Prime Polynomial Patterns

Paul Pollack
Québec-Vermont Number Theory Seminar

April 26, 2007

PART I

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

Classical Two Squares Theorem (Fermat): Let n be a positive integer and write

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

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

Polynomial Two Squares Theorem (Leahey): Fix a finite field $\mathbf{F}_q$ with q odd. 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 $|P_i| \equiv 3 \pmod 4$.

Classical Fermat's Last Theorem: Let $n \geq 3$. Then the equation

$$A^n + B^n = C^n$$

has no nontrivial solutions (i.e., solutions with $ABC \neq 0$).

Polynomial 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 all 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 $T(T+1)$?

A counterexample is necessarily a perfect square and has at least 4 distinct prime divisors and 10 prime divisors counted with multiplicity. It also has degree ≥ 66.

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	.18750000000
6	9	.14062500000
7	18	.14062500000
8	30	.11718750000
9	56	.10937500000
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

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

Let π_d be the number of primes of degree d over $\mathbf{F}_2$.

Theorem. *As $d \to \infty$, the proportion of primes of degree d is asymptotic to $1/d$. In other words,*

$$\pi_d \sim 2^d/d \quad \text{as } d \to \infty.$$

Same theorem holds over $\mathbf{F}_q$ for all q (provided we change 2 to q and count only monics).

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,

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

inverting,

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

a formula already known to Gauss.

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

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

If we write $x = q^m$, then

$$\pi_m = \frac{x}{\log_q x} + O\left(\frac{x^{1/2}}{\log_q x}\right),$$

which bears a striking similarity to the classical prime number theorem.

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 $\Re(s) > 1$,

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

Thus if $u = q^{-s}$, we have

$$\zeta_q(s) = \frac{1}{1 - qu}.$$

We rewrite the Euler product expansion

$$\zeta_q(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} = \prod_{d=1}^{\infty} \prod_{\deg P = d} \left(1 - u^d\right)^{-1}$$

$$= \prod_{d=1}^{\infty} (1 - u^d)^{-\pi_d}.$$

Thus

$$\zeta_q(s) = \frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-\pi_d}.$$

Taking the logarithmic derivative of both sides of the identity

$$\frac{1}{1-qu} = \prod_{d=1}^{\infty} (1-u^d)^{-\pi_d}$$

and multiplying by u, we find

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} d\pi_d \frac{u^d}{1-u^d}.$$

Expand both sides into geometric series and compare the coefficients of u^m: this gives

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

and now we proceed as before.

Riemann Hypothesis for Function Fields (Weil)

So far we have obtained

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

Actually, factoring in the infinite prime,

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

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

$$\zeta_K(s) = \frac{L(u)}{(1-u)(1-qu)}$$

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

$$L(u) = (1 - \alpha_1 u) \ldots (1 - \alpha_{2g} u).$$

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

PART II

Hypothesis H (Schinzel, 1958). *Suppose that* $f_1(T)$, ..., $f_r(T)$ *are irreducible polynomials in* $\mathbf{Z}[T]$ *and that there is no prime* p *for which the congruence*

$$f_1(n)f_2(n)\cdots f_r(n) \equiv 0 \pmod{p}$$

holds for every integer n. *Then there are infinitely many positive integers* n *for which*

$$f_1(n), \ldots, f_r(n)$$

are simultaneously prime.

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*

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

is identically zero. Then there are infinitely many substitutions

$$T \mapsto h(T)$$

which preserve the simultaneous irreducibility of the f_i.

Example: "Twin prime" pairs: take $f_1(T) := T$ and $f_2(T) := T + 1$.

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.*

Observe: We have

$$x^4 + 4y^4 = (x^2 + 2y^2)^2 - (2xy)^2.$$

Example: 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 $\mathbf{F}_q[T]$.*

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

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

$$T \mapsto h(T)$$

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

Example: The single polynomial $T^2 + 1$ (so that $r = 1, \deg f_1 = 2$):

Corollary. *There are infinitely many prime polynomials of the form* $h^2 + 1$ *over every* $\mathbf{F}_q$ *for which* $q \equiv 3 \pmod 4$.

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.

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*

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

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

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

where

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

Theorem (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 $\gcd(q, 2n) = 1$.

Brun's Constant for Twin Prime Polynomials

For every finite field $\mathbf{F}_q$, define

$$B_q = \sum \frac{1}{|P|},$$

where the sum is taken over those monic P for which P and $P+1$ are both prime in $\mathbf{F}_q[T]$.

Theorem (Webb, Hsu)**.** *For every finite field $\mathbf{F}_q$, we have $B_q < \infty$.*

Theorem (P). *As $p \to \infty$ (through prime values),*

$$B_p \to \pi^2/6.$$

Sketch of proof: Write

$$B_p = \sum_{\text{small } n} \sum_{\deg P = n} \frac{1}{|P|} + \sum_{\text{large } n} \sum_{\deg P = n} \frac{1}{|P|}.$$

For small n:

$$\sum_{\deg P = n} \frac{1}{|P|} = \frac{1}{p^n}(1 + o(1)) \left(\frac{p^n}{n^2}\right) \sim \frac{1}{n^2}.$$

For large n sieves give:

$$\sum_{\deg P = n} \frac{1}{|P|} \ll \frac{1}{p^n} \left(\frac{p^n}{n^2}\right) = \frac{1}{n^2}.$$

A Conjecture of Chowla

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 Ree and Cohen (independently) in 1971.

Idea: For most a, the polynomial $T^n + T - a$ factors over $\mathbf{F}_q$ the same way as the prime $u - a$ of $\mathbf{F}_q(u)$ factors over the field obtained by adjoining a root of $T^n + T - u$ over $\mathbf{F}_q(u)$. Now use Chebotarev.

A Substitute for Hilbert Irreducibility

Let $k = \mathbf{F}_q$ be a finite field of characteristic p.
Theorem. *Let $f(T,u)$ be an absolutely irreducible polynomial in $k[T,u]$ which is monic in T of T-degree n, where $p \nmid n$. Let K be the splitting field of $f(T,u)$ over $\overline{k}(u)$, and let $\bar{K} = K\overline{k}$ be the splitting field of $f(T,u)$ over $\overline{k}(u)$. Suppose that*

(i) $\mathfrak{p}_\infty$ is tamely ramified in $\bar{K}/\bar{k}(u)$,

(ii) for each $\beta \in \bar{k}$, the polynomial $f(T,\beta)$ has at most one multiple root, which is then a root of exact multiplicity 2.

Then $f(T,a)$ is irreducible over k for at least $q/n + O(q^{1/2})$ values of a in k.

Application

Theorem. *If $\mathbf{F}_q$ is a finite field with characteristic > 3, then infinitely many monic primes P over $\mathbf{F}_q$ have a representation in the form*

$$P = A^3 + B^3 + C^3,$$

where A, B, C are monic and

$$\deg A > \max\{\deg B, \deg C\}.$$

Remark: By the same method, one can prove the same theorem even we insist A, B, C are also prime!

Proof sketch: Find an $a \in \mathbf{F}_q$ for which

$$P(T) = T^3 + (T+1)^3 + (T^2 + a)^3$$

is irreducible. (Guaranteed for most $q \gg 0$ by irreducibility theorem.)

Then for any $g(T)$, have

$$P(g(T)) = \\ g(T)^3 + (g(T)+1)^3 + (g(T)^2 + a)^3.$$

If $q \gg 0$, there are infinitely many $g(T)$ for which $P(g(T))$ is prime.