

RESEARCH STATEMENT

PAUL POLLACK

INTRODUCTION AND SUMMARY OF RESEARCH

I am interested in questions in elementary and analytic number theory, primarily in the ring of rational integers, but also in other settings of arithmetic importance (such as rings of integers in global fields). In my thesis, I study the arithmetic of polynomials over finite fields, focusing on problems connected with the distribution of irreducible polynomials.

Many of the basic results in the subject of rational prime number theory can be translated fairly routinely (though not necessarily easily) into the polynomial setting. The first such results are the analogues of the prime number theorem (due essentially to Gauss – see [Fre07]), Dirichlet’s theorem (due to Kornblum [Kor19]), and the prime number theorem for arithmetic progressions (due to Artin [Art24]). Important techniques have also been generalized wholesale: e.g., sieve methods here have been investigated by Cherly [Che78], Webb [Web83], Car [Car84a]-[Car84b], and Hsu [Hsu96], and the circle method in this setting has been developed and applied by Hayes [Hay66] (see also his joint monograph with Effinger [EH91]). In many cases, though the broad outline of the proofs are the same in both settings, the polynomial results are sharper than the corresponding rational results, because the Riemann Hypothesis is a theorem in the function field setting (due to Weil [Wei48]).

In my thesis, I focus on classical problems about prime patterns, translated into the setting of polynomials over finite fields. In contrast to the authors mentioned above, I concentrate on methods which appear special to polynomials and seemingly have no classical analogue.

Hall gave the prototypical result of this kind in his 2003 Ph.D. thesis ([Hal03]; see also [Hal06]). There he successfully attacks a polynomial analogue of the twin prime conjecture, showing that over any field with more than three elements, there are infinitely many monic prime pairs $P(T)$ and $P(T) + 1$. Results of this type had been previously conjectured (by Cherly, op. cit., as well as Effinger, Hicks and Mullen [EHM02]-[EHM05]), but Hall’s theorem had seemed out of reach. Surprisingly, Hall’s argument is entirely elementary; apart from simple and short counting arguments, it requires only Capelli’s classification of irreducible binomials, a result which would not be out of place in a first algebra course.

In [Polb], we show how Weil’s Riemann Hypothesis can be used in place of Hall’s counting arguments to obtain more general results. By combining Capelli’s theorem with a modern estimate for character sums due to Lenstra (and proved using Weil’s Riemann Hypothesis), we establish the following theorem:

Theorem 1. *Let $f_1(T), \dots, f_r(T)$ be irreducible polynomials over k , where k is a finite field. If $|k| = q$ is large compared to the sum of the degrees of the f_i , then there is a prime l dividing $q - 1$ and an element $\beta \in k$ for which every substitution*

$$T \mapsto T^{l^m} - \beta \quad \text{with } m = 0, 1, 2, \dots$$

leaves all of f_1, \dots, f_r irreducible.

Selecting $f_1(T) = T$ and $f_2(T) = T + 1$, we recover Hall’s result for large q . But the result of Theorem 1 is far more general and may be viewed as progress towards one possible analogue of Schinzel’s celebrated Hypothesis H.

Classically, Schinzel's Hypothesis H is quantitatively refined by conjectures of Bateman and Horn [BH62]. These conjectures were first proposed in some special cases by Hardy and Littlewood [HL23]. One can formulate analogous predictions in the polynomial context. The next conjecture appears in the appendix to [Polb]. Another analogue of the Hardy-Littlewood conjectures, without uniformity in q but more general in other respects, appears in [CCG06].

Conjecture 2. *Let f_1, \dots, f_r be nonassociate irreducible one-variable polynomials over \mathbf{F}_q with the degree of $f_1 \cdots f_r$ bounded by B . Suppose that there is no prime P of $\mathbf{F}_q[T]$ for which the map*

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

is identically zero. Let $N(n)$ denote the number of monic polynomials $h(T) \in \mathbf{F}_q[T]$ of degree n for which all of $f_1(h(T)), \dots, f_r(h(T))$ are irreducible. Then

$$(1) \quad N(n) = (1 + o_B(1)) \frac{\mathfrak{S}(f_1, \dots, f_r) q^n}{\prod_{i=1}^r \deg f_i} \frac{1}{n^r} \quad \text{as } q^n \rightarrow \infty.$$

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

$$\mathfrak{S}(f_1, \dots, f_r) := \prod_{m=1}^{\infty} \prod_{\substack{\deg P=m \\ P \text{ monic, prime}}} \frac{1 - \omega(P)/q^m}{(1 - 1/q^m)^r},$$

where

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

Perhaps the most notable feature of Conjecture 2 is that the estimate is alleged to be *uniformly* valid in a wide range of q and n . There is no need to fix q , as a naive analogy with the integer case might suggest.

Given the difficulty classically associated with problems of this sort, it is perhaps surprising that we can prove an asymptotic formula which partially confirms Conjecture 2. The following result appears in [Polc]:

Theorem 3. *Let n be a positive integer. Let $f_1(T), \dots, f_r(T)$ be nonassociate irreducible polynomials over \mathbf{F}_q with the degree of the product $f_1 \cdots f_r$ bounded by B . Then with $N(n)$ defined as above,*

$$(2) \quad N(n) = \frac{\mathfrak{S}(f_1, \dots, f_r) q^n}{\prod_{i=1}^r \deg f_i} \frac{1}{n^r} + O(Bnn!^B q^{n-1/2})$$

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

Remark. It is shown in the appendix to [Polb] that the factor preceding q^n/n^r in (2) is $1 + O(B/q)$. (In fact, it is $1 + O(1/q)$ if the local condition of Conjecture 2 is satisfied, which is always the case when $q > B$.) It follows that we can equivalently phrase Theorem 3 with the simpler main term of q^n/n^r (and the same error term). This is the approach taken in [Polc].

Theorem 3 confirms Conjecture 2 in the range when q is much larger than n and prime to $2n$. Despite this restriction on q , it admits a number of applications. For example, it allows one to show that (in a similar range of q and n) the gaps between degree- n prime polynomials over \mathbf{F}_q are Poisson-distributed in a certain precise sense (analogous to that investigated by Gallagher for rational primes in [Gal76]). The proof of Theorem 3 builds on ideas introduced by Ree [Ree72] and Cohen [Coh70] and utilizes an explicit form of the function field Chebotarev density theorem made possible by Weil's Riemann Hypothesis.

The ideas underlying the proofs of Theorem 1 and Theorem 3 can also be applied in each of the following settings:

- Perfect polynomials, the polynomial analogue of perfect numbers; see [Can41], [BOW77] for background and [GPR07] for applications of the above methods.
- Smooth values of polynomials; this depends on an extension of Theorem 3 to count polynomial specializations with different factor types, which is the main result of [Pola]. This allows one to confirm the polynomial analogue of a conjecture of Martin [Mar02] in a certain range.
- Independence results for the multiplicative structure of neighboring polynomials [Pola]. This allows one to confirm (for example) the polynomial analogue of a conjecture of Erdős and Pomerance [EP78] on the independence of the largest prime factor of neighboring integers, again in a restricted range of q and n .

POSSIBILITIES FOR FUTURE WORK

The work discussed above can be extended in a number of ways. Here is one possible direction: Consider the problem of studying $\mathbf{F}_q[T]$ -points on algebraic sets defined over \mathbf{F}_q . In other words, suppose that we have a system of equations

$$f_i(X_1, \dots, X_N) = 0$$

where each f_i belongs to $\mathbf{F}_q[X_1, \dots, X_N]$. Suppose that $(A_1(T), \dots, A_N(T)) \in \mathbf{F}_q[T]^N$ is an initial solution. Then trivially, $(A_1(h(T)), \dots, A_N(h(T)))$ is also a solution for every polynomial $h(T)$. It follows that if there is a single $\mathbf{F}_q[T]$ -valued point on this algebraic set, not having all its coordinates constant, then there are infinitely many. The importance of Theorem 1 is that it allows us to obtain results of the same kind when some of the coordinates X_i are restricted to irreducible values, provided that q is large compared to the sum of the degrees of the initial solution $(A_1(T), \dots, A_N(T))$.

Of course it is not always obvious how to obtain initial solutions (or even whether solutions exist). In this context the method of proof of Theorem 3 is valuable; when it applies, one can show that for large q , there are many ‘small’ solutions to the system. One application of this type appears in [Polc], where this strategy is employed to obtain a generalization of Theorem 1. A more subtle application of these ideas yields the following result (constituting work in progress):

Theorem 4 (tentative). *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*

$$P = A^3 + B^3 + C^3, \quad \text{where } A, B, C \text{ are monic primes, and } \deg A > \max\{\deg B, \deg C\}.$$

Note that the statement corresponding to Theorem 4 for rational integers remains unsolved. Indeed, it was only recently that Heath-Brown [HB01] succeeded in showing that infinitely many primes are the sum of three positive cubes (in accordance with Conjecture N of Hardy and Littlewood [HL23]), as a consequence of his deep investigations in the area of sieve methods.

It would also be worth exploring what improvements result if the Riemann Hypothesis for curves (the key technical tool in most of the theorems thus far) is replaced with the corresponding result of Deligne for nonsingular algebraic varieties. Can one can widen the range of q and n in which the estimate of Theorem 3 can be shown to hold?

Finally, I plan to study elementary analytic number theory in the classical (rational) setting. My interests in this area are rather broad; before withdrawing the manuscript to pursue graduate studies at Dartmouth, I had a book-length treatment of these subjects under consideration by the American Mathematical Society. I am particularly drawn to Erdős-type problems, whose solutions often make use of tools from across the entire spectrum of modern elementary number theory.

REFERENCES

- [Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. I and II. *Math. Z.*, 19(1):153–246, 1924.
- [BH62] P. T. Bateman and R. A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.
- [BOW77] J. T. B. Beard, Jr., J. R. O’Connell, Jr., and K. I. West. Perfect polynomials over $\text{GF}(q)$. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 62:283–291, 1977.
- [Can41] E. F. Canaday. The sum of the divisors of a polynomial. *Duke Math. J.*, 8:721–737, 1941.
- [Car84a] M. Car. Le théorème de Chen pour $\mathbf{F}_q[X]$. *Dissertationes Math. (Rozprawy Mat.)*, 223:54, 1984.
- [Car84b] M. Car. Polynômes irréductibles de $F_q[X]$ de la forme $M + N$ où N est norme d’un polynôme de $F_{q^2}[X]$. *Dissertationes Math. (Rozprawy Mat.)*, 238:50, 1984.
- [CCG06] B. Conrad, K. Conrad, and R. Gross. Prime specialization in genus 0. Transactions of the AMS (to appear); available electronically at <http://www.math.lsa.umich.edu/~bdconrad/papers/hlsingle.pdf>, 2006.
- [Che78] J. Cherly. A lower bound theorem in $F_q[x]$. *J. Reine Angew. Math.*, 303/304:253–264, 1978.
- [Coh70] S. D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.
- [EH91] G. W. Effinger and D. R. Hayes. A complete solution to the polynomial 3-primes problem. *Bull. Amer. Math. Soc. (N.S.)*, 24(2):363–369, 1991.
- [EHM02] G. W. Effinger, K. Hicks, and G. L. Mullen. Twin irreducible polynomials over finite fields. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pages 94–111. Springer, Berlin, 2002.
- [EHM05] G. W. Effinger, K. Hicks, and G. L. Mullen. Integers and polynomials: comparing the close cousins \mathbf{Z} and $\mathbf{F}_q[x]$. *Math. Intelligencer*, 27(2):26–34, 2005.
- [EP78] P. Erdős and C. Pomerance. On the largest prime factors of n and $n + 1$. *Aequationes Math.*, 17(2-3):311–321, 1978.
- [Fre07] G. Frei. The unpublished section eight: on the way to function fields over a finite field. In *The shaping of arithmetic after C. F. Gauss’s Disquisitiones arithmeticae*, pages 159–198. Springer, Berlin, 2007.
- [Gal76] P. X. Gallagher. On the distribution of primes in short intervals. *Mathematika*, 23(1):4–9, 1976.
- [GPR07] L. Gallardo, P. Pollack, and O. Rahavandrany. On a conjecture of Beard, O’Connell and West concerning perfect polynomials. To appear in *Finite Fields and their Applications*, 2007.
- [Hal03] C. J. Hall. *L-functions of twisted Legendre curves*. PhD thesis, Princeton University, 2003.
- [Hal06] C. J. Hall. *L-functions of twisted Legendre curves*. *J. Number Theory*, 119(1):128–147, 2006.
- [Hay66] D. R. Hayes. The expression of a polynomial as a sum of three irreducibles. *Acta Arith.*, 11:461–488, 1966.
- [HB01] D. R. Heath-Brown. Primes represented by $x^3 + 2y^3$. *Acta Math.*, 186(1):1–84, 2001.
- [HL23] G. H. Hardy and J. E. Littlewood. Some problems of Partitio Numerorum III: on the expression of a number as a sum of primes. *Acta Math.*, 44:1–70, 1923.
- [Hsu96] C.-N. Hsu. A large sieve inequality for rational function fields. *J. Number Theory*, 58(2):267–287, 1996.
- [Kor19] H. Kornblum. Über die Primfunktionen in einer arithmetischen Progression. *Math. Zeitschrift*, 5:100–111, 1919.
- [Mar02] G. Martin. An asymptotic formula for the number of smooth values of a polynomial. *J. Number Theory*, 93(2):108–182, 2002.
- [Pola] P. Pollack. Arithmetic properties of polynomial specializations over finite fields. Submitted.
- [Polb] P. Pollack. An explicit approach to Hypothesis H for polynomials over a finite field. In *Proceedings of the Anatomy of Integers Conference, Montréal, March 2006*. To appear.
- [Polc] P. Pollack. Simultaneous prime specializations of polynomials over finite fields. Submitted.
- [Ree72] R. Ree. Proof of a conjecture of S. Chowla. *J. Number Theory* 3 (1971), 210–212; *erratum*, 4:223, 1972.
- [Web83] W. A. Webb. Sieve methods for polynomial rings over finite fields. *J. Number Theory*, 16(3):343–355, 1983.
- [Wei48] A. Weil. *Sur les courbes algébriques et les variétés qui s’en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948.