Some Special Cases of an $\mathbf{F}_q[u]$-variant of Hypothesis H

Paul Pollack
Princeton University/Dartmouth College

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.

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

$$f_1(g)f_2(g)\cdots f_r(g) \equiv 0 \pmod{\pi}$$

holds for every $g \in \mathbf{F}_q[u]$. Then there are infinitely many $g \in \mathbf{F}_q[u]$ for which

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

are simultaneously irreducible in $\mathbf{F}_q[u]$.

This is false: over any $\mathbf{F}_q$, it can be shown that the polynomial

$$T^{4q} + u^{2q-1}$$

satisfies the local conditions but has no prime specializations at all.

History

J. Cherly (1978) proved: Let $\mathbf{F}_q$ be the finite field with q elements.

- if $q > 2$ and $\alpha \in \mathbf{F}_q^*$, then infinitely often $f, f + \alpha$ have at most four prime factors as f runs over $\mathbf{F}_q[u]$

- if $q \equiv 3 \pmod 4$, then infinitely often f^2+1 has at most six prime factors

Twin prime polynomials were again looked at by Effinger, Hicks & Mullen (2002).

Recent Progress

Theorem (C. Hall, 2003). *If $q > 3$, then infinitely often $f, f+1$ are simultaneously prime as f ranges over $\mathbf{F}_q[u]$.*

Theorem (P., 2004). *If $q > 2$ and $\alpha \in \mathbf{F}_q^*$, then infinitely often $f, f+\alpha$ are simultaneously prime as f ranges over $\mathbf{F}_q[u]$.*

Theorem (P., 2006). *If $q \equiv 3 \pmod 4$, then infinitely often f^2+1 is irreducible as f ranges over $\mathbf{F}_q[u]$.*

Common feature: all these cases correspond to polynomials purely in T!

Hypothesis H for Polynomials with $\mathbf{F}_q$ Coefficients. *Suppose $f_1, \ldots, f_r$ are irreducible polynomials in $\mathbf{F}_q[T]$ satisfying the local admissibility condition of the polynomial Hypothesis H. Then there are infinitely many substitutions*

$$T \mapsto g(T)$$

which preserve the simultaneous irreducibility of the f_i.

Main 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 $T^2 + 1$.

Lemma. *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.

Example: 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 $k = 1, 2, \ldots$.

Proof of the Main Theorem when $r = 1$

Let f be an irreducible polynomial over $\mathbf{F}_q$ of degree d. Want that if q is large (depending on d), then there are infinitely many substitutions

$$T \mapsto g(T)$$

that leave f irreducible.

Strategy: If lemma applies to $f(T)$, done. Else apply the Lemma to $f(T-\beta)$ for some $\beta \in \mathbf{F}_q$.

Fix an odd prime l dividing $q-1$. Suffices to produce $\beta \in \mathbf{F}_q$ for which

$$\alpha + \beta \text{ is not an } l\text{th power in } \mathbf{F}_{q^d}.$$

Let χ be a multiplicative character of $\mathbf{F}_{q^d}$ of order l. If $\alpha + \beta$ is an lth power for every $\beta \in \mathbf{F}_q$, then

$$\left| \sum_{\beta \in \mathbf{F}_q} \chi(\alpha + \beta) \right| \geq q - 1.$$

But according to an estimate for incomplete character sums found in a paper of Wan, the left hand side above is

$$\leq (d-1)\sqrt{q},$$

and this is a contradiction for large q.

References:

Cherly, J. **A lower bound theorem in $\mathbf{F}_q[x]$**. J. Reine Angew. Math. 303/304 (1978), 253–264.

Conrad, B.; Conrad, K.; Gross, R. **Prime Specialization in Genus** 0. Submitted.

Effinger, Gove W.; Hicks, Kenneth H.; Mullen, Gary L. **Twin irreducible polynomials over finite fields**. Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), 94–111, Springer, Berlin, 2002.

Hall, Christopher J. **L-functions of twisted Legendre curves**. Ph. D thesis, Princeton University, 2003.

Wan, Daqing. **Generators and irreducible polynomials over finite fields**. Math. Comp. 66 (1997), no. 219, 1195–1212.