Séminaire BOURBAKI Avril 2022
73e année, 2021–2022, no 1193, p. 453 à 478
doi: 10.24033/ast.1194

BINARY ADDITIVE PROBLEMS FOR POLYNOMIALS OVER FINITE FIELDS [*after* W. Sawin and M. Shusterman]

by **Emmanuel Kowalski**

1. Introduction

In the study of prime numbers, robust methods have been discovered during the late 19th century and over the course of the 20th century and the early 21st to solve and understand many of the most natural "additive" questions that curiosity had suggested to mathematicians. These methods include (to name a few): L-functions (from Dirichlet and Riemann to Artin and Langlands); sieve methods (Brun, Selberg, Iwaniec); combinations of these (Bombieri, Vinogradov, Maynard, Tao), bilinear forms methods (Vinogradov, Linnik); and ideas from ergodic theory and additive combinatorics (Green, Tao). We refer, for instance, to the surveys [1, 2, 3, 4, 5, 6, 7] in this seminar for some accounts of these methods and their achievements.

Among the remaining outstanding open questions, we have quite a few belonging to the class of *binary additive problems*, which include what are probably the two most popular among them: the twin prime conjecture, and Goldbach's conjecture for sums of two primes. There are a number of intrinsic limitations to the currently known methods which have blocked all attempts at solving these problems.

We will report in this survey on recent groundbreaking work of W. Sawin and M. Shusterman [37, 38] where, for the first time, problems of this kind are solved in the case of polynomials over a *fixed* finite field, in a very strong quantitative form. Furthermore, we will present results of Sawin [33] where similar ideas are used to prove extremely strong results concerning the level of distribution of arithmetic functions in arithmetic progressions, again in the case of polynomials over *fixed* finite fields.

Here are simple examples of the main achievements of Sawin and Shusterman. For a polynomial f with coefficients in a finite field k with $|k|$ elements, we denote

$$|f| = |k[\mathrm{T}]/fk[\mathrm{T}]| = |k|^{\deg(f)}$$

(the second formula when $f \neq 0$). Given a finite field k, we also denote by k_0 its prime subfield, so $|k_0|$ is the characteristic of k.[(1)]

Theorem 1.1 (Sawin–Shusterman). *Let k be a finite field such that $|k| > 10^6|k_0|^4$. Let $a \in k[\mathrm{T}]$ be a fixed non-zero polynomial.*

(1) (Twin prime conjecture) *We have*

$$|\{p \in k[\mathrm{T}] \mid \deg(p) = d,\ p \text{ and } p+a \text{ are monic irreducible polynomials}\}| \sim \mathfrak{L}_a \frac{|k|^d}{d^2}$$

as $d \to +\infty$, where

$$\mathfrak{L}_a = \prod_{p|a}\Big(1-\frac{1}{|p|}\Big)^{-1} \prod_{p\nmid a}\Big(1-\frac{2}{|p|}\Big)\Big(1-\frac{1}{|p|}\Big)^{-2},$$

which is a strictly positive absolutely convergent product over all monic irreducible polynomials $p \in k[\mathrm{T}]$.

(2) (Quadratic Bateman–Horn conjecture) *Assume that $|k|$ is odd. We have*

$$|\{f \in k[\mathrm{T}] \mid \deg(f) = d,\ f^2+a \text{ is a monic irreducible polynomial}\}| \sim \frac{\mathfrak{Q}_a}{2}\frac{|k|^d}{d}$$

as $d \to +\infty$, where

$$\mathfrak{Q}_a = \prod_p \Big(1-\frac{\varrho_a(p)}{|p|}\Big)\Big(1-\frac{1}{|p|}\Big)^{-2}, \quad \varrho_a(p) = |\{x \in k[\mathrm{T}]/pk[\mathrm{T}] \mid x^2+a(x) = 0\}|$$

which is a strictly positive conditionally *convergent product over all monic irreducible polynomials $p \in k[\mathrm{T}]$, taken as the limit as $d \to +\infty$ of partial products over polynomials of degree $\leqslant d$.*

Remark 1.2. (1) For integers, one often states the twin prime conjecture simply as the question of existence of infinitely many examples, without emphasizing the quantitative version. In the case of polynomials over finite fields, it is interesting to note that one can prove quite easily that there are infinitely many irreducible polynomials p in $k[\mathrm{T}]$ such that $p+1$ is also irreducible. For instance, if $|k^\times|$ is divisible by an odd prime ℓ, one can look for binomials $p = \mathrm{T}^{\ell^m} - a$ where $m \geqslant 1$, in which case the question is to find some $a \in k^\times$ such that neither a nor $a+1$ is an ℓ-th power in k;

(1) We will reserve the letter p to denote *either* prime numbers or irreducible polynomials, hence we do not want to waste it simply for the characteristic of the fixed field k.

there must be some of them, simply because the group of ℓ-th powers has index $\geqslant 2$ among the non-zero elements of k. (This observation can be found, with applications to ranks of twisted Legendre curves, in a paper of C. Hall, see [20, Cor. 14].)

(2) Observe the restriction on the size of k: although we haven't stated the sharpest forms of the results of Sawin and Shusterman (see [37, Th. 1.1] and [38, Th. 1.2], respectively), they require that $|k|$ be large enough compared to the characteristic of k. We will explain the source of this condition, and observe for the moment only that new ideas seem to be necessary to handle the case when $k = k_0$.

And here is a sample result from [33]:

Theorem 1.3 (Sawin). *Let k be a finite field such that $|k| \geqslant 23173$. For polynomials a and q in $k[\mathrm{T}]$, and for integers $d \geqslant 0$, let*

$$\pi(d; q, a) = \sum_{\substack{\deg(p)=d \\ p \equiv a \bmod q}} 1,$$

where the sum is over monic irreducible polynomials. Furthermore, let $\pi(d)$ be the number of monic irreducible polynomials of degree d.[(2)]

There exists $\mathrm{C} \geqslant 0$ and $\delta > 0$ such that, for all $d \geqslant 1$ and for $q \in k[\mathrm{T}]$ squarefree with $\deg(q) \leqslant 3d/4$ and $a \in k[\mathrm{T}]$ coprime with q, we have

$$\left|\pi(d; q, a) - \frac{\pi(d)}{\varphi(q)}\right| \leqslant \mathrm{C}|k|^{(1-\delta)(d-\deg(q))},$$

where $\varphi(q) = |(k[\mathrm{T}]/qk[\mathrm{T}])^\times|$.

Remark 1.4. (1) Again, there is a more precise version (where, for $|k|$ large enough, the constant $3/4$ may be replaced by any number < 1) in [33, Th. 1.2], but note the absolute bound for the size of k, independent of k_0, which highlights a difference with the previous results.

(2) The analogue of this theorem over number fields would be the fact that the primes have level of distribution $3/4$ in *individual* arithmetic progressions, which is currently unknown even under the assumption of the Generalized Riemann Hypothesis (and would have enormous implications in analytic number theory). In fact, there is (to this writer's knowledge) currently no non-trivial example of a sequence of integers with individual level of distribution $\geqslant 3/4$ (see the paper of Nunes [28] for one of the best results currently known, for squarefree integers, with level of distribution $25/36$; a notable non-trivial sequence with level of distribution arbitrarily close to 1 on average over the modulus is the Thue–Morse sequence, by work of Spiegelhofer [31, Th. 1.1]).

(2) As we will recall below, we have $\pi(d) \sim q^d/d$ (which may be checked elementarily by looking at elements of the extension of degree d of k which generate it; there are $\sim q^d$ such elements, each has minimal polynomial irreducible of degree d, and only d elements have the same minimal polynomial).

The outline of the remaining of this survey is the following:

1. We recall the analogy between integers and polynomials over finite fields, and state in parallel the Bateman–Horn conjecture in both cases.
2. We will explain *why* the case of polynomials over finite fields may be more accessible; in particular, we will explain briefly the simpler setting of the conjecture where the finite field k is allowed to change while the degree of the polynomials p is fixed.
3. We then present the strategy of Sawin and Shusterman – this combines beautifully arguments from algebraic as well as analytic number theory, and algebraic geometry. We attempt especially to focus on the points where the case of polynomials presents new phenomena and methods.
4. We sketch briefly some of the key arguments, chosen to emphasize both the similarities with integers, and some of the new ingredients.

Finally, we wish to point out that the papers we discuss contain a wealth of other results, many of which have considerable independent interest (non only more general, precise and uniform versions of the statements above, but also, e.g., proof of existence of cancellation in sums of the Möbius function evaluated at polynomials, which includes Chowla's conjecture for polynomials over finite fields). We invite the interested reader to go back to the source for more details.

Notation.

If X is a set and f, g are complex-valued functions on X, with $g \geqslant 0$, we write equivalently $f \ll g$ or $f = \mathrm{O}(g)$ if there exists a constant $\mathrm{C} \geqslant 0$ such that $|f(x)| \leqslant \mathrm{C}g(x)$ for all $x \in \mathrm{X}$. We then say that C is an *implied constant*. On the other hand, if X is a topological space and x_0 is in X (or is "at infinity"), we write $f(x) \sim g(x)$ as $x \to x_0$ to mean that g is non-zero close to x_0 and f/g tends to 1 as $x \to x_0$.

Acknowledgement. — Many thanks to C. Dartyge, É. Fouvry, J. Fresán, Ph. Michel and Z. Rudnick for comments and corrections on a draft of this text.

2. The polynomial–integer analogy

We will present the classical analogy between integers and polynomials over finite fields, choosing notation so that the parallel is as literal as possible. In particular, we can then present the general Bateman–Horn conjecture (and "standard" level of distribution conjectures) in a uniform manner.

The analogy goes back at least to a famous paper of Dedekind and Weber [16], and the basic dictionary is well-established:

$\mathbf{Z}$	$k[\mathrm{T}]$ where k is a finite field
$n \geqslant 1$	$f \in k[\mathrm{T}]$ monic
p prime	p monic irreducible polynomial
$\lvert n\rvert$ for $n \in \mathbf{Z}$	$\lvert f\rvert = \lvert k\rvert^{\deg(f)}$ for a polynomial f.

The analogy is reinforced by the fact that both $\mathbf{Z}$ and $k[\mathrm{T}]$ are principal ideal domains, and that prime numbers and monic irreducible polynomials, respectively, are in bijection with the set of non-zero prime ideals in $\mathbf{Z}$ and $k[\mathrm{T}]$. Moreover, it is crucial to the arithmetic part of this analogy that for non-zero integer n or polynomial f, the quotient ring $\mathbf{Z}/n\mathbf{Z}$ or $k[\mathrm{T}]/fk[\mathrm{T}]$ is finite, and is a finite field if n is prime or f irreducible.

So for instance, the analogue of the Riemann zeta function for $k[\mathrm{T}]$ is

$$\zeta_{k[\mathrm{T}]}(s) = \prod_p (1 - |p|^{-s})^{-1} = \sum_f |f|^{-s},$$

where the product ranges over all monic irreducible polynomials in $k[\mathrm{T}]$, and the sum over all $f \in k[\mathrm{T}]$ monic. The Prime Number Theorem states that the number $\pi(x)$ of prime numbers $p \leqslant x$ satisfies

$$\pi(x) \sim \frac{x}{\log x}, \qquad x \to +\infty,$$

and the analogue for irreducible polynomials is that

$$\pi(d) \sim \frac{q^d}{d}, \qquad d \to +\infty.$$

If we note that q^d is the number of monic polynomials of degree d, then the two asymptotic are clearly comparable. Intuitively, the second states that a monic polynomial of degree $d \geqslant 1$ has probability about $1/d$ of being irreducible.

We will use the following notation to have completely uniform statements. We write $\mathscr{O} = \mathbf{Z}$ or $k[\mathrm{T}]$ for some finite field; we denote by n (resp. p) a positive integer or a monic polynomial (resp. a prime number or a monic irreducible polynomial). We call p a *prime* in all cases. We sometimes denote by $\mathscr{O}_+$ either the set of positive integers or the set of monic polynomials.

Certain arithmetic functions have definitions which are identical in both cases. For instance, the function τ maps n to the number of divisors d of n, where divisors are either positive integers or monic (i.e., $d \in \mathscr{O}_+$). By convention, this meaning of