Prime numbers and prime polynomials

Paul Pollack
Dartmouth College

May 1, 2008

Analogies everywhere!

- Analogies in elementary number theory (continued fractions, quadratic reciprocity, Fermat's last theorem)

- Analogies in algebraic number theory (the theory of global function fields vs. the theory of algebraic number fields)

- Analogies in analytic number theory, especially prime number theory

A partial dictionary between $\mathbf{Z}$ and $\mathbf{F}_q[T]$

Primes $\longleftrightarrow$ Irreducibles

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

Positive integers $\longleftrightarrow$ Monic polynomials

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

Observe

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

Prime number theorem (Hadamard, de la Vallée Poussin)**.** *If* $\pi(x)$ *denotes the number of primes* $p \leq x$*, then*

$$\pi(x) \sim \frac{x}{\log x} \quad \textit{as } x \to \infty.$$

Prime number theorem for polynomials. *Let* $\pi(q;d)$ *denote the number of monic, degree* d *irreducibles over the finite field* $\mathbf{F}_q$*. Then as* $q^d \to \infty$*, we have*

$$\pi(q;d) \sim \frac{q^d}{d}.$$

Notice that if $X = q^d$, then $q^d/d = X/\log_q X$.

Gauss's take on the prime number theorem: Empirical observations suggest that the primes near x have a density of about $1/\log x$. So we should have

$$\pi(x) \approx \frac{1}{\log 2} + \frac{1}{\log 3} + \cdots + \frac{1}{\log x}.$$

Theorem (von Koch)**.** *If the Riemann Hypothesis is true, then*

$$\pi(x) = \sum_{2 \le n \le x} \frac{1}{\log n} + O(x^{1/2} \log x).$$

In the polynomial setting, Gauss's proof shows that

$$\left|\pi(q;d) - \frac{q^d}{d}\right| \leq 2\frac{q^{d/2}}{d}.$$

But perhaps irregularities surface if we introduce a finer count?

Let p be a prime. To each nonnegative integer in base p, we associate a polynomial in $\mathbf{F}_p[T]$,

$$a_0 + a_1 p + \cdots + a_k p^k \longleftrightarrow a_0 + a_1 T + \cdots + a_k T^k.$$

Say that f is encoded by the integer $\|f\|$.

Define $\pi_p(X)$ as the number of $n \leq x$ which encode irreducible polynomials over $\mathbf{F}_p$.

We might hope that

$$\pi_p(X) \approx \sum_{||f|| \leq x} \frac{1}{\deg f}.$$

Theorem. *If $X \geq p$, then*

$$\pi_p(X) = \sum_{||f|| \leq x} \frac{1}{\deg f} + O\left(dp^{d/2+1}\right),$$

where $p^d \leq X < p^{d+1}$.

Notice $dp^{d/2+1} \asymp_p X^{1/2} \log X$, so this is a von Koch analogue.

Proof idea: To each global function field K (finite extension of $\mathbf{F}_q(T)$) one associates a zeta function,

$$\zeta_K(s) = \sum_{\mathfrak{a} \geq 0} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}.$$

A deep theorem of Weil asserts that these zeta functions all satisfy the analogue of the Riemann Hypothesis.

Define L-functions which are sensitive to the behavior of the initial coefficients of a polynomial in $\mathbf{F}_q[T]$. The analytic properties of this L-function can then be linked to the analytic properties of $\zeta_K(s)$ for an appropriate K and the Riemann Hypothesis brought into play.

Twin primes

Twin prime conjecture. *There are infinitely many prime pairs* $p, p+2$.

Hypothesis H (Schinzel). *Let* $f_1(T), \ldots, f_r(T)$ *be nonconstant polynomials with integer coefficients and positive leading coefficients, all irreducible over* $\mathbf{Z}$. *Suppose that there is no prime* p *for which*

$$p \quad \text{divides} \quad f_1(n) \cdots f_r(n) \quad \text{for all } n.$$

Then for infinitely many positive integers n, *the specializations* $f_1(n), \ldots, f_r(n)$ *are simultaneously prime.*

Examples: Twin prime conjecture, or the infinitude of primes of the form $n^2 + 1$.

Theorem (Hall). *Suppose $q > 3$. Then there are infinitely many monic irreducibles $P(T)$ over $\mathbf{F}_q$ for which $P(T) + 1$ is also irreducible.*

Theorem (P.). *Suppose $q > 3$. Then there are infinitely many monic irreducibles $P(T)$ over $\mathbf{F}_q$ for which $P(T) + 1$ is also irreducible.*

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.

A finite field analogue of Hypothesis H. *Suppose* $f_1, \ldots, f_r$ *are irreducible polynomials in* $\mathbf{F}_q[T]$ *and that there is no irreducible* P *in* $\mathbf{F}_q[T]$ *for which*

$$P(T) \text{ always divides } f_1(h(T)) \cdots f_r(h(T)).$$

Then $f_1(h(T)), \ldots, f_r(h(T))$ *are simultaneously irreducible for infinitely many monic polynomials* $h(T) \in \mathbf{F}_q[T]$*.*

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

Observation: The local condition is always satisfied if

$$q > \sum_{i=1}^{r} \deg f_i.$$

Theorem (P.). *Suppose* $f_1, \ldots, f_r$ *are irreducible polynomials in* $\mathbf{F}_q[T]$*. Let* $D = \sum_{i=1}^{r} \deg f_i$*. If*

$$q > \max\{3, 2^{2r-2} D^2\},$$

then there are infinitely many monic polynomials $h(T)$ *for which all of* $f_1(h(T)), \ldots, f_r(h(T))$ *are simultaneously irreducible.*

Example: Primes one more than a square

Let $\mathbf{F}_q$ be a finite field without a square root of -1; i.e., with $q \equiv 3 \pmod 4$. We prove there are infinitely many irreducibles of the form $h(T)^2+1$, where $h(T)$ is monic.

Fix a square root i of -1 from the extension $\mathbf{F}_{q^2}$. We have

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

Try for $h(T)$ a binomial – say $h(T) = T^{l^k} - \beta$, with l a fixed prime.

By Capelli, it 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 Weil's Riemann Hypothesis gives a bound for this incomplete character sum of $\sqrt{q}$ – a contradiction.

Quantitative problems and results

Twin prime conjecture (quantitative version)**.** *The number of prime pairs* $p, p+2$ *with* $p \leq x$ *is asymptotically*

$$2C_2 \frac{x}{\log^2 x} \quad \textit{as } x \to \infty,$$

where $C_2 = \prod_{p>2}(1 - 1/(p-1)^2)$*.*

Can generalize to the full Hypothesis H situation (Hardy-Littlewood/Bateman-Horn).

A quantitative finite field Hypothesis H. *Let $f_1(T), \ldots, f_r(T)$ be nonassociated polynomials over $\mathbf{F}_q$ satisfying the conditions of Hypothesis H. Then*

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

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

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

where

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

Theorem. *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*

$$q^n/n^r + O((nB)n!^B q^{n-1/2})$$

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

Example: The number of monic polynomials $h(T)$ of degree 3 over $\mathbf{F}_q$ for which $h(T)^2 + 1$ is irreducible is asymptotically $q^3/3$ as $q \to \infty$ with $q \equiv 3 \pmod 4$ and $(q, 3) = 1$.

Some ideas of the proof

The inspiration:

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.

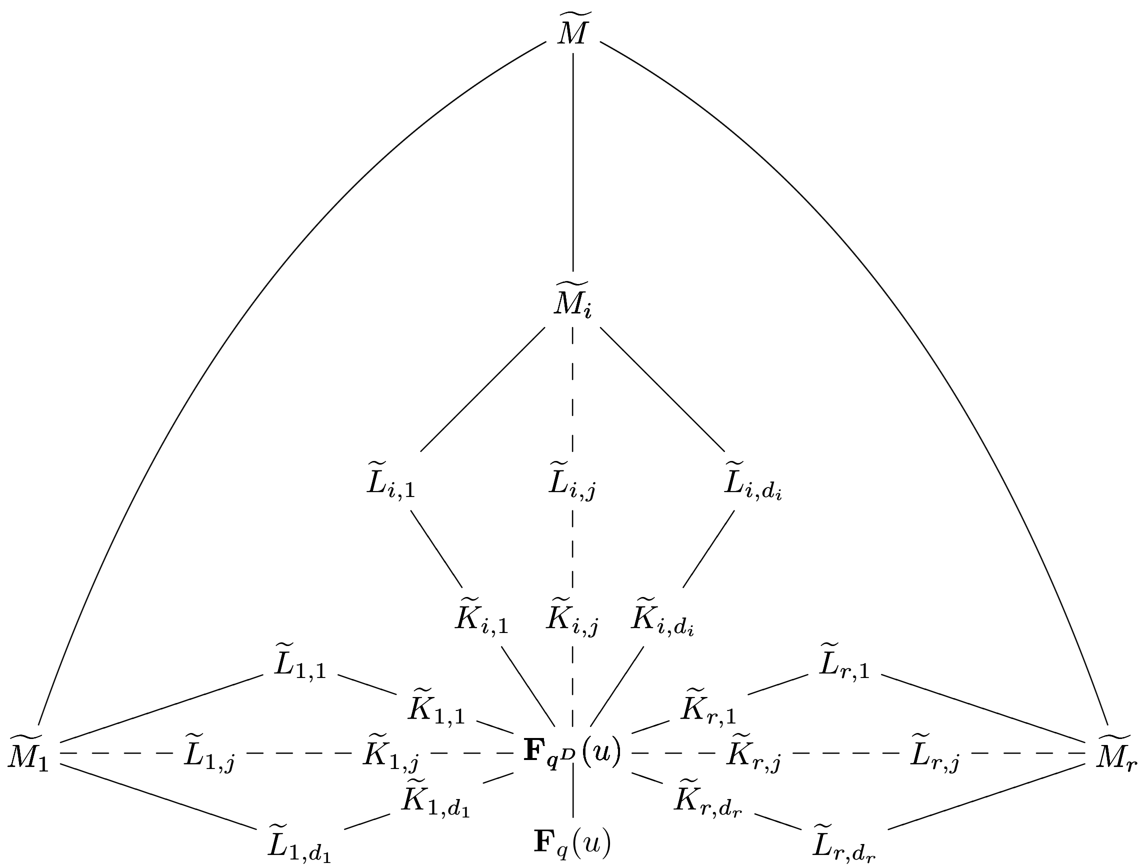
Idea of their proof:

Kummer: 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 $\mathbf{F}_q(u)$.

Chebotarev: The splitting type of primes from $\mathbf{F}_q(u)$, on average, is governed by the Galois group of the splitting field of $T^n + T - u$ over $\mathbf{F}_q(u)$. (Chebotarev.)

Birch and Swinnerton-Dyer: This splitting field is, if q is prime to $n(n-1)$, a geometric Galois extension with Galois group the full symmetric group on n letters.

The proportion of n-cycles in S_n is 1 in n, and this implies that about 1 in n polynomials of the form $T^n + T - a$, with $a \in \mathbf{F}_q$, are irreducible.


$\widetilde{M}$
$\widetilde{M}_i$
$\widetilde{L}_{i,1}$
$\widetilde{L}_{i,j}$
$\widetilde{L}_{i,d_i}$
$\widetilde{K}_{i,1}$
$\widetilde{K}_{i,j}$
$\widetilde{K}_{i,d_i}$
$\widetilde{L}_{1,1}$
$\widetilde{L}_{r,1}$
$\widetilde{K}_{1,1}$
$\widetilde{K}_{r,1}$
$\widetilde{M}_1$
$\widetilde{L}_{1,j}$
$\widetilde{K}_{1,j}$
$\mathbf{F}_{q^D}(u)$
$\widetilde{K}_{r,j}$
$\widetilde{L}_{r,j}$
$\widetilde{M}_r$
$\widetilde{K}_{1,d_1}$
$\widetilde{K}_{r,d_r}$
$\widetilde{L}_{1,d_1}$
$\mathbf{F}_q(u)$
$\widetilde{L}_{r,d_r}$

Prime gaps

Recall that the average gap between primes near N is about $\log N$.

Conjecture (Primes are Poisson distributed)**.** *Fix $\lambda > 0$. Suppose h and N tend to infinity in such a way that $h \sim \lambda \log N$. Then*

$$\frac{1}{N}\#\{n \leq N : \pi(n+h) - \pi(n) = k\} \to e^{-\lambda}\frac{\lambda^k}{k!}$$

for every fixed integer $k = 0, 1, 2, \ldots$.

Gallagher has shown that this follows from a uniform version of the prime k-tuples conjecture.

Polynomial prime gaps

For a prime p and an integer a, let $\overline{a}$ denote the residue class of a in $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$.

For each prime p and each integer $h \geq 0$, define

$$I(p;h) := \{\overline{a_0} + \overline{a_1}T + \cdots + \overline{a_j}T^j : \\ 0 \leq a_0, \ldots, a_j < p \text{ with } \sum a_i p^i < h\}.$$

Let $P_k(p;h,n)$ be the number of polynomials $A(T)$ of degree n over $\mathbf{F}_p$ for which the translated "interval" $A + I(p;h)$ contains exactly k primes.

Conjecture. *Fix* $\lambda > 0$*. Suppose* h *and* n *tend to infinity in such a way that* $h \sim \lambda n$*. Then*

$$\frac{1}{p^n} P_k(p; h, n) \to e^{-\lambda} \frac{\lambda^k}{k!} \quad (\textit{as } n \to \infty)$$

for each fixed $k = 0, 1, 2, 3, \ldots$*, uniformly in the prime* p*.*

Theorem. *Fix* $\lambda > 0$. *Suppose* h *and* n *tend t0o infinity in such a way that* $h \sim \lambda n$. *Then for each fixed integer* $k \geq 0$,

$$\frac{1}{p^n} P_k(p; h, n) \to e^{-\lambda} \frac{\lambda^k}{k!},$$

if both n *and* p *tend to infinity, with* p *tending to infinity faster than any power of* n^{n^2}.