ACTA ARITHMETICA
128.2 (2007)

Prime numbers of the form $p = m^2 + n^2 + 1$ in short intervals

by

KAISA MATOMÄKI (Egham)

1. Introduction. In 1960 Linnik [5] proved an asymptotic formula for

$$\sum_{p \le N} r(p-a),$$

where the summation runs over primes, a is a fixed non-zero integer and $r(n)$ is the number of representations of n as a sum of two squares. This implies the first unconditional proof that there are infinitely many primes of the form $p = m^2 + n^2 + 1$. Huxley and Iwaniec [1] considered primes of the form $m^2 + n^2 + 1$ with $(m, n) = 1$ in the short interval $(x, x + x^\theta]$. They proved that for $\theta = 99/100$ this interval contains primes of this type for every sufficiently large x and more precisely that the number of them is of the expected order of magnitude, that is, $\gg x^\theta/(\log x)^{3/2}$. Wu [7] improved this result to $\theta = 115/121 \approx 0.9504$.

In this paper, we prove the following theorem.

THEOREM 1. *For every $\theta \ge 10/11 = 0.9090\ldots$ and $x \ge x_0(\theta)$, we have*

$$\sum_{x<p\le x+x^\theta} b^*(p-1) \gg x^\theta/(\log x)^{3/2}, \tag{1}$$

where

$$b^*(a) = \begin{cases} 1 & \textit{if } a = m^2 + n^2 \textit{ with } (m, n) = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Since the set $\{m^2 + n^2 \mid (m, n) = 1\}$ consists of numbers with no prime factors belonging to $\mathcal{P}_3 = \{p \mid p \equiv 3 \pmod 4\}$, it is natural to attack this problem by applying the half-dimensional sieve to the set

$$\mathcal{A} = \{p - 1 \mid x < p \le x + x^\theta,\ p \equiv 3 \pmod 8\}.$$

As usual, for a finite set $\mathcal{F} \subset \mathbb{N}$ and a set $\mathcal{P}$ of primes we write

$$P(z) = \prod_{p\in\mathcal{P},\, p<z} p, \qquad S(\mathcal{F}, \mathcal{P}, z) = |\{a \in \mathcal{F} \mid (a, P(z)) = 1\}|.$$

2000 *Mathematics Subject Classification*: 11N05, 11N36.

Then

$$\sum_{x<p\le x+x^\theta} b^*(p-1) = S(\mathcal{A},\mathcal{P}_3,x+x^\theta). \tag{2}$$

As in previous works, for $z = x^{1/\alpha}$, $\alpha\in[2,4)$, we write

$$S(\mathcal{A},\mathcal{P}_3,x+x^\theta) = S(\mathcal{A},\mathcal{P}_3,z) - T. \tag{3}$$

A lower bound for $S(\mathcal{A},\mathcal{P}_3,z)$ is obtained by the half-dimensional sieve as in [1] and [7]. To get an upper bound for T we use the method of [7] but take advantage of an averaging over a parameter l by using a more flexible error term in the linear sieve. This idea of the proof goes back to Iwaniec [2].

Since each element $a\in\mathcal{A}$ has an even number of prime factors belonging to $\mathcal{P}_3$ and $2\,\|\,a$, for $\alpha<4$ we have

$$T = \sum_{\substack{x<p\le x+x^\theta\\ p=1+2np_1p_2}} 1,$$

where $p_1,p_2\in\mathcal{P}_3$, $p_1\ge p_2\ge x^{1/\alpha}$ and n is an integer divisible only by primes of the form $p\equiv 1 \pmod 4$. Define

$$\begin{aligned}\mathcal{L} = \{l = np_2 \mid n\le x^{1-2/\alpha},\ p\,|\,n\Rightarrow p\equiv 1 \ (\mathrm{mod}\,4),&\\ x^{1/\alpha}\le p_2<(x/n)^{1/2},\ p_2\in\mathcal{P}_3\}&\end{aligned}$$

and, for each $l\in\mathcal{L}$,

$$\mathcal{M}(l) = \{m = 2lp_1+1 \mid x/2\le p_1l<(x+x^\theta)/2,\ lp_1\equiv 1 \ (\mathrm{mod}\,4)\}.$$

Then T is at most the number of primes in $\bigcup_{l\in\mathcal{L}}\mathcal{M}(l)$. Thus

$$T\le\sum_{l\in\mathcal{L}}(S(\mathcal{M}(l),\mathcal{P}(l),x^{\theta_0}) + O(x^{\theta_0})), \tag{4}$$

where $\mathcal{P}(l) = \{p \mid (p,2l)=1\}$.

2. Auxiliary results. To get an upper bound for T we need two lemmata. The first one is the linear sieve with a flexible error term, and the second one gives the required estimation for the error term arising from the sieve.

Before stating these lemmata we introduce some more sieve notation. For a square-free d with prime factors in $\mathcal{P}$, we let $\mathcal{F}_d = \{n \mid dn\in\mathcal{F}\}$. Let

$$|\mathcal{F}_d| = \frac{\omega(d)}{d}X + r(\mathcal{F},d),$$

where $X>1$ is independent of d and $\omega(d)$ is a multiplicative function. Define further

$$V(z) = \prod_{p<z,\,p\in\mathcal{P}}\left(1-\frac{\omega(p)}{p}\right).$$

Now we are ready to state the upper bound of the linear sieve. It follows as Theorem 1 of [4] by an obvious modification to the argument in Section 3 of [4].

LEMMA 2. *Assume that*

$$\prod_{\substack{w\le p<z\\ p\in\mathcal{P}}}\left(1-\frac{\omega(p)}{p}\right)^{-1}<\frac{\log z}{\log w}\left(1+\frac{K}{\log w}\right) \tag{5}$$

holds for all $z>w\ge 2$ with some constant K independent of w and z. Let further $s=\log Q/\log z$. Then

$$S(\mathcal{F},\mathcal{P},z)\le XV(z)(F(s)+o_K(1))+\sum_{d<Q,\, d\mid P(z)}a_d r(\mathcal{F},d),$$

where $a_d\ll 1$ depend only on Q but not on $|\mathcal{F}|$, $\mathcal{P}$ or ω. If $1\le s\le 3$, then $F(s)=2e^{\gamma}/s$, where γ is Euler's constant.

The next lemma is a generalisation of the Bombieri–Vinogradov theorem in short intervals. It follows from Theorem 2 of [6].

LEMMA 3. *Let $g(l)$ be an arithmetic function satisfying $g(l)\ll 1$ and let*

$$H(x',h,q,a,l)=\sum_{\substack{x'\le lp<x'+h\\ lp\equiv a\,(\mathrm{mod}\,q)}}1-\frac{1}{\phi(q)}\int_{x'/l}^{(x'+h)/l}\frac{dt}{\log t}.$$

Then for every $A>0$ there exists a positive constant $B=B(A)$ such that

$$\sum_{q\le Q}\max_{(a,q)=1}\max_{h\le x^{\theta}}\max_{x/2<x'\le x}\Big|\sum_{l\le L,\,(l,q)=1}g(l)H(x',h,q,a,l)\Big|\ll\frac{x^{\theta}}{(\log x)^{A}}$$

for $Q=x^{\theta-1/2}(\log x)^{-B}$ and $L=x^{(5\theta-3)/2-\varepsilon}$ with $3/5+\varepsilon\le\theta\le 1$.

To evaluate the upper bound for T which we get from the linear sieve, we need two more lemmata. The first one is Lemma 3 of [7].

LEMMA 4. *Let $u(n)$ be the characteristic function of the integers having all prime factors of the form $4m+1$. Let $f(n)=\prod_{p\mid n,\,p>2}(1-1/(p-1))^{-1}$. Then*

$$\sum_{n\le x}u(n)f(n)=\frac{A}{C_1}\frac{x}{(\log x)^{1/2}}+O\left(\frac{x}{(\log x)^{3/2}}\right),$$

where

$$A=\frac{1}{2\sqrt{2}}\prod_{p\equiv 3\,(\mathrm{mod}\,4)}\left(1-\frac{1}{p^2}\right)^{1/2},\qquad C_1=\prod_{p\equiv 1\,(\mathrm{mod}\,4)}\left(1-\frac{1}{(p-1)^2}\right).$$

The second lemma corresponds to Lemma 4 of [7].

LEMMA 5. *Let $\mathcal{L}$, $f(n)$, A and C_1 be defined as above. Then*

$$\sum_{l\in\mathcal{L}} \frac{f(l)}{l\log(x/l)} = \frac{1+o(1)}{(\log x)^{1/2}} \frac{A}{2C_1} \int_2^\alpha \frac{\log(t-1)}{t(1-t/\alpha)^{1/2}}\,dt. \tag{6}$$

Proof. We follow the proof of Lemma 4 of [7]. Our situation is easier, because we have $\log(x/l)$ instead of $(\log(x/l))^2$. Write Y for the left hand side of (6) and let $u(n)$ be defined as above. Then

$$Y = (1+o(1)) \sum_{n\le x^{1-2/\alpha}} \frac{u(n)f(n)}{n} \sum_{\substack{x^{1/\alpha}\le p_2<(x/n)^{1/2}\\ p_2\equiv 3 \,(\mathrm{mod}\, 4)}} \frac{1}{p_2\log(x/(np_2))}.$$

By the Siegel–Walfisz theorem

$$\sum_{\substack{p\le t\\ p\equiv 3\,(\mathrm{mod}\,4)}} 1 = \pi(t;4,3) = \frac{1}{2}\int_2^t \frac{dv}{\log v} + O(te^{-\sqrt{\log t}}).$$

Thus by partial integration

$$\begin{aligned} Y &= (1+o(1)) \sum_{n\le x^{1-2/\alpha}} \frac{u(n)f(n)}{n} \int_{x^{1/\alpha}}^{(x/n)^{1/2}} \frac{d\pi(t;4,3)}{t\log(x/(nt))} \\ &= \frac{1+o(1)}{2} \sum_{n\le x^{1-2/\alpha}} \frac{u(n)f(n)}{n} \int_{x^{1/\alpha}}^{(x/n)^{1/2}} \frac{dt}{t\log t\log(x/(nt))} \\ &= \frac{1+o(1)}{2\log x} \sum_{n\le x^{1-2/\alpha}} \frac{u(n)f(n)}{n} \frac{\log(\alpha h(n)-1)}{h(n)}, \end{aligned} \tag{7}$$

where $h(n) = 1-\log n/\log x$. Define

$$U(t) = \sum_{n\le t} u(n)f(n), \qquad K(t) = \frac{\log(\alpha h(t)-1)}{th(t)}.$$

Then for $x\ge 10$ and $1\le t\le x^{1-2/\alpha}$ we have

$$K'(t) = -\frac{1}{t^2h(t)}\log(\alpha h(t)-1) + O\left(\frac{1}{t^2\log x}\right),$$

because $h'(t) = -1/(t\log x)$ and $2/\alpha\le h(t)\le 1$ under these restrictions.

Since $U(1-) = K(x^{1-2/\alpha}) = 0$, by partial integration the last sum in (7) equals

$$\int_{1-}^{x^{1-2/\alpha}} K(v)\,dU(v) = -\int_{1}^{x^{1-2/\alpha}} U(v)K'(v)\,dv$$

$$= \frac{A}{C_1}\int_{1}^{x^{1-2/\alpha}} \frac{\log(\alpha h(v)-1)}{vh(v)(\log v)^{1/2}}\,dv + O(1)$$

$$= \frac{A}{C_1}\sqrt{\log x}\int_{2}^{\alpha} \frac{\log(t-1)}{t(1-t/\alpha)^{1/2}}\,dt + O(1),$$

where the last equality is due to the change of variables $t = \alpha h(v)$. ■

3. Application of sieves. First we state a lower bound for $S(\mathcal{A},\mathcal{P}_3,z)$.

PROPOSITION 6. *Let* $1/2 \le \theta \le 1$ *and* $2/(2\theta-1) \le \alpha \le 6/(2\theta-1)$. *Then*

$$S(\mathcal{A},\mathcal{P}_3,x^{1/\alpha}) \ge (W_1(\theta,\alpha)+o(1))\,\frac{x^\theta}{(\log x)^{3/2}},$$

where

$$W_1(\theta,\alpha) = \frac{AC_3}{\sqrt{4\theta-2}}\int_{1}^{\alpha(\theta-1/2)} \frac{dt}{\sqrt{t(t-1)}},$$

$C_3 = \prod_{p\equiv 3\,(\mathrm{mod}\,4)}(1-1/(p-1)^2)$ *and* A *is defined as above.*

Proof. The proof is an application of the half-dimensional sieve [3]. The estimation of the error term comes from the Bombieri–Vinogradov theorem in short intervals (Lemma 3). For details, see [7, Proposition 1]. ■

Next we find an upper bound for T.

PROPOSITION 7. *Let* $3/5 < \theta < 1$ *and let* $2 \le \alpha < \min\{4, 2/(5-5\theta), 6/(5-4\theta)\}$. *Then*

$$T \le (W_2(\theta,\alpha)+o(1))\,\frac{x^\theta}{(\log x)^{3/2}},$$

where

$$W_2(\theta,\alpha) = \frac{AC_3}{2\theta-1}\int_{2}^{\alpha} \frac{\log(t-1)}{t(1-t/\alpha)^{1/2}}\,dt.$$

Proof. For each $l \in \mathcal{L}$, in Lemma 2 choose

$$\mathcal{F} = \mathcal{M}(l), \qquad \mathcal{P} = \mathcal{P}(l), \qquad X = \frac{1}{2}\int_{x/(2l)}^{(x+x^\theta)/(2l)} \frac{dt}{\log t} = \frac{x^\theta}{4l\log(x/l)}\,(1+o(1))$$

and

$$\omega(p) = \begin{cases} p/(p-1) & \text{if } p \in \mathcal{P}(l),\\ 0 & \text{otherwise.}\end{cases}$$

Let d be a square-free integer with all the prime factors belonging to $\mathcal{P}(l)$. Let a_d^* be the unique $\pmod{4d}$ solution to the system of congruences

$$\begin{cases} 2x \equiv -1 \pmod{d}, \\ x \equiv 1 \pmod{4}. \end{cases}$$

Then

$$|\mathcal{M}(l)_d| = \sum_{\substack{x/2 \le p_1 l < (x+x^\theta)/2 \\ p_1 l \equiv a_d^* \pmod{4d}}} 1, \qquad r(\mathcal{M}(l), d) = H(x/2, x^\theta/2, 4d, a_d^*, l).$$

By Lemma 2 we obtain

$$\text{(8)} \qquad S(\mathcal{M}(l), \mathcal{P}(l), x^{\theta_0}) \le XV(x^{\theta_0})\left(F\left(\frac{\log Q}{\theta_0 \log x}\right) + o(1)\right) + \sum_{d<Q,\, d \mid P(l, x^{\theta_0})} a_d H(x/2, x^\theta/2, 4d, a_d^*, l),$$

where

$$P(l, z) = \prod_{p \in \mathcal{P}(l),\, p<z} p.$$

The implied constant here does not depend on l since we can choose the constant K in (5) independently of l: We simply drop out the condition $(p, 2l) = 1$ when we look for this constant.

Now

$$\text{(9)} \qquad V(x^{\theta_0}) = \prod_{p<x^{\theta_0},\, (p,2l)=1} \left(1 - \frac{1}{p-1}\right) = 2(1+o(1))C_1C_3 f(l) \prod_{p<x^{\theta_0}} \left(1 - \frac{1}{p}\right) = (1+o(1))\,\frac{2C_1C_3e^{-\gamma} f(l)}{\theta_0 \log x}$$

by Mertens' formula.

By choosing $Q = x^{\theta-1/2}/(\log x)^B$ and $\theta_0 = (\theta - 1/2)/3$, and summing over all $l \in \mathcal{L}$, from (4), (8) and (9) by Lemma 5 we get

$$T \le (W_2(\theta, \alpha) + o(1))\,\frac{x^\theta}{(\log x)^{3/2}} + O(|\mathcal{L}| x^{\theta_0}) + \sum_{l \in \mathcal{L}} \sum_{d<Q,\, d \mid P(l, x^{\theta_0})} a_d H(x/2, x^\theta/2, 4d, a_d^*, l).$$

Here the second term is

$$\ll x^{1-1/\alpha+\theta_0} \le x^{1-(5-4\theta)/6-\varepsilon+(\theta-1/2)/3} = o(x^\theta/(\log x)^{3/2}).$$

The third term is

$$\ll \sum_{d<Q,\, 2\nmid d} \Big| \sum_{l\in\mathcal{L},\, (l,d)=1} H(x/2, x^\theta/2, 4d, a_d^*, l)\Big| = o(x^\theta/(\log x)^{3/2})$$

by choosing $g(l)$ to be the characteristic function of $\mathcal{L}$ in Lemma 3. Here we have noticed that $|\mathcal{L}| \le x^{1-1/\alpha} \le x^{1-(5-5\theta)/2-\varepsilon} = x^{(5\theta-3)/2-\varepsilon}$. ∎

4. Proof of the theorem. Assume that $3/5 < \theta < 1$ and $2/(2\theta-1) \le \alpha < \min\{4, 2/(5-5\theta), 6/(5-4\theta)\}$. Then, by equations (2) and (3) and Propositions 6 and 7,

$$\sum_{x<p\le x+x^\theta} b^*(p-1) \ge \left(\frac{AC_3}{2\theta-1} W(\theta,\alpha) + o(1)\right)\frac{x^\theta}{(\log x)^{3/2}},$$

where

$$W(\theta,\alpha) = \sqrt{\theta-1/2}\int_1^{\alpha(\theta-1/2)} \frac{dt}{\sqrt{t(t-1)}} - \int_2^{\alpha} \frac{\log(t-1)}{t(1-t/\alpha)^{1/2}}\, dt.$$

The choice $\theta = 10/11$ and $\alpha = 11/4$ satisfies the assumptions. Evaluation of the integrals gives

$$W\left(\frac{10}{11}, \frac{11}{4}\right) > 0.005,$$

which completes the proof. ∎

Numerical calculation gives $\max_\alpha W(0.908, \alpha) < 0$. So there is no possibility to improve the exponent substantially without a new idea.

Acknowledgments. The author thanks Glyn Harman for his helpful comments and suggestions. The author was supported by EPSRC grant GR/T20236/01.

References

[1] M. N. Huxley and H. Iwaniec, *Bombieri's theorem in short intervals*, Mathematika 22 (1975), 188–194.

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

[3] —, *The half dimensional sieve*, ibid. 29 (1976), 69–95.

[4] —, *Rosser's sieve*, ibid. 36 (1980), 171–202.

[5] Yu. V. Linnik, *An asymptotic formula in an additive problem of Hardy and Littlewood*, Izv. Akad. Nauk SSSR Ser. Mat. 24 (1960), 629–706 (in Russian); English transl.: Amer. Math. Soc. Transl. 46 (1965), 65–148.

[6] J. Wu, *Théorèmes généralisés de Bombieri–Vinogradov dans les petits intervalles*, Quart. J. Math. Oxford 44 (1993), 109–128.

[7] J. Wu, *Primes of the form $p = 1 + m^2 + n^2$ in short intervals*, Proc. Amer. Math. Soc. 126 (1998), 1–8.

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom
E-mail: k.s.matomaki@rhul.ac.uk

Received on 6.11.2006 (5313)