Solved and unsolved problems

Dorin Andrica

Starting with the June issue, this column is structured into three parts as follows: olympiad problems, undergraduate problems, and open and research problems. Each part is intended to address a different level of mathematical interest and to encourage broad participation from students, teachers, and researchers alike.

We warmly invite you to submit your solutions, as well as new and original problems that may be of interest to the mathematical community. Contributions that promote creativity, insight, and elegance are especially appreciated.

We also encourage you to contribute research and open problems from any area of mathematics for inclusion in the third part of the section. Submissions that highlight new directions, conjectures, or challenging questions are particularly welcome, as they can stimulate further investigation and collaboration.

For all submissions, questions, and correspondence, please use the following email address: dandrica@math.ubbcluj.ro.

The deadline for submitting solutions to the proposed problems is *one month* from the publication of the Magazine issue.

We look forward to your contributions and to fostering a vibrant and engaging mathematical exchange.

I Proposed problems

I.1 Olympiad problems

O1

The positive real numbers a, b, c, d satisfy $abcd = 1$ and

$$(a^2 + b^2)(b^2 + c^2)(c^2 + d^2)(d^2 + a^2) = 2026.$$

Find the maximum possible value of $(ab + cd)(ad + bc)$.

Titu Andreescu (AwesomeMath, Dallas, USA) and Gabriel Dospinescu (École normale supérieure, Lyon, France)

O2

Given a triangle ABC. Construct equilateral triangles BCD, CAE, and ABF externally on the sides of triangle ABC. Let K and X be the circumcenters of triangles AEF and BCD, respectively. Prove that line XK passes through the nine-point center of triangle ABC.

Nikolaos Dergiades (Thessaloniki, Greece) and Quang Hung Tran (High School for Gifted Students, Vietnam National University, Hanoi, Vietnam)

I.2 Undergraduate problems

U1

Consider the folium of Descartes defined by the plane curve

$$Fo\colon x^3 + y^3 = 3axy.$$

Suppose that from a point P in the plane, four tangents can be drawn to Fo, touching the curve at points A, B, C, and D. Prove that the origin $O(0, 0)$ is the centroid of the quadrilateral $ABCD$.

Nikolaos Dergiades (Thessaloniki, Greece) and Quang Hung Tran (High School for Gifted Students, Vietnam National University, Hanoi, Vietnam)

U2

For $a \geq 0$, let $\mathcal{F}_a$ denote the set of continuous functions $f\colon \mathbb{R} \to \mathbb{R}$ that satisfy:

(i) $$\frac{f(x) - f(y)}{x - y} \geq a, \quad \text{for all } x, y \in \mathbb{R},\ x \neq y;$$

(ii) $$\int_{f(x)}^{f(x)+1} f(t)\,dt = af(x) + \frac{a}{2}, \quad \text{for all } x \in \mathbb{R}.$$

(a) Give an example of a non-constant function in $\mathcal{F}_0$.
(b) If $a > 0$, determine the set $\mathcal{F}_a$.

Dan-Ștefan Marinescu (Hunedoara, Romania)

II Solutions to the proposed problems

We present detailed solutions to problems 284–289, originally proposed in the EMS Magazine **131** (2024), offering not only complete answers but also insights into the methods and ideas underlying each problem.

In the next issue, we will turn our attention to the newly proposed problems O1–O2 and U1–U2 stated above. These problems vary in difficulty and style, encouraging both creative thinking and technical proficiency. We invite readers to engage actively with these challenges and to submit their own solutions, particularly those that offer novel perspectives or unexpected arguments.

As always, our goal is not only to present correct solutions but also to foster a deeper appreciation for problem-solving as a creative and exploratory process.

284

Let V be a finite set and $\tilde{V} \subset V$. For a finite path $\mathbf{w} = (w_0, w_1, \dots, w_\eta)$ on V, we let $n_0 = 0$, and for $i \geq 1$, we let

$$n_i = \begin{cases} \max\{n_{i-1} \leq n \leq \eta : w_n = w_{n_{i-1}}\} + 1, \\ \qquad\qquad\qquad \text{if } w_{n_{i-1}} \in \tilde{V} \text{ and } w_{n_{i-1}} \neq w_\eta, \\ n_{i-1} + 1, \qquad \text{if } w_{n_{i-1}} \notin \tilde{V} \text{ and } n_{i-1} \neq \eta. \end{cases}$$

We call $\mathfrak{L}_{\tilde{V}}(\mathbf{w}) := (w_{n_0}, w_{n_1}, \dots, w_{n_\iota})$, where n_ι is the last index found by the algorithm, the partial loop erasure (PLE) of $\mathbf{w}$.

Let $(X_n, \mathbb{P}_x)$ be a discrete-time irreducible Markov chain on a finite set V, and let $\sigma_A = \min\{n \geq 0 : X_n \in A\}$ and $X|_{[0,\sigma_A]} = (X_0, X_1, \dots, X_{\sigma_A})$. Prove that

$$\mathfrak{L}_V(X|_{[0,\sigma_A]}) \overset{(d)}{=} \mathfrak{L}_V \circ \mathfrak{L}_{\tilde{V}}(X|_{[0,\sigma_A]}),$$

where $\overset{(d)}{=}$ means that both sides have the same law.

Shiping Cao (Department of Mathematics, University of Washington, Seattle, USA)

Solution by the proposer

The question is a simplified version of Theorem 1 of my recent paper [1]. First, we prove that

$$\mathfrak{L}_{V_2}(X|_{[0,\sigma_A]}) \overset{(d)}{=} \mathfrak{L}_{V_2} \circ \mathfrak{L}_{V_1}(X|_{[0,\sigma_A]}) \tag{1}$$

if $V_1 \subset V_2 \subset V$ and $V_2 \setminus V_1 = \{b\}$ for some $\{b\} \notin A$.

We define a random path L as follows: if $\mathfrak{L}_{V_1}(X|_{[0,\sigma_A]})$ does not hit b, we simply let $L = \mathfrak{L}_{V_1}(X|_{[0,\sigma_A]})$; if $\mathfrak{L}_{V_2}(X|_{[0,\sigma_A]}) = (w_{n_0}, w_{n_1}, \dots, w_{n_\iota})$ hits b with $w_{n_j} = b$, we erase loops partially with respect to V_1 in chronological order before n_j and then erase loops partially with respect to V_1 in reverse order after n_j to get L.

For each $\mathbf{w} = (w_0, w_1, \dots, w_\iota)$, we can show that

$$\mathbb{P}_x(\mathfrak{L}_{V_1}(X|_{[0,\sigma_A]}) = \mathbf{w}) = \mathbb{P}_x(L = \mathbf{w}). \tag{2}$$

If $\mathbf{w}$ does not hit b, clearly (2) holds. If $\mathbf{w} = (w_0, w_1, \dots, w_\iota)$ hits b with $w_j = b$, we let $i_0, i_1, \dots, i_\eta$ be all indices corresponding to points contained in $V_1 \setminus A$ (ordered in chronological order), and let $i_0, i_1, \dots, i_k$ be those smaller than j. Then

$$\begin{aligned} \mathbb{P}_x(\mathfrak{L}_{V_1}(X|_{[0,\sigma_A]}) = \mathbf{w}) &= F(w_{i_0}, \dots, w_{i_\eta}) P(w_0, w_1) \cdots P(w_{\iota-1}, w_\iota), \\ \mathbb{P}_x(L = \mathbf{w}) &= F(w_{i_0}, \dots, w_{i_k}, w_{i_\eta}, \dots, w_{i_{k+1}}) \\ &\quad \times P(w_0, w_1) \cdots P(w_{\iota-1}, w_\iota). \end{aligned}$$

Here

$$F(y_0, \dots, y_n) := G_A(y_0, y_0) \cdots G_{A \cup \{y_0, \dots, y_{n-1}\}}(y_n, y_n),$$

and

$$G_B(x, y) = \sum_{m=0}^{\infty} \mathbb{P}_x(X_m = y; \sigma_B > m).$$

By Lawler [2, Proposition 3.3],

$$F(y_0, \dots, y_n) = F(y_{\pi(0)}, \dots, y_{\pi(n)})$$

for any permutation π. Hence (1) follows.

Iterating gives

$$\mathfrak{L}_{V_m} \circ \cdots \circ \mathfrak{L}_{V_1}(X|_{[0,\sigma_A]}) \overset{(d)}{=} \mathfrak{L}_{V_m}(X|_{[0,\sigma_A]}). \tag{3}$$

The remainder follows by conditioning on the path outside $\tilde{V}$ and applying (3).

References

[1] S. Cao, Scaling limits of loop-erased Markov chains on resistance spaces via a partial loop-erasing procedure. *Adv. Math.* **435**, article no. 109382 (2023)

[2] G. F. Lawler, Topics in loop measures and the loop-erased walk. *Probab. Surv.* **15**, 28–101 (2018)

285

The following democratic process is implemented in a population of N sheep during a Yes/No referendum. At the initial time $t = 0$, m sheep are pro-Yes, and $N - m$ sheep are pro-No. At each time $t = 1, 2, \dots$, a sheep is randomly chosen (independently of what happened before) and bleeps its opinion. Instantly, a sheep from the opposite camp (if at least one remains) switches its opinion. The process stops when a consensus is reached.

We denote by $P_{m,N}$ the probability that "Yes" wins when starting with m pro-Yes sheep in the population. Of course, $P_{0,N} = 0$, $P_{N,N} = 1$, and due to the symmetry of the problem $P_{N,2N} = 1/2$.

Question. Find a simple expression for $P_{m,N}$. (*In particular, this expression should allow you to estimate very easily the evolution of this probability when starting from a very small majority, i.e., the estimation of $P_{N+a_N,2N}$ for different sequences $1 \ll a_N \ll N$.*)

Lucas Gerin (CMAP, École Polytechnique, Palaiseau, France)

Solution by the proposer

The starting point is, of course, to condition on the opinion of the first chosen sheep. This yields the recurrence equation

$$P_{m,N} = \frac{m}{N} P_{m+1,N} + \frac{N-m}{N} P_{m-1,N},$$

for every $1 \le m \le N-1$. By playing around with small values of m, N, one can guess that $P_{m,N}$ actually coincides with

$$Q_{m,N} := \sum_{\ell=0}^{m-1} \binom{N-1}{\ell} 2^{-N+1},$$

with the convention $\sum_{\ell=0}^{-1} \cdots = 0$. To prove this we first check that $Q_{0,N} = 0$ and $Q_{N,N} = 1$, as required. Then

$$\begin{aligned}
&\frac{m}{N} Q_{m-1,N} + \frac{N-m}{N} Q_{m+1,N} \\
&\quad = \frac{m}{N} \sum_{\ell=0}^{m} \binom{N-1}{\ell} 2^{-N+1} + \frac{N-m}{N} \sum_{\ell=0}^{m-2} \binom{N-1}{\ell} 2^{-N+1} \\
&\quad = \left(\frac{m}{N} + \frac{N-m}{N}\right) \sum_{\ell=0}^{m-1} \binom{N-1}{\ell} 2^{-N+1} \\
&\qquad + \frac{m}{N} \binom{N-1}{m} 2^{-N+1} - \frac{N-m}{N} \binom{N-1}{m-1} 2^{-N+1} \\
&\quad = Q_{m,N}.
\end{aligned}$$

Thus, $m \mapsto Q_{m,N}$ satisfies the same recurrence of order two as $m \mapsto P_{m,N}$, with the two same boundary values.

It is then convenient for asymptotics to write this expression in the form

$$P_{m,N} = \mathbb{P}\Big(\text{Binomial}\Big(N-1, \frac{1}{2}\Big) \le m-1\Big).$$

(I do not see a direct probabilistic explanation for the appearance of the binomial distribution here.) The central limit theorem implies that $P_{N+a_N,2N} \to 1/2$ as long as $a_N = o(\sqrt{N})$. More interestingly, Hoeffding's inequality implies a sharp threshold for $m \mapsto P_{m,2N}$ around $N \pm \sqrt{N}$: for every integer $a_N \ge 0$

$$P_{N+a_N,2N} \ge 1 - \exp(-a_N^2/N).$$

(Of course by symmetry $P_{N-a_N,2N} \le \exp(-a_N^2/N)$.)

Bibliographical comments

One can find a very detailed study of this model in "P. Flajolet and T. Huillet, Analytic combinatorics of the Mabinogion urn. *Discrete Math. Theor. Comput. Sci.*, Proc. vol. **AI**, 549–572 (2008)," even if the above explicit formula for $P_{m,N}$ does not appear exactly in that form.

286

Let $\alpha \in \mathbb{R}$ and consider the transition probability density $P(x;t|y)$ from a point $y \ge 0$ after a time $t > 0$ of a Brownian motion on the non-negative real line with reflecting boundary conditions, observing that it is the weak solution of the initial value problem with Robin boundary condition:

(1) $\partial_t P(x;t|y) = \alpha \partial_x P(x;t|y) + \frac{1}{2}\partial_x^2 P(x;t|y)$ for all $x, y \ge 0$ and $t > 0$;

(2) $[2\alpha P(x;t|y) + \partial_x P(x;t|y)]_{x=0} = 0$ for all $t > 0$, where the derivative at the origin is the one-sided right derivative;

(3) $\lim_{t\to 0} \int_0^\infty f(x) P(x;t|y)\,dx = f(y)$ for all bounded continuous functions f and $y \ge 0$.

Prove that the solution is given by

$$P(x;t|y) = \frac{1}{2}\partial_x \left(\operatorname{erfc}\left[\frac{y-x-\alpha t}{\sqrt{2t}}\right] - e^{-2\alpha x} \operatorname{erfc}\left[\frac{y+x-\alpha t}{\sqrt{2t}}\right]\right)$$

for any $x, y \ge 0$ and $t > 0$, where $\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-y^2} dy$ is complementary error function and ∂_x is the partial derivative with respect to x.

Mario Kieburg (School of Mathematics and Statistics, University of Melbourne, Parkville, Australia)

Solution by the proposer

This problem has been solved in [1, p. 49]. The slightly more complicated model with two barriers has been studied in [2]. We solve the problem with analytical techniques, though there are other ways to derive the statement. The boundary condition (2) is a regularity condition, guaranteeing that the density stays normalized for any $t > 0$. This condition originates from the assumption of a reflection at the origin of the Brownian motion. The condition (3) is the initial value.

For this goal, we define the function

$$\begin{aligned}
F(x;t;y) = \frac{1}{\sqrt{t}} &\exp\Big[-\frac{\alpha^2 t}{2} - \alpha x\Big] \\
&\times \left(\Big[\frac{y-x}{t} - \alpha\Big] \exp\Big[-\frac{(y-x)^2}{2t}\Big] \right. \\
&\quad \left. + \Big[\frac{y+x}{t} + \alpha\Big] \exp\Big[-\frac{(y+x)^2}{2t}\Big]\right),
\end{aligned}$$

which is related to the presumed solution as

$$P(x;t|y) = \frac{1}{\sqrt{2\pi}} \int_y^\infty F(x;t;\tilde{y}) e^{\alpha \tilde{y}}\, d\tilde{y}. \tag{1}$$

(1) One can readily show

$$\partial_t F(x;t;y) = \alpha \partial_x F(x;t;y) + \frac{1}{2}\partial_x^2 F(x;t;y)$$

for all $x, y \ge 0$ and $t > 0$. As the integrand is analytic in $x \in \mathbb{R}$ and $t > 0$, and the integral (1) is uniformly convergent on compact sets, we may interchange derivatives and integration. Hence, $P(x;t|y)$ satisfies the heat equation with drift.

(2) Similarly, one can show that F satisfies

$$[aF(x;t;y) + \partial_x F(x;t;y)]_{x=0} = 0,$$

so $P(x;t|y)$ satisfies this Robin boundary condition.

(3) For the initial condition, let f be bounded and continuous with $M = \sup_{x\geq 0} |f(x)|$. Consider

$$\begin{aligned}\int_0^\infty f(x)P(x;t|y)\,dx &= \frac{1}{\sqrt{2\pi t}}\int_0^\infty f(x)e^{-(y-x-at)^2/2t}\,dx\\ &\quad+\frac{1}{\sqrt{2\pi t}}\int_0^\infty f(x)e^{-(y+x-at)^2/2t-2ax}\,dx\\ &\quad+a\int_0^\infty f(x)e^{-2ax}\operatorname{erfc}\Big(\frac{y+x-at}{\sqrt{2t}}\Big)\,dx.\end{aligned}$$

After substitution,

$$\begin{aligned}&= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty f(\sqrt{t}x+y-at)\Theta(\sqrt{t}x+y-at)e^{-x^2/2}\,dx\\ &\quad+\frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty f(\sqrt{t}x-y+at)e^{-2a(\sqrt{t}x-y+at)}\\ &\qquad\times\Theta(\sqrt{t}x-y+at)e^{-x^2/2}\,dx\\ &\quad+a\int_0^\infty f(x)e^{-2ax}\operatorname{erfc}\Big(\frac{y+x-at}{\sqrt{2t}}\Big)\,dx.\end{aligned}$$

The first two integrands are dominated by $Me^{-x^2/2}$ and converge pointwise:

$$\lim_{t\to 0} = \begin{cases} f(y)e^{-x^2/2}, & y>0,\\ f(0)e^{-x^2/2}\Theta(x), & y=0.\end{cases}$$

The third term can be bounded and vanishes as $t\to 0$ (or cancels if $y=0$). Hence,

$$\lim_{t\to 0}\int_0^\infty f(x)P(x;t|y)\,dx = f(y).$$

References

[1] J. M. Harrison, *Brownian motion and stochastic flow systems*. Wiley Ser. Probab. Math. Statist., John Wiley & Sons, New York (1985)

[2] O. Kella and W. Stadje, A Brownian motion with two reflecting barriers and Markov-modulated speed. *J. Appl. Probab.* **41**, 1237–1242 (2004)

Open problem

Consider Brownian motion with drift on $\mathrm{Herm}(N)$. The transition density is

$$P(H;t|H^{(0)}) = (2\pi t)^{-N/2}(\pi t)^{-N(N-1)/2}\exp\Big[-\frac{\operatorname{tr}(H-H^{(0)}+At)^2}{2t}\Big].$$

For $A=0$, this induces Dyson Brownian motion [1]:

$$p^{(\mathrm{DB})}(E;t|E^{(0)}) = \det\Big[\frac{1}{\sqrt{2\pi t}}\exp\Big(-\frac{(E_a-E_b^{(0)})^2}{2t}\Big)\Big]\prod_{a<b}\frac{E_b-E_a}{E_b^{(0)}-E_a^{(0)}}.$$

The Karlin–McGregor formula gives

$$p^{(\mathrm{B})}(E;t|E^{(0)}) = \det\Big[\frac{1}{\sqrt{2\pi t}}\exp\Big(-\frac{(E_a-E_b^{(0)})^2}{2t}\Big)\Big].$$

(i) For drift $A=aI$, one obtains

$$\begin{aligned}&p(E;t|E^{(0)})\\ &\quad= \det\Big[\frac{1}{\sqrt{2\pi t}}\exp\Big(-\frac{(E_a-E_b^{(0)}+at)^2}{2t}\Big)\Big]\prod_{a<b}\frac{E_b-E_a}{E_b^{(0)}-E_a^{(0)}}.\end{aligned}$$

(ii) Introducing walls (e.g., positivity constraints on eigenvalues) leads to largely open problems, especially with drift.

References

[1] D. J. Grabiner, Brownian motion in a Weyl chamber, non-colliding particles, and random matrices. *Ann. Inst. H. Poincaré Probab. Statist.* **35**, 177–204 (1999)

287

We place n different pairs of socks in a tumble dryer. When the dryer has thoroughly mixed the socks, they are taken out one by one; if a sock is the partner of one of the socks on the sorting table, both are removed, otherwise it is put on the table until its partner emerges from the dryer. For $k\in\{1,\dots,2n\}$, let X_k be the number of socks on the table when the kth sock is taken from the dryer. With $X_0=0$, the random path $(X_0,\dots,X_{2n})$ is a Dyck path. Recall that a path $(x_0,\dots,x_{2n})$ is called a *Dyck path* if $|x_i-x_{i+1}|=1$, $x_i\geq 0$ for $1\in\{1,\dots,2n-1\}$ and $x_0=x_{2n}=0$.

The number of Dyck paths of a given length is given by the Catalan numbers, but not all Dyck paths come up with the same probability in the sock sorting process. For example, for $n=2$ there are two Dyck paths, $(0,1,0,1,0)$ and $(0,1,2,1,0)$. The former has probability $\frac{1}{3}$ and the latter $\frac{2}{3}$. The problem is now, given a Dyck path $(x_0,\dots,x_{2n})$ of arbitrary length, to find a formula for the probability

$$\mathbb{P}(X_0=x_0,\,X_1=x_1,\,\dots,\,X_{2n}=x_{2n}).$$

Peter Mörters (University of Cologne, Germany)

Solution by the proposer

The suggested solution is taken from [1]. A Dyck path $(x_0,\dots,x_{2n})$ has n upward and n downward steps. Given such a path we construct the vector $(k_1,\dots,k_n)\in\mathbb{N}^n$ representing the heights of the path from which each downward step is taken. Formally, define $\ell_0=0$ and, for $j=1,\dots,n$, inductively $\ell_j=\min\{i>\ell_{j-1}:x_{i+1}=x_i-1\}$ and set $k_j=x_{\ell_j}$. The vector $(k_1,\dots,k_n)$ satisfies

$$k_{i+1}\geq k_i-1,\quad\text{for}\quad 1\leq i<n,\quad\text{and}\quad k_n=1. \qquad (*)$$

Conversely, given $(k_1, k_2, \ldots, k_n)$ satisfying (*) there is a unique associated Dyck path given by $x_i = i$ if $i \le k_1$ and

$$x_{k_j+2j-1+i} = k_j - 1 + i \ \text{ if } \ k_j - 1 + i \le k_{j+1} \ \text{ for } \ j \in \{1, \ldots, n\}.$$

In other words, there is a bijection between the set of Dyck paths of length $2n$ and the set of vectors of length n satisfying (*). We now show that if $(k_1(x), \ldots, k_n(x))$ denotes the vector associated with the Dyck path $x = (x_0, \ldots, x_{2n})$, then

$$\mathbb{P}(X_0 = x_0, X_1 = x_1, \ldots, X_{2n} = x_{2n}) = 2^n \frac{n! \prod_{i=1}^n k_i(x)}{(2n)!}.$$

To this end we look at the probability space Ω_n consisting of all permutations of $2n$ distinguishable socks. In our model each of the $(2n)!$ elements is equally likely. If we write the set of socks as

$$\{1, \ldots, n\} \times \{0, 1\},$$

with 0, 1 indicating whether it is the left, resp. right, sock, then $\omega = (\omega_1, \ldots, \omega_{2n}) \in \Omega_n$ are the socks in the order drawn from the dryer. Write $\omega_m = (s_m, p_m) \in \{1, \ldots, n\} \times \{0, 1\}$ where s_m denotes the type of the sock found in the mth draw and p_m indicates whether it is the left or right partner. We set $s_0 = 0$ and $x_0 = 0$ and define

$$x_m = \begin{cases} x_{m-1} + 1 & \text{if } s_m \notin \{1, \ldots, s_{m-1}\}, \\ x_{m-1} - 1 & \text{if } s_m \in \{1, \ldots, s_{m-1}\}, \end{cases}$$

and observe that $x(\omega) = (x_1, \ldots, x_{2n})$ is the Dyck path associated with ω. Our formula is proved if we show that for given $(k_1, k_2, \ldots, k_n) \in \mathbb{N}^n$ satisfying (*) there are exactly $2^n n! \prod_{i=1}^n k_i$ different elements $\omega \in \Omega_n$ with $k_i(x(\omega)) = k_i$ for all $i \in \{1, \ldots, n\}$.

As above let $(\ell_1, \ldots, \ell_n)$ be the ordered indices at which the Dyck path associated with $(k_1, k_2, \ldots, k_n)$ steps down. We partition the set of indices $I := \{1, \ldots, 2n\}$ into the sets

$$M := \{\ell_1 + 1, \ldots, \ell_n + 1\} \ \text{ and } \ N := I \setminus M.$$

At the indices in N the first instance of a sock type is drawn. There are $n!$ ways to allocate the n types of socks to these n indices and 2^n choices whether the left or right sock is the first. Once this choice is made we look at the indices in M in order. At each of these indices a pair of socks is completed. As there are k_i socks of different type on the table at time ℓ_i, there are exactly k_i choices for ω_{ℓ_i+1}. Altogether, we find exactly $2^n n! \prod_{i=1}^n k_i$ different elements $\omega \in \Omega_n$ with $k_i(x(\omega)) = k_i$ for all $i \in \{1, \ldots, n\}$.

References

[1] S. Korbel and P. Mörters, A path formula for the sock sorting problem. *Theory Probab. Appl.* **66**, 708–712 (2022)

288

In a university hospital, there are 9 major medical departments performing surgery. The cardiology unit performs 21% of all surgeries conducted hospital-wide, with 5% of total cardiac surgeries occurring at least twice a day. A total of 30 patients are assigned to surgery. Assuming that surgeries are equally likely on any given day of the year, if two or more surgeries occur on the same day, what is the probability that they are assigned to the cardiology unit?

Gaetano Valenza (Bioengineering and Robotics Research Center "E. Piaggio" & Department of Information Engineering, School of Engineering, University of Pisa, Italy)

Solution by the proposer

Let us define the events:

C : The surgery is in the cardiology unit.

T : At least two surgeries occur on the same day.

To solve the problem, we can apply Bayes's theorem:

$$P(C \cap C \mid T) = \frac{P(T \mid C \cap C) \cdot P(C \cap C)}{P(T)}$$

where $P(C \cap C)$ is the probability that two surgeries are assigned to the cardiology unit. We already have $P(C) = 0.21$ (probability of cardiology surgery) and $P(T \mid C \cap C) = 0.05$ (probability of at least two surgeries a day given they are performed in the cardiology unit).

Assuming that the two cardiac surgeries may occur independently,

$$P(C \cap C) = P(C) \cdot P(C) = 0.21 \times 0.21 = 0.0441.$$

Given the number of patients $n = 30$, let us calculate $P(T)$ using the Birthday Paradox rule:

$$\begin{aligned} P(T) &= 1 - \frac{365 \times \cdots \times (365 - n + 1)}{365^n} \\ &= 1 - \frac{1}{365^n}\left(\frac{365!}{(365-n)!}\right) = 0.7063, \\ P(C \cap C \mid T) &= \frac{0.05 \times 0.0441}{0.7063} = 0.0031. \end{aligned}$$

289

It is the king's birthday, and he decides to please the republican sentiments in the population and release some prisoners who are held for their republican views. The prisoners all have equally excellent rational skills and are placed in separate castles, so that they are unable to speak and communicate with each other. The king decides to challenge the prisoners and gives each of them a coin. Within a quarter of an hour, each of them, say n prisoners, has to decide whether to toss the coin or not. If at least one coin

is tossed and all coins being tossed show head, all n prisoners are released, otherwise none of them are. The king believes the prisoners have a slim chance of being released. But is that so? What is the probability that they all are released? The prisoners are told the number n.

Carsten Wiuf (Department of Mathematical Sciences, University of Copenhagen, Denmark)

Solution by the proposer

If they could communicate with each other, they could simply decide that one of them should toss the coin and the others not. Hence, they would have 50% of being released. However, this is not a possibility. Since all n prisoners have excellent rationale skills, they instantly know they should control the number of prisoners tossing a coin. Let x be the probability that prisoner $i = 1, \ldots, n$, tosses the coin, which might depend on n and is to be determined. Then, the chance of being released is

$$\begin{aligned} p_n(x) &= \sum_{k=1}^{n} \left(\frac{1}{2}\right)^k \binom{n}{k} x^k (1-x)^{n-k} \\ &= \sum_{k=0}^{n} \left(\frac{1}{2}\right)^k \binom{n}{k} x^k (1-x)^{n-k} - (1-x)^n \\ &= \left(1 - \frac{1}{2}x\right)^n - (1-x)^n. \end{aligned}$$

If $n = 1$, then $x = 1$ (the prisoner should toss the coin). For $n \geq 2$, by differentiation, we find the optimal $x \in [0, 1]$:

$$x^* = \frac{2^{1/(n-1)} - 1}{2^{1/(n-1)} - 0.5} \approx \frac{1}{n-1} 2\log(2),$$

the latter approximation for large n. For $n = 1$, $x^* = 1$ and $p_1(x^*) = 0.5$. For $n = 2$, $x^* = 2/3$ and $p_2(x^*) = 1/3$. Generally, $p_n(x^*)$ is decreasing in n and

$$p_n(x^*) > \frac{1}{4}, \quad p_n(x^*) \approx \frac{1}{4} \quad \text{for large } n.$$

III Open and research problems

Cyclotomic Diophantine norm equations

by Preda Mihăilescu

We discuss variants of the cyclotomic norm equation $\frac{x^p+y^p}{x+y} = p^e z^q$, with coprimes integers x, y, z and $p > 3$, a prime.

III.1 Introduction

The reader familiar with the amazing diversity and richness of criteria developed until 1990, in the attempt to prove that the Fermat's conjecture (also: FLT), purporting that the equation

$$x^p + y^p + z^p = 0; \quad x, y, z \in \mathbb{Z}; \quad xyz \neq 0, \quad p > 2, \qquad (1)$$

the most famous special case of the family of Diophantine equations that we shall discuss, has no solutions, can observe that it long resembled a vast and barren desert, sporadically punctuated by rare and isolated oasis—exceptional, innovative, and surprising conditions that would necessarily have to hold if the conjecture were false. These conditions were so intricate and specific that their fulfillment appeared highly implausible. Nevertheless, none of these investigative approaches succeeded in reaching the definitive resolution—the metaphorical "ocean" beyond the desert—where the ultimate truth of the conjecture would be established. This description is particularly apt in the context of the *First Case* (also FLTI), which assumes that the prime $p \nmid xyz$. Ribenboim's extensive and illuminating survey [17] captures the breadth of attempts made, documenting the numerous avenues pursued and the audacity of those efforts. Lamé's failed proof from 1841, which was using the assumption that the integers of the pth cyclotomic field are a factorial ring, was disproved by Kummer's counterexample of the field $\mathbb{Q}[\zeta_{23}]$, and this led the way to the discovery of Dedekind rings and classical algebraic number theory, which in turn gave raise to the above-mentioned multitude of dead-end attempts.

Before being archived to the room of solved conjectures, Fermat's question motivated one more major progress in mathematics: The proof of the Tanyama–Shimura conjecture by Wiles [22] and then completed by Wiles and Taylor [20]—by now the only major result in global Langlands theory. Wiles's solitary, now legendary effort was triggered by the observation of Hellegouarch, proved in detail by Frey, to the effect that a solution to (1) implies the existence of an elliptic curve

$$Y^2 = X(X - a^p)(X + b^p),$$

later called a *Frey curve*, with *particular* properties. The connection of this curve to the Tanyama–Shimura conjecture depended on Serre's *epsilon conjecture*, which was proved by Ken Ribet to be true, in the mid-eighties, thus yielding the *Ribet descent theorem*. It states that the existence of the Frey curve above together with the conjecture imply the presence of a modular form of level 2—which

however was known not to exist. Wiles, who had proved together with Mazur the *main conjecture of abelian Iwasawa theory*, using Galois representations in a way echoing the proof of the same Ribet for the *converse of Herbrandt's theorem*, took the challenge and eventually accomplished his famous result. One may also consider the consequence from the perspective of Hilbert's famous *bon mot*, regarding (1) as a famous *mathematical curiosity*; nobody will be able to say, to which extent the curiosity itself or the challenge of the major conjecture of Tanyama–Shimura motivated Wiles's work. Fact is that the proof of Fermat's Last Theorem offered *mathematics*, after the discovery of Dedekind rings more than a century before, a new milestone of theoretical mathematics that opened up new horizons.

The proof of Iwasawa's main conjecture had already provided in 1984 the instance of a proof of an intrinsic cyclotomic question, by reaching out to methods from the algebraic geometry of elliptic curves. At the beginning of the following decade however, the work of Thaine and Kolyvagin then succeeded to prove the main conjecture using new ideas in cyclotomy itself. As we shall see in more detail below, the Fermat equation has an inherent cyclotomic nature; there is however to this day no alternative proof known, that would use solely cyclotomic methods.

Another classical Diophantine equation, a *binary exponential one*—as opposed to (1) which is a *ternary* equation, since it involves three distinct bases—is the Catalan equation

$$x^p - y^q = 1, \text{ with } p, q \text{ being distinct odd primes and } x, y \in \mathbb{Z}. \quad (2)$$

The equation has the solution $3^2 - 2^3 = 1$, and Catalan stipulated that this should be the only non-trivial (i.e., with $xy \neq 0$) solution. In this case, the effective bounds proved by Baker for linear forms in logarithms in 1973 led to Tijedeman's ineffective, and shortly after, to Langevin's effective proof of the fact that (2) has at most finitely many solutions. In this case, the powerful, general result of Baker was useful in leading to a long sequence of improvements on upper bounds on the exponents p, q for which a solution might exist; during a quarter of a century of continuous sharpenings—see also [2] for details about this mathematical advances—the bound reached by Mignotte in 2000 was $\min(p, q) < 1.6 \cdot 10^{11}$. In lack of some powerful general result like Ribet's descent in the case of (1), Baker's theory left an open gap of lower bounds on the exponents, necessary for completing the proof of Catalan's conjecture. And this gap was incompletely covered by some cyclotomic algebraic arguments, akin to classical results about (1). The unexpected success of an improved algebraic condition I proposed in 1999—presently called the *double Wieferich criterion*—and which raised the verified lower bound for p, q by a factor of 100, let to the hope that cyclotomy could provide stronger results on the Catalan equation. Upon my question, whether Frey curves could be helpful in this case, Ken Ribet generously replied, explaining that the presence of two distinct exponents made the descent argument impossible, so the answer was negative. This suggested that more research on the cyclotomic track might not be a mad idea—and eventually led to the first proof of the Catalan conjecture, which used arguments of class field theory as a bootstrap for precise and context-specific Diophantine approximation using binomial series. Essentially, algebra helped move the approximation step from the generic setting of Baker theory to one tailored around the properties of the equation (2). This change of strategy leads us to the core question around which this paper is organized: *In the more general context of cyclotomic norm equations, how can one move the balance from proofs using deep structural results, that may not be cyclotomic in nature, to alternatives based on cyclotomy alone, and possibly using dedicated Diophantine approximation?*

In the year 2021, the complete work of S. Mochizuki on inter-universal Teichmüller theory (IUTT) was published in PRIMS [14], after a long-lasting review by a collective of international experts: as announced, it contained an ineffective proof of an abc-inequality. One year later, a team of five—including Mochizuki—proved an effective version of the same inequality and wished to apply it for a proof of FLT and possibly Catalan. Although this should be a simple application of such inequalities, which easily prove upper bounds for the solutions, even in this case, the explicit constant in the proof made the existing—quite substantial—known lower bounds for solutions of FLT, such as featured in [17], insufficient for crossing the upper bound that the abc-inequality offered. I had thus the pleasant opportunity to use methods described in the next chapter, and provide improved lower bounds, which had been useless for more than a decade since I knew them [12, 13]. The paper [16] could thus be published, including a complete proof of FLT, and I followed my ignited interest for the old problem, which led also to the present note.[1] I mention in the next chapter a general framework of the kind of attempts made, and possible improvements.

[1] I must mention that I am very well aware of the unfortunate controversy about Mochizuki's work, and do not write as any kind of expert that would address the technical issues, but as a mere spectator and member of the mathematical community. One that regrets the interruption of communication that happened immediately after Scholze and Stix's publication of the short note [18], that happened unfortunately after they had offered the press the opportunity to drag the issue in the muddy waters of journalistic polarization. Interruption that continued despite the not less than five letters sent by Mochizuki over around five years, inviting for an open peer reviewed debate [15]. Sadly, the muddy waters of journalism spread into the mathematical community, and I experienced personally being interrupted during a lecture, for the mere fact of mentioning the publication of [14], by a violent voice from the audience urging me to "stop with this": the incident could only be curbed by waiting for the colleague to leave the room. I can only hope that, better sooner than later, the mathematical substance will get to speak first, leading to a final universal understanding of strength, possible weaknesses or even flaws of IUTT, thus allowing the entire community to profit of what it can offer, and improve what may be improved.

III.2 The cyclotomic setting

In this note we consider the following Diophantine norm equation:

$$\frac{x^p+y^p}{x+y} = p^e z^q; \quad (x,y,z) \in (\mathbb{Z}^*)^3, \quad (x,y,z)=1, \\ \text{and } p,q \text{ are odd primes—not necessarily distinct,} \\ \text{with } p>3;\ e\in\{0,1\}. \tag{3}$$

We will refer to the case when $e=0$ as the first case and, when $e=1$, as the second case of equation (3). The relation between the value of e and x,y,z is explained below. The connection to (1) will become apparent below, from the classical formulas of Barlow and Abel. The term *strong Fermat* (SFLT) has been coined by Georges Gras and Roland Quême [4] for the case $p=q$ of equation (3). We thereby refer to (3) as the *strong Fermat–Catalan* equation. Note that for $p=3$, (3) has infinitely many solutions that stem from norms of qth powers in the Eisenstein integers: if $(x,y)\in\mathbb{Z}^2$, where ρ is a complex third root of unity and $\xi^q = x+y\rho$ for some $\xi\in\mathbb{Z}[\rho]$, then $\frac{x^3+y^3}{x+y} = z^q$, with $z=\xi\cdot\bar{\xi}\in\mathbb{Z}^*$. The condition $p>3$ is thus necessary.

Andrew Beal investigated solutions of the more general equation

$$x^p+y^q+z^r=0 \tag{4}$$

with prime exponents p,q,r and integers x,y,z and found, by astutely leading computer searches, that the equation does have solutions when $(x,y,z)>1$. He then formulated the conjecture that (4) has no solutions in mutually coprime (x,y,z) and exponents $p,q,r\geq 3$. This bears the name of *Beal conjecture*. The slightly more general equation, in which the exponents are allowed to be 2 or 4, is called *super-Fermat equation*, and a list of sporadic solutions with some even exponents is known and conjectured to be complete. I refer to [1] for a survey of solutions and known special cases of (4); this equation is however beyond the framework of this paper. The Fermat–Catalan equation

$$x^p+y^p=z^q \tag{5}$$

—with odd prime exponents $p\neq q$—appears though as a particular case of (4).

Classical results, notations and prerequisites

A classical fact, often attributed to Euler, states that for coprime integers x,y and $n\in 2\mathbb{N}+1$, $n>1$, the greatest common divisor $d=(\frac{x^n+y^n}{x+y}, x+y)$ divides n. This can be easily verified by using the substitution $s=x+y$ and by introducing it in the fraction $\frac{x^n+y^n}{x+y} = \frac{x^n+(s-x)^n}{s}$: the claim follows from $(x,y)=1$. In our case, $n=p$ and if $d=1$, then $p\nmid z$, while for $d=p$, the same substitution implies that $v_p(\frac{x^p+y^p}{x+y})=1$, hence the introduction of p^e in (3).

Using the methods of Barlow and Abel, we find the generalization of their classical factorization [17, lecture IV]: There exist integers u and v, $(u,v)=1$ and $p\nmid uv$, such that

$$x+y=\frac{u^q}{p^e} \quad \text{and} \quad \frac{x^p+y^p}{x+y} = p^e v^p.$$

We see that having solutions to the equation (3) is a necessary—but not sufficient—condition for the Fermat–Catalan equation (5) to have solutions.

We let $P=\{0,1,\dots,p-1\}$, $P^*=P\smallsetminus\{0\}$ be the minimal positive representatives for $\mathbb{F}_p$ and $\mathbb{F}_p^\times$, respectively; ζ will be a primitive pth root of unity and $\mathbb{K}=\mathbb{Q}[\zeta]$ the pth cyclotomic field, with Galois group $G=\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. The automorphisms $\sigma_c\in G$ are given by $\zeta\mapsto\zeta^c$, for $c\in P^*$. Complex conjugation acting on $\mathbb{K}$ is denoted by $\jmath=\sigma_{p-1}=\sigma^{(p-1)/2}$.

Characteristic numbers and characteristic ideals

In the cyclotomic field $\mathbb{K}$, the norm decomposes as:

$$\frac{x^p+y^p}{p^e(x+y)} = \prod_{c\in P^*}\frac{y+\zeta^c x}{(1-\zeta^c)^e}.$$

This leads naturally to the following definition.

Definition 1. We define

$$\alpha = \frac{y+\zeta x}{(1-\zeta)^e},$$

as the *characteristic number* of equation (3) and

$$\mathfrak{A} = (\alpha, z)\subset\mathbb{Z}[\zeta],$$

as the *characteristic ideal* of the same equation.

One notices that $\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)=z^q$, so the characteristic number encodes the existence of a non-trivial solution to (5). By consequence of the definition, so does the characteristic ideal $\mathfrak{A}$. The characteristic numbers and ideals enjoy the following properties, which open the gate to applications of class field theory:

(C1) The characteristic number α is integral.

(C2) The Galois group G acts on the characteristic number, giving rise to pairwise coprime integral elements; that is, for $1\leq c<d\leq p-1$,

$$(\sigma_c(\alpha),\sigma_d(\alpha))=(1).$$

(C3) $\mathfrak{A}$ is related to the *characteristic number* α by the relations:

$$\mathfrak{A}^q=(\alpha), \quad \mathbf{N}(\mathfrak{A})=(z).$$

(C4) The characteristic number satisfies:

$$\frac{\alpha}{\bar{\alpha}} = \upsilon\cdot\frac{1+\zeta(x/y)}{1+\bar{\zeta}(x/y)}, \quad \text{with} \quad \upsilon=\begin{cases}1 & \text{if } e=0,\\ -\bar{\zeta} & \text{for } e=1,\end{cases}$$

and if $e = 0$ we have

$$a' = \zeta^u a = (x+y) \cdot (1 + O(\lambda^2));$$
$$u \equiv \begin{cases} \frac{x}{x+y} \bmod p & \text{if } e = 0, \\ 0 & \text{if } e = 1. \end{cases} \tag{6}$$

The fact that the characteristic ideal has order dividing q suggest using the Stickelberger ideal for producing algebraic numbers that encode the existence of solutions to (5).

The Stickelberger element $\vartheta = \frac{1}{p}\sum_{c=1}^{p-1} c\sigma_c^{-1} \in \frac{1}{p}\mathbb{Z}[G]$ generates the Stickelberger ideal in the group ring of G over the rational integers, by intersecting its principal ideal with $\mathbb{Z}[G]$, according to

$$I = \vartheta\mathbb{Z}[G] \cap \mathbb{Z}[G].$$

There exists a base for I^-, made of $(p-1)/2$ elements, called *Fueter elements*, e.g., [10], which are

$$\psi_n = \vartheta(1 + \sigma_n - \sigma_{n+1}) = \sum_{c \in S_n} n_c \sigma_c^{-1} \in \mathbb{Z}_{\geq 0}[G],$$
$$\text{for } n \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, \tag{7}$$
$$\text{with } n_c = \left(\left[\frac{(n+1)c}{p}\right] - \left[\frac{nc}{p}\right]\right) \text{ and } n_c + n_{p-c} = 1,$$

where the support $S_n \subset \{1, 2, \ldots, p-1\}$, satisfies[2] $S_n \cup (p - S_n) = P^*$ and is deduced from the definition of ψ_n.

It is known that I annihilates the class group $\mathcal{C}(\mathbb{K})$—see for instance [21, § 15.1]—and more precisely, for $\mathfrak{Q} \subset \mathbb{Z}[\zeta]$ and $t \in I$, the ideal $\mathfrak{Q}^t$ is principal, generated by a *Jacobi number* $\mathfrak{q}(t) \in \mathbb{Z}[\zeta]$, that verifies $\mathfrak{q}(t) \equiv 1 \bmod (1-\zeta)^2$—see [5]. Moreover, the elements $t \in I$ verify $t + \jmath t = w(t) \cdot \mathbf{N}_{\mathbb{K}/\mathbb{Q}}$, for a $w(t) \in \mathbb{Z}$, called the *relative weight of* t.

Diophantine approximation using binomial power series

By applying this to the characteristic ideal, we may define an injective map $\mathcal{B} : I \to \mathbb{Z}[\zeta]$ given by

$$(\mathcal{B}(t)) = \mathfrak{A}^t; \quad \mathcal{B}(t) \equiv 1 \bmod (1-\zeta)^2;$$
$$\mathcal{B} \cdot \bar{\mathcal{B}} = z^{w(t)}; \quad \mathcal{B}(t)^q = \zeta^{ut} \cdot a^t.$$

The exponent ut is determined by the condition $\mathcal{B}(t) \equiv 1 \bmod (1-\zeta)^2$ and (6). This leads to the crucial relation:

$$\left(\frac{\mathcal{B}(t)}{\overline{\mathcal{B}(t)}}\right)^q = (-1)^{et} \cdot \zeta^{2u(t)+et} \cdot \left(\frac{1 + \zeta(x/y)}{1 + \bar{\zeta}x/y}\right)^t. \tag{8}$$

By defining for $t = \sum_{c \in P^*} n_c \sigma_c^{-1} \in I$, the formal power series

$$F_t(T) = (1+\zeta T)^{t(1-\jmath)/q}$$
$$= \prod_{c \in P^*} ((1+\zeta^{1/c}T)^{n_c/q} \cdot (1+\zeta^{-1/c}T)^{-n_c/q})$$
$$=: 1 + \sum_{n>0} a_n(t) T^n \in \mathbb{K}[[T]],$$

we conclude from (8) that in every topology in which $F_t(x/y)$ converges, we have

$$\frac{\mathcal{B}(t)}{\overline{\mathcal{B}(t)}} = \xi \cdot (-1)^{et} \cdot \zeta^{(2u(t)+et)/q} \cdot F_t(x/y),$$

where ξ is some qth root of unity in the respective field. The formal power series is a product of binomial power series and its coefficients are *well-behaved* and understood—see for instance [9, 11]. The root of unity ξ is the bottleneck, since it behaves randomly under Galois action, with the exception of complex conjugation.

The generic idea is the following: For some subset $J \subset I$—for instance the G-orbit of some well-chosen $t \in I$, or a larger set—one considers linear forms

$$\Delta(J, \vec{\ell}) = \sum_{t \in J} \ell(t)\mathcal{B}(t) \in \mathbb{Z}[\zeta],$$

where the vector $\vec{\ell} \in (\mathbb{Z}[\zeta])^{|J|}$ is chosen in order to satisfy the conditions of the following

Strategy 1.

(L1) The infinity-norm $\|\vec{\ell}\| := \max(|\ell(t)|; t \in J) \leq \Lambda \in \mathbb{R}$.

(L2) One proves that $\Delta(t, J) \neq 0$.

(L3) The values of $\ell(t)$ are such that the linear combination $\sum_{t \in J} \ell(t) a_n(t) = 0$ for $n \leq M$, and the bounds M and Λ are such that it is possible to estimate $|\Delta(t, \vec{\ell})|$ and this estimate contradicts the vanishing of the first M terms in the power series development.

(L4) Concretely, in the complex topology, the linear combination of power series will be smaller than 1 in absolute value in all embeddings, while by (L2), $\mathbf{N}(\Delta(t, J))$ is a non-vanishing integer. In local completions, the converse happens: the vanishing of the leading terms of the power series implies that $|\Delta(t, J)|$ is globally *large*—$O(x^M)$—while the choice of Λ and estimates for $|\mathcal{B}(t)| = z^{w(t)/2}$ are used to prove that $|\Delta(t, J)|$ is globally smaller.

The original proof of Catalan's conjecture used a network of additional properties of solutions to (2); these allowed to extend the $\mathcal{B}$-map to annihilators of the real part of $\mathcal{C}(\mathbb{K})$. This way, the dependency of undetermined roots of unity vanishes, and the proof emerged from the investigation of one single series; no linear combinations were necessary. In a few later applications of mine and a few other authors, the generic approach described above was followed more closely, *albeit only in the global case and*

[2] The set $p - S_n$ designates naturally $\{p - r : r \in S_n\}$.

for binary equations. The roots of unity were treated simply as additional unknowns—which of course increases the complexity of the linear algebra and the bounding strategies. Recently, together with my doctoral student Chang Liu, we completed a new proof of the same conjecture using only annihilation by the Stickelberger ideal [8]. When treating the roots of unity as Galois independent indeterminates—which they are—the consequence is an increased number of linear conditions needed for obtaining the same order of vanishing M in (L3); this in return increases the bound Λ in (L1). The result in [8] is noteworthy, since we succeeded to decrease Λ by use of short vectors in lattices, and nevertheless assure the non-vanishing condition (L2), which is reputed as very difficult when using variants of Siegel's box principle.

All the above results use the global variant of Strategy 1. The local strategy requires semi-local power series development, in all the completions at primes $\mathfrak{R}|x$ in $\mathbb{K}$. One thus works in the "*x-idéles*"[3]

$$\mathbb{K}_x := \prod_{\mathfrak{R}|x} \mathbb{K}_{\mathfrak{R}}.$$

While in this case the unknown roots of unity are acted upon by the idelic lift of the Galois group G, the number of independent roots depends on the number of such prime ideals $\mathfrak{R}$, which is not known to obey any bound. The diversity of fascinating alternative power series and relations, already in the case of the Fermat equation, invites to pursued attempts for searching some combination that succeeds to meet all the requirements. However, the final bottleneck remains in all cases the fact that the size of the ideal I/pI limits the size of J, but it is comparable, possibly identical, to the number of various local values that the roots ξ can have. Unlike the global case, where it was possible to control roots of unity either by directly working in $\mathbb{R}$ when possible, or by treating them as unknowns—which have the advantage of having the smallest possible norm, being units—there is no way to simplify the contribution of the *local* roots of unity. In fact, the very assumption that they would vanish for an entire G-orbit Gt, $t \in I$, suffices for obtaining upper bounds on $|x|$ in (3), which imply FLT.

These challenges and the lack of any successful application of the local strategy would seem not to recommend it for further study. On the other hand, the map β produces a large variety of algebraic numbers with both arithmetic specificity and size anchored in the very values of the purported solution of (3)—whose existence one tries to do infirm—and it encrypts by equivalence the existence of these solutions. There remain reasons to expect that some new ideas, and a better combination of Strategy 1 with arithmetic properties and some ideas connecting applications of the Bombieri–Vaaler theorem could lead to the success which is missed by a fraction, in the crude version of the strategy.

[3] The ring used is not formally equal to the x-idéles, but conserves their arithmetic and Galois properties.

An appealing reason for facing these challenges lays in the fact that—at least in the present crude version—the proposed approach does not see deep distinction between the Fermat and the Fermat–Catalan cases, and the equation (3) is one about which very little is known presently.

III.3 Cyclotomic conjectures and properties implying FLT

The hypothesis of Kummer, stating that p does not divide the class number of the real pth cyclotomic field, fascinated Harry Schultz Vandiver. He published in the first half of the 20th century a long series of criteria for FLT, with the apparent expectation to reduce the proof of the conjecture to the hypothesis, which bared for a long time the name of *Vandiver conjecture*; until Lang discovered a correspondence of Kummer and Dedekind, in which the first referred precisely to that hypothesis, so the name became *the Kummer–Vandiver conjecture*. It was proved in the times of Vandiver, that FLTII follows from this conjecture and an additional condition. Vandiver himself published a paper which promised to reduce the truth of the First Case to a mere consequence of the same conjecture. The proof was however incorrect, and still by the time Ribenboim wrote his *13 Lectures* [17], the statement was considered to be irrecoverably false. However, Sitaraman uncovered from Vandiver's writings and proved with more transparent methods in [19], an implicit additional condition that Vandiver had not stated, and which together with the Kummer–Vandiver conjecture implies the truth of FLTI. There is thus today a program in three points—see also [1]—for proving FLT as a consequence of deeper theoretical conjectures or possible facts of cyclotomy. The assumptions to prove are the following:

Strategy 2. *Assumption A:* The Kummer–Vandiver conjecture is true, so p does not divide the class number of the real p-cyclotomic field $\mathbb{K}^+$.

Assumption B: Assume that the exponent of the p-Sylow subgroup $(C(\mathbb{K}))_p$ is p, whereby the p-part of the class group of the pth cyclotomic field is annihilated by p.

Assumption C: Assume that all the units $\delta \in \mathbb{Z}[\zeta_p + \bar{\zeta}_p]^\times$ for which there exists an algebraic integer $\rho \in \mathbb{Z}[\zeta_p + \bar{\zeta}_p]$ such that $\delta \equiv \rho^{p^2} \bmod (p(1-\zeta))^2 \cdot \mathbb{Z}[\zeta_p + \bar{\zeta}_p]$ are global pth powers.

Assumption D: Assume that the relative class number of the p-cyclotomic field verifies

$$|(C(\mathbb{K}))_{\bar{p}}| < \sqrt{p} - 1.$$

The first three assumptions imply FLT, but these results would have wider theoretical consequences than merely such proof. Their application to Diophantine equations however would be restricted to this and possibly few more strongly related exponential equations: the core restriction is that all exponents in an equation to which these facts can be applied, must be p! It is probable that ideas

and facts from Iwasawa theory could indicate useful approaches for the proof of these assumptions, but discussing more details goes beyond the scope of this brief note.

The Assumption D is of particular interest not only because it implies FLTI, by the result of Eichler [3]. But in spite of the fact that Washington's heuristics—see [6, pp. 261–265]—suggest that $|(C(\mathbb{K}))_p^-| = O(\log(p)/\log\log(p))$, the only upper bound known for the p-part is derived from the very accurate upper bounds given by Lepistö in [7] for the entire minus part of the class group, assuming that it is all limited to the p-Sylow subgroup. This is of course a crude assumption, and we conclude this note by suggesting a combinatorial approach that may provide some improvements. If they succeed in proving less or more than Assumption D depends on the accuracy of the combinatorics. The idea is the following: Iwasawa proves—see [21, Theorem 6.21]—that

$$|(\mathbb{Z}[G]/I)_p^-| = h_p^- := |(C(\mathbb{K}))_p^-|.$$

Lower bounds for $|(I/pI)^-|$ thus provide upper bounds for h_p^-. Let

$$\mathcal{F} = \Big\{\psi_n : n \in P^*,\ n \le \frac{p-1}{2}\Big\} \subset I, \quad \text{and} \quad \overline{\mathcal{F}} = \{G\psi : \psi \in \mathcal{F}\}$$

be the Fueter elements in (7) and their G-orbits. For $0 < m < p$, the set

$$\mathbf{F}_m = \Big\{\sum_j c_j t_j \ :\ 0 \le c_j;\ t_j \in \overline{\mathcal{F}} \ \text{ and } \sum_j c_j \le m\Big\} \subset I/pI.$$

The combinatorial problem consists in estimating the number of mutually distinct elements in $\mathbb{Z}[G]$ that lie in $\mathbf{F}_{p-1}$. Since we allow for entire G-orbits in $\overline{\mathcal{F}}$, the linear combinations in $\mathbf{F}$ will contain multiple representations of the same element in $\mathbb{Z}[G]$ modulo the norm, and estimates become hard. Chang Liu computed $|\mathbf{F}_2| = \frac{(p-1)^2((p-2)^2+27)}{72}$ in [8]. One expects that the general result will be of the form $|\mathbf{F}_m| = \frac{h_m(p)}{D_m}$, with $h_m \in \mathbb{Z}[X]$, a polynomial of degree $2m$ and $D_m \in \mathbb{N}$. The size of D_m however grows unpredictably. But even predicting some recursively provable upper bounds for D_m and lower bounds for $h_m(p)$ may provide useful results.

References

[1] M. Bennett, P. Mihăilescu and S. Siksek, The generalized Fermat equation. In *Open Problems in Mathematics*, Springer, Cham, 173–205 (2016)

[2] Y. F. Bilu, Y. Bugeaud and M. Mignotte, *The problem of Catalan*. Springer, Cham (2014)

[3] M. Eichler, Eine Bemerkung zur Fermatschen Vermutung. *Acta Arith.* **11**, 129–131 (1965)

[4] G. Gras and R. Quême, Vandiver papers on cyclotomy revisited and Fermat's Last Theorem. In *Publ. Math. Besançon Algèbre Théorie Nr.* **2012/2**, Presses Univ. Franche-Comté, Besançon, 47–111 (2012)

[5] K. Iwasawa, A note on Jacobi sums. In *Symposia Mathematica, Vol. XV*, Academic Press, London–New York, 447–459 (1975)

[6] S. Lang, *Cyclotomic fields I and II*. second ed., Grad. Texts in Math. 121, Springer, New York (1990)

[7] T. Lepistö, On the growth of the first factor of the class number of the prime cyclotomic field. *Ann. Acad. Sci. Fenn. Ser. A. I.* **577** (1974)

[8] C. Liu and P. Mihăilescu, An alternative proof of the Catalan conjecture. *Bull. Transilv. Univ. Braşov Ser. III. Math. Comput. Sci.* **5(67)**, 161–172 (2025)

[9] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.* **572**, 167–195 (2004)

[10] P. Mihăilescu, A cylcotomic investigation of the Fermat–Catalan equation. arXiv:math/0702766v1 (2007)

[11] P. Mihăilescu, Class number conditions for the diagonal case of the equation of Nagell and Ljunggren. In *Diophantine approximation*, Dev. Math. 16, Springer, Vienna, 245–273 (2008)

[12] P. Mihăilescu, Improved lower bounds for possible solutions in the second case of the Fermat Last Theorem and in the Catalan equation. *J. Number Theory* **225**, 151–173 (2021)

[13] P. Mihăilescu and M. T. Rassias, Double exponential lower bounds for possible solutions in the second case of the Fermat Last Theorem. *J. Number Theory* **238**, 1063–1080 (2022)

[14] S. Mochizuki, Inter-universal Teichmüller theory I, II, III, IV. *Publ. Res. Inst. Math. Sci.* **57**, 3–723 (2021)

[15] S. Mochizuki, https://www.kurims.kyoto-u.ac.jp/~motizuki/Rpt2018.pdf, https://www.kurims.kyoto-u.ac.jp/~motizuki/IUT-report-2025-10.pdf, IUT-report-2024-12, IUT-report-2023-06. (Reports concerning the inter-universal Teichmüller theory.) Research Institute for Mathematical Sciences, Kyoto University

[16] S. Mochizuki, I. Fesenko, Y. Hoshi, A. Minamide and W. Porowski, Explicit estimates in inter-universal Teichmüller theory. *Kodai Math. J.* **45**, 175–236 (2022)

[17] P. Ribenboim, *13 lectures on Fermat's last theorem*. Springer, New York (1979)

[18] P. Scholze and J. Stix, Why *abc* is still a conjecture. (2018) https://www.math.uni-bonn.de/people/scholze/WhyABCisStillaConjecture.pdf

[19] S. Sitaraman, Vandiver revisited. *J. Number Theory* **57**, 122–129 (1996)

[20] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)* **141**, 553–572 (1995)

[21] L. C. Washington, *Introduction to cyclotomic fields*. Second ed., Grad. Texts in Math. 83, Springer, New York (1997)

[22] A. Wiles, Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math. (2)* **141**, 443–551 (1995)