Arithmetic Properties of Polynomial Specializations over Finite Fields

Paul Pollack
Dartmouth College

September 30, 2007

Two examples from rational number theory:

Twin Prime Conjecture. *There are infinitely many pairs of primes* $p, p+2$.

Conjecture (Erdős)**.** *Asymptotically half of all positive integers* n *satisfy*

$$P(n) > P(n+1),$$

where $P(n)$ *is the largest prime factor of* n.

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 $f_2(T) := T + 1$.

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: 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 $P, P+\alpha$.*

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 $q \equiv 3 \pmod 4$.*

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

Gaps between primes

Conjecture. *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*

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

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}.

Other factorization types

Recall:
If $f(T)$ is irreducible over $\mathbf{F}_q$, then the number of proportion of monic polynomials $h(T)$ of degree n for which $f(h(T))$ is irreducible is roughly $1/n$ (provided q is large compared to n and $\gcd(q, 2n) = 1$).

Where does $1/n$ come from?

Answer: $1/n$ is the proportion of n-cycles in the symmetric group on n letters.

Definition. If $F(T)$ is a polynomial over a given field, the *factorization type* of $F(T)$ is the partition of $\deg F(T)$ given by the unordered list of the degrees of the irreducible factors of $F(T)$.

Question: If $f(T)$ is irreducible over $\mathbf{F}_q$, what proportion of monic polynomials $h(T)$ of degree n correspond to a given possible factorization type of $f(h(T))$ (partition of $n \deg f(T)$)?

Observe: Every irreducible polynomial dividing $f(h(T))$ has degree a multiple of $\deg f(T)$. So the factorization type of $f(h(T))$ has the form $\deg f(T) \times \lambda$, where λ is a partition of n.

Definition. If λ is a partition of the positive integer n, define $T(\lambda)$ to be the proportion of permutations on n letters with cycle type λ.

Theorem. *Let n be a positive integer and let $\lambda_1, \ldots, \lambda_r$ be partitions of the integer n. Let $f_1(T), \ldots, f_r(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$ of respective degrees $d_1, \ldots, d_r$, with $\sum_{i=1}^r d_i \leq B$.*

The number of univariate monic polynomials h of degree n for which $f_i(h(T))$ has factorization type $d_i \times \lambda_i$ for every $1 \leq i \leq r$ is

$$q^n \prod_{i=1}^{r} T(\lambda_i) + O((nB)n!^B q^{n-1/2}),$$

provided $\gcd(q, 2n) = 1$*. Here the implied constant is absolute.*

Application: smooth values of polynomials

Theorem (Dickman). *Fix $u > 0$. The number of $n \le x$ which are $x^{1/u}$-smooth is asymptotic to $\rho(u)x$, where ρ is the (unique) continuous solution of the differential-delay equation*

$$u\rho'(u) = -\rho(u-1) \quad \text{satisfying} \quad \rho(u) = 1 \text{ for } 0 \le u \le 1.$$

Conjecture (Martin). *Let F be an arbitrary but fixed nonzero integer-valued polynomial and let $d_1, \ldots, d_K$ be the degrees of the nonassociate irreducible factors of F. Then for each $U > 0$, the asymptotic formula*

$$\Psi(F; x, x^{1/u}) \sim x\rho(d_1 u) \cdots \rho(d_K u)$$

holds as $x \to \infty$, uniformly for $0 < u \le U$.

Some progress on this conjecture has been made by Martin under the assumption of a uniform version of Hypothesis H.

Theorem. *Fix $B, U \geq 1$. Let $F(T)$ be a non-constant polynomial over $\mathbf{F}_q$ of degree at most B. Let K be the number of distinct monic irreducible factors of F, and let $d_1, \ldots, d_K$ be the degrees of these factors. If $n \geq BU$ and $(q, 2n) = 1$, then*

$$\Psi(F; n, n/u) \sim q^n \rho(d_1 u) \cdots \rho(d_K u),$$

for $0 < u \leq U$, if both n and q/n^{4nB} tend to infinity.

Other applications

- Perfect polynomials

- Brun's constant for polynomials

- Sums of prime cubes