WORK IN PROGRESS · MATHEMATICS, NUMBER THEORY

Dissociated sets of irreducible polynomials

MANTIS DISCOVERY

MANTIS · MIT CSAIL

OCTOBER 2026

01

The question

In the polynomials over a finite field with q elements, the monic irreducible polynomials play the part of the primes. Fix a monic modulus Q of degree n. A set R of irreducibles is dissociated modulo Q when the only product $\prod_{P\in R} P^{h_P}$ with every $|h_P| \le \ell$ that is congruent to 1 is the empty one. Equivalently, the $(\ell+1)^{|R|}$ divisors of $\prod_{P\in R} P^{\ell}$ are all different modulo Q. We ask whether, for every Q, almost every set of irreducibles of one degree is dissociated.

The question comes from additive combinatorics, where a set is dissociated when no small combination of its elements collapses to nothing. Here the group is the units modulo Q and the elements are irreducible polynomials, so a dissociated set is one whose products can all be told apart. The difficulty is that the answer has to hold for every modulus at once, including the moduli built to defeat it.

02

How we are approaching it

- We reduce the question to ruling out relations whose exponents are small, and degree alone already rules them out on few primes.
- We bound high moments of characters over the primes of one degree using unique factorization, uniformly over the class we aim at.
- When the exponents are divisible by the characteristic we keep the largest layer and compress by Frobenius, which replaces Q by a smaller modulus.
- We sum over the patterns of exponents with an exponential generating function.
- We take every prime from a single degree, which is what makes the moment bound uniform over the modulus.

03

Which degree to use

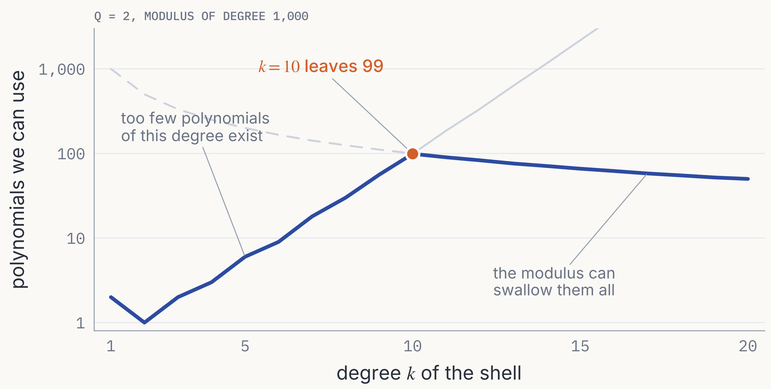


FIGURE 1. Two effects pull against each other. Few irreducibles of low degree exist, and a modulus of degree n can be divisible by every irreducible of high degree. The count we can use peaks near degree $\log_q n$, which is where we take our primes.

04

What we have so far

Fix q, the exponent bound ℓ and a density B. For all large n, every monic modulus Q of degree n and every $r \le Bn/k$ with $k = \lceil \log_q n \rceil + C$: all but a proportion $O(\exp(-cn/\log_q n))$ of the r-element sets of degree-k irreducibles not dividing Q are dissociated.

Uniformly in Q, the largest number of residue classes the divisors of a^{ℓ} reach over $\deg a \le \theta n$ satisfies $\log M = (\theta + o(1)) \log(\ell+1)\, n/\log_q n$.

When $\ell \deg a < \deg Q$ the divisors are already distinct by degree alone, so only the range $\ell\theta \ge 1$ needs an argument.

05

How far the divisors reach

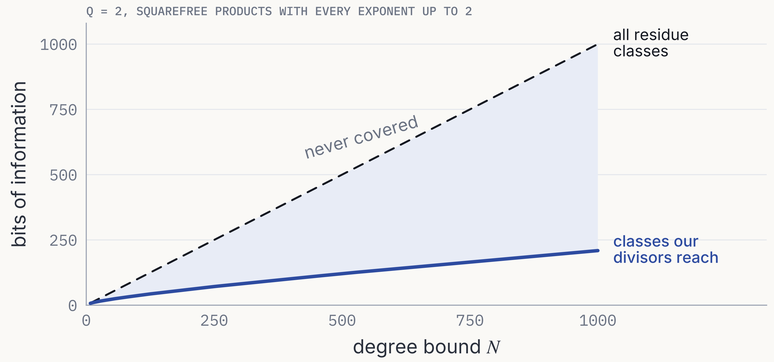


FIGURE 2. With $q = 2$ and exponents up to 2, the divisors of products of degree at most N reach about 209 bits of residue classes at $N = 1{,}000$, against the 1,000 bits the modulus has. The products stay distinct, and they come nowhere near covering the group.

06

Open questions

- The sets we produce are far smaller than the group, so this gives distinctness and not coverage. What reaches every class?
- Our primes all come from one degree. What do several degrees together give?
- The constants, and the point at which n counts as large, are not explicit. What are they?
- We show that almost every set works, without naming one. Is there an explicit set that works for every modulus?