Simultaneous Prime Values of Polynomials in Positive Characteristic

Paul Pollack
Dartmouth College

January 7, 2007

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 $5 \le n \le 32$, 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

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

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

Two questions:

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

2. What about twin prime pairs of (say) 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.

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 F_{3^3}. Neither polynomial has a root which is a 13th power in 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 $k = 0, 1, 2, \ldots$.

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 $T, T+1$.

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.

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 $f^2 + 1$ 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*

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

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

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

where

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

Remarks

1. Under these assumptions on $f_1, \ldots, f_r$, the product defining $\mathfrak{S}(f_1, \ldots, f_r)$ converges to a nonzero constant.

2. If the sum of the degrees of the f_i is bounded, then the ratio $\mathfrak{S}(f_1, \ldots, f_r)/\prod_{i=1}^{r} \deg f_i$ tends uniformly to 1 as q tends to infinity.

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

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 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.

Theorem (P, 2006)**.** *Suppose* $f_1(T), \ldots, f_r(T)$ *are pairwise 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*

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

Theorem. *If $q > 2$, then there are infinitely many monic twin prime pairs $f, f+1$ over $\mathbf{F}_q$ with degree of any prescribed parity.*

This answers a question of Hall.

The Nonconstant Coefficient Problem:

What can be said without the restriction to polynomials with $\mathbf{F}_q$- coefficients?

Twin Prime Conjecture over $\mathbf{F}_2$: Are there infinitely many prime pairs $f, f + T^2 + T$ over $\mathbf{F}_2[T]$?

This is still open.

In the case of a general family of polynomials, Conrad, Conrad and Gross (to appear) have a conjectural correction to the quantitative conjectures.

Concluding Homage to Fermat

Can study Fermat primes for their own sake. Try to classify all 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 $\mathbf{F}_7[T]$.