Санкт-Петербургский государственный университет

Ермошин Иван Алексеевич

Выпускная квалификационная работа

Задачи типа Варинга с простыми переменными

Образовательная программа бакалавриат «Математика»
Направление и код: 01.03.01 «Математика»
Шифр ОП: СВ.5000.2019

Научный руководитель:
Доцент, Факультет математики и компьютерных наук СПбГУ
д.ф.-м.н.,
Степанов Алексей Владимирович

Рецензент:
Научный сотрудник
Международная лаборатория зеркальной симметрии и автоморфных форм,
ФГБОУ ВО «Национальный исследовательский университет «Высшая школа экономики»,
д.ф.-м.н.,
Калмынин Александр Борисович

Санкт-Петербург
2023

Waring type problems with prime variables

Ivan Ermoshin

Contents

Abstract

In [2] J. Friedlander and H. Iwaniec established a conditional asymptotic formula for the mean value of $\Lambda(n)r_0(n-2)r_0(n+2)$, where $\Lambda(n)$ is the von Mangoldt function and $\Lambda(n) = \log n$ for $m = p^k$ with p a prime and is zero otherwise, $r_0(n)$ is the number of ways to write n as a sum of two positive squares. This is equivalent to showing a strengthening of Lagrange's four squares theorem, i.e. finding an asymptotic formula for $p = a^2 + b^2 + c^2 + d^2$ subject to hyperbolic condition $ad - bc = 1$. Here we aim at studying an analogous sum when one of the variables is restricted to prime, i.e. $\Lambda(n)r_1(n-2)r_0(n+2)$, where $r_1(n)$ is the number of ways to represent n as a sum of a square and a square of a prime.

1 Introduction

Notations: The letters p, q, r stand for prime numbers and $\mathbb{P}$ be the set of all primes. All logarithms are to base e. The signs $\ll$, $\gg$ are usual Vinogradov signs.

Let $\Lambda\colon \mathbb{N} \to \mathbb{N}$ be the von Mangoldt function defined as

$$\Lambda(n) = \begin{cases} \log p, & n = p^\alpha, \quad \alpha > 0, \\ 0, & n \neq p^\alpha, \end{cases}.$$

This function is smoothed characteristic function of primes and results about $\psi(x) = \sum\limits_{n \le x} \Lambda(n)$ usually are equivalent to results about $\pi(x) = \sum\limits_{p \le x} 1$.

Alternatively, one can define von Mangold function via

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d,$$

where $\mu(n)$ is the Möbius function,

$$\mu(n) = \begin{cases} (-1)^k, & n = p_1 \cdots p_k, \\ 0, & \exists p\colon p^2 \mid n. \end{cases},$$

and the second equality is an easy corollary of the inclusion exclusion principle, so

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & n = 1 \\ 0, & \text{otherwise} \end{cases}.$$

Also we define some standart number theory functions

$$\pi(x; q, a) = \sum_{\substack{p\le x \\ p\equiv a \bmod q}} 1, \quad \omega(n) = \sum_{p|n} 1.$$

Denote by $\left(\frac{a}{p}\right)$ the Legendre symbol given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \exists x:\ x^2 \equiv a \mod p, \\ 0, & (a,p) > 1, \\ -1, & \text{otherwise} \end{cases}.$$

For $0 \le i \le 2$ let $r_i(n)$ count number of representations of n as a sum of two squares with i prime restrictions

$$\begin{aligned} r_0(n) &= \#\{(a,b) \in \mathbb{N}^2 \colon a^2 + b^2 = n\}, \\ r_1(n) &= \#\{(a,p) \in \mathbb{N}\times\mathbb{P} \colon a^2 + p^2 = n\}, \\ r_2(n) &= \#\{(p,q) \in \mathbb{P}^2 \colon p^2 + q^2 = n\}. \end{aligned} \tag{1}$$

1.1 Preliminary

In [2] J. Friedlander and H. Iwaniec proved an asymptotic equivalence for the number of prime solutions to

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2 \le x$$

hyperbolic condition $x_1x_4 - x_2x_3 = 1$ i.e. they considered

$$\sum_{\substack{x_1^2+x_2^2+x_3^2+x_4^2\le x \\ x_1x_4 - x_2x_3 = 1}} \Lambda(x_1^2 + x_2^2 + x_3^2 + x_4^2) \asymp x$$

subject to weakened version of strong widely believed conjecture about the uniformity of the distribution of primes in arithmetic progressions.
Under the change of variables

$$\begin{cases} y_1 = x_1 + x_4, \\ y_2 = x_2 + x_3, \\ y_3 = x_1 - x_4, \\ y_4 = x_2 - x_3, \end{cases}$$

hence

$$\begin{cases} y_1^2 + y_2^2 = n + 2, \\ y_3^2 + y_4^2 = n - 2 \end{cases}.$$

Note that this change of variables is one-to-one, but due to parity restrictions precisely one of tuples (y_1, y_2, y_3, y_4) and (y_1, y_2, y_4, y_3) rise to an integer solution in the x's.

The sum becomes

$$\frac{1}{2}\sum_{n\le x}\Lambda(n) r_0(n-2) r_0(n+2).$$

This one is easier to consider via sieve techniques.

2 Auxiliary lemmas

Lemma 1. *For $x > 1$ and any $k \geq 1$ we have*

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} = \sum_{j=1}^{k} \frac{(j-1)!x}{(\log x)^j} + O\left(\frac{x}{(\log x)^{k+1}}\right).$$

The following lemma is taken from paper by Andrew Granville [3]

Lemma 2. *For any natural n we have*

$$\Lambda(n) = \log n - \sum_{\substack{l \mid n \\ l \neq n}} \Lambda(l)$$

Proof. Consider cases $n = p^k$ and $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ with $k > 1$, both are obvious. □

Lemma 3. *For $q, a > 1$ let $\varrho(q, a)$ count the number of solutions to $u^2 + v^2 \equiv a \bmod q$ subject to $(v, q) = 1$, i.e.*

$$\varrho(q, a) = \#\{u, v \bmod q, (v, q) = 1\colon u^2 + v^2 \equiv a \bmod q\}. \tag{2}$$

For $p \equiv 1 \bmod 4$

$$\rho(p, a) = \begin{cases} p - 2 - \left(\dfrac{a}{p}\right), & a \not\equiv 0 \bmod p, \\ 2(p-1), & a \equiv 0 \bmod p \end{cases}.$$

For $p \equiv 3 \bmod 4$

$$\rho(p, a) = \begin{cases} p - \left(\dfrac{a}{p}\right), & a \not\equiv 0 \bmod p, \\ 0, & a \equiv 0 \bmod p \end{cases}.$$

Moreover, we have $\varrho(p^\alpha, a) = p^{\alpha-1}\varrho(p, a)$ if $p \geq 3$ and $\alpha \geq 1$, and $\varrho(2^\alpha, a) = 2^{\alpha-3}\varrho(8, a)$ if $\alpha \geq 3$.

Lemma 4. *For $q, a > 1$ let $r(q, a)$ count the number of solutions to $u^2 + v^2 \equiv a \bmod q$, i.e.*

$$r(q, a) = \#\{u, v \bmod q\colon u^2 + v^2 \equiv a \bmod q\}. \tag{3}$$

For $p > 2$

$$r(p, a) = \begin{cases} p - \chi(p), & a \not\equiv 0 \bmod p, \\ p(1 + \chi(p)) - \chi(p), & a \equiv 0 \bmod p \end{cases}.$$

Moreover, we have $r(p^\alpha, a) = p^{\alpha-1} r(p, a)$ if $p \geq 3$ and $\alpha \geq 1$, and $r(2^\alpha, a) = 2^{\alpha-3} r(8, a)$ if $\alpha \geq 3$.

Note that both $\varrho(q, a)$ and $r(q, a)$ are multiplicative over q by the Chinese remainder theorem.

For proofs of both Lemmas above see [4].

3 Lemmas

3.1 The number of integers that can be written as a square and a square of a prime in an arithmetic progression

Lemma 5. *Let $a, q > 1$. Then we have*

$$\sum_{\substack{n\le x\\ n\equiv a \bmod q}} r_1(n) = \frac{\pi}{2}\frac{\varrho(a,q)}{q\varphi(q)} f(x) + O\Bigg(\sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q\\ (v,q)=1}} \frac{\sqrt{x}}{q} E^*(\sqrt{x}; q, v)\Bigg).$$

Proof. Acting as in the proof of [1, Theorem 3] we invoke the definition of r_1 from (1) and split the quadratic congruence into two linear ones, hence

$$\sum_{\substack{n\le x\\ n\equiv a \bmod q}} r_1(n) = \sum_{\substack{m^2+p^2\le x\\ m^2+p^2\equiv a \bmod q}} 1 = \sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q}} \sum_{\substack{m^2+p^2\le x\\ m\equiv u \bmod q\\ p\equiv v \bmod q}} 1.$$

Further, we can bound the contribution of pairs with $(v,q) > 1$ as

$$\sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q\\ (v,q)>1}} \sum_{\substack{m^2+p^2\le x\\ m\equiv u \bmod q\\ p\equiv v \bmod q}} 1 \ll \sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q\\ p\mid q\\ p\equiv v \bmod q}} \sum_{\substack{m^2\le x\\ m\equiv u \bmod q}} 1 \ll \omega(q)x^{1/2}$$

thus arriving at

$$\sum_{\substack{n\le x\\ n\equiv a \bmod q}} r_1(n) = \sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q\\ (v,q)=1}} \sum_{\substack{m^2+p^2\le x\\ m\equiv u \bmod q\\ p\equiv v \bmod q}} 1 + O(\omega(q)x^{1/2}). \tag{4}$$

Write the prime number theorem in arithmetic progressions as

$$\pi(x; q, a) = \frac{\pi(x)}{\varphi(q)} + E(x; q, a), \tag{5}$$

while the classical prime number theorem states

$$\pi(x) = \mathrm{Li}(x) + O(x\exp(-c\sqrt{\log x})), \quad c > 0. \tag{6}$$

Hence the inner sum in (4) is equal to

$$\begin{aligned}\sum_{\substack{m^2+p^2\le x\\ m\equiv u \bmod q\\ p\equiv v \bmod q}} 1 &= -\frac{1}{q}\int_{x^{1/4}}^{x^{1/2}} \pi(t; q, v)d\sqrt{x-t^2} + O(x^{3/4}) = \\ &= -\frac{1}{q}\int_{x^{1/4}}^{x^{1/2}} \frac{\mathrm{Li}(t)}{\varphi(q)} d\sqrt{x-t^2} - \frac{1}{q}\int_{x^{1/4}}^{x^{1/2}} E(t; q, v)d\sqrt{x-t^2} + O(x^{3/4}),\end{aligned} \tag{7}$$

where we applied (5) and bounded the contribution of (6) as

$$\int_2^{x^{1/4}} \pi(t; q, v)d\sqrt{x-t^2} \ll x^{3/4}.$$

We calculate the first integral using Lemma 1. Setting

$$f(x) = \sum_{k\ge 1} \frac{a_k x}{(\log x)^k}, \quad a_1 = 1,$$

where a_k are ... we obtain

$$\frac{\pi}{2}\frac{f(x)}{q\varphi(q)} = \frac{\pi}{2}\frac{1}{q\varphi(q)}\left(\frac{x}{\log x} + \dots\right).$$

The second integral in (7) can be estimated by the maximum of $E(t;q,v)$, i.e.

$$-\frac{1}{q}\int_{x^{1/4}}^{x^{1/2}} E(t;q,v)d\sqrt{x-t^2} = O\left(\frac{\sqrt{x}}{q}\max_{t\le\sqrt{x}}|E(t;q,v)|\right).$$

Thus we have

$$\sum_{\substack{n\le x\\ n\equiv a \bmod q}} r_1(n) = \sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q\\ (v,q)=1}} \frac{\pi}{2}\frac{f(x)}{q\varphi(q)} + O\left(\frac{\sqrt{x}}{q}\max_{t\le\sqrt{x}}|E(t;q,v)|\right) =$$

$$= \frac{\pi}{2}\frac{\varrho(a,q)}{q\varphi(q)}f(x) + O\Bigg(\sum_{\substack{u,v \bmod q\\ u^2+v^2\equiv a \bmod q\\ (v,q)=1}} \frac{\sqrt{x}}{q}E^*(\sqrt{x};q,v)\Bigg),$$

where $E^*(x;q,a) = \max_{t\le x}|E(t;q,a)|$ and $\varrho(a,q)$ is defined in (3).

□

3.2 Correlation of r_1 and r_0

Here we proceed analogously as in [5, Theorem 1, Sedunova]. On recalling that

$$r_0(n) = \sum_{d|n}\chi(d)$$

we divide the range of divisors into three parts

$$S(x) = \sum_{n\le x} r_1(n+2)r_0(n-2) = \sum_{n\le x} r_1(n+2)\sum_{i=1}^{3}\sigma_i(n-2),$$

where

$$\sigma_1(n) = \sum_{\substack{d|n\\ d\le\sqrt{n}/(\log x)^A}}\chi(d), \qquad \sigma_3(n) = \sum_{\substack{d|n\\ d\ge\sqrt{n}(\log x)^A}}\chi(d)$$

and σ_2 sums over missing d-s

$$\sigma_2(n) = \sum_{\substack{d|n\\ d\sim_A\sqrt{n}}}\chi(d).$$

When $2\nmid n$ it is easy to see via going to co-divisors that $\sigma_1(n) = \sigma_3(n)$, and A is some big enough constant.

$$S(x) = 2\sum_{n\le x} r_1(n+2)\sigma_1(n-2) + R(x),$$

where

$$R(x) = R_1(x) + R_1'(x),$$

where

$$R_1(x) = \sum_{n\le x} r_1(n+2)\sigma_2(n-2),$$

$$R_1'(x)=\sum_{\substack{n\le x\\ 2||n}} r_1(n+2)\sum_{\substack{d|n-2\\ 2^{-k}\sqrt{n-2}/(\log x)^A\le d\le \sqrt{n-2}/(\log x)^A}}\chi(d)$$

with $k=k(n)$ such that $2^k\mid\mid n-2$.
Working with both the main and the error term as in [5] we get

$$S(x)=\frac{\pi x}{\log x}\sum_{d\le D}\frac{\chi(d)\varrho(d,4)}{d\varphi(d)}+O\left(\frac{x\log\log x}{(\log x)^2}\right)=\frac{C_0\pi x}{\log x}+O\left(\frac{x\log\log x}{(\log x)^2}\right),$$

where we completed the sum over d to infinity

$$C_0=\sum_{d=1}^{\infty}\frac{\chi(d)\varrho(d,4)}{d\varphi(d)}.$$

3.3 The sum in arithmetic progression

Let d be an odd number. In the following sum we consider only $n\equiv 3 \bmod 4$ as $r_0(n-2)$ vanishes for $n\equiv 1 \bmod 4$. Consider the following sum over arithmetic progressions

$$\sum_{\substack{n\le x\\ n\equiv 3 \bmod 4\\ n\equiv 0 \bmod d}} r_1(n+2)r_0(n-2).$$

Since for $n-2\equiv 1 \bmod 4$ one has

$$r_0(n-2)=2\sum_{\substack{k|n-2\\ k<\sqrt{n-2}}}\chi(k)+\chi(\sqrt{n-2}),\tag{8}$$

where the last term vanishes unless $n-2$ is a square. We thus have

$$\sum_{\substack{n\le x\\ n\equiv 3 \bmod 4\\ n\equiv 0 \bmod d}} r_1(n+2)r_0(n-2)=2\sum_{k<\sqrt{x}}\chi(k)\sum_{\substack{k^2<n\le x\\ n\equiv 3 \bmod 4\\ n\equiv 0 \bmod d\\ n\equiv 2 \bmod k}} r_1(n+2)+O(x^{1/2+\varepsilon}).$$

Note that $\chi(k)$ vanishes at even k, so $(k,4)=1$; $(k,d)=1$ too because if $p\mid d, p\mid k$ then $p\mid n, p\mid n-2$ so $p=2$ or $p=1$. We can use Chinese remainder theorem and substitute r_1 in arithmetic progressions.
Thus

$$\sum_{\substack{n\le x\\ n\equiv 3 \bmod 4\\ n\equiv 0 \bmod d\\ n\equiv 2 \bmod k}} r_1(n+2)=\frac{\varrho(4,1)\varrho(k,4)\varrho(d,2)}{4dk\varphi(4dk)}f(x)+O\Bigg(\sum_{\substack{u,v \bmod 4dk\\ u^2+v^2\equiv a \bmod 4dk\\ (v,4dk)=1}}\frac{\sqrt{x}}{4dk}E^*(\sqrt{x};4dk,v)\Bigg).$$

Hence the main term of the right-hand side of (8) equals

$$2\sum_{\substack{k\le\sqrt{x}\\ (k,d)=1}}\chi(k)\Bigg(\frac{\varrho(4,1)\varrho(k,4)\varrho(d,2)}{4dk\varphi(4dk)}\pi'(x)+O\Bigg(\sum_{\substack{u,v \bmod 4dk\\ u^2+v^2\equiv a \bmod 4dk\\ (v,4dk)=1}}\frac{\sqrt{x}}{4dk}E^*(\sqrt{x};4dk,v)\Bigg)\Bigg)-$$

$$-O\Bigg(\sum_{\substack{k\le\sqrt{x}\\ (k,d)=1}}\frac{\chi(k)\varrho(4,1)\varrho(k,4)\varrho(d,2)}{4dk\varphi(4dk)}\pi'(k^2)\Bigg)=$$

$$= g(d)\biggl(C_0\pi'(x) + O\Bigl(\frac{x}{(\log x)^A}\Bigr)\biggr) + O\biggl(\sum_{\substack{k\le\sqrt{x}\\(k,2d)=1}}\;\sum_{\substack{u,v \bmod 4dk\\u^2+v^2\equiv 1 \bmod 4\\u^2+v^2\equiv 2 \bmod k\\u^2+v^2\equiv 4 \bmod d\\(v,4dk)=1}}\frac{\sqrt{x}}{4dk}E^*(\sqrt{x};4dk,v)\biggr),$$

where

$$C_0 = \sum_{k=1}^{\infty}\frac{\chi(k)\varrho(k,4)}{k\varphi(k)}$$

and $A > 0$ is any arbitrary large number and

$$g(d) = \prod_{\substack{p\equiv 1 \bmod 4\\p|d}}\Bigl(1 - \frac{p-3}{(p-2)(p+1)}\Bigr)\prod_{\substack{p\equiv 3 \bmod 4\\p|d}}\Bigl(1 + \frac{1}{p-2}\Bigr)\frac{\varrho(d,2)}{d\varphi(d)}.$$

4 Upper bound

In this section we prove the upper bound for

$$\sum_{n\le x}\Lambda(n)r_0(n-2)r_1(n+2).$$

Note that if $4 \mid n$ (denote $n = 4k$) than $r_1(n+2)r_0(n-2) \le r_0(n+2)r_0(n-2) = 0$ since if

$$4k+2 = 2^{\alpha}(4a+1), \quad 4k-2 = 2^{\beta}(4b+1),$$

so by parity $\alpha = \beta = 1$ and

$$2k+1 = 4a+1, \quad 2k-1 = 4b+1,$$

has no solutions.

By Lemma 2 we get

$$\sum_{n\le x}\log(n)r_0(n-2)r_1(n+2) - \sum_{\substack{l|n\\l\neq n\\n\le x}}\Lambda(\ell)r_0(n-2)r_1(n+2) = S_1(x) - S_2(x).$$

By partial summation formula

$$\sum_1 = \log x\sum_{n\le x}r_0(n-2)r_1(n+2) - \int_1^x\sum_{n\le t}r_0(n-2)r_1(n+2)\frac{dt}{t} = Cx + O\left(\frac{x\log\log x}{\log x}\right).$$

References

[1] S. Daniel. On the sum of a square and a square of a prime. *Math. Proc. Cambridge Philos. Soc.*, 131(1):1–22, 2001.

[2] John B. Friedlander and Henryk Iwaniec. Hyperbolic prime number theorem. *Acta Mathematica*, 202(1):1 – 19, 2009.

[3] Andrew Granville. An alternative to Vaughan's identity. *Riv. Math. Univ. Parma (N.S.)*, 12(1):119–124, 2021.

[4] V. A. Plaksin. Asymptotic formula for the number of solutions of an equation with primes. *Izv. Akad. Nauk SSSR Ser. Mat.*, 45(2):321–397, 463, 1981.

[5] Alisa Sedunova. Intersections of binary quadratic forms in primes and the paucity phenomenon. *J. Number Theory*, 235:305–327, 2022.