Problem Set Week 8 Solutions

ETHZ Math Olympiad Club

14 April 2025

Simon's Favorite Factoring Trick Problems

SFFT is often used in a Diophantine equation where factoring is needed. We let R be any unitary ring. If we have a multipolynomial in two formal variables X and Y, $P(X, Y) \in R[X, Y]$ of the form

$$P(X, Y) = aXY + bX + cY + d \in R[X, Y]$$

with $a \in R^{\times}$. According to *Simon's Favorite Factoring Trick*, this multipolynomial is:

$$P(X, Y) = a\left(X + a^{-1}c\right)\left(Y + a^{-1}b\right) + d - ca^{-1}b.$$

0.1 AMC 12 (2012)

How many non-congruent right triangles with positive integer leg lengths have areas that are numerically equal to 3 times their perimeters?

Solution:

Solution not written yet

0.2 AIME (1998)

An $m \times n \times p$ rectangular box has half the volume of an $(m+2) \times (n+2) \times (p+2)$ rectangular box, where m, n, and p are integers, and $m \leq n \leq p$. What is the largest possible value of p?

Solution:

Solution not written yet

0.3 BMO (2005)

The integer N is positive. There are exactly 2005 ordered pairs (x, y) of positive integers satisfying:

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{N}.$$

Prove that N is a perfect square.

Solution:

Solution not written yet

0.4 JBMO (2003)

Let n be a positive integer. A number A consists of $2n$ digits, each of which is 4; and a number B consists of n digits, each of which is 8. Prove that $A + 2B + 4$ is a perfect square.

Solution:

Solution not written yet

0.5 AIME (2000)

The system of equations

$$\log_{10}(2000xy) - \log_{10}(x)\log_{10}(y) = 4,$$
$$\log_{10}(2yz) - \log_{10}(y)\log_{10}(z) = 1,$$
$$\log_{10}(zx) - \log_{10}(z)\log_{10}(x) = 0,$$

has two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2). Find $y_1 + y_2$.

Solution:

Solution not written yet

Problem (Wu-Riddles)

Let $n \in \mathbb{N}_{>0}$ and $A, B \in \mathbb{R}^{n \times n}$ be real matrices. Now suppose $I_n - BA$ is invertible, where I_n is the identity matrix. Prove that $I_n - AB$ is also invertible.

Solution:

Let $(R, +_R, \cdot_R, 0_R, 1_R)$ be any (possibly non-commutative) unital ring, let $c, b \in R$, we show that:
$$1_R - bc \in R^\times \leftrightarrow 1_R - cb \in R^\times.$$

By symmetry in $b, c \in R$, we only need to prove one direction of the equivalence. So suppose $1_R - bc \in R^\times$; we show $1_R - cb \in R^\times$.

We claim that the element
$$1_R + c \, (1_R - bc)^{-1} \, b \in R$$

is the inverse of $1_R - cb$; for this, we have to show it is a right inverse:

$$
\begin{aligned}
(1_R - cb) \left(1_R + c \, (1_R - bc)^{-1} \, b \right) &= 1_R - cb + c \, (1_R - bc)^{-1} \, b \\
&\quad - cbc \, (1_R - bc)^{-1} \, b \\
&= 1_R - cb + c \, (1_R - bc) \, (1_R - bc)^{-1} \, b \\
&= 1_R - cb + cb = 1_R.
\end{aligned}
$$

We now verify it is a left inverse (recalling that for any element $a \in R$, we have $-a = (-1_R)a$ and that -1_R commutes with every element in R):

$$
\begin{aligned}
\left(1_R + c \, (1_R - bc)^{-1} \, b \right) (1_R - cb) &= 1_R - cb + c \, (1_R - bc)^{-1} \, b \\
&\quad + c \, (1_R - bc)^{-1} \, b(-cb) \\
&= 1_R - cb + c \, (1_R - bc)^{-1} \, b \\
&\quad + c \, (1_R - bc)^{-1} \, (-bc)b \\
&= 1_R - cb + c \, (1_R - bc)^{-1} \, (1_R - bc) \, b \\
&= 1_R - cb + cb = 1_R.
\end{aligned}
$$

Apply this result to the non-commutative unital ring $(\mathbb{R}^{n \times n}, +, \cdot, \mathbf{0}_{n \times n}, I_n)$.

Problem (unknown)

An enemy submarine is hidden somewhere along the infinite line $\mathbb{R}$. It travels silently, and you know that its path is described by a fixed rational polynomial rule $\sum_{i=0}^{n} c_i T^i \in \mathbb{Q}[X]$; for each time $t \in \mathbb{N}$, its position is given by

$$x(t) = \sum_{i=0}^{n} c_i t^i \in \mathbb{Q}.$$

However, you do not know $n \in \mathbb{N}$, nor the rational coefficients $(c_i)_{i \in n} \in \mathbb{Q}^n$ that form this rational polynomial rule.

Each unit of time (starting from 0), you are allowed to launch a single torpedo at any chosen rational position. If the submarine is at that position at that time, it is struck and sinks. Assume you possess a potentially countably infinite arsenal of torpedoes and potentially countably infinite time.

Devise a strategy — a sequence of torpedo launches — such that, regardless of the submarine's unknown position, you will **eventually** hit it.

Solution:

This solution needs to be written more formally

Notice that $\forall t \in \mathbb{N}$, we have $x(t) \in \mathbb{Q}$. We must find a function

$$f : \mathbb{N} \to \mathbb{Q}$$

(which represents the sequence of torpedo launches — one per unit of time) such that there exists a time $\tilde{t} \in \mathbb{N}$ with

$$f(\tilde{t}) = x(\tilde{t}).$$

The strategy is the following: assume the submarine does not move, i.e. $x(T) = c_0 \in \mathbb{Q}[T]$, then taking any bijection $g : \mathbb{N} \simeq \mathbb{Q}$ and defining $f(t) = g(t)$ works.

If the submarine moves linearly, $x(T) = c_0 + c_1 T \in \mathbb{Q}[T]$, since we do not know c_0, c_1, we enumerate each 2-tuple of rationals in the following way: suppose it started with (c_0', c_1'), and knowing the elapsed time t, we shoot at position $c_0' + c_1' t$. If it truly started with (c_0', c_1'), then we would certainly hit it. If it did not start with (c_0', c_1') and by chance we still hit it, we are done; otherwise, we proceed to try another pair (c_0'', c_1''), and continue this process, incrementing time to $t' = t + 1$ each unit of time. Taking any bijection $g : \mathbb{N} \simeq \mathbb{Q}^2$ and defining $f(t) = g(t)(0) + g(t)(1)t$ works.

If the submarine moves quadratically, $x(T) = c_0 + c_1 T + c_2 T^2 \in \mathbb{Q}[T]$, again, since we do not know c_0, c_1, c_2, we enumerate each 3-tuple of rationals similarly: suppose it started with (c_0', c_1', c_2'), and knowing the elapsed time t, we shoot at position $c_0' + c_1' t + c_2' t^2$. If it truly started with (c_0', c_1', c_2'), we would certainly hit it. If it did not start with that and we still hit it by chance, we are done; otherwise, we proceed to try another triple (c_0'', c_1'', c_2''), incrementing time each step. Taking any bijection $g : \mathbb{N} \simeq \mathbb{Q}^3$ and defining $f(t) = g(t)(0) + g(t)(1)t + g(t)(2)t^2$ works.

The problem you may raise is: we already enumerate $\mathbb{Q}$ in the case the submarine does

not move. How can we have finished that enumeration and moved on to the linear case, and further to the quadratic case, etc.?

The key observation is that we can enumerate all of them simultaneously in a single shot! Indeed, we can enumerate all *finite* sequences of rationals because

$$\mathbb{N} \simeq \bigcup_{k \in \mathbb{N}} \mathbb{Q}^k =: \mathbb{Q}^{<\omega}.$$

Any bijection $g : \mathbb{N} \simeq \mathbb{Q}^{<\omega}$ suffices, since then the strategy at time $t \in \mathbb{N}$ is, if $g(t) = (c_i')_{i \in k}$, to shoot at $\sum_{i \in k} c_i' t^i$. That is, the sequence of torpedo launches $f : \mathbb{N} \to \mathbb{Q}$ is defined by:

$$f(t) := \sum_{i \in \text{dom}(g(t))} g(t)(i) t^i.$$

You may object that such a bijection $g : \mathbb{N} \to \mathbb{Q}^{<\omega}$ requires the axiom of choice and is not realisable in practice; however, we prove otherwise by providing multiple constructive examples of such bijections.

First, we show that $\mathbb{N} \simeq \mathbb{Q}$. Define $s : \mathbb{N} \to \mathbb{Z}$ for $n \in \mathbb{N}$ by:

$$s(n) = (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor,$$

which is clearly a bijection. (The sequence $s(0), s(1), s(2), s(3), \ldots$ is $0, -1, 1, -2, 2, \ldots$, a bijection from $\mathbb{N}$ to $\mathbb{Z}$.)

It suffices then to find a bijection between $\mathbb{Z}$ and $\mathbb{Q}$. Any bijection $h_+ : \mathbb{Z}_{>0} \to \mathbb{Q}_{>0}$ induces a bijection $h : \mathbb{Z} \to \mathbb{Q}$ defined by:

$$h(n) = \begin{cases} h_+(n) & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ -h_+(-n) & \text{if } n < 0. \end{cases}$$

It remains to find a bijection $h_+ : \mathbb{Z}_{>0} \to \mathbb{Q}_{>0}$. Every positive integer has a unique prime factorisation $p_1^{a_1} p_2^{a_2} \cdots$, where p_i is the i-th prime and the a_i are non-negative integers, almost all zero. Similarly, every positive rational number has a unique expression $p_1^{b_1} p_2^{b_2} \cdots$ with finitely many non-zero integers b_i.

Thus, for any $n = p_1^{a_1} p_2^{a_2} \cdots \in \mathbb{Z}_{>0}$, define

$$h_+(n) := p_1^{s(a_1)} p_2^{s(a_2)} \cdots .$$

This defines a bijection $h_+ : \mathbb{Z}_{>0} \to \mathbb{Q}_{>0}$, and h gives a bijection $\mathbb{Z} \to \mathbb{Q}$, hence $\mathbb{N} \simeq \mathbb{Q}$.

Such a bijection induces one between $\mathbb{N}^{<\omega}$ and $\mathbb{Q}^{<\omega}$. So, to get a bijection between $\mathbb{N}$ and $\mathbb{Q}^{<\omega}$, it suffices to give one between $\mathbb{N}$ and $\mathbb{N}^{<\omega}$. We give three examples $f_1, f_2, f_3 : \mathbb{N}^{<\omega} \to \mathbb{N}$ below:

The prime encoding bijection:

$$f_1((a_0, a_1, \ldots, a_{k-1})) := \prod_{i=0}^{k-1} p_i^{a_i+1} - 1,$$

where p_i is the i-th prime. Note $f_1(\varepsilon) = 0$.

The multiset rank encoding bijection:

$$f_2((a_0, a_1, \ldots, a_{k-1})) := \sum_{j=0}^{k-1} \binom{a_j + j}{j + 1}.$$

Again, $f_2(\varepsilon) = 0$.

The recursive Cantor pairing bijection:

Recall the Cantor pairing function:

$$\pi(a, b) := \frac{1}{2}(a + b)(a + b + 1) + b.$$

Define recursively:

$$f_3(\varepsilon) := 0, \quad f_3((a_0, \ldots, a_k)) := \pi(a_0, f_3((a_1, \ldots, a_k))) + 1.$$

These induce constructive bijections $g_1, g_2, g_3 : \mathbb{N} \to \mathbb{Q}^{<\omega}$.

Now, we show that any bijection $g : \mathbb{N} \to \mathbb{Q}^{<\omega}$ induces a well-defined strategy that works. Technically, we only use the surjectivity of g. Let n and $\mathbf{c} := (c_i)_{i \in n} \in \mathbb{Q}^n$ be the true coefficients of the submarine's trajectory. Then by surjectivity of g, there exists $\tilde{t} \in \mathbb{N}$ such that

$$g(\tilde{t}) = \mathbf{c}.$$

At time $\tilde{t}$, the difference between our shot and the submarine's position is:

$$f(\tilde{t}) - x(\tilde{t}) = \left(\sum_{j \in \mathrm{dom}(\mathbf{c})} \mathbf{c}(j)\tilde{t}^j \right) - \left(\sum_{i=0}^{n} c_i \tilde{t}^i \right) = 0.$$

Thus, the torpedo launched at time $\tilde{t}$ will hit the submarine.

The overall strategy is simply to apply f recursively:

At time $t = 0$, shoot at $f(0)$; $\quad t = 1$, shoot at $f(1)$; $\quad t = 2$, shoot at $f(2)$; $\quad \ldots$

By construction, there will be a finite time $\tilde{t}$ when the torpedo hits the submarine.

Problem B1 (Putnam 1960) & A1 (Putnam 1961)

Define
$$A := \{(x, y) \in \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \ : \ x^y = y^x\}\,^{[1]}$$
and find:
$$A, \quad A \cap (\mathbb{Q} \times \mathbb{Q}) \quad \text{and} \quad A \cap (\mathbb{Z} \times \mathbb{Z})\,.$$

Solution:

For general culture: knowing the construction of $\mathbb{R}$ using equivalence classes of rational Cauchy sequences, recall that one can unambiguously define the power a^b (for $a > 0$ and $b \in \mathbb{R}$) in two equivalent ways.

The first method uses the theory of power series and their convergence (which must be developed); using the exponential and logarithmic functions, we define $a^b := \exp(b \cdot \log(a))$.

The second method is a constructive, step-by-step approach: one first defines a^b where b is an integer, then extends to the rationals, and finally to the real numbers.

Since $\exp$ is a group morphism with $\exp(1) > 0$, we can show for all $x \in \mathbb{R}$ the equality $\exp(x) = \exp(1)^x$, where the left-hand side uses power series and the right-hand side uses the constructive approach. Thus, we can easily show that the two definitions of exponentiation yield the same result. The exponentiation a^b, where $a > 0$ and $b \in \mathbb{R}$, can be extended to $a = 0$ and $b \geq 0$, and to $a \in \mathbb{R}^\times$ with $b \in \mathbb{Z}$, as mentioned in the hyperlink (and 0^x is continuous at x, except at $x = 0$). For more information, see the article on Exponentiation, where you can find the proofs in Terence Tao's book *Analysis I*.

Let us now solve the form of A: notice that $(x, y) \in A \Leftrightarrow (y, x) \in A$. Clearly, $\Delta(\mathbb{R}_{\geq 0}) = \{(x, x) \in \mathbb{R}_{\geq 0}\} \subset A$. We now determine $A \setminus \Delta(\mathbb{R}_{\geq 0})$.

Let $(x, y) \in A \setminus \Delta(\mathbb{R}_{\geq 0})$. Then there exists $t \in \mathbb{R}_{\geq 0}$ such that $y = tx$. By hypothesis, $t \neq 1$. If $y = 0$, then since $0 \leq x \neq y$, we have $x > 0$, but $x^y = y^x$ implies in this case $1 \overset{x \geq 0}{=} x^0 = 0^x \overset{x \geq 0}{=} 0$, which is a contradiction. Thus, $y > 0$. Also, if $t = 0$, then $y = 0$, a contradiction. So $t \in \mathbb{R}_{>0} \setminus \{1\}$. Now, if $x = 0$, then $y = 0$, which is also excluded by hypothesis. Therefore, $x, y > 0$. Knowing this, from $x^y = y^x$ we compute:
$$x^{tx} = (tx)^x \Rightarrow t^x = x^{(t-1)x} = \left(x^{t-1}\right)^x\,.$$

Since $x > 0$, the map $a \mapsto a^x$ on $\mathbb{R}_{\geq 0}$ is bijective. This implies from the above equality that $x^{t-1} = t$. Since $t \neq 1$, this implies that $x = t^{\frac{1}{t-1}}$. Therefore:
$$(x, y) = \left(t^{\frac{1}{t-1}}, \ t \cdot t^{\frac{1}{t-1}}\right) = \left(t^{\frac{1}{t-1}}, \ t^{\frac{t}{t-1}}\right)\,.$$

This shows that:
$$A \setminus \Delta(\mathbb{R}_{\geq 0}) \subset \left\{\left(t^{\frac{1}{t-1}}, \ t^{\frac{t}{t-1}}\right) \ \Big| \ t \in \mathbb{R}_{>0} \setminus \{1\}\right\}\,.$$

---

[1] Recall that the exponentiation $a^b := \exp(b \cdot \log(a))$ where $a > 0$ and $b \in \mathbb{R}$ can be extended to $a = 0$ and $b \geq 0$ by:
$$0^b = \begin{cases} 0 & (b > 0), \\ 1 & (b = 0). \end{cases}$$
and extended in the obvious way for $a \in \mathbb{R}^\times$ with $b \in \mathbb{Z}$.

We define in consequence the set

$$S := \left\{ \left(t^{\frac{1}{t-1}},\ t^{\frac{t}{t-1}} \right) \,\middle|\, t \in \mathbb{R}_{>0} \setminus \{1\} \right\} \subset \mathbb{R}_{>0} \times \mathbb{R}_{>0}.$$

The map f defined over $\mathbb{R}_{>0} \setminus \{1\}$ by

$$t \mapsto \left(t^{\frac{1}{t-1}},\ t^{\frac{t}{t-1}} \right)$$

is clearly injective onto S and satisfies the identity

$$\left(t^{\frac{1}{t-1}},\ t^{\frac{t}{t-1}} \right) = \left(\left(\frac{1}{t}\right)^{\frac{1}{1-t}},\ \left(\frac{1}{t}\right)^{\frac{t}{1-t}} \right) = \left(\left(\frac{1}{t}\right)^{\frac{\frac{1}{t}}{\frac{1}{t}-1}},\ \left(\frac{1}{t}\right)^{\frac{1}{\frac{1}{t}-1}} \right),$$

that is, it swaps coordinates under precomposition with the involution $\_^{-1} : t \mapsto \frac{1}{t}$ of $\mathbb{R}_{>0} \setminus \{1\}$:

$$f = \mathrm{swap} \circ f \circ \_^{-1}.$$

For the reverse inclusion $S \subset A \setminus \Delta\left(\mathbb{R}_{\geq 0}\right)$, let $t \in \mathbb{R}_{>0} \setminus \{1\}$. It suffices to check that we have:

$$\left(t^{\frac{1}{t-1}} \right)^{\left(t^{\frac{t}{t-1}} \right)} = \left(t^{\frac{t}{t-1}} \right)^{\left(t^{\frac{1}{t-1}} \right)} \quad \text{and} \quad t^{\frac{1}{t-1}} \neq t^{\frac{t}{t-1}} = t \cdot t^{\frac{1}{t-1}}$$

Indeed, using the properties of powers:

$$\left(t^{\frac{1}{t-1}} \right)^{\left(t^{\frac{t}{t-1}} \right)} = t^{\left(\frac{1}{t-1} \cdot \left(t^{\frac{t}{t-1}} \right) \right)} = t^{\frac{\left(t^{\frac{t}{t-1}} \right)}{t-1}},$$

and

$$\left(t^{\frac{t}{t-1}} \right)^{\left(t^{\frac{1}{t-1}} \right)} = t^{\left(\frac{t}{t-1} \cdot \left(t^{\frac{1}{t-1}} \right) \right)} = t^{\frac{t \cdot \left(t^{\frac{1}{t-1}} \right)}{t-1}} = t^{\frac{\left(t^{\frac{t}{t-1}} \right)}{t-1}}.$$

Both are equal, therefore:

$$\left(t^{\frac{t}{t-1}} \right)^{\left(t^{\frac{1}{t-1}} \right)} = \left(t^{\frac{1}{t-1}} \right)^{\left(t^{\frac{t}{t-1}} \right)},$$

and if $t^{\frac{1}{t-1}} = t^{\frac{t}{t-1}}$ then since $t > 0$ we have $t^{\frac{1}{t-1}} > 0$ so that we can divide by $t^{\frac{1}{t-1}}$ and obtain that $t = 1$ a contradiction to $t \in \mathbb{R}_{>0} \setminus \{1\}$. All of this shows the nice decomposition of A into two symmetric (with respect to swapping the variable) set. Namely the identity line and a symmetric (with respect to the line) curve:

$$A = \Delta(\mathbb{R}_{\geq 0}) \sqcup S.$$

Now it remains to find $A \cap (\mathbb{Q} \times \mathbb{Q})$ and $A \cap (\mathbb{N} \times \mathbb{N})$.

Clearly:

$$\Delta(\mathbb{R}_{\geq 0}) \cap (\mathbb{Q} \times \mathbb{Q}) = \Delta(\mathbb{Q}_{\geq 0}) \quad \text{and} \quad \Delta(\mathbb{R}_{\geq 0}) \cap (\mathbb{Z} \times \mathbb{Z}) = \Delta(\mathbb{Z}_{\geq 0}).$$

We first find $S \cap (\mathbb{Z} \times \mathbb{Z})$ without relying on the more complicated set $S \cap (\mathbb{Q} \times \mathbb{Q})$. We can quickly understand why:

$$S \cap (\mathbb{Z} \times \mathbb{Z}) = \{(2, 4), (4, 2)\}.$$

Indeed, the inclusion $\supset$ is clear. Now, for a pair $(n, m) \in S \cap (\mathbb{Z} \times \mathbb{Z})$, we may assume that $n < m$ (since the set is symmetric with respect to swapping the variables). If we show that $(n, m) = (2, 4)$, we are done, as this proves $\subset$. So, without further ado, since $n, m > 0$:

$$n \cdot \log(m) = m \cdot \log(n) \Rightarrow \frac{\log(n)}{n} = \frac{\log(m)}{m}.$$

Let us consider the function $f(x) = \frac{\log(x)}{x}$ for $x > 0$. Its derivative is

$$f'(x) = \frac{1 - \log(x)}{x^2},$$

which vanishes at e, is positive on $]0, e[$, and negative on $]e, +\infty[$. Therefore, by standard theorems relating monotonicity and derivatives, f strictly increases on $]0, e[$, strictly decreases on $]e, +\infty[$, and thus attains a maximum at e (with value $\frac{1}{e} < 0.5$). In particular, the functions $f|_{]0,e[}$ and $f|_{]e,+\infty[}$ are bijective. This means that for $f(n) = f(m)$, we must have (since $n < m$ and $n, m \neq e$) that $n \in]0, e[$ and $m \in]e, +\infty[$.

Hence, $n \in \{1, 2\}$. If $n = 1$, then $m^1 = 1^m \Rightarrow m = 1$, which contradicts $n \neq m$. So $n = 2$. Then $m^2 = 2^m$. Since both sides are integers and $\mathbb{Z}$ is a UFD, m must be a power of 2: $m = 2^k$ for some $k \in \mathbb{N} \setminus \{0, 1\}$ (as $m > e > 2$). Then, by unique factorisation into primes:

$$2^{2k} = 2^{2^k} \Rightarrow 2k = 2^k.$$

We want to restrict the possible values of $k \geq 2$ for this equality. Consider the function g defined for all $x \in \mathbb{R}$, by $g(x); = 2^x - 2x$. Its derivative is

$$g'(x) = \log(2) \cdot 2^x - 2.$$

We ask for which $x \in \mathbb{R}$, $2^x = 2x$. Since 2^x is strictly increasing, we find that $g'(x) > 0$ if and only if

$$x > \log_2\left(\frac{2}{\log(2)}\right) = 1 - \log_2(\log(2)),$$

and this value lies strictly between 1 and 2, since $-1 = \log_2\left(\frac{1}{2}\right) < \log_2(\log(2)) < \log_2(1) = 0$, as $\frac{1}{2} < \log(2) < 1$, and $\log_2$ is strictly increasing. Hence, by standard theorems relating monotonicity and derivatives, g is at least strictly increasing on $[2, +\infty)$. Since $g(2) = 0$, we have $g(x) > 0$ for $x > 2$, implying that $k = 2$ is the only solution.

Therefore, $m = 2^2 = 4$, and so $(n, m) = (2, 4)$. This concludes the argument.

To finish the problem, we compute $S \cap (\mathbb{Q} \times \mathbb{Q})$.

This is a Diophantine equation that has evoked considerable attention since the days of Euler, who treated it in *Introductio in Analysin Infinitorum* II, page 294. He noticed that if $s \in \mathbb{Z}_{>0}$, then $t(s) := 1 + \frac{1}{s} \in \mathbb{Q}_{>0} \setminus \{1\}$ was such that, through the parametrisation $f(t(s)) \in S$, we have $f(t(s)) \in \mathbb{Q} \times \mathbb{Q}$. Indeed,

$$\frac{1}{t(s) - 1} = s \quad \text{and} \quad \frac{t(s)}{t(s) - 1} = 1 + \frac{1}{t(s) - 1} = 1 + s,$$

thus:

$$f(t(s)) = \left(t(s)^s, t(s)^{1+s}\right) = \left(\left(1 + \frac{1}{s}\right)^s, \left(1 + \frac{1}{s}\right)^{s+1}\right)$$

is certainly a pair of rational numbers.

For now, the problem of such "commutativity of exponentiation" has been active in various settings. The problem appeared in both the 1960 and 1961 Putnam Prize Competitions. There is Banach's result that the same equation has infinitely many solutions in transfinite

cardinals, and Jacobsthal's theorem on the general solution in transfinite ordinal numbers. A description of all complex algebraic solutions appears to be unknown. For related result results, see the proposed papers, [1], and [2].

By symmetry with respect to swapping coordinates of S, and what we have shown previously, we get:

$$\left\{ \left(\left(1+\frac{1}{s}\right)^{s+\tau}, \left(1+\frac{1}{s}\right)^{s+1-\tau} \right) \,\middle|\, s \in \mathbb{Z}_{>0}, \, \tau \in \{0,1\} \right\} \subset S \cap (\mathbb{Q} \times \mathbb{Q}).$$

We shall show that the reverse inclusion $\supset$ holds by reproducing the full solution given in [3]. Let $(n,m) \in S \cap (\mathbb{Q} \times \mathbb{Q})$, and suppose that $(n,m) \notin \mathbb{Z} \times \mathbb{Z}$, otherwise we already know that $(n,m) \in \{(2,4),(4,2)\}$. The goal is to show that $\exists s \in \mathbb{Z}_{>0}$ and $\tau \in \{0,1\}$ with $m = \left(1+\frac{1}{s}\right)^{1+s-\tau}$ and $n = \left(1+\frac{1}{s}\right)^{s+\tau}$. Since the set is symmetric with respect to swapping the variables, we may again assume that $n < m$ so that in fact τ needs to be 0.

Notice that $n > 1$ since if $n \leq 1$, then

$$n^m \overset{\text{hyp}}{=} m^n \overset{m > n}{>} n^n \overset{\overset{1 \geq n}{m > n}}{\geq} n^m,$$

a contradiction to $(n,m) \in S$. Thus $m > n > 1$. Now, write $m = \frac{a}{b}$, $n = \frac{c}{d}$ for $a,b,c,d \in \mathbb{Z}_{>0}$ with $\gcd(a,b) = \gcd(c,d) = 1$. Then $m > n > 1$ implies $a > b > 0$, $c > d > 0$, and $ad > bc$. Write $1 < \frac{ad}{bc} = \frac{\lambda}{\mu}$ for $\lambda, \mu \in \mathbb{Z}_{>0}$ with $\gcd(\lambda, \mu) = 1$ and $\lambda > \mu$.

If $\left(\frac{a}{b}\right)^{\frac{c}{d}} = \left(\frac{c}{d}\right)^{\frac{a}{b}}$, then $\left(\frac{a}{b}\right)^{bc} = \left(\frac{c}{d}\right)^{ad}$, and so $a^{bc} d^{ad} = c^{ad} b^{bc}$. Now, because $\gcd(a,b) = \gcd(c,d) = 1$ and $a,b,c,d > 0$, we have

$$a^{bc} = c^{ad} \quad \text{and} \quad b^{bc} = d^{ad}, \tag{1}$$

since $\mathbb{Z}$ is a UFD. We have that a and c share the same primes in their canonical representations as products of powers of primes, and so must b and d. That is, there exist $k_1, k_2 \in \mathbb{N}$ with distinct prime factors $p \colon k_1 \hookrightarrow \mathbb{P}$, $q \colon k_2 \hookrightarrow \mathbb{P}$ with $\mathrm{ran}(p) \cap \mathrm{ran}(q) = \varnothing$, $\forall i \in k_1$, $v_{p_i}(a), v_{p_i}(c) \geq 1$, $\forall j \in k_2$, $v_{q_j}(b), v_{q_j}(d) \geq 1$, and:

$$a = \prod_{i \in k_1} p_i^{v_{p_i}(a)}, \quad c = \prod_{i \in k_1} p_i^{v_{p_i}(c)}, \quad b = \prod_{j \in k_2} q_j^{v_{q_j}(b)}, \quad d = \prod_{j \in k_2} q_j^{v_{q_j}(d)}.$$

In the case of a and c, these are certainly not empty products since $a > b > 0$ and $c > d > 0$, so $a > 1$, $c > 1$, that is, $k_1 \geq 1$. If $k_2 = 0$, then $b = 1 = d$, so $m = a$ and $n = c$, thus $(m,n) \in \mathbb{N} \times \mathbb{N}$, a contradiction to the choice of $(m,n) \notin \mathbb{N} \times \mathbb{N}$. Therefore, we must also have that the case of b and d involves non-empty products.

It follows from (1) and the fact that the primes are distinct that for each $i \in k_1$ and $j \in k_2$, $v_{p_i}(a)\,bc = v_{p_i}(c)\,ad$ and $v_{q_j}(b)\,bc = v_{q_j}(d)\,ad$, so that (since everything is strictly greater than 0):

$$\frac{v_{p_i}(a)}{v_{p_i}(c)} = \frac{ad}{bc} = \frac{\lambda}{\mu}, \text{ and } \frac{v_{q_j}(b)}{v_{q_j}(d)} = \frac{ad}{bc} = \frac{\lambda}{\mu}.$$

Furthermore, we see that $\mu v_{p_i}(a) = \lambda v_{p_i}(c)$ and $\mu v_{q_j}(b) = \lambda v_{q_j}(d)$. Since $\gcd(\lambda, \mu) = 1$, we conclude that $\lambda \mid v_{p_i}(a)$, $\lambda \mid v_{q_j}(b)$, $\mu \mid v_{p_i}(c)$, $\mu \mid v_{q_j}(d)$. We define in consequence, for each $i \in k_1$ and $j \in k_2$, the following integers:

$$\rho_i := \frac{v_{p_i}(a)}{\lambda} = \frac{v_{p_i}(c)}{\mu} \in \mathbb{Z}_{>0}, \quad \text{and} \quad \tilde{\rho}_j := \frac{v_{q_j}(b)}{\lambda} = \frac{v_{q_j}(d)}{\mu} \in \mathbb{Z}_{>0},$$

10

and define the corresponding products $r := \prod_{i \in k_1} p_i^{\rho_i} \in \mathbb{Z}_{>0}$, $s := \prod_{j \in k_2} q_j^{\tilde{\rho}_j} \in \mathbb{Z}_{>0}$. Then $r, s > 1$ since $k_1, k_2 \geq 1$ and $\rho_i, \tilde{\rho}_j > 0$ respectively. By construction,

$$a = r^\lambda, \quad c = r^\mu, \quad b = s^\lambda, \quad d = s^\mu.$$

Hence

$$\frac{\lambda}{\mu} = \frac{ad}{bc} = \frac{r^\lambda s^\mu}{s^\lambda r^\mu} = \frac{r^{\lambda-\mu}}{s^{\lambda-\mu}} \Rightarrow \mu r^{\lambda-\mu} = \lambda s^{\lambda-\mu}.$$

Since $\lambda > \mu > 0$, we get that $\lambda - \mu \in \mathbb{Z}_{>0}$, and so $r^{\lambda-\mu}, s^{\lambda-\mu} \in \mathbb{Z}_{>0}$. The fact that $\gcd(\lambda, \mu) = 1$ implies that $\lambda \mid r^{\lambda-\mu}$ and $\mu \mid s^{\lambda-\mu}$. Since $\gcd(r, s) = 1$, we have $\gcd\left(r^{\lambda-\mu}, s^{\lambda-\mu}\right) = 1$, which implies that $r^{\lambda-\mu} \mid \lambda$ and $s^{\lambda-\mu} \mid \mu$. Since everything is positive, the only possibility is that

$$\lambda = r^{\lambda-\mu}, \quad \mu = s^{\lambda-\mu} \text{ thus } \lambda - \mu = r^{\lambda-\mu} - s^{\lambda-\mu}. \tag{2}$$

But (2) can hold only if $\lambda - \mu = 1$. For, suppose that $\lambda - \mu > 1$. Since $r > s$,

$$r^{\lambda-\mu} \overset{r \geq s+1}{\geq} (s+1)^{\lambda-\mu}$$

$$= \sum_{k=0}^{\lambda-\mu} \binom{\lambda-\mu}{k} s^{\lambda-\mu-k}$$

$$\overset{\lambda-\mu \geq 2}{=} s^{\lambda-\mu} + (\lambda - \mu)s^{\lambda-\mu-1} + \sum_{k=2}^{\lambda-\mu} \binom{\lambda-\mu}{k} s^{\lambda-\mu-k}$$

$$\overset{s>0}{>} s^{\lambda-\mu} + (\lambda - \mu)s^{\lambda-\mu-1}$$

$$\overset{s>1}{\geq} s^{\lambda-\mu} + \lambda - \mu.$$

It follows that $r^{\lambda-\mu} - s^{\lambda-\mu} > \lambda - \mu$, which is a contradiction since $\lambda - \mu = r^{\lambda-\mu} - s^{\lambda-\mu}$. Thus $\lambda - \mu \leq 1$, and since $\lambda - \mu \in \mathbb{Z}_{>0}$, we get $\lambda - \mu = 1$.

Equation (2) rewrites as:
$$\lambda = r, \quad \mu = s \text{ and } 1 = r - s.$$

From $\lambda = r = 1 + s$, we get

$$a = r^\lambda = (1+s)^{1+s}, \quad c = r^\mu = (1+s)^s, \quad b = s^\lambda = s^{1+s}, \quad d = s^\mu = s^s.$$

Getting back to m and n, we obtain:

$$m = \frac{a}{b} = \left(1 + \frac{1}{s}\right)^{1+s}, \quad n = \frac{c}{d} = \left(1 + \frac{1}{s}\right)^s.$$

This concludes since $s \in \mathbb{Z}_{>0}$.

Summarising, we get:
$$A \cap (\mathbb{Z} \times \mathbb{Z}) = \Delta(\mathbb{Z}_{>0}) \sqcup \{(2,4),(4,2)\}$$

and

$$A \cap (\mathbb{Q} \times \mathbb{Q}) = \Delta(\mathbb{Q}_{\geq 0}) \sqcup \left\{ \left(\left(1 + \frac{1}{s}\right)^{s+\tau}, \left(1 + \frac{1}{s}\right)^{s+1-\tau} \right) \,\middle|\, s \in \mathbb{Z}_{>0}, \tau \in \{0,1\} \right\}.$$

Remark. Notice that as $\mathbb{Z}_{>0} \ni s \to +\infty$, we have $\left(1 + \frac{1}{s}\right)^s \nearrow e$ and $\left(1 + \frac{1}{s}\right)^{s+1} \searrow e$, where e is the Euler constant (transcendental), by a standard result in analysis.

Remark. One could pose the same question over $\mathbb{C}$ or $\mathbb{R}$, restricting to pairs for which the exponentiation is well-defined. In the real case, one may analyse the possible quadrants for (x, y), such as when the signs are compatible or when a sign change occurs. In the complex case: one must restrict to a branch of the logarithm, typically the principal branch, and exclude points where log is undefined, e.g., at 0. Branch cuts and multivaluedness must be acknowledged: x^y is generally not single-valued in $\mathbb{C}$, so the equation must be interpreted either as equality of principal values, as set equality up to branch multiples, or as a non-empty set intersection. This has been partially addressed in the rational case in [3]. In both case, one can similarly ask the intersection question with $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Q} \times \mathbb{Q}$, and obtain almost the same result (for negative rationals and negative integers). This does not require significantly more work, but care is needed since we are working in a domain where exponentiation is sparsely defined.

Bonus: Find $A \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right)$ and $A \cap \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \times \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \right)$.

Solution:

Clearly, $\Delta\left(\mathbb{R}_{\geq 0}\right) \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right) = \Delta\left(\mathbb{Q}^{\mathrm{alg}} \cap \mathbb{R}_{\geq 0} \right)$ and $\Delta\left(\mathbb{R}_{\geq 0}\right) \cap \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \times \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \right) = \Delta\left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \cap \mathbb{R}_{\geq 0} \right)$.

We now compute $S \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right)$ and $S \cap \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \times \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \right)$ by following the solutions provided in [4], which make use of the parametrisation of S by f.

For the computation of $S \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right)$, let $t \in \mathbb{Q}_{>0} \setminus \{1\}$; then certainly $f(t) \in S$. Write $t = \frac{t_1}{t_2}$ for $t_1, t_2 \in \mathbb{Z}_{>0}$ with $\gcd(t_1, t_2) = 1$. Then

$$\frac{1}{t-1} = \frac{t_2}{t_1 - t_2} \in \mathbb{Q}, \quad \text{and} \quad \frac{t}{t-1} = 1 + \frac{1}{t-1} = \frac{t_1}{t_1 - t_2} \in \mathbb{Q}.$$

We get that $t^{\frac{1}{t-1}} = t^{\frac{t_2}{t_1 - t_2}}$ and $t^{\frac{t}{t-1}} = t^{\frac{t_1}{t_1 - t_2}}$; thus, for $\mathrm{sign}(t_2 - t_1)(t_2 - t_1) \in \mathbb{Z}_{>0}$, we get

$$\left(t^{\frac{1}{t-1}} \right)^{\mathrm{sign}(t_2 - t_1)(t_2 - t_1)} = t^{\mathrm{sign}(t_2 - t_1)t_2} \in \mathbb{Q},$$

and

$$\left(t^{\frac{t}{t-1}} \right)^{t_2 - t_1} = t^{\mathrm{sign}(t_2 - t_1)t_1} \in \mathbb{Q}.$$

This shows that $t^{\frac{1}{t-1}}$ and $t^{\frac{t}{t-1}}$ are respectively the roots of the following rational polynomials:

$$X^{\mathrm{sign}(t_2 - t_1)(t_2 - t_1)} - t^{\mathrm{sign}(t_2 - t_1)t_2} \in \mathbb{Q}[X], \quad \text{and} \quad X^{\mathrm{sign}(t_2 - t_1)(t_2 - t_1)} - t^{\mathrm{sign}(t_2 - t_1)t_1} \in \mathbb{Q}[X].$$

This shows that $f(t) \in \mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}}$. In total, we get

$$f\left[\mathbb{Q}_{>0} \setminus \{1\}\right] = \left\{ \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}} \right) \,\middle|\, t \in \mathbb{Q}_{>0} \setminus \{1\} \right\} \subset S \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right).$$

We shall show that the reverse inclusion $\supset$ holds. Let $(x, y) \in S \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right)$; then $x, y > 0$ and x, y are algebraic. Since the set is symmetric, we may again assume that $x < y$. Recalling our construction of the parametrisation, we know that for $t := \frac{y}{x} \in \mathbb{R}_{>0} \setminus \{1\}$, we have $f(t) = f\left(\frac{y}{x}\right) = (x, y)$. Since $\mathbb{Q}^{\mathrm{alg}}$ is a field, $t \in \mathbb{Q}^{\mathrm{alg}}$, and the following constants $u := \frac{1}{t-1} = \frac{y}{x-y} \neq 0$ and $v := \frac{t}{t-1} = \frac{x}{x-y} \neq 0, 1$ are such that $u, v \in \mathbb{Q}^{\mathrm{alg}}$, and $t^u = x$, $t^v = y$. If t is irrational (i.e. $t \in \mathbb{R} \setminus \mathbb{Q}$), then so are u and v. (If either u or v were rational, then $t = (u-1)^{-1} + 1$ or $t = v^{-1} + 1$ would be rational, a contradiction.)

12

But this is impossible because, by the Gelfond–Schneider theorem, as $t \in \mathbb{Q}^{\mathrm{alg}} \setminus \{0, 1\}$ and $u \in \mathbb{Q}^{\mathrm{alg}} \setminus \mathbb{Q}$, it follows that $t^u = x$ is transcendental—a contradiction to $x \in \mathbb{Q}^{\mathrm{alg}}$. For a proof of the Gelfond–Schneider theorem see the Appendix [A]. Thus, t must be rational and so $(x, y) = f(t) \in f[\mathbb{Q}_{>0} \setminus \{1\}]$.

Hence:
$$A \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right) = \Delta \left(\mathbb{Q}^{\mathrm{alg}} \cap \mathbb{R}_{\geq 0} \right) \sqcup \left\{ \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}} \right) \,\middle|\, t \in \mathbb{Q}_{>0} \setminus \{1\} \right\}.$$

Knowing this, since $\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \subset \mathbb{Q}^{\mathrm{alg}}$, we obtain immediately:

$$S \cap \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \times \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \right) \subset \left\{ \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}} \right) \,\middle|\, t \in \mathbb{Q}_{>0} \setminus \{1\} \right\}.$$

Let $(x, y) \in S \cap \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \times \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \right)$. Then $x, y > 0$ and x, y are algebraic integers (i.e., each is annihilated by a monic polynomial in $\mathbb{Z}[X]$). Since the set is symmetric, we may again assume that $x < y$. By our inclusion, we get that $\exists t \in \mathbb{Q}_{>0} \setminus \{1\}$ such that $f(t) = (x, y)$. Write $t = \frac{m}{n}$ for $m, n \in \mathbb{Z}$, with $\gcd(m, n) = 1$ and $m > n$. Since $x \in \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z})$, which is a ring (a classical property), and $m - n \in \mathbb{Z}_{>0}$, we get $x^{m-n} \in \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z})$. But:

$$x^{m-n} = \left(t^{\frac{1}{t-1}} \right)^{m-n} = t^{\frac{m-n}{t-1}} = t^{\frac{n(m-n)}{m-n}} = t^n = \frac{m^n}{n^n}.$$

So $\frac{m^n}{n^n} \in \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z})$, but $\frac{m^n}{n^n} \in \mathbb{Q}$, thus $\frac{m^n}{n^n} \in \mathcal{O}_{\mathbb{Q}}(\mathbb{Z}) = \mathbb{Z}$ (because $\mathbb{Z}$ is a UFD, hence normal). Since $\gcd(m, n) = 1$ and $m, n \in \mathbb{Z}_{>0}$, we have $\gcd(m^n, n^n) = 1$ this implies $n^n = 1$, hence $n = 1$ and $m > n = 1$. Thus $t = m \in \mathbb{Z}_{>1}$, and we get:

$$x = m^{\frac{1}{m-1}}, \quad y = m^{\frac{m}{m-1}}.$$

Hence:

$$S \cap \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \times \mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \right) \subset \left\{ \left(m^{\frac{1}{m-1}}, m^{\frac{m}{m-1}} \right) \,\middle|\, m \in \mathbb{Z}_{>1} \right\}$$
$$= \left\{ \left((1+k)^{\frac{1}{k}}, (1+k)^{\frac{k+1}{k}} \right) \,\middle|\, k \in \mathbb{Z}_{>0} \right\}.$$

The reverse inclusion $\supset$ is easy to verify, since for each $m \in \mathbb{Z}_{>1} \subset \mathbb{R}_{>0} \setminus \{1\}$, we have $f(m) \in S$, and clearly $m^{\frac{1}{m-1}}, m^{\frac{m}{m-1}}$ are respectively the roots of the monic integer polynomials:

$$X^{m-1} - m, \quad X^{m-1} - m^m \in \mathbb{Z}[X].$$

Hence:

$$A \cap \left(\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \right) = \Delta \left(\mathcal{O}_{\mathbb{Q}^{\mathrm{alg}}}(\mathbb{Z}) \cap \mathbb{R}_{\geq 0} \right) \sqcup \left\{ \left((1+k)^{\frac{1}{k}}, (1+k)^{\frac{k+1}{k}} \right) \,\middle|\, k \in \mathbb{Z}_{>0} \right\}.$$

Remark. If one asks the same question over $\mathbb{C}$, with the known subtleties of this generalisation, the intersection with $\mathbb{Q}^{\mathrm{alg}} \times \mathbb{Q}^{\mathrm{alg}} \subset \mathbb{C} \times \mathbb{C}$ appears in the literature to lack a complete characterisation.

Problem (Sudakov & Milojević)

Let $(a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ be non-constant sequences of rational numbers. Suppose that for all $i, j \in \mathbb{N}$,

$$(a_i - a_j)(b_i - b_j) \in \mathbb{Z}.$$

Prove that there exists a non-zero rational number $\gamma \in \mathbb{Q}^{\times}$ such that for all $i, j \in \mathbb{N}$,

$$\gamma(a_i - a_j), \quad \gamma^{-1}(b_i - b_j) \in \mathbb{Z}.$$

Solution:

Clearly, the sequences $(a'_n := a_n - a_0)_{n \in \mathbb{N}}$, $(b'_n := b_n - b_0)_{n \in \mathbb{N}}$ are non-constant rational sequences. Fix $i, j \in \mathbb{N}$; then $a'_i - a'_j = a_i - a_j$ and $b'_i - b'_j = b_i - b_j$, and thus:

$$\forall i, j \in \mathbb{N}, \quad \left(a'_i - a'_j\right)\left(b'_i - b'_j\right) = (a_i - a_j)(b_i - b_j) \in \mathbb{Z}.$$

That is, $(a'_n)_{n \in \mathbb{N}}, (b'_n)_{n \in \mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ satisfy the same property, but they have the advantage that $a'_0 = 0 = b'_0$, which in particular implies $\forall i \in \mathbb{N}$, $a'_i b'_i = (a'_i - a'_0)(b'_i - b'_0) \in \mathbb{Z}$. For all $i, j \in \mathbb{N}$, the equalities $a'_i - a'_j = a_i - a_j$ and $b'_i - b'_j = b_i - b_j$ also imply that $\forall \gamma \in \mathbb{Q}^{\times}$:

$$\forall s, t \in \mathbb{N}, \ \gamma(a'_s - a'_t), \ \gamma^{-1}(b'_s - b'_t) \in \mathbb{Z} \ \Leftrightarrow \ \forall s, t \in \mathbb{N}, \ \gamma(a'_s - a'_t), \ \gamma^{-1}(b'_s - b'_t) \in \mathbb{Z}.$$

So, the problem is equivalent to finding such an invertible rational number for these two new non-constant rational sequences.

Let us consider the sequence of polynomials

$$\left(A_n(X) := \sum_{i=0}^{n} a'_i X^i\right)_{n \in \mathbb{N}}, \quad \left(B_n(X) := \sum_{j=0}^{n} b'_j X^j\right)_{n \in \mathbb{N}} \in \mathbb{Q}[X]^{\mathbb{N}}.$$

and define for each $n \in \mathbb{N}$

$$\Gamma_{A_n,+} := \left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma A_n(X) \in \mathbb{Z}[X]\right\}, \quad \Gamma_{B_n,-} := \left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma^{-1} B_n(X) \in \mathbb{Z}[X]\right\},$$

$$\Gamma_n := \Gamma_{A_n,+} \cap \Gamma_{B_n,-}.$$

Notice that any $\gamma \in \Gamma_n$ satisfies the statement of the problem but only for integers $i, j \leq n$, i.e. for all $i, j \leq n$,

$$\gamma(a_i - a_j), \quad \gamma^{-1}(b_i - b_j) \in \mathbb{Z}.$$

So, the goal is to show that the whole intersection of these sets is non-empty:

$$\Gamma := \bigcap_{n \in \mathbb{N}} \Gamma_n \neq \varnothing.$$

Because then, any element $\gamma \in \Gamma$ is a non-zero rational number satisfying, for all $i, j \in \mathbb{N}$,

$$\gamma(a_i - a_j), \quad \gamma^{-1}(b_i - b_j) \in \mathbb{Z}.$$

To show that this intersection is non-empty, we must work a little. The plan proceeds in three steps. Fix $n \in \mathbb{N}$; we will show, in order, that:

- $\Gamma_n \neq \varnothing$.

14

- $\Gamma_{n+1} \subset \Gamma_n$.

- There exists a rank $M \in \mathbb{N}$ such that, for all $k \geq M$, the set Γ_k is finite.

With these results in the pocket, we obtain by induction that $(\Gamma_i)_{i \in \mathbb{N}}$ is a decreasing nested sequence of non-empty subsets of $\mathbb{Q}^\times$. Hence, this permits us to write:

$$\Gamma = \bigcap_{n \in \mathbb{N}} \Gamma_n = \bigcap_{k \geq M} \Gamma_k.$$

and we can conclude that the last intersection must be non-empty[2], because defining $\forall k \geq M$, $t_k := |\Gamma_k|$, we have:

$$1 \leq t_k \leq t_M < +\infty,$$

so $(t_k)_{k \geq M} \in \mathbb{N}^{\mathbb{N}_{\geq M}}$ and is clearly decreasing. Hence, the limit exists and is equal to $t := \inf \{t_k \,|\, k \geq M\}$, which must satisfy $t \geq 1$. Since the set $\{t_k \,|\, k \geq M\}$ is a subset of the finite set $[\![1, t_M]\!]$, it is finite, hence closed; thus, the infimum is attained. This implies that the sequence $(t_k)_{k \geq M}$ is eventually constant, and so must be the sequence $(\Gamma_k)_{k \geq M}$ (because they are decreasingly nested and finite). That means that there exists $k' \geq M$ such that $\Gamma = \Gamma_{k'} \neq \varnothing$. This will conclude.

Let us finish the problem by proving the three steps. We first carry out some preliminary work:

Notice that for all $i, j \in \mathbb{N}$, the numbers $a_i' b_j' + a_j' b_i'$ must be integers, since they are sums of such:

$$a_i' b_j' + a_j' b_i' = a_i' b_i' + a_j' b_j' - \left(a_i' - a_j'\right)\left(b_i' - b_j'\right).$$

For all $n \in \mathbb{N}$, the polynomial $C_n(X) := A_n(X)B_n(X) \in \mathbb{Q}[X]$ is in fact in $\mathbb{Z}[X]$, since for all $k \leq n$, the k-th coefficient is:

$$c_k\left(C_n(X)\right) = \sum_{j=0}^{k} a_j' b_{k-j}' = \left(\sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor - 1} \left(a_j' b_{k-j}' + a_{k-j}' b_j'\right) \right) + \mathbb{1}_{2\mathbb{N}}(k) \cdot a_{\left\lfloor \frac{k}{2} \right\rfloor}' b_{\left\lfloor \frac{k}{2} \right\rfloor}',$$

and is therefore an integer because it is a sum of all the elements in $\left\{ a_i' b_{k-i}' + a_{k-i}' b_i' \,\middle|\, i \leq \left\lfloor \frac{k}{2} \right\rfloor \right\} \subset \mathbb{Z}$, and possibly (when k is even) one term $a_{\left\lfloor \frac{k}{2} \right\rfloor}' b_{\left\lfloor \frac{k}{2} \right\rfloor}' \in \mathbb{Z}$. Hence, the polynomial $C_n(X)$ has integer coefficients.

Let $N \in \mathbb{N}$ and a rational polynomial $P(X) = \sum_{k=0}^{N} \frac{p_k}{q_k} X^k \in \mathbb{Q}[X]$. Suppose that for all $k \leq N$, the elements $p_k \in \mathbb{Z}$, $q_k \in \mathbb{Z} \setminus \{0\}$ are such that $\gcd(p_k, q_k) = 1$. Define $l_{P(X)} := \operatorname{lcm}\left((q_k)_{k \leq N}\right) \in \mathbb{N} \setminus \{0\}$ and $g_{P(X)} := \gcd\left((p_k)_{k \leq N}\right) \in \mathbb{N}$. Notice that, in this way (by forcing positivity), we obtain two well-defined functions $g\_, l\_ : \mathbb{Q}[X] \to \mathbb{N}$. Now,

---

[2] If you are familiar with the finite intersection property, then this follows easily from the fact that Γ_M, being finite, is a compact subset of $\mathbb{R}$. The set $\mathcal{C} := \{\Gamma_k \,|\, k \geq M\}$ is included in $\mathscr{P}(\Gamma_M)$ (because of the nested property) and is composed of finite subsets of $\mathbb{R}$—hence closed sets. It has the finite intersection property: the intersection over any finite subcollection $\mathcal{C}' \subset \mathcal{C}$ is non-empty, since the poset $(\mathcal{C}', \subset)$ has a unique minimal element Γ_u, as the sets are decreasingly nested with respect to the natural order on $\mathbb{N}$, and therefore their intersection is equal to Γ_u. It is well known that a set is compact if and only if any collection of its closed subsets having the finite intersection property has a non-empty total intersection. Since Γ_M is compact, we may apply this result to obtain $\Gamma = \bigcap \mathcal{C} \neq \varnothing$.

suppose at least one of the coefficients of the polynomial is non-zero (i.e. $P(X) \neq 0$), say for a certain $k' \leq N$, $p_{k'} \neq 0$, then $g_{P(X)} \neq 0$, so we can define $d_{P(X)} := \frac{l_{P(X)}}{g_{P(X)}} \in \mathbb{Q}_{>0}$. We claim:

$$d_{P(X)}\mathbb{Z} \setminus \{0\} = \left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma P(X) \in \mathbb{Z}[X]\right\}. \tag{1}$$

Indeed, the inclusion $\subset$ is evident because $\forall k \leq N$, $q_k \mid l_{P(X)}$ and $g_{P(X)} \mid p_k$. Now, for the reverse inclusion $\supset$: if we let $\gamma \in \mathbb{Q}^{\times}$ with $\gamma P(X) \in \mathbb{Z}[X]$, write $\gamma = \frac{\gamma_1}{\gamma_2}$ with $\gamma_1, \gamma_2 \in \mathbb{Z}$ and $\gcd(\gamma_1, \gamma_2) = 1$. One has for all $k \leq N$, $\gamma \frac{p_k}{q_k} = \frac{\gamma_1 p_k}{\gamma_2 q_k} \in \mathbb{Z}$, thus $\exists t_k \in \mathbb{Z}$ with $\gamma_1 p_k = t_k \gamma_2 q_k$, which implies $\gamma_2 \mid \gamma_1 p_k$ and $q_k \mid \gamma_1 p_k$. Since $\gcd(\gamma_1, \gamma_2) = 1 = \gcd(p_k, q_k)$, we have $\gamma_2 \mid p_k$ and $q_k \mid \gamma_1$. Since $k \leq N$ is arbitrary, we get, by definition of the lcm and gcd, that $\gamma_2 \mid g_{P(X)}$ and $l_{P(X)} \mid \gamma_1$. Hence $\gamma_1 = l_{P(X)}r$ for a certain $r \in \mathbb{Z}$ and $g_{P(X)} = \gamma_2 s$ for a certain $s \in \mathbb{Z}$. That is, $\gamma = \frac{l_{P(X)}rs}{g_{P(X)}} = d_{P(X)}rs \in d_{P(X)}\mathbb{Z}$, and since $\gamma \neq 0$, we have $\gamma \in d_{P(X)}\mathbb{Z} \setminus \{0\}$. This concludes the equality. Notice that $d_{P(X)}\mathbb{Z} \setminus \{0\}$ is a discrete subspace of $\mathbb{R}$.

Clearly, $\left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma P(X) \in \mathbb{Z}[X]\right\}$ is in bijection with $\left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma^{-1} P(X) \in \mathbb{Z}[X]\right\}$ through the map $\gamma \mapsto \gamma^{-1}$. This implies:

$$\left(d_{P(X)}\mathbb{Z} \setminus \{0\}\right)^{-1} = \left\{\left(d_{P(X)}\right)^{-1} \frac{1}{n} \,\middle|\, n \in \mathbb{Z} \setminus \{0\}\right\} = \left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma^{-1} P(X) \in \mathbb{Z}[X]\right\}. \tag{2}$$

Notice that $\left(d_{P(X)}\mathbb{Z} \setminus \{0\}\right)^{-1} \subset \left[-\left(d_{P(X)}\right)^{-1}, \left(d_{P(X)}\right)^{-1}\right]$.

With this in mind, we can prove the steps. Fix $n \in \mathbb{N}$,

- $\Gamma_n \neq \varnothing$.

If $C_n(X) = 0$, then since $\mathbb{Q}$ is a domain, so is $\mathbb{Q}[X]$. Hence, either $A_n(X) = 0$, in which case $\Gamma_{A,n} = \mathbb{Q}^{\times}$ and so $\Gamma_n = \Gamma_{B,n}$, or $B_n(X) = 0$, in which case also $\Gamma_{B,n} = \mathbb{Q}^{\times}$ and $\Gamma_n = \Gamma_{A,n}$. So it suffices to show that $\Gamma_{A,n}, \Gamma_{B,n} \neq \varnothing$, which follows from the fact that for $N \in \mathbb{N}$ and a rational polynomial

$$P(X) = \sum_{k=0}^{N} \frac{p_k}{q_k} X^k \in \mathbb{Q}[X]$$

with $\gcd(p_k, q_k) = 1$ for all $k \leq N$, then, as we saw, $l_{P(X)} \in \mathbb{N} \setminus \{0\}$, and it is clear that

$$l_{P(X)} \in \left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma P(X) \in \mathbb{Z}[X]\right\}, \quad \frac{1}{l_{P(X)}} \in \left\{\gamma \in \mathbb{Q}^{\times} \,\middle|\, \gamma^{-1} P(X) \in \mathbb{Z}[X]\right\}.$$

Hence, in the case $C_n(X) = 0$, we have $\Gamma_n \neq \varnothing$.

Now suppose $C_n(X) \neq 0$. Then both $A_n(X), B_n(X) \in \mathbb{Q}[X] \setminus \{0\}$, thus for $d_1 := g_{\left(l_{A_n(X)} A_n(X)\right)} \in \mathbb{N}$, $d_2 := l_{A_n(X)} \in \mathbb{N} \setminus \{0\}$, $d_3 := g_{\left(l_{B_n(X)} B_n(X)\right)} \in \mathbb{N}$, and $d_4 := l_{B_n(X)} \in \mathbb{N} \setminus \{0\}$, we have, because $A_n(X), B_n(X) \neq 0$, that $d_1 \neq 0 \neq d_3$, and we can write:

$$A_n(X) = \frac{d_1}{d_2} \widetilde{A_n}(X), \quad B_n(X) = \frac{d_3}{d_4} \widetilde{B_n}(X),$$

for certain non-zero integer polynomials $\widetilde{A_n}(X), \widetilde{B_n}(X) \in \mathbb{Z}[X] \setminus \{0\}$. By construction, $\widetilde{A_n}(X), \widetilde{B_n}(X)$ must be primitive and, by Gauss's Lemma I, $\widetilde{A_n}(X)\widetilde{B_n}(X)$ is primitive.

Since $C_n(X) \in \mathbb{Z}[X] \setminus \{0\}$, we can write, with $d_5 := g_{C_n(X)} \in \mathbb{N} \setminus \{0\}$,

$$C_n(X) = d_5 \widetilde{C_n}(X),$$

for a certain $\widetilde{C_n}(X) \in \mathbb{Z}[X] \setminus \{0\}$, which again by construction must be primitive.

Then the product becomes:

$$d_5 \widetilde{C_n}(X) = C_n(X) = A_n(X) B_n(X) = \frac{d_1 d_3}{d_2 d_4} \widetilde{A_n}(X) \widetilde{B_n}(X),$$

implying (since $d_5 \neq 0$)

$$\widetilde{C_n}(X) = \frac{d_1 d_3}{d_2 d_4 d_5} \widetilde{A_n}(X) \widetilde{B_n}(X).$$

Since $\widetilde{C_n}(X), \widetilde{A_n}(X)\widetilde{B_n}(X) \in \mathbb{Z}[X]$, $\widetilde{A_n}(X)\widetilde{B_n}(X)$ is primitive, and $\frac{d_1 d_3}{d_2 d_4 d_5} \in \mathbb{Q}$, we obtain by Gauss's Lemma II that $\frac{d_1 d_3}{d_2 d_4 d_5} \in \mathbb{Z}$; and because $\widetilde{C_n}(X)$ is primitive, we must even have $\frac{d_1 d_3}{d_2 d_4 d_5} \in \mathbb{Z}^\times = \{\pm 1\}$. Hence, choosing (since $d_1 \neq 0 \neq d_2$)

$$\gamma := \frac{d_2}{d_1} \in \mathbb{Q}^\times, \text{ we obtain } \gamma A_n(X) = \widetilde{A_n}(X) \in \mathbb{Z}[X], \gamma^{-1} B_n(X) \in \left\{ \pm d_5 \widetilde{B_n}(X) \right\} \subset \mathbb{Z}[X].$$

That is, $\gamma \in \Gamma_n$, so in the case $C_n(X) \neq 0$ we have $\Gamma_n \neq \varnothing$.

In total, $\Gamma_n \neq \varnothing$.

- $\Gamma_{n+1} \subset \Gamma_n$:

For this, let $\gamma \in \Gamma_{n+1}$. Then $\gamma A_{n+1}(X) \in \mathbb{Z}[X]$ and $\gamma^{-1} B_{n+1}(X) \in \mathbb{Z}[X]$, and thus, trivially,

$$\gamma A_n(X) \in \mathbb{Z}[X], \quad \gamma^{-1} B_n(X) \in \mathbb{Z}[X],$$

so $\gamma \in \Gamma_n$.

- There exists a rank $M \in \mathbb{N}$ such that for all $k \geq M$, the set Γ_k is finite:

Since $(a'_n)_{n\in\mathbb{N}}$ and $(b'_n)_{n\in\mathbb{N}}$ are non-constant, there must exist $M', M'' \in \mathbb{N}$ such that $a'_{M'} \neq 0$ and $b'_{M''} \neq 0$. In particular, the corresponding polynomials from $M := \max\{M', M''\} \in \mathbb{N}$ onward cannot be 0, that is, for $k \geq M$, satisfy $A_k(X), B_k(X) \neq 0$. In this case, we have seen that $d_{A_k(X)}, d_{B_k(X)} \in \mathbb{Q}_{>0}$, and in (1) that

$$\Gamma_{A_k, +} = d_{A_k(X)} \mathbb{Z} \setminus \{0\} \text{ is discrete,}$$

and in (2)

$$\Gamma_{B_k, -} = \left(d_{B_k(X)} \mathbb{Z} \setminus \{0\} \right)^{-1} \subset \left[-\left(d_{B_k(X)} \right)^{-1}, \left(d_{B_k(X)} \right)^{-1} \right].$$

Notice then that Γ_k is finite. This is because

$$\Gamma_k = \Gamma_{A_k, +} \cap \Gamma_{B_k, -}$$
$$\subset \left(d_{A_k(X)} \mathbb{Z} \setminus \{0\} \right) \cap \left[-\left(d_{B_k(X)} \right)^{-1}, \left(d_{B_k(X)} \right)^{-1} \right]$$
$$\subset \left\{ d_{A_k(X)} s \in \mathbb{Q}^\times \,\middle|\, s \in \left[\left\lceil -\left(d_{A_k(X)} d_{B_k(X)} \right)^{-1} \right\rceil, \left\lfloor \left(d_{A_k(X)} d_{B_k(X)} \right)^{-1} \right\rfloor \right] \right\},$$

so that Γ_k is included in a finite set.

This concludes the final steps and finishes the problem.

A

Theorem 1 (Gelfond-Schneider theorem). *Let α and β be algebraic numbers (i.e., $\alpha, \beta \in \mathbb{Q}^{\mathrm{alg}}$) such that $\alpha \neq 0, 1$ and β is irrational. Then any value of α^{β} is transcendental.*

Proof not yet written

References

[1] Michael A. Bennett and Bruce Reznick. *Positive rational solutions to $x^y = y^{mx}$: a number-theoretic excursion.* 2002. arXiv: math/0209072 [math.NT]. URL: https://arxiv.org/abs/math/0209072.

[2] Alvin Hausner. "Algebraic Number Fields and the Diophantine Equation $m^n = n^m$". In: *The American Mathematical Monthly* 68.9 (1961), pp. 856–861. DOI: 10.2307/2311682. URL: https://doi.org/10.2307/2311682.

[3] Solomon Hurwitz. "On the Rational Solutions of $m^n = n^m$ with $m \neq n$". In: *The American Mathematical Monthly* 74.3 (1967), pp. 298–300. DOI: 10.2307/2316032. URL: https://doi.org/10.2307/2316032.

[4] Daihachiro Sato. "Algebraic Solution of $x^y = y^x$ $(0 < x < y)$". In: *Proceedings of the American Mathematical Society* 31.1 (1972), pp. 316–316. DOI: 10.1090/S0002-9939-1972-0288074-5. URL: https://doi.org/10.1090/S0002-9939-1972-0288074-5.