Sums of Two Squares in Function Fields

Lior Bary-Soroker
Tel Aviv University

Franco-German Summer School
Galois Theory and Number Theory
Konstanz, July 2015

Outline

1. **Sums of Two Squares**
   - Classical Theory
   - An Open Problem
2. **Function Fields**
   - Classical Theory
   - Short Intervals
3. **Methods of Proof**
   - A Galois Description of $b_q(f) = 1$
   - Equidistribution

Sums of Two Squares in Function Fields

Bary-Soroker

Outline

Characteristic Function

$$b(n) = \begin{cases} 1, & n = \square + \square \\ 0, & \textit{otherwise.} \end{cases}$$

Examples: $b(1) = b(2) = b(4) = b(5) = 1$,
while $b(3) = b(7) = 0$

Description as Norms of Gaussian integers

$$b(n) = 1 \iff n = \mathrm{Norm}_{\mathbb{Z}[i]}(a + bi)$$

Multiplicative Description – Fermat's Theorem

$$b(n) = 1 \iff N = 2^{\alpha} \prod_{p \equiv 1(4)} p^e \prod_{q \equiv 3(4)} q^{2e}$$

Asymptotic Density
Landau's Theorem

We denote by

$$\langle \varphi(n) \rangle_{n \in I} = \frac{1}{|I|} \sum_{n \in I} \varphi(n)$$

the average of the function φ on the set I

Theorem (Landau)

$$\langle b(n) \rangle_{n \leq x} = \frac{K}{\sqrt{\log x}} + O\left(\frac{1}{(\log x)^{3/2}} \right), \quad x \to \infty$$

Here $K = \frac{1}{\sqrt{2}} \prod_{p \equiv 3(4)} (1 - p^{-2})^{-1/2} \approx 0.764$ is the Landau-Ramanujan constant

Density in Short Intervals

Naive Expectation

$$\langle b(n)\rangle_{|n-x|\leq\phi(x)} \sim \langle b(n)\rangle_{n\leq x} \sim \frac{K}{\sqrt{\log x}}$$

for $\sqrt{\log x} < \phi(x) < x$ with $\phi(x)/\sqrt{\log x} \to \infty$.

Density in Short Intervals

Naive Expectation

$$\langle b(n)\rangle_{|n-x|\leq\phi(x)} \sim \langle b(n)\rangle_{n\leq x} \sim \frac{K}{\sqrt{\log x}}$$

for $\sqrt{\log x} < \phi(x) < x$ with $\phi(x)/\sqrt{\log x} \to \infty$.

Open Problem

How small can $\phi(x)$ be so that the naive expectation will hold?

History of the Problem

How small can $\phi(x)$ be so that $\langle b(n)\rangle_{|n-x|\leq\phi(x)} \sim \frac{K}{\sqrt{\log x}}$?

History of the Problem

How small can $\phi(x)$ be so that $\langle b(n)\rangle_{|n-x|\leq\phi(x)} \sim \frac{K}{\sqrt{\log x}}$?

Not Too Small

Balog-Wooley: Fails for any $\phi(x) = (\log x)^A$

History of the Problem

How small can $\phi(x)$ be so that $\langle b(n) \rangle_{|n-x| \le \phi(x)} \sim \frac{K}{\sqrt{\log x}}$?

Not Too Small

Balog-Wooley: Fails for any $\phi(x) = (\log x)^A$

Best Result

Huxely, Heath-Brown (methods from primes): $\phi(x) \ge x^{7/12}$

History of the Problem

How small can $\phi(x)$ be so that $\langle b(n) \rangle_{|n-x| \leq \phi(x)} \sim \frac{K}{\sqrt{\log x}}$?

Not Too Small

Balog-Wooley: Fails for any $\phi(x) = (\log x)^A$

Best Result

Huxely, Heath-Brown (methods from primes): $\phi(x) \geq x^{7/12}$

Sieve Methods

- Iwaniec (1976)
- Hooley (1974, 1994), Friedlander (1982), Plaskin (1987), Harman (1991)
- Balog-Wooley (2000)

Folklore Conjecture

Conjecture

Let $\epsilon > 0$. Then

$$\langle b(n)\rangle_{|n-x|\leq x^{\epsilon}} \sim \langle b(n)\rangle_{n\leq x} \sim \frac{K}{\sqrt{\log x}}, \quad x\to\infty$$

Folklore Conjecture

Conjecture

Let $\epsilon > 0$. Then

$$\langle b(n) \rangle_{|n-x| \le x^\epsilon} \sim \langle b(n) \rangle_{n \le x} \sim \frac{K}{\sqrt{\log x}}, \quad x \to \infty$$

Since this conjecture is completely open we will study it in function fields

Outline

1. Sums of Two Squares
   - Classical Theory
   - An Open Problem

2. **Function Fields**
   - Classical Theory
   - Short Intervals

3. Methods of Proof
   - A Galois Description of $b_q(f) = 1$
   - Equidistribution

What is the Analogue of Sums of Two Squares?

Instead of $\mathbb{Z}$ we work with $\mathbb{F}_q[T]$ with q odd

$$f(T) = A(T)^2 + B^2(T)$$

What is the Analogue of Sums of Two Squares?

Instead of $\mathbb{Z}$ we work with $\mathbb{F}_q[T]$ with q odd

$\cancel{f(T) = A(T)^2 + B^2(T)}$, e.g. $= (A + 2B)(A - 2B) \mod 5$

What is the Analogue of Sums of Two Squares?

Instead of $\mathbb{Z}$ we work with $\mathbb{F}_q[T]$ with q odd

$\cancel{f(T) = A(T)^2 + B^2(T)}$, e.g. $= (A + 2B)(A - 2B) \mod 5$

$f(T) = A(T)^2 + TB^2(T)$ – a norm from $\mathbb{F}_q[\sqrt{-T}]/\mathbb{F}_q[T]$
$b_q(f) = 1$ in this case, otherwise $b_q(f) = 0$

What is the Analogue of Sums of Two Squares?

Instead of $\mathbb{Z}$ we work with $\mathbb{F}_q[T]$ with q odd

$\cancel{f(T) = A(T)^2 + B^2(T)}$, e.g. $= (A + 2B)(A - 2B) \mod 5$

$f(T) = A(T)^2 + TB^2(T)$ – a norm from $\mathbb{F}_q[\sqrt{-T}]/\mathbb{F}_q[T]$
$b_q(f) = 1$ in this case, otherwise $b_q(f) = 0$

Multiplicative description – "Fermat's Theorem"

$$b_q(f) = 1 \iff f = T^\alpha \prod P^{e_P} \prod Q^{2e_Q}$$

where $T \neq P$ (resp. Q) runs over all prime polynomials with $P(-T^2)$ (resp. $Q(-T^2)$) reducible (resp. irreducible)

Function Field Landau's Theorem
Two Limits Phenomenon

Denote $M_{n,q} \subseteq \mathbb{F}_q[T]$, monic polynomials of degree n

$$M_{n,q} \leftrightsquigarrow \{n : 1 \leq n \leq x\} \quad \text{and} \quad \# M_{n,q} = q^n \leftrightsquigarrow x$$

Function Field Landau's Theorem
Two Limits Phenomenon

Denote $M_{n,q} \subseteq \mathbb{F}_q[T]$, monic polynomials of degree n

$$M_{n,q} \leftrightsquigarrow \{n : 1 \leq n \leq x\} \quad \text{and} \quad \# M_{n,q} = q^n \leftrightsquigarrow x$$

Theorem (BS-Smilanski-Wolf)

$$\langle b_q(f) \rangle_{f \in M_{n,q}} = \frac{K_q}{\sqrt{n}} + O_q(n^{-3/2}), \qquad n \to \infty$$

$$\langle b_q(f) \rangle_{f \in M_{n,q}} = \frac{\binom{2n}{n}}{4^n} + O_n(q^{-1}), \qquad q \to \infty$$

Denote $M_{n,q} \subseteq \mathbb{F}_q[T]$, monic polynomials of degree n

$$M_{n,q} \leftrightsquigarrow \{n : 1 \leq n \leq x\} \quad \text{and} \quad \#M_{n,q} = q^n \leftrightsquigarrow x$$

Theorem (BS-Smilanski-Wolf)

$$\langle b_q(f) \rangle_{f \in M_{n,q}} = \frac{K_q}{\sqrt{n}} + O_q(n^{-3/2}), \qquad n \to \infty$$

$$\langle b_q(f) \rangle_{f \in M_{n,q}} = \frac{\binom{2n}{n}}{4^n} + O_n(q^{-1}), \qquad q \to \infty$$

Comparison of main terms in the different limits

$$\lim_{n\to\infty} \lim_{q\to\infty} \frac{K_q}{\sqrt{n}} \frac{4^n}{\binom{2n}{n}} = \lim_{q\to\infty} \lim_{n\to\infty} \frac{K_q}{\sqrt{n}} \frac{4^n}{\binom{2n}{n}}$$

Main Result
Large Finite Field Limit

Conjecture: $\langle b(n)\rangle_{|n-x|\le x^{\epsilon}} \sim \langle b(n)\rangle_{n\le x} \sim \dfrac{K}{\sqrt{\log x}}$

Norm of a polynomial: $|f| = \#(\mathbb{F}_q[T]/f) = q^{\deg f}$
Analogue of $|n-x|\le x^{\epsilon}$**:** $|f-f_0|\le |f_0|^{\epsilon}$, $f_0\in\mathcal{M}_{n,q}$

Main Result
Large Finite Field Limit

Conjecture: $\langle b(n)\rangle_{|n-x|\le x^\epsilon} \sim \langle b(n)\rangle_{n\le x} \sim \frac{K}{\sqrt{\log x}}$

Norm of a polynomial: $|f| = \#(\mathbb{F}_q[T]/f) = q^{\deg f}$
Analogue of $|n-x|\le x^\epsilon$**:** $|f-f_0|\le |f_0|^\epsilon$, $f_0\in\mathcal{M}_{n,q}$

Theorem (Bank-BS-Fehm)

Fix n and $\frac{2}{n}\le\epsilon<1$. Then

$$\langle b_q(f)\rangle_{|f-f_0|\le|f_0|^\epsilon} = \frac{\binom{2n}{n}}{4^n} + O_n(q^{-1/2}), \quad q\to\infty$$

uniformly on $f_0\in\mathcal{M}_{n,q}$.

Main Result
Large Finite Field Limit

Conjecture: $\langle b(n)\rangle_{|n-x|\leq x^{\epsilon}} \sim \langle b(n)\rangle_{n\leq x} \sim \frac{K}{\sqrt{\log x}}$

Norm of a polynomial: $|f| = \#(\mathbb{F}_q[T]/f) = q^{\deg f}$
Analogue of $|n-x| \leq x^{\epsilon}$: $|f - f_0| \leq |f_0|^{\epsilon}$, $f_0 \in \mathcal{M}_{n,q}$

Theorem (Bank-BS-Fehm)

Fix n and $\frac{2}{n} \leq \epsilon < 1$. Then

$$\langle b_q(f)\rangle_{|f-f_0|\leq|f_0|^{\epsilon}} = \frac{\binom{2n}{n}}{4^n} + O_n(q^{-1/2}), \quad q \to \infty$$

uniformly on $f_0 \in \mathcal{M}_{n,q}$.

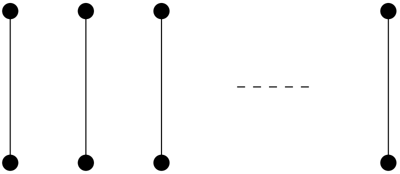
Completely settles the function field conjecture for large q

Outline

Observation

Let $f(T) = \prod_{i=1}^{n}(T + y_i)$ and $g(T) = f(-T^2) = \pm\prod_{i=1}^{n}(T - \sqrt{y_i})(T + \sqrt{y_i})$ be squarefree polynomials over a field K of characteristic $\neq 2$. Then

$$\mathrm{Gal}(g(T)/K) \hookrightarrow H_n$$

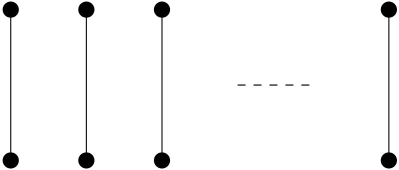
$H_n = Aut$ 

The Hyperoctahedral Group as Galois Group
Over a Finite Field

$$g(T) = f(-T^2) = \prod_{f(-y_i)=0}(T - \sqrt{y_i})(T + \sqrt{y_i})$$

$$\mathrm{Gal}(g(T)/\mathbb{F}_q) = \langle \phi_q \rangle , \qquad \phi_q(x) = x^q$$

So g gives an element $\phi_{q,g} \in H_n$.



Proposition

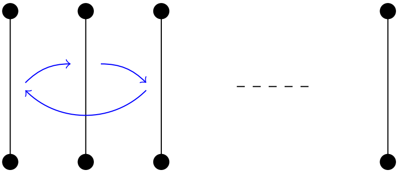
There exists $X_n \subseteq H_n$ such that $b_q(f) = 1$ if and only if $\phi_q \in X_n$

The Hyperoctahedral Group as Galois Group
Over a Finite Field

$$g(T) = f(-T^2) = \prod_{f(-y_i)=0}(T - \sqrt{y_i})(T + \sqrt{y_i})$$

$$\mathrm{Gal}(g(T)/\mathbb{F}_q) = \langle \phi_q \rangle\,, \qquad \phi_q(x) = x^q$$

So g gives an element $\phi_{q,g} \in H_n$.



Proposition

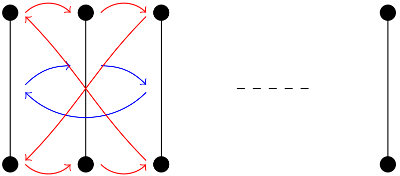
There exists $X_n \subseteq H_n$ such that $b_q(f) = 1$ if and only if $\phi_q \in X_n$

The Hyperoctahedral Group as Galois Group
Over a Finite Field

$$g(T) = f(-T^2) = \prod_{f(-y_i)=0}(T - \sqrt{y_i})(T + \sqrt{y_i})$$

$$\mathrm{Gal}(g(T)/\mathbb{F}_q) = \langle \phi_q \rangle \,, \qquad \phi_q(x) = x^q$$

So g gives an element $\phi_{q,g} \in H_n$.



Proposition

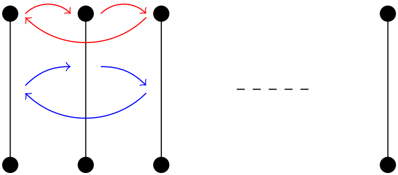
There exists $X_n \subseteq H_n$ such that $b_q(f) = 1$ if and only if $\phi_q \in X_n$

The Hyperoctahedral Group as Galois Group
Over a Finite Field

$$g(T) = f(-T^2) = \prod_{f(-y_i)=0}(T - \sqrt{y_i})(T + \sqrt{y_i})$$

$$\mathrm{Gal}(g(T)/\mathbb{F}_q) = \langle \phi_q \rangle\,, \qquad \phi_q(x) = x^q$$

So g gives an element $\phi_{q,g} \in H_n$.



Proposition

There exists $X_n \subseteq H_n$ such that $b_q(f) = 1$ if and only if $\phi_q \in X_n$

Explicit Chebotarev's Theorem

For $f_0 \in \mathcal{M}_{n,q}$ put

$$\mathcal{F}_A(T) = f_0(T) + \sum_{i \le \epsilon n} A_i T^i$$

with $A = (A_0, \ldots, A_m)$ a tuple of variables ($m = \lfloor \epsilon n \rfloor$). Let

$$\mathcal{G}_A(T) = \mathcal{F}_A(-T^2) \quad \text{and} \quad G = \mathrm{Gal}(\mathcal{G}_A) \subseteq H_n$$

Theorem

$$Prob(a \in \mathbb{F}_q^{\lfloor \epsilon n \rfloor + 1} : \phi_{q,\mathcal{G}_a} \in X_n) \sim Prob_G(\sigma \in X_n)$$

Note that LHS $= \langle b(f) \rangle_{|f - f_0| \le |f_0|^\epsilon}$

Conclusion of the Proof

$$G = \mathrm{Gal}(\mathcal{G}_A(T)) = \mathrm{Gal}(\mathcal{F}_A(-T^2)) \subseteq H_n$$

Key Proposition

$$G = H_n$$

(Builds on Bank-BS-Rosenzweig: $\mathrm{Gal}(\mathcal{F}_A(T)) = S_n$)

Corollary

$$\langle b(f) \rangle_{|f-f_0| \leq |f_0|^\epsilon} \sim \frac{\#X_n}{\#H_n} = \frac{1}{4^n}\binom{2n}{n}$$

Conclusion of the Proof

$$G = \mathrm{Gal}(\mathcal{G}_A(T)) = \mathrm{Gal}(\mathcal{F}_A(-T^2)) \subseteq H_n$$

Key Proposition

$$G = H_n$$

(Builds on Bank-BS-Rosenzweig: $\mathrm{Gal}(\mathcal{F}_A(T)) = S_n$)

Corollary

$$\langle b(f) \rangle_{|f-f_0| \leq |f_0|^\epsilon} \sim \frac{\#X_n}{\#H_n} = \frac{1}{4^n}\binom{2n}{n}$$

Remarks

- This completes the proof

Conclusion of the Proof

$$G = \mathrm{Gal}(\mathcal{G}_A(T)) = \mathrm{Gal}(\mathcal{F}_A(-T^2)) \subseteq H_n$$

Key Proposition

$$G = H_n$$

(Builds on Bank-BS-Rosenzweig: $\mathrm{Gal}(\mathcal{F}_A(T)) = S_n$)

Corollary

$$\langle b(f)\rangle_{|f-f_0|\leq|f_0|^\epsilon} \sim \frac{\#X_n}{\#H_n} = \frac{1}{4^n}\binom{2n}{n}$$

Remarks

- This completes the proof
- The last inequality comes from Ewens' sampling formula

Further Problems to Think About

Further Problems to Think About

- Limit $n \to \infty$

Further Problems to Think About

- Limit $n \to \infty$
- Further study of the error term

$$E = \langle b_q(f) \rangle_{|f - f_0| \leq |f_0|^\epsilon} - \frac{1}{4^n}\binom{2n}{n}$$

(Sharper upper bounds on $|E|$, average, variance,...)

Further Problems to Think About

- Limit $n \to \infty$
- Further study of the error term

$$E = \langle b_q(f) \rangle_{|f-f_0| \leq |f_0|^{\epsilon}} - \frac{1}{4^n}\binom{2n}{n}$$

(Sharper upper bounds on $|E|$, average, variance,...)

- Obtaining main terms in different problems, e.g.

$$\langle b_q(f) b_q(f+h) \rangle_{f \in M_{n,q}}$$

Further Problems to Think About

- Limit $n \to \infty$
- Further study of the error term

$$E = \langle b_q(f) \rangle_{|f-f_0| \le |f_0|^\epsilon} - \frac{1}{4^n}\binom{2n}{n}$$

(Sharper upper bounds on $|E|$, average, variance,...)
- Obtaining main terms in different problems, e.g.

$$\langle b_q(f) b_q(f+h) \rangle_{f \in M_{n,q}}$$

- Landau's theorem in $q^n \to \infty$
Some progress was already obtained by Ofir Gorodetsky