Simultaneous Prime Values of Two Binary Forms

Peter Cho-Ho Lam

Department of Mathematics
Simon Fraser University
chohol@sfu.ca

Twin Primes

Twin Prime Conjecture

There exists infinitely many $x \in \mathbb{Z}$ such that both x and $x + 2$ are prime.

Question 1

Are there infinitely many $x, y \in \mathbb{Z}$ such that both x and $x + 2y$ are primes?

Twin Primes

Twin Prime Conjecture

There exists infinitely many $x \in \mathbb{Z}$ such that both x and $x + 2$ are prime.

Question 1

Are there infinitely many $x, y \in \mathbb{Z}$ such that both x and $x + 2y$ are primes?

Main Problem

Question 2

Let $F, G \in \mathbb{Z}[x, y]$ be two irreducible binary forms. Are there infinitely many $x, y \in \mathbb{Z}$ such that both $F(x, y)$ and $G(x, y)$ are primes?

Fouvry and Iwaniec (1997)

There are infinitely many primes of the form $x^2 + y^2$ such that y is also a prime.

Main Result

Let $F, G \in \mathbb{Z}[X, Y]$ be two irreducible binary forms such that $\deg F = 2$ and $\deg G = 1$. If F is positive definite, then there are infinitely many $x, y \in \mathbb{Z}$ such that $F(x, y)$ and $G(x, y)$ are both primes.

Main Problem

Question 2

Let $F, G \in \mathbb{Z}[x, y]$ be two irreducible binary forms. Are there infinitely many $x, y \in \mathbb{Z}$ such that both $F(x, y)$ and $G(x, y)$ are primes?

Fouvry and Iwaniec (1997)

There are infinitely many primes of the form $x^2 + y^2$ such that y is also a prime.

Main Result

Let $F, G \in \mathbb{Z}[X, Y]$ be two irreducible binary forms such that $\deg F = 2$ and $\deg G = 1$. If F is positive definite, then there are infinitely many $x, y \in \mathbb{Z}$ such that $F(x, y)$ and $G(x, y)$ are both primes.

Main Problem

Question 2

Let $F, G \in \mathbb{Z}[x, y]$ be two irreducible binary forms. Are there infinitely many $x, y \in \mathbb{Z}$ such that both $F(x, y)$ and $G(x, y)$ are primes?

Fouvry and Iwaniec (1997)

There are infinitely many primes of the form $x^2 + y^2$ such that y is also a prime.

Main Result

Let $F, G \in \mathbb{Z}[X, Y]$ be two irreducible binary forms such that $\deg F = 2$ and $\deg G = 1$. If F is positive definite, then there are infinitely many $x, y \in \mathbb{Z}$ such that $F(x, y)$ and $G(x, y)$ are both primes.

Sieve Method - Asymptotic Sieve

We wish to obtain an asymptotic formula for the sum

$$\sum_{n \le x} a_n \Lambda(n)$$

where $\Lambda(n)$ is the von Mangoldt function,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

For example, we can take

$$a_n = 1 \quad \text{or} \quad a_n = \Lambda(n+2).$$

Sieve Method - Asymptotic Sieve

We wish to obtain an asymptotic formula for the sum

$$\sum_{n \leq x} a_n \Lambda(n)$$

where $\Lambda(n)$ is the von Mangoldt function,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

For example, we can take

$$a_n = 1 \qquad \text{or} \qquad a_n = \Lambda(n+2).$$

Asymptotic Sieve

In general, since

$$-\sum_{d|n} \mu(d) \log d = \Lambda(n)$$

where μ is the Möbius function,

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 p_2 ... p_r,\ p_i \text{ are all distinct primes} \\ 0 & \text{otherwise,} \end{cases}$$

we have

$$\sum_{n \leq x} a_n \Lambda(n) = -\sum_{n \leq x} a_n \sum_{d|n} \mu(d) \log d = -\sum_{d \leq x} \mu(d) \log d \sum_{\substack{n \leq x \\ n \equiv 0 \pmod{d}}} a_n.$$

Asymptotic Sieve

In general, since

$$-\sum_{d|n} \mu(d) \log d = \Lambda(n)$$

where μ is the Möbius function,

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 p_2 ... p_r,\ p_i \text{ are all distinct primes} \\ 0 & \text{otherwise,} \end{cases}$$

we have

$$\sum_{n \le x} a_n \Lambda(n) = -\sum_{n \le x} a_n \sum_{d|n} \mu(d) \log d = -\sum_{d \le x} \mu(d) \log d \sum_{\substack{n \le x \\ n \equiv 0 \pmod d}} a_n.$$

Asymptotic Sieve

Suppose for all d we have the following approximation:

$$\sum_{\substack{n \le x \\ n \equiv 0 \pmod{d}}} a_n = g(d) \sum_{n \le x} a_n + r_d(x)$$

for some multiplicative function $g(d)$.

Then the sum we need to estimate turns into

$$-\sum_{d \le x} \mu(d) \log d \sum_{\substack{n \le x \\ n \equiv 0 \pmod{d}}} a_n = -\sum_{d \le x} \mu(d) \log d \left(g(d) \sum_{n \le x} a_n + r_d(x) \right)$$

$$\approx -\left(\sum_{d \le x} \mu(d) g(d) \log d \right) \sum_{n \le x} a_n.$$

Asymptotic Sieve

Suppose for all d we have the following approximation:

$$\sum_{\substack{n\le x\\ n\equiv 0 \pmod d}} a_n = g(d)\sum_{n\le x} a_n + r_d(x)$$

for some multiplicative function $g(d)$.
Then the sum we need to estimate turns into

$$-\sum_{d\le x}\mu(d)\log d \sum_{\substack{n\le x\\ n\equiv 0 \pmod d}} a_n = -\sum_{d\le x}\mu(d)\log d\Big(g(d)\sum_{n\le x} a_n + r_d(x)\Big)$$

$$\approx -\Big(\sum_{d\le x}\mu(d)g(d)\log d\Big)\sum_{n\le x} a_n.$$

ASYMPTOTIC Sieve

For nice functions g (say $g(d) = 1/d$), we have

$$-\sum_{d} \mu(d) g(d) \log d = \prod_{p} (1 - g(p)) \left(1 - \frac{1}{p}\right)^{-1} = H.$$

Therefore if the remainder terms $r_d(x)$ are small on average, then we expect

$$\sum_{n \leq x} a_n \Lambda(n) \sim H \sum_{n \leq x} a_n$$

for some constant H.

When $a_n = 1$, we have $g(d) = 1/d$, $H = 1$, and we get back the Prime Number Theorem.

ASYMPTOTIC Sieve

For nice functions g (say $g(d) = 1/d$), we have

$$-\sum_{d} \mu(d) g(d) \log d = \prod_{p} (1 - g(p)) \left(1 - \frac{1}{p}\right)^{-1} = H.$$

Therefore if the remainder terms $r_d(x)$ are small on average, then we expect

$$\sum_{n \leq x} a_n \Lambda(n) \sim H \sum_{n \leq x} a_n$$

for some constant H.

When $a_n = 1$, we have $g(d) = 1/d, H = 1$, and we get back the Prime Number Theorem.

Type I Estimates

Type I: we wish to show that

$$\sum_{d \leq D} |r_d(x)| \ll o\left(\sum_{n \leq x} a_n\right)$$

for D as large as possible (best possible: $D = x^{1-\epsilon}$).

Type II Estimates

Type II: for large values of d,

$$-\sum_{D<d\leq x}\mu(d)\log d\sum_{\substack{n\leq x\\ n\equiv 0 \pmod d}}a_n=-\sum_{\substack{mn\leq x\\ D<m\leq x}}\mu(m)(\log m)a_{mn}.$$

The logarithm factor can be removed and it suffices to estimate

$$\sum_{n\sim N}\left|\sum_{m\sim M}\mu(m)a_{mn}\right|.$$

Settings

Let $F(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ and

$$a_n = \sum_{\substack{\ell \in \mathbb{Z}, m \in \mathbb{N} \\ F(\ell,m)=n \\ (\ell,m)=1}} \Lambda(m).$$

Two goals: estimate

$$\sum_{d \leq D} \left| \sum_{\substack{n \leq x \\ n \equiv 0 \pmod{d}}} a_n - g(d) \sum_{n \leq x} a_n \right| \quad \text{and} \quad \sum_{n \sim N} \left| \sum_{m \sim M} \mu(m) a_{mn} \right|.$$

Type I Estimates

$$A_d(f) = \sum_{\substack{F(\ell,m)\equiv 0 \pmod d \\ (\ell,m)=1}} \sum \Lambda(m) f(F(\ell,m))$$

$$= \sum_{\substack{\nu \pmod d \\ F(\nu,1)\equiv 0 \pmod d}} \sum_{a\in\mathbb{N}} \mu(a) \sum_{m\in\mathbb{N}} \Lambda(am) \sum_{\substack{\ell\in\mathbb{Z} \\ \ell\equiv \nu m \pmod d}} f(F(a\ell, am)).$$

By Poisson summation formula, the inner sum becomes

$$\sum_{\ell\equiv \nu m \pmod d} f(F(a\ell, am)) = \frac{1}{d} \sum_{h\in\mathbb{Z}} e\left(\frac{h\nu m}{d}\right) F_{a,m}\left(\frac{h}{d}\right)$$

where

$$F_{a,m}(z) = \int_{-\infty}^{\infty} f(F(at, am)) e(-zt)\, dt.$$

Type I Estimates

Large sieve: if $d_1, d_2 \sim D$, $F(\nu_1, 1) \equiv 0 \pmod{d_1}$, $F(\nu_2, 1) \equiv 0 \pmod{d_2}$,

$$\text{then} \quad \left\| \frac{\nu_1}{d_1} - \frac{\nu_2}{d_2} \right\| \gg \frac{1}{D}.$$

Balog, Blomer, Dartyge and Tenenbaum (2011)

Let $F(x,y) = \alpha x^2 + \beta xy + \gamma y^2 \in \mathbb{Z}[x,y]$ be an arbitrary quadratic form whose discriminant $\Delta = \beta^2 - 4\alpha\gamma$ is not a perfect square. For any sequence α_n of complex numbers, positive real numbers D, N, we have

$$\sum_{D \le d \le 2D} \sum_{F(\nu,1) \equiv 0 \pmod{d}} \left| \sum_{n \le N} \alpha_n e\left(\frac{\nu n}{d}\right) \right|^2 \ll_F (D+N) \sum_n |\alpha_n|^2.$$

Type I Estimates

Large sieve: if $d_1, d_2 \sim D$, $F(\nu_1, 1) \equiv 0 \pmod{d_1}$, $F(\nu_2, 1) \equiv 0 \pmod{d_2}$,

$$\text{then} \quad \left\| \frac{\nu_1}{d_1} - \frac{\nu_2}{d_2} \right\| \gg \frac{1}{D}.$$

Balog, Blomer, Dartyge and Tenenbaum (2011)

Let $F(x,y) = \alpha x^2 + \beta xy + \gamma y^2 \in \mathbb{Z}[x,y]$ be an arbitrary quadratic form whose discriminant $\Delta = \beta^2 - 4\alpha\gamma$ is not a perfect square. For any sequence α_n of complex numbers, positive real numbers D, N, we have

$$\sum_{D \le d \le 2D} \sum_{F(\nu,1) \equiv 0 \pmod{d}} \left| \sum_{n \le N} \alpha_n e\left(\frac{\nu n}{d}\right) \right|^2 \ll_F (D+N) \sum_n |\alpha_n|^2.$$

Type II Estimates

We need to estimate

$$\sum_{n\sim N}\left|\sum_{m\sim M}\mu(m)a_{mn}\right|.$$

What do we know about m, n if

$$mn = F(x,y) = \alpha x^2 + \beta xy + \gamma y^2$$

for some $x, y \in \mathbb{Z}, (x,y) = 1$?

Type II Estimates

We need to estimate

$$\sum_{n\sim N}\left|\sum_{m\sim M}\mu(m)a_{mn}\right|.$$

What do we know about m, n if

$$mn = F(x,y) = \alpha x^2 + \beta xy + \gamma y^2$$

for some $x, y \in \mathbb{Z}, (x,y) = 1$?

Type II Estimates

Simple example: $F(x, y) = x^2 + y^2$.

If $m = a^2 + b^2$ and $n = u^2 + v^2$, then $mn = x^2 + y^2$ with $x = au + bv, y = av - bu$ since

$$(a^2 + b^2)(u^2 + v^2) = (au + bv)^2 + (av - bu)^2.$$

Conversely, if $mn = x^2 + y^2$ with $(x, y) = 1$, then we can write $m = a^2 + b^2$ and $n = u^2 + v^2$ such that $x = au + bv, y = av - bu$.

It is NOT true in general.

Type II Estimates

Simple example: $F(x,y) = x^2 + y^2$.

If $m = a^2 + b^2$ and $n = u^2 + v^2$, then $mn = x^2 + y^2$ with $x = au + bv, y = av - bu$ since

$$(a^2 + b^2)(u^2 + v^2) = (au + bv)^2 + (av - bu)^2.$$

Conversely, if $mn = x^2 + y^2$ with $(x,y) = 1$, then we can write $m = a^2 + b^2$ and $n = u^2 + v^2$ such that $x = au + bv, y = av - bu$.

It is NOT true in general.

Type II Estimates

Simple example: $F(x,y) = x^2 + y^2$.

If $m = a^2 + b^2$ and $n = u^2 + v^2$, then $mn = x^2 + y^2$ with $x = au + bv, y = av - bu$ since

$$(a^2 + b^2)(u^2 + v^2) = (au + bv)^2 + (av - bu)^2.$$

Conversely, if $mn = x^2 + y^2$ with $(x, y) = 1$, then we can write $m = a^2 + b^2$ and $n = u^2 + v^2$ such that $x = au + bv, y = av - bu$.

It is NOT true in general.

Type II Estimates

Simple example: $F(x,y) = x^2 + y^2$.

If $m = a^2 + b^2$ and $n = u^2 + v^2$, then $mn = x^2 + y^2$ with $x = au + bv, y = av - bu$ since

$$(a^2 + b^2)(u^2 + v^2) = (au + bv)^2 + (av - bu)^2.$$

Conversely, if $mn = x^2 + y^2$ with $(x,y) = 1$, then we can write $m = a^2 + b^2$ and $n = u^2 + v^2$ such that $x = au + bv, y = av - bu$.

It is NOT true in general.

Type II Estimates

Trickier example: $F(x, y) = x^2 + 5y^2$ and

$$(a^2 + 5b^2)(u^2 + 5v^2) = (au + 5bv)^2 + 5(av - bu)^2.$$

For example, $2 \times 3 = (1)^2 + 5(1)^2$, but both $2 = x^2 + 5y^2$ and $3 = x^2 + 5y^2$ are not even solvable in integers.

But 2 and 3 can be represented by $2x^2 + 2xy + 3y^2$, and we also have the identity

$$(2a^2+2ab+3b^2)(2u^2+2uv+3v^2) = (2au+av+bu+3bv)^2+5(au-bv)^2.$$

Type II Estimates

Trickier example: $F(x,y) = x^2 + 5y^2$ and

$$(a^2+5b^2)(u^2+5v^2) = (au+5bv)^2 + 5(av-bu)^2.$$

For example, $2 \times 3 = (1)^2 + 5(1)^2$, but both $2 = x^2 + 5y^2$ and $3 = x^2 + 5y^2$ are not even solvable in integers.

But 2 and 3 can be represented by $2x^2 + 2xy + 3y^2$, and we also have the identity

$$(2a^2+2ab+3b^2)(2u^2+2uv+3v^2) = (2au+av+bu+3bv)^2 + 5(au-bv)^2.$$

Type II Estimates

Trickier example: $F(x,y) = x^2 + 5y^2$ and

$$(a^2+5b^2)(u^2+5v^2) = (au+5bv)^2 + 5(av-bu)^2.$$

For example, $2 \times 3 = (1)^2 + 5(1)^2$, but both $2 = x^2 + 5y^2$ and $3 = x^2 + 5y^2$ are not even solvable in integers.

But 2 and 3 can be represented by $2x^2 + 2xy + 3y^2$, and we also have the identity

$$(2a^2+2ab+3b^2)(2u^2+2uv+3v^2) = (2au+av+bu+3bv)^2+5(au-bv)^2.$$

Type II Estimates

In general, if $mn = F(x, y)$ and $(x, y) = 1$, then we wish to show that m can be represented by another binary quadratic form of the same discriminant, say f.

And then n can be represented by g, where

$$"f \times g = F, g = F \times f^{-1}".$$

We would also need a precise formula for g and an identity for the convolution.

Type II Estimates

In general, if $mn = F(x, y)$ and $(x, y) = 1$, then we wish to show that m can be represented by another binary quadratic form of the same discriminant, say f.

And then n can be represented by g, where

$$"f \times g = F, g = F \times f^{-1}".$$

We would also need a precise formula for g and an identity for the convolution.

Factorization

Lemma

If $mn = \alpha X^2 + \beta XY + \gamma Y^2$ for some integers X, Y with $(X, Y) = 1$, then there exists a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ and integers u, v, w, z such that $(u, v) = (w, z) = 1$ and

$$
\begin{aligned}
au^2 + buv + cv^2 &= m, \\
a\alpha w^2 + Bwz + \frac{B^2 + \Delta}{4a\alpha} z^2 &= n, \\
\left(au + \frac{b+\beta}{2} v\right) w + \left(\frac{B-\beta}{2\alpha} u + \frac{(b+\beta)B + \Delta - b\beta}{4a\alpha} v\right) z &= X, \\
-\alpha vw + \left(u - \frac{B-b}{2a} v\right) z &= Y;
\end{aligned}
$$

and the choice of f, u, v, w, z are "unique".

Related Problems

1. quadratic+linear
2. cubic+linear
3. quadratic + quadratic

THE END!