ACTA ARITHMETICA
Online First version

Equidistribution for solutions of $p + m^2 + n^2 = N$, and for Châtelet surfaces

by

D. R. Heath-Brown (Oxford)

For Henryk Iwaniec
in celebration of his 75th birthday

1. Introduction. It was shown by Linnik [11, 12] that every large integer N may be represented as $N = p + m^2 + n^2$ with p prime. His work built on a method of Hooley [7], who had established this result subject to the Generalized Riemann Hypothesis. In fact, there is a positive constant δ such that

$$\#\{(p, m, n) : p + m^2 + n^2 = N\} = \frac{N}{\log N} C(N) + O(N(\log N)^{-1-\delta})$$

with

$$C(N) = \pi \prod_{p>2} \left(1 + \frac{\chi_4(p)}{p(p-1)}\right) \prod_{p|N} \frac{(p-1)(p-\chi_4(p))}{p^2 - p + \chi_4(p)},$$

(where χ_4 is the non-trivial character modulo 4) – see Hooley [8, Chapter 5], for example. We remark here that

$$(\log\log N)^{-1/2} \ll C(N) \ll (\log\log N)^{1/2},$$

so that the asymptotic formula saves a power of $\log N$ over the main term.

In this paper we examine the distribution of the solutions p, m, n. There are various ways to do this, but the approach we describe appears to be very flexible. It should be stressed however that most of the results we describe in the context of the equation $N = p + m^2 + n^2$ and its generalizations can be obtained by a different route, given by Bredikhin and Linnik [2].

2020 *Mathematics Subject Classification*: Primary 11D45; Secondary 11G35, 11R44, 14G05.
Key words and phrases: equidistribution, primes, binary quadratic forms, Châtelet surfaces.
Received 5 January 2023.
Published online 4 May 2023.

DOI: 10.4064/aa230105-10-3

There is no difficulty in controlling the size of the variable p, and it is an easy matter to adapt Hooley's argument to show that

$$\#\{(p,m,n) : p+m^2+n^2 = N,\ aN < p \le bN\} \\ = (b-a)\frac{N}{\log N}C(N) + O(N(\log N)^{-1-\delta})$$

uniformly for $0 \le a < b \le 1$. If $aN < p \le bN$ then (m,n) will lie in the annulus $(1-b)N \le m^2+n^2 \le (1-a)N$. In order to describe the equidistribution of (m,n) within this annulus it is natural to write $\alpha = m+in \in \mathbb{Z}[i]$, with $N(\alpha) = m^2+n^2$, and to consider $\arg(\alpha)$. We then have the following result.

THEOREM 1.1. *There is an absolute constant $\delta > 0$ with the following property. Let real numbers a, b, c, d be given, with $0 \le a < b \le 1$ and $0 \le c < d \le 2\pi$. Let $N \in \mathbb{N}$ be given. Then*

$$\#\{(p,\alpha) : p \text{ prime},\ \alpha \in \mathbb{Z}[i],\ p+N(\alpha) = N,\ aN < p \le bN,\ c < \arg(\alpha) \le d\} \\ = \frac{(b-a)(d-c)}{2\pi}\,\frac{N}{\log N}C(N) + O(N(\log N)^{-1-\delta}).$$

The natural way to handle the restriction on $\arg(\alpha)$ is via the Erdős–Turán inequality. For any finite subset A of $\mathbb{Z}[i]$ and any $H \in \mathbb{N}$ we have

$$\#\{\alpha \in A : c < \arg(\alpha) \le d\} \\ = \frac{d-c}{2\pi}\#A + O(H^{-1}\#A) + O\Big(H^{-1}\sum_{h\le H}\Big|\sum_{\alpha\in A}\Big(\frac{\alpha}{|\alpha|}\Big)^h\Big|\Big).$$

In our setting the term $O(H^{-1}\#A)$ will contribute $O(NC(N)/(H\log N))$ in Theorem 1.1, and so we see that the required result will follow from the following estimate, on taking $H = \log N$, for example.

THEOREM 1.2. *Define*

$$g_h(n) = \frac{1}{4}\sum_{N(\alpha)=n}\Big(\frac{\alpha}{|\alpha|}\Big)^h$$

and $f_h(n) = |g_h(n)|$. Then

$$\sum_{p<N} f_h(N-p) \ll_\varepsilon N(\log N)^{-5/4+\varepsilon}$$

for any fixed $\varepsilon > 0$, uniformly for $1 \le h \le \log N$.

We remark that the exponent $5/4$ can be improved to $2-2/\pi$, but this has no qualitative benefit for us.

The reader may be surprised that it is sufficient to consider the average of $f_h(N-p)$, rather than $g_h(N-p)$. The fact that this is indeed enough is

the fundamental observation behind this paper. As motivation, we point out that for most primes p the number $N - p$ will not be a sum of two squares, and $g_h(N - p)$ will therefore vanish. However, when $N - p$ is a sum of two squares, the sum for $g_h(N - p)$ will typically contain many terms α, so that we may expect some cancellation to occur.

The above idea, that we can obtain enough cancellation by considering $|g_h(n)|$ rather than $g_h(n)$, has occurred previously in other contexts. (We are grateful to Valentin Blomer for this observation.) Thus, for example, Holowinsky's work [6] on Quantum Unique Ergodicity looks at shifted convolution sums

$$\sum_{n \le x} |\lambda_1(n)\lambda_2(n + l)|,$$

which can be handled non-trivially using Erdős' method. In Holowinsky's application, one takes $\lambda_1 = \lambda_2$ to be the Fourier coefficients of a holomorphic modular cusp form.

The above ideas can be applied in many other situations. For example, one may consider the equidistribution of points on Châtelet surfaces given by equations

$$F(u, v) = x^2 - ay^2,$$

where $F \in \mathbb{Z}[u, v]$ is a separable quartic polynomial and $a \in \mathbb{Z}$ is not a square. Investigations into Manin's Conjecture for these surfaces have focused on the case $a = -1$, but in this situation the conjecture has been established for all forms F. The most difficult case, in which F is irreducible over $\mathbb{Q}(i)$, has been handled by de la Bretèche and Tenenbaum [4]. Since one is interested in rational points, it is natural to consider solutions to

$$t^2 F(u, v) = x^2 + y^2 \tag{1.1}$$

with

$$t, u, v, x, y \in \mathbb{Z}, \quad \gcd(u, v) = \gcd(t, x, y) = 1, \quad t > 0. \tag{1.2}$$

The counting function considered by de la Bretèche and Tenenbaum is one half the number of solutions satisfying the height condition

$$t^{1/2} \max(|u|, |v|) \le B^{1/2}. \tag{1.3}$$

They then obtain an asymptotic formula

$$\sigma_\infty(F)\mathfrak{S}(F)B \log B + O_F(B(\log B)^{99/100}),$$

where

$$\sigma_\infty(F) = \frac{\pi}{2} \operatorname{meas} \{(u, v) \in [-1, 1]^2 : F(u, v) > 0\}$$

and $\mathfrak{S}(F)$ is a product of p-adic densities. There is no difficulty in adapting the argument to replace (1.3) with a condition

$$t^{1/2}(u, v) \in B^{1/2}\mathcal{R} \tag{1.4}$$

for an arbitrary rectangle $\mathcal{R} \subseteq [-1,1]^2$. This produces an analogous asymptotic formula with $\sigma_\infty(F)$ replaced by

$$\sigma_\infty(F;\mathcal{R}) = \frac{\pi}{2}\,\mathrm{meas}\,\{(u,v) \in \mathcal{R} : F(u,v) > 0\}.$$

We then have the following result, which controls the argument of $x+iy$, in addition to the location of (u,v).

THEOREM 1.3. *Suppose one is given a rectangle $\mathcal{R} \subseteq [-1,1]^2$ and real numbers $a < b$ in $[0,2\pi]$. Let $N(B)$ be half the number of 5-tuples $(t,u,v,x,y) \in \mathbb{Z}^5$ satisfying (1.1) and (1.2), and with*

$$t^{1/2}(u,v) \in B^{1/2}\mathcal{R} \quad \textit{and} \quad \arg(x+iy) \in [a,b].$$

Then

$$N(B) = \frac{b-a}{2\pi}\sigma_\infty(F;\mathcal{R})\mathfrak{S}(F)B\log B + O_F(B(\log B)^{99/100}).$$

The key input here is the following estimate, which we will prove in §3.

LEMMA 1.4. *For any fixed $\varepsilon > 0$ we have*

$$\sum_{t^{1/2}\max(|u|,|v|)\le B^{1/2}} \left| \sum_{\substack{x^2+y^2=t^2F(u,v)\\ \gcd(t,x,y)=1}} \left(\frac{x+iy}{|x+iy|}\right)^{4h} \right| \ll_{F,\varepsilon} B(\log B)^{3/4+\varepsilon}$$

uniformly for $1 \le h \le \log B$.

These ideas are not restricted to the use of Grössencharacters. For example we can consider the equation $N = p+m^2+n^2$ subject to congruence conditions on m and n by looking at $N = p+N(\alpha)$ subject to $\alpha \equiv \alpha_0 \pmod k$, say, with $\alpha_0 \in \mathbb{Z}[i]$ coprime to $k \in \mathbb{N}$. This condition can be detected with Dirichlet characters $\chi \pmod k$ over $\mathbb{Z}[i]$. With these we have the following estimate.

THEOREM 1.5. *Let $k \in \mathbb{N}$ and $\varepsilon > 0$ be given. Then*

$$\sum_{p<N} \left| \frac{1}{4} \sum_{N(\alpha)=N-p} \chi(\alpha) \right| \ll_{k,\varepsilon} N(\log N)^{-5/4+\varepsilon}$$

for every non-principal Dirichlet character $\chi \pmod k$ over $\mathbb{Z}[i]$ such that $\chi(i) = 1$.

We leave the details of the proof to the reader. In order to apply this to examine $N = p+N(\alpha)$ with $\alpha \equiv \alpha_0 \pmod k$ (for α_0 coprime to k), we need to know

$$\sum_{N=p+N(\alpha)} \chi_0(\alpha)$$

where χ_0 is the principal character modulo k. However, α and k are coprime if and only if $N(\alpha)$ and k are coprime, so that it is enough to consider

$$\#\{(p, m, n) : N = p + m^2 + n^2,\ \gcd(N - p, k) = 1\}.$$

This may be tackled by a trivial variant of Hooley's method, in which one puts congruence conditions on p.

One can also handle congruence conditions $\alpha \equiv \alpha_0 \pmod{k}$ when α_0 shares a common factor with k. If $\alpha_0 = \beta\alpha_1$ and $k = \beta\gamma$ with α_1 and γ coprime then the congruence $\alpha \equiv \alpha_0 \pmod{k}$ implies that $\alpha = \beta\alpha'$, say, with

$$\alpha' \equiv \alpha_1 \pmod{\gamma}. \tag{1.5}$$

The equation $N = p + N(\alpha)$ then requires $p \equiv N \pmod{N(\beta)}$, so that we have to solve

$$\frac{N - p}{N(\beta)} = N(\alpha') \quad \text{with} \quad p \equiv N \pmod{N(\beta)},$$

subject to the congruence condition (1.5). We can tackle this with the machinery described above, using a version of Theorem 1.5 in which one restricts to primes $p \equiv N \pmod{N(\beta)}$ and replaces the summation condition $N(\alpha) = N - p$ by $N(\alpha) = (N - p)/N(\beta)$. In particular, this is enough to give an asymptotic formula for the number of solutions to

$$N = p + a^4m^2 + b^4n^2$$

for any fixed $a, b \in \mathbb{N}$, and thereby to count solutions of

$$N = p + m^2 + n^2, \qquad m, n \text{ square-free.}$$

This is the problem for which Hooley [9] proves a positive lower bound. The reader should note though that Hooley [9, p. 202] suggests that the necessary asymptotic formulae "can probably be established ... by a different method involving an elaborate use of the arithmetic of binary quadratic forms."

One can also replace $m^2 + n^2$ by other quadratic forms, and this was the main achievement (in the context of the equation $N = p + m^2 + n^2$) in the work of Bredikhin and Linnik [2] mentioned earlier. As an example, we consider the Châtelet surface

$$F(u, v) = x^2 - 2y^2,$$

where $F(u, v) \in \mathbb{Z}[u, v]$ is a quartic form, assumed now to be irreducible over $\mathbb{Q}(\sqrt{2})$. The function

$$r_2(n) = \sum_{\substack{d \mid n \\ d \,\text{odd}}} \left(\frac{2}{d}\right), \qquad n \in \mathbb{Z} \setminus \{0\},$$

counts solutions of $n = x^2 - 2y^2$ once from each set of associates of $x + y\sqrt{2}$.

Equivalently, $r_2(n)$ counts integral ideals I of $\mathbb{Q}(\sqrt{2})$ having norm $N(I)=|n|$. (Previously we had used $N(*)$ for the norm function on $\mathbb{Q}(i)$, but here it is the norm on $\mathbb{Q}(\sqrt{2})$. We trust this will cause no confusion.) A moment's reflection shows that if $t^2 \mid x^2-2y^2$ then $\gcd(t,x,y)=1$ if and only if $\gcd(t,\alpha,\alpha^\sigma)=1$, where $\alpha = x+y\sqrt{2}$ and σ is the non-trivial automorphism of $\mathbb{Q}(\sqrt{2})$. One therefore wants to count solutions to

$$t^2|F(u,v)| = N(I) \tag{1.6}$$

subject to $\gcd(u,v) = \gcd(t,I,I^\sigma) = 1$, lying in a region (1.4), these being the natural analogues of (1.1)–(1.2). The method of de la Bretèche and Tenenbaum [4] can be readily adapted to show that the number of solutions takes the form

$$c(\mathcal{R})B\log B + O_F(B(\log B)^{99/100}),$$

with a constant $c(\mathcal{R})$ depending on F as well as $\mathcal{R}$. However, one would wish to control the location of the corresponding points (x,y) for which $I=(x+y\sqrt{2})$. If $\mathcal{R}$ is suitably small, one will know the product

$$\left(\frac{|x-y\sqrt{2}|}{t}\right)\left(\frac{|x+y\sqrt{2}|}{t}\right) = t^{-2}N(I) = |F(u,v)|$$

to a good degree of approximation, and hence it is enough to control the quotient

$$\left(\frac{|x-y\sqrt{2}|}{t}\right) / \left(\frac{|x+y\sqrt{2}|}{t}\right) = \frac{|x-y\sqrt{2}|}{|x+y\sqrt{2}|}.$$

We can do this, and indeed slightly more, by using the Grössencharacter

$$\chi(I) = \operatorname{sgn}(x^2-2y^2)\exp\left\{\pi i\frac{\log|x-y\sqrt{2}| - \log|x+y\sqrt{2}|}{2\log(1+\sqrt{2})}\right\},$$

where $I=(x+y\sqrt{2})$. (The reader who is unfamiliar with such things may readily check that this is at least well-defined.) In analogy to Lemma 1.4 we have the following bound.

Lemma 1.6. *For any fixed $\varepsilon>0$ we have*

$$\sum_{t^{1/2}\max(|u|,|v|)\le B^{1/2}} \Big| \sum_{\substack{N(I)=t^2F(u,v)\\ \gcd(t,I,I^\sigma)=1}} \chi(I)^h \Big| \ll_{F,\varepsilon} B(\log B)^{3/4+\varepsilon}$$

uniformly for $1\le h\le \log B$.

This allows us to count solutions to (1.6) asymptotically, with $\chi(I)$ restricted to any given arc of the unit circle. A moment's thought shows that this corresponds to having $I=(x+y\sqrt{2})$ with $(x-y\sqrt{2})/(x+y\sqrt{2})$ in a given interval $(a,b)\subset(-\infty,0)\cup(0,\infty)$. We are then able to count solutions to $t^2F(u,v)=x^2-2y^2$ in which both (u,v) and (x,y) lie in prescribed regions.

Lastly, we mention that one can work analogously with class group characters. Suppose, for example, that we are interested in the Châtelet surface

$$F(u, v) = x^2 + 14y^2,$$

for a quartic form $F \in \mathbb{Z}[u, v]$ which is irreducible over $\mathbb{Q}(\sqrt{-14})$ ([1]). There are four classes of positive definite binary quadratic forms of discriminant -56, with representatives $x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 + 2xy + 5y^2$, and $3x^2 - 2xy + 5y^2$. Since the first two of these lie in the same genus, it is not possible to separate out representations by these two forms using only congruence conditions. The combined number of representations of $n \in \mathbb{N}$ by all four classes of forms is twice the number of integral ideals I of $\mathbb{Q}(\sqrt{-14})$ with norm $N(I) = n$; and the number of representations by x^2+14y^2 is twice the number of such I that are principal. As above, we will want to consider solutions to $t^2F(u, v) = N(I)$ with $\gcd(u, v) = 1$ and $\gcd(t, I, I^\sigma) = 1$, where σ is now complex conjugation. We may obtain an asymptotic formula for the problem in which we count both principal and non-principal ideals I, based on the formula

$$\#\{I : N(I) = n\} = \sum_{\substack{d \mid n \\ \gcd(d,14)=1}} \left(\frac{-14}{d}\right),$$

and following the method laid out by de la Bretèche and Tenenbaum [4]. Then, to restrict the count to principal ideals we use class group characters. Following our previous argument we then see that the following lemma suffices:

LEMMA 1.7. *Let χ be a non-trivial class group character for $\mathbb{Q}(\sqrt{-14})$, and let N be the norm function for $\mathbb{Q}(\sqrt{-14})$. Then for any fixed $\varepsilon > 0$ we have*

$$\sum_{t^{1/2} \max(|u|,|v|) \le B^{1/2}} \Big| \sum_{\substack{N(I)=t^2F(u,v) \\ \gcd(t,I,I^\sigma)=1}} \chi(I) \Big| \ll_{F,\varepsilon} B(\log B)^{3/4+\varepsilon},$$

where I runs over integral ideals of $\mathbb{Q}(\sqrt{-14})$.

This may be proved following the same reasoning as for Lemma 1.6, the key information input being the Prime Ideal Theorem for ideal classes.

2. Proof of Theorem 1.2. It is clear that $g_h(n)$ vanishes unless $4 \mid h$, since each α has associates $\alpha, i\alpha, -\alpha, -i\alpha$, and $1 + i^h + (-1)^h + (-i)^h = 0$ unless $4 \mid h$. We therefore henceforth assume that $4 \mid h$. We now claim that $g_h(n)$ is multiplicative, whence $f_h(n)$ is also multiplicative. To establish the

([1]) We are grateful to Evan O'Dorney for pointing out an error in the discussion of this problem in an earlier version of this paper.

claim, suppose that $n = uv$ with coprime factors u, v. Then it merely suffices to observe that each α of norm n can be written as $\alpha = \beta\gamma$ with $N(\beta) = u$ and $N(\gamma) = v$ in exactly four ways, corresponding to the four associate choices of $\beta = \gcd(\alpha, u)$. (We leave it to the reader to check this.)

We now call on a general result that gives accurate order of magnitude estimates for sums of non-negative multiplicative functions. Such bounds go back to Erdős [5], and were investigated further by Barban and Vehov [1] and Shiu [14] amongst others. For our application we need a version that applies to sums of functions over sifted sequences, and this has been given by Pollack [13, Theorem 1.1]. In his notation we take $k = 1$, $\beta = 1/4$ and $y = x$.

LEMMA 2.1. *Let $f(n)$ be a multiplicative function satisfying $0 \le f(n) \le d(n)$ for all $n \in \mathbb{N}$. Suppose that for each prime $p \le x$ the set $\mathcal{E}_p$ is either the empty set or a non-zero residue class modulo p, and write $\nu(p) = 0$ or $\nu(p) = 1$ accordingly. Let*

$$\mathcal{S} = \bigcap_{p \le x} \mathcal{E}_p^c.$$

Then

$$\sum_{\substack{n \le x \\ n \in \mathcal{S}}} f(n) \ll \frac{x}{\log x} \exp\Bigg(\sum_{p \le x} \frac{f(p) - \nu(p)}{p} \Bigg).$$

The reader should observe that our requirement that $0 \le f(n) \le d(n)$ implies Pollack's condition $f \in \mathcal{M}$.

We apply this lemma with $x = N$ and $f = f_h$. We take $\mathcal{E}_p$ to consist of the residue class $N \pmod p$ when $p \le \sqrt{N}$ does not divide N, and to be the empty set otherwise. Then if $p \ge \sqrt{N}$ is prime we will have $N - p \in \mathcal{S}$. The lemma then tells us that

$$\sum_{\sqrt{N} \le p \le N} f_h(N - p) \ll \frac{N}{\log N} \exp\Bigg(\sum_{p \le N} \frac{f_h(p) - \nu(p)}{p} \Bigg).$$

Here we note that

$$\begin{aligned} \sum_{p \le N} p^{-1} \nu(p) &\ge \sum_{p \le \sqrt{N}} p^{-1} - \sum_{p \mid N} p^{-1} \\ &\ge \log\log N + O(1) - \sum_{p \le \omega(N)} p^{-1} \\ &\ge \log\log N + O(1) - \sum_{p \le \log N} p^{-1} \\ &= \log\log N - \log\log\log N + O(1), \end{aligned} \tag{2.1}$$

so that

$$\sum_{\sqrt{N}\le p\le N} f_h(N-p) \ll \frac{N\log\log N}{(\log N)^2}\exp\Big(\sum_{p\le N}\frac{f_h(p)}{p}\Big),$$

and hence

$$\sum_{p\le N} f_h(N-p) \ll \sqrt{N} + \frac{N\log\log N}{(\log N)^2}\exp\Big(\sum_{p\le N}\frac{f_h(p)}{p}\Big). \tag{2.2}$$

It remains to consider

$$\sum_{p\le N}\frac{f_h(p)}{p}.$$

Of course $f_h(p)=0$ if $p\equiv 3 \pmod 4$, while if $p\equiv 1 \pmod 4$ we may write $p=N(\alpha)$ for some particular α, in which case $f_h(p)=2|\cos(h\arg(\alpha))|$. We now use the famous inequality $3+4\cos\theta+\cos 2\theta\ge 0$, which implies

$$2|\cos\theta| \le \tfrac{3}{2}+\tfrac{1}{2}\cos(2\theta)$$

for all real θ, and hence

$$f_h(p) \le \tfrac{3}{2}+\tfrac{1}{4}g_{2h}(p) \tag{2.3}$$

for $p\equiv 1 \pmod 4$. Since $f_h(p)$ and $g_{2h}(p)$ vanish for $p\equiv 3 \pmod 4$, it follows that

$$\sum_{3\le p\le N}\frac{f_h(p)}{p} \le \frac{3}{2}\sum_{\substack{p\le N\\ p\equiv 1 \pmod 4}}\frac{1}{p}+\frac{1}{4}\sum_{3\le p\le N}\frac{g_{2h}(p)}{p}.$$

The first sum on the right is $\frac{1}{2}\log\log N+O(1)$, whence

$$\sum_{3\le p\le N}\frac{f_h(p)}{p} \le \frac{3}{4}\log\log N + O(1) + \frac{1}{4}\sum_{3\le p\le N}\frac{g_{2h}(p)}{p}. \tag{2.4}$$

To estimate the sum on the right we call on the Prime Number Theorem for primes over $\mathbb{Q}(i)$ with Grössencharacter, in the following form.

LEMMA 2.2. *There is an absolute constant $c>0$ such that*

$$\sum_{\substack{\alpha\in\mathbb{Z}[i]\\ N(\alpha)\le x}}\Lambda(\alpha)\Big(\frac{\alpha}{|\alpha|}\Big)^{4k} \ll x\exp\Big\{-c\frac{\log x}{\sqrt{\log x}+\log k}\Big\}(\log xk)^4$$

uniformly for $x\ge 2$ and $k\in\mathbb{N}$.

This is a special case of Theorem 5.13 in Iwaniec and Kowalski [10], as the reader may confirm. Using partial summation we may deduce from

Lemma 2.2 that if $N_0 = \exp\{(\log 3k)^2\}$ then

$$\sum_{\substack{\alpha\in\mathbb{Z}[i]\\ N_0<N(\alpha)\le N}} \frac{\Lambda(\alpha)}{N(\alpha)\log N(\alpha)}\left(\frac{\alpha}{|\alpha|}\right)^{4k} \ll 1$$

uniformly for $N \ge N_0$ and $k \in \mathbb{N}$. A trivial bound shows that we may include terms with $N(\alpha) \le N_0$ at a cost $O(\log\log k)$, and that we may remove terms in which $N(\alpha)$ is not a prime at a cost $O(1)$. Taking $4k = 2h$ we then deduce that

$$\sum_{3\le p\le N} \frac{g_{2h}(p)}{p} \ll \log\log h$$

whenever $4 \mid h$. Substituting this into (2.4) we find that

$$\sum_{3\le p\le N} \frac{f_h(p)}{p} \le \frac{3}{4}\log\log N + O(\log\log h).$$

Inserting this bound into (2.2) we have

$$\sum_{p\le N} f_h(N-p) \ll \sqrt{N} + \frac{N\log\log N}{(\log N)^{5/4}}(\log h)^A$$

for some absolute constant A. This is sufficient for Theorem 1.2.

3. Proof of Theorem 1.3. In analogy to the argument that leads from Theorem 1.2 to Theorem 1.1, we see that Lemma 1.4 will suffice for the proof of Theorem 1.3. To establish the lemma we first note that t is composed entirely of primes $p \equiv 1 \pmod 4$ whenever $t^2 \mid x^2 + y^2$ with $\gcd(t, x, y) = 1$. Moreover if $p^e \mid t$ with a prime $p = N(\pi)$ over $\mathbb{Z}[i]$, then we must have either $\pi^e \mid x + iy$ or $\pi^e \mid x - iy$. Furthermore, if $\pi^e \mid x + iy$ with $e \ge 1$ it follows that $x + iy$ must be coprime to $\overline{\pi}$. Thus $x + iy$ must be divisible by some μ with $N(\mu) = t$ such that $\gcd(\mu, \overline{\mu}) = 1$, and with $\gcd(x + iy, \overline{\mu}) = 1$. In order to count each set of associates $i^n\mu$ just once, we restrict μ to be primary; that is, we require that $\mu \equiv 1 \pmod{2 + 2i}$.

We now write $x + iy = \mu\alpha$, so that

$$\sum_{\substack{x^2+y^2=t^2F(u,v)\\ \gcd(t,x,y)=1}} \left(\frac{x+iy}{|x+iy|}\right)^{4h} = \sum_{\mu}\left(\frac{\mu}{|\mu|}\right)^{4h} \sum_{\substack{N(\alpha)=F(u,v)\\ \gcd(\alpha,\overline{\mu})=1}} \left(\frac{\alpha}{|\alpha|}\right)^{4h},$$

where the sum over μ is taken over solutions of $N(\mu) = t$ subject to $\gcd(\mu, \overline{\mu})$ $= 1$ and $\mu \equiv 1 \pmod{2 + 2i}$. We therefore set

$$f_k(n;\mu) = \frac{1}{4}\Big|\sum_{\substack{N(\alpha)=n\\ \gcd(\alpha,\overline{\mu})=1}} \left(\frac{\alpha}{|\alpha|}\right)^{k}\Big|,$$

which differs from our previous function $f_h(n)$ only in the condition $\gcd(\alpha, \overline{\mu}) = 1$. It now follows that

$$\sum_{t^{1/2}\max(|u|,|v|)\le B^{1/2}} \Big| \sum_{\substack{x^2+y^2=t^2F(u,v)\\ \gcd(t,x,y)=1}} \Big(\frac{x+iy}{|x+iy|}\Big)^{4h} \Big| \le 4 \sum_{\substack{\gcd(\mu,\overline{\mu})=1\\ \mu\equiv 1 \,(\mathrm{mod}\, 2+2i)}} \sum_{\max(|u|,|v|)\le (B/N(\mu))^{1/2}} f_{4h}(F(u,v);\mu). \tag{3.1}$$

The inner sum above can now be bounded by an Erdős type estimate, a suitable version of which is given in the next lemma, which is an immediate consequence of de la Bretèche and Browning [3, Corollary 1].

LEMMA 3.1. *Let $F(u,v) \in \mathbb{Z}[u,v]$ be an irreducible binary form of degree $d \ge 2$, and let $f(n)$ be a multiplicative function satisfying $0 \le f(n) \le d(n)$ for all $n \in \mathbb{N}$. Then*

$$\sum_{\max(|u|,|v|)\le X} f(|F(u,v)|) \ll_F X^2 \prod_{d<p\le X} \Big(1 + \frac{\rho(p)(f(p)-1)}{p}\Big),$$

where

$$\rho(p) = \frac{1}{p-1}\#\{(u,v) \in (0,p]^2 : p \,|\, F(u,v),\ \gcd(u,v,p) = 1\}.$$

The reader should note that we have $d_1 = d_2 = 0$ and $F = G$ in the notation of [3]. We should also stress that the implied constant in Lemma 3.1 depends only on F, and is uniform over all functions f satisfying $0 \le f(n) \le d(n)$.

In our situation, $\rho(p)$ is the number of zeros modulo p of the polynomial $F(X,1)$ as long as $p > |F(1,0)|$. Since $\rho(p)$ and $f_{4h}(p;\mu)$ are absolutely bounded, we see that Lemma 3.1 yields

$$\sum_{\max(|u|,|v|)\le (B/N(\mu))^{1/2}} f_{4h}(F(u,v);\mu) \ll_F \frac{B}{N(\mu)} \exp\Big\{\sum_{2<p\le B} \frac{\rho(p)(f_{4h}(p;\mu)-1)}{p}\Big\}.$$

However,

$$\sum_{2<p\le B} \frac{\rho(p)(f_{4h}(p;\mu)-1)}{p} = \sum_{2<p\le B} \frac{\rho(p)(f_{4h}(p)-1)}{p} + O\Big(\sum_{p\mid N(\mu)} \frac{1}{p}\Big).$$

The error term is $O(\log\log\log N(\mu))$, by the argument used for (2.1), whence

$$\sum_{\max(|u|,|v|)\le (B/N(\mu))^{1/2}} f_{4h}(F(u,v);\mu) \ll_F \frac{B(\log\log N(\mu))^A}{N(\mu)} \exp\Big\{ \sum_{2<p\le B} \frac{\rho(p)(f_{4h}(p)-1)}{p} \Big\}$$

for a suitable constant A, so that (3.1) yields

$$\sum_{t^{1/2}\max(|u|,|v|)\le B^{1/2}} \Big| \sum_{\substack{x^2+y^2=t^2F(u,v)\\ \gcd(t,x,y)=1}} \Big(\frac{x+iy}{|x+iy|}\Big)^{4h} \Big| \ll_F B(\log\log B)^A(\log B)\exp\Big\{ \sum_{2<p\le B} \frac{\rho(p)(f_{4h}(p)-1)}{p} \Big\}.$$

We now apply the inequality (2.3) to estimate $f_{4h}(p)$ when $p\equiv 1 \pmod 4$, and deduce that

$$\sum_{t^{1/2}\max(|u|,|v|)\le B^{1/2}} \Big| \sum_{\substack{x^2+y^2=t^2F(u,v)\\ \gcd(t,x,y)=1}} \Big(\frac{x+iy}{|x+iy|}\Big)^{4h} \Big| \ll_F B(\log\log B)^A(\log B)\exp\big\{-S_1+\tfrac{3}{2}S_2+\tfrac{1}{4}S_3\big\} \tag{3.2}$$

with

$$S_1 = \sum_{2<p\le B} \frac{\rho(p)}{p},$$

$$S_2 = \sum_{\substack{2<p\le B\\ p\equiv 1 \pmod 4}} \frac{\rho(p)}{p},$$

$$S_3 = \sum_{2<p\le B} \frac{\rho(p)g_{8h}(p)}{p}.$$

We observed above that $\rho(p)$ is just the number of solutions of $F(X,1)$ modulo p, if p is large enough in terms of F. Indeed, if we write $K=\mathbb{Q}(\theta)$ where θ is a root of $F(X,1)$, we see from Dedekind's Theorem that $\rho(p)$ is the number of first degree prime ideals P of K above p, at least if p is large enough in terms of F. It follows that

$$S_1 = \sum_{2<N(P)\le B} \frac{1}{N(P)} + O_F(1),$$

since prime ideals of degree 2 or more contribute $O_F(1)$. The Prime Ideal

Theorem then shows that

$$S_1 = \log\log B + O_F(1). \tag{3.3}$$

In order to examine S_2 and S_3, we will consider the factorization of rational primes in the field $L = K(i)$. This must be a quadratic extension of K, since if $\mathbb{Q}(i) \subset K$ it would follow that θ is quadratic over $\mathbb{Q}(i)$, which is impossible since $F(X, 1)$ was assumed to be irreducible over $\mathbb{Q}(i)$. When $p \equiv 1 \pmod 4$ is a norm $N(\pi)$ over $\mathbb{Q}(i)$, one sees that each prime ideal P of K lying above p will split as $(P, \pi)(P, \overline{\pi})$ over L, so that $\rho(p)$ is half the number of first degree prime ideals of L lying over p. On the other hand, there cannot be a first degree prime ideal P of L lying above a rational prime $p \equiv 3 \pmod 4$, since then $N_{L/\mathbb{Q}(i)}(P)$ would be a first degree prime ideal of $\mathbb{Q}(i)$ above p, which is impossible. It follows that

$$S_2 = \frac{1}{2} \sum_{2<p\le B} \frac{\rho_L(p)}{p},$$

where $\rho_L(p)$ counts first degree primes of L above p. The Prime Ideal Theorem for L then yields

$$S_2 = \tfrac{1}{2}\log\log B + O_F(1). \tag{3.4}$$

To handle S_3 we define a non-trivial Hecke Grössencharacter on prime ideals of L by setting $\chi_h(P) = (\pi/|\pi|)^{4h}$ if $N_{L/\mathbb{Q}(i)}(P) = (\pi)$. With this definition, we have

$$\rho(p) g_{8h}(p) = \sum_{N_{L/\mathbb{Q}}(P)=p} \chi_{2h}(P).$$

In analogy with Lemma 2.2, we deduce from the Prime Ideal Theorem with Grössencharacter that

$$\sum_{N(A)\le x} \Lambda(A)\chi_h(A) \ll_F x \exp\left\{-c\frac{\log x}{\sqrt{\log x} + \log h}\right\} (\log xh)^4$$

uniformly for $x \ge 2$ and $k \in \mathbb{N}$, where A runs over non-zero integral ideals of L. Following a similar argument to that used in §2, we now deduce that

$$S_3 = \sum_{3\le p\le N} \frac{\rho(p) g_{8h}(p)}{p} \ll_F \log\log h.$$

We can now feed this estimate, along with (3.3) and (3.4), into (3.2) to deduce that

$$\sum_{t^{1/2}\max(|u|,|v|)\le B^{1/2}} \left| \sum_{\substack{x^2+y^2=t^2F(u,v)\\ \gcd(t,x,y)=1}} \left(\frac{x+iy}{|x+iy|}\right)^{4h} \right| \ll_F B(\log\log B)^A (\log h)^A (\log B)^{3/4},$$

for a suitable numerical constant A, and Lemma 1.4 follows.

References

[1] M. B. Barban and P. P. Vehov, *Summation of multiplicative functions of polynomials*, Mat. Zametki 5 (1969), 669–680 (in Russian).

[2] B. M. Bredikhin and Yu. V. Linnik, *Asymptotic behaviour and ergodic properties of solutions of the generalized Hardy–Littlewood equation*, Mat. Sb. (N.S.) 71 (113) (1966), 145–161 (in Russian).

[3] R. de la Bretèche and T. D. Browning, *Sums of arithmetic functions over values of binary forms*, Acta Arith. 125 (2006), 291–304.

[4] R. de la Bretèche et G. Tenenbaum, *Sur la conjecture de Manin pour certaines surfaces de Châtelet*, J. Inst. Math. Jussieu 12 (2013), 759–819.

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

[6] R. Holowinsky, *Sieving for mass equidistribution*, Ann. of Math. (2) 172 (2010), 1499–1516.

[7] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. 97 (1957), 189–210.

[8] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Math. 70, Cambridge Univ. Press, Cambridge, 1976.

[9] C. Hooley, *On the representation of a number as the sum of a prime and two squares of square-free numbers*, Acta Arith. 182 (2018), 201–229.

[10] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[11] Yu. V. Linnik, *All large numbers are sums of a prime and two squares (A problem of Hardy and Littlewood). I*, Mat. Sb. (N.S.) 52 (94) (1960), 661–700 (in Russian).

[12] Yu. V. Linnik, *All large numbers are sums of a prime and two squares (A problem of Hardy and Littlewood). II*, Mat. Sb. (N.S.) 53 (95) (1961), 3–38 (in Russian).

[13] P. Pollack, *Nonnegative multiplicative functions on sifted sets, and the square roots of* -1 *modulo shifted primes*, Glasgow Math. J. 62 (2020), 187–199.

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

D. R. Heath-Brown
Mathematical Institute
University of Oxford
Oxford, OX2 6GG, United Kingdom
E-mail: rhb@maths.ox.ac.uk