A note on primes of the form $p = aq^2 + 1$

by

KAISA MATOMÄKI (Egham)

1. Introduction. It is a long-standing conjecture that there are infinitely many primes of the form $n^2 + 1$. Several approximations to this problem have been made. Baier and Zhao [1, Theorem 5'] showed that for any $\varepsilon > 0$, there are infinitely many primes of the form $p = aq^2 + 1$, where $a \leq p^{5/9+\varepsilon}$. We improve this result as follows.

**Theorem 1.** Let $\varepsilon > 0$. There are infinitely many primes of the form $p = aq^2 + 1$, where $a \leq p^{1/2+\varepsilon}$ and $q$ is a prime.

Baier and Zhao obtained their result as a corollary to their Bombieri–Vinogradov type theorem for sparse sets of moduli. Our improvement comes from using the sieve method of Harman [3, 4, 5].

We notice that in the interval $[1, X]$ there are $O(X^{3/4+\varepsilon/2})$ numbers of the form $aq^2 + 1$ with $a \leq X^{1/2+\varepsilon}$, so the set we are considering is quite sparse.

Throughout the paper the symbol $p$ is reserved for a prime variable and $\mathbb{P}$ is the set of primes. Theorem 1 is an immediate consequence of the following stronger result.

**Theorem 2.** Let $\varepsilon > 0$, $X \geq 1$ and $Q \in [X^{3\varepsilon}, X^{1/2-\varepsilon}]$. Then for all but $O(Q^{1/2}X^{-\varepsilon/4})$ prime squares $q^2 \sim Q$, we have, for any $k \in \{1, \ldots, q^2 - 1\}$ and $q \nmid k$,

$$\{aq^2 + k \mid a \sim X/Q\} \cap \mathbb{P} \gg \frac{X}{\phi(q^2) \log X}.$$  

The exponent $1/2$ is the limit of the current method as it is in the Bombieri–Vinogradov prime number theorem. In both cases the limit arises from a large sieve result, more precisely from the term corresponding to the number of points in outer summation in the large sieve ($Q^{3/2}$ in Lemma 3 below, leading to a critical term $(XQ)^{1/2}$ at the end of the proof of Theorem 2).

2000 Mathematics Subject Classification: 11N13, 11N36.

Key words and phrases: primes in quadratic progressions, sieve methods.

DOI: 10.4064/aa137-2-2
2. The method. First we introduce some standard notation. Let $\mathcal{E}$ be a finite subset of $\mathbb{N}$. Then we write $|\mathcal{E}|$ for the cardinality of $\mathcal{E}$,

$$\mathcal{E}_d = \{m \mid dm \in \mathcal{E}\}$$

and

$$S(\mathcal{E}, z) = |\{m \in \mathcal{E} \mid (m, P(z)) = 1\}|,$$

where $P(z) = \prod_{p < z} p$.

The elementary Buchstab’s identity states that

$$S(\mathcal{E}, z) = S(\mathcal{E}, w) - \sum_{w \leq p < z} S(\mathcal{E}_p, p),$$

where $z > w \geq 2$.

We write, for $q^2 \sim Q, AQ = X$,

$$\mathcal{A}(q, k) = \{aq^2 + k \mid a \sim A\},$$

$$\mathcal{A}(q) = \{n \mid n \in [Aq^2 + k, 2Aq^2 + k], (n, q^2) = 1\}.$$

Here $\mathcal{A}(q, k)$ is the set to be sieved and $\mathcal{A}(q)$ is the comparison set. We notice that the number of primes in $\mathcal{A}(q, k)$ is $S(\mathcal{A}(q, k), 3X^{1/2})$. We write $\theta = 3/8 + 2\varepsilon$ and $z = X^{1 - 2\theta}$. Then we use Buchstab’s identity to decompose $S(\mathcal{A}(q, k), 3X^{1/2})$

$$= S(\mathcal{A}(q, k), z) - \sum_{z < p < X^\theta} S(\mathcal{A}(q, k)_p, z) - \sum_{X^\theta \leq p < 3X^{1/2}} S(\mathcal{A}(q, k)_p, p)$$

$$+ \sum_{z < p_2 < p_1 < X^\theta} S(\mathcal{A}(q, k)_{p_1 p_2}, p_2)$$

$$= S_1(q, k) - S_2(q, k) - S_3(q, k) + S_4(q, k)$$

$$\geq S_1(q, k) - S_2(q, k) - S_3(q, k).$$

We write $S_i(q)$ for the sum $S_i(q, k)$ with $\mathcal{A}(q, k)$ replaced by $\mathcal{A}(q)$. We will show in the next section that

$$\sum_{\substack{q \in \mathbb{P} \atop q^2 \sim Q \atop q^k \sim Q}} \max_{1 \leq k < q^2} \left| \frac{S_i(q, k) - S_i(q)}{\phi(q^2)} \right| \ll \frac{X^{1-\varepsilon/3}}{Q^{1/2}}$$

for $i = 1, 2, 3$.

As in [5, Section 3.5], this leads to

$$S(\mathcal{A}(q, k), 3X^{1/2}) \geq \frac{1}{\phi(q^2)} (S(\mathcal{A}(q), 3X^{1/2}) - S_4(q))(1 + o(1))$$

$$= \frac{X (1 + o(1))}{\log X \phi(q^2)} \left( 1 - \int_{1/4}^\theta \int_{1/4}^{\min\{\alpha_1, (1 - \alpha_1)/2\}} \frac{d\alpha_2 \, d\alpha_1}{\alpha_1 \alpha_2 (1 - \alpha_1 - \alpha_2)} \right)$$

$$\geq \frac{X (1 + o(1))}{\log X \phi(q^2)} \left( 1 - \frac{5}{768} \cdot 4^2 \cdot \frac{16}{5} \right) = \frac{2X (1 + o(1))}{3 \log X \phi(q^2)}$$
for almost all prime squares \( q^2 \sim Q \) and all appropriate \( k \). This implies Theorem 2.

3. Proof of the bound (1). Proving (1) reduces to showing that for type I sums

\[
\sum_{q^2 \sim Q} \max_{1 \leq k < q^2} \left| \sum_{m \sim M} a_m - \frac{1}{\phi(q^2)} \sum_{mn \sim M} a_m \right| \ll \frac{X^{1-\varepsilon/2}}{Q^{1/2}},
\]

and for type II sums

\[
\sum_{q^2 \sim Q} \max_{1 \leq k < q^2} \left| \sum_{m \sim M} a_mb_n - \frac{1}{\phi(q^2)} \sum_{mn \sim M} a_m b_n \right| \ll \frac{X^{1-\varepsilon/2}}{Q^{1/2}},
\]

where \(|a_m|, |b_m| \leq \tau(m)\). Indeed, by [4, Lemma 2], and handling cross-conditions using the Perron formula as in the proof of that lemma, we need to show only that (2) holds for any \( M \leq X^\theta \) and that (3) holds for any \( M \in [X^\theta, X^{1-\theta}] \).

We get type I information by the following elementary argument. Since

\[
|A(q,k)_d| = |\{a \sim A \mid aq^2 \equiv -k \pmod{d}\}| = \begin{cases} A/d + O(1) & \text{if } (d,q^2) = 1, \\ 0 & \text{else} \end{cases} = \frac{1}{\phi(q^2)} |A(q)_d| + O(1),
\]

we have

\[
\sum_{mn \sim M} a_m = \frac{1}{\phi(q^2)} \sum_{mn \sim M} a_m + O(M(\log X)^C),
\]

which gives a sufficient bound for \( M \leq X^{1-\varepsilon}Q^{-1} \), and hence, in particular, for \( M \leq X^\theta \).

To get type II information we use the following large sieve result for square moduli.

**Lemma 3.** Let \( \eta > 0 \). Then

\[
\sum_{q^2 \sim Q} \sum_{a=1}^{q^2} \left| \sum_{m \sim M} a_m e\left(\frac{am}{q^2}\right)\right|^2 \ll (QM)^\eta(Q^{3/2} + MQ^{1/4}) \sum_{m \sim M} |a_m|^2.
\]

**Proof.** This follows from [2, Theorem 1]. \( \blacksquare \)
Remark 4. Since the outer summation in (4) goes over approximately $Q^{3/2}$ points $a/q^2$, the expected form of the large sieve would be
\[
\sum_{q^2 \sim Q} \sum_{a=1}^q \left( \sum_{m \sim M} a_m e \left( \frac{am}{q^2} \right) \right)^2 \ll (Q^{3/2} + M) \sum_{m \sim M} |a_m|^2.
\]

A crucial point here is that Lemma 3 implies this apart from a $(QM^\eta)$-factor for $M \ll Q^{5/4}$. In our type II sums we have $\max\{M, X/M\} \ll Q^{5/4}$ in the most difficult case $Q = X^{1/2-\varepsilon}$.

With standard techniques Lemma 3 implies

**Lemma 5.** Let $\eta > 0$. Then
\[
\sum_{q^2 \sim Q} \frac{q^2}{\phi(q^2)} \sum_{\chi \pmod{q^2}} \max_{x \leq X} \left| \sum_{mn \leq x \atop m \sim M} a_m b_n \chi(mn) \right| \ll (QX)^\eta (Q^{3/2} + MQ^{1/4})^{1/2} \times \left( Q^{3/2} + \frac{X}{M} Q^{1/4} \right)^{1/2} \left( \sum_{m \sim M} |a_m|^2 \sum_{n \leq X/M} |b_n|^2 \right)^{1/2}.
\]

Using this and the classical large sieve, we have
\[
\sum_{q \in \mathbb{P}} \max_{q^2 \sim Q} \left| \sum_{mn \in A(q,k) \atop m \sim M} a_m b_n - \frac{1}{\phi(q^2)} \sum_{mn \in A(q) \atop m \sim M} a_m b_n \right| \ll \sum_{q \in \mathbb{P}} \frac{1}{\phi(q^2)} \sum_{\chi \pmod{q^2}} \left| \sum_{mn \sim A(q) \atop m \sim M} a_m b_n \chi(mn) \right| + \sum_{q \in \mathbb{P}} \frac{1}{\phi(q^2)} \sum_{\chi \pmod{q}} \left| \sum_{mn \sim A(q) \atop m \sim M} a_m b_n \chi(mn) \right| \ll \left( (XQ)^{1/2} + \left( M + \frac{X}{M} \right)^{1/2} \frac{X^{1/2}}{Q^{1/8}} + \frac{X}{Q^{3/4}} \right) X^{\varepsilon/4} \ll \frac{X^{1-\varepsilon/2}}{Q^{1/2}}
\]

for $M \in [X^\theta, X^{1-\theta}]$ and $Q \in [X^{3\varepsilon}, X^{1/2-\varepsilon}]$, which completes the proof of condition (1).

**Acknowledgments.** The author thanks Glyn Harman for his helpful comments and suggestions.

The author was supported by EPSRC grant GR/T20236/01.
References


Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX
United Kingdom

Current address:
Department of Mathematics
20014 University of Turku, Finland
E-mail: ksmato@utu.fi

Received on 4.12.2007
and in revised form on 2.12.2008