New results on prime polynomials (joint work with Mark Shusterman)

Will Sawin

Columbia University

November 12, 2020

Twin primes and generalizations

Twin primes conjecture: There exist infinitely many n such that $n, n+2$ are both prime. (e.g. $n = 3, 5, 11, 17, 29, 41, 59, \ldots$)

de Polignac's conjecture: For any nonzero even h, there exist infinitely many n such that n and $n+h$ are prime.

Hardy-Littlewood conjecture: For any nonzero h,

$$\lim_{X \to \infty} \frac{\#\{n < X \mid n, n+h \text{ prime}\}}{X/(\log X)^2} = C_h$$

for an explicit constant C_h.

What is known?

- Y. Zhang: Infinitely many pairs of primes with distance at most $70,000,000$.
- Polymath 8a: ∞ with distance at most $4,422$.
- Maynard: ∞ with distance at most 600.
- Polymath 8b: ∞ with distance at most 246.

Polynomials over finite fields

Let q be any power of a prime p.
There exists a unique field $\mathbb{F}_q$ with q elements.
It is an extension of the field $\mathbb{Z}/(p\mathbb{Z})$ of integers modulo p.

$\mathbb{F}_q[T]$: Polynomials in one variable with coefficients in $\mathbb{F}_q$. ($\approx \mathbb{Z}$)

$\mathbb{F}_q[T]^+$: Polynomials whose leading coefficient is 1 (i.e. monic polynomials). ($\approx \mathbb{N}$)

Prime polynomials: Monic polynomials not 1 with no monic polynomial factors except 1 and themselves. ($\approx \{\text{primes}\}$)

There are analogues of almost all concepts of number theory here, not just primes.

Prime number theorem for polynomials

For any finite field $\mathbb{F}_q$,

$$\lim_{d \to \infty} \frac{\#\{f \in \mathbb{F}_q[T]^+ \mid \deg f = d, f \text{ prime}\}}{q^d/d} = 1.$$

Examples

Prime polynomials: Monic polynomials not 1 with no monic polynomial factors except 1 and themselves.
In $\mathbb{F}_2[T]$, there are four monic polynomials of degree 2:

$$T^2, T^2+1, T^2+T, T^2+T+1$$

We have

$$T^2 = (T)^2, T^2+1 = (T+1)^2, T^2+T = T(T+1)$$

but T^2+T+1 is prime.

In $\mathbb{F}_q[T]$ there are q^2 degree two monic polynomials.

- There are q perfect squares $(T-a)^2$ for $a \in \mathbb{F}_q$.
- There are $\frac{q(q-1)}{2}$ products $(T-a)(T-b)$ with $a \neq b \in \mathbb{F}_q$.
- There are $\frac{q(q-1)}{2}$ remaining polynomials, all prime.

Number of primes $\approx \frac{q^2}{2}$.

Twin primes over $\mathbb{F}_q[T]$

Hardy-Littlewood conjecture for polynomials

For any finite field $\mathbb{F}_q$, for any nonzero $h \in \mathbb{F}_q[T]$

$$\lim_{d \to \infty} \frac{\#\{f \in \mathbb{F}_q[T]^+ \mid \deg f = d, f \text{ is prime}, f + h \text{ is prime}\}}{q^d / d^2} = C_h$$

for an explicit constant C_h.

Theorem 1 (S-Shusterman)

For q a power of a prime p, if p is odd and $q > 685,090p^2$, this conjecture is true.

Prior work

The conjecture that there exists infinitely many f with f and $f + h$ both prime was known as long as h is a monomial and $q > 105$, by Castilo, Hall, Lemke Oliver, Pollack, and Thompson. This adapted ideas of Maynard and a trick due to Entin.

The same result for h a constant was done earlier by Hall.

The limit as q goes to infinity and d is fixed was handled by Bender and Pollack for q odd and Carmon for q even.

Prime values of polynomials

Landau's problem: Show there are infinitely many primes of the form $n^2 + 1$

Bunyakovsky's conjecture: Gives conditions on a polynomial G that ensure $G(n)$ takes a prime value infinitely often.

Bateman-Horn conjecture: If G is nonconstant,

$$\lim_{X \to \infty} \frac{\#\{n \in \mathbb{N} \mid n < X, G(n) \text{ prime}\}}{X / \log X} = C_G$$

for an explicit constant C_G.

What is known? Almost nothing unless $\deg G = 1$ (Dirichlet's theorem.). We know $n^2 + m^4$ takes infinitely many prime values (Friedlander-Iwaniec.)

Bateman-Horn over $\mathbb{F}_q[T]$

Conjecture (Bateman-Horn over $\mathbb{F}_q[T]$)

Let $G \in \mathbb{F}_q[T, x]$ be a polynomial over $\mathbb{F}_q[T]$ but not a polynomial in x^p.

$$\lim_{d \to \infty} \frac{\#\{f \in \mathbb{F}_q[T]^+ \mid \deg f = d, G(T, f) \text{ is prime}\}}{q^d / d} = C_G$$

for an explicit constant C_G.

Theorem 2 (S-Shusterman)

For q a power of a prime p, if p is odd, $q > 2^{10} 3^2 e^2 p^4$ and $G = x^2 + D$ for some $D \in \mathbb{F}_q[T]$, then this conjecture is true.

Prior work

Pollack proved the weaker statement (there exist infinitely many prime values) for certain special G like $G(T, x) = x^\ell - \beta$, $\beta \in \mathbb{F}_q^\times$, by an explicit construction (take f to be a large power of T).

$q \to \infty$ version: Pollack (G depends only on x), Entin (G monic in x), Kowalski (higher genus case)

The parity problem

"To tell if a number is prime, you first have to tell if it has an odd number of prime factors."

Use the Möbius function:

$$\mu(n) = \begin{cases} (-1)^r & n = p_1 \dots p_r \text{ for } p_1, \dots, p_r \text{ prime, distinct} \\ 0 & \text{otherwise} \end{cases}$$

To count primes of the form $n^2 + 1$ with $n < X$, we first need to estimate $\sum_{n<X} \mu(n^2 + 1)$.

To count twin primes, we first need to estimate $\sum_{n<X} \mu(n)\mu(n+2) = \sum_{n<X} \mu(n(n+2))$.

Why do we care about odd vs. even instead of mod 3 or something else? Reason is

$$-\sum_{d|n} \mu(d) \log(d) = \Lambda(n) = \begin{cases} \log p & n = p^r, p \text{ prime} \\ 0 & \text{otherwise} \end{cases}$$

so we can transform counts of primes into sums of Möbius.

Chowla's conjecture

Luckily, we expect $\sum_{n<X} \mu(G(n))$ to cancel for every nonconstant polynomial G:

Chowla's conjecture

For any nonconstant polynomial $G(n)$,

$$\lim_{X\to\infty} \frac{\sum_{n<X} \mu(G(n))}{X} = 0.$$

Unfortunately, we don't know how to prove this.

$\deg G = 1$: essentially Dirichlet's theorem on primes in arithmetic progressions.

$G(n) = \prod_{i=1}^{k}(n+h_i)$: OK if $k=2$ or k is odd, and we make an additional average over X (Matomäki, Radziwiłł, Tao, Teräväinen)

G a product of linear factors: We can at least prove the lim sup is less than 1 (Teräväinen)

Chowla's conjecture over $\mathbb{F}_q[T]$

$$\mu(f) = \begin{cases} (-1)^r & f = \pi_1 \dots \pi_r \text{ for } \pi_1, \dots, \pi_r \text{ prime, distinct} \\ 0 & \text{otherwise} \end{cases}$$

Conjecture (Chowla's conjecture over $\mathbb{F}_q[t]$)

Let $G \in \mathbb{F}_q[T, x]$ be a polynomial over $\mathbb{F}_q[T]$ but not a polynomial in x^p.

$$\lim_{d \to \infty} \frac{\sum_{\substack{f \in \mathbb{F}_q[T]^+ \\ \deg f = d}} \mu(G(T, f))}{q^d} = 0.$$

Theorem 3 (S-Shusterman)

For q a power of a prime p, if p is odd, $q > 4k^2 p^2 e^2$ and $\deg_x G = k$, the conjecture is true.

Prior work

What if $G \in \mathbb{F}_q[u, x^p]$?

Conrad, Conrad and Gross showed that $\mu(G(T, f))$ is a periodic function of f in that case - it depends on the congruence class of f mod some fixed polynomial, and also on the congruence class of $\deg f$ mod 4. They evaluated $\sum_f \mu(G(T, f))$ in this case - it does not always cancel.

So Theorem 3 handles the remaining case.

Our proof of Theorem 3 involves, in a sense, reduction to the case studied by Conrad-Conrad-Gross. We substitute $f = r + s^p$ and show cancellation in s. (Get the sum of a periodic function over a short interval.)

$q \to \infty$ version: Carmon and Rudnick (G a product of linear terms), Pollack, Entin, Kowalski (same cases as Bateman-Horn)

Strategy of proof of Theorem 1 and Theorem 2

$$-\sum_{\substack{g\in\mathbb{F}_q[T]^+\\ g|f}} \mu(g)\deg g = \Lambda(f) = \begin{cases} \deg \pi & f = \pi^r, \pi \text{ prime} \\ 0 & \text{otherwise} \end{cases}$$

Suffices to estimate a sum like

$$\sum_{\substack{f\in\mathbb{F}_q[T]^+\\ \deg f=d}} \sum_{\substack{g\in\mathbb{F}_q[T]^+\\ g|f^2+D}} \mu(g)\deg g$$

or even

$$\sum_{\substack{f\in\mathbb{F}_q[T]^+\\ \deg f=d}} \sum_{\substack{g\in\mathbb{F}_q[T]^+\\ g|f^2+D\\ \deg g=m}} \mu(g).$$

(Similar for the twin primes case, except we have two divisors g_1, g_2 and two degrees.)

Analysis of ranges

$$\sum_{\substack{f\in\mathbb{F}_q[T]^+\\ \deg f=d}} \sum_{\substack{g\in\mathbb{F}_q[T]^+\\ g|f^2+D\\ \deg g=m}} \mu(g).$$

We break into different ranges depending on m:

- If m is small, we can break sum into residue classes of f modulo g and write as a product over prime factors of g. Express in terms of an Euler product. The constant C_h or C_{T^2+D} pops out.
- If m is large, write $h=\frac{f^2+D}{g}$ and $f=h\tilde{f}+\alpha$ then express g in terms of $h,\tilde{f},\alpha$. Fix h,α to obtain a sum that looks like Theorem 3. Apply a strong (power savings), uniform form of Theorem 3.
- The hardest case is when m is just a little bigger than d. Use the theory of quadratic forms / Hooley's trick to conclude.

(Similar for the twin primes case, except we have more different ranges, and instead use a trick based on work of Fouvry and Michel to handle the middle range.)

How to handle Möbius

Conrad-Conrad-Gross showed $\mu(G(T, r + s^p))$ is a periodic function of s to some explicitly computable modulus $M_{G,r}$. We make this more explicit:

$$\mu(G(T, r + s^p)) = \chi(W_{G,r}(T, s))$$

where $\chi \colon (\mathbb{F}_q[T]/M_{G,r})^\times \to \pm 1$ is a quadratic character modulo $M_{G,r}$ and $W_{G,r} \in \mathbb{F}_q[T, x]/M_{G,r}$ is an explicit polynomial.

Why is this useful? We can choose a suitable set $\mathcal{R}$ of r so that

$$\sum_{\substack{f \in \mathbb{F}_q[T]^+ \\ \deg f = d}} \mu(G(T, f)) = \sum_{r \in \mathcal{R}} \sum_{\substack{s \in \mathbb{F}_q[T] \\ \deg s < \frac{d}{p}}} \mu(G(T, r+s^p)) = \sum_{r \in \mathcal{R}} \sum_{\substack{s \in \mathbb{F}_q[T] \\ \deg s < \frac{d}{p}}} \chi(W_{G,r}(T, s)).$$

It is sufficient to express cancellation in the sum over s.

Proof sketch of

$$\mu(G(T, r + s^p)) = \chi(W_{G,r}(T, s))$$

For simplicity, consider the case $G(T, x) = x$:
Let $\chi_2 \colon \mathbb{F}_q^\times \to \pm 1$ be the quadratic character. Let $f \in \mathbb{F}_q[T]$ have degree d. We have

$$\mu(f) = (-1)^d \chi_2(\Delta(f))$$

for Δ the discriminant (Pellet's formula, proof: Galois theory). We have

$$\Delta(f) = \text{Resultant}\left(\frac{df}{dT}, f\right)$$

(proof: express via roots) so we have

$$\mu(r + s^p) = (-1)^d \chi_2\left(\text{Resultant}\left(\frac{dr}{dT} + ps^{p-1}\frac{ds}{T}, r + s^p\right)\right)$$

$$= (-1)^d \chi_2\left(\text{Resultant}\left(\frac{dr}{dT}, r + s^p\right)\right)$$

and $f :\mapsto \chi_2\left(\text{Resultant}\left(\frac{dr}{dT}, f\right)\right)$ is a quadratic character of $\left(\mathbb{F}_q[T]/\frac{dr}{dT}\right)^\times$.

Möbius formula in the general case

For the general case of

$$\mu(G(T, r + s^p)) = \chi(W_{G,r}(T, s)),$$

this argument reduces us to an expression

$$\chi_2(\text{Resultant}(F_1(T, s), F_2(T, s)))$$

for F_1, F_2 depending on T, r. This vanishes when $s(a) = b$ for (a, b) such that $F_1(a, b) = F_2(a, b) = 0$.

There are finitely many such a, b. We define the modulus $M_{G,r}$ as a product of terms $(T - a)$ and write $W_{G,r}(T, x)$ as a product of terms $(x - b)$. It suffices to prove

$$\text{Resultant}(F_1(T, s), F_2(T, s)) = \text{Norm}^{\mathbb{F}_q}_{\mathbb{F}_q[T]/M_{G,r}} W_{G,r}(T, s).$$

To do this, we check that both sides are polynomials in the coefficients of s. We check that they vanish at the same points, and their order of vanishing is the same. It follows from elementary algebraic geometry that they agree (up to a constant).

Étale cohomology

The sum

$$\sum_{\substack{s \in \mathbb{F}_q[T] \\ \deg s < \frac{d}{p}}} \chi(W_{G,r}(T,s))$$

looks like, over the integers,

$$\sum_{s<Y} \chi(W_{G,r}(s)).$$

In classical number theory, we have tools (Polya-Vinogardov, Burgess, ...) to bound these types of sums. But in our case the interval is too short to apply these tools. (unless $p = 3$ and $\deg G = 1$.)

Instead, view this as a sum over $\lceil \frac{d}{p} \rceil$ variables in $\mathbb{F}_q$ (the coefficients of s).

We have a general machine to use non-elementary algebraic geometry to bound such sums. Tools: étale cohomology, sheaves, Grothendieck-Lefschetz fixed point formula, Deligne's Weil II.

Cohomology problem

Our tools are very powerful, but they don't give us the answer for free. We need to bound the cohomology of the complement of a hyperplane arrangement, twisted by a (quadratic) representation of the fundamental group of that complement.

A similar problem was previously studied by Cohen, Dimca, and Orlik. We adapt their proof. (In the first paper, we used a slightly different method.)

This requires us to carefully study how these hyperplanes intersect.

How geometry arises from our sum

How do we get from

$$\sum_{\substack{s \in \mathbb{F}_q[T] \\ \deg s < \frac{d}{p}}} \chi(W_{G,r}(T,s))$$

to the cohomology of the complement of a hyperplane arrangement, twisted by a (quadratic) representation of π_1?

The ambient space is $\lceil \frac{d}{p} \rceil$-dimensional. Its coordinates are the coefficients of s.

The arrangement of hyperplanes are the locus where $\gcd(W_{G,r}(T,s), M_{G,r}) \neq 1$. This is a union over pairs of a root a of $M_{g,r}$ and a zero (a,b) of $W_{G,r}$ of the hyperplane where $s(a) = b$.

The fundamental group representation comes from the character χ (Lang's isogeny).