EXAMPLE SHEET 1 FOR DIOPHANTINE ANALYSIS, MICHAELMAS 2024

PÉTER VARJÚ

About this example sheet:

- Please send comments and corrections to pv270@dpmms.cam.ac.uk.
- Please submit your solutions of Problems 6 and 9, by Monday 28 October, 13:00.
- The purpose of this example sheet is to complement the material of the lectures. The level of difficulty of the problems varies considerably (in a non-monotone fashion), and they are not intended to be mock exam questions.
- The solutions went under minimal proof reading only, so they are error prone. Please handle with care, and corrections sent by email are very much appreciated.

1. Let $P \in \mathbf{Z}[X,Y]$ be a non-zero homogeneous polynomial, and let $m \in \mathbf{Z}_{\neq 0}$. Suppose the equation

$$P(X,Y) = m$$

has infinitely many solutions in $\mathbf{Z}^2$. Prove that $P = aQ^k$ for some $Q \in \mathbf{Z}[X,Y]$ homogeneous polynomial of degree at most 2 and $a \in \mathbf{Z}$.

Hint: If $R \in \mathbf{Z}[X,Y]$ with $R|P$ show that $R(X,Y) = m_0$ has infinitely many solutions in $\mathbf{Z}^2$ for some $m_0|m$.

Solution: Suppose $P(X,Y) = m$ has infinitely many solutions and $Q(X,Y)|P(X,Y)$ for some $Q \in \mathbf{Z}[X,Y]$. Then for each $(x,y) \in \mathbf{Z}^2$ that solves $P(x,y) = m$, we have $Q(x,y)|m$. Since $m \neq 0$, it has only finitely many divisors, there is some $m_1|m$ such that $Q(X,Y) = m_1$ has infinitely many solutions.

Now let $P(X,Y) = a \cdot R_1(X,Y)^{n_1} \cdots R_k(X,Y)^{n_k}$ be the factorization of P into irreducibles in $\mathbf{Z}[X,Y]$. Note that $\mathbf{Z}[X,Y]$ is a UFD and that each R_j is necessarily homogeneous. Now let $Q = R_1 \cdots R_k$ and apply the above considerations. Since Q has no repeated factors, Theorem 4 of the lectures applies except if $\deg Q \leq 2$. Since the equation $Q(X,Y) = m_1$ has infinitely many solutions, we must have $\deg Q \leq 2$.

If Q is irreducible, the claim follows. It remains to rule out the case $Q = R_1R_2$, where $R_1, R_2 \in \mathbf{Z}[X,Y]$ are distinct (that is not associate) polynomials of degree 1. Let $x, y \in \mathbf{Z}$ with $Q(x,y) = m_1$. Then $|R_1(x,y)|, |R_2(x,y)| \leq m_1$. Writing $R_j = a_jX + b_jY$ for $j = 1,2$, we get $|a_j/b_j + y/x| \leq |m_1|/|y|$ and hence

$$|a_1/b_1 - a_2/b_2| \leq 2|m_1|/|y|$$

and

$$|y| \leq 2|m_1|/|a_1/b_1 - a_2/b_2|.$$

In this case, we can only have finitely many solutions, which completes the proof.

2. Let $n \in \mathbf{Z}_{\geq 2}$ and S a finite set of places of $\mathbf{Q}$ containing ∞. For each $v \in S$, let $L_1^{(v)}, \dots, L_n^{(v)}$ be a linearly independent collection of linear forms with coefficients in $\mathbf{Q}$ in n variables. Let $l \subset \mathbf{Q}^n$ be a 1-dimensional linear subspace. Suppose none of the $L_j^{(v)}$ vanishes on l. Prove that there is $c = c(l, L_j^{(v)}) > 0$ such that

$$\prod_{v \in S} \prod_{j=1}^{n} |L_j^{(v)}(x_1, \dots, x_n)|_v > c$$

for all non-zero $(x_1, \dots, x_n) \in l \cap \mathbf{Z}^n$.

Solution: Let $(x_1, \dots, x_n) \in l \cap \mathbf{Z}^n$ be a non-zero vector with relatively prime coordinates. All non-zero points in $l \cap \mathbf{Z}^n$ are of the form $(ax_1, \dots, ax_n)$ for some $0 \neq a \in \mathbf{Z}$. By homogeneity of $L_j^{(v)}$ and multiplicativity of $|\cdot|_v$, we have

$$\prod_{v \in S} \prod_{j=1}^{n} |L_j^{(v)}(ax_1, \dots, ax_n)| = \prod_{v \in S} |a|_v^n \prod_{v \in S} \prod_{j=1}^{n} |L_j^{(v)}(x_1, \dots, x_n)|_v$$

By the product formula,

$$\prod_{v \in S} |a|_v^n = \prod_{v \notin S} |a|_v^{-n} \geq 1.$$

Here we used that $|a|_v \geq 1$ for all finite place v and that $\infty \in S$. Therefore, we have

$$\prod_{v \in S} \prod_{j=1}^{n} |L_j^{(v)}(ax_1, \dots, ax_n)| \geq \prod_{j=1}^{n} |L_j^{(v)}(x_1, \dots, x_n)|_v =: c > 0.$$

3. Let L_1, L_2, L_3 be linearly independent linear forms in three variables with algebraic coefficients, and let $\varepsilon \in (0, 1)$. Let $V \subset \mathbf{Q}^3$ be a 2 dimensional subspace that contains infinitely many solutions of

$$\prod_{j=1}^{3} |L_j(x_1, x_2, x_3)| \leq H(x_1, x_2, x_3)^{-\varepsilon} \tag{1}$$

that cannot be covered by finitely many lines.

Prove that there is some $\alpha \in \overline{\mathbf{Q}}$ and indices $i, j \in \{1, 2, 3\}$ such that $V = \mathrm{Ker}(L_i + \alpha L_j)$.

Conversely show that if $V \subset \mathbf{Q}^3$ is a subspace of the above form, then it contains infinitely many integral solutions of (1).

Solution: Let V be a 2 dimensional subspace that contains infinitely many solutions of (1), which cannot be covered by finitely many lines. For each solution (x_1, x_2, x_3), we have

$$|L_i(x_1, x_2, x_3)||L_j(x_1, x_2, x_3)| \leq H(x_1, x_2, x_3)^{-2\varepsilon/3} \tag{2}$$

for some choice of $i \neq j \in \{1, 2, 3\}$. (Choose the i, j that makes the left hand side the smallest possible.)

We fix some choice of i and j such that (2) has infinitely many solutions in $V \cap \mathbf{Z}^2$ that cannot be covered by finitely many lines. Now we pick a basis of V that generates the $\mathbf{Z}$-module $V \cap \mathbf{Z}^2$ and write $L_i|_V$ and $L_j|_V$ as linear forms in these new coordinates. We try to apply the subspace theorem for these linear forms. However, (2) has infinitely many solutions, and they cannot be covered by finitely many lines. The conclusion of the subspace theorem does not apply so $L_i|_V$ and $L_j|_V$ must be linearly dependent. That is, there is $\alpha \in \overline{Q}$ such that $L_i|_V = \alpha L_j|_V$. (Exchange i and j if necessary.) Therefore $V \subset \mathrm{Ker}(L_i - \alpha L_j)$. Since L_i and L_j are linearly independent $\dim \mathrm{Ker}(L_i - \alpha L_j) = 2$ and $V = \mathrm{Ker}(L_i - \alpha L_j)$.

Conversely, let $V \subset \mathbf{Q}^3$ be such that there is $\alpha \in \overline{\mathbf{Q}}$ with $V = \mathrm{Ker}(L_1 - \alpha L_2)$. Let $v_1, v_2 \in V \cap \mathbf{Z}^3$ be linearly independent. Fix some number $H \in \mathbf{Z}_{>0}$ and consider the points $av_1 + bv_2$ for $a, b = 0, 1, \ldots, H$. There is $C = C(V)$ such that

$$|L_j(av_1 + bv_2)| < CH$$

for $j = 1, 2, 3$. By the box principle, there is $(a_1, b_1) \neq (a_2, b_2)$ such that

$$|L_1(a_1v_1 + b_1v_2) - L_1(a_2v_1 + b_2v_2)| < 2C/H.$$

Write $u_H = (a_1 - a_2)v_1 + (b_1 - b_2)v_2$. Since $L_2|_V = \alpha L_1|_V$, $|L_2(u_H)| = |\alpha L_1(u_H)| \leq 2|\alpha|C/H$. Thus

$$\prod_{j=1}^{3} |L_j(u_H)| \leq 4|\alpha|C^3/H.$$

Since $\varepsilon < 1$, u_H is a solution of (1) provided H is sufficiently large.

If $L_1(u_H) \neq 0$, for any H, then there are arbitrarily small values among $L_1(u_H)$ so there must be infinitely many distinct among the u_H.

If $L_1(u_H) = 0$ for some H, then the line $\mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2) \subset \mathbf{Q}^3 \cap V$, and it contains infinitely many solutions of (1).

Further remarks (not needed for the solution): When the line $\mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$ is irrational, the above argument also shows that the infinitely many solutions of (1) contained in V cannot be covered by finitely many lines. When $\mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$ is rational, it can be showed that all but finitely many solutions of (1) contained in V are covered by at most two lines or $V = \mathrm{Ker}(L_1)$.

It may also happen that there is no rational $V \subset \mathbf{Q}^3$ of the form $V = \mathrm{Ker}(L_1 - \alpha L_2)$.

4. Prove that the $n = 2$ case of the subspace theorem in its Archimedean form (Theorem 6) is equivalent to Roth's theorem.

Solution: We have seen that Roth follows from the subspace theorem in the lectures. We prove the converse. Let L_1, L_2 be linearly independent linear forms in two variables with algebraic coefficients. We may assume $L_j = X - \alpha_j Y$ for some $\alpha_j \in \overline{Q}$. (If $L_j = Y$ for some j, we may exchange X and Y. If this does not help, because $\{L_1, L_2\} = \{X, Y\}$ then the only solution of the inequality in the subspace theorem is when $X = 0$ or $Y = 0$.)

Let $x, y \in \mathbf{Z}$ with $\max(|x, ||y|) = H$. Then there is $c = c(\alpha_1, \alpha_2)$ such that

$$|L_j(x, y)| \leq c$$

implies

$$L_{2-j}(x, y) \geq cH.$$

This is because x/y may be close to only one of α_1, α_2.

Now suppose

$$|L_1(x, y)||L_2(x, y)| \leq H^{-\varepsilon}.$$

If H is large enough so that $H^{-\varepsilon} < c^2$, then $|L_j(x, y)| \leq c$ for $j = 1$ or 2. Then $|L_{2-j}(x, y)| \geq cH$, and hence

$$|L_j(x, y)| = |x - \alpha_j y| \leq c^{-1} H^{-1-\varepsilon}.$$

Dividing by y, we get

$$|x/y - \alpha_j| \leq c^{-1} y^{-2-\varepsilon}.$$

If α_j is irrational, then this inequality has only finitely many solutions by Roth's theorem. If α_j is rational, then all but finitely many solutions are on the line $x - \alpha_j y = 0$.

All in all, we conclude that the inequality has finitely many solutions plus those that are contained in the lines $x - \alpha_1 y = 0$ and $x - \alpha_2 y = 0$.

5. Let $L_1, \ldots, L_n$ be linearly independent linear forms in n variables with real algebraic coefficients. Let $(x_1, \ldots, x_n) \in \mathbf{R}^n$ be non-zero with

$$L_1(x_1, \ldots, x_n) = \ldots = L_{n-1}(x_1, \ldots, x_n) = 0,$$

and suppose the numbers $x_1, \ldots, x_n$ are linearly independent over $\mathbf{Q}$.

Prove that there is a constant $C = C(L_1, \ldots, L_n)$ such that the following holds. Let $V_1, \ldots, V_k \subset \mathbf{Q}^n$ be proper linear subspaces. Then there is $(y_1, \ldots, y_n) \in \mathbf{Z}^n \backslash (V_1 \cup \ldots \cup V_k)$ such that

$$\prod_{j=1}^{n} |L_j(y_1, \ldots, y_n)| \leq C.$$

Solution: This question shows that the subspace theorem is optimal in a certain sense.

Fix some number $H \in \mathbf{Z}_{>0}$. The vectors

$$(L_1(u_1, \ldots, u_n), \ldots, L_n(u_1, \ldots, u_n)) \in \mathbf{R}^n$$

for $(u_1, \ldots, u_n) \in [0, \ldots, H]^n$ are confined in a box with side lengths $C_0 H$ for some constant C_0 depending only on the linear forms. We subdivide this large box to H^n smaller boxes that have side length $C_0 H^{-1/(n-1)}$ in the first $n-1$ coordinates and side length $C_0 H$ in the last coordinate. (OK, maybe some rounding is needed here, but it can be corrected.)

By the box principle, there are two choices of the $(u_1, \ldots, u_n)$ that land in the same small box. We write $(y_1, \ldots, y_n) \in [-H, \ldots, H]^n$ for their difference and show that it has all the required properties. We have

$$\begin{aligned} &|L_j(y_1, \ldots, y_n)| < C_0 H^{1/(n-1)} \qquad \text{for } j = 1, \ldots, n-1, \\ &|L_n(y_1, \ldots, y_n)| < C_0 H. \end{aligned}$$

In particular

$$\prod_{j=1}^{n} |L_j(y_1, \ldots, y_n)| \leq C_0^n.$$

Therefore, it remains to show that $(y_1, \ldots, y_n) \notin V_1 \cup \ldots \cup V_k$. We show that this is the case if H is sufficiently large.

To this end, note that

$$\lim_{H \to \infty} L_j\left(\frac{y_1}{\|y\|_2}, \ldots, \frac{y_n}{\|y\|_2}\right) = 0$$

because $\|y\|_2$ is bounded away from 0. (It is a non-zero integer vector.) From this, we conclude that

$$\lim_{H \to \infty} \left(\frac{y_1}{\|y\|_2}, \ldots, \frac{y_n}{\|y\|_2}\right) = \left(\frac{x_1}{\|x\|_2}, \ldots, \frac{x_n}{\|x\|_2}\right),$$

because $(x_1, \ldots, x_n)$ spans the common 0 set of $L_1, \ldots, L_{n-1}$.

If it was the case that $(y_1, \ldots, y_n) \in V_j$ for some j for a sequence of arbitrarily large H, then we would have $(x_1, \ldots, x_n) \in V_j$. But this is not possible, because V_j is a proper subspace of $\mathbf{Q}^n$ and $x_1, \ldots, x_n$ are linearly independent over $\mathbf{Q}$.

6. Using the p-adic subspace theorem (Theorem 7) or Roth's theorem, prove that for all $n, a_1, \ldots, a_n \in \mathbf{Z}_{>0}$ and $\varepsilon > 0$, there is a constant $c > 0$ such that the following holds. Let $b_1, \ldots, b_n \in \mathbf{Z}$ with $\max(|b_j|) = B$. Then

$$|b_1 \log a_1 + \ldots + b_n \log a_n| \geq c \exp(-\varepsilon B)$$

provided the linear form in logarithms on the left does not vanish.

Solution: We first give a solution using the p-adic subspace theorem. Using that log is Lipschitz in a neighbourhood of 1, the claim will follow if we show

$$|a_1^{b_1} \cdots a_n^{b_n} - 1| \geq c \exp(-\varepsilon B)$$

for some constant $c > 0$, which may be different from the one denoted by the same letter in the claim. We can assume without loss of generality that $b_1, \dots, b_k \geq 0$ for some k and $b_{k+1}, \dots, b_n < 0$. Then it is enough to prove

$$|a_1^{b_1} \cdots a_k^{b_k} - a_{k+1}^{-b_{k+1}} \cdots a_n^{-b_n}| \geq c a_{k+1}^{-b_{k+1}} \cdots a_n^{-b_n} \exp(-\varepsilon B)$$

We write S for the set of all prime divisors of the numbers $a_1, \dots, a_n$ together with ∞.

We prove using the p-adic subspace theorem that the number of pairs $u, w \in \mathbf{Z}_{>0}$ such that $u \neq w$,

$$|u - w| \geq w \max(u, w)^{-\varepsilon'}$$

and all prime divisors of u and w are in S is finite for all fixed $\varepsilon' > 0$. This will prove the claim because

$$\max(a_1^{b_1} \cdots a_k^{b_k}, a_{k+1}^{-b_{k+1}} \cdots a_n^{-b_n}) \leq \exp(CB)$$

for a suitable constant $C > 0$ depending only on $a_1, \dots, a_n$. For this reason, for all $\varepsilon > 0$, there is ε' such that

$$\exp(-\varepsilon B) > \max(a_1^{b_1} \cdots a_k^{b_k}, a_{k+1}^{-b_{k+1}} \cdots a_n^{-b_n})^{-\varepsilon'}.$$

We turn to the above stated claim. We consider the linear forms $L_j^{(v)}(X_1, X_2) = X_j$ for $j = 1, 2$, $v \in S$ with the exception $L_2^{(\infty)}(X_1, X_2) = X_1 - X_2$. We take $u, w \in \mathbf{Z}$ with prime factors in S alone and

$$|u - w| < w \max(u, w)^{-\varepsilon'}.$$

Then

$$\prod_{j=1}^{2} \prod_{v \in S} |L_j^{(v)}(u, w)|_v = \prod_{v \in S} (|u|_v \cdot |w|_v) \cdot \frac{|u - w|_\infty}{|w|_\infty} \leq \max(u, w)^{-\varepsilon'}.$$

By the p-adic subspace theorem the number of such integers u, w not satisfying $u = 0$, $w = 0$ or $u = w$ is finite. This proves the claim.

We give a second solution using Roth's theorem. Again, we prove that for any finite set of primes S, and $\varepsilon > 0$, the number of pairs of integers $u, w \in \mathbf{Z}_{>0}$ with prime factors in S such that

$$0 < |u - w| < w \max(u, w)^{-\varepsilon}$$

is finite. We suppose to the contrary, that this is not true.

We fix a number $N \in \mathbf{Z}_{>0}$, which we will set later to be sufficiently large depending only on ε. We observe that for all $u > 0$ with prime factors in S alone, there is an integer α with $0 < \alpha \leq \prod_{p \in S} p^{N-1}$ and another integer $x \in \mathbf{Z}_{>0}$ such that $u = \alpha x^N$. Therefore, by the box principle and the indirect assumption, there are some $\alpha, \beta \in \mathbf{Z}_{>0}$ such that

$$0 < |\alpha X^N - \beta Y^N| < \beta Y^N \cdot \max(X, Y)^{-N\varepsilon}$$

has infinitely many solutions for $X, Y \in \mathbf{Z}_{>0}$.

Using Lemma 5 from the lectures with $P(X,Y) = \alpha X^N - \beta Y^N$, for each solution $X = x$, $Y = y$, we have

$$0 < |\gamma - x/y| \leq C \max(x,y)^{-N\varepsilon},$$

where γ is a root of P and C is a constant that depends only on P. Now we set $N > 2/\varepsilon$, and get a contradiction to Roth's theorem.

7. Let $n \in \mathbf{Z}_{\geq 2}$, and let $\lambda_1, \ldots, \lambda_n \in \mathbf{C}$, (which are not necessarily logarithms of algebraic numbers). Let $B \in \mathbf{Z}_{>1}$. Prove that there are $b_1, \ldots, b_n \in \mathbf{Z}$ not all 0 with $|b_j| \leq B$ such that

$$|b_1\lambda_1 + \ldots + b_n\lambda_n| \leq C \exp(-(n/2-1)\log B),$$

where $C > 0$ is a constant that may depend on $n, \lambda_1, \ldots, \lambda_n$.

Solution: Consider all numbers

$$u_1\lambda_1 + \ldots + u_n\lambda_n$$

for $(u_1, \ldots, u_n) \in [0, \ldots, B]^n$. They are in the box

$$[-CB, CB] \times [-iCB, iCB]$$

in the complex plane for some C depending only on $\lambda_1, \ldots, \lambda_n$. We subdivide this box into B^n many boxes of side length $2CB^{1-n/2}$.

By the box principle, there are $(u_1, \ldots, u_n) \neq (v_1, \ldots, v_n)$ such that the corresponding points are in the same little box, that is,

$$|(u_1 - v_1)\lambda_1 + \ldots + (u_n - v_n)\lambda_n| \leq 2\sqrt{2}CB^{1-n/2}.$$

This proves the claim with $b_j = u_j - v_j$.

8. Prove that Schanuel's conjecture implies the following two statements, which are known as the four exponentials conjecture.

- Let $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}, \lambda_{2,2}$ be logarithms of algebraic numbers. Suppose $\lambda_{1,1} \neq 0$ and $\lambda_{1,2}/\lambda_{1,1}$ and $\lambda_{2,1}/\lambda_{1,1}$ are irrational. Then $\lambda_{1,1}\lambda_{2,2} - \lambda_{1,2}\lambda_{2,1} \neq 0$.
- Let $x_1, x_2, y_1, y_2 \in \mathbf{C}_{\neq 0}$ such that $x_1/x_2, y_1/y_2 \notin \mathbf{Q}$. Then at least one of the four numbers

  $$\exp(x_1y_1), \exp(x_1y_2), \exp(x_2y_1), \exp(x_2y_2)$$

  are transcendental.

Solution: Suppose to the contrary that $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}, \lambda_{2,2}$ are as in the first statement, but

$$\lambda_{1,1}\lambda_{2,2} - \lambda_{1,2}\lambda_{2,1} = 0.$$

Then the field

$$\mathbf{Q}(\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}, \lambda_{2,2}, \exp(\lambda_{1,1}), \exp(\lambda_{1,2}), \exp(\lambda_{2,1}), \exp(\lambda_{2,2}))$$

has transcendence degree at most 3. By Schanuel's conjecture, $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}, \lambda_{2,2}$ cannot be linearly independent over $\mathbf{Q}$. Say we have

$$\alpha_{1,1}\lambda_{1,1} + \alpha_{1,2}\lambda_{1,2} + \alpha_{2,1}\lambda_{2,1} + \alpha_{2,2}\lambda_{2,2} = 0.$$

We suppose without loss of generality that $\alpha_{2,2} = -1$. (To achieve this, we may need to rearrange the indices to make $\alpha_{2,2} \neq 0$ and then divide by $-\alpha_{2,2}$.

Now apply the Schanuel conjecture again for $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}$, and use

$$\lambda_{1,1}(\alpha_{1,1}\lambda_{1,1} + \alpha_{1,2}\lambda_{1,2} + \alpha_{2,1}\lambda_{2,1}) + \lambda_{1,2}\lambda_{2,1} = 0.$$

This is a nonzero polynomial in $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}$. Indeed, the coefficient of $\lambda_{1,2}\lambda_{2,1}$ is not 0 irrespective of the values of the $\alpha_{i,j}$. So Schanuel's conjecture implies that $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}$ are again $\mathbf{Q}$-linearly dependent.

This allows us to eliminate one more $\lambda_{i,j}$ and write all of them as a linear combination of just two. Since $\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}$ ar all non-zero, the linear relation between them must have at least two non-zero coefficients. This allows us a choice of at least two $\lambda_{i,j}$ to eliminate. We make the choice of not to eliminate $\lambda_{1,1}$. So we will write everything as a linear combination of $\lambda_{1,1}, \lambda_{1,2}$ or $\lambda_{1,1}, \lambda_{2,1}$. We assume without loss of generality that we are in the former case.

Then we may write

$$\lambda_{2,1} = \beta_{1,1}\lambda_{1,1} + \beta_{1,2}\lambda_{1,2},$$
$$\lambda_{2,2} = \beta_{2,1}\lambda_{1,1} + \beta_{2,2}\lambda_{1,2}.$$

Now we have

$$\lambda_{1,1}(\beta_{2,1}\lambda_{1,1} + \beta_{2,2}\lambda_{1,2}) - \lambda_{1,2}(\beta_{1,1}\lambda_{1,1} + \beta_{1,2}\lambda_{1,2}) = 0$$

If this is a trivial polynomial, then $\beta_{2,1} = \beta_{1,2} = 0$, and we get $\lambda_{2,1}/\lambda_{1,1} = \beta_{1,1} \in \mathbf{Q}$, a contradiction. If the polynomial is not trivial, then Schanuel's conjecture can be applied again giving that $\lambda_{1,1}, \lambda_{1,2}$ are dependent over $\mathbf{Q}$, a contradiction again.

For the second statement, suppose to the contrary that under the assumptions of the statement, all of $\exp(x_1y_1), \exp(x_1y_2), \exp(x_2y_1), \exp(x_2y_2)$ are algebraic. Using the first part for $\lambda_{i,j} = x_iy_j$ for $i, j = 1, 2$ and noting that

$$\lambda_{1,1}\lambda_{2,2} = x_1x_2y_1y_2 = \lambda_{1,2}\lambda_{2,1},$$

we conclude that $\lambda_{1,1}/\lambda_{1,2} = y_1/y_2$ or $\lambda_{1,1}/\lambda_{2,1} = x_1/x_2$ is rational, which is a contradiction.

9. Prove that there is an effective absolute constant $C > 0$ such that the following holds. Let $a_1/a_2 \in \mathbf{Q}_{\neq 0}$ and let $n \in \mathbf{Z}_{\geq 2}$. Suppose $\sqrt[n]{a_1/a_2} \in [1/10, 10]$. Then for all $p/q \in \mathbf{Q}$ with $p/q \neq \sqrt[n]{a_1/a_2}$, we have

$$|\sqrt[n]{a_1/a_2} - p/q| > q^{-C \log A \log n},$$

where $A = \max(|a_1|, |a_2|, 2)$.

Solution: Let C be sufficiently large, and suppose to the contrary that

$$|\sqrt[n]{a_1/a_2} - p/q| < q^{-C \log A \log n}.$$

Then

$$|\sqrt[n]{a_1/a_2}q/p - 1| < 10q^{-C\log A\log n}.$$

Since log is Lipschitz near 1, this gives

$$|\frac{1}{n}\log(a_1/a_2) + \log(q/p)| < C\exp(-C\log A\log n\log q)$$

if C is large enough. Multiplying both sides by n, using $C\log A\log n\log q > \log(Cn)$ and adjusting the value of C, we get

$$|\log(a_1/a_2) + n\log(q/p)| < \exp(-C\log A\log n\log q).$$

We use Theorem 17 with $n = 2$, $b_1 = 1$, $\alpha_1 = a_1/a_2$, $b_2 = n$ and $\alpha_2 = p/q$. The reason why we need Theorem 17 is that the definition of B in Theorem 16 has the term $\log A_i$, which may be large if we keep a_1, a_2 and n fixed and let p, q grow.

10. Prove that the largest prime factor of $n(n+1)$ goes to infinity as $n \in \mathbf{Z}_{>0}$ goes to infinity.

Solution: Suppose to the contrary that there is a finite set of primes $p_1, \dots, p_k$ such that

$$n = p_1^{b_1}\cdots p_k^{b_k}, \quad n+1 = p_1^{\widetilde{b}_1}\cdots p_k^{\widetilde{b}_k}.$$

for infinitely many n with some $b_1, \dots, b_k, \widetilde{b}_1, \dots, \widetilde{b}_k \in \mathbf{Z}$.

Then

$$|p_1^{b_1-\widetilde{b}_1}\cdots p_k^{b_k-\widetilde{b}_k} - 1| < 1/n$$

and

$$|(b_1-\widetilde{b}_1)\log p_1 + \ldots + (b_k-\widetilde{b}_k)\log p_k| < C/n$$

for some constant C.

On the other hand Theorem 16 (or 17) gives

$$|(b_1-\widetilde{b}_1)\log p_1+\ldots+(b_k-\widetilde{b}_k)\log p_k| > \exp(-C\log\max|b_j-\widetilde{b}_j|) > \exp(-C\log\log n),$$

where we absorbed into the constant C an upper bound for $\log p_j$.

This is in contradiction with our previous upper bound if n is large.

Alternatively, we may use the subspace theorem with $S = \{p_1, \dots, p_k, \infty\}$ in a similar manner to Proposition 8.

11. Let α be an algebraic number of degree $d \in \mathbf{Z}_{\geq 1}$.

- Prove that there is a proper subspace $V \subset \mathbf{Q}^{d+1}$ and a constant $c > 0$ depending on α such that for all $(q, p_1, \dots, p_d) \in \mathbf{Z}^{d+1}$ with

$$|\alpha^j - p_j/q| < c/q \qquad \text{for all } j = 1, \dots, d$$

we have $(q, p_1, \dots, p_d) \in V$.

- Let $P \in \mathbf{R}[X]$ be a polynomial of degree n. Prove that for all $t \in \mathbf{R}_{\geq 0}$, we have
$$\int_0^t e^{t-X} P(X) dX = e^t \sum_{j=0}^{n} \frac{d^j}{dX^j} P(0) - \sum_{j=0}^{n} \frac{d^j}{dX^j} P(t).$$
Conclude that
$$\Big| e^t \sum_{j=0}^{n} \frac{d^j}{dX^j} P(0) - \sum_{j=0}^{n} \frac{d^j}{dX^j} P(t) \Big| \leq C \max_{X \in [0,t]} |P(X)|$$
for some constant $C = C(t)$.
- Let $P \in \mathbf{Z}[X]$ be a polynomial that vanishes to order m at some $a \in \mathbf{Z}$. Prove
$$m! \Big| \sum_{j=0}^{n} \frac{d^j}{dX^j} P(a).$$
- Prove e is transcendental.

Solution: Let $Q(X) = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0 \in \mathbf{Z}[X]$ be the minimal polynomial of α. Suppose $|\alpha^j - p_j/q| < c/q$ for some $(q, p_1, \ldots, p_d) \in \mathbf{Z}^{d+1}$ and $c > 0$ for $j = 1, \ldots, d$. Then

$$|a_d p_d/q + \ldots a_1 p_1/q + a_0| = |a_d(p_d/q - \alpha^d) + \ldots a_1(p_1/q - \alpha^1) + a_0(1-1)|$$
$$\leq (c/q) \sum_{j=1}^{d} |a_j|.$$

Therefore,
$$|a_d p_d + \ldots a_1 p_1 + a_0 q| \leq c \sum_{j=1}^{d} |a_j|.$$
If we take $c < \Big(\sum_{j=1}^{d} |a_j| \Big)^{-1}$, we get
$$a_d p_d + \ldots + a_1 p_1 + a_0 q = 0,$$
so $(q, p_1, \ldots, p_d)$ belongs to the subspace defined by the equation $a_0 X_0 + \ldots + a_d X_d = 0$.

Integrating by parts, we get
$$\int_0^t e^{t-X} P(X) dX = [(-e^{t-X}) P(X)]_0^t - \int_0^t (-e^{t-X}) \frac{d}{dX} P(X) dX$$
$$= e^t P(0) - P(t) + \int_0^t e^{t-X} \frac{d}{dX} P(X) dX.$$
We iterate this until the polynomial vanishes, and we get the formula claimed in the question. Since $|e^{t-X}| \leq e^t$ for $X \in [0, t]$, we have
$$\Big| \int_0^t e^{t-X} P(X) dX \Big| \leq t e^t \max_{X \in [0,t]} |P(X)|,$$
and the claimed inequality follows with $C = te^t$.

Let $P(X) = b_n X^n + \ldots + b_1 X + b_0$. Then

$$\frac{d^j}{dX^j} P(X) = b_n \frac{n!}{(n-j)!} X^{n-j} + \ldots + \frac{j!}{0!} b_j X^0.$$

If $j \geq m$, then $m!$ divides all the coefficients of $(d^j/dX^j)P$, so $m!$ divides its values at integers. Now suppose P vanishes to order m at some $a \in \mathbf{Z}$. Then all terms in $\sum_{j=0}^n (d^j/dX^j)P(a)$ vanish for $j < m$ and they are divisible by $m!$ for $j \geq m$, as noted above. The claim follows.

Suppose to the contrary that e is algebraic af degree d. Fix some large integers m and n with $m > n/10d$, and let $P \in \mathbf{Z}[X]$ be a polynomial of degree at most n that vanishes at $0, \ldots, d$ to order at least m with $\max_{X \in [0,d]} |P(X)| < C_1^n$ for some constant C_1 that we will set depending on d but independently on n and m. Writing $q = (m!)^{-1} \sum_{j=0}^n (d^j/dX^j)P(0)$ and $p_i = (m!)^{-1} \sum_{j=0}^n (d^j/dX^j)P(i)$ for $i = 1, \ldots, d$, we get

$$\leq |e^i q - p_i| \leq C C_1^n / m!$$

Since $m > n/10d$, if n is sufficiently large in terms of C, C_1 and the constant c in the first part, we get

$$|e^i - p_i/q| < c/q.$$

We conclude from the first part that there are integers $a_0, a_1, \ldots, a_d$ depending only on α, so independent of the choice of P such that

$$a_d \sum_{j=0}^n \frac{d^j}{dX^j} P(d) + a_{d-1} \sum_{j=0}^n \frac{d^j}{dX^j} P(d-1) + \ldots + a_0 \sum_{j=0}^n \frac{d^j}{dX^j} P(0) = 0.$$

The easiest way to reach a contradiction is by choosing a sufficiently large prime p that does not divide any of the coefficients $a_0, \ldots, a_d$. Then we set

$$P = x^{p-1}(x-1)^p \cdots (x-d)^p.$$

Then

$$p | \sum_{j=0}^n \frac{d^j}{dX^j} P(b)$$

for $b = 1, \ldots, d$ by our previous observation. We also use that the order p or higher derivative of P is divisible by p. Therefore

$$\sum_{j=0}^n \frac{d^j}{dX^j} P(0) \equiv (x-1)^p \cdots (x-d)^p \mod p,$$

which is non-zero if $p > d$, which we may assume.

Now we see that only one term of the sum

$$a_d \sum_{j=0}^n \frac{d^j}{dX^j} P(d) + a_{d-1} \sum_{j=0}^n \frac{d^j}{dX^j} P(d-1) + \ldots + a_0 \sum_{j=0}^n \frac{d^j}{dX^j} P(0)$$

is divisible by p, hence the sum cannot be 0, a contradiction.

12. Compute the Mahler measure of $p/q \in \mathbf{Q}$ and the roots of $ax^2 + bx + c = 0$ for $a, b, c \in \mathbf{Z}$ in the case $b^2 < 4ac$.

Solution: Assuming $\gcd(p, q) = 1$, the minimal polynomial of p/q is $qx - p$, which has leading coefficient q and one root p/q. Therefore,

$$M(p/q) = |q| \max(|p/q|, 1) = \max(|p|, |q|).$$

Again, assume $\gcd(a, b, c) = 1$. (If not divide by the gcd.) The polynomial $ax^2 + bx + c$ is the minimal polynomial of its roots. Its leading coefficient is a and it has two roots $(b \pm \sqrt{b^2 - 4ac})/2a$. Since $b^2 < 4ac$, both roots have absolute value

$$\Big(\frac{b^2 - (b^2 - 4ac)}{4a^2}\Big)^{1/2} = (c/a)^{1/2}.$$

Therefore, the Mahler measure is

$$|a| \max(1, (c/a)^{1/2})^2 = \max(|a|, |c|).$$

13. Let α be a non-zero algebraic number. Prove that $M(\alpha) \geq 1$. Determine the set of all numbers for which equality is attained.

Solution: Let $a(X - \alpha_1) \cdots (X - \alpha_d)$ be the minimal polynomial of α in $\mathbf{Z}[X]$. Note that $|a| \geq 1$ and $\max(1, |\alpha_j|) \geq 1$ for all j, so $M(\alpha) \geq 1$. Now let $M(\alpha) = 1$. Then $|a| = 1$ and $|\alpha_j| \leq 1$ for all j. On the other hand, $|a| \prod |\alpha_j|$ is the absolute value of the constant coefficient of the minimal polynomial, which is a positive integer, hence at least 1. We conclude that $|\alpha_j| = 1$ for all j. So α is an algebraic integer, and all its Galois conjugates are on the unit circle. By a theorem of Kronecker, α is a root of unity. Conversely, if α is a root of unity, its Mahler measure is 1, which is seen easily form the definition.

If you do not know Kronecker's theorem. Prove that the minimal polynomial of α^n is of degree at most d with coefficients at most 2^d for all n. Therefore, there are $n \neq m$ such that $\alpha^n = \alpha^m$, so $\alpha^{n-m} = 1$.

14. A Perron number is a real algebraic integer α all of whose Galois conjugates have absolute value strictly less than α. Prove that $M(\alpha)$ is a Perron number for all non-zero algebraic numbers α.

Solution: Let $a(X - \alpha_1) \cdots (X - \alpha_d)$ be the minimal polynomial of α in $\mathbf{Z}[X]$. By definition,

$$M(\alpha) = \pm a_d \prod_{j \in A} \alpha_j,$$

where $A = \{j \in \{1, \dots, d\} : |\alpha_j| \geq 1\}$. (Note that each complex α_j comes together with its conjugate, so the product is real.)

Then $M(\alpha)$ is clearly algebraic. We show that it is also integral. To that end, we show that $|M(\alpha)|_v \leq 1$ for all finite place $v \in M_{K,f}$ of the number field $K = \mathbf{Q}(\alpha_1, \dots, \alpha_d)$. As we have seen in the proof

of Proposition 26, Gauss's Lemma applied to the factorization of the minimal polynomial gives

$$|a_d|_v \prod_{j=1}^{d} \max(1, |\alpha_j|_v) = 1.$$

Therefore,

$$|M(\alpha)|_v = |a_d|_v \prod_{j \in A} |\alpha|_v \leq |a_d|_v \max(1, |\alpha_j|_v) \leq 1.$$

It remains to show that $|\sigma(M(\alpha))| < |M(\alpha)|$ for all $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ such that $\sigma(M(\alpha)) \neq M(\alpha)$. Note that

$$\sigma(M(\alpha)) = \pm a_d \prod_{j \in \widetilde{A}} \alpha_j$$

for some $\widetilde{A} \subset \{1, \ldots, d\}$ with $|\widetilde{A}| = |A|$ and $\widetilde{A} \neq A$. Then necessarily there is some $j \in \widetilde{A}$ such that $|\alpha_j| < 1$. Therefore,

$$|\sigma(M(\alpha))| = |a_d| \prod_{j \in \widetilde{A}} |\alpha_j| < |a_d| \prod_{j \in \widetilde{A}} \max(1, |\alpha_j|) \leq \prod_{j=1}^{d} \max(1, |\alpha_j|) = |M(\alpha)|.$$

For an alternative argument to show that $M(\alpha)$ is an algebraic integer, see Section 10.6 in Baker's book titled "A comprehensive course in number theory".