Czechoslovak Mathematical Journal

Neha Prabhu

Density of solutions to quadratic congruences

Czechoslovak Mathematical Journal, Vol. 67 (2017), No. 2, 439–455

Persistent URL: http://dml.cz/dmlcz/146767

Czechoslovak Mathematical Journal, 67 (142) (2017), 439–455

DENSITY OF SOLUTIONS TO QUADRATIC CONGRUENCES

Neha Prabhu, Pune

(Received December 31, 2015)

Abstract. A classical result in number theory is Dirichlet's theorem on the density of primes in an arithmetic progression. We prove a similar result for numbers with exactly k prime factors for $k > 1$. Building upon a proof by E. M. Wright in 1954, we compute the natural density of such numbers where each prime satisfies a congruence condition. As an application, we obtain the density of squarefree $n \leqslant x$ with k prime factors such that a fixed quadratic equation has exactly 2^k solutions modulo n.

Keywords: Dirichlet's theorem; asymptotic density; primes in arithmetic progression; squarefree number

MSC 2010: 11D45, 11B25, 11N37

1. Introduction

The theory of solving a quadratic equation modulo p for p prime has been well studied. Investigating whether a given quadratic equation has solutions, how many there are and calculating what the solutions are, has led to beautiful theorems such as the law of quadratic reciprocity. A related question is the following:

Suppose we fix a quadratic equation $f(x) = x^2 + bx + c$, where $b, c \in \mathbb{Z}$, and would like to know how often the equation $f(x) = 0$ has solutions modulo N if we vary N in a certain range. Let us first look at the case where we vary over primes p not exceeding x. Dirichlet, in 1837, showed that solutions would exist for approximately half the primes. In 1896, this was made precise by de la Vallée-Poussin. Noting that $f(x)$ has exactly two solutions if and only if the discriminant $D = b^2 - 4c$ is a square $\bmod p$, what Dirichlet and de la Vallée-Poussin showed was essentially the following:

The research of the author is supported by a PhD scholarship from the National Board for Higher Mathematics, India.

DOI: 10.21136/CMJ.0.0712-15

Proposition 1.1. *For a fixed non-square integer D, as $x \to \infty$,*

$$\frac{1}{\pi(x)} \# \Big\{ p \leqslant x,\ p \text{ prime: } \Big(\frac{D}{p}\Big) = 1 \Big\} \sim \frac{1}{2}$$

and

$$\frac{1}{\pi(x)} \# \Big\{ p \leqslant x,\ p \text{ prime: } \Big(\frac{D}{p}\Big) = -1 \Big\} \sim \frac{1}{2},$$

where $(\frac{D}{\cdot})$ is the Kronecker-Legendre symbol and $\pi(x)$ denotes the number of primes not exceeding x.

The main ideas that go into the proof of this result are two classical results: Gauss's law of quadratic reciprocity and the natural density version of Dirichlet's theorem on the infinitude of primes in an arithmetic progression. Dirichlet proved the original theorem around 1836. Later, de la Vallée-Poussin proved the statement about natural density. See Chapter 4, Section IV of [6]. He proved that for positive integers a, q with $\gcd(a, q) = 1$, the set of primes congruent to a mod q has natural density $1/\varphi(q)$. In other words, the number of primes $p \leqslant x$ such that $p \equiv a \bmod q$ is asymptotic to $\pi(x)/\varphi(q)$ as $x \to \infty$. Since then, there have been analogues of this theorem in various settings. For example, by applying the Chebotarev density theorem to the case of cyclotomic extensions $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$, we obtain Dirichlet's theorem. The analogue in the case of function fields was proved by Kornblum and Landau in [2]. It is natural to ask if we can extend the result to numbers with k prime factors, $k > 1$. In order to do so, we first need to talk about the analogue of $\pi(x)$ for numbers with k prime factors, which is defined as

$$\tau_k(x) := \sum_{\substack{n \leqslant x \\ n = p_1 p_2 \dots p_k}} 1,$$

where $n = p_1 p_2 \dots p_k$ is the prime factorization of n, with $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$. If we add an additional condition that the primes dividing n must be distinct, then we are counting the number of squarefree positive integers not exceeding x, having exactly k prime factors, and this quantity is denoted by $\pi_k(x)$.

In 1900, Landau in [3] proved that

$$\pi_k(x) \sim \tau_k(x) \sim \frac{x(\log\log x)^{k-1}}{(k-1)! \log x}. \tag{1.1}$$

In 1954, Wright gave a simpler proof of this in [7], which appears as Theorem 437 in [1]. There have been several attempts since then at deriving a precise estimate with error terms. An exposition of this can be found in Section 7.4 of [4]. With this in mind, it is natural to ask if we can say something analogous to Proposition 1.1 when n varies over squarefree numbers. In this paper, we prove the following:

Theorem 1.2. *Let $D \in \mathbb{Z}$ be a non-square integer and $k \in \mathbb{N}$. Fix a k-tuple $\underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_k)$ where $\varepsilon_i = \pm 1$ for each $i = 1, \ldots, k$. Then*

$$\frac{1}{\pi_k(x)} \# \Big\{ n \leqslant x \colon\ n = p_1 p_2 \ldots p_k \text{ with } p_1 < p_2 < \ldots < p_k, \\ \left(\frac{D}{p_i}\right) = \varepsilon_i \text{ for each } i \Big\} \sim \frac{1}{2^k},$$

where $\pi_k(x)$ denotes the number of squarefree numbers less than x with k prime factors.

The proof involves an analogous version of Dirichlet's theorem, which is the following:

Let us fix $N, k \in \mathbb{N}$ and consider a k-tuple

$$\underline{\mathrm{m}}_{[k]} = (m_1, m_2, \ldots, m_k)$$

where each m_i belongs to $(\mathbb{Z}/N\mathbb{Z})^{\times}$, the multiplicative group of units in $\mathbb{Z}/N\mathbb{Z}$. The m_i's are not necessarily distinct.

Consider positive integers $n \leqslant x$ with k prime factors, counted with multiplicity. Represent such n as $n = p_1 p_2 \ldots p_k$ with $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$. Let $\tau_{k, \underline{\mathrm{m}}_{[k]}}(x)$ denote the number of positive integers $n \leqslant x$ with k prime factors satisfying $p_i \equiv m_i \bmod N$ for each $i = 1, \ldots, k$. If the primes are distinct, then n is squarefree. Let $\pi_{k, \underline{\mathrm{m}}_{[k]}}(x)$ denote the number of such squarefree $n \leqslant x$. Then we prove

Theorem 1.3.

$$\pi_{k, \underline{\mathrm{m}}_{[k]}}(x) \sim \tau_{k, \underline{\mathrm{m}}_{[k]}}(x) \sim \frac{1}{\varphi(N)^k} \frac{x (\log \log x)^{k-1}}{(k-1)! \log x}, \qquad k \geqslant 2.$$

Remark. Note that for $k = 1$, Theorem 1.3 is exactly the statement of Dirichlet's density theorem. The prime number theorem, the non-vanishing of $L(1, \chi)$ and the orthogonality relations satisfied by Dirichlet characters are the key results that are used in the proof. Similarly, in the proof of Theorem 1.3, Dirichlet's density theorem and Landau's result stated in equation (1.1) play a significant role. In fact, we essentially use the technique used by Wright in [7] and an orthogonality relation satisfied by the Dirichlet characters to obtain the result.

The paper is divided as follows. We start by proving Theorem 1.3. The second section sets the stage by introducing functions and notation that will be used in the proof. In Section 3 we prove the nontrivial part of the proof of Theorem 1.3 in detail. With Section 4, we wrap up the proof of this theorem. After that, the proof of Proposition 1.1 is given for the sake of completeness and finally, Theorem 1.2 is presented, which uses Proposition 1.1 and Theorem 1.3. We also include two corollaries of the theorem.

2. Preliminaries

The following notation will be used in the proof of Theorem 1.3:

(1) We write $\underline{\mathrm{m}}_{[k]}$ to denote a k-tuple $(m_1, m_2, \dots, m_k)$.

(2) We use $\underline{\mathrm{m}}^{i}_{[k-1]}$ to denote the tuple $\underline{\mathrm{m}}_{[k]}$ under consideration, with the ith coordinate removed.

(3) Henceforth, the sum $\sum\limits_{p_1p_2\dots p_k \leqslant x}$ is taken over all sets of primes $\{p_1, p_2, \dots, p_k\}$ such that $p_1p_2\dots p_k \leqslant x$, two sets being considered different even if they differ only in the order of primes.

(4) For a fixed $\underline{\mathrm{m}}_{[k]}$, we write

$$\sum_{p_1p_2\dots p_k \leqslant x} \boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}}$$
$$:= \sum_{p_1p_2\dots p_k \leqslant x} \sum_{\sigma \in S'_k} \sum_{\chi} \overline{\chi(m_{\sigma(1)})}\chi(p_1) \sum_{\chi} \overline{\chi(m_{\sigma(2)})}\chi(p_2) \dots \sum_{\chi} \overline{\chi(m_{\sigma(k)})}\chi(p_k)$$

where

1. the set S'_k is the subset of the symmetric group on k symbols consisting of those permutations that give rise to distinct permutations of $\{m_1, m_2, \dots, m_k\}$;
2. the sum $\sum\limits_{\chi}$ runs over the Dirichlet characters modulo N.

Note. We have the following orthogonality relation satisfied by Dirichlet characters mod N:

$$\sum_{\chi} \overline{\chi(m)}\chi(n) = \begin{cases} \varphi(N) & \text{if } m \equiv n \bmod N, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that, for a fixed $n = p_1p_2\dots p_k$ and $\sigma \in S'_k$, the product

$$\sum_{\chi} \overline{\chi(m_{\sigma(1)})}\chi(p_1) \sum_{\chi} \overline{\chi(m_{\sigma(2)})}\chi(p_2) \dots \sum_{\chi} \overline{\chi(m_{\sigma(k)})}\chi(p_k)$$

is nonzero if and only if $p_i \equiv m_{\sigma(i)}$ for all $i = 1, \dots, k$. The orthogonality relation tells us that this nonzero quantity is $\varphi(N)$ for each i. Therefore, for each $n = p_1p_2\dots p_k$, the inner double sum is $\varphi(N)^k$ if, for some $\sigma \in S'_k$, we have $p_i \equiv m_{\sigma(i)}$ for every i and zero otherwise. Observe that this can happen for at most one permutation $\sigma \in S'_k$.

The following are auxiliary functions that will appear in the proof:

1. $\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = \dfrac{1}{\varphi(N)^k} \displaystyle\sum_{p_1p_2\dots p_k \leqslant x} \boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}};$
2. $\vartheta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = \dfrac{1}{\varphi(N)^k} \displaystyle\sum_{p_1p_2\dots p_k \leqslant x} \log(p_1p_2\dots p_k)\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}};$
3. $L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = \dfrac{1}{\varphi(N)^k} \displaystyle\sum_{p_1p_2\dots p_k \leqslant x} \dfrac{1}{(p_1p_2\dots p_k)}\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}}.$

By Dirichlet's theorem, we know that for $i \neq j$ the number of primes $p \equiv m_{\sigma(i)} \bmod N$ is asymptotically the same as the number of primes $p \equiv m_{\sigma(j)} \bmod N$. Thus, if we fix a permutation of $\{m_1, m_2, \dots, m_k\}$, then the number of ordered sets $\{p_1, p_2, \dots, p_k\}$ such that $p_i \equiv m_i \bmod N$ is equal to $\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)/M$, where M is the number of distinct permutations of the multiset $\{m_1, m_2, \dots, m_k\}$.

3. Towards a generalization of Dirichlet's density theorem

The proof of Theorem 1.3 comes down to proving

Proposition 3.1. *For $k \geqslant 2$,*

$$\vartheta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \sim \frac{M}{\varphi(N)^k} kx(\log\log x)^{k-1}.$$

The proof of this proposition will follow after a series of lemmas.

First, we prove a recursive relation for $\vartheta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$:

Lemma 3.2. *For $k \geqslant 1$,*

$$k\vartheta_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x) = (k+1)\sum_{p\leqslant x} \frac{1}{\varphi(N)} {\sum_i}' \Big(\sum_{\chi} \overline{\chi(m_i)}\chi(p)\vartheta_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}\left(\frac{x}{p}\right)\Big),$$

where the dash on top of the second summation symbol denotes that only those $i = 1, \dots, k$ are counted for which the $\underline{\mathrm{m}}^i_{[k+1]}$ are distinct.

Proof.

$$\begin{aligned}
&(k+1)\vartheta_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x)\\
&\quad= \frac{1}{\varphi(N)^{k+1}} \sum_{p_1p_2\dots p_{k+1}\leqslant x} (k+1)\log(p_1p_2\dots p_{k+1})\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}\\
&\quad= \frac{1}{\varphi(N)^{k+1}} \sum_{p_1p_2\dots p_{k+1}\leqslant x} \boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}(\log p_1 + \log(p_2p_3\dots p_{k+1}) + \log p_2\\
&\qquad+ \log(p_1p_3\dots p_{k+1}) + \dots + \log p_{k+1} + \log(p_1p_2\dots p_k))\\
&\quad= \frac{1}{\varphi(N)^{k+1}} \sum_{p_1p_2\dots p_{k+1}\leqslant x} \log(p_1p_2\dots p_{k+1})\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}\\
&\qquad+ \frac{1}{\varphi(N)^{k+1}} \sum_{p_1p_2\dots p_{k+1}\leqslant x} (\log(p_2p_3\dots p_{k+1}) + \dots + \log(p_1p_2\dots p_k))\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}\\
&\quad= \frac{1}{\varphi(N)^{k+1}} \sum_{p_1p_2\dots p_{k+1}\leqslant x} \log(p_1p_2\dots p_{k+1})\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}\\
&\qquad+ \frac{(k+1)}{\varphi(N)^{k+1}} \sum_{p_1p_2\dots p_{k+1}\leqslant x} \log(p_2p_3\dots p_{k+1})\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}.
\end{aligned}$$

The first sum is just $\vartheta_{k+1,\chi,\underline{\mathrm{m}}}(x)$ and this reduces the left hand side to $k\vartheta_{k+1,\chi,\underline{\mathrm{m}}}(x)$.

In the second sum, observe that the $\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}$ appearing there is a $(k+1)$-tuple. Collecting the terms corresponding to p_1 in $\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}$, the second sum can be written as

$$\begin{aligned}
&\sum_{p_1p_2\dots p_{k+1}\leqslant x} \log(p_2p_3\dots p_{k+1})\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k+1]}}\\
&\qquad\qquad= {\sum_i}' \sum_{p_1p_2\dots p_{k+1}\leqslant x} \log(p_2p_3\dots p_{k+1})\boldsymbol{\chi}_{\underline{\mathrm{m}}^i_{[k]}}\Bigl(\sum_{\chi} \overline{\chi(m_i)}\chi(p_1)\Bigr).
\end{aligned}$$

Simplifying, we get

$$k\vartheta_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x) = (k+1)\sum_{p\leqslant x} \frac{1}{\varphi(N)} {\sum_i}' \Bigl(\sum_{\chi} \overline{\chi(m_i)}\chi(p)\vartheta_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}\Bigl(\frac{x}{p}\Bigr)\Bigr).$$

□

Similarly, we prove a recursion formula for the function $L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$:

Lemma 3.3. *Let* $L_{0,\chi,\underline{\mathrm{m}}_{[0]}}(x)=1$. *Then for* $k\geqslant 1$,

$$L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)=\sum_{p\leqslant x}\frac{1}{p}{\sum_i}'\frac{1}{\varphi(N)}\sum_{\chi}\overline{\chi(m_i)}\chi(p)L_{k-1,\chi,\underline{\mathrm{m}}^i_{[k-1]}}\Big(\frac{x}{p}\Big),$$

where the dash on top of the second summation symbol is as defined in Lemma 3.2.

This follows directly from the definitions.

Let

$$f_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)=\varphi(N)^k\vartheta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)-xk\varphi(N)^{k-1}{\sum_i}'L_{k-1,\chi,\underline{\mathrm{m}}^i_{[k-1]}}(x). \tag{3.1}$$

The idea is to first estimate $f_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$ and $L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$. Plugging in these estimates into equation (3.1) will then give an asymptotic formula for $\theta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$ thus proving Proposition 3.1. With this in mind, we first prove a recursion formula for $f_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$.

Lemma 3.4.

$$kf_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x)=(k+1)\sum_{p\leqslant x}{\sum_i}'\sum_{\chi}\overline{\chi(m_i)}\chi(p)f_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}\Big(\frac{x}{p}\Big).$$

Proof. From the definition of $f_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$, we have

$$kf_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x)=k\varphi(N)^{k+1}\vartheta_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x)-xk(k+1)\varphi(N)^k{\sum_i}'L_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}(x).$$

We evaluate the two summands using Lemma 3.2 and Lemma 3.3 proved above. By Lemma 3.2 we have

$$\begin{aligned}&k\varphi(N)^{k+1}\vartheta_{k+1,\chi,\underline{\mathrm{m}}_{[k+1]}}(x)\\&\qquad=\varphi(N)^{k+1}(k+1)\sum_{p\leqslant x}\frac{1}{\varphi(N)}{\sum_i}'\Big(\sum_{\chi}\overline{\chi(m_i)}\chi(p)\vartheta_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}\Big(\frac{x}{p}\Big)\Big),\end{aligned}$$

which simplifies to

$$(k+1)\sum_{p\leqslant x}{\sum_i}'\sum_{\chi}\overline{\chi(m_i)}\chi(p)\Big[\varphi(N)^k\vartheta_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}\Big(\frac{x}{p}\Big)\Big].$$

Also using Lemma 3.3,

$${\sum_i}'L_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}(x)=\sum_{i=1}^{k+1}\sum_{p\leqslant x}\frac{1}{p}{\sum_j}'\frac{1}{\varphi(N)}\sum_{\chi}\overline{\chi(m_j)}\chi(p)L_{k-1,\chi,\underline{\mathrm{m}}^{i,j}_{[k-1]}}\Big(\frac{x}{p}\Big),$$

where $\underline{\mathrm{m}}^{i,j}_{[k-1]}$ denotes $\underline{\mathrm{m}}^{i}_{[k]}$ with the jth coordinate removed and $\sum'_j$ denotes that only distinct $\underline{\mathrm{m}}^{i,j}_{[k-1]}$ are counted.

Therefore,

$$\begin{aligned} &xk(k+1)\varphi(N)^k{\sum_i}' L_{k,\chi,\underline{\mathrm{m}}^i_{[k]}}(x) \\ &\qquad = (k+1)\sum_{p\leqslant x}{\sum_i}'\sum_{\chi}\overline{\chi(m_i)}\chi(p)\Big[k\varphi(N)^{k-1}\frac{x}{p}{\sum_j}' L_{k-1,\chi,\underline{\mathrm{m}}^{i,j}_{[k-1]}}\Big(\frac{x}{p}\Big)\Big].\end{aligned}$$

Putting the two summands together, we obtain the result. □

Next, we use Lemma 3.4 to get an estimate for $f_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$.

Lemma 3.5. *Let $k \geqslant 1$. Then*

$$f_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = o\{x(\log\log x)^{k-1}\}.$$

Proof. By induction on k.

When $k = 1$, writing $\underline{\mathrm{m}}_{[1]} = m$,

$$f_{1,\chi,m}(x) = \varphi(N)\vartheta_{1,\chi,m}(x) - x.$$

From Dirichlet's theorem on the density of primes in an arithmetic progression, $\vartheta_{1,\chi,m}(x) \sim x/\varphi(N)$ and so

$$f_{1,\chi,m}(x) = o(x).$$

Suppose the claim is true for $k = K$, where $K > 1$. This means for any $\varepsilon > 0$, there exists $x_0 = x_0(K,\varepsilon)$ such that

$$|f_{K,\chi,\underline{\mathrm{m}}_{[K]}}(x)| < \varepsilon x(\log\log x)^{K-1}, \quad x \geqslant x_0.$$

Also, for $1 \leqslant x < x_0$, from the definition of $f_{K,\chi,\underline{\mathrm{m}}_{[K]}}$, we can find a real number D depending on K, ε such that

$$|f_{K,\chi,\underline{\mathrm{m}}_{[K]}}(x)| < D.$$

Using the above we deduce

(1) For $p \leqslant x/x_0$,

$$\begin{aligned} &\sum_{p\leqslant x/x_0}\Big|\sum_{i=1}^{K+1}\sum_{\chi}\overline{\chi(m_i)}\chi(p)f_{K,\chi,\underline{\mathrm{m}}^i_{[K]}}\Big(\frac{x}{p}\Big)\Big| \\ &\qquad < (K+1)\varphi(N)\varepsilon(\log\log x)^{K-1}\sum_{p\leqslant x/x_0}\frac{x}{p} \\ &\qquad < (K+2)\varphi(N)\varepsilon x(\log\log x)^{K} \quad \text{for } x \text{ large enough.}\end{aligned}$$

(2) For $x/x_0 < p \leqslant x$,

$$\sum_{x/x_0<p\leqslant x}\Big|\sum_{i=1}^{K+1}\sum_{\chi}\overline{\chi(m_i)}\chi(p)f_{K,\chi,\underline{\mathrm{m}}^i_{[K]}}\Big(\frac{x}{p}\Big)\Big| \\ < (K+1)\varphi(N)D\pi(x) < (K+1)\varphi(N)Dx.$$

Hence, using Lemma 3.4 and the simple inequality $K+1<2K$ for $K>1$, we have $K|f_{K+1,\chi,\underline{\mathrm{m}}_{[K+1]}}(x)| < 2K\varphi(N)x((K+2)\varepsilon(\log\log x)^k+(K+1)D)$.

Thus, for $x > x_1(D,\varepsilon,K)$ we conclude

$$|f_{K+1,\chi,\underline{\mathrm{m}}_{[K+1]}}(x)| < 2(K+2)\varphi(N)\varepsilon x(\log\log x)^K.$$

Since ε was arbitrary, the claim follows for all $k\in\mathbb{N}$ by induction. □

To complete the proof of Proposition 3.1, it suffices to prove

Lemma 3.6.

$$L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \sim \frac{M}{\varphi(N)^k}(\log\log x)^k.$$

Proof. Recall that

$$\begin{aligned} L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) &= \frac{1}{\varphi(N)^k}\sum_{p_1p_2\ldots p_k\leqslant x}\frac{1}{(p_1p_2\ldots p_k)}\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}} \\ &= \frac{1}{\varphi(N)^k}\sum_{p_1p_2\ldots p_k\leqslant x}\frac{1}{(p_1p_2\ldots p_k)} \\ &\quad\times\sum_{\sigma\in S_k}\sum_{\chi}\overline{\chi(m_{\sigma(1)})}\chi(p_1)\sum_{\chi}\overline{\chi(m_{\sigma(2)})}\chi(p_2)\ldots\sum_{\chi}\overline{\chi(m_{\sigma(k)})}\chi(p_k)\end{aligned}$$

and that M is the number of permutations of the (possible) multiset $\{m_1,m_2,\ldots,m_k\}$.

We observe that the following holds: Given a squarefree number n with k factors, if each prime p dividing n satisfies $p\leqslant x^{1/k}$ then $n\leqslant x$. This leads us to write

$$L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \geqslant M\prod_{i=1}^{k}\sum_{p\leqslant x^{1/k}}\frac{1}{p}\Big(\frac{1}{\varphi(N)}\sum_{\chi}\overline{\chi(m_i)}\chi(p)\Big),$$

i.e.,

$$L_{k,\chi,\underline{\mathrm{m}}_{[k]}} \geqslant M\prod_{i=1}^{k}\sum_{\substack{p\leqslant x^{1/k}\\ p\equiv m_i \bmod N}}\frac{1}{p}.$$

Similarly, if $n = p_1 p_2 \dots p_k$ is less than x then $p_i \leqslant x$ for $i = 1, \dots, k$, which gives us an upper bound:

$$L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \leqslant M \prod_{i=1}^{k} \sum_{p \leqslant x} \frac{1}{p} \bigg(\frac{1}{\varphi(N)} \sum_{\chi} \overline{\chi(m_i)} \chi(p) \bigg) = M \prod_{i=1}^{k} \sum_{\substack{p \leqslant x \\ p \equiv m_i \bmod N}} \frac{1}{p}.$$

It is known (see for example [5]) that for any a coprime to N,

$$\sum_{\substack{p \leqslant x \\ p \equiv a \bmod N}} \frac{1}{p} \sim \frac{1}{\varphi(N)} \log \log x.$$

Thus, $L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)$ is bounded below and above by functions that are each asymptotic to $M\varphi(N)^{-k}(\log \log x)^k$, implying that

$$L_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \sim \frac{M}{\varphi(N)^k} (\log \log x)^k.$$

□

Finally, Proposition 3.1 follows by using Lemma 3.5 and Lemma 3.6 in equation (3.1).

Remark. Some care needs to be taken while applying Lemma 3.6. The term $\sum_{i=1}^{k} L_{k-1,\chi,\underline{\mathrm{m}}^i_{[k-1]}}(x)$ appearing in equation (3.1) involves the number of distinct permutations of $\underline{\mathrm{m}}^i_{[k-1]}$, whereas M appearing in Proposition 3.1 is the number of distinct permutations of $\underline{\mathrm{m}}_{[k]}$. This is resolved by using the following simple fact:

Let $k_1 + k_2 + \ldots + k_m = n$. Then

$$\frac{n!}{k_1!\, k_2! \dots k_m!} = \frac{(n-1)!}{(k_1-1)!\, k_2! \dots k_m!} + \frac{(n-1)!}{k_1!\, (k_2-1)! \dots k_m!} + \ldots + \frac{(n-1)!}{k_1!\, k_2! \dots (k_m-1)!}.$$

We are now ready to prove the theorem.

4. Proof of Theorem 1.3

By partial summation we have

$$\vartheta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = \Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)\log x - \int_2^x \frac{\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(t)}{t}\,\mathrm{d}t.$$

Clearly, $\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(t) = O(t)$ and therefore,

$$\int_2^x \frac{\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(t)}{t}\,\mathrm{d}t = O(x).$$

Hence, for $k \geqslant 2$, by Proposition 3.1,

$$\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = \frac{\vartheta_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)}{\log x} + O\Big(\frac{x}{\log x}\Big) \sim \frac{M}{\varphi(N)^k}\frac{kx(\log\log x)^{k-1}}{\log x}.$$

Thus,

$$\frac{1}{M}\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \sim \frac{1}{\varphi(N)^k}\frac{kx(\log\log x)^{k-1}}{\log x}. \tag{4.1}$$

We now relate this to the functions $\pi_{k,\underline{\mathrm{m}}_{[k]}}(x)$ and $\tau_{k,\underline{\mathrm{m}}_{[k]}}(x)$. It is easy to see that

$$k!\,\pi_{k,\underline{\mathrm{m}}_{[k]}}(x) \leqslant \frac{1}{M}\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) \leqslant k!\,\tau_{k,\underline{\mathrm{m}}_{[k]}}(x).$$

We have two cases to consider.

Case 1: The units $m_1, m_2, \dots m_k$ are distinct. Then $\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}} = 0$ unless $p_1, p_2, \dots, p_k$ are all distinct. This forces the equality

$$k!\,\pi_{k,\underline{\mathrm{m}}_{[k]}}(x) = \frac{1}{M}\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x) = k!\,\tau_{k,\underline{\mathrm{m}}_{[k]}}(x),$$

so using equation (4.1) we are done.

Case 2: At least two of the m_i are equal. Certainly, in this case we include those $n = p_1 \dots p_k$ such that at least two of the primes are equal. The number of such $n \leqslant x$ is $\tau_{k,\underline{\mathrm{m}}_{[k]}}(x) - \pi_{k,\underline{\mathrm{m}}_{[k]}}(x)$. These n can be expressed in the form $n = p_1 \dots p_k$ with $p_{k-1} = p_k$ and $\underline{\mathrm{m}}_{[k]}$ with $m_{k-1} = m_k$. Therefore, we have

$$\begin{aligned}\tau_{k,\underline{\mathrm{m}}_{[k]}}(x) - \pi_{k,\underline{\mathrm{m}}_{[k]}}(x) &\leqslant \frac{1}{M}\sum_{p_1p_2\dots p_{k-1}^2 \leqslant x} \frac{1}{\varphi(N)^k}\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}} \\ &\leqslant \frac{1}{M}\sum_{p_1p_2\dots p_{k-1} \leqslant x} \frac{1}{\varphi(N)^{k-1}}\boldsymbol{\chi}_{\underline{\mathrm{m}}_{[k]}} = \frac{1}{M}\Pi_{k-1,\chi,\underline{\mathrm{m}}_{[k-1]}}(x).\end{aligned}$$

Since $\Pi_{k-1,\chi,\underline{\mathrm{m}}_{[k-1]}}(x)/M$ is $o(\Pi_{k,\chi,\underline{\mathrm{m}}_{[k]}}(x)/M)$, from our observation above we have

$$\pi_{k,\underline{\mathrm{m}}_{[k]}}(x) \sim \tau_{k,\underline{\mathrm{m}}_{[k]}}(x) \sim \frac{1}{\varphi(N)^k} \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}, \quad k \geqslant 2$$

thus proving the theorem in this case as well. □

5. Proofs of Proposition 1.1 and Theorem 1.2

In order to prove Proposition 1.1, we note that it suffices to prove the result for p odd, since 2 is the only even prime and the density of finite sets is zero. Thus we will assume that p is odd in the proof.

Proof of Proposition 1.1. Let $D = \pm q_1^{a_1} q_2^{a_2} \dots q_m^{a_m}$ be the decomposition of D. Then, by the multiplicative property of the Legendre symbol, we have

$$\Big(\frac{D}{p}\Big) = \Big(\frac{\pm 1}{p}\Big)\Big(\frac{q_1}{p}\Big)^{a_1}\Big(\frac{q_2}{p}\Big)^{a_2} \dots \Big(\frac{q_m}{p}\Big)^{a_m} = \pm\Big(\frac{q_1}{p}\Big)\Big(\frac{q_2}{p}\Big) \dots \Big(\frac{q_m}{p}\Big).$$

We have two possibilities:

Case (*i*): $2 \nmid D$. Then, either $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. If $p \equiv 1 \bmod 4$ then by quadratic reciprocity, $\big(\frac{q_i}{p}\big) = \big(\frac{p}{q_i}\big)$. Also, $\big(\frac{\pm 1}{p}\big) = 1$. If $p \equiv 3 \bmod 4$, then $\big(\frac{\pm 1}{p}\big) = -1$ and $\big(\frac{q_i}{p}\big) = \pm\big(\frac{p}{q_i}\big)$, depending on whether $q_i \equiv 1$ or $3 \bmod 4$. In general, we can write

$$\Big(\frac{D}{p}\Big) = \pm\Big(\frac{p}{q_1}\Big)\Big(\frac{p}{q_2}\Big) \dots \Big(\frac{p}{q_m}\Big).$$

Since $p \nmid q$, we know that p is a unit mod q, so it is congruent to one of the $q-1$ units in $\mathbb{Z}/q\mathbb{Z}$. We also know that if q is an odd prime, then there are $(q-1)/2$ squares in $(\mathbb{Z}/q\mathbb{Z})^\times$, therefore we conclude that for each q_i, the equations

$$\Big(\frac{p}{q_i}\Big) = 1$$

and

$$\Big(\frac{p}{q_i}\Big) = -1$$

each have $(q_i - 1)/2$ solutions for $p \bmod q_i$.

Let S_i^+ denote the set of $(q_i - 1)/2$ congruences $\bmod\, q_i$ that solve $\big(\frac{p}{q_i}\big) = 1$ and S_i^- denote the set of $(q_i - 1)/2$ congruences $\bmod\, q_i$ that solve $\big(\frac{p}{q_i}\big) = -1$.

Clearly,

$$\Big(\frac{D}{p}\Big) = 1 \ \Leftrightarrow\ \Big(\frac{p}{q_1}\Big)\Big(\frac{p}{q_2}\Big) \dots \Big(\frac{p}{q_m}\Big) = 1. \tag{5.1}$$

Now, the equations

$$x_1x_2\dots x_m = 1 \quad \text{and} \quad x_1x_2\dots x_m = -1$$

each have $M = 2^{m-1}$ solutions in $\{-1,1\}^m$.

Let us enumerate them as

$$\begin{aligned} X_1 &= (x_{11}, x_{12}, \dots, x_{1m}), \\ X_2 &= (x_{21}, x_{22}, \dots, x_{2m}), \\ &\vdots \\ X_M &= (x_{M1}, x_{M2}, \dots, x_{Mm}), \end{aligned} \quad \text{and} \quad \begin{aligned} Y_1 &= (y_{11}, y_{12}, \dots, y_{1m}), \\ Y_2 &= (y_{21}, y_{22}, \dots, y_{2m}), \\ &\vdots \\ Y_M &= (y_{M1}, y_{M2}, \dots, y_{Mm}), \end{aligned}$$

where each of the x_{ij}, y_{ij} are 1 or -1. Depending on whether we need the product in equation (5.1) to be 1 or -1, we solve using X_i's or Y_j's, respectively.

Without loss of generality let us assume that we need the product to be 1.

Then, for each solution X_j, $j = 1, \dots, M$ we need to solve the system:

$$\begin{gathered} p \equiv 1 \bmod 4, \\ \left(\frac{p}{q_i}\right) = x_{ji}, \quad i = 1, \dots m. \end{gathered}$$

For each i, the equation $\left(\frac{p}{q_i}\right) = x_{ji}$ will involve choosing a congruence relation from $S_i^{\pm}$ depending on the parity of x_{ji}. This gives us a total of $\prod\limits_{i=1}^{m} (q_i - 1)/2$ systems of congruences for each X_j. By the Chinese remainder theorem, each system will give rise to a unique solution. Thus, the total number of solutions we obtain is

$$M \prod_{i=1}^{m} \frac{q_i - 1}{2} = 2^{m-1} \prod_{i=1}^{m} \frac{q_i - 1}{2} = \frac{1}{2} \prod_{i=1}^{m} (q_i - 1).$$

Similarly we get $\frac{1}{2} \prod\limits_{i=1}^{m} (q_i - 1)$ solutions coming from the parallel case of $p \equiv 3 \bmod 4$.

So, in total we have $\prod\limits_{i=1}^{m} (q_i - 1)$ of solutions $\pmod{4q_1q_2\dots q_m}$.

If we denote $Q = 4q_1q_2\dots q_m$, then $\left(\frac{D}{p}\right) = 1$ has $\frac{1}{2}\varphi(Q)$ of solutions $\bmod Q$.

Case (ii): $2 \mid D$. Without loss of generality, we may assume that $q_1 = 2$ and q_i is odd for $i = 2, \dots, k$.

Therefore, we need to find solutions to the equation

$$\left(\frac{D}{p}\right) = \pm\left(\frac{2}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_m}{p}\right) = \pm\left(\frac{2}{p}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_m}\right).$$

The only difference in this case is that instead of considering the congruence $p \equiv 1$ or 3 mod 4, we further consider congruences $\bmod 8$:

If $p \equiv 1$ mod 4, we have

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ mod } 8, \\ -1 & \text{if } p \equiv 5 \text{ mod } 8. \end{cases}$$

Thus in this case, for each $i = 2, \dots m$, we have $(q_i - 1)/2$ of congruences $\bmod q_i$ and one congruence $\bmod 8$ corresponding to $i = 1$. Therefore, for every X_j (or Y_j, depending on whether we need the product to be 1 or -1), we get $\prod\limits_{i=2}^{m} (q_i - 1)/2$ of solutions. Hence the total number of solutions is

$$\prod_{i=2}^{m} (q_i - 1).$$

Similarly, if $p \equiv 3$ mod 4, then we use

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 7 \text{ mod } 8, \\ -1 & \text{if } p \equiv 3 \text{ mod } 8 \end{cases}$$

and obtain another set of $\prod\limits_{i=2}^{m} (q_i - 1)$ solutions.

So we have a total of

$$2\prod_{i=2}^{m}(q_i - 1) = \frac{1}{2}\varphi(4q_1q_2 \dots q_m) = \frac{1}{2}\varphi(Q)$$

solutions, which is the same number as in Case (i).

To summarize, for a fixed number D, the number of odd primes $p \bmod Q$ such that $\left(\frac{D}{p}\right) = 1$ is $\frac{1}{2}\varphi(Q)$. Coming back to our problem, we wish to calculate

$$\#\left\{\text{primes } p \leqslant x \colon \left(\frac{D}{p}\right) = 1\right\}.$$

By Dirichlet's density theorem, we know that for any positive integer a which is coprime to n,

$$\#\{ \text{ primes } p \leqslant x \colon p \equiv a \text{ mod } n\} \sim \frac{1}{\varphi(n)}\pi(x).$$

Let $B(1) := \{b_i \colon i = 1, \dots, b_{\varphi(Q)/2}\}$ denote the set of solutions $\bmod Q$ obtained from the discussion above and $B(-1) := \{b'_i \colon i = 1, \dots, b'_{\varphi(Q)/2}\}$ denote the remaining residue classes that correspond to the primes $p \bmod Q$ such that $\left(\frac{D}{p}\right) = -1$. Then,

$\left(\frac{D}{p}\right) = 1$ if and only if p is congruent to any one of the elements in the set $B(1)$. So we have

$$\#\left\{\text{primes } p \leqslant x\colon \left(\frac{D}{p}\right) = 1\right\} = \sum_{i=1}^{\varphi(Q)/2} \#\{p \leqslant x,\ p \text{ prime}\colon\ p \equiv b_i \bmod Q\}$$
$$\sim \sum_{i=1}^{\varphi(Q)/2} \frac{1}{\varphi(Q)}\pi(x) = \frac{1}{2}\pi(x).$$

Hence, the asymptotic density of primes p for which $\left(\frac{D}{p}\right) = 1$ is $\frac{1}{2}$.

Using the set $B(-1)$, the same proof can be used to show that

$$\#\left\{\text{primes } p \leqslant x\colon \left(\frac{D}{p}\right) = -1\right\} \sim \frac{1}{2}\pi(x),$$

implying that the density of primes p for which $f(x)$ has no solution $\bmod p$ is $\frac{1}{2}$. □

We now use this proposition to prove Theorem 1.2.

Remark. From the statement of Proposition 1.1 and Theorem 1.2, it is clear that we are counting only those squarefree numbers with k-prime factors which are coprime to the discriminant D of $f(x)$.

Proof of Theorem 1.2. We first prove the statement for n odd.

In this case, using Proposition 1.1 we conclude that the condition

$$\left(\frac{D}{p_i}\right) = \varepsilon_i \quad \text{for each } i$$

will hold if and only if every prime p_i dividing n belongs to the set $B(\varepsilon_i)$.

Let us represent the (odd) squarefree number as a k-tuple $(p_1, p_2, \ldots, p_k)$ with $p_1 < p_2 < \ldots < p_k$ and choose any k-tuple $(m_1, m_2, \ldots, m_k)$ where each $m_i \in B(\varepsilon_i)$. Since $|B(\pm 1)| = \varphi(Q)/2$, the number of k-tuples such that

$$(p_1, p_2, \ldots, p_k) \equiv (m_1, m_2, \ldots, m_k) \bmod Q \tag{5.2}$$

component-wise is $(\varphi(Q)/2)^k$. Therefore, appplying Theorem 1.3, we have

$$\#\left\{\text{odd } n \leqslant x,\ n = p_1 p_2 \ldots p_k \text{ with } p_1 < p_2 < \ldots < p_k\colon \left(\frac{D}{p_i}\right) = \varepsilon_i \text{ for each } i\right\}$$
$$\sim \frac{1}{\varphi(Q)^k} \frac{x(\log\log x)^{k-1}}{(k-1)!\log x} \left(\frac{\varphi(Q)}{2}\right)^k,$$

setting the odd case.

Note. Even n are counted only if D is odd.

The even case follows by counting the number of odd squarefree $n \leqslant x/2$ with $k-1$ prime factors. From the argument for the odd case, we have

$$\#\Big\{n \leqslant x,\ n = 2p_2 \dots p_k,\ \text{with } 2 = p_1 < p_2 < \dots < p_k\colon \Big(\frac{D}{p_i}\Big) = \varepsilon_i \text{ for each } i\Big\} \\ \sim \frac{1}{\varphi(Q)^{k-1}} \pi_{k-1}(x/2) \Big(\frac{\varphi(Q)}{2}\Big)^{k-1}.$$

Noting that $\pi_{k-1}(x/2)/2^{k-1} = o\big(\pi_k(x)/2^k\big)$, the result follows. □

Corollary 5.1. *The density of squarefree numbers n with k prime factors such that a quadratic equation has exactly 2^k solutions* $\bmod n$ *is $1/2^k$.*

Proof. This easily follows from Theorem 1.2 by taking D as the discriminant of the quadratic equation and $\underline{\varepsilon}$ with $\varepsilon_i = 1$ for each i. □

Note. We may ask what happens when n has k prime factors counted with multiplicity, i.e., when $n = p_1 p_2 \dots p_k$ is not necessarily squarefree. We observe that in this case, the k-tuple $\underline{\mathrm{m}}$ will neccesarily have $m_i = m_j$ whenever $p_i = p_j$. Therefore, for such n, the number of k-tuples satisfying equation 5.2 will be bounded by $\big(\varphi(Q)/2\big)^k$ and equal to it if and only if n is squarefree. Hence, we deduce the following:

Corollary 5.2. *Let $D \in \mathbb{Z} - \{0\}$ and $k \in \mathbb{N}$. For any k-tuple $\underline{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k)$ where each $\varepsilon_i = \pm 1$ for each $i = 1, \dots, k$, we have*

$$\#\Big\{n \leqslant x\colon\ n = p_1 p_2 \dots p_k \text{ with } p_1 \leqslant p_2 \leqslant \dots \leqslant p_k, \\ \Big(\frac{D}{p_i}\Big) = \varepsilon_i \text{ for each prime } p_i \mid n\Big\} = O\Big(\frac{1}{2^k}\tau_k(x)\Big),$$

where $\tau_k(x)$ is the function defined in the introduction.

Acknowledgement. I thank my advisor Dr. Kaneenika Sinha for encouraging me to write this article and giving her comments, and Prof. Ram Murty for his comments, and suggesting some improvements. I would like to thank the referee for useful remarks and pointing out corrections.

References

[1] *G. H. Hardy, E. M. Wright*: An Introduction to the Theory of Numbers. Oxford University Press, Oxford, 2008.

[2] *H. Kornblum, E. Landau*: Über die Primfunktionen in einer arithmetischen Progression. Math. Zeitschr. *5* (1919), 100–111. (In German.)

[3] *E. Landau*: Sur quelques problèmes relatifs à la distribution des nombres premiers. S. M. F. Bull. *28* (1900), 25–38. (In French.)

[4] *H. L. Montgomery, R. C. Vaughan*: Multiplicative Number Theory. I. Classical Theory. Cambridge Studies in Advanced Mathematics 97, Cambridge University Press, Cambridge, 2007.

[5] *C. Pomerance*: On the distribution of amicable numbers. J. Reine Angew. Math. *293/294* (1977), 217–222.

[6] *P. Ribenboim*: The New Book of Prime Number Records. Springer, New York, 1996.

[7] *E. M. Wright*: A simple proof of a theorem of Landau. Proc. Edinb. Math. Soc., II. Ser. *9* (1954), 87–90.

Author's address: Neha Prabhu, Indian Institute of Science Education and Research, Dr Homi Bhabha Rd, NCL Colony, Pashan, Pune, Maharashtra 411008, India, e-mail: neha.prabhu@students.iiserpune.ac.in.