COUNTING THE NUMBER OF SOLUTIONS TO THE ERDŐS-STRAUS EQUATION ON UNIT FRACTIONS

CHRISTIAN ELSHOLTZ AND TERENCE TAO

Abstract. For any positive integer n, let $f(n)$ denote the number of solutions to the Diophantine equation $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ with x, y, z positive integers. The *Erdős-Straus conjecture* asserts that $f(n) > 0$ for every $n \geqslant 2$. To solve this conjecture, it suffices without loss of generality to consider the case when n is a prime p. In this paper we consider the question of bounding the sum $\sum_{p<N} f(p)$ asymptotically as $N \to \infty$, where p ranges over primes. Our main result establishes the asymptotic upper and lower bounds

$$N \log^2 N \ll \sum_{p \leqslant N} f(p) \ll N \log^2 N \log\log N.$$

In particular, $f(p) = O_\delta(\log^3 p \log\log p)$ for a subset of primes of density δ arbitrarily close to 1. Also, for a subset of the primes with density 1 the following lower bound holds: $f(p) \gg (\log p)^{0.549}$. These upper and lower bounds show that a typical prime has a small number of solutions to the Erdős-Straus Diophantine equation; small, when compared with other additive problems, like Waring's problem. We establish several more results on f and related quantities, for instance the bound $f(p) \ll p^{\frac{3}{5}+O(\frac{1}{\log\log p})}$ for all primes p. Eventually we prove lower bounds for the number $f_{m,k}(n)$ of solutions of $\frac{m}{n} = \frac{1}{t_1} + \cdots + \frac{1}{t_k}$,

$$\sum_{n \leqslant N} f_{m,k}(n) \gg_{m,k} N(\log N)^{2^{k-1}-1}$$

and a related result for primes.

1. Introduction

For any natural number[1] $n \in \mathbb{N}$, let $f(n)$ denote the number of solutions $(x, y, z) \in \mathbb{N}^3$ to the Diophantine equation

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \tag{1.1}$$

(we do not assume x, y, z to be distinct or in increasing order). Thus for instance

$$f(1) = 0, f(2) = 3, f(3) = 12, f(4) = 10, f(5) = 12, f(6) = 39, f(7) = 36, f(8) = 46, \ldots$$

We plot the values of $f(n)$ for $n \leqslant 1000$, and separately restricting to primes $p \leqslant 1000$.

From these graphs one might be tempted to draw conclusions, such as "$f(n) \gg n$ infinitely often", that we will refute in our investigations below.

The *Erdös-Straus conjecture* (see e.g. [20]) asserts that $f(n) > 0$ for all $n \geqslant 2$; it remains unresolved, although there are a number of partial results. The earliest references to this conjecture are papers by Erdős [14] and Obláth [44], and we draw attention to the fact that the latter paper was submitted in 1948.

Most subsequent approaches list parametric solutions, which solve the conjecture for n lying in certain residue classes. These soluble classes are either used for analytic approaches via a sieve method, or for computational verifications. For instance, it was shown by Vaughan [73] that the number of

1991 *Mathematics Subject Classification.* 11D68, 11N37 secondary: 11D72, 11N56.

[1]In this paper we consider the natural numbers $\mathbb{N} = \{1, 2, \ldots\}$ as starting from 1.

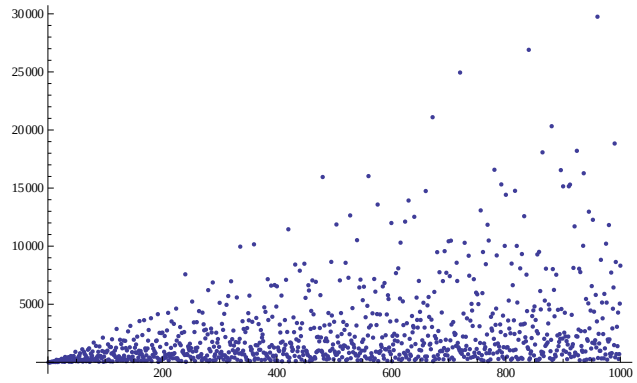

FIGURE 1. The value $f(n)$ for all $n \leqslant 1000$.

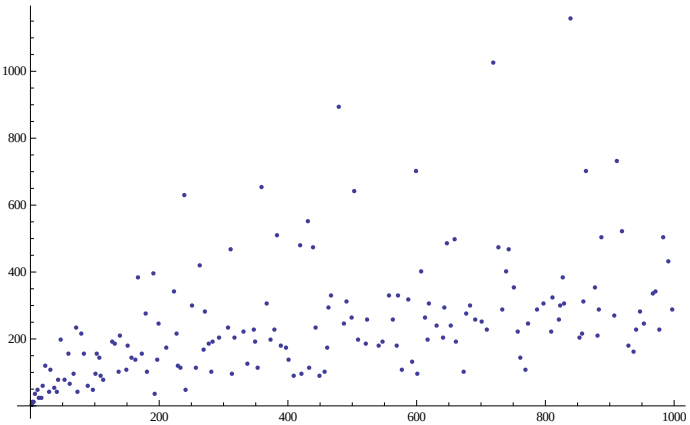

FIGURE 2. The value $f(p)$ for all primes $p \leqslant 1000$.

$n < N$ for which $f(n) = 0$ is at most $N \exp(-c \log^{2/3} N)$ for some absolute constant $c > 0$ and all sufficiently large N. (Compare also [43, 75, 34, 80] for some weaker results).

The conjecture was verified for all $n \leqslant 10^{14}$ in [70]. We list a more complete history of these computations, but there may be many further unpublished computations as well.

5000	$\leqslant 1950$	Straus, see [14]
8000	1962	Bernstein [6]
20000	$\leqslant 1969$	Shapiro, see [39]
106128	1948/9	Oblath [44]
141648	1954	Rosati [52]
10^7	1964	Yamomoto [79]
1.1×10^7	1976	Jollensten [30]
10^8	1971	Terzi[1] [72]
10^9	1994	Elsholtz & Roth[2]
10^{10}	1995	Elsholtz & Roth[2]
1.6×10^{11}	1996	Elsholtz & Roth[2]
10^{10}	1999	Kotsireas [31]
10^{14}	1999	Swett [70]

Most of these previous approaches concentrated on the question whether $f(n) > 0$ or not. In this paper we will instead study the average growth or extremal values of $f(n)$.

Since we clearly have $f(nm) \geqslant f(n)$ for any $n, m \in \mathbb{N}$, we see that to prove the Erdös-Straus conjecture it suffices to do so when n is equal to a prime p.

In this paper we investigate the *average* behaviour of $f(p)$ for p a prime. More precisely, we consider the asymptotic behaviour of the sum

$$\sum_{p \leqslant N} f(p)$$

where N is a large parameter, and p ranges over all primes less than N. As we are only interested in asymptotics, we may ignore the case $p = 2$, and focus on the odd primes p.

Let us call a solution (x, y, z) to (1.1) a *Type I solution* if n divides x but is coprime to y, z, and a *Type II solution* if n divides y, z but is coprime to x. Let $f_{\mathrm{I}}(n), f_{\mathrm{II}}(n)$ denote the number of Type I and Type II solutions respectively. By permuting the x, y, z we clearly have

$$f(n) \geqslant 3f_{\mathrm{I}}(n) + 3f_{\mathrm{II}}(n) \tag{1.2}$$

for all $n > 1$. Conversely, when p is an odd prime, it is clear from considering the denominators in the Diophantine equation

$$\frac{4}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \tag{1.3}$$

that at least one of x, y, z must be divisible by p; also, it is not possible for all three of x, y, z to be divisible by p as this forces the right-hand side of (1.3) to be at most $\frac{3}{p}$. We thus have

$$f(p) = 3f_{\mathrm{I}}(p) + 3f_{\mathrm{II}}(p) \tag{1.4}$$

for all odd primes p. Thus, to understand the asymptotics of $\sum_{p \leqslant N} f(p)$, it suffices to understand the asymptotics of $\sum_{p \leqslant N} f_{\mathrm{I}}(p)$ and $\sum_{p \leqslant N} f_{\mathrm{II}}(p)$. As we shall see, Type II solutions are somewhat easier to understand than Type I solutions, but we will nevertheless be able to control both types of solutions in a reasonably satisfactory manner.

We can now state our first main theorem[2].

Theorem 1.1 (Average value of $f_{\mathrm{I}}, f_{\mathrm{II}}$)**.** *For all sufficiently large N, one has the bounds*

$$N \log^3 N \ll \sum_{n \leqslant N} f_{\mathrm{I}}(n) \ll N \log^3 N$$

$$N \log^3 N \ll \sum_{n \leqslant N} f_{\mathrm{II}}(n) \ll N \log^3 N$$

$$N \log^2 N \ll \sum_{p \leqslant N} f_{\mathrm{I}}(p) \ll N \log^2 N \log\log N$$

$$N \log^2 N \ll \sum_{p \leqslant N} f_{\mathrm{II}}(p) \ll N \log^2 N.$$

[1]It appears that Terzi's set of soluble residue classes is correct, but that the set of checked primes in these classes is incomplete. Another reference to a calculation up to 10^8 due to N. Franceschine III (1978) (see [20, 16] and frequently restated elsewhere) only mentions Terzi's calculation, but is not an independent verification. We are grateful to I. Kotsireas for confirming this.

[2]unpublished

[2]In a previous version of this manuscript, the weaker bound $\sum_{p \leqslant N} f_{\mathrm{II}}(p) \ll N \log^2 N \log\log N$ was claimed. As pointed out subsequently by Jia [29], the argument in that previous version in fact only gave $\sum_{p \leqslant N} f_{\mathrm{II}}(p) \ll N \log^2 N \log\log^2 N$, but can be repaired to give the originally claimed bound $\sum_{p \leqslant N} f_{\mathrm{II}}(n) \ll N \log^2 N \log\log N$. These bounds are of course superceded by the results in Theorem 1.1.

Here, we use the usual asymptotic notation $X \ll Y$ or $X = O(Y)$ to denote the estimate $|X| \leqslant CY$ for an absolute constant C, and use subscripts if we wish to allow dependencies in the implied constant C, thus for instance $X \ll_\varepsilon Y$ or $X = O_\varepsilon(Y)$ denotes the estimate $|X| \leqslant C_\varepsilon Y$ for some C_ε that can depend on ε.

As a corollary of this and (1.4), we see that

$$N \log^2 N \ll \sum_{p \leqslant N} f(p) \ll N \log^2 N \log\log N.$$

From this, the prime number theorem, and Markov's inequality, we see that for any $\varepsilon > 0$, we can find a subset of A primes of relative lower density at least $1 - \varepsilon$, thus

$$\liminf_{N \to \infty} \frac{|\{p \in A : p \leqslant N\}|}{|\{p : p \leqslant N\}|} \geqslant 1 - \varepsilon, \tag{1.5}$$

such that $f(p) = O_\varepsilon(\log^3 p \log\log p)$ for all $p \in A$. Informally, a typical prime has only $O(\log^3 p \log\log p)$ solutions to the Diophantine equation (1.3); or alternatively, for any function $\xi(p)$ of p that goes to infinity as $p \to \infty$, one has $O(\xi(p) \log^3 p \log\log p)$ for all p in a subset of the primes of relative density 1. This provides an explanation as to why analytic methods (such as the circle method) appear to be insufficient to resolve the Erdős-Straus conjecture, as such methods usually only give non-trivial lower bounds on the number of solutions to a Diophantine equation in the case when the number of such solutions grows polynomially with the height parameter N.

The double logarithmic factor $\log\log N$ in the above arguments arises from technical limitations to our method (and specifically, in the inefficient nature of the Brun-Titchmarsh inequality (A.10) when applied to very short progressions), and we conjecture that it should be eliminated.

Remark 1.2. *In view of these results, one can naively model $f(p)$ as a Poisson process with intensity at least $\gg \log^3 p$. Using this probabilistic model as a heuristic, one expects any given prime to have a "probability" $1 - O(\exp(-c \log^3 p))$ of having at least one solution, which by the Borel-Cantelli lemma suggests that the Erdös-Straus conjecture is true for all but finitely many p. Of course, this is only a heuristic and does not constitute a rigorous argument. (However, one can view the results in* [73], [12], *based on the large sieve, as a rigorous analogue of this type of reasoning.)*

Remark 1.3. *From Theorem 1.1 we have the lower bound $\sum_{n \leqslant N} f(n) \gg N \log^3 N$. In fact one has the stronger bound $\sum_{n \leqslant N} f(n) \gg N \log^6 N$ (Heath-Brown, private communication) using the methods from* [23]*; see Remark 2.9 for further discussion.*

To prove Theorem 1.1, we first use some solvability criteria for Type I and Type II solutions to obtain more tractable expressions for $f_{\rm I}(p)$ and $f_{\rm II}(p)$. As we shall see, $f_{\rm I}(p)$ is essentially (up to a factor of two) the number of quadruples $(a, c, d, f) \in \mathbb{N}^4$ with $4acd = p + f$, f dividing $4a^2 d + 1$, and $acd \leqslant \frac{3p}{4}$, while $f_{\rm II}(p)$ is essentially the number of quadruples $(a, c, d, e) \in \mathbb{N}^4$ with $4acde = p + 4a^2 d + e$ and $acde \leqslant \frac{3}{2} p$. (We will systematically review the various known representations of Type I and Type II solutions in Section 2.) This, combined with standard tools from analytic number theory such as the Brun-Titchmarsh inequality and the Bombieri-Vinogradov inequality, already gives most of Theorem 1.1. The most difficult bound is the upper bounds on $f_{\rm I}$, which eventually require an upper bound for expressions of the form

$$\sum_{a \leqslant A} \sum_{b \leqslant B} \tau(kab^2 + 1)$$

for various A, B, k, where $\tau(n) := \sum_{d|n} 1$ is the number of divisors of n, and $d|n$ denotes the assertion that d divides n. By using an argument of Erdős [15], we obtain the following bound on this quantity:

Proposition 1.4 (Average value of $\tau(kab^2 + 1)$)**.** *For any $A, B > 1$, and any positive integer $k \ll (AB)^{O(1)}$, one has*

$$\sum_{a \leqslant A} \sum_{b \leqslant B} \tau(kab^2 + 1) \ll AB \log(A + B) \log(1 + k).$$

Remark 1.5. *Using the heuristic that $\tau(n) \sim \log n$ on the average (see* (A.5)*), one expects the true bound here to be $O(AB\log(A+B))$. The $\log(1+k)$ loss can be reduced (for some ranges of A, B, k, at least) by using more tools (such as the Polya-Vinogradov inequality), but this slightly inefficient bound will be sufficient for our applications.*

We prove Proposition 1.4 (as well as some variants of this estimate) in Section 7. Our main tool is a more quantitative version of a classical bound of Erdős [15] on the sum $\sum_{n\leqslant N}\tau(P(n))$ for various polynomials P, which may be of independent interest; see Theorem 7.1.

We also collect a number of auxiliary results concerning the quantities $f_i(n)$, some of which were in previous literature. Firstly, we have a vanishing property at odd squares:

Proposition 1.6 (Vanishing)**.** *For any odd perfect square n, we have $f_{\rm I}(n) = f_{\rm II}(n) = 0$.*

This observation essentially dates back to Schinzel (see [20][39], [59]) and Yamomoto (see [79]) and is an easy application of quadratic reciprocity (A.7): for the convenience of the reader, we give the proof in Section 4. A variant of this proposition was also established in [5]. Note that this does not disprove the Erdös-Straus conjecture, since the inequality (1.2) does not hold with equality on perfect squares; but it does indicate a key difficulty in attacking this conjecture, in that when showing that $f_{\rm I}(p)$ or $f_{\rm II}(p)$ is non-zero, one can only use methods that *must necessarily fail* when p is replaced by an odd square such as p^2, which already rules out many strategies (e.g. a finite set of covering congruence strategies, or the circle method).

Next, we establish some upper bounds on $f_{\rm I}(n), f_{\rm II}(n)$ for fixed n:

Proposition 1.7 (Upper bounds)**.** *For any $n\in\mathbb{N}$, one has*

$$f_{\rm I}(n) \ll n^{\frac{3}{5}+O(\frac{1}{\log\log n})}$$

and

$$f_{\rm II}(n) \ll n^{\frac{2}{5}+O(\frac{1}{\log\log n})}.$$

In particular, from this and (1.4) *one can conclude that for any prime p one has*

$$f(p) \ll p^{\frac{3}{5}+O(\frac{1}{\log\log p})}.$$

This should be compared with the recent result in [7], which gives the bound $f(n) \ll_\varepsilon n^{2/3+\varepsilon}$ for all n and all $\varepsilon > 0$. For composite n the treatment of parameters dividing n appears to be more complicated and here we concentrate on those two cases that are motivated by the Erdős-Straus equation for prime denominator.

We prove this proposition in Section 3.

The main tools here are the multiple representations of Type I and Type II solutions available (see Section 2) and the divisor bound (A.6). The values of $f(n)$ appear to fluctuate in some respects as the values of the divisor function, but behave much more regular on average. Moreover, in view of Theorem 1.1, one might also expect to have $f(n) \ll_\varepsilon n^\varepsilon$ for any $\varepsilon > 0$, but such logarithmic-type bounds on solutions to Diophantine equations seem difficult to obtain in general (Proposition 1.7 appears to be the limit of what one can obtain purely from the divisor bound (A.6) alone).

In the reverse direction, we have the following lower bounds on $f(n)$ for various sets of n:

Theorem 1.8 (Lower bounds)**.** *For infinitely many n, one has*

$$f(n) \geqslant \exp((\log 3 + o(1))\frac{\log n}{\log\log n}),$$

where $o(1)$ denotes a quantity that goes to zero as $n\to\infty$.

For any function $\xi(n)$ going to $+\infty$ as $n\to\infty$, one has

$$f(n) \geqslant \exp\left(\frac{\log 3}{2}\log\log n - O(\xi(n)\sqrt{\log\log n})\right) \gg (\log n)^{0.549}$$

for all n in a subset A of natural numbers of density 1 (thus $\frac{|A\cap\{1,\dots,N\}|}{N}\to 1$ as $N\to\infty$).

Finally, one has

$$f(p) \geqslant \exp\left((\frac{\log 3}{2} - o(1))\log\log p\right) \gg (\log p)^{0.549}$$

for all primes p in a subset B of primes of relative density 1 (thus $\frac{|\{p\in B: p\leqslant N\}|}{|\{p: p\leqslant N\}|} \to 1$ as $N \to \infty$).

As the proof shows the first two lower bounds are already valid for sums of two unit fractions. The result directly follow from the growth of certain divisor functions. An even better model for $f(n)$ is a suitable superposition of several divisor functions. The proof will be in Section 6.

Finally, we consider (following [39], [59]) the question of finding polynomial solutions to (1.1). Let us call a primitive[3] residue class $n = r \mod q$ *solvable by polynomials* if there exist polynomials $P_1(n), P_2(n), P_3(n)$ which take positive integer values for all sufficiently large n in this residue class (so in particular, the coefficients of P_1, P_2, P_3 are rational), and such that

$$\frac{4}{n} = \frac{1}{P_1(n)} + \frac{1}{P_2(n)} + \frac{1}{P_3(n)}$$

for all n. By Dirichlet's theorem[4], the primitive residue class $r \mod q$ contains arbitrarily large primes p. For each large prime p in this class, we either have one or two of the $P_1(p), P_2(p), P_3(p)$ divisible by p, as observed previously. For p large enough, note that $P_i(p)$ can only be divisible by p if there is no constant term in P_i. We thus conclude that either one or two of the $P_i(n)$ have no constant term, but not all three. Let us call the congruence *Type I solvable* if one can take exactly one of P_1, P_2, P_3 to have no constant term, and *Type II solvable* if exactly two have no constant term. Thus every solvable primitive residue class $r \mod q$ is either Type I or Type II solvable.

It is well-known (see [39]) that any primitive residue class $n = r \mod 840$ is solvable by polynomials unless r is a perfect square. On the other hand, it is also known (see [39], [59]) that a primitive congruence class $n = r \mod q$ which is a perfect square, cannot be solved by polynomials (this also follows from Proposition 1.6). The next proposition classifies all solvable primitive congruences.

Proposition 1.9 (Solvable congruences)**.** *Let $q \mod r$ be a primitive residue class. If this class is Type I solvable by polynomials, then all sufficiently large primes in this class belong to one of the following sets:*

- $\{n = -f \mod 4ad\}$*, where $a, d, f \in \mathbb{N}$ are such that $f|4a^2d + 1$.* [43]
- $\{n = -f \mod 4ac\} \cap \{n = -\frac{c}{a} \mod f\}$*, where $a, c, f \in \mathbb{N}$ are such that $(4ac, f) = 1$.*
- $\{n = -f \mod 4cd\} \cap \{n^2 = -4c^2d \mod f\}$*, where $c, d, f \in \mathbb{N}$ are such that $(4cd, f) = 1$.*
- $\{n = -\frac{1}{e} \mod 4ab\}$*, where $a, b, e \in \mathbb{N}$ are such that $e|a + b$ and $(e, 4ab) = 1$.* [1], [52]

Conversely, any residue class in one of the above four sets is solvable by polynomials.

Similarly, $q \mod r$ is Type II solvable by polynomials if and only if it is a subset of one of the following residue classes:

- $-e \mod 4ab$*, where $a, b, e \in \mathbb{N}$ are such that $e|a + b$ and $(e, 4ab) = 1$.* [1]
- $-4a^2d \mod f$*, where $a, d, f \in \mathbb{N}$ are such that $4ad|f + 1$.* [73], [52]
- $-4a^2d - e \mod 4ade$*, where $a, d, e \in \mathbb{N}$ are such that $(4ad, e) = 1$.* [43]

As indicated by the citations, many of these residue classes were observed to be solvable by polynomials in previous literature, but some of the conditions listed here appear to be new, and they form the complete list of all such classes. We prove Proposition 1.9 in Section 10.

---

[3]A residue class $r \mod q$ is *primitive* if r is coprime to q. One could also consider non-primitive congruences, but these congruences only contain finitely many primes and are thus of less interest to solving the Erdös-Straus conjecture (and if the Erdös-Straus conjecture held for a common factor of r and q, then the residue class $r \mod q$ would trivially be solvable by polynomials.

[4]One does not need the full strength of Dirichlet's theorem for this analysis, as it would suffice to work with *almost primes* p that are coprime to all small natural numbers. Alternatively, one could argue using the profinite (Furstenberg) topology on the natural numbers, but we will not adopt this viewpoint here.

Remark 1.10. *The results in this paper would also extend (with minor changes) to the more general situation in which the numerator* 4 *in* (1.3) *is replaced by some other fixed positive integer, a situation considered first by Sierpiński and Schinzel (see e.g.* [65, 73, 45, 46, 68]*).*

We will not detail all of these extensions here but in Section 11 we extend our study of the average number of solutions to the more general question on sums of k unit fractions

$$\frac{m}{n} = \frac{1}{t_1} + \frac{1}{t_2} + \cdots + \frac{1}{t_k}. \tag{1.6}$$

If $m > k \geqslant 3$, and the t_i are positive integers, then it is an open problem if for each sufficiently large n there is at least one solution. The Erdős-Straus conjecture with $m = 4, k = 3$, discussed above, is the most prominent case. If m and k are fixed, one can again establish sets of residue classes, such that 1.6 is generally soluble if n is in any of these residue classes.

The problem of classifying solutions of 1.6 has been studied by Rav [51], Sós [67] and Elsholtz [12]. Moreover Viola [74], Shen [63] and Elsholtz [13] have used a suitable subset of these solutions to give (for fixed $m > k \geqslant 3$) quantitive bounds on the number of those integers $n \leqslant N$, for which 1.6 does not have any solution.

We will focus on the case[5] *Type II solutions*, in which[6] $t_2, \dots, t_k$ are divisible by n. For given m, k, n, let $f_{m,k,\mathrm{II}}(n)$ denote the number of Type II solutions. Our main result regarding this quantity is the following lower bound on this quantity:

Theorem 1.11. *Let $m > k \geqslant 3$ be fixed. Then, for N sufficiently large, one has*

$$\sum_{n \leqslant N} f_{m,k,\mathrm{II}}(n) \gg_{m,k} N(\log N)^{2^{k-1}-1} \tag{1.7}$$

and

$$\sum_{p \leqslant N} f_{m,k,\mathrm{II}}(p) \gg_{m,k} \frac{N(\log N)^{2^{k-1}-2}}{\log\log N}. \tag{1.8}$$

Our emphasis here is on the exponential growth of the exponent. In particular, as k increases by one, the average number of solutions is roughly squared. The denominator of $\log\log N$ is present for technical reasons (due to use of the crude lower bound (A.11) on the Euler totient function), and it is likely that it could be eliminated (much as it is in the $m = 4, k = 3$ case) with additional effort.

Remark 1.12. *If we let $f_{m,k}(n)$ be the total number of solutions to* (1.6) *(not just Type II solutions), then we of course obtain as a corollary that*

$$\sum_{n \leqslant N} f_{m,k}(n) \gg_k N(\log N)^{2^{k-1}-1}.$$

We do not expect the power of the logarithm to be sharp in this case (cf. Remark 2.9). For instance, in [26] *it is shown that*

$$\sum_{n \leqslant N} f_{m,2}(n) = \left(\frac{1}{\phi(m)} + o(1)\right) N \log^2 N$$

for any fixed m.

[5]The classification of solutions that we give below also works for other divisibility patterns, but Type II solutions are the easiest to count, and so we shall restrict our attention to this case.

[6]Strictly speaking, the definition of a Type II solution here is slightly different from that discussed previously, because we do not require that t_1 is coprime to n. However, this coprimality automatic when n is prime (otherwise the right-hand side of (1.6) would only be at most k/n). For composite n, it is possible to insert this condition and still obtain the lower bound (1.7), but this would complicate the argument slightly and we have chosen not to do so here.

Note that the equation (1.6) can be rewritten as

$$\frac{1}{mt_1} + \cdots + \frac{1}{mt_k} + \frac{1}{-n} = 0,$$

which is primitive when n is prime. As a consequence, we obtain a lower bound for the number of integer points on the (generalised) Cayley surface:

Corollary 1.13. *Let $k \geqslant 3$. The number of integer points of the following generalization of Cayley's cubic surface,*

$$0 = \sum_{i=0}^{k} \frac{1}{t_i},$$

with t_i non-zero integers with $\min_i |t_i| \leqslant N$, is $\gg_k N(\log N)^{2^{k-1}-2}/\log\log N$.

Again, the double logarithmic factor should be removable with some additional effort, although the exponent $2^{k-1}-2$ is not expected to be sharp, and should be improvable also.

Part of the first author's work on ths project was supported by the German National Merit Foundation. The second author is supported by a grant from the MacArthur Foundation, by NSF grant DMS-0649473, and by the NSF Waterman award. The authors thank Nicolas Templier for many helpful comments and references. The first author is very grateful to Roger Heath-Brown for very generous advice on the subject (dating back as far as 1994). Both authors are particularly indebted to him for several remarks (including Remark 2.9), and also for contributing some of the key arguments here (such as the lower bound on $\sum_{n\leqslant N} f_{\mathrm{II}}(n)$ and $\sum_{p\leqslant N} f_{\mathrm{II}}(p)$) which have been reproduced here with permission. The first author also wishes to thank Tim Browning, Ernie Croot and Arnd Roth for discussions on the subject.

2. Representation of Type I and Type II solutions

We now discuss the representation of Type I and Type II solutions. There are many such representations in the literature (see e.g. [1], [5], [6], [43], [51], [52], [73], [76]); we will remark how each of these representations can be viewed as a form of the one given here after using describing a certain algebraic variety in coordinates.

For any non-zero complex number n, consider the algebraic surface

$$S_n := \{(x,y,z) \in \mathbb{C}^3 : 4xyz = nyz + nxz + nxy\} \subset \mathbb{C}^3.$$

Of course, when n is a natural number, $f(n)$ is nothing more than the number of $\mathbb{N}$-points $(x,y,z) \in S_n \cap \mathbb{N}^3$ on this surface.

It is somewhat inconvenient to count $\mathbb{N}$-points on S_n directly, due to the fact that x, y, z are likely to share many common factors. To eliminate these common factors, it is convenient to lift S_n to higher-dimensional varieties Σ_n^{I}, Σ_n^{II} (and more specifically, a three-dimensional variety in $\mathbb{C}^6$), which are adapted to parameterising Type I and Type II solutions respectively. This will replace the three original coordinates x, y, z by six coordinates a, b, c, d, e, f, any three of which can be used to parameterise Σ_n^I. or Σ_n^{II}. This multiplicity of parameterisations will be useful for many of the applications in this paper; rather than pick one parameterisation in advance, it is convenient to be able to pick and choose between them, depending on the situation.

We begin with the description of Type I solutions. More precisely, we define Σ_n^{I} to be the set of all sextuples $(a,b,c,d,e,f) \in \mathbb{C}^6$ which are non-zero and obey the constraints[7]

$$4abd = ne + 1 \tag{2.1}$$

$$ce = a + b \tag{2.2}$$

$$4abcd = na + nb + c \tag{2.3}$$

$$4acde = ne + 4a^2d + 1 \tag{2.4}$$

$$4bcde = ne + 4b^2d + 1 \tag{2.5}$$

$$4acd = n + f \tag{2.6}$$

$$ef = 4a^2d + 1 \tag{2.7}$$

$$bf = na + c \tag{2.8}$$

$$n^2 + 4c^2d = f(4bcd - n). \tag{2.9}$$

This is an algebraic set that can be parameterised by fixing three of the six coordinates a,b,c,d,e,f and solving for the other three coordinates. For instance, using the coordinates a,c,d, one easily verifies that

$$\Sigma_n^{\mathrm{I}} = \left\{ (a, \frac{na+c}{4acd-n}, c, d, \frac{4a^2d+1}{4acd-n}, 4acd-n) : a,c,d \in \mathbb{C}^3; 4acd \neq n \right\}$$

and similarly for the other $\binom{6}{3} - 1 = 14$ choices of three coordinates; we omit the elementary but tedious computations[8]. Thus we see that Σ_n^{I} is a three-dimensional algebraic variety. From (2.3) we see that the map

$$\pi_n^{\mathrm{I}} : (a,b,c,d,e,f) \mapsto (abdn, acd, bcd)$$

maps Σ_n^{I} to S_n. After quotienting out by the dilation symmetry

$$(a,b,c,d,e,f) \mapsto (\lambda a, \lambda b, \lambda c, \lambda^{-2} d, e, f) \tag{2.10}$$

of Σ_n^I, this map is injective.

If n is a natural number, then π_n^I clearly maps $\mathbb{N}$-points of Σ_n^I to $\mathbb{N}$-points of S_n, and if c is coprime to n, gives a Type I solution (note that abd is automatically coprime to n, thanks to (2.1)). In the converse direction, all Type I solutions arise in this manner:

Proposition 2.1 (Description of Type I solutions)**.** *Let $n \in \mathbb{N}$, and let (x,y,z) be a Type I solution. Then there exists a unique $(a,b,c,d,e,f) \in \mathbb{N}^6 \cap \Sigma_n^{\mathrm{I}}$ with $abcd$ coprime to n and a,b,c having no common factor, such that $\pi_n^{\mathrm{I}}(a,b,c,d,e,f) = (x,y,z)$.*

Proof. The uniqueness follows since π_n^{I} is injective after quotienting out by dilations. To show existence, we factor $x = ndx', y = dy', z = dz'$, where x', y', z' are coprime, then after multiplying (1.1) by $ndx'y'z'$ we have

$$4dx'y'z' = y'z' + nx'y' + nx'z'. \tag{2.11}$$

As y', z' are coprime to n, we conclude that x' divides $y'z'$, y' divides $x'z'$, and z' divides $x'y'$. Splitting into prime factors, we conclude that

$$x' = ab, y' = ac, z' = bc \tag{2.12}$$

for some natural numbers a,b,c; since x', y', z' have no common factor, a,b,c have no common factor also. As y,z were coprime to n, $abcd$ is coprime to n also.

[7]There are multiple redundancies in these constraints; to take just one example, (2.9) follows from (2.3) and (2.6). One could in fact specify Σ_n^{I} using just three of these nine constraints if desired. However, this redundancy will be useful in the sequel, as we will be taking full advantage of all nine of these identities.

[8]In a few cases, for instance when using c,d,e as coordinates, one may need to solve some quadratic equations to obtain the remaining variables, so that one may have two points in Σ_n^{I}, rather than one, associated to each triple of coordinates.

Substituting (2.12) into (2.11) we obtain (2.3), which in particular implies (as c is coprime to n) that c divides $a+b$. If we then set $e := \frac{a+b}{c}$ and $f := 4acd - n = \frac{na+c}{b}$, then e, f are natural numbers, and we obtain the other identities (2.1)-(2.9) by routine algebra. By construction we have $\pi_n^{\mathrm{I}}(a,b,c,d,e,f) = (x,y,z)$, and the claim follows. □

In particular, for fixed n, a Type I solution exists if and only if there is an $\mathbb{N}$-point (a,b,c,d,e,f) of Σ_n^{I} with $abcd$ coprime to n (the requirement that a,b,c have no common factor can be removed using the symmetry (2.10)). By parameterising Σ_n^{I} using three or four of the six coordinates, we recover some of the known characterisations of Type I solvability:

Proposition 2.2. *Let n be a natural number. Then the following are equivalent:*

- *There exists a Type I solution (x,y,z).*
- *There exists $a,b,e \in \mathbb{N}$ with $e|a+b$ and $4ab|ne+1$.* [1]
- *There exists $a,b,c,d \in \mathbb{N}$ such that $4abcd = na+nb+c$ with c coprime to n.* [6]
- *There exist $a,c,d,e \in \mathbb{N}$ such that $ne+1 = 4ad(ce-a)$ with c coprime to n.* [52, 39]
- *There exist $a,c,d,f \in \mathbb{N}$ such that $n = 4acd - f$ and $f|4a^2d+1$, with c coprime to n.* [43]
- *There exist b,c,d,e with $ne = (4bcde-1) - 4b^2d$ and c coprime to n.* [5]

The proof of this proposition is routine and is omitted.

Remark 2.3. *Type I solutions (x,y,z) have the obvious reflection symmetry $(x,y,z) \mapsto (x,z,y)$. With* (2.6) *and* (2.9) *the corresponding symmetry for Σ_n^{I} is given by*

$$(a,b,c,d,e,f) \mapsto \left(b,a,c,d,e,\frac{n^2+4c^2d}{f}\right).$$

We will typically only use the Σ_n^{I} parameterisation when $y \leqslant z$ (or equivalently when $a \leqslant b$), in order to keep the sizes of various parameters small.

Remark 2.4. *If we consider $\mathbb{N}$-points (a,b,c,d,e,f) of Σ_n^{I} with $a=1$, they can be explicitly parameterised as*

$$\left(1, ce-1, c, \frac{ef-1}{4}, e, f\right)$$

where e,f are natural numbers with $ef = 1 \mod 4$ and $n = cef - c - f$. This shows that any n of the form $cef-c-f$ with $ef = 1 \mod 4$ solves the Erdős-Straus conjecture, an observation made in [5]. *However, this is a relatively small set of solutions (corresponding to roughly $\log^2 n$ solutions for a given n on average, rather than $\log^3 n$), due to the restriction $a=1$. Nevertheless, in* [5] *it was verified that all primes $p = 1 \mod 4$ with $p \leqslant 10^{10}$ were representable in this form.*

Now we turn to Type II solutions. Here, we replace Σ_n^{I} by the variety Σ_n^{II}, as defined the set of all sextuples $(a,b,c,d,e,f) \in \mathbb{C}^6$ which are non-zero and obey the constraints

$$4abd = n + e \tag{2.13}$$

$$ce = a + b \tag{2.14}$$

$$4abcd = a + b + nc \tag{2.15}$$

$$4acde = n + 4a^2d + e \tag{2.16}$$

$$4bcde = n + 4b^2d + e \tag{2.17}$$

$$4acd = f + 1 \tag{2.18}$$

$$ef = n + 4a^2d \tag{2.19}$$

$$bf = nc + a \tag{2.20}$$

$$4c^2dn + 1 = f(4bcd - 1). \tag{2.21}$$

This is a very similar variety to Σ_n^{I}; indeed the non-isotropic dilation

$$(a,b,c,d,e,f) \mapsto (a,b,c/n^2,dn,n^2e,f/n)$$

is a bijection from Σ_n^{I} to Σ_n^{II}. Thus, as with Σ_n^{I}, Σ_n^{II} is a three-dimensional algebraic variety in $\mathbb{C}^6$ which can be parameterised by any three of the six coordinates in (a,b,c,d,e,f). As before, many of the constraints can be viewed as redundant; for instance, (2.21) is a consequence of (2.15) and (2.18). Note that Σ_n^{II} enjoys the same dilation symmetry (2.10) as Σ_n^{I}, and also has the reflection symmetry (using (2.18) and (2.21))

$$(a,b,c,d,e,f) \mapsto \left(b,a,c,d,e,\frac{4c^2dn+1}{f}\right).$$

Analogously to π_n^{I}, we have the map $\pi_n^{\mathrm{II}} : \Sigma_n^{\mathrm{II}} \to S_n$ given by

$$\pi_n^{\mathrm{II}} : (a,b,c,d,e,f) \mapsto (abd, acdn, bcdn) \tag{2.22}$$

which is injective up to the dilation symmetry (2.10) and which, when n is a natural number, maps $\mathbb{N}$-points of Σ_n^{II} to $\mathbb{N}$-points of S_n, and when abd is coprime to n, gives Type II solutions. (Note that this latter condition is automatic when n is prime, since x,y,z cannot all be divisible by n.)

We have an analogue of Proposition 2.1:

Proposition 2.5 (Description of Type II solutions)**.** *Let $n \in \mathbb{N}$, and let (x,y,z) be a Type II solution. Then there exists a unique $(a,b,c,d,e,f) \in \mathbb{N}^6 \cap \Sigma_n^{\mathrm{II}}$ with abd coprime to n and a,b,c having no common factor, such that $\pi_n^{\mathrm{I}}(a,b,c,d,e,f) = (x,y,z)$.*

Proof. Uniqueness follows from injectivity modulo dilations of π_n^{II} as before. To show existence, we factor $x = dx', y = ndy', z = ndz'$, where x', y', z' are coprime, then after multiplying (1.1) by $ndx'y'z'$ we have

$$4dx'y'z' = ny'z' + x'y' + x'z'. \tag{2.23}$$

As x' are coprime to n, we conclude that x' divides $y'z'$, y' divides $x'z'$, and z' divides $x'y'$. Splitting into prime factors, we again obtain the representation (2.12) for some natural numbers a,b,c; since x', y', z' have no common factor, a,b,c have no common factor also. As x was coprime to n, abd is coprime to n also.

Substituting (2.12) into (2.23) we obtain (2.15), which in particular implies that c divides $a+b$. If we then set $e := \frac{a+b}{c}$ and $f := 4acd-1$, then e,f are natural numbers, and we obtain the other identities (2.13)-(2.21) by routine algebra. By construction we have $\pi_n^{\mathrm{II}}(a,b,c,d,e,f) = (x,y,z)$, and the claim follows. □

Again, we can recover some known characterisations of Type II solvability:

Proposition 2.6. *Let n be a natural number. Then the following are equivalent:*

- *There exists a Type II solution (x,y,z).*
- *There exists $a,b,e \in \mathbb{N}$ with $e|a+b$ and $4ab|n+e$, and $\frac{n+e}{4}$ coprime to n.* [1]
- *There exists $a,b,c,d \in \mathbb{N}$ such that $4abcd = a+b+nc$ with abd coprime to n.* [6, 39]
- *There exists $a,b,d \in \mathbb{N}$ with $4abd-1|b+nc$ with abd coprime to n.* [73]
- *There exist $a,c,d,e \in \mathbb{N}$ such that $n = (4acd-1)e - 4a^2d$ with $\frac{n+e}{4}$ coprime to n.* [52]
- *There exist $a,c,d,f \in \mathbb{N}$ such that $n = 4ad(ce-a) - e = e(4acd-1) - 4a^2d$ with $ad(ce-a)$ coprime to n.* [43]

Next, we record some bounds on the order of magnitude of the parameters a,b,c,d,e,f assuming that $y \leqslant z$.

Lemma 2.7. *Let $n \in \mathbb{N}$, and suppose that $(x,y,z) = \pi^{\mathrm{I}}(a,b,c,d,e,f)$ is a Type I solution such that $y \leqslant z$. Then*

$$\begin{aligned} a &\leqslant b \\ \frac{1}{4}n < acd &\leqslant \frac{3}{4}n \\ b < ce &\leqslant 2b \\ an \leqslant bf &\leqslant \frac{5}{3}an. \end{aligned}$$

If instead $(x,y,z) = \pi^{\mathrm{I}}(a,b,c,d,e,f)$ is a Type II solution such that $y \leqslant z$, then

$$\begin{aligned} a &\leqslant b \\ \frac{1}{4}n < acde &\leqslant n \\ b < ce &\leqslant 2b \\ 3acd \leqslant f &< 4acd \end{aligned}$$

Informally, the above lemma asserts that the magnitudes of the quantities (a,b,c,d,e,f) are controlled entirely by the parameters (a,c,d,f) (in the Type I case) and (a,c,d,e) (in the Type II case), with the bounds $acd \sim n, f \ll n$ in the Type I case and $acde \sim n$ in the Type II case. The constants in the bounds here could be improved slightly, but such improvements will not be of importance in our applications.

Proof. First suppose we have a Type I solution. As $y \leqslant z$, we have $a \leqslant b$. From (2.2) we then have $b < ce \leqslant 2b$, and thus from (2.8) we have

$$an \leqslant bf \leqslant an + \frac{2}{ef}bf.$$

Now, from (2.7), $ef = 1 \mod 4$. If $e = f = 1$, then from (2.2) and (2.8) we would have $b = na + c = na + a + b$, which is absurd, thus $ef \geqslant 5$. This gives $bf \leqslant \frac{5}{3}an$ as claimed. From (2.8) this implies that $c \leqslant \frac{2an}{3}$, which in particular implies that $bcd < abdn$ and so $y \leqslant z < x$. From (1.1) we conclude that

$$\frac{4}{3n} \leqslant \frac{1}{x} < \frac{4}{n}$$

which gives the bound $\frac{1}{4}n < acd \leqslant \frac{3}{4}n$ as claimed.

Now suppose we have a Type II solution. Again $a \leqslant b$ and $b < ce \leqslant 2b$. From (2.15) we have

$$nc < 4abcd \leqslant nc + 2abcd$$

and thus $\frac{n}{4} < abd \leqslant \frac{n}{2}$, which by the ce bound gives $\frac{n}{4} < acde \leqslant n$. Since $f = 4acd - 1$, we have $3acd \leqslant f < 4acd$, and the claim follows. □

Remark 2.8. *From the above bounds one can also easily deduce the following observation: if $\frac{4}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, then the largest denominator $\max(x,y,z)$ is always divisible by p. (This observation also appears in* [12]*.)*

Remark 2.9. *Propositions 2.1, 2.5 can be viewed as a special case of the classification by Heath-Brown* [23] *of primitive integer points $(x_1,x_2,x_3,x_4) \in (\mathbb{Z}\backslash\{0\})^4$ on Cayley's surface*

$$\left\{(x_1,x_2,x_3,x_4) : \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \frac{1}{x_4} = 0\right\},$$

where by "primitive" we mean that x_1,x_2,x_3,x_4 have no common factor. Note that if n,x,y,z solve (1.1)*, then $(-n,4x,4y,4z)$ is an integer point on this surface, which will be primitive when n is prime. In* [23, Lemma 1] *it is shown that such integer points (x_1,x_2,x_3,x_4) take the form*

$$x_i = \epsilon y_j y_k y_l z_{ij} z_{ik} z_{il}$$

for $\{i,j,k,l\} = \{1,2,3,4\}$*, where* $\epsilon \in \{-1,+1\}$ *is a sign, and the* y_i, z_{ij} *are non-zero integers obeying the coprimality constraints*

$$(y_i, y_j) = (z_{ij}, z_{kl}) = (y_i, z_{ij}) = 1$$

for $\{i,j,k,l\} = \{1,2,3,4\}$*, and obeying the equation*

$$\sum_{\{i,j,k,l\}=\{1,2,3,4\}} y_i z_{jk} z_{kl} z_{lj} = 0.$$

Conversely, any ϵ, y_i, z_{ij} *obeying the above conditions induces a primitive integer point on Cayley's surface. The Type I (resp. Type II) solutions correspond, roughly speaking, to the cases when one of the* z_{1i} *(resp. one of the* y_i*) in the factorisation*

$$n = x_1 = \epsilon y_2 y_3 y_4 z_{12} z_{13} z_{14}$$

are equal to $\pm n$*. The* y_i, z_{ij} *coordinates are closely related to the* (a,b,c,d,e,f) *coordinates used in this section; in* [23] *it is observed that the variety parameterised by these coordinates can be viewed as the universal torsor* [9] *of Cayley's surface.*

In [23] *it was shown that the number of integer points* (x_1,x_2,x_3,x_4) *on Cayley's surface of maximal height* $\max(|x_1|,\dots,|x_4|)$ *bounded by* N *was comparable to* $N \log^6 N$*. This is not quite the situation considered in our paper; a solution to* (1.1) *with* $n \leqslant N$ *induces an integer point* (x_1,x_2,x_3,x_4) *whose* minimal *height* $\min(|x_1|,\dots,|x_4|)$ *is bounded by* N*. Nevertheless, the results in* [23] *can be easily modified (by minor adjustments to account for the restriction that three of the* x_i *are positive, and restricting* n *to be a multiple of* 4 *to eliminate divisibility constraints) to give a* lower bound $\sum_{n \leqslant N} f(n) \gg N \log^6 N$ *for the number of such points, though it is not immediately obvious whether this lower bound can be matched by a corresponding upper bound. Nevertheless, we see that there are several logarithmic factors separating the general solution count from the Type I and Type II solution count; in particular, for generic* n*, the majority of solutions to* (1.1) *will neither be Type I nor Type II.*

We close this section with a small remark about solutions to the equation

$$\frac{m}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

for $m > 3$ and p coprime to m, namely that none of the denominators can be divisible by p^2. (We will not use this fact though in the rest of the paper.)

Proposition 2.10. *Let* $\frac{m}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ *where* $m > 3$*,* p *is a prime not dividing* m*, and* x,y,z *are natural numbers. Then none of* x,y,z *are divisible by* p*.*

Note that there are a small number of counterexamples to this proposition for $m \leqslant 3$, such as $\frac{3}{2} = \frac{1}{1} + \frac{1}{4} + \frac{1}{4}$.

Proof. We may assume that (x,y,z) is either a Type I or Type II solution (replacing 4 by m as needed). In the Type I case $(x,y,z) = (abdp, acd, bcd)$, the claim is already clear since $abcd$ is known to be coprime to p. In the Type II case $(x,y,z) = (abd, acdp, bcdp)$ it is known that abd is coprime to p, so the only remaining task is to establish that c is coprime to p also.

Suppose c is not coprime to p; then y,z are both divisible by p^2. In particular

$$\frac{1}{y} + \frac{1}{z} \leqslant \frac{2}{p^2}$$

and hence

$$\frac{m}{p} > \frac{1}{x} \geqslant \frac{m}{p} - \frac{2}{p^2}.$$

Taking reciprocals, we conclude that

$$p < mx \leqslant p(1 - \frac{2}{mp})^{-1}.$$

Bounding $(1-\varepsilon)^{-1} < 1+2\varepsilon$ when $0 < \varepsilon < 1/2$, we conclude that

$$p < mx < p + \frac{4}{m}.$$

But if $m > 4$, this forces mx to be a non-integer, a contradiction. □

3. Upper bounds for $f_i(n)$

We may now prove Proposition 1.7.

We begin with the bound for $f_{\mathrm{I}}(n)$. By symmetry we may restrict attention to Type I solutions (x,y,z) for which $y \leqslant z$. By Proposition 2.1 and Lemma 2.7, these solutions arise from sextuples $(a,b,c,d,e,f) \in \mathbb{N}^6 \cap \Sigma_n^{\mathrm{I}}$ obeying the Type I bounds in Lemma 2.7. In particular we see that

$$e \cdot f \cdot (cd)^2 \cdot ac = (acd)^2 (\frac{ce}{b})(\frac{bf}{a}) \ll n^3,$$

and so by the pigeonhole principle, at least one of e, f, cd, ac is $O(n^{3/5})$.

Suppose first that $e \ll n^{3/5}$. For fixed e, we see from (2.1) and the divisor bound (A.6) that there are $n^{O(\frac{1}{\log\log n})}$ choices for a, b, d, giving a net total of $n^{3/5+O(\frac{1}{\log\log n})}$ points in Σ_n^{I} in this case.

Similarly, if $f \ll n^{3/5}$, (2.7) and the divisor bound gives $n^{O(\frac{1}{\log\log n})}$ choices for a, d for each f, giving $n^{3/5+O(\frac{1}{\log\log n})}$ solutions. If $cd \ll n^{3/5}$, one uses (2.9) and the divisor bound to get $n^{O(\frac{1}{\log\log n})}$ choices for b, f, c, d for each choice of cd, and if $ak \ll n^{3/5}$, then (2.8) and the divisor bound gives $n^{O(\frac{1}{\log\log n})}$ choices for a, b, c, f for each fixed ak. Putting all this together (and recalling that any three coordinates in Σ_n^{I} determine the other three) we obtain the first part of Proposition 1.7.

Now we prove the bound for $f_{\mathrm{II}}(n)$, which is similar. Again we may restrict attention to sextuples $(a,b,c,d,e,f) \in \mathbb{N}^6 \cap \Sigma_n^{\mathrm{II}}$ obeying the Type II bounds in Lemma 2.7. In particular we have

$$e^2 \cdot (ad) \cdot (ac) \cdot (cd) = (acde)^2 \leqslant n^2$$

and so at least one of e, ad, ac, cd is $O(n^{2/5})$.

If $e \ll n^{2/5}$, we use (2.13) and the divisor bound to get $n^{O(\frac{1}{\log\log n})}$ choices for a, b, d for each e. If $ad \ll n^{2/5}$, we use (2.19) and the divisor bound to get $n^{O(\frac{1}{\log\log n})}$ choices for a, d, e, f for each fixed ad. If $ac \ll n^{2/5}$, we use (2.20) to get $n^{O(\frac{1}{\log\log n})}$ choices for a, c, b, f for each fixed ac. If $cd \ll n^{2/5}$, we use (2.21) and the divisor bound to get $n^{O(\frac{1}{\log\log n})}$ choices for b, c, d, f for each fixed cd. Putting all this together we obtain the second part of Proposition 1.7.

Remark 3.1. *This argument, together with the fact that a large number n can be factorised in expected $O(n^{o(1)})$ time (using, say, the quadratic sieve* [49]*), gives an algorithm to find all Type I solutions for a given n in expected time $O(n^{3/5+o(1)})$, and a algorithm to find all the Type II solutions in expected run time $O(n^{2/5+o(1)})$.*

4. Insolvability for odd squares

We now prove Proposition 1.6. Suppose for contradiction that n is an odd perfect square (in particular, $n = 1 \mod 8$) with a Type I solution. Then by Proposition 2.1, we can find an $\mathbb{N}$-point (a,b,c,d,e,f) in Σ_n^{I}.

Let q be the largest odd factor of ab. From (2.1) we have $ne + 1 = 0 \mod q$. Since n is a perfect square, we conclude that

$$\left(\frac{e}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{(q-1)/4}$$

thanks to (A.8). Since $n = 1 \mod 8$, we see from (2.1) that $e = 3 \mod 4$. By quadratic reciprocity (A.7) we thus have

$$\left(\frac{q}{e}\right) = 1.$$

On the other hand, from (2.2) we see that $ab = -a^2 \mod e$, and thus

$$\left(\frac{ab}{e}\right) = \left(\frac{-1}{e}\right) = -1$$

by (A.8). This forces $ab \neq q$, and so (by definition of q) ab is even. By (2.1), this forces $e = 7 \mod 8$, which by (A.9) implies that $\left(\frac{2}{e}\right) = 1$ and thus $\left(\frac{q}{e}\right) = \left(\frac{ab}{e}\right)$, a contradiction.

The proof in the Type II case is almost identical, using (2.13), (2.14) in place of (2.1), (2.2); we omit the details.

5. Lower bounds I

Now we prove the lower bounds in Theorem 1.1.

We begin with the lower bound

$$\sum_{n \leqslant N} f_{\mathrm{II}}(n) \gg N \log^3 N. \tag{5.1}$$

Suppose a, c, d, e are natural numbers with d square-free, e coprime to ad, $e > a$, and $acde \leqslant N/4$. Then the quantity

$$n := 4acde - e - 4a^2 d \tag{5.2}$$

is a natural number of size at most N, and $(a, ce - a, c, d, e, 4acd - 1)$ is an $\mathbb{N}$-point of $\Sigma^{\mathrm{II}}_{\mathbf{n}}$. Applying π^{II}_n, we obtain a solution

$$(x, y, z) = (a(ce - a)d, acdn, (ce - a)cdn)$$

to (1.1). We claim that this is a Type II solution, or equivalently that $a(ce - a)d$ is coprime to n. As e is coprime to ad, we see from (5.2) that n is coprime to ade, so it suffices to show that n is coprime to $b := ce - a$. But if q is a common factor of both n and b, then from the identity (2.20) (with $f = 4acd - 1$) we see that q is also a common factor of a, a contradiction. Thus we have obtained a Type II solution. Also, as d is square-free, any two quadruples (a, c, d, e) will generate different solutions[9], as the associated sextuples $(a, ce - a, c, d, e, 4acd - 1)$ cannot be related to each other by the dilation (2.10). Thus, it will suffice to show that there are $\gg N \log^3 N$ quadruples $(a, c, d, e) \in \mathbb{N}$ with d square-free, e coprime to ad, $e > a$, and $acde \leqslant N/4$. Restricting a, c, d to be at most $N^{0.1}$ (say), we see that the number of possible choices of e is $\gg \frac{N}{acd} \frac{\phi(ad)}{ad}$, where ϕ is the Euler totient function. It thus suffices to show that

$$\sum_{a,c,d \leqslant N^{0.1}} \mu^2(d) \frac{\phi(ad)}{ad} \frac{1}{adc} \gg \log^3 N,$$

where μ is the Möbius function (so $\mu^2(d) = 1$ exactly when d is square-free). Using the elementary estimate $\phi(ad) \geqslant \phi(a)\phi(d)$ and factorising, we see that it suffices to show that

$$\sum_{d \leqslant N^{0.1}} \frac{\mu(d)^2 \phi(d)}{d^2} \gg \log N. \tag{5.3}$$

But this follows from Lemma A.1.

Now we prove the lower bound

$$\sum_{n \leqslant N} f_{\mathrm{I}}(n) \gg N \log^3 N,$$

which follows by a similar method.

[9]Note the slight difference between the approach here and the approach given by Proposition 2.5, in that we use a squarefree hypothesis on d to force the injectivity of the parameterisation, whereas in Proposition 2.5 it is the coprimality of the a, b, c that is the primary source of injectivity. The reason for this change is that squarefree-ness is an easier constraint to deal with than coprimality for the purposes of obtaining asymptotics. However, this trick is only available for lower bounds and not for upper bounds, as not all Type II solutions can be associated with a squarefree d. We will generalise this trick to sums of more than three fractions in Section 11 below.

Suppose a, c, d, f are natural numbers with d square-free, f dividing $4a^2d+1$ and coprime to c, $d \geqslant f$, and $acd \leqslant N/4$. Then the quantity

$$n := 4acd - f \tag{5.4}$$

is a natural number which is at most N, and $(a, b, c, d, \frac{4a^2d+1}{f}, f)$ is an $\mathbb{N}$-point of Σ_n^{I}, where

$$b := c\frac{4a^2d+1}{f} - e = \frac{na+c}{f}.$$

Applying π_n^{I}, this gives a solution

$$(x, y, z) = (abdn, acd, bcd)$$

to (1.1), and as before the square-free nature of d ensures that each quadruple (a, c, d, f) gives a different solution. We claim that this is a Type I solution, i.e. that $abcd$ is coprime to n. As f divides $4a^2d+1$, f and with (5.4) also n is coprime to ad. As f and c are coprime by assumption, n is coprime to acd by (5.4). As $b = (na+c)/f$, we conclude that n is also coprime to b.

Thus it will suffice to show that there are $\gg N\log^3 N$ quadruples $(a, c, d, f) \in \mathbb{N}^4$ with f coprime to $2ac$, and d square-free with f dividing $4a^2d+1$, $d \geqslant f$, and $acd \leqslant N/4$.

We restrict a, c, f to be at most $N^{0.1}$. If f is coprime to $2ac$, then there is a unique primitive residue class of f such that $4a^2d+1$ is a multiple of f for all d in this class. Also, there are $\gg \frac{N}{acf}$ elements d of this residue class with $d \geqslant f$ and $acd \leqslant N/4$; a standard sieving argument shows that a positive proportion of these elements are square-free. Thus, we have a lower bound of

$$\sum_{a,c,f \leqslant N^{0.1}:(f,2ac)=1} \frac{N}{acf}$$

for the number of quadruples. Restricting f to be odd and then using the crude sieve

$$1_{(f,2ac)=1} \geqslant 1 - \sum_p 1_{p|f}1_{p|a} - \sum_p 1_{p|f}1_{p|c} \tag{5.5}$$

where p ranges over odd primes, one easily verifies that the above expression is $\gg N\log^3 N$, and the claim follows.

Now we establish the lower bound

$$\sum_{p \leqslant N} f_{\mathrm{II}}(p) \gg N\log^2 N.$$

We will repeat the proof of (5.1), but because we are now counting primes instead of natural numbers we will need to invoke the Bombieri-Vinogradov inequality at a key juncture.

Suppose a, c, d, e are natural numbers with d square-free, $a, c, d \leqslant N^{0.1}$, and e between $N^{0.6}$ and $N/4acd$ with

$$p := 4acde - e - 4a^2d \tag{5.6}$$

prime. Then p is at most N and at least $N^{0.6}$, and in particular is automatically coprime to ade (and thus $ce - a$, by previous arguments). Thus, as before, each such (a, c, d, e) gives a Type II solution for a prime $p \leqslant N$, with different quadruples giving different solutions. Thus it suffices to show that there are $\gg N\log^2 N$ quadruples (a, c, d, e) with the above properties.

Fix a, c, d. As e ranges from $N^{0.6}$ to $N/4acd$, the expression (5.6) traces out a primitive residue class modulo $4acd - 1$, omitting at most $O(N^{0.6})$ members of this class that are less than N. Thus, the number of primes of the form (5.6) for fixed acd is

$$\pi(N; 4acd - 1, -4a^2d) - O(N^{0.6}),$$

where $\pi(N;q,t)$ denotes the number of primes $p < N$ that are congruent to t mod q. We replace $\pi(N;4acd-1,-4a^2d)$ by a good approximation, and bound the error. If we set

$$D(N;q) := \max_{(a,q)=1} \left|\pi(N;q,a) - \frac{\mathrm{li}(N)}{\phi(q)}\right|$$

(as in (A.13)), where $\mathrm{li}(x) := \int_0^x \frac{dt}{\log t}$ is the logarithmic integral, the number of primes of the form (5.6) for fixed acd is at least

$$\frac{\mathrm{li}(N)}{\phi(4acd-1)} - D(N;4acd-1) - O(N^{0.6})$$

The overall contribution of those acd combinations referring to the $O(N^{0.6})$ error term is at most $O((N^{0.1})^3 N^{0.6}) = o(N\log^2 N)$, while $\mathrm{li}(N)$ is comparable to $N/\log N$, so it will suffice to show the lower bound

$$\sum_{a,c,d\leqslant N^{0.1}} \frac{\mu^2(d)}{\phi(4acd-1)} \gg \log^3 N \tag{5.7}$$

and the upper bound

$$\sum_{a,c,d\leqslant N^{0.1}} D(N;4acd-1) = o(N\log^2 N). \tag{5.8}$$

We first prove (5.7). Using the trivial bound $\phi(4acd-1) \leqslant 4acd$, it suffices to show that

$$\sum_{a,c,d\leqslant N^{0.1}} \frac{\mu^2(d)}{acd} \gg \log^3 N$$

which upon factorising reduces to showing

$$\sum_{d\leqslant N^{0.1}} \frac{\mu^2(d)}{d} \gg \log N.$$

But this follows from Lemma A.1.

Now we show (5.8). Writing $q := 4acd-1$, we can upper bound the left-hand side of (5.8) somewhat crudely by

$$\sum_{q\leqslant N^{0.3}} D(N;q)\tau(q+1)^2.$$

From divisor moment estimates (see (A.4)) we have

$$\sum_{q\leqslant N^{0.3}} \frac{\tau(q+1)^4}{q} \ll \log^{O(1)} N;$$

hence by Cauchy-Schwarz, we may bound the preceding quantity by

$$\ll \log^{O(1)} N \left(\sum_{q\leqslant N^{0.3}} qD(N;q)^2\right)^{1/2}.$$

Using the trivial bound $D(N;q) \ll N/q$, we bound this in turn by

$$\ll N^{1/2}\log^{O(1)} N \left(\sum_{q\leqslant N^{0.3}} D(N;q)\right)^{1/2}.$$

But from the Bombieri-Vinogradov inequality (A.14), we have

$$\sum_{q\leqslant N^{0.3}} D(N;q) \ll_A N\log^{-A} N$$

for any $A > 0$, and the claim (5.8) follows.

Finally, we establish the lower bound

$$\sum_{p \leqslant N} f_{\mathrm{I}}(p) \gg N \log^2 N.$$

Unsurprisingly, we will repeat many of the arguments from preceding cases. Suppose a, c, d, f are natural numbers with $a, c, f \leqslant N^{0.1}$ with $(a, c) = (2ac, f) = 1$, $N^{0.6} \leqslant d \leqslant N/4ac$, such that f divides $4a^2 d + 1$, and the quantity

$$p := 4acd - f \tag{5.9}$$

is prime. Then p is at most N and is at least $N^{0.4}$, and in particular is coprime to a, c, f; from (5.9) it is coprime to d also. This thus yields a Type I solution for p; by the coprimality of a, c, these solutions are all distinct as no two of the associated sextuples $(a, b, c, d, \frac{4a^2 d+1}{f}, f)$ can be related by (2.10). Thus it suffices to show that there are $\gg N \log^2 N$ quadruples (a, c, d, f) with the above properties.

For fixed a, c, f, the parameter d traverses a primitive congruence class modulo f, and $p = 4acd - f$ traverses a primitive congruence class modulo $4acf$, that omits at most $O(N^{0.6})$ of the elements of this class that are less than N. By (A.13), the total number of d that thus give a prime p for fixed acf is at least

$$\frac{\mathrm{li}(N)}{\phi(4acf)} - D(N; 4acf) - O(N^{0.6})$$

and so by arguing as before it suffices to show the bounds

$$\sum_{a,c,f \leqslant N^{0.1}} 1_{(a,c)=(2ac,f)=1} \frac{1}{\phi(4acf)} \gg \log^3 N$$

and

$$\sum_{a,c,f \leqslant N^{0.1}} D(N; 4acf) = o(N \log^2 N).$$

But this is proven by a simple modification of the arguments used to establish (5.8), (5.7) (the constraints $(a, c) = (2ac, f) = 1$ being easily handled by an elementary sieve such as (5.5)). This concludes all the lower bounds for Theorem 1.1.

6. Lower bounds II

Here we prove Theorem 1.8.

Proof. For any natural numbers m, n, let $g_2(m, n)$ denote the number of solutions $(x, y) \in \mathbb{N}^2$ to the Diophantine equation $\frac{m}{n} = \frac{1}{x} + \frac{1}{y}$. Since

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{x} + \frac{1}{2y} + \frac{1}{2y}$$

we conclude the crude bound $f(n) \geqslant g_2(4, n)$ for any n.

In [7, Theorem 1] it was shown that $g_2(m, n) \gg 3^s$ whenever n is the product of s distinct primes congruent to $-1 \mod m$. Since $g_2(kn) \geqslant g_2(n)$ for any k, we conclude that

$$f(n) \geqslant g_2(4, n) \geqslant \frac{3^{w_4(n)}}{2} \tag{6.1}$$

for all n, where $w_m(n)$ is the number of distinct prime factors of n that are congruent to $-1 \mod m$.

Now we prove the first part of the theorem. Let s be a large number, and let n be the product of the first s primes equal to $-1 \mod 4$, then from the prime number theorem in arithmetic progressions we have $\log n = (1 + o(1)) s \log s$, and thus $s = (1 + o(1)) \frac{\log n}{\log \log n}$. From (6.1) we then have

$$f(n) \gg \exp\left(\log 3 (1 + o(1)) \frac{\log n}{\log \log n} \right).$$

Letting $s \to \infty$ we obtain the claim.

For the second part of the theorem, we use the Turán-Kubilius inequality (Lemma A.2) to the additive function w_4. This inequality gives that

$$\sum_{n\leqslant N} |w_4(n) - \frac{1}{2}\log\log N|^2 \ll N\log\log N.$$

From this and Chebyshev's inequality (see also [71, p. 307]), we see that

$$w_4(n) \geqslant \frac{1}{2}\log\log n + O(\xi(n)\sqrt{\log\log n})$$

for all n in a density 1 subset of $\mathbb{N}$. The claim then follows from (6.1).

Now we turn to the third part of the theorem. We first deal with the case when $p = 4t-1$ is prime, then

$$\frac{4}{p} = \frac{4}{p+1} + \frac{1}{t(4t-1)}$$

which in particular implies that

$$f(p) \geqslant g_2(4, p+1)$$

and thus

$$f(p) \gg 3^{w_4(p+1)}.$$

By Lemma A.3 we know that

$$w_4(p+1) \geqslant \left(\frac{1}{2} - o(1)\right)\log\log p \tag{6.2}$$

a set of primes of relative prime density 1.

It remains to deal with those primes p congruent to 1 mod 4. Writing

$$\frac{4}{p} = \frac{1}{(p+3)/4} + \frac{3}{p(p+3)/4}$$

we see that

$$f(p) \geqslant g_2(3, p(p+3)/4) \gg 3^{w_3((p+3)/4)} \gg 3^{w_3(p+3)}.$$

It thus suffices to show that

$$w_3(p+3) \geqslant \left(\frac{1}{2} - o(1)\right)\log\log p$$

for all p in a set of primes of relative density 1. But this can be established by the same techniques used to establish (6.2).

□

7. Sums of divisor functions

Let $P : \mathbb{Z} \to \mathbb{Z}$ be a polynomial with integer coefficients, which for simplicity we will assume to be non-negative, and consider the sum

$$\sum_{n\leqslant N} \tau(P(n)).$$

In [15], Erdős established the bounds

$$N\log N \ll_P \sum_{n\leqslant N} \tau(P(n)) \ll_P N\log N \tag{7.1}$$

for all $N > 1$ and for P irreducible; note that the implied constants here can depend on both the degree and the coefficients of P. This is of course consistent with the heuristic $\tau(n) \sim \log n$ "on average". Of course, the irreducibility hypothesis is necessary as otherwise $P(n)$ would be expected to have many more divisors.

In this section we establish a refinement of the Erdős upper bound that gives a more precise description of the dependence of the implied constant on P (and with irreducibility replaced by a much weaker hypothesis), which may be of some independent interest:

Theorem 7.1 (Erdős-type bound)**.** *Let $N > 1$, let P be a polynomial with degree D and coefficients being non-negative integers of magnitude at most N^l. For any natural number m, let $\rho(m)$ be the number of roots of $P \mod m$ in $\mathbb{Z}/m\mathbb{Z}$, and suppose one has the bound*

$$\rho(p^j) \leqslant C \tag{7.2}$$

for all primes p and all $j \geqslant 1$. Then

$$N \sum_{m \leqslant N} \frac{\rho(m)}{m} \ll \sum_{n \leqslant N} \tau(P(n)) \ll_{D,l,C} N \sum_{m \leqslant N} \frac{\rho(m)}{m}.$$

Remark 7.2. *For any fixed P, one has (7.2) for some $C = C_P$ (by many applications[10] of Hensel's lemma, and treating the case of small p separately), and when P is irreducible one can use tools such as Landau's prime ideal theorem to show that $\sum_{m \leqslant N} \frac{\rho(m)}{m} \ll_P \log N$ (indeed, much more precise asymptotics are available here). Thus we see that Erdős' original result (7.1) is a corollary of Theorem 7.1. For special types of P (e.g. linear or quadratic polynomials), more precise asymptotics on $\sum_{n \leqslant N} \tau(P(n))$ are known (see e.g. [17], [18] for the linear case, and [25], [61], [36], [37], [38] for the quadratic case), but the methods used are less elementary (e.g. Kloosterman sum bounds in the linear case, and class field theory in the quadratic case), and do not cover all ranges of coefficients of P for the applications to the Erdös-Straus conjecture.*

Proof. Our argument will be based on the methods in [15]. In this proof all implied constants will be allowed to depend on D, l and C.

We begin with the lower bound, which is very easy. Clearly

$$\tau(P(n)) \geqslant \sum_{m \leqslant N : m | P(n)} 1 \tag{7.3}$$

and thus

$$\sum_{n \leqslant N} \tau(P(n)) \geqslant \sum_{m \leqslant N} \sum_{n \leqslant N : m | P(n)} 1.$$

The expression $P(n) \mod m$ is periodic in n with period m, and thus for $m \leqslant N$ one has

$$N \frac{\rho(m)}{m} \ll \sum_{n \leqslant N : m | P(n)} 1 \ll N \frac{\rho(m)}{m} \tag{7.4}$$

which gives the lower bound on $\sum_{n \leqslant N} \tau(P(n))$.

Now we turn to the upper bound, which is more difficult. We first establish a preliminary bound

$$\sum_{n \leqslant N} \tau(P(n))^2 \ll N \log^{O(1)} N \tag{7.5}$$

using an argument of Landreau [33]. Let $n \leqslant N$. By the coefficient bounds on P we have

$$P(n) \ll N^{O(1)}. \tag{7.6}$$

Using the main lemma from [33], we conclude that

$$\tau(P(n))^2 \ll \sum_{m \leqslant N : m | P(n)} \tau(m)^{O(1)}$$

[10] See [69] for more precise bounds on C in terms of quantities such as the discriminant $\Delta(P)$ of P; bounds of this type go back to Nagell [40] and Ore [48] (see also [58], [27]). One should in fact be able to establish a version of Theorem 7.1 in which the implied constant depends explicitly on the $\Delta(P)$ rather than on C by using the estimates of Henriot [24] (which build upon earlier work of Barban-Vehov [2], Daniel [10], Shiu [64], Nair [41], and Nair-Tenenbaum [42]), but we will not do so here, as we will need to apply this bound in a situation in which the discriminant may be large, but for which the bound C in (7.2) can still be taken to be small.

and thus

$$\sum_{n\leqslant N}\tau(P(n))^2 \ll \sum_{m\leqslant N}\tau(m)^{O(1)}\sum_{n\leqslant N:m|P(n)}1.$$

Using (7.2), we may crudely bound $\sum_{n\leqslant N:m|P(n)}1\leqslant\tau(m)^{O(1)}$, thus

$$\sum_{n\leqslant N}\tau(P(n))^2 \ll \sum_{m\leqslant N}\tau(m)^{O(1)}$$

and the claim then follows from Lemma A.1.

In view of (7.5) and the Cauchy-Schwarz inequality, we may discard from the n summation any subset of $\{1,\dots,N\}$ of cardinality at most $N\log^{-C'}N$ for sufficiently large C'. We will take advantage of this freedom in the sequel.

Suppose for the moment that we could reverse (7.3) and obtain the bound

$$\tau(P(n)) \ll \sum_{m\leqslant N:m|P(n)}1. \tag{7.7}$$

Combining this with (7.4), we would obtain

$$\begin{aligned}\sum_{n\leqslant N}\tau(P(n)) &\ll \sum_{m\leqslant N}\sum_{n\leqslant N:m|P(n)}1\\ &\ll \sum_{m\leqslant N}\frac{N}{m}\rho(m)\end{aligned}$$

which would give the theorem. Unfortunately, while (7.7) is certainly true when $P(n)\leqslant N^2$, it can fail for larger values of $P(n)$, and from the coefficient bounds on P we only have the weaker upper bound (7.6).

Nevertheless, as observed by Erdős, we have the following substitute for (7.7):

Lemma 7.3. *Let C' be a fixed constant. For all but at most $O(N\log^{-C'}N)$ values of n in the range $1\leqslant n\leqslant N$, either (7.7) holds, or one has*

$$\tau(P(n)) \ll O(1)^r\sum_{m\in S_r:m|P(n)}1$$

for some $2\leqslant r\ll(\log\log N)^2$, where S_r is the set of all m with the following properties:

- *m lies between $N^{1/4}$ and N.*
- *m is $N^{1/r}$-smooth (i.e. m is divisible by any prime larger than $N^{1/r}$).*
- *m has at most $(\log\log N)^2$ prime factors.*
- *m is not divisible by any prime power p^k with $p\leqslant N^{1/2}$, $k>1$, and $p^k\geqslant N^{1/8(\log\log N)^2}$.*

The point here is that the exponential loss in the $O(1)^r$ factor will be more than compensated for by the $N^{1/r}$-smooth requirement, which as we shall see gains a factor of r^{-cr} for some absolute constant $c>0$.

Proof. The claim follows from (7.7) when $P(n)\leqslant N^2$, so we may assume that $P(n)>N^2$.

We factorise $P(n)$ as

$$P(n)=p_1\dots p_J$$

where the primes $p_1\leqslant\dots\leqslant p_J$ are arranged in non-decreasing order. Let $0\leqslant j<J$ be the largest integer such that $p_1\dots p_j\leqslant N$. If $j=0$ then all prime factors of $P(n)$ are greater than N, and thus by (7.6) we have $J=O(1)$ and thus $\tau(P(n))=O(1)$, which makes the claim (7.7) trivial. Thus we may assume that $j\geqslant 1$.

Suppose first that all the primes $p_{j+1},\dots,p_J$ have size at least $N^{1/2}$. Then from (7.6) we in fact have $J=j+O(1)$, and so

$$\tau(P(n)) \ll \tau(p_1\dots p_j).$$

Note that every factor of $p_1 \dots p_j$ divides $P(n)$ and is at most N, which gives (7.7). Thus we may assume that p_{j+1}, in particular, is less than $N^{1/2}$, which forces

$$N^{1/2} < p_1 \dots p_j \leqslant N \tag{7.8}$$

and $p_j < N^{1/2}$.

Following [15], we eliminate some small exceptional sets of natural numbers n. First we consider those n for which $P(n)$ has at least $(\log\log N)^2$ distinct prime factors. For such $P(n)$, one has $\tau(P(n)) \geqslant 2^{(\log\log N)^2}$, which is asymptotically larger than any given power of $\log N$; thus by (7.5), the set of such n has size at most $O(N \log^{-C'} N)$ and can be discarded.

Next, we consider those n for which $P(n)$ is divisible by a prime power p^k with $p \leqslant N^{1/2}$, $k > 1$, and $p^k \geqslant N^{1/8(\log\log N)^2}$. By reducing k if necessary we may assume that $p^k \leqslant N$. For each p and k, there are at most $O(\frac{N}{p^k}\rho(p^k)) = O(\frac{N}{p^k})$ numbers n with $P(n)$ divisible by p^k, thanks to (7.2); thus the total number of such n is bounded by

$$\ll N \sum_{p \leqslant N^{1/2}} \sum_{j \geqslant 2 : p^j \geqslant N^{1/8(\log\log N)^2}} \frac{1}{p^j}$$

which can easily be computed to be $O(N \log^{-C'} N)$. Thus we may discard all n of this type.

After removing all such n, we must have $p_j > N^{1/8(\log\log N)^2}$. Indeed, after eliminating the exceptional n as above, $p_1 \dots p_j$ is the product of at most $(\log\log N)^2$ prime powers, each of which is bounded by $N^{1/8(\log\log N)^2}$, or is a single prime larger than $N^{1/8(\log\log N)^2}$. The former possibility thus contributes at most $N^{1/8}$ to the final product $p_1 \dots p_j$; from (7.8) we conclude that the latter possibility must occur at least once, and the claim follows.

Let r be the positive integer such that

$$N^{1/(r+1)} < p_j \leqslant N^{1/r},$$

then $2 \leqslant r \ll (\log\log N)^2$. The primes $p_{j+1}, \dots, p_J$ have size at least $N^{1/(r+1)}$, so by (7.6) we have $J = j + O(r)$, which implies that

$$\tau(P(n)) \ll O(1)^r \tau(p_1 \dots p_j).$$

As $p_1 \dots p_j$ is at least $N^{1/2}$, we have

$$\tau(p_1 \dots p_j) \leqslant 2 \sum_{m | p_1 \dots p_j ; m \geqslant N^{1/4}} 1.$$

Note that all m in the above summand lie in S_r and divide $P(n)$. The claim follows. □

Invoking the above lemma, it remains to bound

$$\sum_{m \leqslant N} \sum_{n \leqslant N : m | P(n)} 1 \quad + \quad \sum_{r=2}^{O((\log\log N)^2)} O(1)^r \sum_{m \in S_r} \sum_{n \leqslant N : m | P(n)} 1.$$

by $O(N \sum_{n \leqslant N} \frac{P(m)}{m})$. The first term was already shown to be acceptable by (7.4). For the second sum, we also apply (7.4) and bound it by

$$\ll N \sum_{r=2}^{O((\log\log N)^2)} O(1)^r \sum_{m \in S_r} \frac{\rho(m)}{m}. \tag{7.9}$$

To estimate this expression, let r, m be as in the above summation, and factor m into primes. As in the proof of Lemma 7.3, the contribution to m coming from primes less than $N^{1/8(\log\log N)^2}$ is at most $N^{1/8}$, and the primes larger than $N^{1/8(\log\log N)^2}$ that divide m are distinct. Hence, by the pigeonhole principle (as in [15]), there exists $t \geqslant 1$ with $r2^t \ll (\log\log N)^2$ such that the $N^{1/r}$-smooth number m has at least $\lfloor \frac{rt}{100} \rfloor$ distinct prime factors between $N^{1/2^{t+1}r}$ and $N^{1/2^t r}$, and can thus be factored as

$m = q_1 \dots q_{\lfloor \frac{rt}{100} \rfloor} u$ where $q_1 < \dots < q_{\lfloor \frac{rt}{100} \rfloor}$ are primes between $N^{1/2^{t+1}r}$ and $N^{1/2^t r}$, and u is an integer of size at most N. From the Chinese remainder theorem and (7.2) we have the crude bound

$$\rho(m) \ll O(1)^{rt} \rho(u)$$

and thus

$$\sum_{m \in S_r} \frac{\rho(m)}{m} \ll \sum_{t=1}^{\infty} O(1)^{rt} \frac{1}{\lfloor \frac{rt}{100} \rfloor!} \left(\sum_{N^{1/2^{t+1}r} \leqslant p \leqslant N^{1/2^t r}} \frac{1}{p} \right)^{\lfloor \frac{rt}{100} \rfloor} \sum_{u \leqslant N} \frac{\rho(u)}{u}.$$

By the standard asymptotic $\sum_{p<x} \frac{1}{p} = \log\log x + O(1)$, we have

$$\sum_{N^{1/2^{t+1}r} \leqslant p \leqslant N^{1/2^t r}} \frac{1}{p} = O(1);$$

putting this all together, we can bound (7.9) by

$$\ll \left(\sum_{r=2}^{\infty} \sum_{t=1}^{\infty} \frac{O(1)^{rt}}{\lfloor \frac{rt}{100} \rfloor!} \right) \sum_{m \leqslant N} \frac{\rho(m)}{m}$$

and the claim follows. □

We isolate a simple special case of Theorem 7.1, when the polynomial P is linear:

Corollary 7.4. *If a, b, N are natural numbers with $a, b \ll N^{O(1)}$, then*

$$\sum_{n \leqslant N} \tau(an+b) \ll \tau((a,b)) N \log N$$

where (a,b) is the greatest common divisor of a and b.

Proof. By the elementary inequality $\tau(nm) \leqslant \tau(n)\tau(m)$ we may factor out (a,b) and assume without loss of generality that a, b are coprime.

We apply Theorem 7.1 with $P(n) := an + b$. From the coprimality of a, b and elementary modular arithmetic, we see that $\rho(m) \leqslant 1$ for all m, and the claim follows. □

We may now prove Proposition 1.4 from the introduction.

Proof of Proposition 1.4. We divide into two cases, depending on whether $A \geqslant B$ or $A \leqslant B$.

First suppose that $A \geqslant B$. From Corollary 7.4 we have

$$\sum_{a \leqslant A} \tau(kab^2+1) \ll A \sum_{m \leqslant A} \frac{1}{m} \ll A \log A,$$

for each fixed $b \leqslant B$, and the claim follows on summing in B. (Note that this argument in fact works whenever $A \geqslant B^\varepsilon$ for any fixed $\varepsilon > 0$.)

Now suppose that $A \leqslant B$. For each fixed $a \in A$, we apply Theorem 7.1 to the polynomial $P_{ka}(b) := kab^2 + 1$. To do this we first must obtain a bound on $\rho_{ka}(p^j)$, where $\rho_{ka}(m)$ is the number of solutions $b \mod m$ to $kab^2 + 1 = 0 \mod m$. Clearly $\rho_{ka}(m)$ vanishes whenever m is not coprime to ka, so it suffices to consider $\rho_{ka}(p^j)$ when p does not divide ka. Then P_{ka} is quadratic, and a simple application of Hensel's lemma reveals that $\rho_{ka}(p^j) \leqslant 2$ for all prime powers p^j (the case $p = 2$, as usual, has to be treated separately). We may therefore apply Theorem 7.1 and conclude that

$$\sum_{b \leqslant B} \tau(kab^2+1) \ll B \sum_{m \leqslant B} \frac{\rho_{ka}(m)}{m}.$$

It thus suffices to show that

$$\sum_{a \leqslant A} \sum_{m \leqslant B} \frac{\rho_{ka}(m)}{m} \ll A \log B \log(1+k). \tag{7.10}$$

To control $\rho_{ka}(m)$, the obvious tool to use here is the quadratic reciprocity law (A.7). To apply this law, it is of course convenient to first reduce to the case when a and m are odd. If $m = 2^j m'$ for some odd m', then $\rho_{ka}(m) \ll \rho_{ka}(m')$, and from this it is easy to see that the bound (7.10) follows from the same bound with m restricted to be odd. Similarly, by splitting $a = 2^l a'$ and absorbing the 2^l factor into k (and dividing A by 2^l to compensate), we may assume without loss of generality that a is odd.

As previously observed, $\rho_{ka}(m)$ vanishes unless ka and m are coprime, so we may also restrict to the case $(ka, m) = 1$, where (n, m) denotes the greatest common divisor of n, m. If p is an odd prime not dividing ka, then from elementary manipulation and Hensel's lemma we see that

$$\rho_{ka}(p^j) = \rho_{ka}(p) \leqslant 1 + \left(\frac{-ka}{p}\right),$$

and thus for odd m coprime to ka we have

$$\rho_{ka}(m) \leqslant \prod_{p|m} \left(1 + \left(\frac{-ka}{p}\right)\right).$$

For odd m, not necessarily coprime to ka, we thus have

$$\rho_{ka}(m) \leqslant \prod_{p|m;(p,2ka)=1} \left(1 + \left(\frac{-ka}{p}\right)\right).$$

using the multiplicativity properties of the Jacobi symbol, one has

$$1 + \left(\frac{-ka}{p}\right) \leqslant \sum_{j:p^j|m} \left(\frac{-ka}{p^j}\right)$$

whenever $p|m$ and $(p, 2ka) = 1$, and thus

$$\rho_{ka}(m) \leqslant \prod_{p|m;(p,2ka)=1} \sum_{j:p^j|m} \left(\frac{-ka}{p^j}\right).$$

The right-hand side can be expanded as

$$\sum_{q|m;(q,2ka)=1} \left(\frac{-ka}{q}\right).$$

We can thus bound the left-hand side of (7.10) by

$$\sum_{q\leqslant B:(q,2k)=1} \sum_{a\leqslant A;(a,2q)=1} \left(\frac{-ka}{q}\right) \sum_{m\leqslant B;q|m} \frac{1}{m}.$$

The final sum is of course $\frac{\log \frac{B}{q}}{q} + O(\frac{1}{q})$. The contribution of the error term is bounded by

$$O(\sum_{q\leqslant B} \sum_{a\leqslant A} \frac{1}{q}) = O(A \log B)$$

which is acceptable, so it suffices to show that

$$\left| \sum_{q\leqslant B:(q,2k)=1} \sum_{a\leqslant A;(a,2q)=1} \left(\frac{-ka}{q}\right) \frac{\log \frac{B}{q}}{q} \right| \ll A \log B \log(1+k). \tag{7.11}$$

We first dispose of an easy contribution, when q is less than A. The expression $a \mapsto \left(\frac{-ka}{q}\right) 1_{(a,2q)=1}$ is periodic with period $2q$ and sums to zero (being essentially a quadratic character on $\mathbb{Z}/2q\mathbb{Z}$), and so[11]

[11] One could obtain better estimates and deal with somewhat larger q here by using tools such as the Polya-Vinogradov inequality, but we will not need to do so here. Similarly for the treatment of the regime $A \leqslant q \leqslant kA$.

in this case we have

$$\sum_{a\leqslant A;(a,2q)=1}\left(\frac{-ka}{q}\right)=O(q).$$

Thus the contribution of this case is bounded by

$$O\left(\sum_{q\leqslant A} q\frac{\log\frac{B}{q}}{q}\right)=O(A\log B)$$

which is acceptable.

Next, we deal with the contribution when q is between A and kA. Here we crudely bound the Jacobi symbol in magnitude by 1 and obtain a bound of

$$O(\sum_{A\leqslant q\leqslant kA}\sum_{a\leqslant A}\frac{\log B}{q})=O(A\log B\log(1+k))$$

which is acceptable.

Finally, we deal with the case when q exceeds kA. We write $k=2^m k'$ where k' is odd, then from quadratic reciprocity (A.7) (and (A.8), (A.9)) we have

$$\left(\frac{-ka}{q}\right)=c(q)\left(\frac{q}{k'a}\right)$$

where $c(q):=(-1)^{(q-1)/2+m(q^2-1)/8}$ is periodic with period 8. We can thus rewrite this contribution to (7.11) as

$$\left|\sum_{a\leqslant A;(a,2)=1}\sum_{kA\leqslant q\leqslant B:(q,2ak)=1} c(q)\left(\frac{q}{k'a}\right)\frac{\log\frac{B}{q}}{q}\right|.$$

For any fixed a in the above sum, the expression $q\mapsto c(q)\left(\frac{q}{k'a}\right)1_{(q,2ak)=1}$ is periodic with period $8k'a=O(kA)$, is bounded in magnitude by 1 and has mean zero. A summation by parts then gives

$$\left|\sum_{kA\leqslant q\leqslant B:(q,2ak)=1} c(q)\left(\frac{q}{k'a}\right)\frac{\log\frac{B}{q}}{q}\right|\ll\log B$$

and so on summing in A we see that this contribution is acceptable. This concludes the proof of the proposition. □

We now record some variants of Proposition 1.4 that will also be useful in our applications.

Proposition 7.5 (Average value of $\tau_3(ab+1)$)**.** *For any $A,B>1$, one has*

$$\sum_{a\leqslant A}\sum_{b\leqslant B}\tau_3(ab+1)\ll AB\log^2(A+B). \tag{7.12}$$

Proof. By symmetry we may assume that $A\leqslant B$, so that $ab\ll B^2$ for all $a\leqslant A$ and $b\leqslant B$. For any n, τ_3 is the number of ways to represent n as the product $n=d_1d_2d_3$ of three terms. One of these terms must be at most $n^{1/3}$, and so

$$\tau_3(n)\ll\sum_{d|n:d\leqslant n^{1/3}}\tau(\frac{n}{d}).$$

We can thus bound the left-hand side of (7.12) by

$$\ll\sum_{d\ll B^{2/3}}\sum_{a\leqslant A}\sum_{b\leqslant B:d|ab+1}\tau(\frac{ab+1}{d}).$$

Note that for fixed a, d, the constraint $d|ab+1$ is only possible if a is coprime to d, and restricts b to some primitive residue class $q \mod d$ for some $q = q_{a,d}$ between 1 and d. Writing $b = cd + q$, we can thus bound the above expression by

$$\ll \sum_{d \ll B^{2/3}} \sum_{a \leqslant A} \sum_{c \ll B/d} \tau(ac + r)$$

where $r = r_{a,d} := \frac{aq+1}{d}$. Note that r is clearly coprime to a. Thus by Corollary 7.4, we may bound the preceding expression by

$$\ll \sum_{d \ll B^{2/3}} \sum_{a \leqslant A} \frac{B}{d} \log B$$

which is $O(AB \log^2 B)$. The claim follows. □

Proposition 7.6 (Average value of $\tau(ab+cd)$)**.** *For any $A, B, C, D > 1$, one has*

$$\sum_{a \leqslant A, b \leqslant B, c \leqslant C, d \leqslant D : (a,b,c,d)=1} \tau(ab+cd) \ll ABCD \log(A+B+C+D). \tag{7.13}$$

Proof. By symmetry we may assume that $A, B, C \leqslant D$. Then for fixed a, b, c coprime, we have

$$\sum_{d \leqslant D} \tau(abcd) \ll D \log D$$

by Corollary 7.4, and the claim follows by summing in a, b, c, d. □

Remark 7.7. *Informally, one can view the above propositions as asserting that the heuristics $\tau(n) \ll \log n$, $\tau_3(n) \ll \log^2 n$ are valid on average (in a first moment sense) on the range of various polynomial forms in several variables.*

8. Upper bound for $\sum_{n \leqslant N} f_{\mathrm{I}}(n)$ and $\sum_{p \leqslant N} f_{\mathrm{I}}(p)$

Now that we have established Proposition 1.4, we can obtain upper bounds on sums of f_{I}.

We begin with the bound

$$\sum_{n \leqslant N} f_{\mathrm{I}}(n) \ll N \log^3 N.$$

By Proposition 2.1 and symmetry followed by Lemma 2.7, it suffices to show that there are at most $O(N \log^3 N)$ septuples $(a, b, c, d, e, f, n) \in \mathbb{N}^7$ obeying (2.1)-(2.9) and the Type I estimates from Lemma 2.7. In particular, $acd \ll N$, f is a factor of $4a^2d + 1$, and $n = 4acd - f$. As a, c, d, f determine the remaining components of the septuple, we may thus bound the number of such septuples as

$$\sum_{a,c,d : acd \ll N} \tau(4a^2d + 1).$$

Dividing a, c, d into dyadic blocks ($A/2 \leqslant a \leqslant A$, etc.) and applying Proposition 1.4 (with $k = 4$) to each block, we obtain the desired bound $O(N \log^3 N)$.

Now we establish the bound

$$\sum_{p \leqslant N} f_{\mathrm{I}}(p) \ll N \log^2 N \log\log N.$$

As before, it suffices to count quadruples (a, c, d, f) with $acd \ll N$, and f a factor of $4a^2d+1$; but now we can restrict $p = 4acd - f$ to be prime. Also, from Proposition 2.1 we may assume that p is coprime to acd (and hence to $4acd$, if we discard the prime $p = 2$).

Thus we may assume without loss of generality that $-f \mod 4ad$ is a primitive residue class. From the Brun-Titchmarsh inequality (A.10), we conclude that for each fixed a, d, f, there are $O(\frac{N}{\phi(4ad)\log(N/4ad)})$ primes p in this residue class that are less than N if $ad \leqslant N/100$ (say); if instead $ad > N/100$, then

we of course only have $O(1) = O(\frac{N}{\phi(4ad)})$ primes in this class. Thus, in any event, we can bound the number of such primes as $O(\frac{N}{\phi(4ad)\log(2+N/ad)})$. We therefore have the bound

$$\sum_{p\leqslant N} f_{\mathrm{I}}(p) \ll \sum_{a,d:ad\ll N} \tau(4a^2d+1)\frac{N}{\phi(4ad)\log(2+N/ad)}. \tag{8.1}$$

By dyadic decomposition (and bounding $\phi(4ad) \geqslant \phi(ad)$), it thus suffices to show that

$$\sum_{a,d:N/2\leqslant ad\leqslant N} \frac{\tau(4a^2d+1)}{\phi(ad)} \ll \log^2 N. \tag{8.2}$$

Indeed, assuming this bound for all N, we can bound the right-hand side of (8.1) by

$$\sum_{j=1}^{O(\log N)} \frac{N\log^2 N}{j} \ll N\log^2 N\log\log N$$

and the claim follows.

To prove (8.2), we would like to again apply Proposition 1.4, but we must first deal with the $\phi(ad)$ denominator. From (A.12) one has

$$\frac{1}{\phi(ad)} \ll \frac{1}{ad}\sum_{s|a}\sum_{t|d}\frac{1}{st}.$$

Writing $a = sa'$, $d = td'$, we may thus bound the left-hand side of (8.2) by

$$\ll \frac{1}{N}\sum_{s,t:st\leqslant N}\frac{1}{st}\sum_{a',d':a'd'\leqslant N/st}\tau(4s^2t(a')^2d'+1).$$

Applying Proposition 1.4 to the inner sum (decomposed into dyadic blocks, and setting $k = 4s^2t$), we see that

$$\sum_{a',d':a'd'\leqslant N/st}\tau(4s^2t(a')^2d'+1) \ll \frac{N}{st}\log^2\frac{N}{st}\log(1+s^2t).$$

Inserting this bound and summing in s,t we obtain the claim.

9. Upper bound for $\sum_{n\leqslant N} f_{\mathrm{II}}(n)$ and $\sum_{p\leqslant N} f_{\mathrm{II}}(p)$

Now we prove the upper bound

$$\sum_{n\leqslant N} f_{\mathrm{II}}(n) \ll N\log^3 N.$$

By Proposition 2.5 followed by Lemma 2.7 (and symmetry), it suffices to show that there are at most $O(N\log^3 N)$ $\mathbb{N}$-points (a,b,c,d,e,f) that lie in Σ_n^{II} for some $n \leqslant N$, which also obeys the Type II bound $acde \leqslant N$ in Lemma 2.7.

Observe from (2.13)-(2.21) that a,c,d,e determine the other variables b,f,n. Thus, it suffices to show that there are $\ll N\log^3 N$ quadruples $(a,b,d,e) \in \mathbb{N}^4$ with $acde \leqslant N$. But this follows from (A.2) with $k = 4$.

Finally, we prove the upper bound

$$\sum_{p\leqslant N} f_{\mathrm{II}}(p) \ll N\log^2 N.$$

By dyadic decomposition, it suffices to show that

$$\sum_{N/2\leqslant p\leqslant N} f_{\mathrm{II}}(p) \ll N\log^2 N. \tag{9.1}$$

As before, we can bound the left-hand side (up to constants) by the number of quadruples $(a,c,d,e) \in \mathbb{N}^4$ with $acde \ll N$. However, by (2.16), we may also add the restriction that $4acde - 4a^2d - e$ is a prime

between $N/2$ and N. Also, if we set $b := ce - a$, then by Lemma 2.7 we may also add the restrictions $a \leqslant b$ and $b \geqslant ce/2$, and from Proposition 2.5 we can also require that a, b be coprime. Since

$$\begin{aligned}(ade)(acd)(ab)^{1/2} &\ll (ade)(acd)b \\ &\ll (ade)(acd)(ce) \\ &= (acde)^2 \\ &\ll N^2\end{aligned}$$

we see that one of the quantities ade, acd, ab must be at most $\ll N^{4/5}$ (cf. Section 3). As we shall soon see, the ability to take one of these quantities to be significantly less than N allows us to avoid the inefficiencies in the Brun-Titchmarsh inequality (A.10) that led to a double logarithmic loss in the Type I case. (Unfortunately, it does not seem that a similar trick is available in the Type II case.)

Let us first consider those quadruples with $ade \ll N^{4/5}$, which is the easiest case. For fixed a, d, e, $4acde - 4a^2d - e$ traverses (a possibly non-primitive) residue class modulo $4ade$. As $ade \ll N^{4/5}$, there are no primes in this class that are at least $N/2$ if the class is not primitive. If it is primitive, we may apply the Brun-Titchmarsh inequality (A.10) to bound the number of primes between $N/2$ and N in this class by $\ll \frac{N}{\phi(4ade)\log(N)}$, noting that $\log(N/4ade)$ is comparable to $\log N$. Thus, we can bound this contribution to the left-hand side of (9.1) by

$$\ll \frac{N}{\log N} \sum_{a,d,e:ade\ll N^{4/5}} \frac{1}{\phi(4acd)};$$

setting $m := ade$ and bounding $\phi(4ade) \geqslant \phi(ade)$, we can bound this in turn by

$$\ll \frac{N}{\log N} \sum_{m\ll N^{4/5}} \frac{\tau_3(m)}{\phi(m)}$$

where $\tau_3(m) := \sum_{a,d,e:ade=m} 1$. Applying Lemma A.1, we have

$$\sum_{m\ll N^{4/5}} \frac{\tau_3(m)}{\phi(m)} \ll \log^3 N, \tag{9.2}$$

and so this contribution is acceptable.

Now we consider the case $acd \ll N^{4/5}$. Here, we rewrite $4acde - 4a^2d - e$ as $(4acd-1)e - 4a^2d$, which then traverses a (possibly non-primitive) residue class modulo $4acd-1$. Applying the Brun-Titchmarsh inequality as before, we may bound this contribution by

$$\ll \frac{N}{\log N} \sum_{a,c,d:acd\ll N^{4/5}} \frac{1}{\phi(4acd-1)}$$

and hence (setting $m := 4acd - 1$) by

$$\ll \frac{N}{\log N} \sum_{m\ll N^{4/5}} \frac{\tau_3(m+1)}{\phi(m)},$$

so that it suffices to establish the bound

$$\sum_{m\ll N^{4/5}} \frac{\tau_3(m+1)}{\phi(m)} \ll \log^3 N. \tag{9.3}$$

This is superficially similar to (9.2), but this time the summand is not multiplicative in m, and we can no longer directly apply Lemma A.1. To deal with this, we apply (A.12) and bound (9.3) by

$$\ll \sum_{m\ll N^{4/5}} \sum_{d|m} \frac{\tau_3(m+1)}{dm};$$

writing $m = dn$, we can rearrange this as

$$\ll \sum_{d \ll N^{4/5}} \frac{1}{d^2} \sum_{n \ll N^{4/5}/d} \frac{\tau_3(dn+1)}{n}.$$

Applying dyadic decomposition of the d, n variables and using Proposition 7.5, we obtain (9.3) as required.

Finally, we consider the case $ab \ll N^{4/5}$. Here, we rewrite $4acde - 4a^2d - e$ as $4abd - e$, and note that e divides $a + b = ce$. If we fix a, b, there are thus at most $\tau(a+b)$ choices for e (which also fixes c), and once one fixes such a choice, $4abd - e$ traverses a (possibly non-primitive) residue class modulo $4ab$. Applying the Brun-Titchmarsh inequality again, we may bound this contribution by

$$\ll \frac{N}{\log N} \sum_{a,b: ab \ll N^{4/5}; (a,b)=1} \frac{\tau(a+b)}{\phi(4ab)}.$$

Bounding $\phi(4ab) \geqslant \phi(ab)$ and using (A.12), we can bound this by

$$\ll \frac{N}{\log N} \sum_{a,b: ab \ll N^{4/5}; (a,b)=1} \sum_{k|a} \sum_{l|b} \frac{\tau(a+b)}{abkl}.$$

Writing $a = km$, $b = ln$, we may bound this by

$$\ll \frac{N}{\log N} \sum_{k,l,m,n: klmn \ll N^{4/5}; (k,l,m,n)=1} \frac{1}{k^2 l^2 mn} \tau(km + ln).$$

Dyadically decomposing in k, l, m, n and using Proposition 7.6, we see that this contribution is also $O(N \log^2 N)$. The proof of (9.1) (and thus Theorem 1.1) is now complete.

10. Solutions by polynomials

We now prove Proposition 1.9. We first verify that each of the sets is solvable by polynomials (which of course implies that any residue class contained in such classes are also solvable by polynomials). We first do this for the Type I sets. In view of the π_n^{I} map (which clearly preserves polynomiality), it will suffice to find polynomials $a = a(n), \ldots, f = f(n)$ of n that take values in $\mathbb{N}$ for sufficiently large n in these sets, and such that $(a(n), \ldots, f(n)) \in \Sigma_n^{\mathrm{I}}$ for all n. This is achieved as follows:

- If $n = -f \mod 4ad$, where $a, d, f \in \mathbb{N}$ are such that $f | 4a^2d + 1$, then we take
$$(a, b, c, d, e, f) := \left(a, \frac{n+f}{4ad} e - a, \frac{n+f}{4ad}, d, e, \frac{4a^2d+1}{e}\right).$$
- If $n = -f \mod 4ac$ and $n = -\frac{c}{a} \mod f$, where $a, c, f \in \mathbb{N}$ are such that $(4ac, f) = 1$, then we take
$$(a, b, c, d, e, f) := \left(a, \frac{na+c}{f}, c, \frac{n+f}{4ac}, \frac{na+af+c}{fc}, f\right);$$
note from the hypotheses that $na + af + c$ is divisible by the coprime moduli f and c, and is thus also divisible by fc.
- If $n = -f \mod 4cd$ and $n^2 = -4c^2d \mod f$, where $c, d, f, q \in \mathbb{N}$ are such that $(4cd, f) = 1$, then we take
$$(a, b, c, d, e, f) := \left(\frac{n+f}{4cd}, \frac{n^2+4c^2d+nf}{4cdf}, c, d, \frac{(n+f)^2+4c^2d}{4c^2df}, f\right);$$
note from the hypotheses that $(n+f)^2 + 4c^2d$ is divisible by the coprime moduli $4c^2d$ and f, and is thus also divisible by $4c^2df$.
- If $n = -\frac{1}{e} \mod 4ab$, where $a, b, e \in \mathbb{N}$ are such that $e | a + b$ and $(e, 4ab) = 1$, then we take
$$(a, b, c, d, e, f) := \left(a, b, \frac{a+b}{e}, \frac{ne+1}{4ab}, e, 4a\frac{a+b}{e}\frac{ne+1}{4ab} - n\right)$$

One easily verifies in each of these cases that one has an $\mathbb{N}$-point of Σ_n^{I} for n large enough.

Now we turn to the Type II case. We use the same arguments as before, but using Σ_n^{II} in place of Σ_n^{I} of course:

- If $n = -e \mod 4ab$, where $a, b, e \in \mathbb{N}$ are such that $e|a+b$ and $(e, 4ab) = 1$, then we take
$$(a, b, c, d, e, f) := \left(a, b, \frac{a+b}{e}, \frac{n+e}{4ab}, e, \frac{a+b}{e}\frac{n+e}{b} - 1\right).$$
- If $n = -4a^2 d \mod f$, where $a, d, f \in \mathbb{N}$ are such that $4ad|f+1$, then we take
$$(a, b, c, d, e, f) := \left(a, \frac{f+1}{4ad}\frac{n+4a^2d}{f} - a, \frac{f+1}{4ad}, d, \frac{n+4a^2d}{f}, f\right).$$
- If $n = -4a^2 d - e \mod 4ade$, where $a, d, e \in \mathbb{N}$ are such that $(4ad, e) = 1$, then we take
$$(a, b, c, d, e, f) := \left(a, \frac{n+e}{4ad}, \frac{n+4a^2d+e}{4ade}, d, e, \frac{n+4a^2d}{e}\right).$$

Again, one easily verifies in each of these cases that one has an $\mathbb{N}$-point of Σ_n^{II} for n large enough.

Now we establish the converse claim. Suppose first that we have a primitive residue class $q \mod r$ that can be Type I solved by polynomials, and is maximal with respect to this property, then we have
$$\frac{4}{p} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$
for all sufficiently large primes p in this class, where $x = x(p), y = y(p), z = z(p)$ are polynomials of p that take natural number values for all large p in this class. For all sufficiently large p, we either have $y(p) \leqslant z(p)$ for all p, or $y(p) \geqslant z(p)$ for all p; by symmetry we may assume the latter.

Applying Proposition 2.1, we see that
$$(x, y, z) = (abdp, acd, bcd)$$
for some $\mathbb{N}$-point $(a, \dots, f) = (a(p), \dots, f(p))$ in Σ_p^{I} with $a(p), b(p), c(p)$ having no common factor. In particular, $d = d(p)$ is the least common multiple of $x(p), y(p), z(p)$. Applying the Euclidean algorithm to the polynomials $x(p), y(p), z(p)$, we conclude that for sufficiently large p in the primitive residue class, d is also a polynomial in p, which divides the polynomials x, y, z. Dividing out by d and repeating these arguments, we conclude that $a = a(p)$, $b = b(p)$, and $c = c(p)$ are also polynomials in p for sufficiently large p in the primitive residue class. Applying the identities (2.1)-(2.9) we also see that $e = e(p)$ and $f = f(p)$ are polynomials in p for sufficiently large p.

From Lemma 2.7 we have $a(p)c(p)d(p) = O(p)$ and $f(p) = O(p)$ for all p, which implies that at least two of the polynomials $a(p), c(p), d(p)$ must be constant in p, and that $f(p)$ has degree at most 1 in p. We now divide into several cases.

First suppose that a, d are independent of p. By (2.7) this forces e, f to be independent of p as well, and f divides $4a^2d + 1$. By (2.6) we have
$$p = -f \mod 4ad$$
for all sufficiently large primes $p = q \mod r$ and thus (by Dirichlet's theorem on primes[12] in arithmetic progressions) the primitive residue class $q \mod r$ is contained in the residue class $-f \mod 4ad$, and the claim follows in this case.

Now suppose that a, c are independent of p, and f has degree 0 (i.e. is also independent of p). Then from (2.6) we have $p = -f \mod 4ac$, and from (2.8) we have $p = -\frac{c}{a} \mod f$; since p is a large prime this also forces $(4ac, f) = 1$, and the claim follows.

Now suppose that a, c are independent of p, and f has degree p (and thus grows linearly in p). By Lemma 2.7, b, e are then bounded and thus constant in p. From (2.2) we have $e|a+b$, and from (2.1)

[12] As noted in the introduction, one could avoid the use of Dirichlet's theorem, and work instead with almost primes or the profinite topology instead.

we have $p = -\frac{1}{e} \mod 4ab$. As p is an arbitrarily large prime, this forces $(4ab, e) = 1$, and the claim follows.

Next, suppose that c, d are independent of p, and f has degree 0. Then from (2.6) one has $p = -f \mod 4cd$, which in particular forces $(4cd, f) = 1$. From (2.9) one has $p^2 = -4c^2d \mod f$, and the claim follows.

Finally, suppose that c, d are independent of p, and f has degree 1. By (2.9), $f(p)$ divides $p^2 + 4c^2d$ for all large primes p in the primitive residue class. Applying the Euclidean algorithm, we conclude that f in fact divides $p^2 + 4c^2d$ *as a polynomial* in p. But as c, d are positive, $p^2 + 4c^2d$ is irreducible over the reals, a contradiction. This concludes the treatment of the Type I case.

We now turn to the Type II case. Let $q \mod r$ be a residue class that is Type II solvable by polynomials. Arguing as in the Type I case, we obtain a $\mathbb{N}$-point $(a, \dots, f) = (a(p), \dots, f(p))$ in Σ_p^{II} for all sufficiently large primes p in this class, and obeying the bounds in Lemma 2.7, with $a(p), \dots, f(p)$ all depending in a polynomial fashion on p.

From Lemma 2.7 we have $a(p)c(p)d(p)e(p) = O(p)$, and so three of these polynomials $a(p), c(p), d(p), e(p)$ must be independent of p.

Suppose first that a, c, e are independent of p. By (2.2), b is independent of p also, and $e|a + b$. By (2.13), $p = -e \mod 4ab$, and thus $(e, 4ab) = 1$, and the claim then follows from Dirichlet's theorem.

Now suppose that a, c, d are independent of p. By (2.18), f is independent of p also, and $4ad|f + 1$. From (2.19) one has $p = -4a^2d \mod f$, and the claim follows.

Next, suppose a, d, e are independent of p. By (2.16) one has $p = -4a^2d - e \mod 4ade$, which implies $(4ad, e) = 1$, and the claim follows.

Finally, suppose c, d, e are independent of p. By (2.14) this forces a, b to be bounded, and hence also independent of p; and so this case is subsumed by the preceding cases.

11. Lower bounds III

11.1. **Generation of solutions.** We begin the proof of Theorem 1.11; the method of proof will be a generalisation of that in Section 5. For the rest of this section, m and k are fixed, and all implied constants in asymptotic notation are allowed to depend on m, k. We assume that N is sufficiently large depending on m, k.

In the $m = 4, k = 3$ case, Type II solutions were generated by the ansatz

$$(t_1, t_2, t_3) = (abd, acdn, bcdn)$$

for various quadruples (a, b, c, d) (or equivalently, quadruples (a, c, d, e), setting $b := ce - a$); see (2.22). We will use a generalisation of this ansatz for higher k; for instance, when $k = 4$ we will construct solutions of the form

$$(t_1, t_2, t_3, t_4) = (bx_{12}x_{123}x_{124}x_{1234}, x_{12}x_{23}x_{24}x_{123}x_{124}x_{234}x_{1234}n, bx_{23}x_{123}x_{234}x_{1234}n, bx_{24}x_{124}x_{234}x_{1234}n)$$

for various octuples $(b, x_{12}, x_{23}, x_{24}, x_{123}, x_{124}, x_{234}, x_{1234})$, or equivalently, using octuples

$$(x_{12}, x_{23}, x_{24}, x_{123}, x_{124}, x_{234}, x_{1234}, e),$$

and setting

$$b = ex_{23}x_{24}x_{234} - x_{12}x_{24}x_{124} - x_{12}x_{23}x_{123}.$$

More generally, we will generate Type II solutions via the following lemma.

Lemma 11.2 (Generation of Type II solutions)**.** *Let $\mathcal{P}$ denote the set $2^{k-1} - 1$-element set*

$$\mathcal{P} := \{I \subset \{1, \dots, k\} : 2 \in I; I \neq \{2\}\}.$$

Let $(x_I)_{I \in \mathcal{P}}$ be a tuple of natural numbers, and let e be another natural number, obeying the inequalities

$$\frac{1}{2m}N \leqslant e \prod_{I \in \mathcal{P}} x_I \leqslant \frac{1}{m}N \tag{11.1}$$

and

$$1 < x_I \leqslant N^{1/2^{k+2}} \tag{11.2}$$

whenever $I \in \mathcal{P}$. *Suppose also that the quantity*

$$w := \prod_{I \in \mathcal{P}: I \neq \{1,2\}} x_I \tag{11.3}$$

is square-free. Set

$$b := e \prod_{I \in \mathcal{P}: 1 \notin I} x_I - \sum_{j=3}^{k} \prod_{I \in \mathcal{P}: j \notin I} x_I \tag{11.4}$$

$$t_1 := b \prod_{I \in \mathcal{P}: 1 \in I} x_I \tag{11.5}$$

$$n := mt_1 - e \tag{11.6}$$

$$t_2 := n \prod_{I \in \mathcal{P}} x_I \tag{11.7}$$

and

$$t_j := bn \prod_{I \in \mathcal{P}: j \in I} x_I. \tag{11.8}$$

Then n *is a natural number with* $n \leqslant N$, *and* $(t_1, \dots, t_k)$ *is a Type II solution for this value of* n. *Furthermore, each choice of* $(x_I)_{I \in \mathcal{P}}$ *and* e *generates a distinct Type II solution.*

Remark 11.3. *In the* $m = 4, k = 3$ *case, the parameters* x_I *are related to the coordinates* (a, b, c, d, e, f) *appearing in Proposition 2.5 by the formula*

$$(a, b, c, d, e, f) = (x_{12}, b, x_{23}, x_{123}, e, 4x_{12}x_{23}x_{123} - 1);$$

however, the constraint that a, b, c *have no common factor and* abd *is coprime to* n *has been replaced by the slightly different criterion that* d *is squarefree, which turns out to be more convenient for obtaining lower bounds (note that the same trick was also used to prove* (5.1)*). Parameterisations of this type have appeared numerous times in the previous literature (see* [19, 22, 54, 12]*, or indeed Propositions 2.1, 2.5), though because most of these parameterisations were focused on dealing with* all *solutions of a given type, as opposed to an easily countable subset of solutions, there were more parameters* x_I *(indexed by all non-empty subsets of* $\{1, \dots, k\}$*, not just the ones in* $\mathcal{P}$*), and there were some coprimality conditions on the* x_I *rather than square-free conditions.*

Proof. Let the notation be as in the lemma. Then from (11.2) one has

$$\sum_{j=3}^{k} \prod_{I \in \mathcal{P}: j \notin I} x_I \leqslant (k-2) N^{2^{k-2}/2^{k+2}} \ll N^{1/16}$$

while since

$$\prod_{I \in \mathcal{P}} x_I \ll N^{2^{k-1}/2^{k+2}} \ll N^{1/8}$$

we see from (11.1) that

$$e \gg N^{7/8}.$$

From (11.4) we then have that

$$\frac{1}{2} e \prod_{I \in \mathcal{P}: 1 \notin I} x_I \leqslant b \leqslant e \prod_{I \in \mathcal{P}: 1 \notin I} x_I$$

and thus by (11.5)

$$\frac{1}{2}e\prod_{I\in\mathcal{P}}x_I \leqslant t_1 \leqslant e\prod_{I\in\mathcal{P}}x_I$$

and thus by (11.6) (noting that $m \geqslant 4$)

$$\frac{1}{4}me\prod_{I\in\mathcal{P}}x_I \leqslant n \leqslant me\prod_{I\in\mathcal{P}}x_I.$$

These bounds ensure that $b, n, t_1, \dots, t_k$ are natural numbers with $n \leqslant N$, and with with $t_2, \dots, t_k$ divisible by n. Dividing (11.4) by $bn\prod_{I\in\mathcal{P}}x_I$ and using (11.5), (11.7), (11.8), we conclude that

$$\frac{1}{t_2} = \frac{e}{nt_1} - \sum_{j=3}^{k}\frac{1}{t_j};$$

applying (11.6) one concludes that $(t_1, \dots, t_k)$ is a Type II solution.

It remains to demonstrate that each choice of $(x_I)_{I\in\mathcal{P}}$ and e generates a distinct Type II solution, or equivalently that the Type II solution $(t_1, \dots, t_k)$ uniquely determines $(x_I)_{I\in\mathcal{P}}$ and e. To do this, first observe from (1.6) that $(t_1, \dots, t_k)$ determines n, and from (11.6) we see that e is determined also. Next, observe from (11.5), (11.7), (11.8) that for any $3 \leqslant j \leqslant k$, one has

$$\frac{t_2t_j}{n^2t_1} = \left(\prod_{I\in\mathcal{P}:j\in I;1\notin I}x_I\right)^2\left(\prod_{I\in\mathcal{P}:j\in I \text{ XOR } 1\notin I}x_I\right) \tag{11.9}$$

where XOR denotes the exclusive or operator; in particular, the left-hand side is necessarily a natural number. Note that all the factors x_I appearing on the right-hand side are components of the square-free quantity w given by (11.3). We conclude that $(\prod_{I\in\mathcal{P}:j\in I;1\notin I}x_I)^2$ is the largest perfect square dividing $\frac{t_2t_j}{n^2t_1}$. We conclude that the Type II solution $(t_1, \dots, t_k)$ determines all the products

$$\prod_{I\in\mathcal{P}:j\in I;1\notin I}x_I \tag{11.10}$$

for $3 \leqslant j \leqslant k$. Note (from the square-free nature of w) that the x_I with $1 \notin I$ are all coprime. Taking the greatest common divisor of the (11.10) for all $3 \leqslant j \leqslant k$, we see that the Type II solution determines $x_{\{2,3,\dots,k\}}$. Dividing this quantity out from all the expressions (11.10), and then taking the greatest common divisor of the resulting quotients for $4 \leqslant j \leqslant k$, one recovers $x_{\{2,4,\dots,k\}}$; a similar argument gives x_I for any $I \in \mathcal{P}$ with $1 \notin I$ of cardinality $k-3$. Dividing out these quantities and taking greatest common divisors again, one can then recover x_I for any $I \in \mathcal{P}$ with $1 \notin I$ of cardinality $k-4$; continuing in this fashion we can recover all the x_I with $I \in \mathcal{P}$ and $1 \notin I$.

Returning to (11.9), we can then recover the products $\prod_{I\in\mathcal{P}:1,j\in I}x_I$ for all $3 \leqslant j \leqslant k$. Taking greatest common divisors iteratively as before, we can then recover all the x_I with $I \in \mathcal{P}$ and $1 \in I$, thus reconstructing all of the data $(x_I)_{I\in\mathcal{P}}$ and e, as claimed. □

In view of this above lemma, we see that to prove (1.7), it suffices to show that the number of tuples $((x_I)_{I\in\mathcal{P}}, e)$ obeying the hypotheses of the lemma is $\gg N(\log N)^{2^{k-1}-1}$.

Observe that if we fix x_I with $I \in \mathcal{P}$ obeying (11.2) and with the quantity w defined by (11.3), then there are

$$\gg \frac{N}{\prod_{I\in\mathcal{P}}x_I}$$

choices of e that obey (11.1). Thus, noting that $\mu^2(w) \geqslant \mu^2(\prod_{I\in\mathcal{P}}x_I)$, the number of tuples obeying the hypotheses of the lemma is

$$\gg N\sum_{*}\frac{\mu^2(\prod_{I\in\mathcal{P}}x_I)}{\prod_{I\in\mathcal{P}}x_I}, \tag{11.11}$$

where the sum $\sum_*$ ranges over all choices of $(x_I)_{I\in\mathcal{P}}$ obeying the bounds (11.2). To estimate (11.11), we make use of [13, Theorem 6.4], which we restate as a lemma:

Lemma 11.4. *Let $l \geqslant 1$, and for each $1 \leqslant i \leqslant l$, let $\alpha_i < \beta_i$ be positive real numbers. Then*

$$\sum_{N^{\alpha_i}\leqslant n_i\leqslant N^{\beta_i} \text{ for all } 1\leqslant i\leqslant l} \frac{\mu^2(n_1\cdots n_l)}{n_1\cdots n_l} \gg_l (\log N)^l \prod_{i=1}^l (\beta_i-\alpha_i), \tag{11.12}$$

for N sufficiently large depending on l and the $\alpha_1,\dots,\alpha_l,\beta_1,\dots,\beta_l$.

From this lemma (and noting that there are $2^{k-1}-1$ parameters x_I in the sum $\sum_*$) we see that

$$\sum_* \frac{\mu^2(\prod_{I\in\mathcal{P}} x_I)}{\prod_{I\in\mathcal{P}} x_I} \gg \log^{2^{k-1}-1} N; \tag{11.13}$$

inserting this into (11.11) we obtain the claim.

Now we prove (1.8). As in Section 5, the arguments are similar to those used to prove (1.7), but with the additional input of the Bombieri-Vinogradov inequality.

As in the proof of (1.7), it suffices to obtain a lower bound (in this case, $\gg \frac{N(\log N)^{2^{k-1}-2}}{\log\log N}$) on the number of tuples $((x_I)_{I\in\mathcal{P}}, e)$, but now with the additional constraint that the quantity

$$p := mt_1 - e = mb \prod_{I\in\mathcal{P}:1\in I} x_I - e$$

is prime.

Suppose we fix $(x_I)_{I\in\mathcal{P}}$ obeying (11.2) with w squarefree. We may write

$$p = qe + r$$

where

$$q := m \prod_{I\in\mathcal{P}} x_I - 1 \tag{11.14}$$

and

$$r := -m \prod_{I\in\mathcal{P}:1\in I} x_I \sum_{j=3}^k \prod_{I\in\mathcal{P}:j\notin I} x_I.$$

Thus as e varies in the range given by (11.1), $qe+r$ traces out an arithmetic progression of spacing q whose convex hull contains $[0.6N, 0.9N]$ (say). Thus, every prime p in this interval $[0.6N, 0.9N]$ that is congruent to $r \mod q$ will provide an e that will give a Type II solution with $n = p$ prime, and different choices of $(x_I)_{I\in\mathcal{P}}$ and p will give different Type II solutions.

For fixed $(x_I)_{I\in\mathcal{P}}$, if r is coprime to q, then we see from (A.13) (and estimating $\mathrm{li}(x) = (1+o(1))\frac{x}{\log x}$) that the number of such p is at least

$$\geqslant c\frac{N}{\log N\phi(q)} - D(0.6N; q) - D(0.9N; q)$$

for some absolute constant $c > 0$. It thus suffices to show that

$$\sum_* \mu^2(w) 1_{(r,q)=1} \frac{N}{\log N\phi(q)} \gg \frac{N(\log N)^{2^{k-1}-2}}{\log\log N} \tag{11.15}$$

and

$$\sum_* D(cN; q) = o\left(\frac{N(\log N)^{2^{k-1}-2}}{\log\log N}\right) \tag{11.16}$$

for $c = 0.6, 0.9$.

We first show (11.15). Since $\mathrm{li}(N/100)$ is comparable to $N/\log N$, and $\phi(q) \leqslant q \ll w$, we may simplify (11.15) as

$$\sum_{*} \frac{\mu^2(w)}{\prod_{I\in\mathcal{P}} x_I} 1_{(r,q)=1} \gg \frac{(\log N)^{2^{k-1}-1}}{\log\log N}. \tag{11.17}$$

The expression on the left-hand side is similar to (11.11), but now one also has the additional constraint $1_{(r,q)=1}$. To deal with this constraint, we restrict the ranges of the x_I parameters somewhat to perform an averaging in the $x_{\{1,2\}}$ parameter (taking advantage of the fact that this parameter does not appear in the $\mu^2(w)$ term). More precisely, we restrict to the ranges where

$$x_I \leqslant N^{1/2^{100k}} \tag{11.18}$$

(say) for $I \neq \{1,2\}$, and

$$x_{\{1,2\}} \leqslant N^{1/2^{k+2}}. \tag{11.19}$$

We now analyse the constraint that r and q are coprime. We can factor

$$r = -m x_{\{1,2\}}^2 s$$

where

$$s := \left(\prod_{I\in\mathcal{P}:1\in I; I\neq\{1,2\}} x_I\right) \sum_{j=3}^{k} \prod_{I\in\mathcal{P}:j\notin I; I\neq\{1,2\}} x_I;$$

the point is that s does not depend on $x_{\{1,2\}}$. Since $q+1$ is divisible by $m x_{\{1,2\}}$, we see that $m x_{\{1,2\}}^2$ is coprime to q, and thus $(q,r) = 1$ iff $(q,s) = 1$. We can write $q = u x_{\{1,2\}} - 1$, where $u := m\prod_{I\in\mathcal{P}:I\neq\{1,2\}} x_I$, and so $(q,r) = 1$ iff $(u x_{\{1,2\}} - 1, s) = 1$.

We may replace s here by the largest square-free factor s' of s. If we then factor $s' = vy$, where $v := (s', u)$ and $y := s'/v$, then $u x_{\{1,2\}} - 1$ is already coprime to v, and so we conclude that $(q,r) = 1$ iff $(u x_{\{1,2\}} - 1, y) = 1$.

Fix x_I for $I \neq \{1,2\}$. By construction, u and y are coprime, and so the constraint $(u x_{\{1,2\}} - 1, y) = 1$ restricts $x_{\{1,2\}}$ to $\phi(y)$ distinct residue classes modulo y. Since

$$y \leqslant s \ll N^{1/2^{90k}}$$

(say) thanks to (11.18), we conclude that

$$\sum_{x_{\{1,2\}}\leqslant N^{1/2^{k+2}}} \frac{1_{(q,r)=1}}{x_{\{1,2\}}} \gg \frac{\phi(y)}{y}\log N.$$

Using the crude bound[13] (A.11), we may lower bound $\frac{\phi(y)}{y} \gg \frac{1}{\log\log N}$. We may thus lower bound the left-hand side of (11.17) by

$$\frac{\log N}{\log\log N} \sum_{**} \frac{\mu^2(w)}{w},$$

where $\sum_{**}$ sums over all x_I for $I \neq \{1,2\}$ obeying (11.18). But by Lemma 11.4 we have

$$\sum_{**} \frac{\mu^2(w)}{w} \gg (\log N)^{2^{k-1}-2},$$

and the claim (11.17) follows.

[13] It is quite likely that by a finer analysis of the generic divisibility properties of y, one can remove this double logarithmic loss, but we will not attempt to do so here.

Finally, we show (11.16). Observe that each q can be represented in the form (11.14) in at most $\tau_{2^{k-1}-1}(q+1)$ different ways; also, from (11.2) we have $q \ll N^{2^{k-1}/2^{k+2}} = N^{1/8}$. We may thus bound the left-hand side of (11.16) by

$$\sum_{q \ll N^{1/8}} D(cN;q)\tau_{2^{k-1}-1}(q+1).$$

From the Bombieri-Vinogradov inequality (A.14) and the trivial bound $D(cN;q) \ll N/q$ one has

$$\sum_{q \ll N^{1/8}} qD(cN;q)^2 \ll_A N \log^{-A} N$$

for any $A > 0$, while from Lemma A.1 (and shifting q by 1) one has

$$\sum_{q \ll N^{1/8}} \frac{\tau_{2^{k-1}-1}(q+1)^2}{q} \ll \log^{O(1)} N.$$

The claim then follows from the Cauchy-Schwarz inequality (taking A large enough). The proof of Theorem 1.11 is now complete.

Appendix A. Some results from number theory

In this section we record some well-known facts from number theory that we will need throughout the paper. We begin with a crude estimate for averages of multiplicative functions.

Now we record some asymptotic formulae for the divisor function τ. From the Dirichlet hyperbola method we have the asymptotic

$$\sum_{n \leqslant N} \tau(n) = N \log N + O(N) \tag{A.1}$$

(see e.g. [28, §1.5]). More generally, we have

$$\sum_{n \leqslant N} \tau_k(n) = N \log^{k-1} N + O_k(N \log^{k-2} N) \tag{A.2}$$

for all $k \geqslant 1$, where $\tau_k(n) := \sum_{d_1,\dots,d_k : d_1 \dots d_k = n} 1$. Indeed, the left-hand side of (A.2) can be rearranged as

$$\sum_{d_1 \leqslant N} \sum_{d_2 \leqslant N/d_1} \dots \sum_{d_k \leqslant N/d_1 \dots d_{k-1}} 1$$

and the claim follows by evaluating each of the summations in turn.

We can perturb this asymptotic:

Lemma A.1 (Crude bounds on sums of multiplicative functions)**.** *Let $f(n)$ be a multiplicative function obeying the bounds*

$$f(p) = m + O(\frac{1}{p})$$

for all primes p and some integer $m \geqslant 1$, and

$$|f(p^j)| \ll j^{O(1)}$$

for all primes p and $j > 1$. Then one has

$$\sum_{n \leqslant N} f(n) \ll_m N \log^{m-1} N$$

for N sufficiently large depending on m; from this and summation by parts we have in particular that

$$\sum_{n \leqslant N} \frac{f(n)}{n} \ll_m \log^m N$$

If f is non-negative, we also have the corresponding lower bound

$$\sum_{n\leqslant N} f(n) \gg_m N \log^{m-1} N$$

and hence

$$\sum_{n\leqslant N} \frac{f(n)}{n} \gg_m \log^m N$$

One can of course get much better estimates by contour integration methods (and these estimates also follow without much difficulty from the more general results in [21]), but the above crude bounds will suffice for our purposes.

Proof. We allow all implied constants to depend on m. By Möbius inversion, we can write

$$f(n) = \sum_{d|n} \tau_m(d) g(\frac{n}{d})$$

where g is a multiplicative function obeying the bounds

$$g(p) = O(\frac{1}{p})$$

and

$$|g(p^j)| \ll j^{O(1)}$$

for all $j > 1$. In particular, the Euler product

$$\sum_{n=1}^{\infty} \frac{|g(n)|}{n} = \prod_p \left(1 + \frac{|g(p)|}{p} + \sum_{j=2}^{\infty} \frac{|g(p^j)|}{p^j}\right) = \prod_p \left(1 + O\left(\frac{1}{p^2}\right)\right)$$

is absolutely convergent.

We may therefore write $\sum_{n\leqslant N} f(n)$ as

$$\sum_{k\leqslant N} g(k) \sum_{d\leqslant N/k} \tau_m(d). \tag{A.3}$$

Applying (A.2), we conclude

$$|\sum_{n\leqslant N} f(n)| \ll \sum_{k\leqslant N} \frac{|g(k)|}{k} N \log^{m-1} N$$

and the upper bound follows from the absolute convergence of $\sum_{n=1}^{\infty} \frac{|g(n)|}{n}$.

Now we establish the lower bound. By zeroing out f at various small primes p (and all their multiples), we may assume that $f(p^j) = g(p^j) = 0$ for all $p \leqslant w$ for any fixed threshold w. By making w large enough, we may ensure that

$$1 - \sum_{n=2}^{\infty} \frac{|g(n)|}{n} > 0.$$

If we then insert the bound (A.2) into (A.3) we obtain the claim. □

As a typical application of Lemma A.1 we have

$$\sum_{n\leqslant N} \tau^k(n) \ll_k N \log^{2^k-1} N \tag{A.4}$$

for any $N > 1$ and $k \geqslant 1$, (see also [35]).

To study some more detailed distribution of divisors and prime divisors we recall the *Turán-Kubilius inequality* for additive functions. A function w is called additive, if $w(n_1 n_2) = w(n_1) + w(n_2)$, whenever $\gcd(n_1, n_2) = 1$.

Lemma A.2 (Turán-Kubilius inequality (see [60], page 20)). *Let $w : \mathbb{N} \to \mathbb{R}$ denote an arithmetic function which is additive (thus $w(nm) = w(n) + w(m)$ whenever n, m are coprime). Let $A(N) = \sum_{p^k \leqslant N} \frac{w(p^k)}{p^k}$ and $D^2(N) = \sum_{p^k \leqslant N} \frac{|w(p^k)|^2}{p^k}$. For every $N \geqslant 2$ and for any additive function w the following inequality holds:*

$$\sum_{n \leqslant N} |w(n) - A(N)|^2 \leqslant 30 N D^2(N).$$

(Here $\sum_{p^k}$ denotes the sum over all prime powers.)

Example. Let $\omega(n)$ denote the number of distinct prime factors of n, then $A(N) = \sum_{p^k \leqslant N} \frac{\omega(p^k)}{p^k} = \log\log N + O(1)$ and $D^2(N) = \sum_{p^k \leqslant N} \frac{\omega(p^k)^2}{p^k} = A(N) = \log\log N + O(1)$. The Turán-Kubilius inequailty then gives

$$\sum_{n \leqslant N} |\omega(n) - \log\log N|^2 \leqslant 30 N \log\log N + O(N).$$

In particular, if $\xi(n) \to \infty$ as $n \to \infty$, then one has $|\omega(n) - \log\log n| \leqslant \xi(n)\sqrt{\log\log n}$ for all n in a set of integers of density 1. For more details see [71].

From (A.1) one might guess the heuristic

$$\tau(n) \approx \log n \tag{A.5}$$

on average. But it follows from the Turán-Kubilius inequality that for "typical" n, the number of divsors is about $2^{\log\log n} = (\log n)^{\log 2}$, which is considerably smaller, and that a small number of integers with an exceptionally large number of divisors heavily influences this average. The influence of these integers with a very large number of divsiors dominates even more for higher moments. The extremal cases heuristically consist of many small prime factors, and the following "divisor bound" holds

$$\tau(n) \leqslant 2^{(1+o(1))\frac{\log n}{\log\log n}} = O(n^{\frac{1}{\log\log n}}) \tag{A.6}$$

for any $n \geqslant 1$; see [50].

The Turán-Kubilius type inequalities have been studied for shifted primes as well. We make use of the following result of Barban, (see Elliott [11], Theorem 12.10).

Lemma A.3. *A function $w : \mathbb{N} \to \mathbb{R}^+$ is said to be strongly additive if it is additive and $w(p^k) = w(p)$ holds, for every prime power p^k, $k \geqslant 1$. Let w denote a real nonnegative strongly additive function. Define $S(N) = \sum_{p \leqslant N} \frac{w(p)}{p-1}$ and $\Lambda(N) = \max_{p \leqslant N} w(p)$. Suppose that $\Lambda(N) = o(S(N))$, as $N \to \infty$. Then for any fixed $\varepsilon > 0$, the prime density*

$$\nu_N(p; |w(p+1) - S(N)| > \varepsilon S(N)) \to 0 \text{ as } N \to \infty.$$

The same holds for other shifts $p + a$, where $a \neq 0$.

The function $\omega(n)$ is strongly additive. This lemma implies that for primes with relative prime density 1, $p+1$ contains about $\frac{1}{2}\log\log p$ primes of the form 1 mod 4. To see this one chooses $w(p) = 1$ if $p \equiv 1 \bmod 4$, and 0 otherwise. In this example one has $S(N) \sim \frac{1}{2}\log\log N$ and $\Lambda(N) = 1$.

We recall the quadratic reciprocity law

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(n-1)(m-1)/4} \tag{A.7}$$

for all odd m, n, where $\left(\frac{m}{n}\right)$ is the Jacobi symbol, as well as the companion laws

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/4} \tag{A.8}$$

and

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} \tag{A.9}$$

for odd n.

For any primitive residue class $a \mod q$ and any $N > 0$, let $\pi(N; q, a)$ denote the number of primes $p < N$ that are congruent to a mod q. We recall the *Brun-Titchmarsh inequality* (see e.g. [28, Theorem 6.6])

$$\pi(N; q, a) \ll \frac{N}{\phi(q) \log \frac{N}{q}} \tag{A.10}$$

for any such class with $N \geqslant q$. This bound suffices for upper bound estimates on primes in residue classes. Due to the q in the denominator of $\log(\frac{N}{q})$, it will only be efficient to apply this inequality when q is much smaller than N, e.g. $q \leqslant N^c$ for some $c < 1$.

The Euler totient function $\phi(q)$ in the denominator is also inconvenient; it would be preferable if one could replace it with q. Unfortunately, this is not possible; the best bound on $\frac{1}{\phi(q)}$ in terms of q that one has in general is

$$\frac{1}{\phi(q)} \ll \frac{\log\log q}{q} \tag{A.11}$$

(see e.g. [53]). Using this bound would simplify our arguments, but one would lose an additional factor of $\log\log N$ or so in the final estimates. To avoid this loss, we observe the related estimate

$$\frac{1}{\phi(q)} \ll \frac{1}{q} \sum_{d|q} \frac{1}{d}. \tag{A.12}$$

Indeed, we have

$$\begin{aligned}
\frac{q}{\phi(q)} &= \prod_{p|q} \frac{p}{p-1} \\
&= \prod_{p|q} (1 + \frac{1}{p})(1 + O(\frac{1}{p^2})) \\
&\ll \prod_{p|q} (1 + \frac{1}{p}) \\
&\leqslant \sum_{d|q} \frac{1}{d},
\end{aligned}$$

and (A.12) follows. (One could restrict d to be square-free here if desired, but we will not need to do so in this paper.)

The Brun-Titchmarsh inequality only gives upper bounds for the number of primes in an arithmetic progression. To get lower bounds, we let $D(N; q)$ denote the quantity

$$D(N; q) := \max_{(a,q)=1} \left| \pi(N; q, a) - \frac{\mathrm{li}(N)}{\phi(q)} \right|. \tag{A.13}$$

where $\mathrm{li}(x) := \int_0^x \frac{dt}{\log t}$ is the logarithmic integral. The Bombieri-Vinogradov inequality (see e.g. [28, Theorem 17.1]) implies in particular [14] that

$$\sum_{q \leqslant N^\theta} D(N; q) \ll_{\theta, A} N \log^{-A} N \tag{A.14}$$

for all $0 < \theta < 1/2$ and $A > 0$. Informally, this gives lower bounds on $\pi(N; q, a)$ on the average for q much smaller than $N^{1/2}$.

[14] The inequality is usually phrased using the summatory von Mangoldt function $\psi(N; q, a) = \sum_{n \leqslant N; n = a \mod q} \Lambda(n)$. A summation by parts converts it to an estimate using the prime counting function, see [8] for details.

References

[1] A. Aigner, *Brüche als Summe von Stammbrüchen*, J. Reine Angew. Math. **214/215** (1964), 174-179.

[2] M. B. Barban, P. P. Vehov, *Summation of multiplicative functions of polynomials*, Mat. Zametki **5** (1969), 669680.

[3] P. Bartoš. K Riešitel'nosti Diofantickej Rovnice $\sum_{j=1}^{n} \frac{1}{x_j} = \frac{a}{b}$. *Časopis pro pěstování matematiky*, 98 (1973), 261–264.

[4] P. Bartoš and K. Pehatzová-Bošanká. K Riešeniu Diofantickej Rovnice $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{a}{b}$. *Časopis pro pěstování matematiky*, 96 (1971), 294–299.

[5] M. Bello-Hernandez, M. Benito, E. Fernández, *On egyptian fractions*, preprint, `arXiv:1010.2035`

[6] L. Bernstein, *Zur Lösung der diophantischen Gleichung* $\frac{m}{n}$*, insbesondere im Fall* $m = 4$, J. Reine Angew. Math. **211**, 1962, 1-10.

[7] T. Browning, C. Elsholtz, *The number of representations of rationals as a sum of unit fractions*, to appear in Illinois Journal of Mathematics.

[8] J. Brüdern. *Einführung in die analytische Zahlentheorie*. Springer, Berlin, Heidelberg, 1995.

[9] J-L. Colliot-Théelène, J-J. Sansuc, *Torseurs sous des groupes de type multiplicatif; applications á l'étude des points rationnels de certaines variétés algébriques*, C. R. Acad. Sci. Paris Sér. A-B 282 (1976), no. 18, Aii, A1113–A1116.

[10] S. Daniel, *Uniform bounds for short sums of certain arithmetic functions of polynomial arguments*, Unpublished manuscript.

[11] P. D. T. A. Elliott, Probabilistic number theory. II. Central limit theorems. Grundlehren der Mathematischen Wissenschaften, 240. Springer-Verlag, Berlin-New York, 1980.

[12] C. Elsholtz, Sums of k unit fractions, PhD thesis, Technische Universität Darmstadt, 1998.

[13] C. Elsholtz, *Sums of k unit fractions* Trans. Amer. Math. Soc. **353** (2001), 3209–3227.

[14] P. Erdős. Az $\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} = \frac{a}{b}$ egyenlet egész számú megoldásairól, *Matematiki Lapok* **1** (1950), 192–210.

[15] P. Erdős, *On the sum* $\sum_{k=1}^{x} f(k)$), J. London Math. Soc. **27** (1952), 7-15.

[16] P. Erdős, P.; R.L. Graham, Old and new problems and results in combinatorial number theory. Monographies de L'Enseignement Mathématique, 28. L'Enseignement Mathmatique, Geneva, 1980. 128 pp.

[17] É. Fouvry, *Sur le probléme des diviseurs de Titchmarsh*, J. Reine Angew. Math. **357** (1985), 51-76.

[18] É. Fouvry, H. Iwaniec, *The divisor function over arithmetic progressions*, With an appendix by Nicholas Katz. Acta Arith. 61 (1992), no. 3, 271-287.

[19] H. Gupta, Selected topics in number theory. Abacus Press, Tunbridge Wells, 1980. 394 pp.

[20] R. Guy, *Unsolved Problems in Number Theory*, 2nd ed. New York: Springer-Verlag, pp. 158-166, 1994.

[21] H. Halberstam, H.-E. Richert, On a result of R. R. Hall. J. Number Theory **11** (1979), no. 1, 76-89.

[22] R.R. Hall, *Sets of Multiples*, Cambridge University Press, Cambridge, 1996.

[23] D. R. Heath-Brown, *The density of rational points on Cayley's cubic surface*, Proceedings of the Session in Analytic Number Theory and Diophantine Equations, 33 pp., Bonner Math. Schriften, 360, Univ. Bonn, Bonn, 2003

[24] K. Henriot, *Nair-Tenenbaum bounds uniform with respect to the discriminant*, `arXiv:1102.1643`

[25] C. Hooley, *On the number of divisors of quadratic polynomials*, Acta Math. **110** (1963), 97–114.

[26] J. Huang, R. C. Vaughan, *Mean value theorems for binary Egyptian fractions*, J. Number Theory 131 (2011), 1641–1656

[27] M. N. Huxley, *A note on polynomial congruences*, Recent Progress in Analytic Number Theory, Vol. I (H. Halberstam and C. Hooley, eds.), Academic Press, London, 1981, pp. 193-196.

[28] H. Iwaniec, E. Kowalski, Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[29] C. Jia, *A Note on Terence Tao's Paper "On the Number of Solutions to* $4/p = 1/n_1 + 1/n_2 + 1/n_3$*"*, preprint.

[30] R.W. Jollenstein. A note on the Egyptian problem,*Congressus Numerantium, 17, Utilitas Math., Winnipeg, Man.* In *Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing*, 351–364, Louisiana State Univ., Baton Rouge, La., 1976.

[31] I. Kotsireas, *The Erdős-Straus conjecture on Egyptian fractions*, Paul Erdős and his mathematics (Budapest, 1999), 140–144, János Bolyai Math. Soc., Budapest, 1999.

[32] N. V. Kuznecov, *The Petersson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums*, Mat. Sb. (N.S.) 111(153) (1980), no. 3, 334-383, 479.

[33] B. Landreau, *A new proof of a theorem of van der Corput*, Bull. London Math. Soc. 21 (1989), no. 4, 366-368.

[34] Delang Li. On the Equation $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$. *Journal of Number Theory* **13** (1981), 485–494, 1981.

[35] C. Mardjanichvili, Estimation d'une somme arithmetique. *Comptes Rendus (Doklady) de l'Académie des Sciences de l'URSS* **22** (1939), 387–389.

[36] J. McKee, *On the average number of divisors of quadratic polynomials*, Math. Proc. Cambridge Philos. Soc. 117 (1995), no. 3, 389-392.

[37] J. McKee, *A note on the number of divisors of quadratic polynomials. Sieve methods, exponential sums, and their applications in number theory* (Cardiff, 1995), 275–281, London Math. Soc. Lecture Note Ser., 237, Cambridge Univ. Press, Cambridge, 1997.

[38] J. McKee, *The average number of divisors of an irreducible quadratic polynomial*, Math. Proc. Cambridge Philos. Soc. **126** (1999), no. 1, 17–22.

[39] L.J. Mordell, Diophantine Equations, volume 30 of Pure and Applied Mathematics. Academic Press, 1969.

[40] T. Nagell, *Généralisation d'un theórème de Tchebicheff*, J. Math. **8** (1921), 343–356.

[41] M. Nair, *Multiplicative functions of polynomial values in short intervals*, Acta Arith. **62** (1992), no. 3, 257269.

[42] M. Nair, G. Tenenbaum, *Short sums of certain arithmetic functions*, Acta Math. **180** (1998), 119-144.

[43] M. Nakayama, *On the decomposition of a rational number into "Stammbrüche."*, Tôhoku Math. J. **46**, (1939). 1-21.

[44] M.R. Obláth. Sur l' équation diophantienne $\frac{4}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$. *Mathesis* **59** (1950), 308–316.

[45] G. Palamà. Su di una congettura di Sierpiński relativa alla possibilità in numeri naturali della $\frac{5}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$. *Bollettino della Unione Matematica Italiana (3)*, 13 (1958), 65–72.

[46] G. Palamà. Su di una congettura di Schinzel. *Bollettino della Unione Matematica Italiana (3)*, 14 (1959), 82–94.

[47] C.P. Popovici. On the diophantine equation $\frac{a}{b} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$. *Analele Universităţii Bucureşti. Seria Ştiinţele Naturii. Matematică-Fizikă* 10 (1961), 29–44, 1961.

[48] O. Ore, *Anzahl der Wurzeln höherer Kongruenzen*, Norsk Matematisk Tidsskrift, 3 Aagang, Kristiana (1921), 343–356.

[49] C. Pomerance, Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory, Part I, H.W. Lenstra, Jr. and R. Tijdeman, eds., Math. Centre Tract 154, Amsterdam, 1982, pp 89–139.

[50] S. Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. **14** (1915), 347-409.

[51] Y. Rav, *On the representation of rational numbers as a sum of a fixed number of unit fractions*, J. Reine Angew. Math. 222 1966 207–213.

[52] L. Rosati, *Sull'equazione diofantea* $4/n = 1/x_1 + 1/x_2 + 1/x_3$, Boll. Un. Mat. Ital. (3) **9**, (1954). 59-63.

[53] J. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962) 64-94.

[54] I.Z. Ruzsa, *On an additive property of squares and primes,* Acta Arithmetica **49** (1988), 281–289.

[55] J.W. Sander. On $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ and Rosser's sieve. *Acta Arithmetica* 59 (1991), 183–204.

[56] J.W. Sander. On $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ and Iwaniec' Half Dimensional Sieve. *Journal of Number Theory* 46 (1994), 123–136.

[57] J.W. Sander. Egyptian Fractions and the Erdős-Straus Conjecture. *Nieuw Archief voor Wiskunde (4)* 15 (1997),43–50.

[58] G. Sándor, *Über die Anzahl der Lösungen einer Kongruenz*, Acta. Math. **87** (1952), 13–17.

[59] A. Schinzel, *On sums of three unit fractions with polynomial denominators*, Funct. Approx. Comment. Math. 28:187–194, 2000.

[60] W. Schwarz, J. Spilker, Arithmetical functions. London Mathematical Society Lecture Note Series, 184. Cambridge University Press, Cambridge, 1994.

[61] E.J. Scourfield, *The divisors of a quadratic polynomial*, Proc. Glasgow Math. Assoc. 5 (1961) 8–20.

[62] A. Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc. (N.S.) 20 (1956), 47–87.

[63] Shen Zun, *On the diophantine equation* $\sum_{i=0}^{k} \frac{1}{x_i} = \frac{a}{n}$, Chinese Ann. Math. Ser. B, **7** (1986), 213–220.

[64] P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. **313** (1980), 161–170.

[65] W. Sierpiński, *Sur les décompositions de nombres rationnels en fractions primaires*, Mathesis **65** (1956), 16–32, MR 17#1185d.

[66] W. Sierpiński. *On the Decomposition of Rational Numbers into Unit Fractions (Polish)*. Pánstwowe Wydawnictwo Naukowe, Warsaw, 1957.

[67] E. Sós. Die diophantische Gleichung $\frac{1}{x} = \frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}$. *Zeitschrift für mathematischen und naturwissenschaftlichen Unterricht*, 36:97–102, 1905.

[68] B.M. Stewart. *Theory of Numbers*. 2nd ed. New York: The Macmillan Company; London: Collier-Macmillan, 1964.

[69] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. 4 (1991), no. 4, 793–835.

[70] A. Swett, `http://math.uindy.edu/swett/esc.htm` accessed on 27 July 2011.

[71] G. Tenenbaum, Introduction to analytic and probabilistic number theory. Cambridge Studies in Advanced Mathematics, 46. Cambridge University Press, Cambridge, 1995.

[72] D.G. Terzi. On a conjecture by Erdős-Straus. *Nordisk Tidskr. Informations-Behandling (BIT)* 11 (1971), 212–216.

[73] R. Vaughan, *On a problem of Erdős, Straus and Schinzel*, Mathematika **17**, 1970 193–198.

[74] C. Viola, *On the diophantine equations* $\prod_0^k x_i - \sum_0^k x_i = n$ *and* $\sum_0^k \frac{1}{x_i} = \frac{a}{n}$, Acta Arith. **22** 1973, 339–352.

[75] W. Webb, *On* $4/n = 1/x + 1/y + 1/z$, Proc. Amer. Math. Soc. **25** (1970), 578–584.

[76] W. Webb, *On a theorem of Rav concerning Egyptian fractions*, Canad. Math. Bull. 18 (1975), no. 1, 155156.

[77] W. Webb, *On the Diophantine equation* $\frac{k}{n} = \frac{a_1}{x_1} + \frac{a_2}{x_2} + \frac{a_3}{x_3}$, Časopis pro pěstováni matematiy, roč. 101 (1976), 360–365.

[78] A. Wintner, Eratosthenian Averages. Waverly Press, Baltimore, Md., 1943. v+81 pp.

[79] K. Yamamoto, *On the Diophantine Equation* $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, Mem Fac. Sci. Kyushu Univ. Ser. A, V. **19**, No. 1, 1965, 37–47.
[80] Xun Qian Yang. A note on $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$. *Proceedings of the American Mathematical Society*, 85 (1982), 496–498.

Institut für Mathematik A, Steyrergasse 30/II, Technische Universität Graz, A-8010 Graz, Austria
E-mail address: elsholtz@math.tugraz.at

Department of Mathematics, UCLA, Los Angeles CA 90095-1555
E-mail address: tao@math.ucla.edu