Mathematische Annalen (2023) 387:291–320
https://doi.org/10.1007/s00208-022-02452-2

Mathematische Annalen

Bias in the number of steps in the Euclidean algorithm and a conjecture of Ito on Dedekind sums

Paolo Minelli[1] · Athanasios Sourmelidis[1] · Marc Technau[1]

Received: 28 March 2022 / Revised: 3 July 2022 / Accepted: 22 July 2022 /
Published online: 6 September 2022

Abstract
We investigate the number of steps taken by three variants of the Euclidean algorithm on average over Farey fractions. We show asymptotic formulae for these averages restricted to the interval $(0, 1/2)$, establishing that they behave differently on $(0, 1/2)$ than they do on $(1/2, 1)$. These results are tightly linked with the distribution of lengths of certain continued fraction expansions as well as the distribution of the involved partial quotients. As an application, we prove a conjecture of Ito on the distribution of values of Dedekind sums. The main argument is based on earlier work of Zhabitskaya, Ustinov, Bykovskiĭ and others, ultimately dating back to Lochs and Heilbronn, relating the quantities in question to counting solutions to a certain system of Diophantine inequalities. The above restriction to only half of the Farey fractions introduces additional complications.

Mathematics Subject Classification Primary 11A55; Secondary 11F20 · 11K50 · 11J25

Paolo Minelli, Athanasios Sourmelidis and Marc Technau have contributed equally to this work.

✉ Marc Technau
mtechnau@math.tugraz.at

Paolo Minelli
minelli@math.tugraz.at

Athanasios Sourmelidis
sourmelidis@math.tugraz.at

[1] Institute for Analysis and Number Theory, Graz University of Technology, Kopernikusgasse 24/II, 8010 Graz, Austria

1 Introduction

1.1 Euclidean algorithm (classical version)

The Euclidean algorithm—referred to as 'EA$^{(\mathrm{sub})}$' in the sequel—for the computation of the greatest common divisor (gcd) of two positive integers a and b, has been described as *'the oldest non-trivial algorithm that has survived to the present day'* by Knuth [16, p. 318]. In its most basic form the algorithm proceeds by replacing the input tuple (a, b) by $(a - b, b)$ if $a < b$ ('Case A') and $(a, b - a)$ if $a \geq b$ ('Case B') until one of the arguments becomes zero ('Case C'), in which case the gcd of the original input is given by the other argument. (There is some leeway in describing the algorithm and we shall choose what is convenient for our exposition rather than what is historically most accurate; the reader is referred to *loc. cit.* for a more detailed discussion of that matter.) For instance, on the input $(11, 3)$, the algorithm takes the following six steps:

$$\begin{aligned}(11, 3) \mapsto (8, 3) \mapsto (5, 3) \overset{*}{\mapsto} (2, 3) \overset{*}{\mapsto} (2, 1)\\ \mapsto (1, 1) \overset{*}{\mapsto} (\underline{1}, 0) \quad (\text{hence, } \gcd(11, 3) = \underline{1}),\end{aligned} \tag{1.1}$$

where the asterisks $(*)$ mark the positions where the algorithm switches between cases. Observe that the number $11/3$ has the continued fraction expansion

$$\frac{11}{3} = 3 + \cfrac{1}{1 + \cfrac{1}{2}}. \tag{1.2}$$

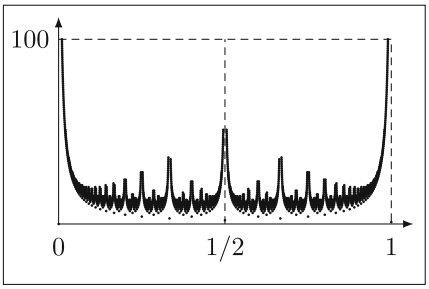
and $6 = 3 + 1 + 2$ is the sum of the partial quotients herein.

If one modifies Case A of EA$^{(\mathrm{sub})}$ as to replace (a, b) by $(a - B, b)$, where B is the largest multiple of b not exceeding a, and modifies Case B similarly, then the modified algorithm skips all steps $(\mapsto)$ not marked with an asterisk in the above example; this amounts to precisely 3 steps which is also the number of partial quotients in the continued fraction expansion (1.2); we shall refer to this version of EA$^{(\mathrm{sub})}$ by EA$^{(\mathrm{div})}$.

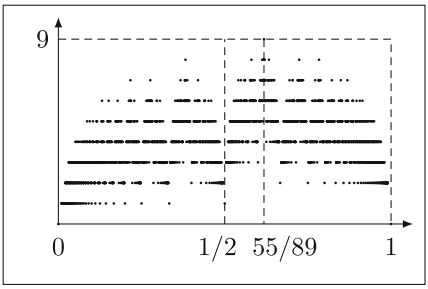
It is easy to see that the correspondence of number of steps on the input (a, b) and properties of the continued fraction expansion

$$\frac{a}{b} = [0; a_1, \ldots, a_n] := 0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} \tag{1.3}$$

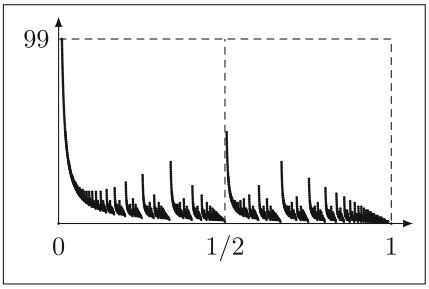
of $a/b \in [0, 1)$ (where $n \in \mathbb{N}_0$ and the so-called *partial quotients* $a_1, a_2, \ldots, a_n$ are positive integers and $a_n \geq 2$) holds in general, i.e.,



(a) $\mathrm{EA}^{(\mathrm{sub})}$. The maximum number of steps occurs at $1/100$ and $99/100$ which have the continued fraction expansion $[0;\ 100]$ and $[0;\ 1, 99]$ respectively.



(b) $\mathrm{EA}^{(\mathrm{div})}$. The maximum number of steps occurs at $55/89$ which has continued fraction expansion $[0;\ 1, 1, 1, 1, 1, 1, 1, 1, 2]$.



(c) $\mathrm{EA}^{(\mathrm{div})}_{(\text{by-excess})}$ (defined in § 1.2). The maximum number of steps occurs at $1/100$ which has the minus continued fraction expansion $[\![1;\ 2, \ldots, 2, 2]\!]$ (with '2' occurring 99 times).

Fig. 1 The number of steps of $\mathrm{EA}^{(\mathrm{sub})}$, $\mathrm{EA}^{(\mathrm{div})}$ & $\mathrm{EA}^{(\mathrm{div})}_{(\text{by-excess})}$ when applied to all reduced $a/b \in [0, 1) \cap \mathbb{Q}$ with $1 \le b \le 100$

- the number of steps taken by $\mathrm{EA}^{(\mathrm{sub})}$ when applied to (a, b) (or any tuple (ka, kb) with some positive integer k) is $a_1 + a_2 + \cdots + a_n$ (see Fig. 1a for a plot of its behavior), and
- the number of steps taken by $\mathrm{EA}^{(\mathrm{div})}$ is n. We denote this number by $s(a/b)$. (See Fig. 1b for a plot of its behavior.)

1.2 Variants of the Euclidean algorithm

Several other variants of the Euclidean algorithm have been considered in the literature (see, e.g., [27, 28] for a selection). For the most part, they arise (ignoring some technicalities) from modifying the distinguishing conditions of the cases A and B as introduced in Sect. 1.1. Here we discuss only one such variant. In fact, for convenience, we restrict our discussion to only stating a variant that is more similar in spirit to $\mathrm{EA}^{(\mathrm{div})}$ rather than $\mathrm{EA}^{(\mathrm{sub})}$. To obtain this variant—referred to as $\mathrm{EA}^{(\mathrm{div})}_{(\text{by-excess})}$ in the sequel—modify Case A of $\mathrm{EA}^{(\mathrm{div})}$ to replace the input (a, b) by $(B - a, b)$, where B is the smallest multiple of b not smaller than a and make a similar modification to Case B. Given this modification, our example (1.1) takes the shape $(11, 3) \overset{*}{\mapsto} (1, 3) \overset{*}{\mapsto} (\underline{1}, 0)$.

Once more, one can associate a certain continued fraction expansion of a number $a/b \in [0, 1)$ to the behaviour of the algorithm on the input (a, b). The particular continued fraction expansion relevant in this case is often called *minus continued fraction expansion*[1] and takes the shape

$$\frac{a}{b} = [\![1; b_1, \ldots, b_m]\!] := 1 - \cfrac{1}{b_1 - \cfrac{1}{b_2 - \cdots \cfrac{}{\cdots - \cfrac{1}{b_m}}}}, \tag{1.4}$$

where $m \in \mathbb{N}$ and $b_1, b_2, \ldots, b_m \geq 2$ are integers. When expanding a/b as in (1.4), then $m + 1$ can be seen to be the number of steps taken by $\mathrm{EA}^{(\mathrm{div})}_{(\text{by-excess})}$ on the input (a, b). We shall write $\ell(a/b)$ for the number m from (1.4) in the sequel. (See Fig. 1c for a plot of $\ell(a/b)$.) For further background on continued fractions we refer to [20].

1.3 Asymptotics for the number of steps of Euclidean algorithms

It is an interesting question to study statistical properties of the number of steps of the Euclidean algorithm (and its variants), or—equivalently—distribution properties of continued fractions. It was Heilbronn [12] who first identified the principal term of the asymptotics for the average number of steps in the case of the classical Euclidean algorithm, the average being taken over *numerators*:

$$\frac{1}{\varphi(b)} \sum_{\substack{a \leq b \\ \gcd(a,b)=1}} s\left(\frac{a}{b}\right) = A_1 \log b + O((\log\log b)^4) \quad (\text{as } b \to \infty);$$

here $\varphi(n) := \#\{1 \leq m \leq n : \gcd(m, n) = 1\}$ $(n \in \mathbb{N})$ is Euler's totient function and A_1 is an explicitly given non-zero constant.[2] For the same average, an asymptotic formula with two significant terms was obtained later by Porter [21]:

$$\frac{1}{\varphi(b)} \sum_{\substack{a \leq b \\ \gcd(a,b)=1}} s\left(\frac{a}{b}\right) = A_1 \log b + A_2 + O_\epsilon(b^{-1/6+\epsilon});$$

here A_1 is as before and A_2 is also an explicitly given non-zero constant. Bykovskiĭ and Frolenkov [6] have recently obtained a generalisation of this and obtained an improved error term.

Considering averages over both numerators *and* denominators, an asymptotic formula with power-law fall-off in the error term was obtained by Vallée [27] through the use of probability theory and ergodic-theoretic methods. This was improved by

[1] Instead of 'minus', some authors use the attribute 'backwards' or 'regular' instead.

[2] See Sect. 2.3 for a comment on the notation.

Ustinov [24], who obtained an asymptotic formula with better fall-off in the error term than the one that can be derived from Porter's result:

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{\substack{b\le Q \\ \gcd(a,b)=1}} \sum_{a\le b} s\left(\frac{a}{b}\right) = B_1 \log Q + B_2 + O((\log Q)^5/Q), \tag{1.5}$$

where

$$B_1 = \frac{\log 2}{2\zeta(2)}, \quad B_2 = \frac{\log 2}{4\zeta(2)}\left(3\log 2 + 4\gamma - 2\frac{\zeta'(2)}{\zeta(2)} - 3\right) - \frac{1}{4},$$

γ denotes the Euler–Mascheroni constant, ζ is the Riemann zeta function, and

$$\mathscr{F}(Q) = \{\, a/b \in \mathbb{Q} : \gcd(a,b) = 1,\ 0 \le a \le b \le Q \,\}$$

denotes the set of *Farey fractions of order* Q. In this regard it is worth noting that another natural way of averaging is over all pairs (a, b) with $1 \le a \le b \le Q$ without assuming coprimality of a and b. However, this situation is easily covered using (1.5) and Möbius inversion.

While examining the statistical properties of different variations of the Euclidean algorithm, Vallée [28] obtained also the leading term of the asymptotic formula for the expectation of the number of steps of the by-excess Euclidean algorithm (and hence for the average length of minus continued fractions). This was improved by Zhabitskaya [30] (following the approach of Ustinov [24]), a few years later, who showed that

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{\substack{b\le Q \\ \gcd(a,b)=1}} \sum_{a\le b} \ell\left(\frac{a}{b}\right) = C_1(\log Q)^2 + C_2 \log Q + C_3 + O((\log Q)^6/Q), \tag{1.6}$$

where C_1, C_2, C_3 are explicitly given non-zero constants, the first two being given by

$$C_1 = \frac{1}{2\zeta(2)}, \quad C_2 = \frac{1}{\zeta(2)}\left(2\gamma - \frac{3}{2} - 2\frac{\zeta'(2)}{\zeta(2)}\right), \tag{1.7}$$

and the value of C_3 being given by a somewhat longer, yet similar expression which we omit here. Both error terms in (1.5) and (1.6) have been improved to $O((\log Q)^3/Q)$ by Frolenkov [10] who incorporated ideas of Selberg from the elementary proof of the prime number theorem.

For more results regarding the expectation and the variance of the number of steps of the classical and by-excess Euclidean algorithm, we also refer to the work of Baladi and Vallée [1], Bykovskiĭ [5], Dixon [8, 9], Hensley [13] and Ustinov [25, 26].

1.4 Dedekind sums

Let $\lfloor \eta \rfloor = \min\{ n \in \mathbb{Z} : n \le \eta \}$ denote the integer part of $\eta \in \mathbb{R}$. Then the *saw-tooth function* is defined as

$$((\eta)) = \begin{cases} \eta - \lfloor \eta \rfloor - 1/2 & \text{if } \eta \in \mathbb{R} \setminus \mathbb{Z}, \\ 0 & \text{if } \eta \in \mathbb{Z}. \end{cases}$$

For any pair $a, b \in \mathbb{Z}$, $b \neq 0$, the *Dedekind sum*[3] $D(a, b)$ is defined as

$$D(a, b) = \sum_{n \le b} \left(\!\!\left(\frac{n}{b} \right)\!\!\right) \left(\!\!\left(\frac{na}{b} \right)\!\!\right).$$

It can be verified that $D(a, b) = D(ka, kb)$ for any non-zero integer k. Hence, $D(a/b) := D(a, b)$ is well defined. Moreover, the function $D\colon \mathbb{Q} \to \mathbb{Q}$ just defined is periodic with period one.

Dedekind sums originally arose in connection with the multiplier system for Dedekind's *eta* function over the modular group of two by two integer matrices of determinant one [7] and also satisfy a curious reciprocity law. By means of the latter Barkan [2] and (independently) Hickerson [14] have obtained the following identity which connects Dedekind sums with continued fraction expansions:

$$D(a/b) = \frac{(-1)^n - 1}{8} + \frac{a/b - (-1)^n [0; a_n, \ldots, a_2, a_1] + \Sigma_{\pm}(a/b)}{12}; \tag{1.8}$$

here $a/b = [0; a_1, a_2, \ldots, a_n]$ is as in (1.3) and

$$\Sigma_{\pm}(a/b) := \sum_{j \le n} (-1)^{j-1} a_j. \tag{1.9}$$

(See Fig. 2 for a plot of $\Sigma_{\pm}$.) In particular, Hickerson employed (1.8) to prove that the set $\{(a/b, D(a/b)) : a/b \in \mathbb{Q}\}$ is dense in $\mathbb{R}^2$.

Concerning distribution properties of Dedekind sums observe that via the symmetry property $D(x) = -D(1 - x)$ it is easy to see that

$$\sum_{x \in \mathscr{F}(Q)} D(x) = 0.$$

On the other hand, let $\mathscr{F}_0(Q) = \mathscr{F}(Q) \cap [0, 1/2)$ denote 'half' of all Farey fractions with denominators bounded by Q. Then, on the basis of numerical evidence, it has been conjectured by Ito [15] that

$$\lim_{Q \to \infty} \Sigma(Q) = +\infty, \quad \text{where} \quad \Sigma(Q) := \frac{1}{\#\mathscr{F}(Q)} \sum_{x \in \mathscr{F}_0(Q)} D(x). \tag{1.10}$$

[3] The notation $s(a/b)$ is also commonly used, but would conflict with our notation for the length of (1.3).

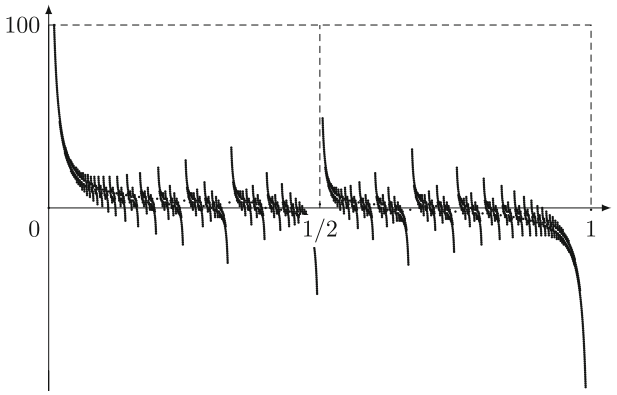


Fig. 2 Plot of $\Sigma_{\pm}(a/b)$ when applied to all Farey fractions $a/b \in [0,1] \cap \mathbb{Q}$ with $1 \le b \le 100$. Note that the average of the plotted values over the interval $[0, 1/2)$ is clearly positive, whereas the average of the plotted values over the interval $[1/2, 1)$ is negative

For an exposition of results on Dedekind sums we refer to the classical work of Rademacher and Grosswald [22], as well as a more up-to-date survey of Girstmair [11] with a focus on distribution properties.

2 Main results

2.1 Results

One of the main results of the present work is a proof of Ito's conjecture:

Theorem 2.1 (Ito's conjecture is true) *The statement in* (1.10) *holds. In fact, one even has the following stronger quantitative version:*

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{x \in \mathscr{F}_0(Q)} D(x) = \frac{1}{16} \log Q + O(1). \tag{2.1}$$

The proof of Theorem 2.1 rests crucially on the following variant of (1.6) which we believe to be of independent interest:

Theorem 2.2 (Bias in $\mathrm{EA}^{(\mathrm{div})}_{(\mathrm{by\text{-}excess})}$) *We have*

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{x \in \mathscr{F}_0(Q)} \ell(x) = c_1 (\log Q)^2 + c_2 \log Q + O(1),$$

where c_1, c_2 are non-zero constants satisfying $2c_1 = C_1$ and $2c_2 > C_2$ with the constants C_1 and C_2 given in (1.7)*. More precisely,*

$$c_1 = \frac{1}{4\zeta(2)}, \quad c_2 = \frac{1}{2\zeta(2)} \left(2\gamma - \frac{3}{2} - 2\frac{\zeta'(2)}{\zeta(2)} + \frac{3\zeta(2)}{4} \right) = \frac{C_2}{2} + \frac{3}{8}.$$

The above theorem may be interpreted as a quantitative version of the statement that the length $\ell(a/b)$ of the minus continued fraction expansion (1.4) tends to be larger on average on $\mathscr{F}_0(Q)$ than on $\mathscr{F}(Q) \setminus \mathscr{F}_0(Q)$ (due to $2c_2 > C_2$; see (1.6)). This may be phrased equivalently as saying that $\mathrm{EA}^{(\mathrm{div})}_{(\text{by-excess})}$ takes longer on average for fractions in $[0, 1/2)$ than it does for fractions in $[1/2, 1)$.

In view of the above it seems natural to ask if similar results can be obtained for the other algorithms $\mathrm{EA}^{(\mathrm{sub})}$ and $\mathrm{EA}^{(\mathrm{div})}$ discussed in Sect. 1.1. This turns out to be a rather easier question. For $\mathrm{EA}^{(\mathrm{sub})}$ one sees no difference in behaviour on $\mathscr{F}_0(Q)$ versus on $\mathscr{F}(Q) \setminus \mathscr{F}_0(Q)$, as should be evident from the symmetry in Fig. 1a about the vertical line through $1/2$. The latter symmetry may be verified easily by noting that $x = [0; a_1, a_2, \ldots, a_n]$ (with $a_1 \geq 2$ so that $x \leq 1/2$) and $1 - x = [0; 1, a_1 - 1, a_2, \ldots, a_n]$ have the same sum of partial quotients, *viz.* identical running time when fed into $\mathrm{EA}^{(\mathrm{sub})}$. On the other hand, an analogue of Theorem 2.2 may be obtained for $\mathrm{EA}^{(\mathrm{div})}$:

Proposition 2.3 (Bias in $\mathrm{EA}^{(\mathrm{div})}$) *We have*

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{x \in \mathscr{F}_0(Q)} s(x) = b_1 \log Q + b_2 + O((\log Q)^5/Q),$$

where $2b_1 = B_1$ *and* $2b_2 < B_2$ *with the constants* B_1 *and* B_2 *given from* (1.5). *More precisely,* $2b_2 = B_2 - 1/2$.

Proof This follows immediately from (1.5) and the fact that $s(x) = s(1 - x) - 1$ for $x \in (0, 1/2)$. □

We should like to mention that Bykovskiĭ [5] has obtained an asymptotic formula for averaging $s(a/q)$ over all a in some arbitary interval of length at most q. However, the error term in his result does not permit one to deduce Proposition 2.3.

Generalising Theorem 2.2 and Proposition 2.3 to averages over $\mathscr{F} \cap [0, \alpha)$ seems to be an interesting problem. However, this requires a more careful analysis and a sufficiently flexible generalisation of Lemma 4.2 below. As this seemed dispensable for our primary intent of proving Theorem 2.1, we shall address this elsewhere in forthcoming work (see also the first author's doctoral dissertation [18]).

2.2 Plan of the paper

In the next section we show how Theorem 2.1 can be deduced from Theorem 2.2. The proof of Theorem 2.2 is rather more involved. In Sect. 4 we sketch the overall argument and show how Theorem 2.2 can be deduced from a technical proposition (Proposition 4.5). The proof of the latter is carried out in Sect. 5.

2.3 Notation

We use the Landau notation $f(x) = O(g(x))$ and the Vinogradov notation $f(x) \ll g(x)$ to mean that there exists some constant $C > 0$ such that $|f(x)| \leq Cg(x)$ holds

for all admissible values of x (where the meaning of 'admissible' will be clear from the context). Unless otherwise indicated, any dependence of C on other parameters is specified using subscripts. Similarly, we write '$f(x) = o(g(x))$ as $x \to \infty$' if $g(x)$ is positive for all sufficiently large values of x and $f(x)/g(x)$ tends to zero as $x \to \infty$.

Given two coprime integers a and $q \neq 0$ we write $\mathrm{inv}_q(a)$ for the smallest positive integer in the residue class $(a \bmod q)^{-1}$.

3 Deducing Theorem 2.1 from Theorem 2.2

Throughout this section we shall assume that Theorem 2.2 has already been proved. The main tool for deducing Theorem 2.1 from Theorem 2.2 is the formula (1.8) of Barkan and Hickerson. In this vein, recall also the definition of $\Sigma_{\pm}(x)$ given in (1.9). For a number $x \in [0, 1)$ as in (1.3) let

$$\Sigma_{\mathrm{odd}}(x) = \sum_{\substack{i=1 \\ i \text{ odd}}}^{n} a_i, \quad \Sigma_{\mathrm{even}}(x) = \sum_{\substack{i=2 \\ i \text{ even}}}^{n} a_i.$$

Then, clearly,

$$\Sigma_{\pm}(x) = \Sigma_{\mathrm{odd}}(x) - \Sigma_{\mathrm{even}}(x). \tag{3.1}$$

The connection with minus continued fraction expansions and, thus, Theorem 2.2 arises as follows: in [29] Zhabitskaya notes[4] that it is implicit in an article of Myerson [19] that

$$\ell(x) = \Sigma_{\mathrm{odd}}(x) - \epsilon(x), \tag{3.2}$$

$$\ell(1 - x) = \Sigma_{\mathrm{even}}(x) + \epsilon(x). \tag{3.3}$$

Here $\epsilon(x) \in \{0, 1\}$ is some correction term which is related to our way of forcing uniqueness in the continued fraction expansion (1.3) by means of requiring the last partial quotient a_n to exceed 1. In fact, one can describe the value of $\epsilon(x)$ quite precisely (see [29]), but this is not necessary for our particular application.

Corollary 3.1 *We have*

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{x \in \mathscr{F}_0(Q)} \Sigma_{\pm}(x) = \frac{3}{4} \log Q + O(1).$$

Proof From (3.2) and Theorem 2.2 we deduce that

$$\frac{1}{\#\mathscr{F}(Q)} \sum_{x \in \mathscr{F}_0(Q)} \Sigma_{\mathrm{odd}}(x) = c_1 (\log Q)^2 + c_2 \log Q + O(1).$$

[4] There appears to be a misprint in [29, Eq. (8)]: the left hand side should read $l'((b-a)/b)$, as can be deduced from the equations (5) and (7) in *loc. cit.*

Moreover, by (3.3),

$$\sum_{x\in\mathscr{F}_0(Q)} \Sigma_{\text{even}}(x) = \sum_{x\in\mathscr{F}_0(Q)} \ell(1-x) + O(Q^2) = \sum_{x\in\mathscr{F}(Q)\setminus\mathscr{F}_0(Q)} \ell(x) + O(Q^2).$$

On the other hand, (1.6) and Theorem 2.2 show that, after dividing by $\#\mathscr{F}(Q)$, the right hand side in the above is

$$(C_1 - c_1)(\log Q)^2 + (C_2 - c_2)\log Q + O(1).$$

In view of (3.1), the result follows from the previous considerations. □

Proof of Theorem 2.1 Clearly it suffices to prove (2.1). To this end, observe that, by (1.8), we have $D(x) = \Sigma_{\pm}(x)/12 + O(1)$. Now (2.1) follows immediately from this and Corollary 3.1. □

4 Proof of Theorem 2.2

Before stating the key lemmas needed for the proof of Theorem 2.2, we give a short informal sketch of the overall argument. In Sect. 4.2 we state the three key lemmas we require. The proof of Theorem 2.2 is given in Sect. 4.3.

4.1 Sketch of the proof

In proving Theorem 2.2, we adapt the approach of Zhabitskaya [30]. The idea, which goes back to Lochs [17] and Heilbronn [12], is to transfer the problem of computing the (restricted) average of the lengths of (minus) continued fractions into a problem of counting lattice points inside certain regions. By virtue of Lemmas 4.3 and 4.4 (below), the proof of Theorem 2.2 boils down to evaluating asymptotically the number of integer solutions of the system

$$\begin{cases} \gcd(p,q) = 1, & p,q \geq 1, \\ \mathrm{inv}_p(q) \leq p/2, & \\ 2 \leq nq + kp \leq Q, & 1 \leq k < n. \end{cases}$$

This amounts to counting the lattice points inside some region subject to some coprimality condition and the additional restriction $\mathrm{inv}_p(q) \leq q/2$. The latter restriction is not present in [30] and complicates the overall analysis. Following [30], we split the problem of counting the solutions to the above system into five sub-cases. For every case we have to count lattice points with certain properties inside regions (see Sect. 4.3 for the details). This counting problem is solved in Proposition 4.5 and it should be apparent from the proof of Proposition 4.5 that the reason for the bias ($2c_2 > C_2$) in Theorem 2.2 is found within two of the considered cases. More specifically, for one of these cases, the number of lattice points to be counted is given, up to some error term, by

$$\sum_{q<Q^{1/4}} \frac{1}{q} \sum_{\substack{q/2<b\le q \\ \gcd(b,q)=1}} \frac{1}{q} \log \frac{Q^{1/2}}{q^2} = \sum_{q<Q^{1/4}} \frac{1}{q^2} \log \frac{Q^{1/2}}{q^2} \delta^+(q),$$

where δ^+ is the function appearing in Lemma 4.2. The same procedure carried out for fractions greater than $1/2$ leads to the same expression with δ^+ being replaced by δ^-. As Lemma 4.2 shows, the functions δ^+ and δ^- agree everywhere except at 1 and 2; this is the reason for $2c_2 > C_2$.

4.2 Four lemmas

Each of the following lemmas plays a crucial rôle in the proof of Theorem 2.2. In fact, in spite of its simplicity, Lemma 4.1 turns out to be particularly useful in establishing Proposition 4.5: it permits a simple, yet important modification of the considered systems, allowing us to evaluate $R_3(U)$ and $R_5(U)$ (to be defined below) with the required precision (see Sect. 5 for details). The relevance of Lemma 4.2 as the source of bias was already explained in Sect. 4.1. Lemmas 4.3 and 4.4 are adapted from [30, Lemma 2 in § 2.3] and allow us to translate our problem into the enumeration of the solutions of a system of inequalities (see (4.2)).

Lemma 4.1 *(Inversion trick) Let $p, q \ge 2$ be two coprime integers. Then*

$$\mathrm{inv}_p(q) \le \frac{p}{2} \quad \textit{if and only if} \quad \mathrm{inv}_q(p) > \frac{q}{2}.$$

Proof By coprimality, there are integers a and b such that $aq + bp = 1$, where $a = \mathrm{inv}_p(q) + tp$ and $b = \mathrm{inv}_q(p) + sq$ for some integers s and t. Hence

$$\mathrm{inv}_p(q)q + \mathrm{inv}_q(p)q - qp \equiv 1 \bmod pq.$$

On the other hand, the left hand side of the above is contained in the interval $(-pq, pq)$. Hence, we conclude

$$\mathrm{inv}_p(q)q + \mathrm{inv}_q(p)p = 1 + pq,$$

from which the lemma follows. □

Lemma 4.2 *Let φ be Euler's totient function and define for every positive integer q the counting functions*

$$\delta^-(q) = \sum_{\substack{b\le q/2 \\ \gcd(b,q)=1}} 1 \quad \textit{and} \quad \delta^+(q) = \sum_{\substack{q/2<b\le q \\ \gcd(b,q)=1}} 1.$$

Then the following assertions hold:

1. $\delta^+(1) = \delta^-(2) = 1$;

2. $\delta^+(2) = \delta^-(1) = 0$;
3. $\delta^+(q) = \delta^-(q) = \varphi(q)/2$ *for* $q \geq 3$.

Proof The assertions for $q \leq 2$ are trivial to check. For $q \geq 3$ note that the sets

$$\{\, 1 \leq b \leq q/2 : \gcd(b, q) = 1 \,\} \quad \text{and} \quad \{\, q/2 < b < q : \gcd(b, q) = 1 \,\}$$

are disjoint and in bijection by means of the map $b \mapsto q - b$. As the union of both sets contains exactly $\varphi(q)$ elements, we are done. □

Lemma 4.3 *The sum $N_0(Q)$ of the lengths of the minus continued fraction expansions of the numbers a/q with $1 \leq a < q/2$, $q \leq Q$ is*

$$N_0(Q) = T_0(Q) + O(Q^2),$$

where $T_0(Q)$ denotes the number of solutions $(a_1, q_1, a_2, q_2, m, n, a, b) \in \mathbb{N}^8$ to the following system of equalities and inequalities:

$$\begin{cases} a_1 q_2 - a_2 q_1 = 1, & 1 \leq a_1 \leq q_1, \quad 1 \leq a_2 \leq q_2/2, \\ n a_2 - m a_1 = a, & n q_2 - m q_1 = b, \quad 1 \leq a < b \leq Q, \\ 1 \leq m < n, & 1 \leq q_1 < q_2. \end{cases} \tag{4.1}$$

Proof The claim follows *mutatis mutandis* from [30, pp. 1185–1186]. □

Next, discarding an acceptable number of solutions in the process, we reduce the system (4.1) to a system with four variables.

Lemma 4.4 *Let $R(Q)$ denote the number of solutions $(p, q, n, m) \in \mathbb{N}^4$ of the system*

$$\begin{cases} \gcd(p, q) = 1, & p, q \geq 1, \\ \mathrm{inv}_p(q) \leq p/2, & \\ 2 \leq nq + kp \leq Q, & 1 \leq k < n. \end{cases} \tag{4.2}$$

Then, the number $N_0(Q)$ defined as in Lemma 4.3 satisfies

$$N_0(Q) = R(Q) + O(Q^2).$$

Proof By virtue of Lemma 4.3, we only need to show that $R(Q) = T_0(Q) + O(Q^2)$. It is convenient to exclude the solutions with $q_1 = 1$ from the discussion. We claim that their number is $O(Q^2)$ and, thus, negligible. To this end, consider first all the solutions of the system (4.1) with $q_1 = 1$. The conditions in system (4.1) force that $a_1 = a_2 = q_1 = 1$ and $q_2 = 2$, reducing the system to

$$\begin{cases} n - m = a, & 2n - m = b, \\ 1 \leq a < b \leq Q, & 1 \leq m < n, \end{cases}$$

for which one easily sees that its number of solutions is $\ll Q^2$.

For the remainder of the proof we shall assume that $q_1 \geq 2$. We claim that this assumption also implies that $a_1 \leq q_1/2$. Indeed, suppose to the contrary that there was some solution to (4.1) with $q_1 \geq 2$ and $a_1 > q_1/2$. We then deduce that

$$2 = 2(a_1q_2 - a_2q_1) \geq (q_1 + 1)q_2 - 2a_2q_1 \geq (q_1 + 1)q_2 - q_2q_1 = q_2 > q_1,$$

in contradiction with $q_1 \geq 2$.

Upon reducing the equation $a_1q_2 - a_2q_1 = 1$ modulo q_1, we obtain $a_1 = \mathrm{inv}_{q_1}(q_2) + tq_1$ for some integer t. As a_1 is positive and $q_1 < q_2$, it follows that t must vanish. Hence, $a_1 = \mathrm{inv}_{q_1}(q_2)$. Consequently, $\mathrm{inv}_{q_1}(q_2) \leq q_1/2$. Now consider the system

$$\begin{cases} \gcd(q_1, q_2) = 1, & 1 \leq q_1 < q_2,\ \mathrm{inv}_{q_1}(q_2) \leq q_1/2, \\ 2 \leq nq_2 - mq_1 \leq Q, & 1 \leq m < n. \end{cases} \tag{4.3}$$

We now contend that the map Ψ sending solutions $\boldsymbol{u} = (a_1, q_1, a_2, q_2, m, n, a, b)$ of (4.1) with $q_1 \geq 2$ to solutions $\boldsymbol{v} = (q_1, q_2, m, n)$ of (4.3) (by means of dropping the entries a_1, a_2, a, and b) is a bijection. Indeed, above we have just seen that this map is well defined. To see that it is injective, suppose that $\boldsymbol{v}$ arises from some solution $\boldsymbol{u}$ of (4.1). As we have seen, $a_1 = \mathrm{inv}_{q_1}(q_2)$ is already determined by $\boldsymbol{v}$. But then, by $a_1q_2 - a_2q_1 = 1$, also a_2 is determined by $\boldsymbol{v}$. Similarly, (4.1) then yields that also a and b are determined by $\boldsymbol{v}$, showing that Ψ is injective.

To show that Ψ is also surjective, we start out with some solution $\boldsymbol{v} = (q_1, q_2, m, n)$ of (4.3) and need to exhibit some preimage of $\boldsymbol{v}$ under Ψ. As q_1 and q_2 are coprime, there exist integers a_1 and a_2 such that $a_1q_2 - a_2q_1 = 1$. Moreover, by replacing (a_1, a_2) by $(a_1 + tq_1, a_2 + tq_2)$ with an appropriate integer t, we may assume that $0 \leq a_1 < q_1$. Furthermore, define $a = na_2 - ma_1$ and $b = nq_2 - mq_1$. We now show that the octuple $\boldsymbol{u} = (a_1, q_1, a_2, q_2, m, n, a, b)$ is the desired preimage $\boldsymbol{v}$ under Ψ. We have shown above that $a_1 = \mathrm{inv}_{q_1}(q_2)$. Similarly, by reducing $a_1q_2 - a_2q_1 = 1$ modulo q_2, we find that $a_2 = t_2q_2 - \mathrm{inv}_{q_2}(q_1)$ for some integer t_2. We claim that $t_2 = 1$. To see this, first observe that

$$a_1q_2 - (q_2 - \mathrm{inv}_{q_2}(q_1))q_1 \equiv a_1q_2 - a_2q_1 = 1 \mod q_1q_2. \tag{4.4}$$

From (4.3) we see that $a_1 = \mathrm{inv}_{q_1}(q_2) \leq q_1/2$ and Lemma 4.1 shows that $\mathrm{inv}_{q_2}(q_1) > q_2/2$. Therefore,

$$a_1q_2 - (q_2 - \mathrm{inv}_{q_2}(q_1))q_1 \begin{cases} > q_1q_2/2 - (q_2 - q_2/2)q_1 = 0, \\ < q_1q_2. \end{cases} \tag{4.5}$$

Upon combining (4.4) and (4.5) we infer that the left hand side of (4.5) is equal to one and this shows that $a_2 = q_2 - \mathrm{inv}_{q_2}(q_1)$, as claimed. In particular, we have $a_2 < q_2/2$. Moreover (4.3) shows that $b \leq Q$. It remains to show that $a < b$. We have

$$q_1a = q_1(na_2 - ma_1) = n(a_1q_2 - 1) - ma_1q_1 = a_1(nq_2 - mq_1) - n = a_1b - n.$$

Using $a_1 \leq q_1$, this shows that $a < b$. We conclude that Ψ is surjective.

Finally, we transform the system (4.3) into the system (4.2) by changing the variables slightly by means of the following map:

$$\{\text{solutions } (q_1, q_2, m, n) \text{ of (4.3)}\} \xrightarrow{1:1} \{\text{solutions } (p, q, k, n) \text{ of (4.2)}\},$$
$$(q_1, q_2, m, n) \longmapsto (q_1, q_2 - q_1, n - m, m).$$

This is easily checked to be a bijection; we omit the details. □

4.3 Proof of Theorem 2.2

In view of Lemma 4.4, it suffices to count the number of solutions of the system

$$\begin{cases} \gcd(p, q) = 1, & p, q \geq 1, \\ \mathrm{inv}_p(q) \leq p/2, & \\ 2 \leq nq + kp \leq Q, & 1 \leq k < n, \end{cases} \tag{4.6}$$

with an error term of size $O(Q^2)$. The reader may notice the similarity between the system (4.6) and the system [30, Eq. (42)]: they are almost identical, up to the additional constraints concerning coprimality and modular inversion. Set $U = Q^{1/2}$ and consider the following five cases:

- $p \leq q \leq U$; ('Case 1')
- $p \leq q, U < q$; ('Case 2')
- $q < p \leq U$; ('Case 3')
- $q < p, U < p, n \leq U$; ('Case 4')
- $q < p, U < p, U < n$. ('Case 5')

Those cases are exactly the five cases appearing in [30]. The following proposition provides us the asymptotic number of solutions for each single case.

Proposition 4.5 *Suppose that $1 \leq i \leq 5$ and let $R_i(U)$ denote the number of solutions to the system (4.6) subject to the additional constraint that 'Case i' be satisfied. Then we have*

1. $R_1(U) = \dfrac{\log 2}{4\zeta(2)} U^4 \log U + O(U^4)$,
2. $R_2(U) = \dfrac{\log 2}{4\zeta(2)} U^4 \log U + O(U^4)$,
3. $R_3(U) = \dfrac{U^4 (\log U)^2}{8\zeta(2)} + \dfrac{U^4 \log U}{4\zeta(2)} \left(\gamma - \dfrac{\zeta'(2)}{\zeta(2)} + \dfrac{3\zeta(2)}{4} - \log 2 \right) + O(U^4)$,
4. $R_4(U) = \dfrac{U^4 (\log U)^2}{8\zeta(2)} + \dfrac{U^4 \log U}{4\zeta(2)} (\gamma - \log 2) + O(U^4)$,
5. $R_5(U) = \dfrac{U^4}{4\zeta(2)} (\log U)^2 + \dfrac{U^2}{2\zeta(2)} \left(\gamma - \dfrac{\zeta'(2)}{2\zeta(2)} - \dfrac{3}{2} + \dfrac{3\zeta(2)}{8} \right) \log U + O(U^4)$.

The proof of Proposition 4.5 is the most technical part of the paper. We postpone it until Sect. 5.

Assuming the conclusion of Proposition 4.5 for the moment, we are now in a position to finish the *proof of Theorem* 2.2. Indeed, by the above, we find that the number of solutions of the system (4.6) is equal to

$$\frac{U^4}{2\zeta(2)}(\log U)^2 + \frac{U^4}{2\zeta(2)}\left(2\gamma - \frac{\zeta'(2)}{\zeta(2)} - \frac{3}{2} + \frac{3\zeta(2)}{4}\right)\log U + O(U^4).$$

Substituting $U = Q^{1/2}$, we conclude for real numbers $Q > 0$ which are not squares that

$$N_0(Q) = \frac{Q^2}{8\zeta(2)}(\log Q)^2 + \frac{Q^2}{4\zeta(2)}\left(2\gamma - \frac{\zeta'(2)}{\zeta(2)} - \frac{3}{2} + \frac{3\zeta(2)}{4}\right)\log Q + O(Q^2), \tag{4.7}$$

where $N_0(Q)$ is the quantity described in Lemma 4.3. To obtain the same result in case Q is a square, it suffices to notice that the asymptotic formula for $N_0(Q + 1/2)$ matches (4.7) up to an error of order $O(Q \log Q)$. To finish the proof, we still have to restrict to the set $\mathscr{F}_0(Q)$. To this end, notice that by Möbius inversion we have

$$\begin{aligned}\sum_{x\in\mathscr{F}_0(Q)} \ell(x) &= \sum_{\substack{b\le Q \\ \gcd(a,b)=1}} \sum_{a<b/2} \ell\left(\frac{a}{b}\right) = \sum_{d\le Q} \mu(d) \sum_{b\le Q/d} \sum_{a<b/2} \ell\left(\frac{a}{b}\right) \\ &= \sum_{d\le Q} \mu(d) N_0\left(\frac{Q}{d}\right).\end{aligned}$$

Hence, we deduce from Lemma A.3 and (4.7) that

$$\sum_{x\in\mathscr{F}_0(Q)} \ell(x) = \frac{Q^2(\log Q)^2}{8\zeta(2)^2} + \frac{Q^2\log Q}{4\zeta(2)^2}\left(2\gamma - \frac{3}{2} - 2\frac{\zeta'(2)}{\zeta(2)} + \frac{3\zeta(2)}{4}\right) + O(Q^2).$$

This concludes the proof of Theorem 2.2. □

5 Proof of Proposition 4.5

As mentioned in Sect. 4.3, we count the solutions of (4.6) in five different cases which are exactly those considered by Zhabitskaya with the additional restrictions on coprimality and modular inversion. Therefore, in what follows we often refer to the proof of [30, Theorem 2] as it contains several estimates which we employ directly here to simplify our exposition.

Case 1

We count the number of solutions $R_1(U)$ of

$$\begin{cases} \gcd(p,q)=1, & 1 \le p \le q \le U, \\ \mathrm{inv}_p(q) \le p/2, & \\ 2 \le nq+kp \le U^2, & 1 \le k < n. \end{cases} \tag{5.1}$$

If p and q are fixed, then the number of solutions of the above system with respect to the various $1 \le k < n$ has been shown in [30, (45)] to be equal to

$$\Sigma(p,q) := \frac{U^4}{2q(p+q)} + E(U,p,q),$$

where $E(U,p,q)$ is given explicitly in [30, (45)]. Thus, the number of solutions of (5.1) is equal to

$$\sum_{\substack{q\le U \\ \gcd(p,q)=1 \\ \mathrm{inv}_p(q)\le p/2}} \sum_{p\le q} \Sigma(p,q) = \frac{U^4}{2} \sum_{\substack{p\le U \\ \gcd(p,q)=1 \\ \mathrm{inv}_p(q)\le p/2}} \sum_{p\le q\le U} \frac{1}{q(p+q)} + O\Bigg(\sum_{q\le U} \sum_{p\le q} E(U,p,q) \Bigg). \tag{5.2}$$

The error term above has been proved in [30, (45)–(47)] to be $O(U^3)$. It remains to compute the first double sum in the right-hand side of (5.2). We deal with the inner sum over q first. To this end, we set

$$f(x) = \frac{1}{x(p+x)}, \quad g(x) = \frac{\varphi(p)}{2p}(x-p) \quad \text{and} \quad M(x) = \frac{x}{p^{1/2-\epsilon}}.$$

Then Lemmas A.2 and A.1 yield that

$$\begin{aligned} \sum_{\substack{p\le q\le U \\ \gcd(p,q)=1 \\ \mathrm{inv}_p(q)\le p/2}} \frac{1}{q(p+q)} &= \frac{\varphi(p)}{2p} \int_p^U \frac{\mathrm{d}x}{x^2+xp} \\ &\quad + O_\epsilon\Bigg(\frac{1}{p^{3/2-\epsilon}} + \int_p^U \frac{x(2x+p)}{p^{1/2-\epsilon}(x^2+xp)^2}\,\mathrm{d}x \Bigg) \\ &= \frac{\varphi(p)}{2p^2} \int_p^U \left(\frac{1}{x} - \frac{1}{x+p} \right) \mathrm{d}x + O_\epsilon\Big(p^{-3/2+\epsilon} \Big) \\ &= \frac{\varphi(p)}{2p^2} \log 2 + O(U^{-1}) + O_\epsilon\Big(p^{-3/2+\epsilon} \Big). \end{aligned}$$

We now take $\epsilon = 1/3$ (any $\epsilon < 1/2$ would do) and sum the above terms over $p \le U$. Our choice of ϵ ensures that the sum over the error terms remains bounded. In view of Lemma A.5 (3), we conclude that

$$\sum_{\substack{p\le U\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\sum_{p\le q\le U}\frac{1}{q(q+p)}=\frac{\log 2}{2}\sum_{p\le U}\frac{\varphi(p)}{p^2}+O(1)=\frac{\log 2}{2\zeta(2)}\log U+O(1). \tag{5.3}$$

For later use, observe also that the relation

$$\sum_{\substack{q<U\\ \gcd(p,q)=1\\ \mathrm{inv}_q(p)>q/2}}\sum_{q<p\le U}\frac{1}{p(q+p)}=\frac{\log 2}{2\zeta(2)}\log U+O(1) \tag{5.4}$$

can be derived in the same way as relation (5.3) was. Finally, upon combining (5.2) with (5.3), we conclude that

$$R_1(U)=\frac{\log 2}{4\zeta(2)}U^4\log U+O(U^4).$$

Case 2

We count the number of solutions $R_2(U)$ of

$$\begin{cases}\gcd(p,q)=1, & 1\le p\le q,\ U<q,\\ \mathrm{inv}_p(q)\le p/2,\\ 2\le nq+kp\le U^2, & 1\le k<n.\end{cases} \tag{5.5}$$

In this case the inequalities $n\le U^2/q<U$ hold as well.

Let $\mathcal{C}:=\{(p,q)\in\mathbb{N}^2:\gcd(p,q)=1\}$ and fix k and n. If $n+k\le U$, then the domain of solutions of the above system can be expressed as the lattice[5]

$$S_1(n,k)=\left\{(p,q)\in\mathcal{C}:1\le p\le\frac{U^2}{n+k},\ U<q\le\frac{U^2-kp}{n},\ \mathrm{inv}_p(q)\le\frac{p}{2}\right\}$$

without the points of the lattice

$$S_2(n,k)=\left\{(p,q)\in\mathcal{C}:U<p\le\frac{U^2}{n+k},\ U<q\le p,\ \mathrm{inv}_p(q)\le\frac{p}{2}\right\}.$$

The number of integer points in $S_1(n,k)$ is equal to

$$\Sigma_1(n,k):=\sum_{p\le U^2/(n+k)}A_p\left(U,\frac{U^2-kp}{n}\right),$$

[5] The interested reader can have a look at the figures in [30, p. 1200] for a visual representation of those regions. The domain is the same but we restrict to its intersections with modular hyperbolas.

where $A_p(y,x)$ is defined in Lemma A.1. Therefore, it follows that

$$\begin{aligned}\Sigma_1(n,k) &= \sum_{p\le U^2/(n+k)} \frac{\varphi(p)}{2p}\left(\frac{U^2}{n}-U-p\frac{k}{n}\right)+\\ &\quad+\sum_{p\le U^2/(n+k)} O_\epsilon\left(\frac{U^2-kp-nU+np}{np^{1/2-\epsilon}}\right)\\ &=: S_{11}+S_{12}.\end{aligned}\tag{5.6}$$

Regarding the first sum, Lemma A.5 (1)–(2) and inequalities $k<n<U$ yield that

$$\begin{aligned}S_{11} &= \left(\frac{U^2}{n}-U\right)\left(\frac{U^2}{2\zeta(2)(n+k)}+O\left(\log\frac{U^2}{n+k}\right)\right)\\ &\quad-\frac{k}{n}\left(\frac{U^4}{4\zeta(2)(n+k)^2}+O\left(\frac{U^2}{n+k}\log\frac{U^2}{n+k}\right)\right)\\ &= \frac{U^4}{2\zeta(2)n(n+k)}-\frac{U^3}{2\zeta(2)(n+k)}-\frac{kU^4}{4\zeta(2)n(n+k)^2}+O\left(\frac{U^2}{n}\log\frac{U^2}{n+k}\right)\\ &= \frac{U^4}{4\zeta(2)n(n+k)}+\frac{U^4}{4\zeta(2)(n+k)^2}-\frac{U^3}{2\zeta(2)(n+k)}+O\left(\frac{U^2}{n}\log\frac{U^2}{n+k}\right).\end{aligned}$$

For the sum S_{12} over the error terms, we estimate

$$S_{12}\ll_\epsilon \frac{U^2-nU}{n}\left(\frac{U^2}{n+k}\right)^{1/2+\epsilon}+\frac{n-k}{n}\left(\frac{U^2}{n+k}\right)^{3/2+\epsilon}\ll_\epsilon \frac{U^{3+2\epsilon}}{n(n+k)^{1/2+\epsilon}}.$$

We work similarly for the number of integer points in $S_2(n,k)$:

$$\begin{aligned}\Sigma_2(n,k) &= \sum_{U<p\le U^2/(n+k)} A_p(U,p)\\ &= \sum_{U<p\le U^2/(n+k)}\left(\frac{\varphi(p)}{2p}(p-U)+O_\epsilon\left(\frac{2p+U}{p^{1/2-\epsilon}}\right)\right).\end{aligned}$$

Once more, Lemma A.5 (1)–(2) and inequalities $k<n<U$ yield that

$$\begin{aligned}&\sum_{U<p\le U^2/(n+k)}\frac{\varphi(p)}{2p}(p-U)=\frac{1}{4\zeta(2)}\left(\frac{U^4}{(n+k)^2}-U^2\right)+O\left(\frac{U^2}{n+k}\log\frac{U^2}{n+k}\right)\\ &-\frac{U}{2\zeta(2)}\left(\frac{U^2}{n+k}-U+O\left(\log\frac{U^2}{n+k}\right)\right)\\ &=\frac{U^4}{4\zeta(2)(n+k)^2}-\frac{U^3}{2\zeta(2)(n+k)}+O\left(U^2+\frac{U^2}{n}\log\frac{U^2}{n+k}\right),\end{aligned}$$

while for the sum of the error terms we obtain that

$$\sum_{U<p\le U^2/(n+k)} O_\epsilon\left(\frac{2p+U}{p^{1/2-\epsilon}}\right) \ll_\epsilon \sum_{U<p\le U^2/(n+k)} p^{1/2+\epsilon} \ll_\epsilon \frac{U^{3+2\epsilon}}{(n+k)^{3/2+\epsilon}}. \quad (5.7)$$

In view of (5.6)–(5.7) and Lemma A.4 (1), we conclude that the number of solutions of the system (5.5) for pairs $(n,k)\in\mathbb{N}^2$ such that $1\le k<n$ and $n+k\le U$, is equal to

$$\begin{aligned}
&\sum_{\substack{n<U\\ n+k\le U}}\sum_{k<n}(\Sigma_1(n,k)-\Sigma_2(n,k))\\
&\quad=\frac{U^4}{4\zeta(2)}\sum_{\substack{n<U\\ n+k\le U}}\sum_{k<n}\frac{1}{n(n+k)}+\sum_{\substack{n<U\\ n+k\le U}}\sum_{k<n}\left[O(U^2)+O_\epsilon\left(\frac{U^{3+2\epsilon}}{nk^{1/2+\epsilon}}\right)\right]\\
&\quad=\frac{\log 2}{4\zeta(2)}U^4\log U+O(U^4)+O_\epsilon\left(U^{7/2+2\epsilon}\right).
\end{aligned}$$

Now we consider the pairs $(n,k)\in\mathbb{N}^2$ for which $1\le k<n$ and $n+k>U$. In that case the number of solutions of the system (5.5) is smaller than the number of solutions of the same system without the restrictions on coprimality and modular inversion. This number has been computed in [30, (54)–(56)] to be $O(U^4)$. Therefore, by fixing $\epsilon\in(0,1/4)$, we obtain that

$$R_2(U)=\frac{\log 2}{4\zeta(2)}U^4\log U+O(U^4).$$

Case 3

We count the number of solutions $R_3(U)$ of

$$\begin{cases}\gcd(p,q)=1, & 1\le q<p\le U,\\ \mathrm{inv}_p(q)\le p/2,\\ 2\le nq+kp\le U^2, & 1\le k<n.\end{cases}$$

Similar as in Case 1 (see also [30, (58)–(60)]), the number of solutions of the above system is equal to

$$\frac{U^4}{2}\sum_{\substack{p\le U\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\sum_{q<p}\frac{1}{q(p+q)}+O(U^3\log U). \quad (5.8)$$

It remains to compute the double sum

$$\begin{aligned}\sum_{\substack{p\le U}}\sum_{\substack{q<p\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{q(p+q)} &= \sum_{\substack{p\le U}}\sum_{\substack{q<p\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{pq} - \sum_{\substack{p\le U}}\sum_{\substack{q<p\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{p(q+p)}\\ &= \sum_{\substack{p\le U}}\sum_{\substack{p^{1/2}\le q<p\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{pq} + \sum_{\substack{p\le U}}\sum_{\substack{q<p^{1/2}\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{pq} - \sum_{\substack{p\le U}}\sum_{\substack{q<p\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{p(q+p)}\\ &=: S_1+S_2-S_3.\end{aligned} \tag{5.9}$$

In view of Lemma 4.1 and our remark (5.4), we have that

$$S_3 = \sum_{\substack{p\le U}}\sum_{\substack{q<p\\ \gcd(p,q)=1\\ \mathrm{inv}_p(q)\le p/2}}\frac{1}{p(q+p)} = \sum_{\substack{q<U}}\sum_{\substack{q<p\le U\\ \gcd(p,q)=1\\ \mathrm{inv}_q(p)>q/2}}\frac{1}{p(q+p)} = \frac{\log 2}{2\zeta(2)}\log U + O(1). \tag{5.10}$$

Interchanging the sums in S_1 and applying Lemma 4.1 yield that

$$S_1 = \sum_{q<U}\frac{1}{q}\sum_{\substack{q<p\le V_q\\ \gcd(p,q)=1\\ \mathrm{inv}_q(p)>q/2}}\frac{1}{p},$$

where $V_q := \min\{U, q^2\}$. If we set

$$f(x)=\frac{1}{x},\quad g(x)=\frac{\varphi(q)}{2q}(x-q)\quad\text{and}\quad M(x)=\frac{x}{q^{1/2-\epsilon}},$$

then it follows from Lemmas A.1 and A.2 that

$$\begin{aligned}\sum_{\substack{q<p\le V_q\\ \gcd(p,q)=1\\ \mathrm{inv}_q(p)>q/2}}\frac{1}{p} &= \frac{\varphi(q)}{2q}\int_q^{V_q}\frac{\mathrm{d}x}{x} + O_\epsilon\left(q^{-1/2+\epsilon}+\int_q^{V_q}\frac{\mathrm{d}x}{xq^{1/2-\epsilon}}\right)\\ &= \frac{\varphi(q)}{2q}\log\frac{V_q}{q} + O_\epsilon\left(q^{-1/2+2\epsilon}\right).\end{aligned}$$

Hence,

$$S_1 = \sum_{q<U^{1/2}}\frac{\varphi(q)}{2q^2}\log q + \sum_{U^{1/2}\le q<U}\frac{\varphi(q)}{2q^2}(\log U-\log q) + \sum_{q<U}O_\epsilon\left(q^{-3/2+2\epsilon}\right).$$

We now take $\epsilon = 1/5$, so that the last sum on the right hand side converges if U is replaced by ∞ (any $\epsilon < 1/4$ would do). Therefore, in view of Lemma A.5 (3)–(4), we obtain that

$$\begin{aligned} S_1 &= \frac{(\log U)^2}{16\zeta(2)} + \frac{(\log U)^2}{4\zeta(2)} + O\left(\frac{(\log U)^2}{U}\right) - \frac{3(\log U)^2}{16\zeta(2)} + O(1) \\ &= \frac{(\log U)^2}{8\zeta(2)} + O(1). \end{aligned} \tag{5.11}$$

Lastly, we proceed with the computation of S_2 where the bias in the $\mathrm{EA}^{(\mathrm{div})}_{(\mathrm{by\text{-}excess})}$ makes its appearance for the first time. Interchanging the sums in S_2 and applying Lemma 4.1 yield that

$$\begin{aligned} S_2 &= \sum_{\substack{p\le U \\ \gcd(p,q)=1 \\ \mathrm{inv}_p(q)\le p/2}} \sum_{q<p^{1/2}} \frac{1}{pq} = \sum_{q<U^{1/2}} \frac{1}{q} \sum_{\substack{q^2<p\le U \\ \gcd(p,q)=1 \\ \mathrm{inv}_q(p)>q/2}} \frac{1}{p} \\ &= \sum_{q<U^{1/2}} \frac{1}{q} \sum_{\substack{q/2<b\le q \\ \gcd(b,q)=1}} \sum_{\substack{q^2<p\le U \\ p\equiv \mathrm{inv}_q(b) \bmod q}} \frac{1}{p}. \end{aligned} \tag{5.12}$$

Since

$$\#\{\, p \le x : p \equiv \mathrm{inv}_q(b) \bmod q \,\} = \frac{x}{q} + O(1),$$

for any coprime integers $1 \le b \le q$, we know from Lemma A.2 that

$$\sum_{\substack{q^2<p\le U \\ p\equiv \mathrm{inv}_q(b) \bmod q}} \frac{1}{p} = \frac{1}{q}\log\frac{U}{q^2} + O(q^{-2}).$$

Inserting this to (5.12) yields that

$$\begin{aligned} S_2 &= \sum_{q<U^{1/2}} \frac{1}{q} \sum_{\substack{q/2<b\le q \\ \gcd(b,q)=1}} \left[\frac{1}{q}\log\frac{U}{q^2} + O(q^{-2})\right] \\ &= \sum_{q<U^{1/2}} \left[\frac{\delta^+(q)}{q^2}\log\frac{U}{q^2} + O\left(\frac{\delta^+(q)}{q^3}\right)\right], \end{aligned} \tag{5.13}$$

where $\delta^+(q)$ is defined in Lemma 4.2.

It is clear from relation (5.13) and Lemma 4.2 where the bias occurs. In the case we are considering (for fractions less than $1/2$), the terms which correspond to $q = 1$ and $q = 2$ come with weight 1 and 0, while in the complementary case (for fractions

greater than $1/2$) where the counting function δ^+ is replaced by δ^-, they come with weight 0 and $1/2$, respectively.

Now in view of Lemma 4.2, Lemma A.5 (3)–(4) we have that

$$\begin{aligned} S_2 &= \log U + \sum_{3\le q<U^{1/2}} \frac{\varphi(q)}{2q^2}\log\frac{U}{q^2} + O(1) \\ &= \frac{1}{2}\log U - \frac{1}{8}\log U + \sum_{q<U^{1/2}} \frac{\varphi(q)}{2q^2}(\log U - 2\log q) + O(1) \\ &= \frac{3}{8}\log U + \frac{(\log U)^2}{8\zeta(2)} + \frac{\log U}{2\zeta(2)}\left(\gamma - \frac{\zeta'(2)}{\zeta(2)}\right) + O(1). \end{aligned} \tag{5.14}$$

Finally, we deduce from (5.8), (5.9), (5.10), (5.11) and (5.14) that

$$R_3(U) = \frac{U^4(\log U)^2}{8\zeta(2)} + \frac{U^4\log U}{4\zeta(2)}\left(\gamma - \frac{\zeta'(2)}{\zeta(2)} + \frac{3\zeta(2)}{4} - \log 2\right) + O(U^4).$$

Case 4

We count the number of solutions $R_4(U)$ of

$$\begin{cases} \gcd(p,q) = 1, & 1 \le q < p, \qquad U < p, \\ \mathrm{inv}_p(q) \le p/2, & \\ 2 \le nq + kp \le U^2, & 1 \le k < n \le U. \end{cases} \tag{5.15}$$

Similar as in Case 2, we fix k and n and count the number of the above system, when $n + k \le U$ and when $n + k > U$.

If $n + k \le U$, then the domain of solutions of (5.15) can be expressed as the union of the lattices[6]

$$S_1(n,k) = \left\{(p,q) \in \mathcal{C} : U < p \le \frac{U^2}{n+k},\ 1 \le q \le p,\ \mathrm{inv}_p(q) \le \frac{p}{2}\right\}$$

and

$$\begin{aligned} S_2(n,k) &= \left\{(p,q) \in \mathcal{C} : \frac{U^2}{n+k} < p \le \frac{U^2}{k},\ 1 \le q \le \frac{U^2-kp}{n},\ \mathrm{inv}_p(q) \le \frac{p}{2}\right\} \\ &= \left\{(p,q) \in \mathcal{C} : 1 \le q \le \frac{U^2}{n+k} - \theta,\ \frac{U^2}{n+k} < p \le \frac{U^2-nq}{k},\ \mathrm{inv}_q(p) > \frac{q}{2}\right\}, \end{aligned}$$

[6] See [30, p. 1206] for figures.

where we have employed above Lemma 4.1 and have introduced a parameter $\theta \in [0,1]$ which may vary. The number of integer points in $S_1(n,k)$ is equal to

$$\Sigma_1(n,k) := \sum_{U<p\le U^2/(n+k)} \sum_{\substack{b\le p/2\\ \gcd(b,p)=1}} \sum_{\substack{q\le p\\ q\equiv \mathrm{inv}_p(b) \bmod p}} 1 = \sum_{U<p\le U^2/(n+k)} \frac{\varphi(p)}{2}.$$

It follows now from Lemma A.5 (1) that

$$\begin{aligned}\Sigma_1(n,k) &= \frac{1}{4\zeta(2)}\left(\left(\frac{U^2}{n+k}\right)^2 - U^2\right) + O\left(\frac{U^2}{n+k}\log\frac{U^2}{n+k}\right)\\ &= \frac{U^4}{4\zeta(2)(n+k)^2} + O\left(U^2 + \frac{U^2}{n+k}\log\frac{U^2}{n+k}\right).\end{aligned} \tag{5.16}$$

The number of integer points in $S_2(n,k)$ is equal to

$$\Sigma_2(n,k) := \sum_{q\le U^2/(n+k)-\theta} B_q\left(\frac{U^2}{n+k}, \frac{U^2-nq}{k}\right),$$

where $B_q(y,x)$ is defined in Lemma A.1. Upon applying said lemma, we infer that

$$\Sigma_2(n,k) = S_{21} + O_\epsilon(S_{22}),$$

where

$$\begin{aligned}S_{21} &= \sum_{q\le U^2/(n+k)-\theta} \frac{\varphi(q)}{2q}\left(\frac{nU^2}{k(n+k)} - \frac{nq}{k}\right),\\ S_{22} &= \sum_{q\le U^2/(n+k)-\theta} \left(\frac{nU^2}{k(n+k)} - \frac{nq}{k} + q\right)q^{-1/2+\epsilon}.\end{aligned}$$

From Lemma A.5 (1)–(2) and inequalities $k < n < n+k \le U$ we obtain that

$$\begin{aligned}S_{21} &= \frac{nU^2}{2k(n+k)\zeta(2)}\left(\frac{U^2}{n+k} - \theta + O\left(\log\frac{U^2}{n+k}\right)\right) +\\ &\quad - \frac{n}{4k\zeta(2)}\left(\left(\frac{U^2}{n+k}-\theta\right)^2 + O\left(\frac{U^2}{n+k}\log\frac{U^2}{n+k}\right)\right)\\ &= \frac{nU^4}{4\zeta(2)k(n+k)^2} + O\left(\frac{nU^2}{k(n+k)}\log\frac{U^2}{n+k}\right).\end{aligned}$$

For the sum over the error terms we estimate

$$S_{22} \ll_\epsilon \frac{nU^2}{k(n+k)}\left(\frac{U^2}{n+k}\right)^{1/2+\epsilon} + \frac{n-k}{k}\left(\frac{U^2}{n+k}\right)^{3/2+\epsilon}$$

$$\ll_\epsilon \frac{nU^{3+2\epsilon}}{k(n+k)^{3/2+\epsilon}}. \tag{5.17}$$

In view of (5.16)–(5.17) and Lemma A.4 (2), we deduce that the number of solutions of the system (5.15) for pairs $(n,k) \in \mathbb{N}^2$ such that $1 \le k < n$ and $n+k \le U$, is equal to

$$\begin{aligned}
&\sum_{\substack{n<U \\ n+k\le U}} \sum_{k<n} (\Sigma_1(n,k) + \Sigma_2(n,k)) \\
&= \frac{U^4}{4\zeta(2)} \sum_{\substack{n<U \\ n+k\le U}} \sum_{k<n} \frac{1}{k(n+k)} + \sum_{\substack{n<U \\ n+k\le U}} \sum_{k<n} \left[O(U^2) + O_\epsilon\left(\frac{U^{3+2\epsilon}}{kn^{1/2+\epsilon}}\right)\right] \\
&= \frac{U^4(\log U)^2}{8\zeta(2)} + \frac{U^4 \log U(\gamma - \log 2)}{4\zeta(2)} + O(U^4) + O_\epsilon\left(U^{7/2+2\epsilon}\right).
\end{aligned}$$

Now we consider the pairs $(n,k) \in \mathbb{N}^2$ for which $1 \le k < n$ and $n+k > U$. In that case the number of solutions of the system (5.15) is smaller than the number of solutions of the same system without the restrictions on coprimality and modular inversion. This number has been computed in [30, (64)–(65)] to be $O(U^4)$. Therefore, by fixing $\epsilon \in (0, 1/4)$, we see that

$$R_4(U) = \frac{U^4(\log U)^2}{8\zeta(2)} + \frac{U^4 \log U}{4\zeta(2)}(\gamma - \log 2) + O(U^4).$$

Case 5

We now count the number of solutions $R_5(U)$. Employing Lemma 4.1, we find that this is the same as counting the number of solutions of the system

$$\begin{cases} \gcd(p,q) = 1, & 1 \le q < p,\ U < p, \\ \mathrm{inv}_q(p) > q/2, & \\ 2 \le nq + kp \le U^2, & 1 \le k < n,\ U < n. \end{cases} \tag{5.18}$$

Notice that the set of solutions of the above system is non-empty if, and only if, $k + q < U$.

For fixed k and q the number of solutions of (5.18) with respect to the various n and p is equal to

$$\begin{aligned}
\Sigma(k,q) &= \sum_{U<n\le (U^2-k\lceil U\rceil)/q} \sum_{\substack{q/2<b\le q \\ \gcd(b,q)=1}} \sum_{\substack{U<p\le (U^2-nq)/k \\ p\equiv \mathrm{inv}_q(b) \bmod q}} 1 \\
&= \sum_{U<n\le (U^2-k\lceil U\rceil)/q} \sum_{\substack{q/2<b\le q \\ \gcd(b,q)=1}} \left(\frac{1}{q}\left(\frac{U^2-nq}{k} - U\right) + O(1)\right)
\end{aligned}$$

$$= \sum_{U<n\le(U^2-k\lceil U\rceil)/q} \left(\frac{\delta^+(q)}{q}\left(\frac{U^2-nq}{k}-U\right)+O\left(\frac{\delta^+(q)}{q}\right)\right),$$

where $\lceil x\rceil := \lfloor x\rfloor + 1$ is the ceiling function. From Lemma 4.2 and $k < U$ we deduce that

$$\begin{aligned}\Sigma(k,1) &= \sum_{U<n\le U^2-k\lceil U\rceil}\left(\frac{U^2}{k}-U-\frac{n}{k}\right)+O(U^2)\\ &= \left(\frac{U^2}{k}-U\right)(U^2-k\lceil U\rceil-\lfloor U\rfloor)+\\ &\quad -\frac{(U^2-k\lceil U\rceil)^2+U^2-k\lceil U\rceil-\lceil U\rceil\lfloor U\rfloor}{2k}+O(U^2)\\ &= \frac{U^4}{2k}+O(U^3)\end{aligned}$$

and $\Sigma(k,2) = 0$. Here is another case where the bias in the Euclidean algorithm appears. Lastly, if $q \ge 3$, then

$$\begin{aligned}\Sigma(k,q) &= \sum_{U<n\le\left(U^2-k\lceil U\rceil\right)/q}\frac{\varphi(q)}{2q}\left(\frac{U^2}{k}-U-\frac{nq}{k}\right)+O(U^2)\\ &= \frac{\varphi(q)}{2q}\left(\frac{U^2}{k}-U\right)\left(\frac{U^2-kU+O(k)}{q}-U+O(1)\right)+O(U^2)+\\ &\quad -\frac{\varphi(q)}{4k}\left(\left(\frac{U^2-kU+O(k)}{q}+O(1)\right)^2-(U+O(1))^2\right)\end{aligned}$$

and by expanding each of the products we obtain that

$$\begin{aligned}\Sigma(k,q) &= \frac{\varphi(q)}{2q}\left(\frac{U^4}{kq}-\frac{2U^3}{q}-\frac{U^3}{k}+\frac{kU^2}{q}+O(U^2)\right)+O(U^2)+\\ &\quad -\frac{\varphi(q)}{4k}\left(\frac{U^4-2kU^3+k^2U^2}{q^2}+O\left(\frac{kU^2}{q^2}+\frac{U^2}{q}\right)-U^2+O(U)\right)\\ &= \frac{\varphi(q)U^4}{4kq^2}-\frac{\varphi(q)U^3}{2q^2}-\frac{\varphi(q)U^3}{2qk}+\frac{\varphi(q)kU^2}{4q^2}+\frac{\varphi(q)U^2}{4k}+O(U^2).\end{aligned}$$

Now we sum up over all pairs $(k, q) \in \mathbb{N}^2$ such that $k + q < U$, which is essentially equal to $R_5(U)$:

$$\sum_{\substack{k \\ k+q<U}} \sum_{q} \Sigma(k,q) = \frac{U^4}{4}\left(\sum_{\substack{k \\ k+q<U}} \sum_{q} \frac{\varphi(q)}{kq^2} + \sum_{k \le U-1} \frac{1}{k} - \sum_{k \le U-2} \frac{1}{4k}\right) + O(U^4) + \\ - \frac{U^3}{2} \sum_{\substack{k \\ k+q<U}} \sum_{q} \left(\frac{\varphi(q)}{q^2} + \frac{\varphi(q)}{qk}\right) + \frac{U^2}{4} \sum_{\substack{k \\ k+q<U}} \sum_{q} \left(\frac{\varphi(q)k}{q^2} + \frac{\varphi(q)}{k}\right).$$

Each of the above sums is already given in Lemma A.6, except of the harmonic sums

$$\sum_{k \le U-1} \frac{1}{k} - \sum_{k \le U-2} \frac{1}{4k} = \frac{3}{4} \log U + O(1)$$

which have occurred here, because the quantities $\Sigma(k, 1)$ and $\Sigma(k, 2)$ are *not* of the form

$$\frac{U^2 \varphi(q)}{4kq^2} + O(U^3), \quad q = 1, 2,$$

respectively. Thus, we conclude that

$$R_5(U) = \frac{U^4 (\log U)^2}{4\zeta(2)} + \frac{U^2 \log U}{4\zeta(2)} \left(2\gamma - \frac{\zeta'(2)}{\zeta(2)} - 3 + \frac{3\zeta(2)}{4}\right) + O(U^4).$$

Acknowledgements It is the authors' pleasure to thank the anonymous referee for spotting some inaccuracies in an earlier draft and providing helpful suggestions. During the preparation of this manuscript, the first-named author has been an associated student in the doctoral school programme 'discrete mathematics' at Graz University of Technology. MT is supported by the joint FWF–ANR project *ArithRand* (FWF I 4945-N and ANR-20-CE91-0006).

Funding Open access funding provided by Graz University of Technology. PM is supported by the Austrian Science Fund (FWF), project I-3466. AS is supported by FWF projects Y-901 and F-5512.

Declarations

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

Appendix A: Some asymptotic formulae

We start by recalling, for the reader's convenience, a special case of a classical result on the distribution of points on modular hyperbolas.

Lemma A.1 *(Points on the modular hyperbola) Let p be a positive integer and $x > y \geq 0$. Let*

$$A_p(y,x) := \sum_{\substack{y<q\leq x \\ \gcd(p,q)=1 \\ \mathrm{inv}_p(q)\leq p/2}} 1 \quad \text{and} \quad B_p(y,x) := \sum_{\substack{y<q\leq x \\ \gcd(p,q)=1 \\ \mathrm{inv}_p(q)> p/2}} 1.$$

Then, for any $\epsilon > 0$,

$$A_p(y,x) = \frac{\varphi(p)}{2p}(x-y) + O_\epsilon\left(\frac{x-y+p}{p^{1/2-\epsilon}}\right) = B_p(y,x).$$

Proof This is a consequence of a more general folklore result about points $(q, \mathrm{inv}_p(q))$ on a modular hyperbola (mod p) where both coordinates are restricted to intervals. The interested reader may consult the survey [23] (in particular, see Theorem 13 in Sect. 3.1 therein). A version with a slightly more explicit error term can be found, for instance, in [3, Lemma 1.7]. Strictly speaking, in both of the above sources, the intervals in question are restricted to have length not exceeding p. Nevertheless, the version required here easily follows from that by splitting $(y, x]$ into $\ll 1 + (x-y)/p$ intervals of length at most p. □

The next result is a version of Abel's summation formula.

Lemma A.2 *(Abel's summation formula) Let $f, g\colon [0,\infty) \to \mathbb{R}$ be continuously differentiable functions. Let $y \geq 0$ be arbitrary. Suppose that $(a_n)_{n\in\mathbb{N}}$ is a sequence of complex numbers such that the approximation*

$$\sum_{y<n\leq x} a_n = g(x) + O(M(x)),$$

holds with some continuous function $M\colon [0,\infty) \to [1,\infty)$. Then

$$\sum_{y<n\leq x} a_n f(n) = \int_y^x f(t)g'(t)\,\mathrm{d}t + O\left(\max_{t=x,y} |f(t)M(t)| + \int_y^x \left|f'(t)\right| M(t)\,\mathrm{d}t\right).$$

We also require the following lemma, which is an application of Möbius inversion.

Lemma A.3 *Let $\Psi(Q) = aQ^2(\log Q)^2 + bQ^2\log Q + O(Q^2)$. Then*

$$\sum_{d\leq Q} \mu(d)\Psi\left(\frac{Q}{d}\right) = \frac{a}{\zeta(2)}Q^2(\log Q)^2 + \frac{1}{\zeta(2)}\left(b - 2a\frac{\zeta'(2)}{\zeta(2)}\right)Q^2\log Q + O(Q^2).$$

Proof For a proof see, e.g., [30, Corollary 3]. □

We conclude with recording two technical lemmas which are used in the proof of Proposition 4.5.

Lemma A.4 *The following asymptotic formulae hold for any $U \geq 2$:*

1. $$\sum_{\substack{n<U \\ n+k\leq U}} \sum_{k<n} \frac{1}{n(n+k)} = \log 2 \log U + O(1),$$
2. $$\sum_{\substack{n<U \\ n+k\leq U}} \sum_{k<n} \frac{1}{k(n+k)} = \frac{(\log U)^2}{2} + (\gamma - \log 2) \log U + O(1).$$

Proof For a proof see [30, Lemma 9]. Notice that the formulae there are being proved for $U \notin \mathbb{N}$, but they are readily seen hold for $U \in \mathbb{N}$ as well. □

Lemma A.5 *The following asymptotic formulae hold for any $x \geq 2$:*

1. $$\sum_{q<x} \varphi(q) = \frac{x^2}{2\zeta(2)} + O(x \log x),$$
2. $$\sum_{q<x} \frac{\varphi(q)}{q} = \frac{x}{\zeta(2)} + O(\log x),$$
3. $$\sum_{q<x} \frac{\varphi(q)}{q^2} = \frac{1}{\zeta(2)} \left(\log x + \gamma - \frac{\zeta'(2)}{\zeta(2)} \right) + O\left(\frac{\log x}{x} \right),$$
4. $$\sum_{q<x} \frac{\varphi(q)}{q^2} \log q = \frac{(\log x)^2}{2\zeta(2)} + O(1).$$

Proof The first two formulae are well known and the proof of the third one can be found in [4, Corollary 4.5]. The last formula can be deduced easily from (3) and Lemma A.2. □

Lemma A.6 *The following asymptotic formulae hold for any $U \geq 2$:*

1. $$\sum_{\substack{k \\ k+q<U}} \sum_{q} \frac{\varphi(q)}{kq^2} = \frac{(\log U)^2}{\zeta(2)} + \frac{\log U}{\zeta(2)} \left(2\gamma - \frac{\zeta'(2)}{\zeta(2)} \right) + O(1),$$
2. $$\sum_{\substack{k \\ k+q<U}} \sum_{q} \frac{\varphi(q)}{q^2} = \frac{U \log U}{\zeta(2)} + O(U) = \sum_{\substack{k \\ k+q<U}} \sum_{q} \frac{\varphi(q)}{qk},$$
3. $$\sum_{\substack{k \\ k+q<U}} \sum_{q} \frac{\varphi(q)k}{q^2} = \frac{U^2 \log U}{2\zeta(2)} + O(U^2) = \sum_{\substack{k \\ k+q<U}} \sum_{q} \frac{\varphi(q)}{k}.$$

Proof They follow directly from the formulae of Lemma A.5 and the asymptotic formula of the truncated harmonic sum. □

References

1. Baladi, V., Vallée, B.: Euclidean algorithms are Gaussian. J. Number Theory **110**(2), 331–386 (2005)
2. Barkan, Ph.: Sur les sommes de Dedekind et les fractions continues finies. C. R. Acad. Sci. Paris Sér. A-B **284**(16), 923–926 (1977)
3. Boca, F.P., Cobeli, C., Zaharescu, A.: Distribution of lattice points visible from the origin. Commun. Math. Phys. **213**(2), 433–470 (2000)
4. Boca, F.P.: Products of matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and the distribution of reduced quadratic irrationals. J. Reine Angew. Math. **606**, 149–165 (2007)
5. Bykovskiĭ, V.A.: An estimate for the dispersion of lengths of finite continued fractions. Fundam. Prikl. Mat. **11**(6), 15–26 (2005)
6. Bykovskiĭ, V.A., Frolenkov, D.A.: The average length of finite continued fractions with fixed denominator. Sb. Math. **208**(5), 644–683 (2017)
7. Dedekind, R.: Erläuterung zu Den Vorstehenden Fragmenten [XXVII], In: Bernhard Riemanns Gesammelte Mathematische Werke. Dover, New York (1953)
8. Dixon, J.D.: A simple estimate for the number of steps in the Euclidean algorithm. Amer. Math. Mon. **78**, 374–376 (1971)
9. Dixon, J.D.: The number of steps in the Euclidean algorithm. J. Number Theory **2**, 414–422 (1970)
10. Frolenkov, D.A.: Asymptotic behavior of the first moment for the number of steps in Euclid's excess and deficiency algorithm. Sb. Mat. **203**(2), 143–160 (2012)
11. Girstmair, K.: On the distribution of Dedekind sums. Surv. Math. Appl. **13**, 251–263 (2018)
12. Heilbronn, H.: On the average length of a class of finite continued fractions. In: Turán, P. (ed.) Abh. Zahlentheorie Anal., zur Erinnerung an E. Landau, pp. 87–96. Plenum, New York (1968)
13. Hensley, D.: The number of steps in the Euclidean algorithm. J. Number Theory **49**(2), 142–182 (1994)
14. Hickerson, D.: Continued fractions and density results for Dedekind sums. J. reine angew. math. **290**, 113–116 (1977)
15. Ito, H.: A density result for elliptic Dedekind sums. Acta Arith. **112**(2), 199–208 (2004)
16. Knuth, D.E.: The Art of Computer Programming, vol. 2: Seminumerical Algorithms, 2nd edn. Addison-Wesley, London (1981)
17. Lochs, G.: Statistik der Teilnenner der zu den echten Brüchen gehörigen regelmäßigen Kettenbrüche. Monatsh. Math. **65**, 27–52 (1961)
18. Minelli, P.: On Diophantine approximation, a conjecture of Ito on Dedekind sums and Poissonian pair correlation of sequences. Doctoral dissertation, Graz University of Technology (2022)
19. Myerson, G.: On semi-regular finite continued fractions. Arch. Math. **48**, 420–425 (1987)
20. Perron, O.: Die Lehre Von Den Kettenbrüchen, vol. I. Elementare Kettenbrüche. B. G. Teubner Verlagsgesellschaft, Stuttgart (1954)
21. Porter, J.W.: On a theorem of Heilbronn. Mathematika **22**(1), 20–28 (1975)
22. Rademacher, H., Grosswald, E.: Dedekind Sums. AMS, Washington, D.C. (1972). The Carus Mathematical Monographs, No. 16
23. Shparlinski, I.E.: Modular hyperbolas. Jpn. J. Math. **7**(2), 235–294 (2012)
24. Ustinov, A.V.: Asymptotic behavior of the first and second moments for the number of steps in the Euclidean algorithm. Izv. Ross. Akad. Nauk Ser. Mat. **72**(5), 189–224 (2008)
25. Ustinov, A.V.: Calculation of variance in a problem from the theory of continued fractions. Mat. Sb. **198**(6), 139–158 (2007)
26. Ustinov, A.V.: On the statistical properties of finite continued fractions. J. Math. Sci. **137**(2), 186–211 (2005)
27. Vallée, B.: A unifying framework for the analysis of a class of Euclidean algorithms. In: Gonnet, G.H., Panario, D., Viola, A. (eds.) LATIN 2000: Theoretical Informatics. 4th Latin American Symposium, Punta del Este, Uruguay, April 10–14, 2000. Proceedings, pp. 343–354. Springer, Berlin (2000)
28. Vallée, B.: Dynamical analysis of a class of Euclidean algorithms. Theor. Comput. Sci. **297**(1–3), 447–486 (2003)

29. Zhabitskaya, E.N.: Mean value of sums of partial quotients of continued fractions. Math. Notes **89**(3), 450–454 (2011)
30. Zhabitskaya, E.N.: The average length of reduced regular continued fractions. Sb. Math. **200**(8), 1181–1214 (2009)