A FEW OPEN QUESTIONS

PAUL POLLACK

- **Fermat Primes in Function Fields**: One could try to classify tuples $(\mathbf{F}_q,\ A, B, m)$ for which
$$A^{m^k} - B$$
is irreducible over $\mathbf{F}_q$ for each $k \gg 0$. Over the rationals, the usual heuristics offered for the Fermat sequence $2^{2^n} + 1$ suggest that families of this type should not exist. But over $\mathbf{F}_q$, Capelli's theorem supplies us with numerous examples where $A = T$ (or a power of T); e.g., $T^{3^k} - 2$ over $\mathbf{F}_7$ is always irreducible. By combining Capelli's theorem with the $\mathbf{F}_q[T]$-power reciprocity law of Kühne & Schmidt, one can produce other examples, e.g., $(T^3 - 2)^{3^k} - 2$ is always irreducible over $\mathbf{F}_7$. If we restrict to cases where B is constant, can all examples be explained by these ideas? or is there something else at work? Are there any examples with B nonconstant?
- **Dirichlet-Weber Theorem for $\mathbf{F}_q[T]$**: The theorem of Dirichlet-Weber asserts that an irreducible binary quadratic form $ax^2 + bxy + cy^2$ with a, b, c coprime positive integers represents infinitely many rational primes. In fact, one can establish an asymptotic formula for the number of primes $p \le x$ that are representable by the form. To prove this one investigates the distribution of primes in ideal classes in orders of quadratic fields. Thanks to Artin, there is a theory of quadratic function fields, and a similar theorem should be provable.
- **A question of Granville on prime gaps**: Fix a polynomial $f(T) \in \mathbf{Z}[T]$ of a large degree n, and for each prime p set
$$R(p) = \sup\{a \ge 0 : f(T) + 1, \dots, f(T) + a \text{ are all reducible}\}.$$
What can be said about the average order of $R(p)$? The maximal order? The density theorems of algebraic number theory imply that $\limsup R(p)$ is infinite – one can make this quantitative, but can one prove anything close to what is conjecturally best possible?
- **Moments?** Granville suggests that by estimating the higher moments of certain character sums that appear in the Montreal paper, one might be able to prove Hypothesis H for "almost-all" constant-coefficient polynomial families of certain types.
- **Sieve results?** Car has shown that for a fixed finite field $\mathbf{F}_q$, every polynomial over $\mathbf{F}_q$ of large enough degree and satisfying the appropriate local conditions is the sum of a prime and a 2-almost prime. This is the polynomial Goldbach version of Chen's theorem. What about the twin prime

2000 *Mathematics Subject Classification.* Primary: 11T55, Secondary: 11N32.
The author is supported by an NSF Graduate Research Fellowship.

version? Presumably the details will be nearly the same, but the way in which Car's paper is written does not make this obvious.

- **Other counting theorems:** The main result of the counting paper is an asymptotic formula for constant-coefficient polynomials, useful when q is much larger than the sampling degree n. What about nonconstant-coefficient polynomials?

  Cohen has a result of this type for linear polynomials (corresponding to primes in arithmetic progressions). More specifically, he proves the following result:

  Theorem 1. *Consider the progression $A \bmod M$, where $\gcd(A, M) = 1$ and $\deg M = s$. If $n \geq s + 2$, then the number of monic primes $P \equiv A \bmod M$ with $P \in \mathbf{F}_q[T]$ of degree n is*

  $$\frac{1}{n} q^{n-s} + O_n(q^{n-s-1/2}),$$

  provided the characteristic of $\mathbf{F}_q$ exceeds n. More generally, fix a cycle type λ of S_n. Then $T(\lambda)q^{n-s} + O_n(q^{n-s-1/2})$ degree n monic polynomials $P \equiv A \pmod M$ possess that cycle type decomposition, where for $\lambda = 1^{a_1} \dots n^{a_n}$ we let

  $$T(\lambda) := \frac{1}{\prod_{i=1}^{n} a_i! i^{a_i}}$$

  denote the proportion of elements of S_n with cycle type λ.

  In the case when $\lambda = n$ (so that we are counting irreducibles), this is usually weaker than the prime number theorem for arithmetic progressions. But there are cases where it is better (e.g. when n is smaller than about $2s$, the estimate of the PNT for APs is trivial, even though we know RH).

  Can an asymptotic estimate be proven in the next hardest case, say for quadratic polynomials with nonconstant coefficients?

- **Effinger's idea and twins over $\mathbf{F}_2$:** For $n > 3$, define $\mathbf{F}_2$-polynomials

  $$P_n(T) = T^n + T^3 + T^2 + T + 1 \quad \text{and} \quad Q_n(T) = T^n + T^3 + 1.$$

  Notice that $P_n(T)$ and $Q_n(T)$ differ by $T^2 + T$, and that

  $$Q_n(T) \mid (T^n)^3 + (T^3 + 1)^3 = T^{3n} + T^9 + T^6 + T^3 + 1 = P_n(T^3).$$

  From this it is not hard to prove that if $P_n(T)$ is prime, then $Q_n(T)$ is as well, and that the converse holds whenever n is odd. Thus if $P_n(T)$ can be shown irreducible infinitely often, the existence of infinitely many twin prime pairs $P, P + T^2 + T$ follows, and similarly if $Q_n(T)$ can be shown irreducible for infinitely many odd n.

  This seems difficult. What can be said about primes in sequences of the form $T^n + g(T)$? For example, are almost all elements composite regardless of the choice of $g(T)$? Can one formulate a plausible conjecture as to exactly when we expect infinitely many primes in a sequence like this?

  To what extent can Effinger's construction be generalized – e.g., for which D is there an argument of this type to get primes pairs $P, P + D$?

Department of Mathematics, Dartmouth College, Hanover, NH 03755
E-mail address: paul.pollack@dartmouth.edu