ASYMPTOTICS OF $D(q)$-PAIRS AND TRIPLES VIA L-FUNCTIONS OF DIRICHLET CHARACTERS

NIKOLA ADŽAGA, GORAN DRAŽIĆ, ANDREJ DUJELLA, AND ATTILA PETHŐ

ABSTRACT. Let q be an integer. A $D(q)$-m-tuple is a set of m distinct positive integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i a_j + q$ is a perfect square for all $1 \leqslant i < j \leqslant m$. By counting integer solutions $x \in [1, b]$ of congruences $x^2 \equiv q \pmod{b}$ with $b \leqslant N$, we count $D(q)$-pairs with both elements up to N, and give estimates on asymptotic behaviour. We show that for prime q, the number of such $D(q)$-pairs and $D(q)$-triples grows linearly with N. Up to a factor of 2, the slope of this linear function is the quotient of the value of the L-function of an appropriate Dirichlet character (usually a Kronecker symbol) and of $\zeta(2)$.

1. INTRODUCTION

A Diophantine pair is a set of two positive integers $\{a, b\}$ such that $ab + 1$ is a perfect square. Dujella has proven that the number of Diophantine pairs with both elements less than or equal to N asymptotically grows as $\frac{6}{\pi^2} N \log N$ in [Duj08] (while the error term was further estimated in [Lao10]). The problem is equivalent to counting solutions of $x^2 \equiv 1 \pmod{n}$, where n ranges from 1 to N. This congruence has $2^{\omega(n)}$ solutions for each n (where $\omega(n)$ denotes the number of distinct prime factors of n), so the problem is reduced to estimating the sum $\sum_{n=1}^{N} 2^{\omega(n)}$.

In [Duj08], it was also shown that the number of Diophantine triples (i.e. the number of sets of three positive integers such that the product of any two is one less than a perfect square) is roughly half of the number of Diophantine pairs, while the number of Diophantine quadruples was shown to have the order of magnitude of $\sqrt[3]{N} \log N$. Martin and Sitar in [MS11] have then determined that the number of Diophantine quadruples with all elements less than or equal to N asymptotically grows as $\frac{2^{4/3}}{3\Gamma(2/3)^3} \sqrt[3]{N} \log N$.

One natural generalization of Diophantine m-tuples is obtained by replacing 1 with a different but fixed integer: $D(q)$-m-tuple is a set of m positive integers $\{a_1, \ldots, a_m\}$ such that $a_i a_j + q$ is a perfect square for all $1 \leqslant i < j \leqslant m$. So far, infinitely many $D(q)$-quadruples have been found only for square numbers q. Therefore, we wish to estimate the number of $D(q)$-pairs and $D(q)$-triples. Denote by $D_{m,q}(N) := |\{S \subset \{1, 2, \ldots, N\} : S \text{ is a } D(q)\text{-}m\text{-tuple}\}|$.

We often deal with quadratic congruences $x^2 \equiv q \pmod{b}$, where b and q are integers and $b \geqslant 2$. Under the number of its solutions we mean the number of integers $x \in [1, b]$ satisfying it.

Let q be any integer such that $|q|$ is prime. In this paper we estimate $D_{2,q}(N)$, the number of $D(q)$-pairs (a, b) such that $a < b$ where b ranges from 1 to N. We do this by counting the

number of solutions of congruences

$$(1) \qquad\qquad x^2 \equiv q \pmod{b}$$

where b ranges from 1 to N. We will prove asymptotic estimates on the number of solutions to said congruence equations, and these estimates will easily translate to $D_{2,q}(N)$, since the two quantities differ by $O(1)$.

In Section 2 we explain how the problem reduces to counting solutions of congruences (1). We use quadratic reciprocity to characterize moduli b such that equation (1) has a solution, and express the number of its solutions (in a complete residue system) as a function of the number of distinct prime factors of b. Finally, we proceed to estimate the relevant weighted sums (of $2^{\omega(n)}$) by analyzing their Dirichlet series and applying a tauberian theorem.

L-functions of Dirichlet characters appear in our results – we use the same notation as in LMFDB [LMFDB], and the relevant background is stated in the Appendix of this paper to make it self-contained.

Here we state our results for prime 2 (and -2).

Theorem 1. *The number of $D(2)$-pairs with both elements in the set $\{1, 2, \ldots, N\}$ satisfies*

$$D_{2,2}(N) \sim \frac{L(1, \chi_{8,5})}{\zeta(2)} \cdot N \approx 0.37888N,$$

while the number of $D(-2)$-pairs with both elements in the set $\{1, 2, \ldots, N\}$ satisfies

$$D_{2,-2}(N) \sim \frac{L(1, \chi_{8,3})}{\zeta(2)} \cdot N \approx 0.67524N.$$

The estimates for other primes q are more involved. The results depend on the remainder of prime q modulo 8 (i. e. on the power of 2 dividing $q - 1$), and it turns out that the relevant Dirichlet character is always the Kronecker symbol.

Theorem 2. *Let q be an integer such that $|q|$ is a prime or $q = -1$, and denote by $D_{2,q}(N)$ the number of $D(q)$-pairs with both elements in the set $\{1, 2, \ldots, N\}$.*

a) *If $q \equiv 3 \pmod 4$, then*

$$D_{2,q}(N) \sim \frac{L(1, \chi_{4|q|,4|q|-1})}{\zeta(2)} \cdot N.$$

b) *If $q \equiv 5 \pmod 8$, then*

$$D_{2,q}(N) \sim \frac{2L(1, \chi_{|q|,|q|-1})}{\zeta(2)} \cdot N.$$

c) *If $q \equiv 1 \pmod 8$, then*

$$D_{2,q}(N) \sim \frac{L(1, \chi_{|q|,|q|-1})}{\zeta(2)} \cdot N.$$

In the last section, for any integer n, we relate the number of $D(n)$-triples with all elements up to N with the number of $D(n)$-pairs. More precisely, we show the following theorem.

Theorem 3. *Let n be an integer. The number of $D(n)$-triples with all elements in the set $\{1, 2, \ldots, N\}$ is asymptotically equal to half the number of $D(n)$-pairs. More precisely,*

$$D_{3,n}(N) \sim \frac{D_{2,n}(N)}{2}.$$

Finally, we list the estimates we obtain (by applying Theorem 1 and Theorem 2) on the number of $D(q)$-triples for integers q such that $|q|$ is prime.

2. REDUCING THE PROBLEM TO CONGRUENCES

The results of this section hold for arbitrary integer q (not necessarily prime). We estimate the number of $D(q)$-pairs (a, b) such that $a < b$ using the number of solutions x of the equation (1). Almost all such solutions induce a $D(q)$ pair (a, b) such that $a \leqslant b$, simply by setting $a = \frac{x^2 - q}{b}$. The almost part comes from the fact that $x^2 - q$ can be negative, but the total amount of such cases for all $b \in \mathbb{N}$ is finite. Also, almost all $D(q)$ pairs (a, b) such that $a < b$ are induced by a solution of Equation (1). It is possible that there exist pairs $(a, b), a < b$ such that $a > \frac{x^2 - q}{b}$ for all solutions of Equation (1). Then there exists some $x \geqslant b + 1$ such that $a = \frac{x^2 - q}{b}$. This leads to $b \geqslant a \geqslant \frac{(b+1)^2 - q}{b} \iff b \leqslant \frac{q-1}{2}$. All in all, again only finitely many cases when b runs through $\mathbb{N}$. For the sake of our calculations, we identify the number of $D(q)$ pairs (a, b) such that $a < b$ with the number of solutions of Equation (1).

Lemma 4. *Let q be an odd prime and $b \in \mathbb{N}$ such that $\gcd(b, 2q) = 1$. Then the number of solutions of the congruence*

$$(2) \qquad\qquad x^2 \equiv 1 \pmod{b}$$

such that $1 \leqslant x \leqslant b$ is $2^{\omega(b)}$. Consequently, the number of solutions of the congruence

$$(1) \qquad\qquad x^2 \equiv q \pmod{b}$$

such that $1 \leqslant x \leqslant b$ is either zero or $2^{\omega(b)}$.

Proof. The first statement of the lemma is proved in [Vin03, Section V.4]. If there is no solution to Equation (1), we are done. If there exists a solution x_q, then every other solution x' of Equation (1) satisfies

$$(3) \qquad\qquad \left(\frac{x'}{x_q}\right)^2 \equiv 1 \pmod{b},$$

where division by x_q corresponds to multiplying by the inverse of x_q modulo b. Also, if x_1 is any solution to Equation (2), then $x_1 x_q$ is a solution of Equation (1) and all solutions obtained in such a way have different residues mod b. $\qquad\square$

We now give all the details for Theorem 1. Estimating the number of $D(2)$-pairs is somewhat easier than estimating the number of $D(q)$-pairs for other prime q. However, as the proof of this theorem contains all the essential steps necessary for all other q, we believe that reading this first will make it easier for the reader to follow the more involved proofs.

3. ESTIMATING THE NUMBER OF $D(2)$-PAIRS AND $D(-2)$-PAIRS

We first estimate $D_{2,2}(N)$, the number of $D(2)$-pairs up to N, by counting solutions of the congruence (1) for $q = 2$, and proceed similarly for $D_{2,-2}$.

3.1. **Existence and the number of congruence solutions.**
In the next lemma, we record when does the relevant congruence equation have a solution, as well as the number of its solutions.

Lemma 5. *For odd b, the equation*

$$(4) \qquad x^2 \equiv 2 \pmod{b},$$

has a solution if and only if each prime factor p of b satisfies $p \equiv \pm 1 \pmod 8$. For even b, equation (4) has a solution if and only if $2\|b$ and each odd prime factor p of b satisfies $p \equiv \pm 1 \pmod 8$.

Analogously, the equation

$$(5) \qquad x^2 \equiv -2 \pmod{b}$$

has a solution if and only if each prime factor p of b satisfies $p \equiv 1,3 \pmod 8$. For even b, equation (5) has a solution if and only if $2\|b$ and each odd prime factor p of b satisfies $p \equiv 1,3 \pmod 8$.

When equation (4) or (5) is solvable with odd b, the number of its solutions x such that $1 \leqslant x \leqslant b$ is exactly $2^{\omega(b)}$.

Proof. Since $b \mid x^2 - 2$ implies that for each prime factor p of b it holds that $p \mid x^2 - 2$, we have to check for which primes p is 2 a quadratic residue. The statement on the existence of solutions then holds because $x^2 - 2$ cannot be divisible by 4 and because

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

and analogously for -2. The last statement follows from Lemma 4. $\qquad\square$

The previous lemma motivates us to define the set of *good primes* as

$$\mathcal{G}_2 = \{p \in \mathbb{P} \colon p \equiv \pm 1 \pmod 8\}.$$

The set of good primes for -2 is given by

$$\mathcal{G}_{-2} = \{p \in \mathbb{P} \colon p \equiv 1,3 \pmod 8\}.$$

The sum $\sum_{n=1}^{N} 2^{\omega(n)}$ is already estimated in [Duj08], but now we have to estimate a weighted version of this sum. The weights are binary, i.e. non-zero if n consists only of good prime factors:

$$\lambda_{\mathcal{G}_2}(n) = \begin{cases} 1, & \text{if } n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \quad p_i \in \mathcal{G}_2 \ \forall i = 1, \ldots, k \\ 0, & \text{otherwise.} \end{cases}$$

To begin estimating the weighted sum, we define

$$b_2(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}_2}(n).$$

If n has only good prime factors, then $b_2(n)$ is equal to the number of solutions to congruence $x^2 \equiv 2 \pmod{n}$, otherwise the value of $b_2(n)$ is zero. We want to estimate the weighted sum

$$B_2(N) = \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}_2}(n) = \sum_{1 \leqslant n \leqslant N} b_2(n).$$

$B_2(N)$ counts the total number of solutions $x \in \{1, \ldots, n\}$ of all congruences $x^2 \equiv 2 \pmod{n}$ where n is odd and $1 \leqslant n \leqslant N$. We will account for the possibility of $2 \| n$ later, so understanding the asymptotic behavior of $B_2(N)$ will be enough to understand $D_{2,2}(N)$.

3.2. **Dirichlet series manipulation.** To understand the asymptotic behavior of $B_2(N)$, we analyze the behavior of the Dirichlet series $\beta_2(s) = \mathcal{D}b_2(s)$, where

$$\beta_2(s) = \mathcal{D}b_2(s) = \sum_{n=1}^{\infty} \frac{b_2(n)}{n^s} = \sum_{n=1}^{\infty} \frac{2^{\omega(n)} \lambda_{\mathcal{G}_2}(n)}{n^s}.$$

The next lemma will be used throughout the following sections as well, so we state it in a more general manner.

Lemma 6. *Let $\mathcal{G}$ be a set of primes called* good *primes. Let $\lambda_G \colon \mathbb{N} \to \{0, 1\}$ be the indicator function of a multiplicative monoid in $\mathbb{N}$ generated by $\mathcal{G}$. Then the Dirichlet series $\beta(s)$ of $b(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n)$ satisfies*

$$\beta(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)},$$

for $\Re s > 1$, where $\zeta_{\mathcal{G}}(s)$ is

$$\zeta_{\mathcal{G}}(s) := \mathcal{D}\lambda_{\mathcal{G}}(s) = \sum_{n=1}^{\infty} \frac{\lambda_{\mathcal{G}}(n)}{n^s}.$$

Proof. Since Dirichlet series behave nicely with respect to Dirichlet convolution, we wish to express $B(N)$ as a convolution of two arithmetic functions. One of these functions will be *the $\mathcal{G}$-modified Möbius function* which we define as

$$\mu_{\mathcal{G}}(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if } n = p_1 \ldots p_k, \quad p_i \in \mathcal{G} \ \forall i = 1, \ldots, k, \text{ and } p_i \neq p_j \text{ whenever } i \neq j \\ 0, & \text{otherwise} \end{cases}.$$

Now we can express

$$B(N) = \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) = \sum_{1 \leqslant n \leqslant N} \sum_{d | n} \mu_{\mathcal{G}}^2(d) \cdot \lambda_{\mathcal{G}}(n)$$

$$\stackrel{(**)}{=} \sum_{1 \leqslant n \leqslant N} \sum_{d | n} \mu_{\mathcal{G}}^2(d) \cdot \lambda_{\mathcal{G}}\left(\frac{n}{d}\right) = \sum_{1 \leqslant n \leqslant N} \left(\mu_{\mathcal{G}}^2 * \lambda_{\mathcal{G}}\right)(n)$$

where equality $(**)$ holds because of the following fact: If n only has good prime factors then $\lambda_{\mathcal{G}}\left(\frac{n}{d}\right) = \lambda_{\mathcal{G}}(n)$ for any d such that $d | n$. If n has at least one bad prime factor then $\lambda_{\mathcal{G}}(n) = 0$, as well as $\mu_{\mathcal{G}}^2(d) \cdot \lambda_{\mathcal{G}}\left(\frac{n}{d}\right) = 0$.

Since $\mathcal{D}(\mu_{\mathcal{G}}^2 * \lambda_{\mathcal{G}})(s) = \mathcal{D}\mu_{\mathcal{G}}^2(s)\mathcal{D}\lambda_{\mathcal{G}}(s)$, we only need to calculate $\mathcal{D}\mu_{\mathcal{G}}^2(s)$. As $\mu_{\mathcal{G}}^2$ is multiplicative, we can expand $\mathcal{D}\mu_{\mathcal{G}}^2(s)$ into an Euler product (see e.g. [MV06, Theorem 1.9] – this theorem is also stated herein at the end of the Appendix as Theorem 28) to obtain

$$\mathcal{D}(\mu_{\mathcal{G}}^2) = \prod_{p \in \mathcal{G}} \left(1 + \frac{1}{p^s}\right) = \frac{\prod_{p \in \mathcal{G}}\left(1 - \frac{1}{p^{2s}}\right)}{\prod_{p \in \mathcal{G}}\left(1 - \frac{1}{p^s}\right)} = \frac{\prod_{p \in \mathcal{G}}\left(1 - \frac{1}{p^s}\right)^{-1}}{\prod_{p \in \mathcal{G}}\left(1 - \frac{1}{p^{2s}}\right)^{-1}} = \frac{\zeta_{\mathcal{G}}(s)}{\zeta_{\mathcal{G}}(2s)} \qquad \square$$

We obtain the following corollary by noting that our $\lambda_{\mathcal{G}_2}$ and $\lambda_{\mathcal{G}_{-2}}$ are indicator functions as required by the previous lemma.

Corollary 7. *The Dirichlet series $\beta_2(s)$ and $\beta_{-2}(s)$ satisfy*

$$(6) \qquad \beta_2(s) = \frac{\zeta_{\mathcal{G}_2}^2(s)}{\zeta_{\mathcal{G}_2}(2s)}, \quad \beta_{-2}(s) = \frac{\zeta_{\mathcal{G}_{-2}}^2(s)}{\zeta_{\mathcal{G}_{-2}}(2s)},$$

where $\zeta_{\mathcal{G}_2}$ and $\zeta_{\mathcal{G}_{-2}}$ are the Dirichlet series of $\lambda_{\mathcal{G}_2}$ and $\lambda_{\mathcal{G}_{-2}}$.

Using the previous corollary, we show how β_2 and β_{-2} can be expressed in terms of the classical zeta function and the L-functions of certain Dirichlet characters.

Lemma 8. *The following holds.*

    a) *The Dirichlet series $\beta_2(s) = \mathcal{D}b_2(s)$ of $b_2(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}_2}(n)$ satisfies*

$$\beta_2(s) = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{8,5})}{(1 + 2^{-s})}.$$

    b) *The Dirichlet series $\beta_{-2}(s) = \mathcal{D}b_{-2}(s)$ of $b_{-2}(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}_{-2}}(n)$ satisfies*

$$\beta_{-2}(s) = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{8,3})}{(1 + 2^{-s})}.$$

Proof. We begin proving a) by complementing the Euler product of $\zeta_{\mathcal{G}_2}$ from Corollary 7 to obtain the usual zeta function:

$$\zeta_{\mathcal{G}_2}(s) = \prod_{p \in \mathcal{G}_2} (1 - p^{-s})^{-1} = \zeta(s) \prod_{p \notin \mathcal{G}_2} (1 - p^{-s})$$

$$= \zeta(s)(1 - 2^{-s}) \prod_{p \equiv 3} (1 - p^{-s}) \prod_{p \equiv 5} (1 - p^{-s}),$$

where the products go over all primes p congruent to 3 and 5 modulo 8 (according to our description of $\mathcal{G}_2$, the primes that are not in $\mathcal{G}_2$ include 2 and all primes of this form). The further products will also go over congruences modulo 8.

We now rewrite

$$\frac{\zeta_{\mathcal{G}_2}^2(s)}{\zeta_{\mathcal{G}_2}(2s)} = \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1 - 2^{-s})^2}{(1 - 2^{-2s})} \cdot \frac{\prod_{p \equiv 3}(1 - p^{-s})^2 \prod_{p \equiv 5}(1 - p^{-s})^2}{\prod_{p \equiv 3}(1 - p^{-2s}) \prod_{p \equiv 5}(1 - p^{-2s})}$$

$$= \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1 - 2^{-s})}{(1 + 2^{-s})} \cdot \frac{\prod_{p \equiv 3}(1 - p^{-s}) \prod_{p \equiv 5}(1 - p^{-s})}{\prod_{p \equiv 3}(1 + p^s) \prod_{p \equiv 5}(1 + p^{-s})}.$$

We invert our products and complement them with the remaining possible remainder of an odd prime modulo 8:

$$\frac{\zeta_{\mathcal{G}_2}^2(s)}{\zeta_{\mathcal{G}_2}(2s)} = \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1-2^{-s})}{(1+2^{-s})} \cdot \frac{\prod\limits_{p\equiv1}(1-p^{-s})^{-1}\prod\limits_{p\equiv3}(1+p^s)^{-1}\prod\limits_{p\equiv5}(1+p^{-s})^{-1}\prod\limits_{p\equiv7}(1-p^{-s})^{-1}}{\prod\limits_{p\equiv1}(1-p^{-s})^{-1}\prod\limits_{p\equiv3}(1-p^s)^{-1}\prod\limits_{p\equiv5}(1-p^{-s})^{-1}\prod\limits_{p\equiv7}(1-p^{-s})^{-1}}$$

$$= \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1-2^{-s})}{(1+2^{-s})} \cdot \frac{L(s,\chi_{8,5})}{L(s,\chi_{8,1})} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s,\chi_{8,5})}{(1+2^{-s})}.$$

For b) part about -2, the proof is completely analogous, and the character $\chi_{8,3}$ appears instead of $\chi_{8,5}$ due to a different set of good primes $\mathcal{G}_{-2}$. $\square$

3.3. The total number of solutions of all congruences with odd moduli.
The asymptotic behaviour of $B_2(N) = \sum\limits_{1\leqslant n\leqslant N} b_2(n)$ is a direct consequence of a corollary of a theorem by Wiener and Ikehara.

Theorem 9 (Corollary of Wiener-Ikehara [Ike31]). *Let $a(n) \geqslant 0$. If the Dirichlet series of the form*

$$\sum_{n=1}^{\infty} a(n)n^{-s}$$

converges to an analytic function in the half-plane $\Re(s) \geqslant 1$ with a simple pole of residue c at $s = 1$, then

$$\sum_{n\leqslant N} a(n) \sim cN.$$

Let us remind the reader that $B_2(N)$ counts the total number of solutions $x \in \{1,\ldots,n\}$ of all congruences $x^2 \equiv 2 \pmod{n}$ where n is odd and $1 \leqslant n \leqslant N$.

Proposition 10. *The following holds.*

a) *The partial sums of $b_2(n)$ satisfy*

$$B_2(N) \sim \frac{2L(1,\chi_{8,5})}{3\zeta(2)} \cdot N \approx 0.25258N.$$

b) *The partial sums of $b_{-2}(n)$ satisfy*

$$B_{-2}(N) \sim \frac{2L(1,\chi_{8,3})}{3\zeta(2)} \cdot N \approx 0.45016N.$$

Proof. The function $B_2(N) = \sum\limits_{n\leqslant N} b_2(n)$ is the partial sum of the sequence $(b_2(n))_{n\geqslant1}$ with Dirichlet series rewritten in Lemma 8 as

$$\beta_2(s) = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s,\chi_{8,5})}{(1+2^{-s})}.$$

The function $\beta_2(s)$ is analytic on the half-plane given by $\Re s > 1$, and to apply the previous theorem, we need the residue at $s = 1$. Among all factors, only $\zeta(s)$ is not holomorphic at

$s = 1$. Factors in the denominators have no zeroes for $\Re s > \frac{1}{2}$. Since $\zeta(s)$ has a simple pole at $s = 1$, we will multiply its residue, which is equal to 1, with the value of the remaining factors at $s = 1$. Therefore the residue of $\beta_2(s)$ at $s = 1$ is $\frac{1}{\zeta(2)} \cdot \frac{2L(1,\chi_{8,5})}{3}$ and the claim now follows by the Wiener-Ikehara theorem. Part b) is completely analogous. $\qquad\square$

Remark 11. One could likely use Perron's formula to find the explicit error term, but this would be computationally harder than our determination of the main term.

3.4. **The asymptotics of $D_{2,2}(N)$ and $D_{2,-2}(N)$.** We can now finally prove that $D_{2,2}(N)$, the number of $D(2)$-pairs up to N, grows linearly with N and determine its gradient.

Proof of Theorem 1. The number of $D(2)$-pairs up to N is equal to the number of congruence solutions $x^2 \equiv 2 \pmod{n}$ with $x \in \{1, 2, \ldots, n\}$ and $n \in \{1, \ldots, N\}$ plus some $O(1)$. Let us denote the number of congruence solutions by $C_2(N)$. We now let n vary through all integers between 1 and N, both odd and even. For even n, since 2 and $n/2$ are coprime (due to $2\|n$), the number of solutions is $2^{\omega(n/2)} = 2^{\omega(n)-1}$. The total count of congruence solutions for $n \leqslant N$ is hence

$$C_2(N) = \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) + \sum_{\substack{1 \leqslant n \leqslant N \\ 2\|n}} 2^{\omega(n)-1} \cdot \lambda_{\mathcal{G}}\left(\frac{n}{2}\right) = B_2(N) + B_2\left(\left\lfloor \frac{N}{2} \right\rfloor\right).$$

Since $B_2(N) \sim \frac{2L(1,\chi_{8,5})}{3\zeta(2)} \cdot N$, it follows that $C_2(N) \sim \left(1 + \frac{1}{2}\right) \frac{2L(1,\chi_{8,5})}{3\zeta(2)} \cdot N = \frac{L(1,\chi_{8,5})}{\zeta(2)} \cdot N$, where the error from replacing the floor of $N/2$ by $N/2$ is $O(1)$. Part b) is again completely analogous. $\qquad\square$

4. ESTIMATING THE NUMBER OF $D(q)$-PAIRS FOR ODD PRIMES q

The asymptotic estimation and its proof will have the same outline for odd primes q, with the following differences. In Subsection 4.1, we determine whether the congruence (1) has a solution by using quadratic reciprocity (instead of its supplement for ± 2). In Subsection 4.2, we carefully analyze the number of solutions with respect to the occurrences of primes 2 and q in n. The usage of the Wiener-Ikehara theorem requires identifying proper characters and computing the residue in the same manner – this is done in Subsection 4.3. Expressions for $C(N)$, the total count of solutions of all congruences, are going to vary according to the possible appearances of primes 2 and q in the prime factorization of n. This final analysis is done in Subsection 4.4.

4.1. **Existence of congruence solutions.** We first investigate when equation (1) has a solution. Since the number of solutions is 0 or $2^{\omega(b)}$, in the next several lemmas we give conditions on whether the number of solutions is non-zero, depending on the residue of q modulo 8.

Lemma 12. *Let prime $q \equiv 3 \pmod 4$. Equation (1) has a solution if and only if $b = \delta \prod_{p_i \neq q} p_i^{\alpha_i}$ such that $\left(\frac{q}{p_i}\right) = 1$ for all i, and $\delta \in \{1, 2, q, 2q\}$. The condition $\left(\frac{q}{p_i}\right) = 1$ is equivalent to $\left(\frac{p_i}{q}\right) = (-1)^{\frac{p_i-1}{2}}$.*

Proof. First we notice that no higher powers of 2 or q are possible in the factorization of b. The number b is not divisible by 4 since that would imply that 4 divides $x^2 - 3$, whereas b is not divisible by q^2 since then q^2 would divide $x^2 - q$. If $\gcd(b, 2q) = 1$ and $x^2 \equiv q \pmod{b}$ then exactly one of the numbers $x, x + b, x + 2b, \ldots, x + (2q - 1)b$ will be the solution of $y^2 \equiv q \pmod{2qb}$. This means it is enough to analyze the case $\gcd(b, 2q) = 1$.

We now focus on such b. Assume that for a fixed b, Equation (1) has a solution x_0 and let $p | b$. Then $x^2 \equiv q \pmod{p}$, which by quadratic reciprocity implies that $1 = \left(\frac{q}{p} \right) = \left(\frac{p}{q} \right) \cdot (-1)^{\frac{p-1}{2}}$. We call p *good for* q if $\left(\frac{p}{q} \right) = (-1)^{\frac{p-1}{2}}$.

We proved that b must be of the form given in the statement of the lemma. Now we prove that every such b works.

Assume p is good for q. We prove by induction that $x^2 \equiv q \pmod{p^n}$ has a solution for every $n \in \mathbb{N}$. The base case is true because from the fact that p is good for q we have that $1 = \left(\frac{p}{q} \right) \cdot (-1)^{\frac{p-1}{2}} = \left(\frac{q}{p} \right)$, that is q is a quadratic residue mod p. Let x_0 be a solution for p^n. If it is also a solution for p^{n+1}, we are done. Otherwise, look at the numbers $x_0, x_0 + p^n, x_0 + 2p^n, \ldots, x_0 + (p - 1)p^n$, more specifically, for $i \neq j$, look at $\left[(x_0 + ip^n)^2 - q \right] - \left[(x_0 + jp^n)^2 - q \right] = (i - j)p^n(2x_0 + (i + j)p^n)$. Since $\gcd(p, 2q) = 1$ we know that $p \nmid 2x_0 + (i + j)p^n$ and trivially $p \nmid i - j$, so the numbers $(x_0 + ip^n)^2 - q$ give p different residues $\pmod{p^{n+1}}$ and one of these numbers must be divisible by p^{n+1}.

If $\gcd(b_1, b_2) = 1$ and $x_i^2 \equiv q \pmod{b_i}$, then $\{x_1, x_1 + b_1, \ldots, x_1 + (b_2 - 1)b_1\}$ is the complete residue system mod b_2 so one of the elements must be the solution of the equation $x^2 \equiv q \pmod{b_2}$. As each of these numbers is also a solution to the equation $x^2 \equiv q \pmod{b_1}$, then there is at least one simultaneous solution (this also follows from the Chinese remainder theorem). $\qquad \square$

Lemma 13. *Let prime $q \equiv 5 \pmod{8}$. Equation (1) has a solution if and only if $b = \delta \prod p_i^{\alpha_i}$ such that $\left(\frac{p_i}{q} \right) = 1$ for all i, and $\delta \in \{1, 2, 4, q, 2q, 4q\}$.*

Let prime $q \equiv 1 \pmod{8}$. Equation (1) has a solution if and only if $b = \delta \cdot 2^{\alpha_0} \prod p_i^{\alpha_i}$ such that $\left(\frac{p_i}{q} \right) = 1$ for all i, and $\delta \in \{1, q\}$.

Proof. If $q \equiv 5 \pmod{8}$ the proof mimics that of Lemma 12. If $q \equiv 1 \pmod{8}$ we only need to prove that any power of 2 is possible as a factor of b. We again do this by induction. Taking any odd x, we have $x^2 \equiv q \pmod{8}$. For any odd b such that there exists a solution to Equation (1) we can construct a solution of $x^2 \equiv q \pmod{8b}$ since $\gcd(8, b) = 1$, so a base case follows. Let x be such that $x^2 \equiv q \pmod{2^\alpha b}$ where b is odd. If it is also true that $x^2 \equiv q \pmod{2^{\alpha+1}b}$ we are done, otherwise look at $x + b \cdot 2^{\alpha-1}$. Now we have $(x + b \cdot 2^{\alpha-1})^2 - q = x^2 - q + xb2^\alpha + b^2 2^{2\alpha-2}$. The right hand side is divisible by b, the number $2^{2\alpha-2}$ is divisible by $2^{\alpha+1}$ since $\alpha \geqslant 3$, and both numbers $x^2 - q$ and $xb2^\alpha$ are divisible by exactly 2^α so their sum is divisible by $2^{\alpha+1}$. $\quad \square$

Lemma 14. *Let $p, |q|$ be odd primes such that $|q| \neq p$. Then*

$$\left(\frac{q}{p} \right) = \left(\frac{p}{|q|} \right) \cdot (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

Proof. If $q > 0$ then this is simply quadratic reciprocity. If $q < 0$ we have

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{|q|}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{|q|}\right)\cdot(-1)^{\frac{p-1}{2}\frac{|q|-1}{2}} = \left(\frac{p}{|q|}\right)\cdot(-1)^{\frac{p-1}{2}\frac{|q|+1}{2}}$$

$$= \left(\frac{p}{|q|}\right)\cdot(-1)^{\frac{p-1}{2}\frac{-q+1}{2}} = \left(\frac{p}{|q|}\right)\cdot(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

$\square$

4.2. The number of congruence equation solutions. The following lemma counts the number of solutions when they exist. Some results in it could be written in a shorter form, but this form was chosen to make further proofs easier to understand.

Lemma 15. *(Extension of Lemma 1) Let $|q|$ be a prime number and $b \in \mathbb{N}$ such that $\gcd(b, 2q) = 1$, and b has only good prime factors for q.*

Let $q \equiv 3 \pmod 4$. Then the following table gives the number of solutions of the congruence equation in the appropriate interval

equation	interval	the number of solutions in the interval
$x^2 \equiv q \pmod{2b}$	$1 \leqslant x \leqslant 2b$	$2^{\omega(2b)-1}$
$x^2 \equiv q \pmod{qb}$	$1 \leqslant x \leqslant |q|b$	$2^{\omega(qb)-1}$
$x^2 \equiv q \pmod{2qb}$	$1 \leqslant x \leqslant 2|q|b$	$2^{\omega(2qb)-2}$

Let $q \equiv 5 \pmod 8$. Then the following table gives the number of solutions of the congruence equation in the appropriate interval

equation	interval	the number of solutions in the interval
$x^2 \equiv q \pmod{2b}$	$1 \leqslant x \leqslant 2b$	$2^{\omega(2b)-1}$
$x^2 \equiv q \pmod{4b}$	$1 \leqslant x \leqslant 4b$	$2^{\omega(4b)}$
$x^2 \equiv q \pmod{qb}$	$1 \leqslant x \leqslant |q|b$	$2^{\omega(qb)-1}$
$x^2 \equiv q \pmod{2qb}$	$1 \leqslant x \leqslant 2|q|b$	$2^{\omega(2qb)-2}$
$x^2 \equiv q \pmod{4qb}$	$1 \leqslant x \leqslant 4|q|b$	$2^{\omega(4qb)-1}$

Let $q \equiv 1 \pmod 8$ and $n \in \mathbb{Z}$ such that $n \geqslant 0$. Then the following table gives the number of solutions of the congruence equation in the appropriate interval

equation	interval	the number of solutions in the interval
$x^2 \equiv q \pmod{2b}$	$1 \leqslant x \leqslant 2b$	$2^{\omega(2b)-1}$
$x^2 \equiv q \pmod{4b}$	$1 \leqslant x \leqslant 4b$	$2^{\omega(4b)}$
$x^2 \equiv q \pmod{2^{n+3}b}$	$1 \leqslant x \leqslant 2^{n+3}b$	$2^{\omega(2^{n+3}b)+1}$
$x^2 \equiv q \pmod{qb}$	$1 \leqslant x \leqslant |q|b$	$2^{\omega(qb)-1}$
$x^2 \equiv q \pmod{2qb}$	$1 \leqslant x \leqslant 2|q|b$	$2^{\omega(2qb)-2}$
$x^2 \equiv q \pmod{4qb}$	$1 \leqslant x \leqslant 4|q|b$	$2^{\omega(4qb)-1}$
$x^2 \equiv q \pmod{2^{n+3}qb}$	$1 \leqslant x \leqslant 2^{n+3}|q|b$	$2^{\omega(2^{n+3}qb)}$

Proof. We prove the statements $\pmod{qb}$. The number of solutions $\pmod{b}$ such that $1 \leqslant x \leqslant b$ is $2^{\omega(b)}$. Take any such solution x_0 and look at the numbers $x_0, x_0 + b, x_0 + 2b, \ldots, x_0 + (|q| - 1)b$. Exactly one of them will be divisible by q so there will be exactly $2^{\omega(b)} = 2^{\omega(qb)-1}$ solutions $\pmod{qb}$ in the interval $[1, |q|b]$.

The other cases are analogous, and the cases where the modulus and q are coprime also follow from [Vin03, V.4.g]. □

4.3. Sets of good primes $\mathcal{G}_q$ for various q with accompanying arithmetic functions.

As before with Lemma 5, Lemmas 12, 13 and 14 motivate definitions of sets $\mathcal{G}_q$ for various residues of $q \pmod 8$. Let $q \equiv 3 \pmod 4$ such that $|q|$ is prime and denote by $\mathcal{G}_q$ the set of good primes for q

$$\mathcal{G} = \mathcal{G}_q = \{p \in \mathbb{P} \colon \left(\frac{p}{|q|}\right) \equiv (-1)^{\frac{p-1}{2}}\},$$

and in addition for $q = -1$ let

$$\mathcal{G} = \mathcal{G}_{-1} = \{p \in \mathbb{P} \colon p \equiv 1 \pmod 4\}.$$

Let

$$\lambda_{\mathcal{G}}(n) = \begin{cases} 1, & \text{if } n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \quad p_i \in \mathcal{G} \\ 0, & \text{otherwise} \end{cases},$$

along with

$$b_q(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}_q}(n).$$

We want to estimate the weighted sum

$$B_q(N) = \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) = \sum_{1 \leqslant n \leqslant N} b_q(n).$$

$B_q(N)$ counts the total number of solutions $x \in \{1, \ldots, n\}$ of all congruences $x^2 \equiv q \pmod n$, where $\gcd(n, 2q) = 1$ and $1 \leqslant n \leqslant N$. We can easily account for possible factors of 2 and q in n later; understanding the asymptotic behavior of $B_q(N)$ will be enough to understand $D_{2,q}(N)$.

As before, we define the following two Dirichlet series (which both depend on q):

$$\zeta_{\mathcal{G}}(s) := \mathcal{D}\lambda_{\mathcal{G}}(s) = \sum \frac{\lambda_{\mathcal{G}}(n)}{n^s}, \quad \beta_q(s) := \mathcal{D}b_q(s) = \sum \frac{b_q(n)}{n^s},$$

for which Lemma 6 holds. We rewrite $\beta_q(s)$ in terms of the zeta function and the L-function of a Dirichlet character mod $4q$.

Lemma 16.

$$\beta_q(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{4|q|, 4|q|-1})}{(1 + 2^{-s})(1 + |q|^{-s})},$$

$$\beta_{-1}(s) = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{4,3})}{(1 + 2^{-s})}.$$

Proof. As in the proof of Lemma 8 we first rewrite $\zeta_{\mathcal{G}}(s)$:

$$\zeta_{\mathcal{G}}(s) = \prod_{p \in \mathcal{G}}(1 - p^{-s})^{-1} = \zeta(s)\prod_{p \notin \mathcal{G}}(1 - p^{-s})$$

$$= \zeta(s) \cdot (1 - 2^{-s})(1 - |q|^{-s}) \cdot \prod_{\substack{p \notin \mathcal{G} \\ p \neq 2,|q|}}(1 - p^{-s}).$$

Plugging this in the expression for $\beta_q(s)$ we have

$$\frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1 - 2^{-s})^2(1 - |q|^{-s})^2}{(1 - 2^{-2s})(1 - |q|^{-2s})} \cdot \prod_{\substack{p \notin \mathcal{G} \\ p \neq 2,|q|}}\frac{(1 - p^{-s})^2}{(1 - p^{-2s})}$$

$$= \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1 - 2^{-s})(1 - |q|^{-s})}{(1 + 2^{-s})(1 + |q|^{-s})} \cdot \prod_{\substack{p \notin \mathcal{G} \\ p \neq 2,|q|}}\frac{(1 - p^{-s})}{(1 + p^{-s})} \cdot \prod_{p \in \mathcal{G}}\frac{(1 - p^{-s})}{(1 - p^{-s})}$$

$$= \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{1}{(1 + 2^{-s})(1 + |q|^{-s})} \cdot \prod_{\substack{p \notin \mathcal{G} \\ p \neq 2,|q|}}(1 + p^{-s})^{-1}\prod_{p \in \mathcal{G}}(1 - p^{-s})^{-1}$$

$$= \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{4|q|,4|q|-1})}{(1 + 2^{-s})(1 + |q|^{-s})}.$$

The statement for β_{-1} follows the same proof, except there is no $(1 - |q|^{-s})$ factor in $\zeta_{\mathcal{G}}$ (and consequently, no $(1 + |q|^{-s})^{-1}$ in β_{-1}). $\qquad\square$

Proposition 17. *If $q \equiv 3 \pmod 4$ such that $|q|$ is prime, then* $B_q(N) \sim \frac{2|q|}{3(|q|+1)}\frac{L(1,\chi_{4|q|,4|q|-1})}{\zeta(2)}N$, *while* $B_{-1}(N) \sim \frac{2}{3}\frac{L(1,\chi_{4,3})}{\zeta(2)}N$.

Proof. Analogous to the proof of Proposition 10. $\qquad\square$

For $q \equiv 1, 5 \pmod 8$ we set

$$\mathcal{G} = \mathcal{G}_q = \left\{p \in \mathbb{P}\colon \left(\frac{p}{|q|}\right) = 1\right\}$$

and define $\lambda_{\mathcal{G}}, b_q(n), B_q(N), \zeta_{\mathcal{G}}(s), \beta_q(s)$ as in the case $q \equiv 3 \pmod 4$ (accordingly with respect to the appropriate set $\mathcal{G}$).

Lemma 18. *For $q \equiv 5 \pmod 8$ such that $|q|$ is prime we have*

$$\beta_q(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{|q|,|q|-1})}{(1 + |q|^{-s})},$$

while for $q \equiv 1 \pmod 8$ such that $|q|$ is prime we have

$$\beta_q(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{(1 - 2^{-s})L(s, \chi_{|q|,|q|-1})}{(1 + 2^{-s})(1 + |q|^{-s})}.$$

Proof. Analogous to the proof of Lemma 16. $\qquad\square$

Proposition 19. *If $q \equiv 5 \pmod 8$ then*

$$B_q(N) \sim \frac{|q|}{|q| + 1}\frac{L(1, \chi_{|q|,|q|-1})}{\zeta(2)}N,$$

and if $q \equiv 1 \pmod 8$ then

$$B_q(N) \sim \frac{|q|}{3(|q|+1)} \frac{L(1, \chi_{|q|, |q|-1})}{\zeta(2)} N.$$

4.4. **The asymptotics of $D_{2,q}(N)$ for prime $|q|$.** We complete the task of calculating the asymptotics of $D_{2,q}(N)$ where $|q|$ is prime.

Proof of Theorem 2. The proofs of parts a) and b) are similar to the proof of Theorem 1. Part c) is a bit more involved as $C(N)$ is more complicated.

According to Lemma 15, the number of corresponding congruence solutions is

$$C_q(N) = B_q(N) + B_q\left(\left\lfloor \frac{N}{2} \right\rfloor\right) + 2B_q\left(\left\lfloor \frac{N}{4} \right\rfloor\right) + 4\sum_{m \geq 0} B_q\left(\left\lfloor \frac{N}{2^{m+3}} \right\rfloor\right) +$$

$$+ B_q\left(\left\lfloor \frac{N}{|q|} \right\rfloor\right) + B_q\left(\left\lfloor \frac{N}{2|q|} \right\rfloor\right) + 2B_q\left(\left\lfloor \frac{N}{4|q|} \right\rfloor\right) + 4\sum_{m \geq 0} B_q\left(\left\lfloor \frac{N}{2^{m+3}|q|} \right\rfloor\right)$$

First, we notice that both sums over m are finite, since when m is large enough the term $\frac{N}{2^{m+3}}$ is strictly smaller than 1, hence the function B_q is constantly equal to zero. To get a hold on the function $C_q(N)$, we look at the difference $C_q(2N) - C_q(N)$. When expanding $C_q(2N)$ we "take out" the first term of both sums over m to obtain:

$$C_q(2N) = B_q(2N) + B_q(N) + 2B_q\left(\left\lfloor \frac{N}{2} \right\rfloor\right) + 4B_q\left(\left\lfloor \frac{N}{4} \right\rfloor\right) + 4\sum_{m \geq 0} B_q\left(\left\lfloor \frac{N}{2^{m+3}} \right\rfloor\right) +$$

$$+ B_q\left(\left\lfloor \frac{2N}{|q|} \right\rfloor\right) + B_q\left(\left\lfloor \frac{N}{|q|} \right\rfloor\right) + 2B_q\left(\left\lfloor \frac{N}{2|q|} \right\rfloor\right) + 4B_q\left(\left\lfloor \frac{N}{4|q|} \right\rfloor\right) + 4\sum_{m \geq 0} B_q\left(\left\lfloor \frac{N}{2^{m+3}|q|} \right\rfloor\right).$$

This implies that

$$C_q(2N) - C_q(N) = B_q(2N) + B_q\left(\left\lfloor \frac{N}{2} \right\rfloor\right) + 2B_q\left(\left\lfloor \frac{N}{4} \right\rfloor\right) +$$

$$+ B_q\left(\left\lfloor \frac{2N}{|q|} \right\rfloor\right) + B_q\left(\left\lfloor \frac{N}{2|q|} \right\rfloor\right) + 2B_q\left(\left\lfloor \frac{N}{4|q|} \right\rfloor\right).$$

Since $B_q(N) \sim \frac{|q|}{3(|q|+1)} \frac{L(1, \chi_{|q|, |q|-1})}{\zeta(2)} N$, this implies $C_q(2N) - C_q(N) \sim \frac{L(1, \chi_{|q|, |q|-1})}{\zeta(2)} N$. We now apply the classical Cesàro-Stolz theorem [Ces88; Sto85] to $\dfrac{C_q(2N) - C_q(N)}{2N - N}$ and conclude that $C_q(N) \sim \frac{L(1, \chi_{|q|, |q|-1})}{\zeta(2)} N$.

Remark 20. We conjecture that similar results hold for all positive squarefree integers q. More precisely, we conjecture that if $q \equiv 1 \pmod 8$, then $D_{2,q}(N) \sim \frac{12h(4q)\log(u_{4q})}{\pi^2 \sqrt{q}} N$, if $q \equiv 5 \pmod 8$, then $D_{2,q}(N) \sim \frac{8h(4q)\log(u_{4q})}{\pi^2 \sqrt{q}} N$, and $D_{2,q}(N) \sim \frac{6h(4q)\log(u_{4q})}{\pi^2 \sqrt{q}} N$ otherwise (i. e. if $q \not\equiv 1, 5 \pmod 8$), where $h(n)$ denotes the class number of a real quadratic field of discriminant n, while u_n denotes the fundamental unit of the same field. By Dirichlet's class number formula, the constants given here are equal to the constants shown in Theorems 1 and 2.

$\square$

5. $D(n)$-TRIPLES

Definition 1. Let $a < b < c$. A $D(n)$-triple $\{a, b, c\}$ is called *regular* if $c = a + b + 2r$, where $r^2 = ab + n$. A $D(n)$-triple $\{a, b, c\}$ is called *irregular* if it is not regular.

Let $D_{3,n}^{\mathrm{reg}}(N)$ denote the number of regular $D(n)$-triples $\{a, b, c\}$ such that $a < b < c \leqslant N$.

The following theorem holds for all integers n, and its proof is mostly concerned with showing that different cases give at most $O(1)$-triples. We note here that the number of $D(n^2)$-pairs and $D(n^2)$-triples grows faster than a linear function. Namely, a $D(1)$-pair $\{a, b\}$ induces a $D(n^2)$-pair $\{na, nb\}$. Therefore the number of $D(n^2)$-pairs with all elements up to N is greater or equal than the number of $D(1)$-pairs with all elements up to $\frac{N}{n}$, which grows as $\frac{6}{\pi^2} \frac{N}{n} \log \frac{N}{n}$.

Theorem 21 (Minor refinement of Theorem 3). *Let n be an integer. The number of $D(n)$-triples with all elements in the set $\{1, 2, \ldots, N\}$ is asymptotically equal to the number of regular $D(n)$-triples, which is in turn half the number of $D(n)$-pairs. More precisely,*

$$D_{3,n}(N) \sim D_{3,n}^{reg}(N) \sim \frac{D_{2,n}(N)}{2}.$$

Proof (also a proof of Theorem 3). Since $\{a, b, c\}$ is a $D(n)$-triple, there exist positive integers r, s, t satisfying $ab + n = r^2, ac + n = s^2, bc + n = t^2$. According to [Duj02, Lemma 3], there exist integers e, x, y, z such that

$$ae + n^2 = x^2, \quad be + n^2 = y^2, \quad ce + n^2 = z^2,$$

and

$$(7) \qquad\qquad c = a + b + \frac{e}{n} + \frac{2}{n^2}(abe + rxy),$$

We consider three cases, depending on the sign of e.

1) If $e < 0$, then $c \leqslant n^2$. Hence, the number of such triples is $O(1)$ (it is less then $\frac{n^6}{6}$, so the implied constant in O depends on n).

2) If $e = 0$, then $c = a + b + 2r$. Also, $b = a + c - 2s$, where $ac + n = s^2$, $s \geqslant 0$. Every pair $\{a, c\}, ac + n = s^2, a < c \leqslant N$ induces a regular $D(n)$ triple $\{a, a + c - 2s, c\} \subseteq \{1, 2, \ldots, N\}$, unless $a + c - 2s > N$, $a + c - 2s \leqslant 0$, or $a + c - 2s = a$, or $a + c - 2s = c$. The inequality $a + c - 2s > N$ implies $a - 2s > N - c \geqslant 0$. However, $a > 2s$ implies $-4n > a(4c - a) > a \cdot 3c$, which can hold only if $c < \frac{4}{3}|n|$. Therefore the contribution of this case is $O(n) = O(1)$.

    Before analyzing the remaining degenerate cases, let us note here that $a + c - 2s < 0$ is equivalent to $(c - a)^2 < 4n$. Assume that $a + c - 2s = 0$. Then $(c - a)^2 = 4n$. Hence, this case is impossible if n is not a perfect square. If n is a perfect square, then we obtain $c = a + 2\sqrt{n}$, and therefore the contribution of this case is $N + O(1)$.

    The case $a + c - 2s < 0$, after squaring gives $(c - a)^2 < 4n$, which is impossible for $n < 0$, while for $n > 0$ we have $c < a + 2\sqrt{n}$, which implies $(c - \sqrt{n})^2 < ac + n < (c + \sqrt{n})^2$. If we put $ac + n = (c - \alpha)^2$, we find that $|\alpha| < \sqrt{n}$ and $c \mid (n - \alpha^2)$. Hence, $c \leqslant n$, and the contribution of this case is $O(1)$.

If $a + c - 2s = a$, then $c^2 - 4ac = 4n$, and $c \leqslant 4|n|$, while if $a + c - 2s = c$, then $1 \cdot 3c < a(4c - a) = 4|n|$. Hence, the contribution of these both cases is $O(1)$.

Note that every regular $D(n)$-triple $\{a, b, c\}$ is obtained twice by this construction: from $\{a, c\}$ and from $\{b, c\}$. Thus, the total contribution of the case 2), i.e the number of regular $D(n)$-triples, is

$$D_{3,n} = \frac{1}{2} \left(D_{2,n}(N) - N \cdot [n \text{ is a square }] + O(1) \right).$$

Here we use the convention that if S is any statement which can be true or false, then the bracketed notation $[S]$ stands for 1 if S is true, and 0 otherwise.

3) If $e \geqslant 1$, then

$$c = a + b + \frac{e}{n} + \frac{2abe}{n^2} + \frac{2\sqrt{(ab+n)(ae+n^2)(be+n^2)}}{n^2} > \frac{2ab}{n^2}.$$

For now, let us assume that $ab > n$. We have $N \geqslant c \geqslant \frac{2ab}{n^2} > \frac{r^2}{n^2}$. Let us estimate the number of such pairs $\{a, b\}$ satisfying

$$ab + n = r^2, \quad r < n\sqrt{N}.$$

Consider the congruence $x^2 \equiv n \pmod{a}$. In each interval of the size a, there are at most $2^{\omega(a)+1}$ solutions. Hence, the number of pairs $\{a, b\}$ is bounded above by

$$\sum_{a=1}^{n\sqrt{N}} 2^{\omega(a)+1} \cdot \left(\frac{n\sqrt{N}}{a} + 1 \right) = 2n\sqrt{N} \sum_{a=1}^{n\sqrt{N}} \frac{2^{\omega(a)}}{a} + 2 \sum_{a=1}^{n\sqrt{N}} 2^{\omega(a)}$$

$$= O\left(\sqrt{N} \log^2 N \right) + O(\sqrt{N} \log N) \text{ by [Mur08, p. 9.3.12]}$$

$$= O\left(\sqrt{N} \log^2 N \right)$$

On the other hand, if $ab \leqslant n$, adding at most $O(n^2)$-pairs $\{a, b\}$ to the above estimate does not change it.

If a and b are given, then finding c is equivalent to choosing a solution of the Pellian equation

$$bs^2 - at^2 = n(b - a).$$

Each solution belongs to some recursive sequence (growing exponentially). Hence, in each sequence there are $O(\log N)$ solutions with $s \leqslant N$.

The number of the sequences is bounded by $2^{k + \omega(n) + 1}$, where $k = \omega(b - a)$ (this bound can be found in [Duj21, p.399] and in this reference one can also find previously stated results about Pellian equations). We have $b - a \geqslant p_1 \cdots p_k$ (product of first k primes) and $\log b > \log(b - a) > \frac{1}{2} p_k > \frac{1}{2} k \log k$. The last inequalities follow by [Ros39] and [RS62, Theorem 4, Theorem 18] for $p_k > 16$. For products of smallest $k \in \{2, \ldots, 6\}$ primes, one confirms it directly, while for $k = 1$, the intermediate inequality does not hold, but $\log p_1 = \log 2 > \frac{1}{2} \log 1$ holds.

Therefore, we can conclude that

$$2^k < 2^{\frac{2\log b}{\log k}} < b^{\frac{1.4}{\log k}}.$$

If $2^k \geqslant b^{0.01}$, then we have $k < e^{140}$ and $b < 2^{100 \cdot e^{140}}$, hence, the number of such sequences is $O(1)$. If $2^k < b^{0.01}$, then the number of the corresponding sequences is less that $2 \cdot 2^{\omega(n)} \cdot N^{0.01}$. Therefore, the contribution of the case 3) is

$$O\left(\sqrt{N}\log^2 N \cdot N^{0.01} \cdot \log N\right) = O\left(N^{0.52}\right).$$

$\square$

Remark 22. For $n = 1$, we can refine the estimate for the number of irregular triples. Indeed, if $\{a, b, c\}$ is an irregular $D(1)$-triple, then there exists $0 < c_0 < \frac{c}{4ab}$ such that $\{a, b, c_0, c\}$ is a regular $D(1)$-quadruple ($c_0 = d_-$ in the notation of [Duj04]). Hence, the number of irregular $D(1)$-triples is bounded by $D_4(N) = O(\sqrt[3]{N}\log N) = O\left(N^{0.34}\right)$ ([Duj08], Theorem 3).

Before proceeding, let us record a gap principle for irregular $D(n)$-triples which we have proven as a corollary – we believe it might be useful for studying $D(n)$-sets.

Corollary 23. *If an irregular $D(n)$-triple $\{a, b, c\}$ satisfies $a < b < c$ and $c > n^2$, then*

$$c \geqslant \frac{2}{n^2}ab.$$

Proof. Since $\{a, b, c\}$ is a $D(n)$-triple, there are positive integers r, s, t satisfying $ab+n = r^2, ac+n = s^2, bc+n = t^2$. According to [Duj02, Lemma 3], there exist integers e, x, y, z such that

$$ae + n^2 = x^2, be + n^2 = y^2, ce + n^2 = z^2,$$

and

$$(8) \qquad\qquad c = a + b + \frac{e}{n} + \frac{2}{n^2}(abe + rxy),$$

where $x = at - rs, y = bs - rt$ (and $z = cr - st$). We show that both x and y are negative. Namely, x being negative is equivalent to $at < rs$, i. e. $a\sqrt{bc + n} < \sqrt{a^2bc + n(ab + ac) + n^2}$. Dividing by a and squaring gives an equivalent inequality $bc + \frac{n(b+c)}{a} + \left(\frac{n}{a}\right)^2 > bc + n$, which holds since $c > a$. Analogously one shows that y is negative.

We now show that $c > n^2$ implies $e \geqslant 0$. Since $ce + n^2 = z^2$ is non-negative, this means that $e \geqslant \frac{-n^2}{c} > -1$. So $e \geqslant 0$ because it's an integer.

Irregularity of our triple implies that $e \neq 0$. This was already noted in [Duj02], but in the context of quadruples, so we provide the proof. Assuming $e = 0$ implies $x = -n, y = -n$, so $c = a + b + 2r$, which would imply that $\{a, b, c\}$ is regular, contrary to our assumption.

Therefore, $e \geqslant 1$. Now equation (8) implies that $c \geqslant 2\frac{ab}{n^2}$. $\square$

Remark 24. For positive n, since $(rxy)^2 \geqslant (ab)^2$, one can improve this lower bound to $c \geqslant \frac{4}{n^2}ab$.

Theorem 21, together with Theorem 1 and Theorem 2, immediately gives the following asymptotics for the number of $D(q)$-triples.

Corollary 25. *Let q be an integer (such that $|q|$ is prime or 1). The number of $D(q)$-triples is given by the following.*

a) *For even q,*

$$D_{3,2}(N) \sim \frac{L(1, \chi_{8,5})}{2\zeta(2)} \cdot N, \ \text{ while } D_{3,-2}(N) \sim \frac{L(1, \chi_{8,3})}{2\zeta(2)} \cdot N.$$

b) *Let $q \equiv 3 \pmod 4$ such that $|q|$ is prime, or $q = -1$. Then*

$$D_{3,q}(N) \sim \frac{L(1, \chi_{4|q|,4|q|-1})}{2\zeta(2)} \cdot N.$$

c) *Let $q \equiv 5 \pmod 8$ such that $|q|$ is prime. Then*

$$D_{3,q}(N) \sim \frac{L(1, \chi_{|q|,|q|-1})}{\zeta(2)} \cdot N.$$

d) *Let $q \equiv 1 \pmod 8$ such that $|q|$ is prime. Then*

$$D_{3,q}(N) \sim \frac{L(1, \chi_{|q|,|q|-1})}{2\zeta(2)} \cdot N.$$

6. Acknowledgments

Appendix A. Arithmetic functions and their Dirichlet series

To make the paper more self-contained, we collect the basic definitions, notations and results here. Interested reader can find more background in books [Apo98] and [MV06].

Definition 2. A *Dirichlet character of modulus m* (where m is a positive integer) is a function $\chi \colon \mathbb{Z} \to \mathbb{C}$ which satisfies

1) $\chi(a)\chi(b) = \chi(ab)$,
2) $\chi(a + m) = \chi(a)$,
3) $\chi(a) \begin{cases} = 0, & \text{if } \gcd(a, m) > 1 \\ \neq 0, & \text{if } \gcd(a, m) = 1. \end{cases}$

Our paper uses the following Dirichlet characters:

1) $\chi_{8,1}, \chi_{8,3}$ and $\chi_{8,5}$, of modulus 8, as well as $\chi_{4,3}$ of modulus 4 defined by

	1	3	5	7
$\chi_{8,1}$	1	1	1	1
$\chi_{8,3}$	1	1	-1	-1
$\chi_{8,5}$	1	-1	-1	1
$\chi_{4,3}$	1	-1		

2) For any prime $q \equiv 1 \pmod 4$ we denote

$$\chi_{q,q-1}(a) = \left(\frac{q}{a}\right)$$

3) For any prime $q \equiv 3 \pmod 4$ we denote

$$\chi_{4q,4q-1}(a) = \left(\frac{q}{a}\right),$$

where $\left(\frac{q}{a}\right)$ is the Kronecker symbol.

Definition 3. A *Dirichlet L-series* is a function of the form

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where χ is a Dirichlet character and s is a complex variable with real part greater than one. By analytic continuation, this function can be extended to a meromorphic function on the whole plane and is then called a *Dirichlet L-function*, also denoted by $L(s,\chi)$.

Dirichlet had shown that $L(s,\chi)$ is non-zero at $s = 1$. Moreover, the L-function is entire whenever χ is not principal, as is the case for all the Dirichlet characters in our paper which we evaluate at $s = 1$.

Lemma 26. *Let $\mathcal{G}$ be some set of primes, and $b(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n)$, where $\lambda_{\mathcal{G}}(n) = 1$ if all prime factors of n are in $\mathcal{G}$, and 0 otherwise. Then $|b(n)| = n^{o(1)}$.*

Proof. Assume $\omega(n) = k$ for some $k \in \mathbb{N}$. If we denote the j-th prime number by p_j then $\frac{b(n)}{n}$ is at most $\dfrac{2^k}{\prod_{j=1}^{k} p_j}$, which tends to zero as $k \to \infty$. $\qquad\square$

Corollary 27. *With notation as in Lemma 26, the Dirichlet series β of $b(n)$ and the Dirichlet series $\zeta_{\mathcal{G}}$ of $\lambda_{\mathcal{G}}$ are both holomorphic in the region $\Re s > 1$.*

Theorem 28 ([MV06, Theorem 1.9])**.** *If f is multiplicative and $\sum_{n=1}^{\infty} \frac{|f(n)|}{n^\delta} < \infty$, where δ is the real part of s, then*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right).$$

References

[Apo98]   T. M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer New York, 1998 (cit. on p. 17).

[Ces88]   E. Cesàro. "Sur la convergence des séries". In: *Nouvelles annales de mathématiques* Series 3 (7 1888), pp. 49–59 (cit. on p. 13).

[Duj02]   A. Dujella. "On the size of Diophantine m-tuples". In: *Math. Proc. Cambridge Philos. Soc.* 132.1 (2002), pp. 23–33 (cit. on pp. 14, 16).

[Duj04]   A. Dujella. "There are only finitely many Diophantine quintuples". In: *J. Reine Angew. Math.* 566 (2004), pp. 183–214 (cit. on p. 16).

[Duj08]   A. Dujella. "On the number of Diophantine m-tuples". In: *Ramanujan J.* 15.1 (2008), pp. 37–46 (cit. on pp. 1, 4, 16).

[Duj21]   A. Dujella. *Number theory*. Školska knjiga, Zagreb, 2021, pp. x+621 (cit. on p. 15).

[Ike31]   S. Ikehara. "An extension of Landau's theorem in the analytic theory of numbers". In: *Journal of Mathematics and Physics of the Massachusetts Institute of Technology* 10 (1931), pp. 1–12 (cit. on p. 7).

[Lao10]   H. Lao. "On the Number of Diophantine m-tuples". In: *Advances in Mathematics (China)* 39 (3 2010), pp. 277–282 (cit. on p. 1).

[LMFDB]   T. LMFDB Collaboration. *The L-functions and modular forms database*. http://www.lmfdb.org. [Online; accessed 10 November 2022]. 2022 (cit. on p. 2).

[MS11]   G. Martin and S. Sitar. "Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples". In: *Mathematika* 57.1 (2011), pp. 1–29 (cit. on p. 1).

[MV06]   H. L. Montgomery and R. C. Vaughan. *Multiplicative Number Theory I: Classical Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006 (cit. on pp. 5, 17, 18).

[Mur08]   M. R. Murty. *Problems in Analytic Number Theory*. Graduate Texts in Mathematics. Springer New York, 2008 (cit. on p. 15).

[Ros39]   B. Rosser. "The n-th Prime is Greater than $n \log n$". In: *Proc. Lond. Math. Soc. (2)* S2-45.1 (1939), pp. 21–44. eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms/s2-45.1.21 (cit. on p. 15).

[RS62]   J. B. Rosser and L. Schoenfeld. "Approximate formulas for some functions of prime numbers". In: *Illinois J. Math.* 6 (1962), pp. 64–94 (cit. on p. 15).

[Sto85]   O. Stolz. *Vorlesungen über allgemeine Arithmetik: nach den Neueren Ansichten*. 1885 (cit. on p. 13).

[Vin03]   I. M. Vinogradov. *Elements of Number Theory*. Dover phoenix editions. Dover Publications, 2003 (cit. on pp. 3, 11).

Department of Mathematics, Faculty of Civil Engineering, University of Zagreb, Croatia
Email address: nikola.adzaga@grad.unizg.hr

Faculty of Food Technology and Biotechnology, University of Zagreb, Croatia
Email address: goran.drazic@pbf.unizg.hr

Department of Mathematics, Faculty of Science, University of Zagreb, Croatia
Email address: duje@math.hr

Department of Computer Science, University of Debrecen, Hungary
Email address: petho.attila@unideb.hu