Parametric Algorithms for the 5-Modular Analog of ES (Sierpiński): Structure of Solutions, Parameterization, and Constructive Proofs (SERP)

E. Dyachenko
dyachenko.eduard@gmail.com

November 26, 2025

Abstract

We consider the problem of representing the fraction $\frac{5}{P}$ as a sum of three distinct unit fractions:

$$\frac{5}{P} = \frac{1}{A} + \frac{1}{B} + \frac{1}{C}, \qquad A < B < C, \quad A, B, C \in \mathbb{N}.$$

We analyze the case of primes $P \equiv 1 \pmod 5$, for which two types of solutions are distinguished: ED1 (exactly one denominator divisible by P, namely $C = cP$) and ED2 (exactly two denominators divisible by P, namely $B = bP$ and $C = cP$). Parametric constructions and enumeration algorithms are developed, including transitions between types of solutions.

The paper proposes a deterministic algorithm based on searching for the intersection of a parametric lattice, defined by a pair (α_i, d_i'), with the box $\mathcal{B}_k(T)$. For any fixed prime $P \equiv 1 \pmod 5$ the algorithm constructively produces a solution. Using analytic methods (Bombieri–Vinogradov theorem, Chebotarev theorem), it is shown that the density of admissible parameters is high, which ensures polylogarithmic search complexity in the average case, i.e., for most primes. A strict complexity guarantee for all primes remains conditional and depends on the finite covering hypothesis.

This study continues the work for coefficient 4 (the Erdős–Straus conjecture) [2]; here a similar structure of parameterization and solutions is extended to coefficient 5. In the analytic applications, averaging tools are provided, used for density estimates in parametric boxes.

1 Introduction

The Sierpiński problem in the 5-modular variant is formulated as follows: for a prime P one must find natural numbers $A < B < C$ satisfying

$$\frac{5}{P} = \frac{1}{A} + \frac{1}{B} + \frac{1}{C}. \tag{1.1}$$

2020 *Mathematics Subject Classification*: Primary 11N05, 11P21; Secondary 94A60, 20P05.

Key words and phrases: factorization, Bombieri–Vinogradov large sieve, the larger sieve of Greaves, deterministic algorithms; analytic number theory; number theory.

Analogous to the Erdős–Straus conjecture for $\frac{4}{P}$, here the coefficient 5 leads to a change in the structure of parameterizations and to new types of solutions. For primes $P \equiv 1 \pmod 5$ two constructive classes are distinguished:

- ED1: exactly one denominator divisible by P (without loss of generality $C = cP$);
- ED2: exactly two denominators divisible by P (namely $B = bP$ and $C = cP$).

1.1 Transition from $4/P$ to $5/P$

The methods of parameterization and proofs from [2] are preserved in the present study, but the core formulas change in the transition $4 \to 5$. In particular:

- estimate for the minimal denominator: $P < 5A < 3P$;
- in ED1 the relation takes the form $5c - 1 = \gamma P$ (instead of $4c - 1 = \gamma P$);
- in ED2 the core takes the form $t = 5bc - b - c$ and $(5b - 1)(5c - 1) = 5P\delta + 1$.

Thus, the problem $5/P$ is a direct analogue of the case $4/P$, but requires new constructive techniques. Unlike factorization-based approaches used in classical works on ESC, here methods of finite covering of residue classes and lattice algorithms are applied. These tools allow one to prove the existence of solutions for every prime $P \equiv 1 \pmod 5$ and ensure polylogarithmic complexity of the search algorithm.

2 Motivation

The parameterization of the equation and the division into multiplicity configurations ($P \mid B$ and/or $P \mid C$) make it possible to construct explicit search procedures and to prove the existence of solutions for the case $P \equiv 1 \pmod 5$. This approach not only guarantees the existence of solutions but also defines the structure of families in arithmetic progressions.

The possibility of transferring the constructive method from coefficient 4 to coefficient 5 was correctly noted in [7]. In the present work this transfer is carried out explicitly within the framework of the ED1/ED2 methods developed in [2]. The key element here is the mechanism of *finite covering of residue classes*, which guarantees the existence of solutions for every prime $P \equiv 1 \pmod 5$ without recourse to factorization. Thus, the motivation of the study is to show that constructive methods based on lattices and covering of residue classes allow one to move from asymptotic reasoning to effective algorithms with polylogarithmic complexity.

3 Ordering

For the classes $P \equiv 4, 3, 2 \pmod 5$ explicit decompositions are available; the remaining case is $P \equiv 1 \pmod 5$.

3.1 Explicit decompositions for $P \not\equiv 1 \pmod 5$

Let $P = 5P' + 4$ be prime:

$$\frac{5}{P} = \frac{5}{5P' + 4} = \frac{1}{P' + 1} + \frac{1}{2 \cdot (P' + 1) \cdot (5P' + 4)} + \frac{1}{2 \cdot (P' + 1) \cdot (5P' + 4)}.$$

Let $P = 5P' + 3$ be prime:

$$\frac{5}{P} = \frac{1}{P' + 1} + \frac{1}{(P' + 1)(5P' + 3)} + \frac{1}{(P' + 1)(5P' + 3)}.$$

Let $P = 5P' + 2$ be prime (here P' is odd):

$$\frac{5}{P} = \frac{5}{5P'+2} = \frac{1}{P'+1} + \frac{2}{(P'+1)\cdot(5P'+2)} + \frac{1}{(P'+1)\cdot(5P'+2)} = \frac{1}{P'+1} + \frac{1}{\frac{(P'+1)}{2}\cdot(5P'+2)} + \frac{1}{(P'+1)\cdot(5P'+2)}$$

where the third summand is further detailed as a sum of two parts, since $P'+1$ is even. The case $P = 5P' + 1$ is the subject of this paper.

3.2 Estimate for the minimal denominator

If $A \leq B \leq C$ and $A, B, C \in \mathbb{N}$, then

$$\frac{5}{P} > \frac{1}{A} \quad \Rightarrow \quad 5A > P \quad \Rightarrow \quad P < 5A.$$

Moreover, from $A \leq B \leq C$ it follows that

$$\frac{5}{P} = \frac{1}{A} + \frac{1}{B} + \frac{1}{C} \leq \frac{3}{A} \quad \Rightarrow \quad 5A \leq 3P,$$

and, excluding the degenerate case $A = B = C$, we obtain strict bounds:

$$P < 5A < 3P. \tag{3.1}$$

4 Notation

Main parameters	
P	prime number > 2, with $5 \nmid P$; often $P \equiv 1 \pmod 5$, $P \equiv 2 \pmod 5$, $P \equiv 3 \pmod 5$, $P \equiv$
P'	integer: $P = 5P' + 1$
A, B, C	denominators in the Sierpiński hypothesis formula, ordered $A \le B \le C$
H(S)	Sierpiński hypothesis: $\frac{5}{P} = \frac{1}{A} + \frac{1}{B} + \frac{1}{C}$
Parameters of the ED1 and ED2 methods	
γ	$\frac{5c-1}{P}$ (or $\frac{5b-1}{P}$ in the second case); often $\gamma \equiv 4 \pmod 5$, $\gcd(\gamma, c) = 1$ or $\gcd(\gamma, b) = 1$
u, v	"multipliers" in the identity: for ED1 $u = \gamma A - c$, $v = \gamma B - c$, $uv = c^2$; for the variant with b: $u = \gamma A - b$, $v = \gamma C - b$, $uv = b^2$; always $u \le v$. The factorization d
δ	$t = P \cdot \delta$, with ED2 requiring $\delta \mid bc$
b, c	in ED2 $B = bP$ and/or $C = cP$
t	$t = 5bc - b - c$
r, s	$r = 5b - 1$, $s = 5c - 1$, with $r \equiv s \equiv 4 \pmod 5$, $rs = 5P\delta + 1$
g	$\gcd(b, c)$
b', c'	decomposition $b = b'g$, $c = c'g$ (normalized form)
d'	square factor in the decomposition of δ
α	squarefree factor in the decomposition of δ
Transitions between methods	
$\mathcal{C}_{\mathrm{ED1}}(P)$	set of admissible quadruples (γ, c, u, v) for ED1
$\mathcal{C}_{\mathrm{ED2}}(P)$	set of admissible triples (δ, b, c) for ED2
y	minimal divisor of $5c - 1$, with $y \equiv 3 \pmod 5$
P''	modulus for ED1 in convolution, defined via γ by the formula ...
ED2→ED1	transition: $A = \frac{bc}{\delta}$, $B = bP$; $u = \gamma A - c$, $v = \gamma B - c$
ED1→ED2	transition: $A = \frac{u+c}{\gamma}$, $b = \frac{v+c}{\gamma P}$, $\delta = \frac{bc}{A}$
Anticonvolution	algorithm for the reverse step ED1→ED2 according to the formulas above
Lattices and boxes	
k	dimension of the vector parameter
$u_0(P)$	vector shift for the affine class
Λ, Λ_j	sublattices of $\mathbb{Z}^k$ of index M or M_j
M, M_j	indices of sublattices
$\mathcal{B}_k(T)$	box $\{u \in \mathbb{Z}^k : 1 \le u_i \le T\}$
$\mathcal{B}_P^{(I)}$, $\mathcal{B}_P^{(II)}$	boxes of type I/II with additional conditions
$\mathcal{G}_P(T)$	admissible parameters in the box
$\mathcal{G}_P^*$	class of admissible quadruples (γ, c, u, v) for ED1, satisfying: $\gamma \in \mathbb{N}$, $c \in \mathbb{Z}$, $u = \gamma A - c$, $v = \gamma B - c$, $uv = c^2$, $u \le v$
Analytic notation	
$\left(\frac{a}{P}\right)$	Legendre symbol; for composite modulus the $\left(\frac{a}{\gamma}\right)$ (Jacobi symbol, for prime P) is used
$\pi(y)$	prime counting function
$\ll$, $\gg$, $\asymp$	standard asymptotic symbols
D	set $\delta \le X$, $\delta \equiv 4 \pmod 5$
$T(\delta)$	prime counting function in progression, see Appendix §A

5 Parametrization of ED1 (one multiple, $C = cP$)

5.1 Kernel and identities

Let $C = cP$. From (1.1) it follows that

$$(5c-1)AB = cP(A+B). \tag{5.1}$$

Setting $\gamma = \dfrac{5c-1}{P} \in \mathbb{N}$, we obtain

$$(\gamma A - c)(\gamma B - c) = c^2. \tag{5.2}$$

Hence $\gamma \equiv 4 \pmod 5$ and $\gcd(\gamma, c) = 1$ (since $5c \equiv 1 \pmod\gamma$).

Lemma 5.1. *We always have* $\gcd(\gamma, c) = 1$.

Proof. From $5c - 1 = \gamma P$ we obtain $5c \equiv 1 \pmod\gamma$, hence $\gcd(\gamma, c) = 1$. □

5.2 Full parametrization of ED1 with filters by P

Theorem 5.2. *Let* $P \equiv 1 \pmod 5$, $\gamma \equiv 4 \pmod 5$, $5c - 1 = \gamma P$, $\gcd(\gamma, c) = 1$. *Let* $u, v \in \mathbb{N}$ *such that*

$$uv = c^2, \qquad u \equiv v \equiv -c \pmod\gamma, \qquad u \not\equiv -c \pmod P, \quad v \not\equiv -c \pmod P.$$

Then

$$A = \frac{u+c}{\gamma}, \quad B = \frac{v+c}{\gamma}, \quad C = cP$$

give a solution of (1.1) *of type* ED1 *with* $P \nmid A, B$. *Conversely, every* ED1*-solution generates such* γ, c, u, v.

Proof. From (5.1) it follows that (5.2) holds. Setting $u = \gamma A - c$, $v = \gamma B - c$, we obtain $uv = c^2$ and $u \equiv v \equiv -c \pmod\gamma$, whence $\gamma \mid (u + c)$, $\gamma \mid (v + c)$ and $A, B \in \mathbb{N}$. The conditions $u \not\equiv -c \pmod P$, $v \not\equiv -c \pmod P$ are equivalent to $P \nmid A$, $P \nmid B$ thanks to $\gcd(\gamma, c) = 1$ and $5c - 1 = \gamma P$. Reversibility follows from (5.2). □

5.3 Multiplicity filters by P

From $A = (u + c)/\gamma$, $B = (v + c)/\gamma$, $5c - 1 = \gamma P$ we have

$$P \mid A \iff u \equiv -c \pmod P, \qquad P \mid B \iff v \equiv -c \pmod P.$$

For ED1 it is required simultaneously that $u \not\equiv -c \pmod P$ and $v \not\equiv -c \pmod P$.

5.4 Example: $P = 11$

The minimal $\gamma \equiv 4 \pmod 5$ with $5c - 1 = \gamma P$ gives $\gamma = 4$, $c = (4 \cdot 11 + 1)/5 = 9$. Divisors of $c^2 = 81$, compatible with $u \equiv -c \equiv 3 \pmod 4$ and $u \not\equiv -c \equiv 2 \pmod{11}$, include $u = 3$, $v = 27$. Then

$$A = \frac{3+9}{4} = 3, \quad B = \frac{27+9}{4} = 9, \quad C = 99, \quad \frac{1}{3} + \frac{1}{9} + \frac{1}{99} = \frac{5}{11}.$$

6 Parametrization of ED2 (two multiples, $B = bP$, $C = cP$)

6.1 Setup and identities

Consider

$$\frac{5}{P} = \frac{1}{A} + \frac{1}{bP} + \frac{1}{cP}, \qquad A < bP \le cP, \quad P \nmid A.$$

Multiplying by $AbcP$, we obtain

$$A(5bc - b - c) = Pbc. \tag{6.1}$$

Let $t := 5bc - b - c = P\delta$, $\delta \in \mathbb{N}$. Then

$$A = \frac{bc}{\delta}. \tag{6.2}$$

Equivalently,

$$(5b - 1)(5c - 1) = 5P\delta + 1. \tag{6.3}$$

Setting $r = 5b - 1$, $s = 5c - 1$, we obtain $rs = 5P\delta + 1$ and $r \equiv s \equiv 4 \pmod 5$.

6.2 Full parametrization of ED2

Theorem 6.1. *Let P be prime and $\delta \in \mathbb{N}$. Let $r, s \in \mathbb{N}$ such that*

$$r\,s = 5P\delta + 1, \qquad r \equiv s \equiv 4 \pmod 5.$$

Set $b = (r + 1)/5$, $c = (s + 1)/5$. If $\delta \mid bc$, then

$$A = \frac{bc}{\delta}, \qquad B = bP, \qquad C = cP$$

give a solution of (1.1) of type ED2*. Under permutation $r \leftrightarrow s$ we have $b \leftrightarrow c$ and $B \leftrightarrow C$; ordering $B \le C$ is achieved by choosing $r \le s$. Moreover, for $b \le c$ we have $A \le B$.*

Proof. From (6.1) and $t = P\delta$ it follows that (6.2) holds. Equality (6.3) is obtained from $(5b - 1)(5c - 1) = 25bc - 5b - 5c + 1 = 5(5bc - b - c) + 1 = 5P\delta + 1$. The congruences $r \equiv s \equiv 4 \pmod 5$ are obvious. For $b \le c$ we have

$$A \le B \iff \frac{bc}{\delta} \le bP \iff c \le P\delta = 5bc - b - c \iff c(5b - 2) \ge b,$$

which holds for $b \ge 1$, $c \ge b$. □

6.3 Example: $P = 11$

Take $\delta = 1$. Then $5P\delta + 1 = 56 = 4 \cdot 14$, $4 \equiv 14 \equiv 4 \pmod 5$. The pair $r = 4$, $s = 14$ gives $b = 1$, $c = 3$, $A = 3$, $B = 11$, $C = 33$. Verification:

$$\frac{1}{3} + \frac{1}{11} + \frac{1}{33} = \frac{11 + 3 + 1}{33} = \frac{15}{33} = \frac{5}{11}.$$

7 Multiplicity configurations with respect to P and classification

Lemma 7.1. *In any solution of (1.1) at least one of A, B, C is divisible by P.*

Proof. Multiplying (1.1) by $ABCP$: $5ABC = P(AB + AC + BC)$. Modulo P: $5ABC \equiv 0$, hence $P \mid ABC$. □

Lemma 7.2. *It is impossible that $A = aP$, $B = bP$, $C = cP$ simultaneously.*

Proof. Then $5 = 1/a + 1/b + 1/c \leq 3$ — impossible. □

Lemma 7.3. *The minimal denominator A is not divisible by P.*

Proof. From (3.1) we have $5A < 3P$; if $A = aP$, then $5A \geq 5P > 3P$, a contradiction. □

Proposition 7.4. *Every solution of (1.1) for prime $P \neq 5$ falls into exactly one of the classes: - ED1: exactly one denominator divisible by P (without loss of generality $C = cP$), with $P \nmid A, B$; - ED2: exactly two denominators divisible by P (namely $B = bP$, $C = cP$), with $P \nmid A$. The cases "none" and "all three" are excluded by Theorems 7.1 and 7.2, and Theorem 7.3 excludes $P \mid A$.*

7.1 Intermediate transition to parameters b', c'

From Theorem 7.4 it follows that every solution of (1.1) for $P \equiv 1 \pmod 5$ belongs either to class ED1 or to class ED2. In both cases it is convenient to isolate normalized parameters that describe the part of denominators divisible by P.

- In the case ED1 we have $C = cP$, and the parameters γ, c arise from normalizing the condition $5c - 1 = \gamma P$.
- In the case ED2 we have $B = bP$, $C = cP$, and the parameters b', c' arise from the kernel $(5b - 1)(5c - 1) = 5P\delta + 1$.

Thus, in the case ED2 the problem reduces to analyzing pairs (b', c') with additional divisibility and congruence conditions.

7.2 Parametric box in coordinates (b', c')

For a fixed threshold T consider the set

$$B_{b',c'}(T) = \{(b', c') \in \mathbb{N}^2 : 1 \leq b', c' \leq T,\ b' < c'\}.$$

This set contains all candidates for solutions in the original parameters. Additional conditions (e.g., $\gcd(b', c') = 1$, congruences modulo d, divisibility $4b'c' = P + d$) are imposed as filters on the points (b', c').

7.3 Box threshold via A and P

From the inequality

$$P < 5A < 3P$$

it follows that the minimal denominator A always lies in the interval $(P/5,\ 3P/5)$. This provides natural bounds for the parametric box.

Definition 7.5. For a fixed prime P we define the box in the original parameters (b', c') as

$$B_{b',c'}(P) = \{(b', c') \in \mathbb{N}^2 : 1 \leq b', c' \leq 3P/5,\ b' < c'\}.$$

7.4 Transition to coordinates (x, y)

Under the linear transformation

$$x = b' + c', \qquad y = c' - b',$$

the image of the set $B_{b',c'}(P)$ is the sublattice

$$B_{x,y}(P) = \{(x, y) \in \mathbb{Z}^2 : x \equiv y \pmod 2,\ x > y > 0,\ x, y \le 6P/5\}.$$

7.5 Condition for d'

In the original system the parameter d' appears as the square factor in the decomposition of δ. In the new coordinates the condition $d' \mid (b' + c')$ is rewritten as

$$d' \mid x.$$

Proposition 7.6. *The existence of a point $(x, y) \in B_{x,y}(P)$ satisfying the conditions $x \equiv y \pmod 2$, $y > 0$, $x, y \le 6P/5$ and $d' \mid x$, is equivalent to the existence of an admissible pair (b', c') and hence to a solution of (1.1).*

7.6 Corollary

Defining the box $B_{b',c'}(T)$ and transferring it to coordinates (x, y), we obtain a lattice with simple linear conditions: - parity $x \equiv y \pmod 2$, - order $y > 0$, - bound $x, y \le 2T$, - divisibility $d' \mid x$.

Thus, the existence of a solution is equivalent to the presence of a point (x, y) in the box $B_{x,y}(T)$ satisfying these conditions. This makes the proof constructive and allows the use of methods of finite covering of residue classes.

Example Table 1

Table 1: ED2-decompositions for $P = 73$

P	A	B	C	b	c	δ	α, d'
73	15	584	8760	8	120	64	$\alpha = 1,\ d' = 8$
73	15	657	3285	9	45	27	$\alpha = 3,\ d' = 3$
73	15	730	2190	10	30	20	$\alpha = 5,\ d' = 2$
73	15	876	1460	12	20	16	$\alpha = 1,\ d' = 4$

7.7 Geometry of the surface and thickenings

Consider the quadratic surface

$F(\delta, b, c) = (5b - 1)(5c - 1) - 5P\delta - 1 = 0.$

The thickening of this surface, given by the condition $|F| \le \Delta$ in the parameter space (δ, b, c), yields the set of ED2 candidates. Since we work in the context of discrete values, it is critical to estimate the number of solutions satisfying modular conditions.

Lemma 7.7 (Window in δ)**.** *For fixed values of b and c, and for $\Delta \ge 0$, the number of integers δ satisfying the condition $|F(\delta, b, c)| \le \Delta$ does not exceed:*

$1 + \left\lfloor \frac{2\Delta}{5P} \right\rfloor.$

Proposition 7.8 (Estimate of thickening size)**.** *In the box where $b \in [B, 2B]$ and $c \in [C, 2C]$, the total number of triples (δ, b, c) for which the condition $|F| \le \Delta$ holds can be estimated as:*

$\ll \left(1 + \frac{\Delta}{P}\right) BC + B + C.$

Remark 7.9. For pairs (b, c) subject to the condition $\delta \mid bc$, the number of such pairs in the corresponding rectangle is $\ll \frac{BC}{\delta}\tau(\delta) + B + C$.

8 Constructive geometry of ED2 for the Sierpiński hypothesis (preserving the logic of ESC)

8.1 Setup and kernel, fully analogous to ESC

For a prime $P \equiv 1 \pmod 5$ we prove the existence of a solution

$$\frac{5}{P} = \frac{1}{A} + \frac{1}{B} + \frac{1}{C}, \qquad B = bP,\ C = cP,\ P \nmid A,\ b \neq c.$$

Multiplying by $AbcP$ and introducing the parameter $\delta \in \mathbb{N}$, we obtain

$$A(5bc - b - c) = P\,bc, \qquad 5bc - b - c = P\delta, \qquad A = \frac{bc}{\delta}.$$

Quadratic kernel ED2:

$$(5b - 1)(5c - 1) = 5P\delta + 1.$$

This is fully isomorphic to the kernel for ESC ($k = 4$) under the substitution $4 \mapsto 5$: all checks and constructions transfer verbatim.

8.2 Normalization and linear system (as in ESC)

Let $b = g\,b'$, $c = g\,c'$, where $g = \alpha d'$ and $\gcd(b', c') = 1$, and

$$\delta = \alpha\,(d')^2, \quad \alpha \text{ squarefree.}$$

Then the canonical conditions (ED2) take the linear form

$$b'c' = M = A\alpha, \qquad b' + c' = m\,d', \qquad m = 5A - P > 0.$$

In coordinates $x = b' + c'$, $y = c' - b'$ we have

$$x = m\,d', \qquad \frac{x^2 - y^2}{4} = A\alpha, \qquad x \equiv y \pmod 2.$$

This is exactly the same affine lattice of finite index as in the ESC section, with the coefficient k replaced.

8.3 Parametric box and geometric covering (transfer from ESC)

The minimal denominator is bounded by

$$\frac{P}{5} < A < \frac{3P}{5}.$$

The projection of the lattice Λ_{ED2} onto the (x, y)-plane lies in a box of linear size $O(P)$; the diagonal period equals d', and for $H, W \geq d'$ the intersection of the box with the lattice is nonempty. The lattice index does not depend on P, as in ESC, which stabilizes the density of admissible points and ensures constructive covering without factorization.

8.4 Back-test filters and non-degeneration (identical to ESC scheme)

For any assembled row we check:

$$(5b - 1) \equiv (5c - 1) \equiv 4 \pmod 5, \quad \delta \mid bc, \quad \gcd(b', c') = 1,$$

$$b' + c' = m\,d', \quad b'c' = A\alpha, \quad A = \frac{bc}{\delta} \in \mathbb{Z}, \quad \frac{P}{5} < A < \frac{3P}{5}.$$

Order and distinctness: $b \neq c$, consistent ordering of denominators (according to your editorial scheme), without degeneration.

Table 2: Examples of ED2-decompositions for $k = 5$ (Sierpiński)

P	A	B	C	b	c	δ	$\alpha,\ d'$
73	15	657	3285	9	45	27	$\alpha = 3,\ d' = 3$
97	22	194	1067	2	11	1	$\alpha = 1,\ d' = 1$

8.5 Examples of ED2 for insertion (audit)

8.6 Conclusion (in the logic of ESC)

The ED2 method translates the search for solutions for $k = 5$ into a linear lattice problem in a bounded box, fully analogous to the ESC section: kernel, normalization, finite-index lattice, back-test, and geometric covering provide constructive existence for every prime $P \equiv 1 \pmod 5$ without recourse to factorization. Examples for $P = 73$ and $P = 97$ demonstrate practical assembly of rows in this canonical form.

9 Connection ED2 $\leftrightarrow$ ED1: convolution and anticonvolution

The mechanism of transition between the parametrizations ED2 and ED1 plays a key role in the completeness of the algorithm. If (δ, b, c) is an admissible ED2-triplet, then by setting

$$\gamma = \frac{5c - 1}{P}, \quad u = \gamma A - c, \quad v = \gamma B - c,$$

one can obtain an admissible ED1-quadruple (γ, c, u, v). This transition is called the *convolution* ED2 $\to$ ED1.

The reverse transition (anticonvolution) ED1 $\to$ ED2 is not one-to-one: several distinct ED1-quadruples may map to the same ED2-triplet. This effect of *power compression* simplifies the proof of existence, eliminating multiplicity of solutions associated with the choice of divisors.

A detailed analysis of the convolution and anticonvolution mechanism for the case $k = 4$ is given in the work on the Erdős–Straus conjecture [2]; here we transfer the same construction to coefficient 5.

10 Key points closing the claim about factorization

What is used in the current methods

- Integer arithmetic and gcd operations; - Checks modulo prime P and the corresponding symbols $\binom{a}{P}$ and $\binom{a}{\gamma}$ — without requiring factorization of moduli; - Parity comparisons, conditions $u \equiv v \pmod 2$, $\gcd(u, v) = 1$, equality $uv = c^2$.

What is not used

- Factorization of the numbers C, γ, or intermediate quantities; - Root finding modulo composite numbers; - Factorization for testing squareness: the fact $uv = c^2$ is guaranteed by normalization.

We rely on: - **Sum and discriminant** - **Back-test** - **Quadratic reparametrization**

Correctness via minimal lemmas

We rely on: - **Sum and discriminant - Back-test - Quadratic reparametrization**

Proposition 10.1 (Current methodology does not rely on factorization)**.** *The applied methods, forming and checking pairs (u, v) for fixed prime P, use only: (i) integer operations and* gcd*; (ii) checks modulo P and symbols $\left(\frac{\cdot}{P}\right)$ / $\left(\frac{\cdot}{\gamma}\right)$; (iii) linear formulas reconstructing A, B and establishing $C = cP$ from $uv = c^2$.*

At no stage is factorization required.

- Establishes the link with (u, v);
- Ensures sufficiency of local conditions;
- $C = cP$ follows from $uv = c^2$.

  All checks reduce to arithmetic, gcd, and Legendre/Jacobi symbols.

Remark 10.2 (Optional accelerations). Sieving by small primes is allowed as a method of acceleration, but it is not necessary for correctness of the current methods and is not used in Theorem 10.1

11 Algorithms: lattice boxes and enumeration

- Enumeration of δ within reasonable bounds; factorization of $N = 5P\delta + 1$ and pairs $rs = N$ with $r \equiv s \equiv 4 \pmod 5$; reconstruction of b, c, filter $\delta \mid bc$; check of ordering and (3.1). - For ED1 — enumeration of divisors $u \mid c^2$ in congruent classes modulo γ and exclusion of multiples modulo P.

12 Integration of pre-sieving by progressions into the ED2 algorithm

12.1 Idea

For fixed δ and a set of small moduli $r \equiv 4 \pmod 5$ (with $\gcd(r, 5\delta) = 1$), the progressions

$$P \equiv 1 \pmod 5, \qquad P \equiv -(5\delta)^{-1} \pmod r$$

give "thin" classes for enumerating primes P. By Theorems B.1 and B.4 their density is controllable, and the average number of such progressions per P grows (see (B.1)). This allows replacing brute-force enumeration of P with scanning already prepared AP, saving time.

Listing 1: ED2 algorithm with finite parameter set $\mathcal{F}$

```
# Input: prime P = 5*P'+1 ; delta; finite set S from (alpha, d')
# Core identity: (5*b - 1)*(5*c - 1) = 5*P*delta + 1

def case_A(P, delta, S):
    N = 5 * P * delta + 1
    for r in S:
        if N % r != 0:
            continue
        s = N // r
        if s % 5 != 4:
            continue
        b = (r + 1) // 5
```

```
        c = (s + 1) // 5
        if (b * c) % delta != 0:
            continue
        A = (b * c) // delta
        if not (A <= b * P < c * P):
            b, c = c, b
        B = b * P
        C = c * P
        return (A, B, C)
    return None
```

Comment on the algorithm. The algorithm `case_A` implements enumeration over the set S, constructed from parameters (α, d'). The filter $s \equiv 4 \pmod 5$ reflects the structure of the ED2 parametrization and excludes unsuitable residue classes. For each fixed prime P the algorithm produces a solution if it exists within S. Polylogarithmic complexity is justified via density theorems, while a strict guarantee for all P remains conditional.

12.2 Complexity

- For fixed P: enumeration of $r \le R$ requires $O(R)$ divisibility checks; small R (polylogarithmic in P) is usually sufficient. - For searching $P \le X$: the cost of sieving by the union of AP is of order $X \sum_{r \le R} 1/\varphi(5r) \asymp X \log R$ at the elementary level; the number of candidate primes found agrees with Theorem B.4. - Practically: one chooses $R = (\log X)^B$ and small δ (including $\delta = 1$), which yields near-linear time in X with a weak logarithmic factor.

13 Experiments for Sierpiński

13.1 General overview

The study of solutions of the equation $5/P = 1/A + 1/B + 1/C$ in the Sierpiński class focuses on finding values satisfying given criteria. Experiments were conducted for primes $P \equiv 1 \pmod 5$. For each P the values b, c, A, B, and C were found. Solutions are presented in Table 3.

Table 3: Results for $P = 31, 41, 2521$ with verification by the lemma $X \cdot Y = 5\alpha P(d')^2 + 1$

#	α	b'	c'	g	b	c	δ	X	Y	N	A	B	C	d'	OK
$P = 31$															
1	1	1	8	1	1	8	1	4	39	156	8	31	248	1	✓
2	1	1	7	2	2	14	4	9	69	621	7	62	434	2	✓
$P = 41$															
1	3	1	3	3	3	9	9	14	44	616	616	123	369	1	✓
$P = 2521$															
1	5	193	2	10	1930	20	49	9649	99	955251	788	486	50420	7	✓
2	9	183	11	25	4575	275	50	22874	1374	31413876	251	277310	289915	5	✓
3	3	2	87	3	6	261	3	29	1304	37816	522	15126	657981	1	✓
4	3	2	85	9	18	765	27	89	3824	340336	510	45378	1928565	3	✓
5	15	39	1	13	39	39	507	194	2534	491596	507	98319	1278147	13	✓

13.2 Implementation notes

- For several δ, combine lists of classes via CRT, ensuring mutual independence of moduli. - The check $s \equiv 4 \pmod 5$ and integrity of b, c, A are constant filters. - Ordering $B \le C$ is achieved by permuting $r \leftrightarrow s$. - The "anticonvolution" block ED1 $\to$ ED2 is applicable in the reverse direction

Table 4: Solutions for $P = 3511$ with $\alpha = 1$, $d' = 1$ verified

#	α	b_1	c_1	g	b	c	δ	X	Y	N	A	B	C	Check
1	1	1	878	1	1	878	1	4	4389	17556	878	3511	3082658	OK
2	1	3	251	1	3	251	1	14	1254	17556	753	10533	881261	OK
3	1	4	185	1	4	185	1	19	924	17556	740	14044	649535	OK
4	1	9	80	1	9	80	1	44	399	17556	720	31599	280880	OK
5	1	17	42	1	17	42	1	84	209	17556	714	59687	147462	OK
6	1	23	31	1	23	31	1	114	154	17556	713	80753	108841	OK

if ED1-data with $P \mid (v + c)$ is already available (see 9.12 in the work on the Erdős–Straus conjecture [2]).

14 Convergence and lattice density

Theorem 14.1. *Let $\Lambda \subset \mathbb{Z}^k$ be a sublattice of index M, independent of P. For the box $\mathcal{B}_k(T) = \{1 \le u_i \le T\}$ and the class $u_0(P) + \Lambda$ we have*

$$|\{u \in \mathcal{B}_k(T) : u \equiv u_0(P) \pmod{\Lambda}\}| = \frac{T^k}{M} + O_k(T^{k-1}),$$

in particular, for $T = (\log P)^A$ — logarithmic growth of cardinality.

Theorem 14.2 (average-case complexity)**.** *For most primes $P \equiv 1 \pmod 5$ the enumeration algorithm finds a solution in $O((\log P)^A)$ steps. The proof relies on the independence of the lattice index from P and on density estimates (Appendices A, B). In the worst-case regime a strict guarantee remains open.*

15 Conclusion

The combined use of the geometric construction (*diagonal layer hitting the window*; see Proposition 9.25 in the work on the Erdős–Straus conjecture [2]) and the algebraic ED2 model (Appendix B), as well as its geometric deepening in Appendix D in the work on the Erdős–Straus conjecture [2], leads to the following conclusions.

- **General case.** For an infinite set of primes P, a constructive proof of the existence of solutions has not been obtained in the present work. Sections of Appendix D, which use Dirichlet's theorem and the mechanism of finite coverings, formulate conditional results depending on the validity of the hypothesis of finite covering of parameters.
- **Particular case.** For each fixed odd prime P, the existence of a solution is strictly proven. The algebraic and geometric conditions are consistent: by Lemma D.33 we have $S = u$, $\Delta = v^2$, and Proposition 9.25 guarantees that the diagonal layer hits the target window (see also Theorem 9.21 in the work on the Erdős–Straus conjecture [2]).

Acknowledgments

Software tools with elements of artificial intelligence were used for refining formulations, technical proofreading, and generating illustrative Python examples.

Funding Statement

No funding was received.

Conflict of Interest

We have no conflicts of interest to disclose.

References

[1] E. Bombieri. On the large sieve. *Mathematika*, 12(2):201–225, 1965.

[2] E. Dyachenko. Constructive proofs of the Erdős–Straus conjecture for prime numbers with $p \equiv 1 \pmod 4$, 2025. Preprint on arXiv.

[3] P. Erdős. Az $x_1^{-1} + x_2^{-1} + \ldots + x_n^{-1} = b$ egyenlet egész számú megoldásairól. *Matematikai Lapok*, 1:192–210, 1950.

[4] P. X. Gallagher. The large sieve. *Mathematika*, 14(1):14–20, 1967.

[5] H. W. Lenstra and P. Stevenhagen. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[6] Y. V. Linnik. The large sieve. *Doklady Akademii Nauk SSSR*, 30:292–294, 1941.

[7] Philemon Urbain Mballa. Partial resolution of the Erdős–Straus, Sierpiński, and generalized erdős–straus conjectures using new analytical formulas, 2025. Preprint on arXiv.

[8] A. Schinzel. Sur quelques propriétés des nombres n^3 et n^4, où n est un nombre impair. *Mathesis*, 65:219–222, 1956.

[9] W. Sierpinski. Sur les décompositions de nombres rationnels en fractions primaires. *Mathesis*, 65:16–32, 1956.

[10] N. Tschebotareff. Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, 1926.

[11] A. I. Vinogradov. The density hypothesis for dirichlet l-series. *Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya*, 29(4):903–934, 1965.

A Analytic tools

Theorem A.1 (Bombieri–Vinogradov)**.** *For any $A > 0$ there exists $x_0(A)$ such that uniformly for $Q \le x^{1/2}/(\log x)^{C(A)}$, $x \ge x_0$,*

$$\sum_{q \le Q} \max_{(a,q)=1} \left| \pi(x; q, a) - \frac{\mathrm{Li}(x)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

Theorem A.2 (Greaves, larger sieve)**.** *If $A \subset \{1, \ldots, N\}$ excludes a positive proportion of residue classes for many primes $p \le B$, then*

$$|A| \ll N \exp\Big(-c \frac{\log B}{\log\log B}\Big),$$

where $c > 0$ is an absolute constant.

Theorem A.3 (Chebotarev)**.** *Let L/K be a finite normal extension of number fields with Galois group G, $C \subset G$ a conjugacy class. Then*

$$\pi_C(x) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\Big(x e^{-c\sqrt{\log x}}\Big),$$

where $c > 0$ depends only on L/K.

B Local applications

From Theorem A.1 follows the standard average asymptotic for the number of primes in the intersection of two progressions. In our context the modulus and class are given by the conditions

$$P \equiv 1 \pmod 5, \qquad P \equiv -(5\delta)^{-1} \pmod r, \qquad r \equiv 4 \pmod 5,\ \gcd(r, 5\delta) = 1,$$

which arise from the identity $(5b-1)(5c-1) = 5P\delta + 1$ in the case ED2 and the factorization $rs = 5P\delta + 1$.

Proposition B.1 (BV for progressions with fixed δ and r)**.** *Let $\delta \in \mathbb{N}$ be fixed, $r \equiv 4 \pmod 5$, $\gcd(r, 5\delta) = 1$. Then the number of primes $P \le x$ in the class*

$$P \equiv 1 \pmod 5, \qquad P \equiv -(5\delta)^{-1} \pmod r$$

satisfies

$$\#\{P \le x : P \equiv 1\ (5),\ P \equiv -(5\delta)^{-1}\ (r)\} \;=\; \frac{\mathrm{Li}(x)}{\varphi(5r)} \;+\; O\!\left(\frac{x}{(\log x)^A}\right)$$

uniformly for all $r \le x^{1/2}/(\log x)^{C(A)}$.

Idea of proof. Apply Theorem A.1 with modulus $q = 5r$. Compatibility of classes via CRT is ensured since $\gcd(5, r) = 1$. Uniformity for $q \le x^{1/2}/(\log x)^C$ gives the stated estimate. □

Lemma B.2 (CRT correctness and residue $s \equiv 4 \pmod 5$)**.** *Let $r \equiv 4 \pmod 5$, $\gcd(r, 5\delta) = 1$, and $P \equiv 1 \pmod 5$, $P \equiv -(5\delta)^{-1} \pmod r$. Then*

$$s \;:=\; \frac{5P\delta + 1}{r} \;\in \mathbb{N}, \qquad s \equiv 4 \pmod 5.$$

Proof. By the second condition $r \mid (5P\delta + 1)$, hence $s \in \mathbb{N}$. Modulo 5: $5P\delta + 1 \equiv 1$, and $r \equiv 4$ is invertible, with $r^{-1} \equiv 4 \pmod 5$. Thus $s \equiv 1 \cdot r^{-1} \equiv 4 \pmod 5$. □

Corollary B.3 ($\delta = 1$: infinitely many P)**.** *Let $\delta = 1$ and fix $r \equiv 4 \pmod 5$. Then there exist infinitely many primes $P \equiv 1 \pmod 5$ with $r \mid (5P + 1)$. For each such P we have*

$$b = \frac{r+1}{5}, \qquad s = \frac{5P+1}{r} \equiv 4 \pmod 5, \qquad c = \frac{s+1}{5}, \qquad A = bc$$

yielding an ED2 *solution with $\delta = 1$.*

Proof. There is exactly one class modulo $5r$, given by the system $P \equiv 1 \pmod 5$, $P \equiv -5^{-1} \pmod r$ (CRT). By Dirichlet's theorem there are infinitely many primes in it; the quantitative form follows from Theorem B.1. The statement about s follows from Theorem B.2. □

Proposition B.4 (Counting over r and total asymptotic)**.** *Let $R \le x^{1/2}/(\log x)^C$. Then*

$$\sum_{\substack{r \le R \\ r \equiv 4\ (5) \\ \gcd(r, 5\delta) = 1}} \#\{P \le x : P \equiv 1\ (5),\ P \equiv -(5\delta)^{-1}\ (r)\} \;=\; \mathrm{Li}(x) \sum_{\substack{r \le R \\ r \equiv 4\ (5) \\ \gcd(r, 5\delta) = 1}} \frac{1}{\varphi(5r)} \;+\; O\!\left(\frac{x\,R}{(\log x)^A}\right).$$

Moreover,

$$\sum_{\substack{r \le R \\ r \equiv 4\ (5) \\ \gcd(r, 5\delta) = 1}} \frac{1}{\varphi(5r)} \;=\; C_{5,\delta}\,\log R \;+\; O(1),$$

where $C_{5,\delta} > 0$ is a constant depending only on the class modulo 5 and the divisors of δ.

Comment. Summation of the main term follows from Theorem B.1 and linearity; summation of error terms gives the stated remainder. The estimate of $\sum 1/\varphi(5r)$ is standard: $\varphi(5r) = 4\varphi(r)$ when $\gcd(r,5) = 1$, and $\sum_{n\le R,\,(n,m)=1} 1/\varphi(n) = c(m)\log R + O(1)$. □

Proposition B.5 (Exceptional set via the larger sieve)**.** *Let $R \le x^{1/2}/(\log x)^C$. Then the number of $r \le R$, $r \equiv 4 \pmod 5$, $\gcd(r, 5\delta) = 1$, for which the progression*

$$P \equiv 1 \pmod 5, \qquad P \equiv -(5\delta)^{-1} \pmod r$$

contains no primes $P \le x$, satisfies

$$\ll R \exp\Big(-c\,\frac{\log R}{\log\log R}\Big),$$

where $c > 0$ is an absolute constant (follows from Theorem A.2).

Remark B.6 (Chebotarev: additional local filters). If necessary, one can simultaneously impose splitting conditions for r and/or $s = (5P\delta + 1)/r$ in a fixed extension of number fields; by Theorem A.3 the corresponding classes have positive natural density, and intersection with the specified AP retains positive density.

How to use in the algorithm. - Preselection of r: fix several small $r \equiv 4 \pmod 5$ (or enumerate $r \le R$ in the BV range). - Pre-sieving by progressions: for each r precompute the class $P \equiv -(5\delta)^{-1} \pmod r$ and combine with $P \equiv 1 \pmod 5$ (CRT). - Enumeration of P: scan primes P in the combined classes; by Theorem B.1 the expected frequency is $\asymp 1/\varphi(5r)$. - Verification of ED2: for a found P compute $s = (5P\delta + 1)/r$, check $s \equiv 4 \pmod 5$, and reconstruct $b = (r + 1)/5$, $c = (s + 1)/5$, $A = bc/\delta$. - Balancing: choosing $R \le x^{1/2}/(\log x)^C$ gives an optimal compromise between the number of progressions and control of errors (BV), while Theorem B.5 guarantees the smallness of the exceptional set of r.

Double summation: average over primes P

Define for fixed δ and $R \ge 2$ the quantity

$$N(P; R, \delta) \;=\; \#\Big\{\, r \le R :\; r \equiv 4 \pmod 5,\; \gcd(r, 5\delta) = 1,\; r \mid (5P\delta + 1) \,\Big\}.$$

This is the number of "local" parameters r for a given prime P. Then for $R \le x^{1/2}/(\log x)^C$ we have the average asymptotic

$$\frac{1}{\#\{P \le x :\; P \equiv 1 \pmod 5\}} \sum_{\substack{P\le x\\ P\equiv 1\ (5)}} N(P; R, \delta) \;=\; C_{5,\delta}\,\log R \;+\; O(1), \tag{B.1}$$

where $C_{5,\delta} > 0$ is a constant depending only on δ and classes modulo 5.

Idea of proof. Change the order of summation:

$$\sum_{\substack{P\le x\\ P\equiv 1\ (5)}} N(P; R, \delta) = \sum_{\substack{r\le R\\ r\equiv 4\ (5)\\ \gcd(r,5\delta)=1}} \#\{P \le x :\; P \equiv 1\ (5),\; P \equiv -(5\delta)^{-1}\ (r)\}.$$

For each r apply Theorem B.1 (modulus $5r$) and sum the main terms:

$$\sum_r \frac{\mathrm{Li}(x)}{\varphi(5r)} \;=\; \mathrm{Li}(x) \sum_{\substack{r\le R\\ r\equiv 4\ (5)\\ \gcd(r,5\delta)=1}} \frac{1}{\varphi(5r)} \;=\; \mathrm{Li}(x)\big(C_{5,\delta}\log R + O(1)\big),$$

and the total error is controlled linearly in r using Theorem B.1. Division by the number of primes $P \le x$, $P \equiv 1\ (5)$, gives (B.1). □

Corollary B.7 (Average supply of local parameters)**.** *For $R = (\log x)^B$ with fixed $B > 0$, the average value of $N(P; R, \delta)$ over primes $P \le x$, $P \equiv 1 \pmod 5$, grows as $C_{5,\delta}\, B \log\log x + O(1)$. In particular, the average number of admissible r tends to infinity.*

Remark B.8 (On estimates of "most P"). The transition from the average to a statement of the form "for most P there exists at least one $r \le R$" can be obtained by second moment methods or via the larger sieve (Theorem B.5) with a coordinated choice of R and x. These details are not required for the constructive part of the algorithm, but they explain its good average behavior.