear combination with integer coefficients among the 12 numbers x_1, \dots, x_{12} is a multiplicative dependence relation among the following 6 numbers

$$\log 2, \log 3, 2^{\sqrt{2}}, e, \pi, e^e, \pi^\pi.$$

Hence we are led to prove (assuming Schanuel's Conjecture) that these 7 numbers are algebraically independent, and for this purpose we introduce a third set of x_i 's and their exponentials, namely

$$\begin{array}{cccccc} \log 2 & \log 3 & \sqrt{2} \log 2 & 1 & i\pi & e & \pi \log \pi \\ 2 & 3 & 2^{\sqrt{2}} & e & -1 & e^e & \pi^\pi. \end{array}$$

A linear combination among the 7 numbers x_1, \dots, x_7 of the third set is a polynomial in the 5 numbers $\log 2, \log 3, e, \pi$ and $\log \pi$. We introduce a fourth set of x_i 's with their exponentials:

$$\begin{array}{cccc} \log 2 & \log 3 & 1 & i\pi & \log \pi \\ 2 & 3 & e & -1 & \pi. \end{array}$$

Finally Schanuel's Conjecture implies the algebraic independence of e and π , hence the multiplicative independence of $2, 3, e$ and π , hence the linear independence over \mathbb{Q} of the 5 numbers $\log 2, \log 3, 1, i\pi$ and $\log \pi$.

(b) Among the given 31 numbers, the following 13 ones are known to be transcendental: from Hermite Lindemann Theorem on the transcendence of e^α :

$$e, \pi, e^{\sqrt{2}}, e^i;$$

from Lindemann Weierstrass Theorem on the algebraic independence of e^{α_i} :

$$e^{\sqrt{5}} + ie^{\sqrt{7}};$$

from Gel'fond-Schneider Theorem on the transcendence of α^β :

$$e^\pi, 2^{\sqrt{2}}, \frac{1}{\pi} \log 3;$$

from Baker's Theorem on linear independence of logarithms of algebraic numbers:

$$e^\pi 2^{\sqrt{3}}, \pi + \log 5, 2^{\sqrt{2}} 3^{\sqrt{3}};$$

from Nesterenko's Theorem on the algebraic independence of π and e^π :

$$\pi + e^\pi, \pi e^\pi.$$

For the 18 other ones, we do not know even that they are irrational.

Remark. Some further partial results are known, for instance that one at least of $e + \pi, e\pi$ is transcendental; the same for e^e, e^{e^e} , also $e + \pi, e^{\pi^2}$, and also $e\pi, e^{\pi^2}$. \square