# ON A THEOREM OF BREDIHIN AND LINNIK

J.B. FRIEDLANDER* AND H. IWANIEC**

*Dedicated to the memory of Yu. V. Linnik.*

**Abstract:** We give a new proof of a theorem of B. M. Bredihin which was originally proved by extending Linnik's solution, via his dispersion method, of a problem of Hardy and Littlewood. [1]

## 1. **Introduction**

Among the many beautiful consequences of Linnik's dispersion method is an asymptotic formula for the number of solutions to the equation

$$p = a^2 + b^2 + 1$$

in primes $p \leqslant x$ and integers $a$ and $b$. This result of 1965, due to Bredihin [B] was a follow-up to Linnik's celebrated work on the Hardy-Littlewood problem, cf. Chapter 7 of [L]. The involved arguments are lengthy and complicated, though very inventive. Due to much progress over the intervening years, much shorter arguments can now be put forward. This of course does not mean that they are shorter ab-initio. Our purpose here is to illustrate how these arguments can be applied.

**THEOREM 1.** Let $S(x)$ be the number of solutions to

$$p = a^2 + b^2 + 1 \tag{1.1}$$

in integers $a$ and $b$ and primes $p \equiv 3 (\mathrm{mod}\, 8)$, $p \leqslant x$. We have

$$S(x) = c\,\frac{x}{\log x} + O\Big(x\Big(\frac{\log\log x}{\log x}\Big)^2\Big), \tag{1.2}$$

where the constant $c$ is given by

$$c = \frac{\pi}{2}\prod_p\Big(1 + \frac{\chi(p)}{p(p-1)}\Big), \tag{1.3}$$

with $\chi$ being the Dirichlet character of conductor 4.

* Supported in part by NSERC grant A5123.

** Supported in part by NSF grant DMS-1406981.

[1]keywords: primes, dispersion, Bombieri-Vinogradov theorem

The other reduced residue classes modulo 8 can be covered by essentially the same arguments but we do not treat them.

Note that the theorem shows that the integers $p-1$ tend to have about as many representations as the sum of two squares as does a typical integer $n$. Recall also that, if the number of representable $p-1$ is counted without multiplicity in $a$ and $b$, then the order of magnitude is given by $x/(\log x)^{3/2}$ by a theorem of the second-named author [I].

## 2. **Dirichlet divisor switching**

Let $\lambda = 1 * \chi$ that is

$$\lambda(n) = \sum_{ab=n} \chi(a) \tag{2.1}$$

This is similiar in many respects to the divisor function $\tau(n)$. The number of representations of $n$ as the sum of two squares is equal to $4\lambda(n)$. If $n \equiv 1 (\mathrm{mod}\, 4)$ then, in (2.1), $\chi(a)$ can be replaced by $\chi(b)$; therefore we can write

$$\lambda(n) = \sum_{\substack{a|n \\ a\leqslant y}} \chi(a) + \sum_{\substack{b|n \\ b<n/y}} \chi(b) \tag{2.2}$$

for any $y > 0$. We can refine this partition by integrating over $y$ against a smooth weight function. Let $w(t)$ be a smooth function supported on $1 \leqslant t \leqslant 2$ such that

$$\int_0^\infty w(t) t^{-1} dt = 1. \tag{2.3}$$

Let $Y \geqslant 1$, multiply (2.2) by $w(y/Y)$ and integrate with the measure $y^{-1}dy$, getting

$$\lambda(n) = \int_0^\infty \Big[ w\big(\frac{y}{Y}\big) + w\big(\frac{n}{yY}\big) \Big] \Big( \sum_{\substack{b|n \\ b<y}} \chi(b) \Big) \frac{dy}{y} \ . \tag{2.4}$$

Note that if $X < n \leqslant 2X$ we can choose $Y = \sqrt{X}$ so the integration in (2.4) runs over the segment $\frac{1}{2}\sqrt{X} < y < 2\sqrt{X}$.

## 3. **Primes in arithmetic progressions**

The key input which greatly streamlines the proof is the main result of [BFI] which gives asymptotics of Bombieri-Vinogradov type for the distribution of primes in arithmetic progressions and which treats moduli of the progression which go beyond the range of that which can be sucessfully handled even on the assumption of the Generalized Riemann Hypothesis.

We state this restricted to a range somewhat lesser than that in [BFI], which is however sufficient for our needs and is conveniently recorded as Theorem 2.2.1 of [FI].

$$\sum_{\substack{q\leqslant Q\\(q,a)=1}}\Big|\pi(x;q,a)-\frac{\pi(x)}{\varphi(q)}\Big|\ll x\Big(\frac{\log\log x}{\log x}\Big)^2 \tag{3.1}$$

for $Q=\sqrt{x}(\log x)^A$ with any $a\neq 0$, $A\geqslant 0$, $x\geqslant 3$, the implied constant depending only on $a$ and $A$.

We actually require a slightly modified form of (3.1) which follows from it in two easy steps. In the first place we have

$$\sum_{\substack{q\leqslant Q\\(q,a)=1\\(q,k)=1}}\Big|\sum_{\substack{p\leqslant x\\p\equiv a(\mathrm{mod}\,q)\\p\equiv \ell(\mathrm{mod}\,k)}}1-\frac{\pi(x)}{\varphi(qk)}\Big|\ll x\Big(\frac{\log\log x}{\log x}\Big)^2 \tag{3.2}$$

for $Q=\sqrt{x}(\log x)^A$ with any $a\neq 0$, $k\geqslant 1$, $(\ell,k)=1$, $A\geqslant 0$, $x\geqslant 3$, the implied constant depending only on $a$,$k$ and $A$. To this end one merely splits the indexed variables into classes modulo $k$, which is harmless for $k$ fixed.

In the second step we modify (3.2) to a counting of primes with smooth weight.

**LEMMA 3.1.** *Let $f(t)$ be a smooth function supported on $1\leqslant t\leqslant 2$. We have*

$$\sum_{\substack{q\leqslant Q\\(q,a)=1\\(q,k)=1}}\Big|\sum_{\substack{p\leqslant x\\p\equiv a(\mathrm{mod}\,q)\\p\equiv \ell(\mathrm{mod}\,k)}}f\big(\frac{p}{X}\big)-\frac{1}{\varphi(qk)}\sum_p f\big(\frac{p}{X}\big)\Big|\ll x\Big(\frac{\log\log x}{\log x}\Big)^2 \tag{3.3}$$

*for $Q=\sqrt{x}(\log x)^A$ with any $a\neq 0$, $k\geqslant 1$, $(\ell,k)=1$, $A\geqslant 0$, $x\geqslant 3$, the implied constant depending only on $a$,$k$, $A$ and $f$.*

*Proof.* We write

$$f\big(\frac{p}{X}\big)=-\int_{p/X}^{\infty}f'(t)dt.$$

Given $1\leqslant t\leqslant 2$ this implies $p\leqslant tX$. Applying (3.2) with $x=tX$ and integrating the result over $t$, we derive (3.3). □

## 4. **Proof of the theorem**

We have

$$S(x) = 4 \sum_{\substack{p\leqslant x\\ p\equiv 3 (\mathrm{mod}\, 8)}} \lambda\big(\frac{p-1}{2}\big). \tag{4.1}$$

We are going to evaluate

$$T(X) = S(2X) - S(X) = 4 \sum_{\substack{X<p\leqslant 2X\\ p\equiv 3 (\mathrm{mod}\, 8)}} \lambda\big(\frac{p-1}{2}\big) \tag{4.2}$$

for every $X \geqslant 3$. Applying (2.4) we write

$$T(X) = 4 \int \sum_{b<y} \chi(b) \sum_{\substack{X<p\leqslant 2X\\ p\equiv 1 (\mathrm{mod}\, b)\\ p\equiv 3 (\mathrm{mod}\, 8)}} \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p-1}{2yY}\big)\Big]\frac{dy}{y}$$

where we choose $Y = \sqrt{X}$. Here we can replace $w((p-1)/2yY)$ by $w(p/2yY)$ up to an error term $O(1/yY)$ which contributes to $T(X)$ a bounded amount:

$$T(X) = 4 \int \sum_{b<y} \chi(b) \sum_{\substack{X<p\leqslant 2X\\ p\equiv 1 (\mathrm{mod}\, b)\\ p\equiv 3 (\mathrm{mod}\, 8)}} \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p}{2yY}\big)\Big]\frac{dy}{y} + O(1)\,.$$

Note that the integration runs over the segment $\frac{1}{4}\sqrt{X} < y < 2\sqrt{X}$. Now we can apply (3.2) for the first term and (3.3) for the second term with $q = b$, $k = 8$, $\ell = 3$, getting

$$T(X) = \int \sum_{b<y} \frac{\chi(b)}{\varphi(b)} \sum_{X<p\leqslant 2X} \Big[w\big(\frac{y}{Y}\big)+w\big(\frac{p}{2yY}\big)\Big]\frac{dy}{y} + O\Big(X\Big(\frac{\log\log X}{\log X}\Big)^2\Big)\,.$$

Next, we replace the sum over $b < y$ by the complete series

$$c_1 = \sum_b \frac{\chi(b)}{\varphi(b)} = L(1,\chi)\prod_p\Big(1 + \frac{\chi(p)}{p(p-1)}\Big) \tag{4.3}$$

up to an error term $O(1/y)$ which contributes to $T(X)$ at most $O(\sqrt{X}/\log X)$. Now the free integration over $y$ yields (see (2.3))

$$\int \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p}{2yY}\big)\Big]\frac{dy}{y} = 2\,.$$

Therefore,

$$T(X) = 2c_1\big(\pi(2X) - \pi(X)\big) + O\Big(X\Big(\frac{\log\log X}{\log X}\Big)^2\Big)\,.$$

Summing this over $X = 2^{-n}x$, $n = 1, 2, 3, \ldots$, we derive (1.2), thus completing the proof of theorem 1.

## References


[BFI] E. Bombieri, J.B. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli III, *J. Amer. Math. Soc.* **2** (1989), 215–224.

[B] B.M. Bredihin, Binary additive problems of indeterminate type. II. Analogue of the problem of Hardy and Littlewood, *Izv. Akad. Nauk SSSR Ser. Mat.* **27** (1963), 577–612.

[FI] J.B. Friedlander and H. Iwaniec, Opera de Cribro, *Amer. Math. Soc. Colloq. Pub.* **57** AMS (Providence), 2010.

[I] H. Iwaniec, Primes of the type $\phi(x, y) + A$ where $\phi$ is a quadratic form, *Acta Arith.* **21** (1972), 203–234.

[L] Yu. V. Linnik, The Dispersion Method in Binary Additive Problems (translated from the Russian by S. Schuur), AMS (Providence), 1963



Department of Mathematics, University of Toronto
Toronto, Ontario M5S 2E4, Canada

Department of Mathematics, Rutgers University
Piscataway, NJ 08903, USA