Simultaneous Prime Values of Polynomials in Positive Characteristic

Paul Pollack
Dartmouth College
paul.pollack@dartmouth.edu

January 15, 2007

PART I:
INTRODUCTION

Number Theory?

Global field: a finite extension of $\mathbf{Q}$ or $\mathbf{F}_q(T)$ for some finite field $\mathbf{F}_q$.

> It is ordinary rational arithmetic that attracts the ordinary man.
> – G. H. Hardy

What are the analogies between $\mathbf{Q}$ and $\mathbf{F}_q(T)$, or between $\mathbf{Z}$ and $\mathbf{F}_q[T]$?

A Partial Dictionary Between $\mathbf{Z}$ and $\mathbf{F}_q[T]$

Primes $\Longleftrightarrow$ Irreducibles

Positive integers $\Longleftrightarrow$ Monic Polynomials

$\{\pm 1\} \Longleftrightarrow \mathbf{F}_q[T]^\times = \mathbf{F}_q^\times$

Usual absolute value $\Longleftrightarrow |f| = q^{\deg f}$

Observe

$$\#\mathbf{Z}/n\mathbf{Z} = |n| \quad \text{and} \quad \#\mathbf{F}_q[T]/(p(T)) = |p(T)|.$$

An Assortment of Analogies

Two Squares Theorem (Leahey): Suppose the monic polynomial $A \in \mathbf{F}_q[T]$ factors as

$$A = P_1^{e_1} P_2^{e_2} \ldots P_k^{e_k},$$

where the P_i are distinct monic primes. Then A is a sum of two squares if and only if e_i is even for every prime P_i with $|P_i| \equiv 3 \pmod 4$.

Fermat's Last Theorem: Let $n \geq 3$. Consider the equation $A^n + B^n = C^n$, with all $A, B, C \in \mathbf{F}_q[T]$. Should assume n is prime to the characteristic of $\mathbf{F}_q$, since

$$(A + B)^p = A^p + B^p$$

modulo p. With this assumption, in any solution (A, B, C) to the Fermat equation with $ABC \neq 0$, all of A, B and C are constant polynomials.

Perfect Polynomials

For a polynomial A over $\mathbf{F}_2$, define

$$\sigma(A) = \sum_{D|A} D,$$

where the sum is taken over the monic divisors of A. For example,

$$\sigma(T^2) = 1 + T + T^2.$$

Call a polynomial *perfect* if

$$\sigma(A) = A.$$

For example, $T^2 + T$ is perfect since

$$\begin{aligned}\sigma(T^2 + T) &= 1 + T + (T + 1) + T^2 + T \\ &= T^2 + T.\end{aligned}$$

Theorem. *If A is a perfect polynomial and A splits over $\mathbf{F}_2$, then A has the form*

$$A = (T(T+1))^{2^n-1}$$

for some positive integer n. Conversely, for any such n the polynomial A defined this way is perfect.

Proof of sufficiency. For A defined as above,

$$\sigma(A) = \sigma(T^{2^n-1})\sigma((T+1)^{2^n-1}).$$

Now

$$\sigma(T^{2^n-1}) = 1 + T + \cdots + T^{2^n-1} = \frac{T^{2^n}-1}{T-1}$$
$$= \frac{(T-1)^{2^n}}{T-1} = (T-1)^{2^n-1}.$$

Similarly, $\sigma((T+1)^{2^n-1}) = T^{2^n-1}$. $\square$

Known Nonsplitting Perfect Polynomials

Deg	Factorization into Irreducibles
5	$T(T+1)^2(T^2+T+1)$
	$T^2(T+1)(T^2+T+1)$
11	$T(T+1)^2(T^2+T+1)^2(T^4+T+1)$
	$T^2(T+1)(T^2+T+1)^2(T^4+T+1)$
	$T^3(T+1)^4(T^4+T^3+1)$
	$T^4(T+1)^3(T^4+T^3+T^2+T+1)$
15	$T^3(T+1)^6(T^3+T+1)(T^3+T^2+1)$
	$T^6(T+1)^3(T^3+T+1)(T^3+T^2+1)$
16	$T^4(T+1)^4(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
20	$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
	$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1)$

Open problem: Is every perfect polynomial divisible by $T(T+1)$?

Such a polynomial is necessarily a perfect square and has at least 4 distinct prime divisors and 10 prime divisors counted with multiplicity.

Distribution of Primes in $\mathbf{F}_q[T]$

Consider the case $q = 2$, i.e., $\mathbf{Z}/2\mathbf{Z}$.

Degree	# of Primes	Proportion
5	6	.1875
6	9	.140625
7	18	.140625
8	30	.1171875
9	56	.109375
10	99	.09667968750
11	186	.09082031250
12	335	.08178710938
13	630	.07690429688
14	1161	.07086181641
15	2182	.06658935547
16	4080	.06225585938
17	7710	.05882263184
18	14532	.05543518066
19	27594	.05263137817
20	52377	.04995059967

The Prime Number Theorem for $\mathbf{F}_q[T]$

An Easy Proof: For every $m \geq 1$,

$$T^{q^m} - T = \prod_{\substack{\deg P \mid m \\ P \text{ monic prime}}} P.$$

Let π_d be the number of monic primes of degree d.

Comparing degrees in the above factorization,

$$q^m = \sum_{d \mid m} d\pi_d;$$

inverting,

$$\pi_m = \frac{1}{m} \sum_{d \mid m} q^d \mu(m/d),$$

a formula already known to Gauss.

The largest contribution to the right hand side occurs for $d = 1$, and we obtain

$$\pi_m = \frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right).$$

A Hard Proof

Define

$$\zeta_q(s) = \sum_{A \text{ monic}} \frac{1}{|A|^s}.$$

Then $\zeta_q(s)$ converges absolutely for $\Re(s) > 1$, and in the same domain has the product expansion

$$\zeta_q(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1}.$$

For $\Re(s) > 1$,

$$\zeta_q(s) = \sum_{n=1}^{\infty} \sum_{\substack{A \text{ monic} \\ \deg A = n}} \frac{1}{q^{ns}} = \sum_{n=1}^{\infty} \frac{q^n}{q^{ns}} = \frac{1}{1 - qq^{-s}}.$$

We now compute the logarithm of $\zeta_q(s)$ in two different ways. Let π_n denote the number of monic primes of degree n.

On the one hand,

$$\begin{aligned}\log \zeta_q(s) &= \log \frac{1}{1 - qq^{-s}} \\ &= qq^{-s} + \frac{q^2}{2} q^{-2s} + \frac{q^3}{3} q^{-3s} + \dots \\ &= \sum_{m=1}^{\infty} \frac{q^m}{m} q^{-ms}.\end{aligned}$$

But we can also take the logarithm of the Euler product to find

$$\begin{aligned}
\log \zeta_q(s) &= \log \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} \\
&= \sum_P \left(\frac{1}{|P|^s} + \frac{1}{2|P|^{2s}} + \dots\right) \\
&= \sum_{n=1}^{\infty} \pi_n \left(q^{-ns} + \frac{1}{2} q^{-2ns} + \dots\right) \\
&= \sum_{n=1}^{\infty} \pi_n \sum_{r=1}^{\infty} r^{-1} q^{-rns} \\
&= \sum_{m=1}^{\infty} q^{-ms} \sum_{rn=m} \pi_n r^{-1} \\
&= \sum_{m=1}^{\infty} \frac{q^{-ms}}{m} \sum_{d|m} d\pi_d.
\end{aligned}$$

So we have both

$$\log \zeta_q(s) = \sum_{m=1}^{\infty} q^m \frac{q^{-ms}}{m}$$

and

$$\log \zeta_q(s) = \sum_{m=1}^{\infty} \left(\sum_{d|m} d\pi_d \right) \frac{q^{-ms}}{m}.$$

Comparing coefficients, we see

$$\sum_{d|m} d\pi_d = q^m,$$

and we can proceed as before.

Riemann Hypothesis for Function Fields (Weil)

Write $T = q^{-s}$. Then we obtained

$$\zeta_q(s) = \frac{1}{1 - qq^{-s}} = \frac{1}{1 - qT}.$$

Actually, factoring in the infinite prime,

$$\zeta_{\mathbf{F}_q(u)}(s) = \frac{1}{(1-T)(1-qT)}.$$

In general, if $K/\mathbf{F}_q(u)$ is a global function field, then

$$\zeta_K(s) = \frac{L(T)}{(1-T)(1-qT)}$$

for some integral polynomial $L(T)$ which factors as

$$L(T) = (1 - \alpha_1 T) \dots (1 - \alpha_{2g} T).$$

Here g is the *genus* of K, and $\alpha_1, \dots, \alpha_{2g}$ are complex numbers of absolute value $\sqrt{q}$.

Theorem (Kornblum). *Suppose* $A \pmod{M}$ *is a coprime congruence class in* $\mathbf{F}_q[T]$. *Then there are infinitely many monic primes* $P \equiv A \pmod{M}$.

Need to know $L(s, \chi)$ is nonvanishing at $s = 1$.

Theorem. *Suppose* $A \pmod{M}$ *is a coprime congruence class in* $\mathbf{F}_q[T]$. *Then the number of primes* $P \equiv A \pmod{M}$ *of degree* d *is*

$$\frac{q^d}{d\phi(M)} + O(q^{d/2}(\deg M + 1)/d).$$

We can understand the zeros of $L(s, \chi)$ because $L(s, \chi)$ is a factor of $\zeta_K(s)$ for an appropriate K.

PART II:
THE VINDICATION OF FERMAT

Fermat to Frenicle, 1640:

But here is what I admire the most: that I am almost persuaded that all the progressive numbers augmented by one, for which the exponents are the members of the double progression, are prime numbers, such as

$$3, 5, 17, 257, 65537, 4294967297$$

and the following with 20 digits

$$18446744073709551617; \text{etc.}$$

I do not have the exact proof, but I have excluded such a large number of divisors by infallible proofs, and I have such a strong insight, which is the foundation of my thought, that it would be hard for me to retract it.

Euler (1732):

$$2^{2^5} + 1 = 4294967297 = 641 \times 6700417.$$

Theorem: $F_n := 2^{2^n} + 1$ is composite for $5 \leq n \leq 32$, and many other values of n (e.g., $n = 2478782$).

Folklore Conjecture: F_n is composite whenever $n > 4$: in other words, Fermat was as wrong as he could be!

Theorem (Capelli's Theorem). *Let F be any field. The binomial $T^m - a$ is reducible over F if and only if either of the following holds:*

- *there is a prime l dividing m for which a is an lth power in F,*
- *4 divides m and $a = -4b^4$ for some b in F.*

Example (vindication of Fermat): The cubes in $\mathbf{F}_7 = \mathbf{Z}/7\mathbf{Z}$ are $-1, 0, 1$. So by Capelli's theorem,

$$T^{3^k} - 2$$

is irreducible over $\mathbf{F}_7$ for $k = 0, 1, 2, 3, \ldots$.

Similarly, $T^{3^k} - 3$ is always irreducible. Hence:

$$T^{3^k} - 2, \quad T^{3^k} - 3$$

is a pair of prime polynomials over $\mathbf{F}_7$ differing by 1 for every k.

Twin Prime Theorem (Hall). *If $q > 3$, then there are infinitely many monic twin prime pairs $f, f+1$ in $\mathbf{F}_q[T]$.*

Idea: if possible, choose an odd prime $l \mid (q-1)$. Then one can find a pair of consecutive non l-th powers $\alpha, \alpha+1$. Look at

$$T^{l^k} - \alpha, \quad T^{l^k} - (\alpha+1) \quad (k = 0, 1, 2, \dots).$$

If not possible, then $4 \mid (q-1)$ and do the same with $l = 2$.

More on this last case...

If $q-1$ is a power of 2, then either

- q is a prime (so a Fermat prime), or
- $q = 9$.

Latter case: Find a paper of nonresidues directly.

Former case: Can argue with quadratic reciprocity (use the pair $5, 6$) – or one can use a character sum estimate.

Two questions of Hall:

1. What about twin prime pairs over $\mathbf{F}_3$?

2. What about different families of twin prime pairs? For example, what if one wants twin prime pairs of odd degree?

A Corollary of Capelli's Theorem

Lemma (Serret, Dickson)**.** *Let $f(T)$ be an irreducible polynomial over $\mathbf{F}_q$ of degree d. Let α be a root of f inside the splitting field $\mathbf{F}_{q^d}$ of f. If l is an odd prime for which α is not an lth power in $\mathbf{F}_{q^d}$, then each of the substitutions*

$$T \mapsto T^{l^k}, \quad k = 1, 2, 3, \ldots$$

preserves the irreducibility of f. The same holds if $l = 2$, provided $q^d \equiv 1 \pmod 4$.

Twin Prime Polynomials over $\mathbf{F}_3$

Begin with the twin prime pair

$$T^3 - T + 1, \quad T^3 - T + 2.$$

The splitting field of both polynomials is $\mathbf{F}_{3^3}$. Neither polynomial has a root which is a 13th power in $\mathbf{F}_{3^3}$, and so

$$T^{3 \cdot 13^k} - T^{13^k} + 1, \quad T^{3 \cdot 13^k} - T^{13^k} + 2$$

is a twin prime pair for each $k = 0, 1, 2, \ldots$.

Two-step Strategy:

1. Find a configuration of power nonresidues by either combinatorial or analytic means – this accounts for all but finitely many exceptional cases.

2. Enumerate the exceptional cases and treat them directly. This step involves some trial and error.

Theorem (Extended Twin Prime Theorem). *If* $\#\mathbf{F}_q > 2$*, and if* α *is any nonzero element of* $\mathbf{F}_q$*, then there are infinitely many monic twin prime pairs* $P, P + \alpha$*.*

Remark: The analogous theorem is also true for prime triples $P, P + \alpha, P + \beta$ for $q > 3$.

It appears much more difficult to handle "twin prime pairs" with *nonconstant difference*.

For example, the following tantalizing problem remains open:

Question: Are there infinitely many prime pairs

$$P, P + T^2 + T$$

in $\mathbf{F}_2[T]$?

Henceforth we restrict our attention to problems of "Hypothesis H" type where the polynomials have $\mathbf{F}_q$-coefficients.

An Analogue of Schinzel's Hypothesis H for Polynomials with $\mathbf{F}_q$ Coefficients. *Suppose $f_1, \ldots, f_r$ are irreducible polynomials in $\mathbf{F}_q[T]$ and that there is no prime π of $\mathbf{F}_q[T]$ for which the map*

$$g(T) \mapsto f_1(g(T)) \cdots f_r(g(T)) \pmod{\pi}$$

is identically zero. Then there are infinitely many substitutions

$$T \mapsto g(T)$$

which preserve the simultaneous irreducibility of the f_i.

Example: Includes the case of twin prime pairs $T, T+\alpha$.

Example: Suppose $f(T) = T^2+1$ is irreducible over $\mathbf{F}_q$. Then we expect infinitely many $g \in \mathbf{F}_q[T]$ for which g^2+1 is irreducible.

The Constant-Coefficient Hypothesis H is True for "large q":

Theorem (P, 2006)**.** *Suppose $f_1, \ldots, f_r$ are irreducible polynomials in $\mathbf{F}_q[T]$. Then there are infinitely many substitutions*

$$T \mapsto g(T)$$

which leave the f_i simultaneously irreducible provided q is sufficiently large, depending only on r and the degrees of the f_i.

Remark: The substitutions produced have the "Fermat" form

$$g(T) = T^{l^k} - \beta \quad (\text{for } k = 1, 2, 3, \ldots)$$

for a fixed prime l and a fixed $\beta \in \mathbf{F}_q$.

Example: Primes One More Than A Square

Let $f(T) = T^2 + 1$, and suppose $f(T)$ is irreducible over $\mathbf{F}_q$, so that $q \equiv 3 \pmod 4$. Fix a root i of $T^2 + 1$ from $\mathbf{F}_{q^2}$.

We look for a prime l and a $\beta \in \mathbf{F}_q$ so that $f(T - \beta)$ remains irreducible if T is replaced by T^{l^k} for $k = 1, 2, 3, \ldots$.

Suffices to find $\beta \in \mathbf{F}_q$ so that $\beta + i$ is a non-lth power.

Choose any prime l dividing $q^2 - 1$, and let let χ be an lth power-residue character on $\mathbf{F}_{q^2}$. If there is no such β, then

$$\sum_{\beta \in \mathbf{F}_q} \chi(\beta + i) = q.$$

But in fact, Weil's Riemann Hypothesis gives a bound for this incomplete character sum of $\sqrt{q}$, a contradiction.

Lemma. *Let $f_1(T), \ldots, f_s(T)$ be pairwise nonassociated irreducible polynomials over $\mathbf{F}_q$. Fix roots*

$$\alpha_1, \ldots, \alpha_s$$

of $f_1, \ldots, f_s$ respectively lying in an algebraic closure of $\mathbf{F}_q$. Suppose that for each $1 \leq i \leq s$ we have a character χ_i of $\mathbf{F}_q(\alpha_i)$ and that at least one of these χ_i is nontrivial. Then

$$\left| \sum_{\beta \in \mathbf{F}_q} \chi_1(\alpha_1 + \beta) \cdots \chi_s(\alpha_s + \beta) \right| \leq (D-1)\sqrt{q},$$

where D is the sum of the degrees of the f_i.

PART III: APPLICATIONS OF THE CHEBOTAREV DENSITY THEOREM

Return to Hall's question:

Are there infinitely many twin prime pairs $f, f+1$ of odd degree over $\mathbf{F}_q$, with $q > 2$?

May assume $q-1$ is a power of 2, so $q = 9$ or a Fermat prime.

Strategy (for large q):

1. Choose a degree 3 twin prime pair $f, f+1$ over $\mathbf{F}_q$.

2. Bootstrap this pair by the usual process: find an odd prime l and a $\beta \in \mathbf{F}_q$ so that the substitutions $T \mapsto T^{l^k} - \beta$ preserve irreducibility.

Step 2 is relatively easy. But is Step 1 possible?

Conjecture (Chowla, 1966). *Fix a positive integer* n. *Then for all large primes* p, *there is always an irreducible polynomial in* $\mathbf{F}_p[T]$ *of the form* $T^n + T + a$ *with* $a \in \mathbf{F}_p$.

In fact, for fixed n *the number of such* a *is asymptotic to* p/n *as* $p \to \infty$.

Proved by Cohen and Ree independently in 1970:

Idea: Consider the extension K of $\mathbf{F}_q(u)$ obtained by adjoining a root of $T^n + T - u$.

For each $a \in \mathbf{F}_q$, one has a first-degree prime P_a of $\mathbf{F}_q(u)$ corresponding to the $u - a$-adic valuation.

Kummer-Dedekind: Assume $p \nmid n(n-1)$. Then for all but $O(n)$ primes P_a, the factorization of $T^n + T - a$ over $\mathbf{F}_q$ mirrors the factorization of the prime P_a in the extension K.

In particular, $T^n + T - a$ is irreducible over $\mathbf{F}_q$ if and only if P_a is inert.

Let M be the Galois closure of K.

Understanding the Galois Group of M/K

Lemma. *Let h be a polynomial of degree $n \geq 2$ with coefficients from a finite field F whose characteristic is prime to n. Suppose that with u an indeterminate over F, we have*

$$\mathrm{disc}_u \mathrm{disc}_T(h(T) - u) \neq 0. \qquad (1)$$

Then the Galois group of $h(T) - u$ over the rational function field $\overline{F}(u)$ is the full symmetric group on the n roots of $h(T) - u$. Consequently, if E is any algebraic extension of F, then the Galois group of $h(T) - u$ over $E(u)$ is also the full symmetric group.

Corollary. *As long as $p \nmid n(n-1)$, the extension $M/\mathbf{F}_q(u)$ is geometric (has $\mathbf{F}_q$ as its full field of constants) and Galois group the full symmetric group of n letters.*

Lemma. *Suppose P is unramified in M. Then P is inert if and only if its associated Frobenius conjugacy class is an n-cycle.*

Now we appeal to an explicit version of the Chebotarev density theorem.

The proportion of n-cycles in the full symmetric group on n letters is $1/n$, and this proves Chowla's conjecture.

An Explicit Chebotarev Density Theorem for First Degree Primes. *Suppose* $M/\mathbf{F}_q(u)$ *is a finite Galois extension having full field of constants* $\mathbf{F}_{q^D}$. *Let* $\mathcal{C}$ *be a conjugacy class of* Gal$(M/\mathbf{F}_q(u))$ *every element of which restricts down to the* q*th power map on* $\mathbf{F}_{q^D}$.

Let $\mathcal{P}$ *be the set of first degree primes* P *of* $\mathbf{F}_q(u)$ *unramified in* M *for which*

$$\left(\frac{M/\mathbf{F}_q(u)}{P}\right) = \mathcal{C}.$$

Then

$$\left|\#\mathcal{P} - \frac{\#C}{[M:\mathbf{F}_{q^D}(u)]}q\right| \leq 2\frac{\#C}{[M:\mathbf{F}_{q^D}(u)]}(gq^{1/2} + g + [M:\mathbf{F}_{q^D}(u)]),$$

where g *denotes the genus of* $M/\mathbf{F}_{q^D}$.

To get our twin prime pairs of degree 3, we apply the same techniques to get a pair of irreducibles

$$T^3 + T + a, \quad T^3 + T + (a + 1)$$

over large finite fields $\mathbf{F}_q$ with $\gcd(q, 6) = 1$.

Example: Return to $f^2 + 1$

Suppose $q \equiv 3 \pmod 4$. Observe that

$$g(T)^2 + 1 \text{ is irreducible over } \mathbf{F}_q \Longleftrightarrow$$
$$g(T) + i \text{ is irreducible over } \mathbf{F}_q(i) = \mathbf{F}_{q^2}.$$

Suppose $g(T)$ is monic of degree n and has the form

$$T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + const,$$

where $a_{n-1}, \ldots, a_1$ are prescribed.

Adjoin a root of

$$T^n + a_{n-1}T^{n-1} + \cdots + a_1 T - u + i$$

to $\mathbf{F}_{q^2}(u)$, and look at the Galois closure over $\mathbf{F}_q(u)$.

$$
\begin{tikzcd}
 & M \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 & & L_2 \\
K_1 \arrow[u, dash] & & K_2 \arrow[u, dash] \\
 & \mathbf{F}_{q^2}(u) \arrow[ul, dash] \arrow[ur, dash] & \\
 & \mathbf{F}_q(u) \arrow[u, dash] &
\end{tikzcd}
$$

$K_1 =$ field obtained by adjoining a root of $T^n + \cdots + a_1 T - u + i$ to $\mathbf{F}_{q^2}(u)$.

$K_2 =$ field obtained by adjoining a root of $T^n + \cdots + a_1 T - u - i$ to $\mathbf{F}_{q^2}(u)$.

$L_i =$ Galois closure of K_i over $\mathbf{F}_{q^2}(u)$.

$M =$ compositum of L_1 and L_2.

Theorem (P, 2006). *Let n be a positive integer. Let $f_1(T), \ldots, f_r(T)$ be pairwise nonassociated irreducible polynomials over $\mathbf{F}_q$ with the degree of the product $f_1 \cdots f_r$ bounded by B.*

The number of univariate monic polynomials h of degree n for which all of $f_1(h(T)), \ldots, f_r(h(T))$ are irreducible over $\mathbf{F}_q$ is

$$q^n/n^r + O_{n,B}(q^{n-1/2})$$

provided $\text{gcd}(q, 2n) = 1$.

A Quantitative Hypothesis H for Polynomials with $\mathbf{F}_q$ Coefficients. *Let $f_1(T), \ldots, f_r(T)$ be nonassociated polynomials over $\mathbf{F}_q$ satisfying the conditions of Hypothesis H. Then*

$$\#\{h(T) : h \textit{ monic}, \ \deg h = n, \\ \textit{and } f_1(h(T)), \ldots, f_r(h(T)) \textit{ are all prime}\} \sim \\ \mathfrak{S}(f_1, \ldots, f_r) \frac{1}{\prod_{i=1}^{r} \deg f_i} \frac{q^n}{n^r} \quad \textit{as } n \to \infty.$$

Here the local factor $\mathfrak{S}(f_1, \ldots, f_r)$ is defined by

$$\mathfrak{S}(f_1, \ldots, f_r) := \\ \prod_{n=1}^{\infty} \prod_{\substack{\deg \pi = n \\ \pi \textit{ monic prime of } \mathbf{F}_q[T]}} \frac{1 - \omega(\pi)/q^n}{(1 - 1/q^n)^r},$$

where

$$\omega(\pi) := \\ \#\{a \bmod \pi : f_1(a) \cdots f_r(a) \equiv 0 \pmod{\pi}\}.$$

Theorem. *Let* $f_1(T), \ldots, f_r(T)$ *be nonassociated irreducibles over* $\mathbf{F}_q$ *with the degree of* $f_1 \cdots f_r$ *bounded by* B*. Let* $a \bmod m$ *be an arbitrary infinite arithmetic progression of integers.*

If the finite field $\mathbf{F}_q$ *is sufficiently large, depending just on* m*,* r*, and* B*, and if* q *is prime to* $2\gcd(a, m)$*, then there are infinitely many univariate monic polynomials* h *over* $\mathbf{F}_q$ *with*

$$\deg h \equiv a \pmod{m} \quad \textit{and}$$
$$f_1(h(T)), \ldots, f_r(h(T)) \textit{ all irreducible over } \mathbf{F}_q.$$

PART IV: VISTAS

Bunyakovsky's Conjecture (constant coefficient case)

Conjecture. *Let $f(T)$ be an irreducible polynomial over $\mathbf{F}_q$. Then there are infinitely many monic $g(T)$ over $\mathbf{F}_q$ with $f(g(T))$ irreducible.*

Remark: The number of roots of f modulo $f(T)$ is at most $\deg f$, which is less than $|f| = q^{\deg f}$.

The conjecture holds when q is large compared to $\deg f$.

What about q fixed?

Fix $\mathbf{F}_q$. Given d, let L be the largest odd squarefree divisor of $q^d - 1$.

The number of polynomials of degree d over $\mathbf{F}_q$ for which no substitution $T \mapsto T^{l^k}$ preserves irreducibility is

$$\ll \frac{1}{L}\frac{q^d}{d}.$$

Moreover,

$$L \gg d \qquad \text{(Bang's Theorem)},$$
$$L \gg d^{3+o(1)} \qquad \text{(Stewart \& Yu)},$$
$$L \gg_\epsilon q^{d/(1+\epsilon)-1} \qquad \text{(on ABC)}.$$

So as $d \to \infty$, "almost all" polynomials of degree d fit Bunyakowsky's conjecture!

But even more is true...

Call a prime l a q-Wieferich prime if

$$q^{l-1} \equiv 1 \pmod{l^2}.$$

Assume:

$$\sum_{l \ q-\text{Wieferich}} \frac{1}{\text{ord}_l(q)} < \infty.$$

Then for almost all d, the following holds:

For *every* irreducible polynomial of degree d, we can find an odd prime l dividing $q^d - 1$ for which all the substitutions $T \mapsto T^{l^k}$ preserve irreducibility.

Recall our twin prime pairs over $\mathbf{F}_3$.

Had cubic polynomials over $\mathbf{F}_3$ which we wanted to show remained irreducible under substitutions $T \mapsto T^{13^k}$. Took a root α.

If not, then α is a 13th power, so

$$1 = \alpha^{\frac{27-1}{13}} = \alpha^2.$$

Thus $\alpha^3 = \alpha$. So α wasn't a root of an irreducible cubic!

In the same way, we get a contradiction whenever

$$\mathrm{ord}_{\frac{q^d-1}{L}} q < d,$$

and this happens for almost all d under our hypothesis.

A Twin Prime Conjecture and a Lightweight Analogue

Conjecture. *Let D be a polynomial in $\mathbf{F}_q[T]$, assumed divisible by $T(T+1)$ in the case when $q = 2$. Then there are infinitely many monic prime pairs $P, P+D$.*

This seems difficult. If we measure size by "weight" instead of degree, we get a more attackable problem.

Say that a polynomial A has *weight* k if k is the number of nonzero coefficients of A.

A (Light)weight Twin Prime Conjecture. *Fix a finite field* $\mathbf{F}_q$. *For each integer* $s \geq 0$, *there are infinitely many pairs of primes* P_1, P_2 *over* $\mathbf{F}_q$ *for which* $P_2 - P_1$ *has weight* s, *where* s *is assumed even in the case* $q = 2$.

It seems this can be settled using our bootstrapping method and estimates for the exceptional set in Goldbach-type problems for $\mathbf{F}_q(u)$.

Other Applications of the Chebotarev Density method

1. **Binary Forms:**

   Example: Let $F(X,Y)$ denote an irreducible binary form with $\mathbf{F}_q$ coefficients. For fixed m and $q \to \infty$ (with restrictions), probably one can count the number of X, Y of degree m for which $F(X,Y)$ is prime.

2. **Higher Degree Forms?**

   Example: In characteristic > 3, there are infinitely many primes in $\mathbf{F}_q[u]$ which are strict sums of three prime cubes.

3. **Anything else interesting?**

   Example: It seems one can show that in characteristic > 3, there are infinitely many primes of the form $4A^3 + 27B^2$. As a corollary, there are infinitely many elliptic curves over $\mathbf{F}_q(u)$ with prime conductor.

To what extent can one unify all these results?

Concluding Homage to Fermat

Can study Fermat primes for their own sake. Try to classify tuples $(\mathbf{F}_q,\ A, B, m)$ for which

$$A^{m^k} - B$$

is irreducible over $\mathbf{F}_q$ for each $k \gg 0$.

Familiar example: $T^{3^k} - 2$ over $\mathbf{F}_7$.

Less-familiar example: $(T^3 - 2)^{3^k} - 2$ over $\mathbf{F}_7$. Proof uses cubic reciprocity in $\mathbf{F}_7[T]$.