Pattern formation Statistics on Fermat Quotients

Cristian Cobeli[1*†], Alexandru Zaharescu[1,2†] and Zhuo Zhang[2†]

[1] "Simion Stoilow", Institute of Mathematics of the Romanian Academy, 21 Calea Griviţei Street, P. O. Box 1-764, Bucharest, 014700, Romania.
[2] Department of Mathematics, University of Illinois at Urbana-Champaign, Altgeld Hall, 1409 W. Green Street, Urbana, 61801, IL, USA.

*Corresponding author(s). E-mail(s): cristian.cobeli@imar.ro;
Contributing authors: zaharesc@illinois.edu; zhuoz4@illinois.edu;
†These authors contributed equally to this work.

Abstract

For a prime p and integers $0 \le b \le p^2 - 1$ for which $\gcd(b,p) = 1$, the Fermat quotients modulo p are defined by $\mathtt{q}_p(b) := \frac{b^{p-1}-1}{p} \pmod p$ and can be arranged in a $p \times (p-1)$ matrix $\mathtt{FQM}(p)$. Despite their simple definition, Fermat quotients are well known for their lack of regularity. Here, we continue to argue about this contrasting effect by showing that, on one hand, a row of the Fermat quotient matrix behaves like a randomly selected sequence of numbers, and on the other hand, the spatial statistics of distances on regular N-patterns confirm the natural expectations.

Keywords: Fermat quotients, Fermat quotient matrix, pattern formation, multi-dimensional correlation size test, Wieferich primes

MSC Classification: Primary 11B99; Secondary 11A07

1 Introduction

The widely known arithmetical fact brought out in front by Fermat's little theorem has in the background a deep wealth of arithmetic, algebraic, geometric, or analytic phenomena. A particular branch of this subject, which has been recently extensively studied, develops the theory of δ_p-differentiation and uses it, among other things, to bound the number of rational points on curves (see Joyal [1], Buium [2], Jeffries [3] and the references therein).

For the first time, the *Fermat quotients* defined as the ratios $Q_p(n) = (n^{p-1}-1)/p$, which are integers, proved to be important for recognizing the role of the prime numbers for which $(n^{p-1}-1)/p$ is again divisible by p in the study of Fermat's Last Theorem (see Mirimanoff [4, 5], Lerch [6], Wieferich [7], Shanks and Williams [8], Suzuki [9]). Fermat quotients have been studied over the years for their remarkable arithmetic and algebraic properties (see Eisenstein [10], Johnson [11, 12], Ernvall and Metsänkylä [13], Sauerberg and Shu [14], Agoh [15]), particularly for their relevance to number-theoretic problems (see Shparlinski [16–19] and Alexandru et al. [20]) and their association to pseudo-random number generators, primes factorization and cryptographic algorithms (see Lehmer [21], Lenstra [22], Ostafe and Shparlinski [23], Shparlinski [24], Chang [25], Chen and Winterhof [26]).

Working with the standard representatives modulo p from $\{0, 1, \ldots, p-1\}$, the Fermat quotients $Q_p(n) \pmod p$ of *base* n and *exponent* p, for $1 \le n < p^2$ and $p \nmid n$, denoted

$$\mathfrak{q}_p(b) := \frac{b^{p-1}-1}{p} \pmod p, \text{ for } 1 \le b \le p^2-1 \text{ and } \gcd(b,p) = 1, \tag{1}$$

are arranged in order in the $\mathtt{FQM}(p)$ matrix, $p-1$ per line, for a total of p successive lines (see [13, 27] and an example in Table 1).

Although the elements of $\mathtt{FQM}(p)$ are not independent from each other (in Proposition 3 there are stated some relations between them), numerical calculations indicate that there is still a pronounced aspect of pseudo-randomness in the Fermat quotient matrix. In this article our main goal is to substantiate this observation, generalizing a result [27, Theorem 3] according to which, beyond the inherent symmetries, if p is sufficiently large, two elements of the matrix, regardless of their position, are not found in any particular relationship in terms of size.

But first we will prove a common but somewhat peculiar characteristic of the Fermat quotient matrix. We call a *Fermat quotient point* the first line of $\mathtt{FQM}(p)$. Then the next theorem shows that the average distance of the Fermat quotient point to a straight line is, in the limit, equal to $1/3$. Note that in the mod p modular context, straight lines are composed of equally spaced parallel segments, and their number increases as the slope of the line increases (see Figure 1 for some typical examples of such lines).

Theorem 1. *Let $\{C_p\}_{p\in\mathcal{P}}$ and $\{D_p\}_{p\in\mathcal{P}}$ be two sequences of integers indexed by prime numbers. Suppose $C_p \neq 0$ and $C_p = o(p^{1/12}\log^{-2/3} p)$ as p tends to infinity. Then*

$$\frac{1}{p}\sum_{b=1}^{p-1}\left|\frac{\mathfrak{q}_p(b)}{p} - \left\{C_p\frac{b}{p} + D_p\right\}\right| = \frac{1}{3} + O\Big(C_p^{3/5}p^{-1/20}\log^{2/5} p\Big). \tag{2}$$

In the Theorem 1, we allowed the slopes of the lines to change as p increases, with the result remaining valid even when the slopes increase together with the number of the segments that compose the lines.

The common version, with the distance between the Fermat quotient point and any fixed line, is the object of the following corollary.

Corollary 1. *Let $C \neq 0$ and D be fixed. Then,*

$$\sum_{b=1}^{p-1} \Big| \frac{\mathfrak{q}_p(b)}{p} - \Big\{ C\frac{b}{p} + D \Big\} \Big| = \frac{p}{3} + O_C\Big(p^{19/20} \log^{2/5} p\Big) .$$

Our second subject refers to the entire $\mathtt{FQM}(p)$ matrix, with our objective being the comparison of the sizes of Fermat quotients in specific pre-established geometric positions. In order to use the common notation for the entries in the matrix, we denote the elements of $\mathtt{FQM}(p)$ by $A_{a,b}$, where $0 \leq a \leq p-1$ and $1 \leq b \leq p-1$, so that

$$A_{a,b} := \mathfrak{q}_p(ap+b).$$

Next, let $N \geq 1$ and consider as fixed N two-dimensional vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N \in \mathbb{Z}^2$, whose components will be denoted by $\boldsymbol{v}_j = (s_j, t_j)$. In the following, we will assume that all integers t_j are distinct pairwise, because otherwise, the specific mutual relations among the vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N$ make the general result we will prove to no longer be valid.

We will use the set of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N \in \mathbb{Z}^2$ as a spanning pattern that we apply across $\mathtt{FQM}(p)$ to compare among each other the size of Fermat quotients. Let $\mathcal{V} \in (\mathbb{Z}^2)^N$ denote the ordered set of the vectors that defines the pattern.

If p becomes sufficiently large, applying the $\mathcal{V}$-span to the elements of $\mathtt{FQM}(p)$ most of the time we will remain in the matrix, since $\mathcal{V}$ is fixed. The only elements that are moved outside of $\mathtt{FQM}(p)$ by $\mathcal{V}$ are near the border, and their total number is at most $O(p)$. In the following we denote by $\mathcal{G}_N(p) \subset \mathbb{Z}^2$ the set of places that are kept inside while translated by $\mathcal{V}$, that is,

$$\mathcal{G}_N(p) := \bigcap_{j=1}^{N} \Big\{ (a,b) \in [0,p-1] \times [1,p-1] : 0 \leq a+s_j \leq p-1,\ 1 \leq b+t_j \leq p-1 \Big\} . \quad (3)$$

Let us note that the collection of pairs of indices from $\mathcal{G}_N(p)$ cut out from $\mathtt{FQM}(p)$ parts that together are close to a square table of

$$\#\mathcal{G}_N(p) = p^2 + O_M(p) \quad (4)$$

points, where $M = \max\limits_{1 \leq j \leq N} \|\boldsymbol{v}_j\|_\infty$.

Finally, for each $(a,b) \in \mathcal{G}_N(p)$, consider the normalized $\mathcal{V}$-spanned vectors of Fermat quotients mod p defined by

$$\boldsymbol{x}_{a,b}(p) := \frac{1}{p}\big(A_{(a,b)+\boldsymbol{v}_1}, \ldots, A_{(a,b)+\boldsymbol{v}_N}\big) \in [0,1]^N . \quad (5)$$

We will show that if p is sufficiently large, then the set

$$\mathcal{X}(p) := \{\boldsymbol{x}_{a,b}(p) : (a,b) \in \mathcal{G}(p)\} \subset [0,1]^N \tag{6}$$

is uniformly distributed.

For any permutation $\sigma \in S_N$, we denote by $T(\sigma, N)$ the N-dimensional *polyhedron* whose coordinates permuted by σ are ordered increasingly, that is,

$$T(\sigma, N) := \{\boldsymbol{x} \in [0,1]^N : \boldsymbol{x} = (x_1, \dots, x_N),\ x_{\sigma(1)} < x_{\sigma(2)} < \cdots < x_{\sigma(N)}\}. \tag{7}$$

Next, by employing $T(\sigma, N)$ and the uniform distribution of $\mathcal{X}(p)$, we can precisely estimate the size of clusters for all possible order relations among the elements of $\mathtt{FQM}(p)$.

Theorem 2. *Let $N \geq 1$ and let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_N \in \mathbb{Z}^2$ be fixed and having the property that their second components are different from each other. Suppose p is prime and $\mathcal{G}_N(p)$, $\boldsymbol{x}_{a,b}(p)$ are defined by* (3) *and* (5)*. Then, for any permutation $\sigma \in S_N$, we have*

$$\#\{(a,b) \in \mathcal{G}_N(p) : \boldsymbol{x}_{a,b}(p) \in T(\sigma, N)\} = \frac{p^2}{N!} + O_{M,N}\left(p^{(2N+1)/(N+1)} \log^{N/(N+1)} p\right), \tag{8}$$

where $M := \max_{1 \leq j \leq N} \|\boldsymbol{v}_j\|_\infty$.

We remark that the size of the main term in (5) is proportional to the volume of the N-dimensional polyhedron set put in Lemma 2.4.

Theorem 2 generalizes the specific case of the pairs [27], where the number of two generic elements in the matrix $\mathtt{FQM}(p)$ that are relative to each other in a certain a priori fixed geometric position. Thus, if $N = 2$, the results proves that in roughly half of the cases, one element is larger than the other, and vice versa.

Corollary 2 ([27, Theorem 3])**.** *Let s, t be integers not both equal to zero and let*

$$\mathcal{G}(p) = \{(a,b) \in [0,p) \times [1,p) : 0 \leq a + s < p,\ 1 \leq b + t < p\} \cap \mathbb{Z}^2.$$

Then,

$$\#\{(a,b) \in \mathcal{G}(p) : \mathfrak{q}_{a,b} \lesseqgtr \mathfrak{q}_{a+s,b+t}\} = \frac{p^2}{2} + O_{|s|,|t|}\left(p^{5/3} \log^{2/3} p\right),$$

where $\lesseqgtr$ stands for either $\leq$ or $\geq$.

The condition in Theorem 2 that all the second components of $\boldsymbol{v}_j$'s must be distinct is necessary and guarantees the validity of the result for nearly all possible displacement vectors, when M becomes sufficiently large. We remark that even though the result may still hold true even if some of the second components of the displacement vectors are equal to some other, the regime changes in these cases. Indeed, if fewer and fewer second components are distinct, regardless of the validity of the theorem's result, the set of pairs whose cardinality is estimated by (8) becomes more and more regular, while the set of vectors $\mathcal{X}(p) \cap T(\sigma, N)$ may no longer be equidistributed in the cube $[0,1]^N$. In the Addenda, we show in Figures 2–4 the graphical representations of several such typical situations.

Table 1: The Fermat quotient matrix FQM(11) with entries $\mathfrak{q}_{11}(n) = \frac{n^{10}-1}{11} \pmod{11}$.

b	1	2	3	4	5	6	7	8	9	10
b^{-1}	1	6	4	3	9	2	8	7	5	10
$\mathfrak{q}_p(b)$	0	5	0	10	7	5	2	4	0	1
$\mathfrak{q}_p(p+b)$	10	10	7	7	9	3	5	8	6	2
$\mathfrak{q}_p(2p+b)$	9	4	3	4	0	1	8	1	1	3
$\mathfrak{q}_p(3p+b)$	8	9	10	1	2	10	0	5	7	4
$\mathfrak{q}_p(4p+b)$	7	3	6	9	4	8	3	9	2	5
$\mathfrak{q}_p(5p+b)$	6	8	2	6	6	6	6	2	8	6
$\mathfrak{q}_p(6p+b)$	5	2	9	3	8	4	9	6	3	7
$\mathfrak{q}_p(7p+b)$	4	7	5	0	10	2	1	10	9	8
$\mathfrak{q}_p(8p+b)$	3	1	1	8	1	0	4	3	4	9
$\mathfrak{q}_p(9p+b)$	2	6	8	5	3	9	7	7	10	10
$\mathfrak{q}_p(10p+b)$	1	0	4	2	5	7	10	0	5	0

2 Preparatory Lemmas

The elements of the Fermat quotient matrix are related to each other through various basic relations, including some that are indicated in the next proposition (see also [13]).

Proposition 3. *Let $A_{a,b}$ be the elements of* FQM(p)*, for $0 \le a < p$ and $1 \le b < p$. Then, with any indices and entries taken modulo p, we have*

1. $A_{a,b} = \mathfrak{q}_p(ap+b)$;
2. $A_{a,b} = A_{p-1-a,p-b}$;
3. $A_{a,b} = \mathfrak{q}_p(b) - ab^{-1}$;
4. $A_{a+s,b} = A_{a,b} - sb^{-1}$;
5. $e_p\big(A_{a,b_1b_2}\big) = e_p\big(A_{a,b_1}\big)e_p\big(A_{a,b_1}\big)e_p\big(a(b_1+b_2-1)b_1^{-1}b_2^{-1}\big)$, *where* $e_p(x) := e^{\frac{2\pi i x}{p}}$.

Proof. Part (1) is listed as the definition and the others are straightforward calculations using $(ap+b)^{p-1} \equiv b^{p-1} \pmod{p^2}$, and the translation of the notation $\mathfrak{q}_p(n) = \dfrac{n^{p-1}-1}{p} \pmod{p}$, which particularly implies

$$\mathfrak{q}(ap+b) \equiv \mathfrak{q}_p(b) = ab^{-1} \pmod{p}.$$

Also, note that $A_{a+s,b}$ is equal to

$$\begin{aligned}\mathfrak{q}_p\big((a+s)p+b\big) &= \frac{\big((a+s)p+b\big)^{p-1}-1}{p} \pmod{p} \\ &= \frac{(p-1)(a+s)pb^{p-2}+b^{p-1}-1}{p} \pmod{p},\end{aligned}$$

which further leads to

$$A_{a+s,b} = -(a+s)b^{-1} + \frac{b^{p-1}-1}{p} \pmod p = -(a+s)b^{-1} + \mathfrak{q}_p(b).$$

The proof of part (5) yields as follows. Using part (3), we have:

$$e_p\big(A_{a,b_1b_2}\big) = e_p\big(\mathfrak{q}_p(b_1b_2) - ab_1^{-1}b_2^{-1}\big) = e_p\big(\mathfrak{q}_p(b_1)\big)e_p\big(\mathfrak{q}_p(b_2)\big)e_p\big(-ab_1^{-1}b_2^{-1}\big), \tag{9}$$

because $\mathfrak{q}_p(b_1b_2) = \mathfrak{q}_p(b_1)b_2^{p-1} + \mathfrak{q}_p(b_2)$, which implies, $\mathfrak{q}_p(b_1b_2) \equiv \mathfrak{q}_p(b_1) + \mathfrak{q}_p(b_2) \pmod p$ for $\gcd(b_1b_2, p) = 1$. Then, the sequence of equalities in (9) is further continued by

$$\begin{aligned} e_p\big(A_{a,b_1b_2}\big) &= e_p\big(\mathfrak{q}_p(b_1) - ab_1^{-1}\big)e_p\big(\mathfrak{q}_p(b_2) - ab_2^{-1}\big)e_p\big(ab_1^{-1} + ab_2^{-1} - ab_1^{-1}b_2^{-1}\big) \\ &= e_p\big(A_{a,b_1}\big)e_p\big(A_{a,b_2}\big)e_p\big(a(b_1+b_2-1)b_1^{-1}b_2^{-1}\big). \end{aligned}$$

□

Let us remark that parts (3) and (4) of Proposition 3 unfolds a link between the Fermat quotient point and the other entries in the matrix $\mathtt{FQM}(p)$, indicating that the elements of the Fermat quotient matrix might share similarities with the type of distribution and the expected spread of geometric patterns of the inverses modulo p (see [28–30]).

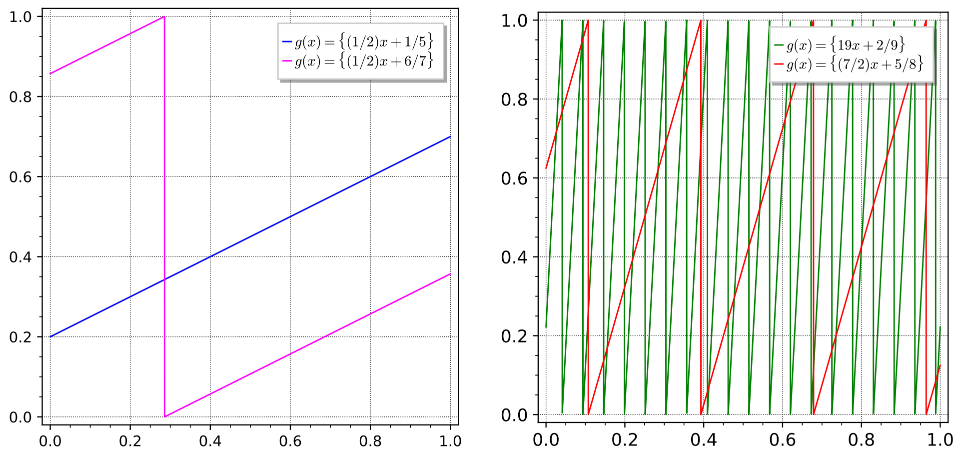

Fig. 1: The graphs of four straight lines mod 1 with four different slopes and y-intercepts.

Lemma 2.1. *Let $C, D > 0$ be real numbers and let $g(x) := \{Cx + D\}$. Then*

$$I(g) := \int_0^1 \int_0^1 |y - g(x)| \,\mathrm{d}x \,\mathrm{d}y = \frac{1}{3}\,.$$

Proof. Note that since $0 \le g(x) < 1$, we have

$$\begin{aligned}\int_0^1 |y - g(x)| \,\mathrm{d}y &= \int_0^{g(x)} (g(x) - y) \,\mathrm{d}y + \int_{g(x)}^1 (y - g(x)) \,\mathrm{d}y \\ &= \big(g(x)\big)^2 - \frac{y^2}{2}\bigg|_0^{g(x)} + \frac{y^2}{2}\bigg|_{g(x)}^1 - g(x)\big(1 - g(x)\big)\,,\end{aligned}$$

and, as a result,

$$I(g) = \int_0^1 \left(\big(g(x)\big)^2 - g(x) + \frac{1}{2}\right) \mathrm{d}x. \tag{10}$$

Remark 1. *We can simplify the calculation of the integral noticing that the function $x \mapsto \{Cx + D\}$ is periodic of period $1/C$. Indeed, we have*

$$\left\{C\Big(x + \frac{1}{C}\Big) + D\right\} = \big\{Cx + 1 + D\big\} = \{Cx + D\}\,.$$

Next, one checks that if $x \in [0, 1/C)$, then

$$\{Cx + D\} = \begin{cases} Cx + D & \text{if } 0 \le x \le \dfrac{1-D}{C}, \\ Cx + D - 1 & \text{if } \dfrac{1-D}{C} \le x \le \dfrac{1}{C}. \end{cases} \tag{11}$$

Then, on combining (10) and (11), we have

$$\begin{aligned} I(g) &= C \int_0^{1/C} \left(\{Cx + D\}^2 - \{Cx + D\} + \frac{1}{2}\right) \mathrm{d}x \\ &= C \int_0^{\frac{1-D}{C}} \left((Cx + D)^2 - (Cx + D) + \frac{1}{2}\right) \mathrm{d}x \\ &\qquad + C \int_{\frac{1-D}{C}}^{\frac{1}{C}} \left((Cx + D - 1)^2 - (Cx + D - 1) + \frac{1}{2}\right) \mathrm{d}x. \end{aligned}$$

Summing the terms alike in the two integrals, yields

$$\begin{aligned} I(g) = C \int_0^{1/C} & \Big((Cx+D)^2 - (Cx+D) + \frac{1}{2} \Big) \, \mathrm{d}x \\ & + C \int_{\frac{1-D}{C}}^{\frac{1}{C}} \big(-2(Cx+D) + 1 + 1 \big) \, \mathrm{d}x \\ = C \left(\frac{(Cx+D)^3}{3C} - \frac{(Cx+D)^2}{2C} + \frac{x}{2} \right) \Bigg|_0^{1/C} & + C \left(\frac{-2(Cx+D)^2}{2C} + 2x \right) \Bigg|_{(1-D)/C}^{1/C} . \end{aligned}$$

Next, a straightforward calculation leads to the conclusion that $I(g) = 1/3$, which concludes the proof of the lemma. $\square$

For any finite sequence $\mathcal{S} \subset [0,1]$, and any $\alpha, \beta \in [0,1]$, let $\mathrm{D}(\mathcal{S}; \alpha, \beta) := \big| \mathcal{S} \cap [\alpha, \beta] \big| - |\mathcal{S}|(\beta - \alpha)$ be its *discrepancy* in the interval $[\alpha, \beta]$. Then, the *uniform discrepancy* of $\mathcal{S}$, denoted by $\mathrm{D}(\mathcal{S})$, is defined by

$$\mathrm{D}(\mathcal{S}) := \frac{1}{|\mathcal{S}|} \cdot \sup_{0 \le \alpha \le \beta \le 1} \big| \mathrm{D}(\mathcal{S}; \alpha, \beta) \big| ,$$

The uniform discrepancy can be bounded by the Erdős-Turán inequality.

Lemma 2.2 (Erdős-Turán [31, Corollary 1.1, Chap. 1])**.** *For any integer $K > 1$*

$$\big| \mathrm{D}(\mathcal{S}) \big| \le \frac{|\mathcal{S}|}{K} + 3 \sum_{m=1}^{K} \frac{1}{m} \Big| \sum_{s \in \mathcal{S}} e(ms) \Big| , \tag{12}$$

where $e(x) := \exp(2\pi i x)$.

We will need to estimate exponential sums with Fermat quotients, and to do so, we will make use of the following bound.

Lemma 2.3 (Heath–Brown [32])**.** *For any integer m relatively prime to p we have*

$$\sum_{\substack{X < n \le X+Y \\ \gcd(n,p)=1}} e\left(\frac{m \mathfrak{q}_p(n)}{p} \right) = O\big(Y^{1/2} p^{3/8} \big), \tag{13}$$

uniformly for $X, Y > 1$.

The next lemma is a simple calculation of the hyper-polyhedron's volume, which we include for completeness.

Lemma 2.4. *Let σ be a permutation of size $N \ge 1$ and let $T(\sigma, N) \subset [0,1]^N$ be the polyhedron defined by*

$$T(\sigma, N) := \big\{ (x_1, \ldots, x_N) \in [0,1]^N : x_{\sigma(1)} < x_{\sigma(2)} < \cdots < x_{\sigma(N)} \big\}.$$

Then the Lebesgue measure of $T(\sigma, N)$ is

$$\mu\big(T(\sigma, N)\big) = \frac{1}{N!}.$$

Proof. The result follows by noting the following recursion when we reduce the dimension:

$$\begin{aligned}\int_0^1 \int_0^{z_N} \cdots \int_0^{z_3} \int_0^{z_2} 1 \, \mathrm{d}z_1 \, \mathrm{d}z_2 \cdots \mathrm{d}z_N &= \int_0^1 \int_0^{z_N} \cdots \int_0^{z_4} \int_0^{z_3} z_2 \, \mathrm{d}z_2 \, \mathrm{d}z_3 \cdots \mathrm{d}z_N \\ &= \int_0^1 \int_0^{z_N} \cdots \int_0^{z_5} \int_0^{z_4} \frac{z_3^2}{2} \, \mathrm{d}z_3 \, \mathrm{d}z_4 \cdots \mathrm{d}z_N \\ &= \int_0^1 \int_0^{z_N} \cdots \int_0^{z_6} \int_0^{z_5} \frac{z_4^3}{2 \cdot 3} \, \mathrm{d}z_4 \, \mathrm{d}z_5 \cdots \mathrm{d}z_N \,.\end{aligned}$$

Differently, the same result is a consequence of the observation that $\mu\big(T(\sigma, N)\big)$ is the same for any σ. □

We will also need a basic tool analogous to the Erdős-Turán inequality, which is useful for classifying sequences in multi-dimensional spaces as uniformly distributed. For this, consider the sequence $\boldsymbol{x} = \{\boldsymbol{x}_n\}_{n \geq 1} \subset [0, 1)^N$ and denote by $\mathscr{B}$ a generic box in the unit cube:

$$\mathscr{B} = \prod_{1 \leq j \leq N} [a_j, b_j) \subset [0, 1)^N.$$

Then the *extreme discrepancy* of $\boldsymbol{x}$ with respect to $\mathscr{B}$ is defined by

$$\mathrm{D}_N(\boldsymbol{x}, R) := \sup_{\mathscr{B} \subset [0,1)^N} \left| \mu(\mathscr{B}) - \frac{1}{R} \#\big\{n \leq R : \boldsymbol{v}_n \in \mathscr{B}\big\} \right|,$$

where μ denotes the Lebesgue measure.

The next lemma gives the Koksma–Szüsz inequality [33, 34] which bounds the extreme discrepancy in terms of the level of cancellation in the exponential sums associated to the sequence in question. It shows that if the sequence $\boldsymbol{x} = \{\boldsymbol{x}_n\}_{n \geq 1} \subset [0, 1)^N$ is uniformly distributed at random in $[0, 1)^N$ and independently for any $n \geq 1$, then $\mu(\mathscr{B})$ approximates effectively the proportion of the elements $\boldsymbol{x}_n$ that belong to $\mathscr{B}$.

Lemma 2.5 (Koksma–Szüsz)**.** *For any integer $H > 1$ and any sequence $\boldsymbol{x} = \{\boldsymbol{x}_n\}_{n \geq 1} \subset [0, 1)^N$, we have*

$$\mathrm{D}_N(\boldsymbol{x}, R) \leq C_N \left(\frac{2}{H+1} + \sum_{0 < \|\boldsymbol{h}\|_\infty \leq H} \frac{1}{r(\boldsymbol{h})} \left| \frac{1}{R} \sum_{j=1}^{R} e\Big(2\pi i \langle \boldsymbol{h}, \boldsymbol{x}_j \rangle\Big) \right| \right), \tag{14}$$

where $r(\boldsymbol{h}) = \prod_{i=1}^{N} \max\{1, |h_i|\}$ for $\boldsymbol{h} = (h_1, \ldots, h_N) \in \mathbb{Z}^N$, $\langle \cdot, \cdot \rangle$ denotes the inner product, and C_N denotes an absolute constant depending on the dimension N.

The following lemma estimates the exponential sum in (14) for the sequence of elements in the Fermat quotient matrix translated by the displacements $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N\} \subset \mathbb{Z}^2$.

Lemma 2.6. *Let p be prime, $H, M, N \geq 1$, and let $\boldsymbol{v}_j = (s_j, t_j) \in \mathbb{Z}^2$ for $1 \leq j \leq N$ be fixed and chosen such that $\max\limits_{1\leq j\leq N} \|\boldsymbol{v}_j\|_\infty \leq M$. Assume that one of the integers t_j is different from all the others, and denote by J its index. Let*

$$\mathcal{G}_N(p) := \bigcap_{j=1}^{N} \Big\{(a,b) \in \Big([0,p)\times[1,p)\Big) \cap \mathbb{Z}^2 : 0 \leq a + s_j < p,\ 1 \leq b + t_j < p\Big\},$$

and let $\boldsymbol{x}_{a,b} = (x_1, \ldots, x_N)$, where $x_j := \mathfrak{q}_p\big((a+s_j)p + (b+t_j)\big)/p$ for $1 \leq j \leq N$ and $(a,b) \in \mathcal{G}_N(p)$. Then, for any $\boldsymbol{h} = (h_1, \ldots, h_N) \in \big([-H,H]\cap\mathbb{Z}\big)^N$, for which $h_J \neq 0$, we have

$$S(p) := \sum_{(a,b)\in\mathcal{G}_N(p)} e(\langle \boldsymbol{h}, \boldsymbol{x}_{a,b}\rangle) = O_{M,N}(p)\,. \tag{15}$$

Proof. First, let us complete the sum $S(p)$ to a sum over the entire torus $[0,p)^2$. Let

$$S_0(p) := \sum_{(a,b)\in[0,p)\times[1,p)} e(\langle \boldsymbol{h}, \boldsymbol{x}_{a,b}\rangle),$$

where $\boldsymbol{x}_{a,b} = (x_1, \ldots, x_N)$ for $(a,b) \notin \mathcal{G}_N(p)$ are defined by the same formula in the lemma except that the arguments are replaced by the representatives of $a + s_j$ and $b + t_j$ modulo p taken from $\{0, \ldots, p-1\}$. Then, if p is sufficiently large, the sums $S(p)$ and $S_0(p)$ coincide except for at most $4Mp$ new terms added in $S_0(p)$, that is,

$$S(p) = S_0(p) + O_M(p)\,. \tag{16}$$

The complete sum is

$$\begin{aligned} S_0(p) &= \sum_{a=0}^{p-1}\sum_{b=1}^{p-1} e(h_1x_1 + \cdots h_Nx_N) \\ &= \sum_{a=0}^{p-1}\sum_{b=1}^{p-1} e\left(\frac{h_1\mathfrak{q}_p\big((a+s_1)p + (b+t_1)\big) + \cdots + h_N\mathfrak{q}_p\big((a+s_N)p + (b+t_N)\big)}{p}\right). \end{aligned}$$

By Proposition 3, we know that for $1 \leq j \leq N$ we have

$$\mathfrak{q}_p\big((a+s_j)p + (b+t_j)\big) = \mathfrak{q}_p(b+t_j) - (a+s_j)(b+t_j)^{-1}.$$

Then, $S_0(p)$ can be written as

$$S_0(p) = \sum_{b=1}^{p-1} e\left(\frac{h_1\big(\mathfrak{q}_p(b+t_1) - s_1(b+t_1)^{-1}\big) + \cdots + h_N\big(\mathfrak{q}_p(b+t_N) - s_N(b+t_N)^{-1}\big)}{p}\right) \\ \times \sum_{a=0}^{p-1} e\left(\frac{aR(b;\boldsymbol{h},\mathcal{V})}{p}\right), \tag{17}$$

where $X \mapsto R(X;\boldsymbol{h},\mathcal{V})$ is a rational function in $\mathbb{F}_p(X)$. More explicitly,

$$R(X;\boldsymbol{h},\mathcal{V}) = \frac{P(X,\boldsymbol{h},\mathcal{V})}{Q(\boldsymbol{h},b,\mathcal{V})},$$

where $P(X;\boldsymbol{h},\mathcal{V})$ and $Q(X;\boldsymbol{h},\mathcal{V})$ are polynomials over $\mathbb{F}_p[X]$ of degrees

$$0 \le \deg(P) < \deg(Q) \quad \text{ and } \quad 1 \le \deg(Q) \le N.$$

Note that the roots of $Q(X;\boldsymbol{h},\mathcal{V})$ belong to the set $\{-t_1,\dots,-t_N\}$, but not all elements of the set are always roots, as certain terms may cancel each other through addition. Nevertheless, the requirement in the hypothesis, which implies that one of the roots is distinct from all the others, ensures that $\deg(Q) \ge 1$, so that, in particular, $R(X;\boldsymbol{h},\mathcal{V})$ is not identically zero.

Then, for any b with $1 \le b \le p-1$, there are two possibilities: either b is a root of $P(X;\boldsymbol{h},\mathcal{V})$ or b is not a root of $P(X;\boldsymbol{h},\mathcal{V})$. In the first case, in the sum over a in (17) all terms are equal to 1, while in the second case, the terms run over the set of all roots of unity of order p. Therefore

$$\sum_{a=0}^{p-1} e\left(\frac{aR(b;\boldsymbol{h},\mathcal{V})}{p}\right) = \begin{cases} p & \text{if } R(b;\boldsymbol{h},\mathcal{V}) \equiv 0 \pmod p, \\ 0 & \text{if } R(b;\boldsymbol{h},\mathcal{V}) \not\equiv 0 \pmod p. \end{cases} \tag{18}$$

Then, since $P(X;\boldsymbol{h},\mathcal{V})$ has at most N roots modulo p, on inserting (18) in (17), yields

$$\big|S_0(p)\big| \le Np\,. \tag{19}$$

The lemma then follows on combining (16) and (19). $\square$

Lemma 2.7. *Let $H, N \ge 1$ be integers and let $r(\boldsymbol{h}) := \prod_{j=1}^N \max\{1,|h_j|\}$, where $\boldsymbol{h} = (h_1,\dots,h_N) \in \mathbb{Z}^N$. Then*

$$\sum_{0<\|\boldsymbol{h}\|_\infty \le H} \frac{1}{r(\boldsymbol{h})} = O_N\big(\log^N H\big). \tag{20}$$

Proof. If we assume exactly ℓ entries of $\boldsymbol{h}$ are nonzero, then the corresponding sum is bounded by

$$\ll \binom{N}{\ell} \sum_{1\le |h_1|\le H} \cdots \sum_{1\le |h_\ell|\le H} \frac{1}{|h_1|\cdots|h_\ell|} \ll \binom{N}{\ell}(\log H)^N.$$

Hence, as ℓ ranges over $1,\dots,N$, we have

$$\sum_{0<\|\boldsymbol{h}\|_\infty\le H} \frac{1}{r(\boldsymbol{h})} \ll \sum_{\ell=1}^{N} \binom{N}{\ell}(\log H)^N < 2^N \log^N H.$$

□

3 Average distances from the the Fermat Quotients to a line

Let p be a large prime number. Let L be a positive integer less than p whose value will be chosen later. Define

$$\mathcal{T}_{jk} = \left(\frac{j-1}{L}, \frac{j}{L}\right] \times \left(\frac{k-1}{L}, \frac{k}{L}\right], \quad 1\le j\le L,\ 2\le k\le L,$$

while, for $k=1$, we keep the left end of the second interval closed, that is,

$$\mathcal{T}_{j1} = \left(\frac{j-1}{L}, \frac{j}{L}\right] \times \left[0, \frac{1}{L}\right], \quad 1\le j\le L.$$

These rectangles are disjoint and form the set partition

$$(0,1]\times[0,1] = \bigcup_{j=1}^{L}\bigcup_{k=1}^{L} \mathcal{T}_{jk}\,.$$

Next, consider the set of normalized points based on the Fermat quotient matrix:

$$\mathcal{B}_{jk} := \left\{1\le b\le p-1 : \left(\frac{b}{p}, \frac{\mathfrak{q}_p(b)}{p}\right) \in \mathcal{T}_{jk}\right\} \quad \text{for } 1\le j,k\le L.$$

Note that, since $b/p\ne 0$, each $b\in\{1,\dots,p-1\}$ lies in exactly one of the sets $\mathcal{B}_{jk}$.

Now, let $C,D>0$ be fixed real numbers and let

$$f(x,y) := \left|y - \{Cx+D\}\right|.$$

In order to prove Theorem 1, we need to estimate the average

$$M(p, C, D) := \frac{1}{p} \sum_{b=1}^{p-1} f\left(\frac{b}{p}, \frac{\mathfrak{q}_p(b)}{p}\right). \tag{21}$$

With the notations of the partition above, this is

$$M(p, C, D) = \frac{1}{p} \sum_{j=1}^{L} \sum_{k=1}^{L} \sum_{b \in \mathcal{B}_{jk}} f\left(\frac{b}{p}, \frac{\mathfrak{q}_p(b)}{p}\right). \tag{22}$$

Note that for each $b \in \mathcal{B}_{jk}$, we have

$$f\left(\frac{b}{p}, \frac{\mathfrak{q}_p(b)}{p}\right) = f\left(\frac{j}{L}, \frac{k}{L}\right) + O\left(\frac{C}{L}\right). \tag{23}$$

Next we estimate the size of the sets $\mathcal{B}_{jk}$. Note that $b \in \mathcal{B}_{jk}$ if and only if both of the following conditions are satisfied:

(i) $\frac{j-1}{L}p < b \leq \frac{j}{L}p$,

(ii) $\frac{k-1}{L}p < \frac{\mathfrak{q}_p(b)}{p} \leq \frac{k}{L}p$ for $1 \leq k \leq L$.

The size of $\mathcal{B}_{jk}$ will follow if we know the discrepancy of the sequence

$$\mathcal{S}_p(j) = \left\{\frac{\mathfrak{q}_p(b)}{p} : \frac{j-1}{L}p < b \leq \frac{j}{L}p\right\} \subset [0,1] \quad \text{for } 1 \leq j \leq L.$$

According to Erd?s-Turán inequality [35, Corollary 1.1], the discrepancy is bounded by

$$D\big(\mathcal{S}_p(j)\big) \leq \frac{p/L}{K+1} + 3\sum_{m=1}^{K} \frac{1}{m}\Bigg|\sum_{\frac{j-1}{L}p<b\leq\frac{j}{L}p} e\left(\frac{m\mathfrak{q}_p(b)}{p}\right)\Bigg|.$$

The exponential sum above is bounded by Heath-Brown's Lemma 2.3:

$$\sum_{\frac{j-1}{L}p<b\leq\frac{j}{L}p} e\left(\frac{m\mathfrak{q}_p(b)}{p}\right) \ll \left(\frac{p}{L}\right)^{1/2} p^{3/8} = L^{-1/2}p^{7/8},$$

for all integers m relatively prime to p. Therefore, it follows that

$$\begin{aligned} D\big(\mathcal{S}_p(j)\big) &\ll \frac{p}{L(K+1)} + 3\sum_{m=1}^{K} \frac{1}{m} L^{-1/2}p^{7/8} \\ &\leq \frac{1}{\sqrt{L}}\left(\frac{p}{K+1} + 3p^{7/8}\log K\right), \end{aligned}$$

for any integer $K \geq 1$. To balance the terms, we choose $K = \lfloor p^{1/8} \rfloor$, and obtain

$$D\big(\mathcal{S}_p(j)\big) \ll L^{-1/2} p^{7/8} \log p\,.$$

Thus, by the definition of the discrepancy,

$$|\mathcal{B}_{jk}| = \frac{p}{L} \cdot \frac{1}{L} + O\left(L^{-1/2} p^{7/8} \log p\right), \tag{24}$$

for $1 \leq j, k \leq L$.

Now we can estimate the average defined by (21). For this, we use the decomposition in rectangles (22), where the values of f can be approximated by those on the corners (23):

$$\begin{aligned} M(p,C,D) &= \frac{1}{p} \sum_{j=1}^{L} \sum_{k=1}^{L} \sum_{b \in \mathcal{B}_{jk}} f\left(\frac{b}{p}, \frac{\mathfrak{q}_p(b)}{p}\right) \\ &= \frac{1}{p} \sum_{j=1}^{L} \sum_{k=1}^{L} |\mathcal{B}_{jk}| \Big(f\Big(\frac{j}{L}, \frac{k}{L}\Big) + O\Big(\frac{C}{L}\Big)\Big)\,. \end{aligned}$$

On inserting the size of $|\mathcal{B}_{jk}|$ from (24), yields

$$\begin{aligned} M(p,C,D) =& \frac{1}{p} \left(\frac{p}{L^2} + O\left(L^{-1/2} p^{7/8} \log p\right)\right) \sum_{j=1}^{L} \sum_{k=1}^{L} \left(f\left(\frac{j}{L}, \frac{k}{L}\right) + O\left(\frac{C}{L}\right)\right) \\ =& \frac{1}{L^2} \sum_{j=1}^{L} \sum_{k=1}^{L} f\left(\frac{j}{L}, \frac{k}{L}\right) + O\bigg(\frac{\log p}{L^{1/2} p^{1/8}} \sum_{j=1}^{L} \sum_{k=1}^{L} f\left(\frac{j}{L}, \frac{k}{L}\right)\bigg) \\ &+ O\bigg(\frac{C}{L^3} \sum_{j=1}^{L} \sum_{k=1}^{L} 1\bigg) + O\left(C L^{1/2} p^{-1/8} \log p\right). \end{aligned} \tag{25}$$

Next, to continue, it should be noted that, by Lemma 2.1, the first term on the right-hand side of (25), which is a Riemann sum, tends to $1/3$ if $L \to \infty$, because $C \neq 0$. Furthermore, counting on the maximal possible offset makeing use of (23), we find that

$$\frac{1}{L^2} \sum_{j=1}^{L} \sum_{k=1}^{L} f\left(\frac{j}{L}, \frac{k}{L}\right) = \frac{1}{3} + O\left(\frac{C}{L}\right). \tag{26}$$

Using (26) again, it follows that the sum of the three error terms in (25) is

$$O\left(\frac{C}{L} + (L+C) L^{1/2} p^{-1/8} \log p\right) = O\left(\frac{C}{L} + L^{3/2} p^{-1/8} \log p\right), \tag{27}$$

because we need to choose L such that $C = o(L)$, in order to have a proper estimate with the error term that is not larger than the main one, which is equal to $1/3$, as we have learned from (26).

Now we choose $L = C^{2/5} p^{1/20} \log^{-2/5} p$, so that the terms in (27) have equal contributions. Then, under the assumption that $C = o\big(p^{1/12} \log^{-2/3} p\big)$, from (25),(26), and (27) it follows

$$M(p, C, D) = \frac{1}{3} + O\big(C^{3/5} p^{-1/20} \log^{2/5} p\big)\,,$$

with an absolute constant in the error term. This concludes the proof of Theorem 1.

4 Distribution of Fermat quotients in geometric configuration respecting relative size conditions. Proof of Theorem 2

The proof of Theorem 2 goes through the following steps. First, we decompose the unit cube that contain the N-dimensional vectors $\boldsymbol{x}_{a,b}$ into boxes of a generic size and then we estimate the number of vectors $\boldsymbol{x}_{a,b}$ in each box. Next, we count the number of boxes that contain "good" vectors, meaning those that follow the increasing order given by σ. Finally, we add up all the numbers of good vectors and choose the optimal size value of the boxes for which the error term is smaller.

4.1 Breaking the unit cube into pieces

Let $L > 1$, whose precise value will be chosen later, be fixed. We divide the unit cube into L^N boxes:

$$\mathscr{B}_{i_1,\dots,i_N} = \Big[\frac{i_1}{L}, \frac{i_1+1}{L}\Big) \times \cdots \times \Big[\frac{i_N}{L}, \frac{i_N+1}{L}\Big), \quad 0 \le i_1, \dots, i_N \le L-1.$$

Let $\mathcal{V} \in (\mathbb{Z}^2)^N$ be the ordered set of vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_N$ that defines the pattern of displacement vectors and let $\mathcal{G}_N(p)$ be the set of admissible positions in the Fermat quotient matrix $\mathtt{FQM}(p)$ defined by (3), positions that still remain in the matrix after translations by any $\boldsymbol{v} \in \mathcal{V}$.

To evaluate the spread of vectors $\boldsymbol{x}_{a,b} = \frac{1}{p}(A_{(a,b)+\boldsymbol{v}_1}, \dots, A_{(a,b)+\boldsymbol{v}_N})$ with $A_{a,b} = \mathfrak{q}_p(ap+b)$ and $(a,b) \in \mathcal{G}_N(p)$, we will use the fact that their set is uniformly distributed in $[0,1]^N$. In order to verify this fact, let us estimate the discrepancy of

$$\mathcal{X} = \{\boldsymbol{x}_{a,b} : (a,b) \in \mathcal{G}_N(p)\}.$$

The Koksma–Szüsz inequality (2.5) imply that for any integer $H > 1$, we have

$$\frac{\#\big(\mathcal{X} \cap \mathscr{B}_{i_1,\dots,i_N}\big)}{|\mathcal{X}|} = \mu(\mathscr{B}_{i_1,\dots,i_N}) + O_N\Bigg(\frac{1}{H} + \sum_{0<\|\boldsymbol{h}\|_\infty \le H} \frac{1}{r(\boldsymbol{h})}\Bigg|\frac{1}{|\mathcal{X}|}\sum_{(a,b)\in\mathcal{G}_N(p)} e\Big(2\pi i\langle \boldsymbol{h}, \boldsymbol{x}_j\rangle\Big)\Bigg|\Bigg),$$

On using (4) and the bound (15) for the exponential sum, it follows

$$\#\big(\mathcal{X} \cap \mathscr{B}_{i_1,\dots,i_N}\big) = \frac{p^2}{L^N} + O_{M,N}\left(\frac{p^2}{H} + \frac{p}{L^N} + p \sum_{0<\|\boldsymbol{h}\|_\infty \le H} \frac{1}{r(\boldsymbol{h})}\right).$$

It should be noted that we were able to apply (15) because the condition $0 < \|\boldsymbol{h}\|_\infty$ in the summation ensures that there exists j for which $h_j \neq 0$, call J this index, and from the hypothesis of the theorem we know that t_J is different from each other t_j with $1 \le j \le N$ and $j \neq J$.

Bounding the sum over $\boldsymbol{h}$ by (20) and taking $H = p$, we conclude

$$\#\big(\mathcal{X} \cap \mathscr{B}_{i_1,\dots,i_N}\big) = \frac{p^2}{L^N} + O_{M,N}\big(p \log^N p\big). \tag{28}$$

4.2 Counting on the boxes that contain ordered vectors

Let σ be a permutation of N elements and let $T(\sigma, N)$ be the polyhedron

$$T(\sigma, N) = \big\{(x_1, \dots, x_N) \in [0,1]^N : x_{\sigma(1)} < x_{\sigma(2)} < \dots < x_{\sigma(N)}\big\},$$

which we know from Lemma 2.4 that has volume $\mu\big(T(\sigma, N)\big) = 1/N!$.

Note that some of these boxes are completely included in $T(\sigma, N)$, others are only partially, intersecting the boundary of $T(\sigma, N)$, while others are outside of $T(\sigma, N)$. Precisely, if $i_{\sigma(1)} < \dots < i_{\sigma(N)}$, then $\mathscr{B}_{i_1,\dots,i_N} \subseteq T(\sigma, N)$. If any of the inequalities becomes an equality, then points in $\mathscr{B}_{i_1,\dots,i_N}$ may or may not lie in $T(\sigma, N)$. If any of the inequalities gets reversed, then points in $\mathscr{B}_{i_1,\dots,i_N}$ do not lie in $T(\sigma, N)$.

We need to know the number of boxes included in $T(\sigma, N)$, respectively the ones that have a non-empty intersection with $T(\sigma, N)$.

Remark. *(1) Let N, L be integers such that $1 \le N \le L$. Then*

$$B^*(N, L) : \#\big\{(i_1, \dots, i_N) \in \{1, \dots, L\}^N : i_1 < \dots < i_N\big\} = \binom{L}{N}. \tag{29}$$

This follows by an induction argument by counting the numbers of tuples with i_N on all possible positions and observing that

$$\binom{L-1}{N-1} + \binom{L-2}{N-1} + \dots + \binom{N-1}{N-1} = \binom{L}{N},$$

equality known as the "hockey stick formula".

(2) Let N, L be integers such that $1 \le N \le L$. Then

$$B(N, L) := \#\big\{(i_1, \dots, i_N) \in \{1, \dots, L\}^N : i_1 \le \dots \le i_N\big\} = \binom{L+N-1}{N}. \tag{30}$$

The exact equality above follows by induction in the same way as (29), the only difference in the counting being the allowance for i_N to be equal to i_{N-1}.

Then, (29) and (30) imply that the number of boxes $\mathscr{B}_{i_1,\dots,i_N}$ included in $T(\sigma, N)$ and the number of boxes that intersect $T(\sigma, N)$ are approximately equal as L becomes sufficiently large:

$$B^*(N,L) = \frac{L^N}{N!} + O_N\big(L^{N-1}\big) \quad \text{and} \quad B(N,L) = \frac{L^N}{N!} + O_N\big(L^{N-1}\big). \tag{31}$$

4.3 Completion of the proof of Theorem 2

Knowing, on one hand, the cardinality of 'good' vectors $\boldsymbol{x}_{a,b}$ in a box $\mathscr{B}_{i_1,\dots,i_N}$, which is given by (28), and, on the other hand, the number of boxes that intersect the polyhedron $T(\sigma, N)$, we find that

$$\begin{aligned}
\#\left\{(a,b) \in \mathcal{G} : \boldsymbol{x}_{a,b} \in T(\sigma,N)\right\} &= \#\big(\mathcal{X} \cap T(\sigma,N)\big) \\
&= \left(\frac{L^N}{N!} + O_N\big(L^{N-1}\big)\right)\left(\frac{p^2}{L^N} + O_{M,N}\big(p\log^N p\big)\right) \\
&= \frac{p^2}{N!} + O_{M,N}\left(pL^N \log^N p + \frac{p^2}{L}\right).
\end{aligned}$$

To balance the error terms, we choose $L = \lfloor p^{1/(N+1)} \log^{-N/(N+1)p} \rfloor$ and obtain

$$\#\left\{(a,b) \in \mathcal{G} : \boldsymbol{x}_{a,b} \in T(\sigma,N)\right\} = \frac{p^2}{N!} + O_{M,N}\left(p^{(2N+1)/(N+1)} \log^{N/(N+1)} p\right).$$

This concludes the proof of Theorem 2.

Addenda

We include here several representations, on one hand of the set of pairs $(a,b) \in \mathcal{G}_N(p)$ for which the vectors $\boldsymbol{x}_{a,b}$ defined by (5) belong to the polyhedra $T(\sigma, N)$, and on the other hand, of the sets of vectors $\mathcal{X}(p) \cap T(\sigma, N)$ defined by (6) and (7).

Let $\mathcal{D}(\sigma, N, p)$ denote the set of points whose cardinality is estimated in Theorem 2, that is,

$$\mathcal{D}(\sigma,N,p) = \big\{(a,b) \in \mathcal{G}_N(p) : \boldsymbol{x}_{a,b}(p) \in T(\sigma,N)\big\}. \tag{32}$$

In the three sets $\mathcal{D}(\sigma, N, p)$ shown in Figure 2, one can see that an increasing number of equal second components in displacement vectors $\mathcal{V}$ causes the distribution of points to change from pseudo-random to increasingly regular.

We also remark that the ratios $p^2/\#(\mathcal{X}(p) \cap T(\sigma, 3))$ might strongly depend on σ, unlike the case treated in the Theorem 2, where all the second components of the vectors in $\mathcal{V}$ are distinct. To compare the dependency, see the different proportions in the case of the three images in Figure 3, where only the changed permutations σ make them distinct.

Table 2: The parameters used for generating the set of pairs $(a, b) \in \mathcal{D}(\sigma, N, p)$ in Figure 2 positioned from left to right and numbered sequentially from 1 to 3. The prime is $p = 601$ in all cases and the dimension is $N = 4$ in the 1st image and $N = 3$ in the last two images. Then $p^2 = 361201$, $p^2/4! \approx 15050.041$ and $p^2/3! \approx 60200.166$.

	σ	$\mathcal{V}$	$\#\mathcal{G}_N(p)$	$\#(\mathcal{X}(p) \cap T(\sigma, N))$	$\frac{p^2/N}{\#(\mathcal{X}(p) \cap T(\sigma,3))}$
1	$(2, 4, 1, 3)$	$(0, 4), (7, 5), (3, 10), (7, 16)$	346896	14360	1.048
2	$(2, 3, 1)$	$(10, 11), (1, 6), (2, 6)$	348099	57802	1.041
3	$(2, 3, 1)$	$(38, 6), (1, 6), (2, 6)$	334422	56512	1.065

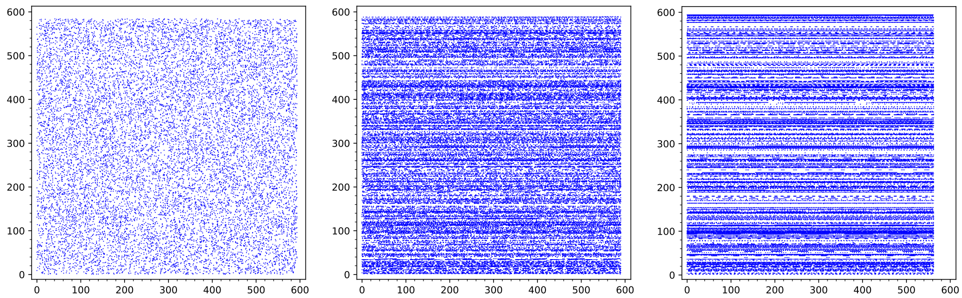

Fig. 2: Three representations of the set $\mathcal{D}(\sigma, N, p)$ in which the second components of displacement vectors become increasingly similar. The exact values of the generating parameters are listed in Table 2.

Table 3: The parameters used for generating the set of pairs $(a, b) \in \mathcal{D}(\sigma, N, p)$ in Figure 3 positioned from left to right and numbered sequentially from 1 to 3. The prime is $p = 503$ in all cases and the dimension is $N = 4$. Then $p^2 = 253009$ and $p^2/4! \approx 10542.041$.

	σ	$\mathcal{V}$	$\#\mathcal{G}_N(p)$	$\#(\mathcal{X}(p) \cap T(\sigma, N))$	$\frac{p^2/N}{\#(\mathcal{X}(p) \cap T(\sigma,3))}$
1	$(1, 2, 3, 4)$	$(0, 6), (1, 6), (2, 6), (3, 6)$	248000	41624	0.253
2	$(1, 3, 2, 4)$	$(0, 6), (1, 6), (2, 6), (3, 6)$	248000	10480	1.005
3	$(1, 4, 2, 3)$	$(0, 6), (1, 6), (2, 6), (3, 6)$	248000	6912	1.525

In Figure 4 are shown, in three dimensions, the set of points $\mathcal{X}(p)$ defined by (6) that are contained in the tetrahedrons $T(\sigma, 3)$ for different permutations σ and sets of displacement vectors $\mathcal{V}$. We remark that if all second components of the displacement vectors are equal, then the points in $\mathcal{X}(p) \cap T(\sigma, 3)$ are no longer equidistributed in the cube $[0, 1]^3$, but they arrange themselves in several triangles that transversely intersect their minimal containing tetrahedron. It should be noted that the ratio $p^2/\#\big(\mathcal{X}(p) \cap T(\sigma, 3)\big)$ may slowly approach a certain value (in Table 4, the comparison is made with 3!), but the number of parallel transverse triangles, on which the points $\boldsymbol{x}_{a,b}$ with $(a, b) \in \mathcal{D}(\sigma, 3, p)$ are aligned, becomes apparent even for small values of p.

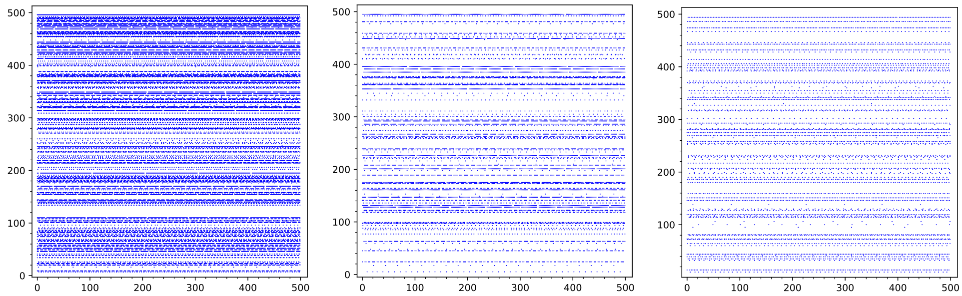

Fig. 3: The set of points $\mathcal{D}(\sigma, N, p)$ with generating parameters shown in Table 3, where only the permutation σ is changed from set to set.

Table 4: The parameters used for generating the set of points $\mathcal{X}(p) \cap T(\sigma, N)$ in Figure 4 positioned from left to right and top to bottom, and numbered sequentially from 1 to 6. In all cases $p = 211$, $N = 3$, so that $p^2 = 44521$ and $p^2/N! \approx 7420.166$.

	σ	$\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$	$\#\mathcal{G}_N(p)$	$\#(\mathcal{X}(p) \cap T(\sigma, N))$	$\frac{p^2/N}{\#(\mathcal{X}(p)\cap T(\sigma,3))}$
1	$(2,1,3)$	$(26,-11),(26,12),(26,33)$	30710	4995	1.485
2	$(2,3,1)$	$(10,6),(1,6),(2,6)$	41004	7256	1.022
3	$(2,3,1)$	$(10,11),(1,6),(2,6)$	39999	6555	1.131
4	$(3,2,1)$	$(1,16),(4,16),(7,16)$	39576	10070	0.736
5	$(3,1,2)$	$(3,12),(6,12),(12,12)$	39402	5338	1.390
6	$(1,2,3)$	$(91,26),(2,26),(5,26)$	37904	7125	1.041

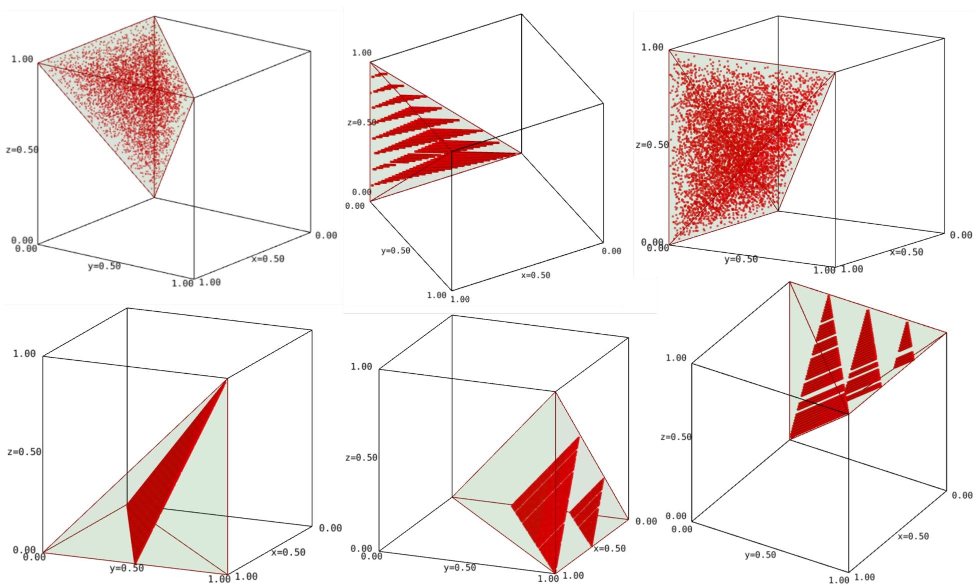

Fig. 4: Six instances representing the set of points $\mathcal{X}(p)$ belonging to the tetrahedrons $T(\sigma, 3)$, with the generating parameters presented in Table 4.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

[1] Joyal, A.: δ-anneaux et vecteurs de witt. (δ-rings and Witt vectors). C. R. Math. Acad. Sci., Soc. R. Can. **7**, 177–182 (1985)

[2] Buium, A.: Geometry of p-jets. Duke Math. J. **82**(2), 349–367 (1996) https://doi.org/10.1215/S0012-7094-96-08216-2

[3] Jeffries, J.: Differentiating by prime numbers. Notices Am. Math. Soc. **70**(11), 1772–1779 (2023) https://doi.org/10.1090/noti2833

[4] Mirimanoff, D.: Sur la congruence $(r^{p-1} - 1) : p \equiv q_r \pmod p$. J. Reine Angew. Math. **CXV**, 295–306 (1895)

[5] Mirimanoff, D.: Sur le dernier théorème de *Fermat*. J. Reine Angew. Math. **139**, 309–324 (1911) https://doi.org/10.1515/crll.1911.139.309

[6] Lerch, M.: Zur theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$. Math. Ann. **60**(4), 471–490 (1905) https://doi.org/10.1007/BF01561092

[7] Wieferich, A.: Zum letzten Fermatschen Theorem. Journal für die reine und angewandte Mathematik **1909**(136), 293–302 (1909) https://doi.org/10.1515/crll.1909.136.293

[8] Shanks, D., Williams, H.C.: Gunderson's function in Fermat's last theorem. Mathematics of Computation **36**(153), 291–295 (1981) https://doi.org/10.1090/S0025-5718-1981-0595065-7

[9] Suzuki, J.: On the generalized Wieferich criteria. Proc. Japan Acad., Ser. A **70**(7), 230–234 (1994) https://doi.org/10.3792/pjaa.70.230

[10] Eisenstein, G.: Neue gattung zahlentheoret. funktionen, die v. 2 elementen abhangen und durch gewisse lineare funktional-gleichungen definirt werden. Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königl. Preuß. Akademie der Wissenschaften zu Berlin. Math. Werke, Gotthold Eisenstein, Band II, Chelsea, New York, 2nd ed., 1989, pp. 705-711 (p. 710)., 36–42 (1850)

[11] Johnson, W.: On the nonvanishing of Fermat quotients (mod p). J. Reine Angew. Math. **292**, 196–200 (1977) https://doi.org/10.1515/crll.1977.292.196

[12] Johnson, W.: On the p-divisibility of the Fermat quotients. Math. Comput. **32**, 297–301 (1978) https://doi.org/10.2307/2006280

[13] Ernvall, R., Metsänkylä, T.: On the p-divisibility of Fermat quotients. Math. Comput. **66**(219), 1353–1365 (1997) https://doi.org/10.1090/S0025-5718-97-00843-0

[14] F, L.: Fermat quotients over function fields. Finite Fields Appl. **3**(4), 275–286 (1997) https://doi.org/10.1006/ffta.1996.0165

[15] Agoh, T.: The square and cube of Fermat quotients and values of Mirimanoff polynomials. JP J. Algebra Number Theory Appl. **11**(1), 113–127 (2008)

[16] Shparlinski, I.E.: Bounds of multiplicative character sums with Fermat quotients of primes. Bull. Aust. Math. Soc. **83**(3), 456–462 (2011) https://doi.org/10.1017/S000497271000198X

[17] Shparlinski, I.E.: On the value set of Fermat quotients. Proc. Am. Math. Soc. **140**(4), 1199–1206 (2012) https://doi.org/10.1090/S0002-9939-2011-11203-6

[18] Shparlinski, I.E.: On vanishing Fermat quotients and a bound of the Ihara sum. Kodai Math. J. **36**(1), 99–108 (2013) https://doi.org/10.2996/kmj/1364562722

[19] Shparlinski, I.E.: Fermat quotients: exponential sums, value set and primitive roots. Bull. Lond. Math. Soc. **43**(6), 1228–1238 (2011) https://doi.org/10.1112/blms/bdr058

[20] Alexandru, V., Cobeli, C., Vâjâitu, M., Zaharescu, A.: On Wieferich and non-Wieferich primes with prime bases. Mediterr. J. Math. **20**(2), 15 (2023) https://doi.org/10.1007/s00009-023-02298-1 . Id/No 93

[21] Lehmer, D.H.: On Fermat's quotient, base two. Math. Comput. **36**, 289–290 (1981) https://doi.org/10.2307/2007748

[22] Lenstra, H.W.j.: Miller's primality test. Inf. Process. Lett. **8**, 86–88 (1979) https://doi.org/10.1016/0020-0190(79)90149-2

[23] Ostafe, A., Shparlinski, I.E.: Pseudorandomness and dynamics of Fermat quotients. SIAM J. Discrete Math. **25**(1), 50–71 (2011) https://doi.org/10.1137/100798466

[24] Shparlinski, I.E.: Character sums with Fermat quotients. Q. J. Math. **62**(4), 1031–1043 (2011) https://doi.org/10.1093/qmath/haq028

[25] Chang, M.-C.: Short character sums with Fermat quotients. Acta Arith. **152**(1), 23–38 (2012) https://doi.org/10.4064/aa152-1-3

[26] Chen, Z., Winterhof, A.: On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients. Int. J. Number Theory **8**(3), 631–641 (2012) https://doi.org/10.1142/S1793042112500352

[27] Alexandru, V., Cobeli, C., Vâjâitu, M., Zaharescu, A.: Statistical distribution of

Fermat quotients. Chaos, Solitons & Fractals **161**, 112335 (2022) https://doi.org/10.1016/j.chaos.2022.112335

[28] Cobeli, C.I., Gonek, S.M., Zaharescu, A.: The distribution of patterns of inverses modulo a prime. J. Number Theory **101**(2), 209–222 (2003) https://doi.org/10.1016/S0022-314X(03)00059-3

[29] Cobeli, C., Vâjâitu, M., Zaharescu, A.: Distribution of gaps between the inverses mod q. Proc. Edinb. Math. Soc., II. Ser. **46**(1), 185–203 (2003) https://doi.org/10.1017/S0013091501000724

[30] Cobeli, C., Vâjâitu, M., Zaharescu, A.: Average estimates for the number of tuples of inverses mod p in short intervals. Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **43(91)**(2), 155–164 (2000)

[31] Montgomery, H.L.: Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis. Reg. Conf. Ser. Math., vol. 84. Providence, RI: American Mathematical Society, ??? (1994)

[32] Heath-Brown, D.R.: An estimate for Heilbronn's exponential sum. In: Analytic Number Theory. Vol. 2. Proceedings of a Conference in Honor of Heini Halberstam, May 16-20, 1995, Urbana, IL, USA, pp. 451–463. Boston, MA: Birkhäuser, ??? (1996). https://ora.ox.ac.uk/objects/uuid:455db511-6d3c-433c-b391-7b7dc22b723c

[33] Koksma, J.F.: Some theorems on diophantine inequalities. Actual. Math. Centrum, Amsterdam, Scriptum 5, 51 p. (1950). (1950)

[34] Szüsz, P.: Über ein Problem der Gleichverteilung. C. R. I. Congr. Math. Hongr. 1950, 461-472 (1952).

[35] Montgomery, H.L.: Topics in Multiplicative Number Theory. Lect. Notes Math., vol. 227. Springer, ??? (1971). https://doi.org/10.1007/BFb0060851