Acta Math., 202 (2009), 1–19
DOI: 10.1007/s11511-009-0033-z

Hyperbolic prime number theorem

by

John B. Friedlander
University of Toronto
Toronto, Ontario, Canada

Henryk Iwaniec
Rutgers University
Piscataway, NJ, U.S.A.

1. Introduction

The prime number theorem provides an asymptotic formula for the number of integer points m on the real line at a prime distance no more than x units from the origin, namely $\pi_1(x){\sim}2x/\log x$. The simplest case of the prime ideal theorem provides an asymptotic formula for the number of integer lattice points $m+ni$ in the complex plane at a prime norm (so distance squared) at most x units from the origin, namely $\pi_2(x){\sim}4x/\log x$.

By analogy, one can consider the number of prime vectors among integer lattice points in the 3-dimensional ball (or, for that matter, n-dimensional).

Theorem 1. *The number of integer points* (x_1, x_2, x_3) *with*

$$x_1^2+x_2^2+x_3^2=p\leqslant x$$

satisfies

$$\pi_3(x)\sim\frac{4\pi}{3}\frac{x^{3/2}}{\log x}.$$

Although the problem of counting the number of integer lattice points in the ball has a long history, see for example [CI], there seems to be no record of the corresponding theorem for primes. Hence, we provide the sketch of a proof in §2.

Our main concern however is an analogous problem for the hyperbolic plane. As a model of the hyperbolic plane we take the upper half-plane

$$\mathbb{H}=\{z=x+iy: x\in\mathbb{R} \text{ and } y\in\mathbb{R}^+\},$$

The first author is supported in part by NSERC grant A5123. The second author is supported in part by NSF grant DMS-03-01168.

which is acted on by the modular group

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} : x_1, x_2, x_3, x_4 \in \mathbb{Z} \text{ and } x_1x_4 - x_2x_3 = 1 \right\},$$

by fractional linear transformations. As a distance function on $\mathbb{H}$, we choose

$$u(z,w) = \frac{|z-w|^2}{\operatorname{Im} z \operatorname{Im} w},$$

and, as the origin, we choose $z=i$. As "integers" we choose the orbit $\{\gamma i : \gamma \in \Gamma\}$. We wish to count the number of points γi at a distance $p-2$ from the origin, with $p \leqslant x$. Let us denote this number by $\pi_\Gamma(x)$.

The number of all points γi within this disc is given asymptotically (see [I2]) by

$$N_\Gamma(x) = 8x + O(x^{2/3}). \tag{1.1}$$

We expect that $\pi_\Gamma(x)$ satisfies the asymptotic formula

$$\pi_\Gamma(x) \sim \frac{cx}{\log x}, \tag{1.2}$$

where

$$c = 16 \prod_p \left(1 + \frac{2\chi(p)}{(p+1)(p+\chi(p))}\right). \tag{1.3}$$

Here, and throughout the paper, $\chi = \chi_4$ is the non-principal character of modulus 4.

In this paper we are able to show that this order of magnitude is correct, that is

$$\frac{c_1 x}{\log x} < \pi_\Gamma(x) < \frac{c_2 x}{\log x}, \tag{1.4}$$

for suitable positive constants c_1 and c_2, and all large x, subject to a standard conjecture concerning the distribution of rational primes in arithmetic progressions.

Let $\Lambda(n)$ denote the usual von Mangoldt function and

$$\psi(x;q,a) = \sum_{\substack{n \leqslant x \\ n \equiv a \pmod q}} \Lambda(n).$$

The expected main term for $\psi(x;q,a)$, when a and q are coprime, is $x/\varphi(q)$, so we define the "remainder term"

$$E(x;q,a) = \psi(x;q,a) - \frac{x}{\varphi(q)}, \tag{1.5}$$

and the "remainder of level Q"

$$E(x,Q) = \sum_{q \leqslant Q} \max_{(a,q)=1} \max_{y \leqslant x} |E(y;q,a)|. \tag{1.6}$$

We introduce, for $0 < \theta \leqslant 1$, the following assumption.

Assumption $A(\theta)$. The bound

$$E(x,Q) \ll x(\log x)^{-A}$$

holds for $Q=x^{\theta-\varepsilon}$, for every $\varepsilon>0$ and $A>0$, with an implied constant that depends only on ε and A.

We remark that $A\left(\frac{1}{2}\right)$ is known to be true, the famous Bombieri–Vinogradov theorem, and that the expectation that $A(1)$ holds is also well-known, as the conjecture of Elliott and Halberstam.

Our main result is the following.

THEOREM 2. *If* $A(\theta)$ *holds for some* θ, *less than* 1 *but sufficiently close to* 1, *then there are positive constants* c_1 *and* c_2 *such that*

$$\frac{c_1 x}{\log x} < \pi_\Gamma(x) < \frac{c_2 x}{\log x} \tag{1.7}$$

for all $x \geqslant 2$.

As is customary, we denote this relationship by $\pi_\Gamma(x) \asymp x/\log x$. Actually, the upper bound is unconditional and an easy consequence of the sieve (well, the Riemann hypothesis for curves is indirectly involved).

We stress that we do not need to assume $A(\theta)$ for $\theta=1$. Conceivably, one could get the asymptotics with the aid of this stronger assumption. The method allows for the determination of an admissible value for θ but we did not carry this out. We actually need a considerably weaker form of the conjecture and some results in this direction have been provided by Fouvry [Fo], and by Bombieri, Friedlander and Iwaniec [BFI].

We can re-state our problem explicitly in terms of the coordinates x_1, x_2, x_3 and x_4. We have

$$u(\gamma i, i)+2 = x_1^2+x_2^2+x_3^2+x_4^2; \tag{1.8}$$

therefore, we are looking for prime numbers

$$p = x_1^2+x_2^2+x_3^2+x_4^2 \tag{1.9}$$

with x_1, x_2, x_3 and x_4 satisfying the determinant equation

$$x_1x_4 - x_2x_3 = 1. \tag{1.10}$$

Thus, an equivalent formulation of our main theorem is the following.

Theorem 3. *Under the same assumption as Theorem* 2, *we have*

$$\sum_{\substack{x_1^2+x_2^2+x_3^2+x_4^2\leqslant x\\ x_1x_4-x_2x_3=1}} \Lambda(x_1^2+x_2^2+x_3^2+x_4^2)\asymp x. \tag{1.11}$$

It is because of the interpretation of our main result, given by (1.8) and (1.9), that it seems more natural to consider points at a distance $p-2$ rather than those at prime distance, even though it makes the problem sound a little more like the twin prime question than the prime number theorem. We shall have more to say about the points at distance p toward the end of this section.

A more general problem in which the quadratic form (1.9) is replaced by a polynomial in four variables has been considered recently by Bourgain, Gamburd and Sarnak in [BGS]. Actually, they consider a still more general situation for a system of polynomials in many variables and with GL_n in place of GL_2, a setting in which they succeeded in producing almost-primes. We were motivated to look at the problem (1.11) because of their work.

We can reinterpret the system

$$\begin{cases} x_1^2+x_2^2+x_3^2+x_4^2=n,\\ x_1x_4-x_2x_3=1,\end{cases} \tag{1.12}$$

as the system

$$\begin{cases} y_1^2+y_2^2=n+2,\\ (y_1^2+y_2^2)-(y_3^2+y_4^2)=4,\end{cases} \tag{1.13}$$

by making the linear transformation $(x_1,x_2,x_3,x_4)\mapsto(y_1,y_2,y_3,y_4)$, where

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

The inverse is given by

$$\begin{cases} x_1=\frac12(y_1+y_3),\\ x_2=\frac12(y_2+y_4),\\ x_3=\frac12(y_2-y_4),\\ x_4=\frac12(y_1-y_3).\end{cases}$$

These provide a one-to-one correspondence as real numbers. Assume now that n is an odd integer. If x_1, x_2, x_3 and x_4 are integers, then so are y_1, y_2, y_3 and y_4. Conversely, given y_1, y_2, y_3, y_4, we learn from the first equation in (1.13) that y_1 and y_2 have opposite parity, and then we learn from the second equation that so do y_3 and y_4. Hence, given a pair of integer solutions (y_1, y_2, y_3, y_4) and (y_1, y_2, y_4, y_3), precisely one of them gives rise to an integer solution in the x's. Therefore, the number of integer solutions in the x's is equal to one half of the number of integer solutions in the y's.

(On the other hand, if n is even, then automatically y_1 and y_2 have the same parity as do y_3 and y_4, so the correspondence between x's and y's is one-to-one.)

Denote by $r(m)$, as is customary, the number of representations of m as the sum of two squares. From the above discussion it follows that the number of solutions to the system (1.12), for n odd, is just

$$\tfrac{1}{2} r(n-2) r(n+2). \tag{1.14}$$

Hence, the statement of our main theorem now becomes the following.

THEOREM 4. *Under the same assumption as Theorem* 2, *we have*

$$S(x) = \sum_{n \leqslant x} r(n-2) r(n+2) \Lambda(n) \asymp x. \tag{1.15}$$

It is in this form that we shall give the proof. Here too, we can note the similarity of the formula (1.15) to the twin prime conjecture. See the remarks at the end of the proof.

If we consider prime distances, rather than those of the form $p-2$, by the above argument, the problem translates into an evaluation of the sum

$$T(x) = \sum_{n \leqslant x} r(n-2) r(n+2) \Lambda(n+2). \tag{1.16}$$

Since $r(p)=8$ if $p \equiv 1 \pmod 4$, and $r(p)=0$ if $p \equiv 3 \pmod 4$, this becomes

$$T(x) = \sum_{p \leqslant x} r(p-4) \log p + O(\sqrt{x}\,), \tag{1.17}$$

which, using [BFI, Theorem 9], we shall directly and unconditionally evaluate in §3, getting the following result.

THEOREM 5. *We have*

$$T(x) = \pi x \prod_{p} \left(1 + \frac{\chi(p)}{p(p-1)} \right) + O(x (\log x)^{-A}),$$

for any $A > 0$, with an implied constant depending on A.

2. Primes in the 3-ball

In this section we sketch the proof of Theorem 1. See, for example [CI], for background material.

We have

$$\pi_3(x)=\sum_{p\leqslant x} r_3(p),$$

where $r_3(n)$ denotes the number of representations of n as the sum of three squares. By Gauss' formula, for $p>2$,

$$r_3(p)=\frac{c_p}{\pi}\sqrt{p}\,L(1,\chi_p), \tag{2.1}$$

where

$$c_p=\begin{cases} 24, & \text{if } p\equiv 1 \pmod 4,\\ 16, & \text{if } p\equiv 3 \pmod 8,\\ 0, & \text{if } p\equiv 7 \pmod 8.\end{cases}$$

The L-function is that which accompanies the Kronecker symbol

$$\chi_p(n)=\left(\frac{-4p}{n}\right).$$

Using (2.1), we have

$$\pi_3(x)=\frac{1}{\pi}\sum_{p\leqslant x} c_p\sqrt{p}\,L(1,\chi_p). \tag{2.2}$$

Here, we open the L-series and truncate it to

$$\sum_{n\leqslant N}\left(\frac{-4p}{n}\right),$$

where $N=(\log x)^A$. The error term so made is acceptable, due to the inequality

$$\sum_{P<p\leqslant 2P}\Bigg|\sum_{N<n\leqslant 2N}\left(\frac{-4p}{n}\right)\Bigg|\ll PN^{3/4}(\log N)^2,$$

which follows by a direct application of Cauchy's inequality, the Pólya–Vinogradov inequality and quadratic reciprocity (see for example [He]).

Given $n\leqslant N$, we sum over p, getting, by the Siegel–Walfisz theorem (see for example [IK, Corollary 5.29]), for any $A>0$,

$$\sum_{p\leqslant x} c_p\sqrt{p}\left(\frac{-4p}{n}\right)=s(n)\sum_{p\leqslant x} c_p\sqrt{p}+O(x^{3/2}(\log x)^{-A}), \tag{2.3}$$

where $s(n)=1$ if n is the square of an odd integer and is zero otherwise. Here,

$$\sum_{p\leqslant x} c_p\sqrt{p}\sim \frac{32}{3}\frac{x^{3/2}}{\log x}$$

and

$$\sum_{n\leqslant N}\frac{s(n)}{n}\sim\frac{\pi^2}{8}.$$

Putting these together, we complete the proof of Theorem 1.

3. Hyperbolic prime distance theorem

We give here a sketch of the proof of Theorem 5. For $m\equiv 1 \pmod 4$ we have

$$r(m)=8\sum_{\substack{kl=m\\ k<\sqrt{m}}}\chi(k)+4\chi(\sqrt{m}\,), \tag{3.1}$$

where we adopt the convention that the last term vanishes in case m is not a square. Hence

$$T(x)=\sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod 4}} r(p-4)\log p+O(\sqrt{x}\,)=8\sum_{k\leqslant\sqrt{x}}\chi(k)\sum_{\substack{k^2<p\leqslant x\\ p\equiv 1 \pmod 4\\ p\equiv 4 \pmod k}}\log p+O(\sqrt{x}\,).$$

Estimating the inner sum with the aid of [BFI, Theorem 9], we obtain

$$T(x)=8\sum_{k\leqslant\sqrt{x}}\chi(k)\frac{x-k^2}{\varphi(4k)}+O(x(\log x)^{-A})=4x\sum_{k=1}^{\infty}\frac{\chi(k)}{\varphi(k)}+O(x(\log x)^{-A}).$$

Here we have

$$\sum_{k=1}^{\infty}\frac{\chi(k)}{\varphi(k)}=\prod_p\left(1+\frac{\chi(p)}{p-1}\left(1-\frac{\chi(p)}{p}\right)^{-1}\right)=L(1,\chi)\prod_p\left(1+\frac{\chi(p)}{p(p-1)}\right),$$

and $L(1,\chi)=\frac{1}{4}\pi$ (remember that $\chi=\chi_4$), completing the proof of the theorem.

4. Properties of $r(m)$

We need results about the distribution of the function $r(m)$ over arithmetic progressions in a wide range of moduli. If one uses the formula

$$r(m)=4\sum_{d\mid m}\chi(d), \tag{4.1}$$

where as before $\chi=\chi_4$, then not surprisingly one controls the error term by means of Kloosterman sums. The Weil bound for these, produces results more than sufficient for our needs. We refer to the result of Smith [S1], [S2]; see also [IK].

Lemma 4.1. *Let* $(a,q)=1$. *Then*

$$\sum_{\substack{m\leqslant x\\ m\equiv a \pmod q}} r(m)=\frac{\pi x}{q}\prod_{p|q}\left(1-\frac{\chi(p)}{p}\right)+O(q^{-1/2}x^{2/3+\varepsilon}) \tag{4.2}$$

when $q\not\equiv 0 \pmod 4$ *and the main term is multiplied by* $1+\chi(a)$ *when* $q\equiv 0 \pmod 4$.

Note that this gives the asymptotic within the range $q<x^{2/3-\varepsilon}$.

We also need a bound for the shifted convolution of r against itself.

Lemma 4.2. *We have, for d odd,*

$$\sum_{\substack{n\leqslant x\\ n\equiv 3 \pmod 4\\ n\equiv 0 \pmod d}} r(n-2)r(n+2)=g(d)8x+O(x^{11/12+\varepsilon}), \tag{4.3}$$

where

$$g(d)=\frac{1}{d}\prod_{p|d}\frac{p-\chi(p)}{p+\chi(p)}, \tag{4.4}$$

and the implied constant depends only on ε.

Note that (4.3) accounts for all odd n since, for $n\equiv 1 \pmod 4$, both of $r(n\pm 2)$ vanish.

Remark. The result in Lemma 4.2 solves the lattice point problem in the hyperbolic plane with respect to a congruence group. The spectral theory produces a very good error term for this, namely $O(x^{2/3})$, see [I2]. However, we need a wide range of uniformity in d, which is easier to obtain using Lemma 4.1.

Proof of Lemma 4.2. Since, for $m\equiv 1 \pmod 4$,

$$r(m)=8\sum_{\substack{kl=m\\ k<\sqrt{m}}}\chi(k)+4\chi(\sqrt{m}\,), \tag{4.5}$$

we have

$$\sum_{\substack{n\leqslant x\\ n\equiv 3 \pmod 4\\ n\equiv 0 \pmod d}} r(n-2)r(n+2)=8\sum_k\sum_n+O(x^{1/2+\varepsilon}),$$

where

$$\begin{aligned}\sum_k\sum_n &= \sum_{\substack{k<\sqrt{x}\\(k,d)=1}}\chi(k)\sum_{\substack{k^2<n\leqslant x\\ n\equiv 3 \ (\mathrm{mod}\, 4)\\ n\equiv 0 \ (\mathrm{mod}\, d)\\ n\equiv 2 \ (\mathrm{mod}\, k)}} r(n+2)\\
&= 2\pi\sum_{\substack{k<\sqrt{x}\\(k,d)=1}}\chi(k)\biggl(\frac{x-k^2}{4dk}\prod_{p\mid dk}\Bigl(1-\frac{\chi(p)}{p}\Bigr)+O((dk)^{-1/2}x^{2/3+\varepsilon})\biggr)\\
&= \frac{\pi x}{2d}\prod_{p\mid d}\Bigl(1-\frac{\chi(p)}{p}\Bigr)\sum_{(k,d)=1}\frac{\chi(k)}{k}\prod_{p\mid k}\Bigl(1-\frac{\chi(p)}{p}\Bigr)+O(x^{11/12+\varepsilon})\\
&= \frac{x}{d}\prod_{p\mid d}\Bigl(1-\frac{\chi(p)}{p}\Bigr)\Bigl(1+\frac{\chi(p)}{p}\Bigr)^{-1}+O(x^{11/12+\varepsilon}),\end{aligned}$$

giving Lemma 4.2. □

We also need an asymptotic formula for a shifted convolution of r with the von Mangoldt function. In this case we shall leave the remainder term untreated for the time being.

Lemma 4.3. *Let* $(a,q)=1$, $q\equiv 0 \ (\mathrm{mod}\, 4)$, *and* $a\equiv 3 \ (\mathrm{mod}\, 4)$. *Then we have*

$$\sum_{\substack{n\leqslant x\\ n\equiv a \ (\mathrm{mod}\, q)}} r(n+2)\Lambda(n) = \frac{Hx}{\varphi(q)}\prod_{p\mid q}\Bigl(1+\frac{\chi(p)}{p(p-1)}\Bigr)^{-1}+O\biggl(\sum_{k\leqslant\sqrt{x}}E_{\max}(x,qk)+\sqrt{x}\,\log x\biggr),$$

where

$$H=2\pi\prod_p\Bigl(1+\frac{\chi(p)}{p(p-1)}\Bigr)\quad and\quad E_{\max}(x,q)=\max_{(a,q)=1}\max_{y\leqslant x}|E(y;q,a)|,$$

the latter quantity being as defined in (1.5).

Proof. Using (4.5) we obtain

$$\begin{aligned}\sum_{\substack{n\leqslant x\\ n\equiv a \ (\mathrm{mod}\, q)}} r(n+2)\Lambda(n) &= 8\sum_{k\leqslant\sqrt{x}}\chi(k)\sum_{\substack{k^2<n\leqslant x\\ n\equiv a \ (\mathrm{mod}\, q)\\ n\equiv -2 \ (\mathrm{mod}\, k)}}\Lambda(n)+O(\sqrt{x}\,\log x)\\
&= 8\sum_{k\leqslant\sqrt{x}}\chi(k)\biggl(\frac{x-k^2}{\varphi(kq)}+O(E_{\max}(x,qk))\biggr)+O(\sqrt{x}\,\log x)\\
&= \frac{8x}{\varphi(q)}\sum_{k\geqslant 1}\frac{\chi(k)}{k}\prod_{\substack{p\mid k\\ p\nmid q}}\Bigl(1-\frac{1}{p}\Bigr)^{-1}+O\biggl(\sum_{k\leqslant\sqrt{x}}E_{\max}(x,qk)+\sqrt{x}\,\log x\biggr),\end{aligned}$$

giving the lemma. □

5. The upper bound

In this section we prove the upper bound of Theorem 4 and hence of Theorems 2 and 3. This is a linear sieve problem for the sequence $\mathcal{A}=\{a_n\}_n$ with $a_n=r(n-2)r(n+2)$.

We have already shown in Lemma 4.2 that this sequence has a level of distribution $D=D(x)=x^{1/12-2\varepsilon}$; therefore any upper bound sieve, such as Brun's, yields the result.

6. Preliminaries for the lower bound

Our goal is to show that

$$S(x)\gg x.$$

We are going to use the semilinear sieve and hence it will be convenient to replace the function r in one factor by b, the characteristic function of such integers. Define $b(n)=1$ if all prime factors of n are congruent to 1 (mod 4) and zero otherwise (so that $b(n)=1$ if and only if n is an odd number which has a primitive representation as the sum of two squares). Note that b is totally multiplicative.

In case $b(n)\neq 0$ then $\chi(d)=1$ for every $d|n$. Thus, for every positive integer m we have, by (4.1),

$$r(m)\geqslant 4b(m)\tau(m). \tag{6.1}$$

Hence

$$S(x)\geqslant 4\sum_{n\leqslant x} b(n-2)\tau(n-2)r(n+2)\Lambda(n)\geqslant 4\sum_{\delta\leqslant\Delta} b(\delta)\sum_{\substack{n\leqslant x\\ n\equiv 2\ (\mathrm{mod}\ \delta)}} b(n-2)r(n+2)\Lambda(n) \tag{6.2}$$

for any $\Delta=\Delta(x)$, which will be chosen to be relatively small, $\Delta=x^{\vartheta}$.

We detect the factor $b(n-2)$ by the semilinear sieve with respect to the set

$$\mathcal{P}=\{p\equiv 3\ (\mathrm{mod}\ 4)\}.$$

To this end we consider the sifting sequence

$$\mathcal{A}^{(\delta)}=\{a_n\}_n,\quad a_n=r(n+4)\Lambda(n+2)$$

for $n\leqslant x-2$, $n\equiv 1$ (mod 4), $n\equiv 0$ (mod δ), and so

$$\sum_{\substack{n\leqslant x\\ n\equiv 2\ (\mathrm{mod}\ \delta)}} b(n-2)r(n+2)\Lambda(n)=S(\mathcal{A}^{(\delta)},\mathcal{P},\sqrt{x}\,), \tag{6.3}$$

where, in the usual sieve notation, this is the sum of the a_n in $\mathcal{A}^{(\delta)}$ over those n having no prime factor in $\mathcal{P}$ up to $\sqrt{x}$. Here $\sqrt{x}$ suffices because, if $n\equiv 1 \pmod 4$ has one prime factor from $\mathcal{P}$, it must have a second one.

We are going to apply the lower bound semilinear sieve to the sequence $\mathcal{A}^{(\delta)}$ for every $\delta\leqslant\Delta$. To this end we need to verify approximations of the type

$$\mathcal{A}_d^{(\delta)}(x) = g(d)X^{(\delta)} + r_d(x), \tag{6.4}$$

for d squarefree and having all prime factors congruent to 3 (mod 4). Note that this implies that $(d, 2\delta)=1$. Lemma 4.3, with $q=4\delta d$, provides such an approximation where

$$X^{(\delta)} = \frac{Hx}{2\varphi(\delta)} \prod_{p|\delta} \left(1 + \frac{1}{p(p-1)}\right)^{-1} \tag{6.5}$$

and

$$g(d) = \frac{1}{\varphi(d)} \prod_{p|d} \left(1 - \frac{1}{p(p-1)}\right)^{-1}. \tag{6.6}$$

The remainder term in (6.4) satisfies, by Lemma 4.3,

$$r_d(x) \ll \sum_{k\leqslant\sqrt{x}} E_{\max}(x, 4\delta dk) + \sqrt{x}\,\log x. \tag{6.7}$$

The function $g(d)$ in (6.6) is a linear sieve density, but we shall be sifting by only half of the primes, so this becomes a semilinear sieve problem, see [I1]. Since the sieving limit for the semilinear sieve is $\beta=1$ and our level of distribution is $D=D(x)<\sqrt{x}$, we cannot successfully apply the lower bound sieve to $S(\mathcal{A}^{(\delta)}, \mathcal{P}, \sqrt{x}\,)$, but we can come close to this.

Let $z=D^{1/s}$ with $1<s<3$. Then we have (see (B.2) in Appendix B)

$$S(\mathcal{A}^{(\delta)}, \mathcal{P}, z) \geqslant X^{(\delta)} V(z)(f(s)+o(1)) - R_\delta(x) \geqslant c\frac{x}{\delta\sqrt{\log x}}(\sqrt{s-1}+o(1)) - R_\delta(x), \tag{6.8}$$

where c is a positive absolute constant and

$$R_\delta(x) = \sum_{k\leqslant\sqrt{x}} \sum_{d\leqslant D} E_{\max}(x, 4\delta dk). \tag{6.9}$$

We shall choose

$$D = D(x) = x^{\theta-1/2-\vartheta-\varepsilon}, \tag{6.10}$$

so that the modulus $4\delta dk$ in (6.9) does not exceed $4x^{\theta-\varepsilon}$.

7. Reinterpreting the sieve problem

In order to turn our lower bound (6.8) into a lower bound for the sum in (6.3), it remains to estimate the difference

$$T(\mathcal{A}^{(\delta)},\mathcal{P},z)=S(\mathcal{A}^{(\delta)},\mathcal{P},z)-S(\mathcal{A}^{(\delta)},\mathcal{P},\sqrt{x}\,),$$

and, for the purpose of utilizing (6.2), we are only required to do this on average over δ.

We behave as if $\theta<1$ is quite close to 1 and ϑ is very small, so the level of distribution $D=D(x)$ of $\mathcal{A}^{(\delta)}$ is only slightly smaller than $\sqrt{x}$ and is in particular greater than $x^{1/3}$. Assuming that $1<s\leqslant\frac{4}{3}$, we have $z=D^{1/s}>x^{1/4}$; therefore $T(\mathcal{A}^{(\delta)},\mathcal{P},z)$ counts only integers having two prime factors in $\mathcal{P}$. Thus

$$T(\mathcal{A}^{(\delta)},\mathcal{P},z)=\sum_{\substack{n\leqslant x+2\\ n\equiv1\ (\mathrm{mod}\,4)\\ n\equiv4\ (\mathrm{mod}\,\delta p_1p_2)\\ z\leqslant p_1<p_2\\ p_1,p_2\in\mathcal{P}}} r(n)\Lambda(n-2).$$

We are looking for an upper bound and so can ignore some constraints. We reinterpret the congruence $n\equiv4\ (\mathrm{mod}\,\delta p_1p_2)$ as the equation

$$n=4+\delta ap_1p_2,$$

so that a runs through integers

$$a\leqslant\frac{x}{\delta z^2}\leqslant\frac{x}{z^2},$$

with a having only prime factors $\equiv1\ (\mathrm{mod}\,4)$.

We record the fact that $z<p_1\leqslant\sqrt{x}$ and, having done that, we ignore the conditions for the prime p_2 and replace it by way of an upper bound linear sieve

$$\sum_{\substack{\nu_2\mid q_2\\ \nu_2\leqslant x^{1/60}}}\lambda_{\nu_2},$$

where $q_2=(n-4)/\delta ap_1$. Similarly, we relax $\Lambda(n-2)$, majorizing it by

$$\Lambda(n-2)\leqslant(\log x)\sum_{\substack{\nu\mid n-2\\ \nu\leqslant x^{1/60}}}\lambda_\nu.$$

As a result, we obtain

$$T(\mathcal{A}^{(\delta)},\mathcal{P},z)\leqslant(\log x)\sum_{a\leqslant xz^{-2}}b(a)\sum_{\substack{z<p_1\leqslant\sqrt{x}\\ p_1\equiv3\ (\mathrm{mod}\,4)}}\sum_{\substack{\nu,\nu_2\leqslant x^{1/60}\\ 2\nmid\nu\nu_2\\ (\nu,\delta a\nu_2)=1}}\sum\lambda_\nu\lambda_{\nu_2}\sum_{\substack{n\leqslant x+2\\ n\equiv1\ (\mathrm{mod}\,4)\\ n\equiv2\ (\mathrm{mod}\,\nu)\\ n\equiv4\ (\mathrm{mod}\,\delta ap_1\nu_2)}} r(n).$$

At this point we cannot apply crude estimates because we cannot afford to lose the sign changes in λ_ν and λ_{ν_2}. Therefore, we apply Lemma 4.1 to the inner sum above, getting

$$\sum_n r(n) = \frac{\pi x}{4\nu\delta a p_1 \nu_2} \prod_{p\mid\delta a\nu\nu_2} \left(1 - \frac{\chi(p)}{p}\right) + O(z^{-1/2} x^{2/3+\varepsilon}).$$

Hence,

$$T(\mathcal{A}^{(\delta)}, \mathcal{P}, z) \ll \frac{x\log x}{\delta} \prod_{p\mid\delta}\left(1-\frac{1}{p}\right)\left(\sum_{z<p_1<\sqrt{x}} \frac{1}{p_1}\right) \\ \times \sum_{a\leqslant xz^{-2}} \frac{b(a)}{a} \left| \mathop{\sum\sum}_{\substack{\nu,\nu_2\leqslant x^{1/60}\\ 2\nmid\nu\nu_2\\ (\nu,\delta a\nu_2)=1}} \frac{\lambda_\nu\lambda_{\nu_2}}{\nu\nu_2} \prod_{\substack{p\mid\nu\nu_2\\ p\nmid\delta a}} \left(1-\frac{\chi(p)}{p}\right)\right| + z^{-5/2}x^{11/5+\varepsilon}.$$

Here, for the sum over ν and ν_2, we apply Theorem A.5 from Appendix A, getting

$$\sum_{\nu,\nu_2} \ll \frac{\delta a}{\varphi(\delta a)} (\log x)^{-2}.$$

Hence,

$$T(\mathcal{A}^{(\delta)}, \mathcal{P}, z) \ll \frac{x}{\delta\log x} \log\left(\frac{\log\sqrt{x}}{\log z}\right) \sqrt{\log\frac{x}{z^2}} + z^{-5/2}x^{11/5+\varepsilon}.$$

For $z = D^{1/s} = x^{(\theta-1/2-\vartheta-\varepsilon)/s}$ the above estimation simplifies to

$$T(\mathcal{A}^{(\delta)}, \mathcal{P}, z) \ll \frac{x}{\delta\sqrt{\log x}} \left(1 - \frac{2}{s}\left(\theta - \frac{1}{2} - \vartheta - \varepsilon\right)\right)^{3/2}. \tag{7.1}$$

We want the upper bound (7.1) to be small compared to the lower bound (6.8). This is possible because when $\theta<1$ is near 1 and ϑ is even closer to zero, then the above factor behaves like $(s-1)^{3/2}$ which tends to zero faster than $\sqrt{s-1}$. Specifically, we choose $\vartheta = \frac{1}{2}(1-\theta)$ and $s = 2-\theta$ so that

$$\left(1 - \frac{2}{s}\left(\theta - \frac{1}{2} - \vartheta - \varepsilon\right)\right)^{3/2} < 8(1-\theta)^{3/2},$$

while $\sqrt{s-1} = \sqrt{1-\theta}$. Subtracting (7.1) from (6.8), we get

$$S(\mathcal{A}^{(\delta)}, \mathcal{P}, \sqrt{x}) \geqslant \frac{cx\sqrt{1-\theta}}{2\delta\sqrt{\log x}} - R_\delta(x).$$

Now, summing over δ, we conclude from (6.2) that $S(x) \gg x$ subject to the condition $\mathcal{A}(\theta)$.

Note that we actually require $\mathcal{A}(\theta)$ for the sum weighted by a divisor function, but this extra factor can be handled by an application of Cauchy's inequality. This completes the proof of our main Theorem 4.

As remarked earlier, the sum

$$S(x)=\sum_{n\leqslant x} r(n-2)r(n+2)\Lambda(n)$$

bears some resemblance to the twin prime sum

$$\sum_{n\leqslant x}\Lambda(n)\Lambda(n+2),$$

not just superficially but also from a sieve-theoretic viewpoint. The latter counts survivors of two linear sieves, while the former counts survivors of one linear and two semi-linear sieves. The assumption of the full conjecture $A(1)$ narrowly misses resolving the twin prime conjecture, see [Bo], whereas the extra flexibility in the sum $S(x)$ allows us to succeed, even with the weaker assumption.

Appendix A. Reduced composition of sieves

Let $\Lambda=\{\lambda_d\}_d$ be a finite sequence supported on squarefree numbers. Let $g(d)$ be a multiplicative function supported on a finite set of squarefree numbers with

$$0\leqslant g(p)<1. \tag{A.1}$$

Consider the sum

$$G=\sum_d \lambda_d g(d). \tag{A.2}$$

We shall express this in terms of the sequence

$$\varrho=1*\lambda. \tag{A.3}$$

Lemma A.1. *We have*

$$G=VG^*, \tag{A.4}$$

where

$$V=\prod_p (1-g(p)), \tag{A.5}$$

$$G^*=\sum_d \varrho_d h(d) \tag{A.6}$$

and $h(d)$ is the multiplicative function supported on squarefree numbers with

$$h(p)=\frac{g(p)}{1-g(p)}. \tag{A.7}$$

Proof. By Möbius inversion,

$$\lambda = \mu * \varrho. \tag{A.8}$$

Hence

$$G = \sum_a \sum_b \mu(a) \varrho_b g(ab) = \sum_b \varrho_b g(b) \prod_{p \nmid b} (1 - g(p)) = VG^*. \qquad \square$$

Next, we consider the double sum for a pair of such sequences

$$G' * G'' = \sum\sum_{(d_1, d_2) = 1} \lambda'_{d_1} \lambda''_{d_2} g'(d_1) g''(d_2). \tag{A.9}$$

LEMMA A.2. *We have*

$$G' * G'' = \sum\sum_{(b_1, b_2) = 1} \varrho'_{b_1} \varrho''_{b_2} g'(b_1) g''(b_2) \prod_{p \nmid b_1 b_2} (1 - g'(p) - g''(p)). \tag{A.10}$$

Proof. Using (A.8), we get

$$\begin{aligned} G' * G'' &= \sum\sum\sum\sum_{(a_1 b_1, a_2 b_2) = 1} \mu(a_1 a_2) \varrho'_{b_1} \varrho''_{b_2} g'(a_1 b_1) g''(a_2 b_2) \\ &= \sum\sum_{(b_1, b_2) = 1} \varrho'_{b_1} \varrho''_{b_2} g'(b_1) g''(b_2) W(b_1 b_2), \end{aligned}$$

where

$$\begin{aligned} W(b) &= \sum\sum_{(a_1 a_2, b) = 1} \mu(a_1 a_2) g'(a_1) g''(a_2) \\ &= \sum_{(a_1, b) = 1} \mu(a_1) g'(a_1) \prod_{p \nmid a_1 b} (1 - g''(p)) \\ &= \prod_{p \nmid b} (1 - g''(p)) \sum_{(a_1, b) = 1} \mu(a_1) g'(a_1) \prod_{p \mid a_1} \frac{1}{1 - g''(p)} \\ &= \prod_{p \nmid b} (1 - g''(p)) \prod_{p \nmid b} \left(1 - \frac{g'(p)}{1 - g''(p)}\right) = \prod_{p \nmid b} (1 - g'(p) - g''(p)). \end{aligned}$$

This completes the proof. $\square$

Note that, at every p, we have

$$1 - g' - g'' = (1 - g')(1 - g'')(1 - h'h''), \tag{A.11}$$

where $h' = g'(1 - g')^{-1}$ and $h'' = g''(1 - g'')^{-1}$; see (A.7). By $|1 - h'h''| \leqslant 1 + h'h''$, we get

$$|W(b)| \leqslant \prod_{p \nmid b} (1 - g'(p))(1 - g''(p))(1 + h'h''(p)).$$

Hence,

$$|W(b)| \leqslant CV'V'' \prod_{p|b} \frac{1}{(1-g'(p))(1-g''(p))}, \tag{A.12}$$

where

$$C = \prod_p (1+h'h''(p)), \tag{A.13}$$

$$V' = \prod_p (1-g'(p)) \quad \text{and} \quad V'' = \prod_p (1-g''(p)). \tag{A.14}$$

Inserting (A.12) into (A.10) and dropping the condition $(b_1, b_2)=1$, we obtain the following result.

Corollary A.3. *We have*

$$|G' * G''| \leqslant CV'V'' G_{12}^* G_{21}^*, \tag{A.15}$$

where

$$G_{12}^* = \sum_b |\varrho_b'| h_{12}(b) \quad \textit{and} \quad G_{21}^* = \sum_b |\varrho_b''| h_{21}(b), \tag{A.16}$$

and $h_{12}(b)$ *and* $h_{21}(b)$ *are the multiplicative functions supported on squarefree numbers such that*

$$h_{12}(p) = \frac{g'(p)}{(1-g'(p))(1-g''(p))} \quad \textit{and} \quad h_{21}(p) = \frac{g''(p)}{(1-g'(p))(1-g''(p))}. \tag{A.17}$$

Now assume that (λ') and (λ'') are upper-bound sieves, that is $\varrho' \geqslant 0$ and $\varrho'' \geqslant 0$, hence the absolute values in (A.16) are redundant. Define the corresponding multiplicative functions g_{12} and g_{21} by the formula (A.7), so we have (at primes)

$$g_{12} = \frac{h_{12}}{1+h_{12}} \quad \text{and} \quad g_{21} = \frac{h_{21}}{1+h_{21}}. \tag{A.18}$$

Using (A.17), these are (at primes)

$$g_{12} = \frac{g'}{1-g''(1-g')} \quad \text{and} \quad g_{21} = \frac{g''}{1-g'(1-g'')}. \tag{A.19}$$

By Lemma A.1, we get

$$V_{12} G_{12}^* = G_{12} = \sum_d \lambda_d' g_{12}(d) \quad \text{and} \quad V_{21} G_{21}^* = G_{21} = \sum_d \lambda_d'' g_{21}(d), \tag{A.20}$$

where

$$V_{12} = \prod_p (1-g_{12}(p)) \quad \text{and} \quad V_{21} = \prod_p (1-g_{21}(p)). \tag{A.21}$$

Inserting (A.20) into (A.15), we get the following result.

PROPOSITION A.4. *Let $\{\lambda'\}$ and $\{\lambda''\}$ be upper-bound sieves, and let g' and g'' be density functions. We have*

$$|G' * G''| \leqslant BCG_{12}G_{21}, \tag{A.22}$$

where

$$B = \frac{V'V''}{V_{12}V_{21}} = \prod_p \frac{(1-g'(p))(1-g''(p))}{(1-g_{12}(p))(1-g_{21}(p))}. \tag{A.23}$$

Note that, at primes, we have

$$\frac{(1-g')(1-g'')}{(1-g_{12})(1-g_{21})} = 1+g'g''+h'h'' \leqslant 1+2h'h'' \leqslant (1+h'h'')^2.$$

Hence $B \leqslant C^2$ and (A.22) gives

$$|G' * G''| \leqslant C^3 G_{12}G_{21}. \tag{A.24}$$

Now suppose that the density functions g' and g'' satisfy the linear sieve conditions, in which case so do the functions g_{12} and g_{21}. Take λ' and λ'' to be the optimal linear sieve weights of level D' and D'', respectively (either those from the beta-sieve or else those from the Selberg sieve corresponding to the density functions g_{12} and g_{21}, respectively). Then

$$G_{12} \leqslant (2e^{\gamma}+o(1))V_{12} \quad \text{and} \quad G_{21} \leqslant (2e^{\gamma}+o(1))V_{21}, \tag{A.25}$$

where V_{12} and V_{21} are the products (A.21) restricted by $p<D'$ and $p<D''$, respectively. Hence (A.22) gives

$$|G' * G''| \leqslant 4CV'V''(e^{2\gamma}+o(1)), \tag{A.26}$$

where

$$V' = \prod_{p<D'} (1-g'(p)) = (e^{-\gamma}+o(1))\frac{H'}{\log D'},$$
$$V'' = \prod_{p<D''} (1-g''(p)) = (e^{-\gamma}+o(1))\frac{H''}{\log D''},$$

by Mertens' formula, and H' and H'' are the products

$$H' = \prod_p (1-g'(p))\left(1-\frac{1}{p}\right)^{-1} \quad \text{and} \quad H'' = \prod_p (1-g''(p))\left(1-\frac{1}{p}\right)^{-1}. \tag{A.27}$$

Inserting these asymptotic formulas into (A.26), we conclude the main result of this section.

Theorem A.5. *Let $\{\lambda'\}$ and $\{\lambda''\}$ be the linear sieves of level D' and D'', respectively, and let g' and g'' be density functions which satisfy the linear sieve conditions. Then*

$$|G'*G''| \leqslant (4+o(1)) \frac{CH'H''}{(\log D')(\log D'')}, \tag{A.28}$$

where C, H' and H'' are given by the infinite products (A.13) *and* (A.27), *respectively.*

Example. Let q' and q'' be positive integers and set

$$g'(d) = \begin{cases} d^{-1}, & \text{if } (d,q')=1, \\ 0, & \text{otherwise,} \end{cases} \qquad \text{and} \qquad g''(d) = \begin{cases} d^{-1}, & \text{if } (d,q'')=1, \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$H' = \frac{q'}{\varphi(q')}, \quad H'' = \frac{q''}{\varphi(q'')}$$

and

$$C \leqslant \prod_p \left(1+\frac{1}{(p-1)^2}\right) < 3.$$

In this case we obtain

$$|G'*G''| \leqslant \frac{q'q''}{\varphi(q')\varphi(q'')} \frac{12+o(1)}{(\log D')(\log D'')}. \tag{A.29}$$

Appendix B. The semilinear beta-sieve

In this section we state immediate consequences of some results for the semilinear sieve which we apply in the paper. Detailed proofs are given in [I1].

The sieve is based on the construction of two sequences $\{\lambda_d^+\}_d$ and $\{\lambda_d^-\}_d$, with $\lambda_1^\pm = 1$, $|\lambda_d^\pm| \leqslant 1$, and

$$\pm \sum_{d|n} \lambda_d^\pm \geqslant 0 \quad \text{for } n>1.$$

They have the following properties. Let $g(d)$ be a multiplicative function such that $0 \leqslant g(p) < 1$ at primes, and

$$\prod_{\substack{w\leqslant p<z \\ p\equiv 3 \pmod 4}} \frac{1}{1-g(p)} \leqslant \sqrt{\frac{\log z}{\log w}} \left(1+\frac{L}{\log w}\right)$$

for any $z \geqslant w \geqslant 2$ and some constant $L \geqslant 1$. We remark that the condition $p \equiv 3 \pmod 4$ is what we need in our application, but this could be replaced by any set of primes of asymptotic density $\frac{1}{2}$.

Let

$$P(z)=\prod_{\substack{p<z\\ p\equiv 3 \pmod 4}} p \quad\text{and}\quad V(z)=\prod_{p\mid P(z)}(1-g(p)),$$

and define

$$V^{\pm}(D,z)=\sum_{d\mid P(z)}\lambda_d^{\pm}g(d).$$

Then we have, for $1\leqslant s\leqslant 2$ and $z\geqslant 2$,

$$V^{+}(D,z)\leqslant V(z)(2+O((\log D)^{-1/6})), \tag{B.1}$$

$$V^{-}(D,z)\geqslant V(z)\big(\tfrac{1}{2}\sqrt{s-1}+O((\log D)^{-1/6})\big), \tag{B.2}$$

where $s=\log D/\log z$.

References

[Bo] Bombieri, E., On twin almost primes. *Acta Arith.*, 28 (1975/76), 177–193.

[BFI] Bombieri, E., Friedlander, J. B. & Iwaniec, H., Primes in arithmetic progressions to large moduli. *Acta Math.*, 156 (1986), 203–251.

[BGS] Bourgain, J., Gamburd, A. & Sarnak, P., Sieving and expanders. *C. R. Math. Acad. Sci. Paris*, 343 (2006), 155–159.

[CI] Chamizo, F. & Iwaniec, H., On the sphere problem. *Rev. Mat. Iberoamericana*, 11 (1995), 417–429.

[Fo] Fouvry, É., Autour du théorème de Bombieri–Vinogradov. *Acta Math.*, 152 (1984), 219–244.

[He] Heilbronn, H., On the averages of some arithmetical functions of two variables. *Mathematika*, 5 (1958), 1–7.

[I1] Iwaniec, H., The half dimensional sieve. *Acta Arith.*, 29 (1976), 69–95.

[I2] — *Spectral Methods of Automorphic Forms.* Graduate Studies in Mathematics, 53. Amer. Math. Soc., Providence, RI, 2002.

[IK] Iwaniec, H. & Kowalski, E., *Analytic Number Theory.* American Mathematical Society Colloquium Publications, 53. Amer. Math. Soc., Providence, RI, 2004.

[S1] Smith, R. A., On $\sum r(n)r(n+a)$. *Proc. Nat. Inst. Sci. India Sect. A*, 34 (1968), 132–137.

[S2] — The circle problem in an arithmetic progression. *Canad. Math. Bull.*, 11 (1968), 175–184.

John B. Friedlander
Department of Mathematics
University of Toronto
Toronto, Ontario M5S 2E4
Canada
frdlndr@utsc.utoronto.ca

Henryk Iwaniec
Department of Mathematics
Rutgers University
Piscataway, NJ 08903
U.S.A.
iwaniec@math.rutgers.edu

Received December 12, 2006