Primes of the form $aq^2 + 1$

Kaisa Matomäki

Department of Mathematics
Royal Holloway, University of London

March 6, 2008

Outline

Primes of the Form n^2+1

A long-standing conjecture:

Conjecture

There are infinitely many primes of the form n^2+1.

The first twelve instances of such primes are

$$2 = 1^2+1 \qquad 101 = 10^2+1 \qquad 577 = 24^2+1$$
$$5 = 2^2+1 \qquad 197 = 14^2+1 \qquad 677 = 26^2+1$$
$$17 = 4^2+1 \qquad 257 = 16^2+1 \qquad 1297 = 36^2+1$$
$$37 = 6^2+1 \qquad 401 = 20^2+1 \qquad 1601 = 40^2+1$$

Primes Represented by Polynomials

The case of primes of the form $n^2+1=f(n)$ is a special case of a more general conjecture.

Conjecture

Any reasonable polynomial $f(n)\in\mathbb{Z}[x]$ takes prime values infinitely often.

- The linear case $f(n)=an+b$ (where reasonable means $\gcd(a,b)=1$) was proved by Dirichlet in 1837.
- No instance of the conjecture in higher degree is known.
- In 1922, Hardy and Littlewood gave a conjectural asymptotic formula for the number of primes of the form $f(n)$.

Prime factors of n^2+1

Theorem (Iwaniec 1978)

There are infinitely many integers n such that n^2+1 has at most two prime factors.

Write $P(m)$ for the greatest prime factor of m. Then of course

$$m \in \mathbb{P} \iff P(m) = m.$$

The previous theorem implies $P(n^2+1) > n$ infinitely often.

Theorem (Deshouillers and Iwaniec 1982)

There are infinitely many integers n such that $P(n^2+1) > n^{6/5}$.

In the proof the authors use their deep results on averages of Kloosterman sums.

Approximations with Polynomials in Two Variables

Theorem (Harman and Lewis 2001)

There exists infinitely many primes p with

$$p = n^2 + m^2, \quad m, n \in \mathbb{Z}, m < p^{0.119}.$$

The proof uses a generalization of Harman's sieve method to Gaussian integers (complex numbers $m + ni$ with $m, n \in \mathbb{Z}$).

Theorem (Friedlander and Iwaniec 1998)

There are infinitely many primes of the form $n^2 + m^4$.

The proof is almost one hundred pages long!

Approximations Using Fractional Parts

- For $x \in \mathbb{R}$, write $\{x\}$ for the fractional part of x.
- So $\{x\} \in [0,1)$ and $x - \{x\} \in \mathbb{Z}$.
- If $0 < \{x^{1/2}\} < x^{-1/2}$, then for some integer n,

$$n < x^{1/2} < n + x^{-1/2} \implies n^2 < x < n^2 + 2.$$

- Thus if we could show that $\{p^{1/2}\} < p^{-1/2}$ infinitely often, our conjecture would follow. But we only know

Theorem (Balog 1983, Harman 1983)

For any $\epsilon > 0$, there are infinitely many solutions to

$$\{p^{1/2}\} < p^{-1/4+\epsilon}.$$

Approximating with aq^2+1

- Still another way to approach primes of the form n^2+1 is to consider primes of the form $p = aq^2+1$ with a as small as possible.
- The case $a = 1$ is of course the conjecture itself.
- Baier and Zhao 2006: $a \leq p^{5/9+\epsilon}$ for any $\epsilon > 0$.

Theorem (Matomäki)

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

Refining the Task

- Let X be a large number. We write, for $q^2 \sim Q = X^{1/2-\epsilon}$,

$$\mathcal{A}(q) = \{aq^2+1 \mid aq^2+1 \sim X\} = \{n \sim X \mid n \equiv 1 \pmod{q^2}\}.$$

- We need that for infinitely many q holds $\sum_{p \in \mathcal{A}(q)} 1 > 0$.
- No reason for the residue class $1 \pmod{q^2}$ to be special among those coprime to q^2 and thus defining

$$\mathcal{B}(q) = \{n \sim X \mid \gcd(n, q^2) = 1\}$$

we would expect that

$$\sum_{p \in \mathcal{A}(q)} 1 = \frac{1}{\varphi(q^2)} \sum_{p \in \mathcal{B}(q)} 1 + \text{smaller error} \overset{PNT}{=} \frac{X(1+o(1))}{\varphi(q^2)\log X}.$$

- This holds assuming the generalized Riemann hypothesis.

Sums over Primes

- Sums over primes difficult to handle.
- But, it is possible to decompose them into easier sums.
- We want to split $\sum_{p\in\mathcal{A}(q)} 1 \approx \frac{1}{\varphi(q^2)} \sum_{p\in\mathcal{B}(q)}$ into showing that for type I sums

$$\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}} a_m = \frac{1}{\varphi(q^2)} \sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}} a_m + error$$

and type II sums

$$\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}} a_m b_n = \frac{1}{\varphi(q^2)} \sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}} a_m b_n + error,$$

where M lays in certain ranges.

Type I Sums

For a set $\mathcal{E} \subset \mathbb{N}$, we write $\mathcal{E}_d = \{m \mid dm \in \mathcal{E}\}$. Then

$$\begin{aligned}
|\mathcal{A}(q)_d| &= |\{m \sim X/d \mid dm = aq^2+1\}| \\
&= |\{a \sim X^{1/2+\epsilon} \mid aq^2 \equiv -1 \pmod{d}\}| \\
&= \begin{cases} \frac{X^{1/2+\epsilon}}{d} + O(1) & \text{if } \gcd(d,q^2)=1, \\ 0 & \text{else,} \end{cases} \\
&= \frac{1}{\varphi(q^2)} \sum_{\substack{k=1 \\ (k,q^2)=1}}^{q^2} |\{a \sim X^{1/2+\epsilon} \mid aq^2 \equiv -k \pmod{d}\}| + O(1) \\
&= \frac{|\mathcal{B}(q)_d|}{\varphi(q^2)} + O(1).
\end{aligned}$$

Type I Sums Continue

Since

$$|\mathcal{A}(q)_d| = \frac{|\mathcal{B}(q)_d|}{\varphi(q^2)} + O(1),$$

we have

$$\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}} a_m = \sum_{m\sim M} a_m|\mathcal{A}(q)_m| = \sum_{m\sim M} a_m \left(\frac{|\mathcal{B}(q)_m|}{\varphi(q^2)} + O(1)\right)$$

$$= \frac{1}{\varphi(q^2)} \sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}} a_m + O(M)$$

$$= \frac{1}{\varphi(q^2)} \sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}} a_m + O\left(\frac{X^{1-\epsilon/4}}{Q}\right)$$

for $M \le X^{1/2}$.

Type II Sums

- For type II sums we need deeper arguments.
- A large sieve result by Baier and Zhao implies that

$$\sum_{\substack{q\in\mathbb{P}\\ q^2\sim Q}}\left|\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}}a_m b_n-\frac{1}{\phi(q^2)}\sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}}a_m b_n\right|=O\left(\frac{X^{1-\epsilon/2}}{Q^{1/2}}\right)$$

for $M\in[X^{3/8+2\epsilon},X^{5/8-2\epsilon}]$.

- Thus for most prime squares $q^2\sim Q$ (all but $O(Q^{1/2}X^{-\epsilon/4})$)

$$\left|\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}}a_m b_n-\frac{1}{\phi(q^2)}\sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}}a_m b_n\right|=O\left(\frac{X^{1-\epsilon/4}}{Q}\right).$$

Arithmetic information

- By previous slides, we have type I information

$$\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}} a_m = \frac{1}{\varphi(q^2)} \sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}} a_m + O\left(\frac{X^{1-\epsilon/4}}{Q}\right)$$

  for $M \le X^{1/2}$ and type II information

$$\sum_{\substack{mn\in\mathcal{A}(q)\\ m\sim M}} a_m b_n = \frac{1}{\varphi(q^2)} \sum_{\substack{mn\in\mathcal{B}(q)\\ m\sim M}} a_m b_n + O\left(\frac{X^{1-\epsilon/4}}{Q}\right).$$

  for most q with $M \in [X^{3/8+2\epsilon}, X^{5/8-2\epsilon}]$.
- Next task is to split $\sum_{p\in\mathcal{A}(q)} 1$ into type I and type II sums for which we use Harman's sieve method.

Sieve Notation

- We write

$$S(\mathcal{E}, z) = |\{m \in \mathcal{E} \mid p \mid m \implies p > z\}|.$$

- Then $\mathcal{A}(q) \cap \mathbb{P} = S(\mathcal{A}(q), 3X^{1/2})$.
- *Buchstab's identity* states that for $z > w \geq 1$,

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

- This holds since by definitions

$$\begin{aligned} S(\mathcal{E}_p, p) &= |\{pn \in \mathcal{E} \mid p_0 \mid n \implies p_0 > p\}| \\ &= |\{n \in \mathcal{E} \mid \text{smallest prime factor of } n \text{ equals } p\}|. \end{aligned}$$

Decomposing $\mathcal{A}(q) \cap \mathbb{P}$

- So we want information about $\mathcal{A}(q) \cap \mathbb{P} = S(\mathcal{A}(q), 3X^{1/2})$.
- We use Buchstab's identity with $w = X^{1/4-4\epsilon}$ in order to decompose

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

and further

$$S(\mathcal{A}(q), w) = \sum_{n \in \mathcal{A}(q)} 1 - \sum_{p_1<w} \sum_{p_1 n \in \mathcal{A}(q)} 1 + \sum_{p_1<p_2<w} \sum_{p_1 p_2 n \in \mathcal{A}(q)} 1 - \dots$$

Finding type I and type II sums

- So, we ended up with sums of the form

$$\sum_{p_1<\cdots<p_j<w} \sum_{p_1\dots p_j n\in\mathcal{A}(q)} 1.$$

- If $p_1 \dots p_j \le X^{1/2}$, we have a type I sums with

$$a_m = \begin{cases} 1 & \text{if } m = p_1 \cdots p_j \text{ with } p_1 < \cdots < p_j < w, \\ 0 & \text{otherwise.} \end{cases}$$

- If $p_1 \dots p_j > X^{1/2}$, then for some $k \le j$, the product $p_1 \dots p_k \in [X^{3/8+2\epsilon}, X^{5/8-2\epsilon}]$ since $p_i < w = X^{1/4-4\epsilon}$. Thus we have a type II sum.
- Hence

$$S(\mathcal{A}(q), w) = \text{type I sums } + \text{ type II sums.}$$

Further decomposing

- Since

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

  we still need to handle

$$\sum_{w<p<3X^{1/2}} S(\mathcal{A}(q)_p, p)$$

- If $p > X^{3/8+2\epsilon}$, we have type II sum. Also if summand is replaced by $S(\mathcal{A}(q)_p, w)$ we have type I and II sums as before.
- Hence we can apply Buchstab's identity and find that

$$S(\mathcal{A}(q), 3X^{1/2}) = \text{type I/II sums} + \sum_{w<p_2<p_1<X^{3/8+2\epsilon}} S(\mathcal{A}(q)_{p_1p_2}, p_2).$$

Final steps of the proof

Now we have

$$S(\mathcal{A}(q),3X^{1/2}) \geq S(\mathcal{A}(q),3X^{1/2}) - \sum_{w<p_2<p_1<X^{3/8+2\epsilon}} S(\mathcal{A}(q)_{p_1p_2},p_2)$$

$$= \text{type I sums} + \text{type II sums}$$

$$= \frac{1}{\varphi(q^2)}\left(S(\mathcal{B}(q),3X^{1/2}) - \sum_{w<p_2<p_1<X^{3/8+2\epsilon}} S(\mathcal{B}(q)_{p_1p_2},p_2)\right)$$

$$+ O\left(\frac{X^{1-\epsilon/4}}{Q}\right) \geq \frac{X}{2Q\log X} > 0$$

for most q: Using the prime number theorem it is easy to see that

$$S(\mathcal{B}(q),3X^{1/2}) - \sum_{w<p_2<p_1<X^{3/8+2\epsilon}} S(\mathcal{B}(q)_{p_1p_2},p_2) \geq \frac{2X}{3\log X}. \quad \square$$

Further thoughts

- We have actually proved that for most prime squares $q^2 \sim X^{1/2-\epsilon}$, there are at least $X/(\phi(q^2)2\log X)$ primes with $p \sim X$ and $p \equiv 1 \pmod{q^2}$.
- The residue class 1 is not special here, and the result could be shown even uniformly for any k such that $\gcd(k, q^2) = 1$.
- Getting over barrier $1/2$ needs new ideas - type II information disappears at this point.

Summary

- Different approximations to $p = n^2 + 1$ showed well how innocent-looking number theoretic problems lead to very deep methods.
- Actually it does not seem likely that any of the approaches can finally settle the conjecture.
- Our approach was to show that there are primes p such that $p - 1$ possesses a large square factor.

Thank you

Any questions?