Algunas relaciones entre números primos y polinomios irreducibles sobre cuerpos finitos

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Seminario Latinoamericano de Teoría de Números
28 de octubre de 2021

Introduction

As unique factorization domains, the integer numbers and the polynomials over finite fields share many properties. Results on the decomposition of integers into prime integers can be similarly derived for the decomposition of polynomials over finite fields into irreducible factors.

For example: for q a prime power, it is well-known that a polynomial of degree n over $\mathbb{F}_q$ is irreducible with probability close to $1/n$. Can we have more results like we do have for the decomposition of integers into primes?

This takes us to counting polynomials over finite fields satisfying some properties. For that, we (briefly) review a methodology from analytic combinatorics adapted to polynomials over finite fields.

We consider monic univariate polynomials over a finite field $\mathbb{F}_q$. We want:

- to count polynomials with special forms;
- to explain the decomposition of polynomials into irreducible factors;
- to study probabilistic properties of polynomials that can be used to understand the behaviour of algorithms; and
- to estimate average-case analysis of algorithms.

We exemplify the methodology studying largest and smallest degree irreducible factors and their relations to Dickman and Buchstab functions.

We briefly comment on other relations between famous number theoretic theorems and conjectures (like the existence of infinitely many twin primes, Goldbach problems, etc) and polynomials over finite fields.

Finally, we also provide a (long) list of references for further consultation.

Relations between integers and polynomials

- How many irreducible factors a random polynomial has?
- How often will it be squarefree or *k*-free?
- What is the expected largest (smallest) degree among its irreducible factors?
- How is the degree distribution among its irreducible factors?
- How often a polynomial is *m*-smooth (all irreducible factors of degree at most *m*)?
- How often two polynomials are *m*-smooth and coprime?
- How is the degree distribution among the irreducible factors of the gcd of several polynomials?

These sort of results can be obtained with a general framework from analytic combinatorics. This methodology is easy to adapt to diverse polynomial counting problems.

Analytic combinatorics

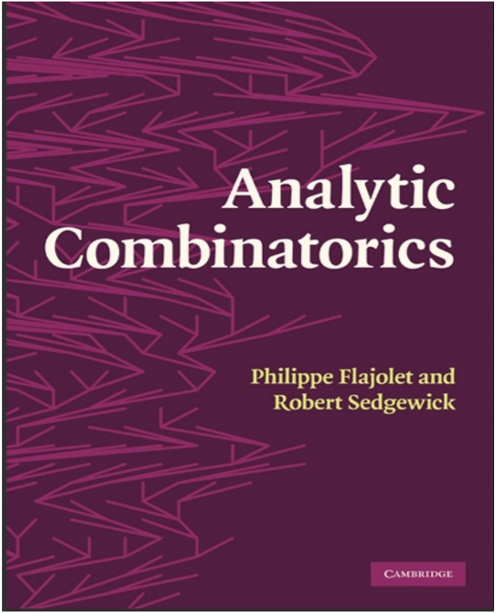
Analytic combinatorics is based on:

- the symbolic method for generating functions, and
- asymptotic methods for the derivation of the results.

The main reference for this research area is the book:

Analytic Combinatorics
by Philippe Flajolet and Robert Sedgewick
Cambridge University Press, 2009.

Winner of the 2019 Leroy P. Steele Prize for Mathematical Exposition of the American Mathematical Society.


Analytic
Combinatorics
Philippe Flajolet and
Robert Sedgewick
CAMBRIDGE

General framework

Let I_n be the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$. The generating functions of monic irreducible polynomials and monic polynomials are

$$I(z) = \sum_{n \geq 1} I_n z^n, \qquad \text{and}$$
$$P(z) = \prod_{j \geq 1} (1 + z^j + z^{2j} + \cdots)^{I_j} = \prod_{j \geq 1} (1 - z^j)^{-I_j}.$$

Since $[z^n]P(z)$ is q^n, we have $P(z) = (1 - qz)^{-1}$, and these relations implicitly determine I_n

$$I_n = \frac{1}{n} \sum_{k|n} \mu(k) q^{n/k}.$$

From

$$\frac{1}{1-qz} = \prod_{j=1}^{\infty}(1-z^j)^{-I_j},$$

we get

$$\log\frac{1}{1-qz} = \sum_{j\geq 1}(I_j)\log(1-z^j)^{-1} = \sum_{j\geq 1}\frac{I(z^j)}{j}.$$

Expanding the log and equating coefficients we get

$$\frac{q^n}{n} = \sum_{k|n}\frac{I_{n/k}}{k}.$$

Möbius inversion formula gives

$$I_n = \frac{1}{n}\sum_{k|n}\mu(k)q^{n/k}.$$

The probability of a polynomial of degree n be irreducible is close to $1/n$.

Parameters and multivariate generating functions

As usual, we consider bivariate generating functions to take care of critical parameters of the problems we are interested in. Asymptotic analysis is then used to extract coefficient information.

Example: number of irreducible factors. Let

$$P(u,z) = \prod_{j\geq 1}(1 + uz^j + u^2z^{2j} + \cdots)^{I_j} = \prod_{j\geq 1}(1 - uz^j)^{-I_j}$$

where $[u^m z^n]P(u,z)$ is the number of polynomials of degree n with m irreducible factors.

Differentiating $P(u,z) = \sum_j \sum_i a_{i,j} u^i z^j$ two times with respect to the parameter u, putting $u = 1$ and extracting the nth coefficient asymptotically gives expectation $\log n$ and standard deviation $\sqrt{\log n}$.

Theorem. Let Ω_n be a random variable counting the number of irreducible factors of a random polynomial of degree n over $\mathbb{F}_q$, where each factor is counted with its order of multiplicity.

1. The mean value of Ω_n is asymptotic to $\log n$ (Berlekamp; Knuth).
2. The variance of Ω_n is asymptotic to $\log n$ (Knopfmacher and Knopfmacher; Flajolet and Soria).
3. For any two real constants $\lambda < \mu$,

$$\Pr\left\{\log n + \lambda\sqrt{\log n} < \Omega_n < \log n + \mu\sqrt{\log n}\right\} \to \frac{1}{\sqrt{2\pi}} \int_{\lambda}^{\mu} e^{-t^2/2} dt.$$

4. The distribution of Ω_n admits exponential tails (Flajolet and Soria).
5. A local limit theorem holds (Gao and Richmond).
6. For all m, $\Pr\{\Omega_n = m\}$ is known (Cohen; Car; Hwang).

Singularity analysis

Theorem. Let f be a complex function analytic in a domain

$$D = \left\{ z : |z| \le s_1, |\operatorname{Arg}(z-s)| > \frac{\pi}{2} - \eta \right\},$$

where $s_1 > s$, η and s are three positive real numbers. Assume that, with $\sigma(u) = u^\alpha \log^\beta u$ and $\alpha \notin \{0, -1, -2, \dots\}$, we have

$$f(z) \sim \sigma\left(\frac{1}{1-z/s}\right) \qquad \text{as } z \to s \text{ in } D. \tag{1}$$

Then the Maclaurin coefficients of f satisfy, as $n \to \infty$,

$$[z^n]f(z) \sim s^{-n} \frac{\sigma(n)}{n\Gamma(\alpha)}. \tag{2}$$

Singularity analysis (Flajolet and Odlyzko 1990) entails that if the generating function $f(z)$ behaves as in (1) when z is close to the dominant singularity s then, asymptotically, the n-th Maclaurin coefficient of $f(z)$ behaves as in (2). In our case $s = 1/q$.

A simplified picture of a random polynomial

A random polynomial over $\mathbb{F}_q$ of degree n:

- is irreducible with probability tending to 0 as $n \to \infty$;
- is k-free with probability $1 - 1/q^{k-1}$;
- has $\log n$ irreducible factors (concentrated);
- has no linear factors with asymptotic probability ranging from 0.25 to $0.3678\ldots$ as q grows;
- has irreducible factors of distinct degree with asymptotic probability between $0.6656\ldots$ and $e^{-\gamma} = 0.5614\ldots$ as $q \to \infty$;

A simplified picture of a random polynomial (cont)

- has $c_k n$ expected kth largest degree irreducible factor, where $c_1 = 0.62433\ldots$, $c_2 = 0.20958\ldots$, $c_3 = 0.08831\ldots$ and the remaining irreducible factors have small degree (here c_1 is Dickman-Golomb's constant);

- has expected first and second smallest degree factors asymptotic to $e^{-\gamma}\log n$ and $e^{-\gamma}\log^2 n/2$ (not concentrated);

- has limiting distribution for the total degree of the gcd of several polynomials following a geometric distribution, and for the number of (distinct) irreducible factors in the gcd following very closely Poisson distributions when $q \geq 64$;

and so on.

Largest degree irreducible factors

Polynomials with all of their irreducible factors with degree not greater than certain bound m, the m-smooth polynomials, play a central role in algorithms for computing discrete logarithms.

Odlyzko (1985) provides an asymptotic estimate when $n \to \infty$ for the case $q = 2$ and $n^{1/100} \leq m \leq n^{99/100}$ using the saddle point method.

Car (1987) gives an asymptotic expression in terms of the Dickman function that holds for m large with respect to n, typically $m > c\, n \log \log n / \log n$.

Soundararajan (1998) completes the full range $1 \leq m \leq n$ by giving more precise boundaries. He also shows that the number of smooth polynomials behaves like the Dickman function when $m \geq \sqrt{n} \log n$.

Definition. The Dickman function, $\rho(u)$, is the unique continuous solution of the difference-differential equation

$$\begin{aligned} \rho(u) &= 1 & 0 \leq u \leq 1, \\ u\rho'(u) &= -\rho(u-1) & u > 1. \end{aligned}$$

Theorem. For ρ the Dickman function, the main term of the number $N_q(n,m)$ of m-smooth polynomials of degree n over $\mathbb{F}_q$ is $q^n \rho\left(\frac{n}{m}\right)$.

Remarks. The error term depends on the range of m as a function of n.

Proof (Sketch).

The generating function $S_m(z)$ of m-smooth polynomials is

$$S_m(z) = \prod_{k=1}^{m} \left(\frac{1}{1-z^k}\right)^{I_k}.$$

The Cauchy formula implies

$$N_q(n,m) = [z^n]S_m(z) = \frac{1}{2\pi i}\int_{\mathcal{C}} S_m(z)\,\frac{dz}{z^{n+1}},$$

where the contour $\mathcal{C}$ is chosen to be $z = e^{-1/n+i\theta}$, $-\pi \le \theta \le \pi$. The change of variable $z = e^{-h/n}$ gives

$$N_q(n,m) = \frac{1}{2\pi i}\int_{1+ni\pi}^{1-ni\pi} S_m(e^{-h/n})\left(-\frac{1}{n}\right)\frac{dh}{e^{-h}}.$$

For $r_m^{[j]}(z) = \sum_{k>m} I_k z^{kj}$, we have

$$\begin{aligned} S_m(z) &= \prod_{k\ge 1}(1-z^k)^{-I_k}\prod_{k>m}(1-z^k)^{I_k} \\ &= \frac{1}{1-qz}\exp\left(-r_m^{[1]}(z) - \frac{r_m^{[2]}(z)}{2} - \frac{r_m^{[3]}(z)}{3}\dots\right). \end{aligned}$$

The estimate $I_k = q^k/k + O(q^{k/2}/k)$ gives

$$r_m^{[1]}\left(\frac{z}{q}\right) = \sum_{k>m} \frac{z^k}{k} + O(q^{-m/2}) \qquad \text{for } |z| < \frac{1}{q},$$

and,

$$\sup_{|z|\le 1/q} r_m^{[j]}\left(\frac{z}{q}\right) = O\left(\frac{1}{q^{m(j-1)}}\right) \qquad \text{for } j \ge 2.$$

Lemma (Gourdon 1996).

Let $r_m(z) = \sum_{k>m} \frac{z^k}{k}$. Then,

$$r_m(e^{-h}) = E(mh) + O\left(\frac{1}{m}\right),$$

where E is the exponential integral function defined by

$$E(a) = \int_a^{+\infty} \frac{e^{-s}}{s}\, ds.$$

Then, for $\mu = m/n$,

$$N_q(n,m) = q^n \frac{1}{2\pi i} \int_{1-ni\pi}^{1+ni\pi} \frac{e^{-E(\mu h)+O(1/m)}}{n(1-e^{-h/n})} e^h \, dh.$$

Let $\psi(z) = \frac{1}{1-e^{-z}} - \frac{1}{z}$. Then, the main term of $N_q(n,m)$ is

$$q^n \frac{1}{2\pi i} \int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)} \left(\frac{1}{h} + \frac{1}{n} \psi\left(\frac{h}{n}\right)\right) e^h \, dh.$$

The study of these integrals gives for the main term of $N_q(n,m)$

$$q^n \frac{1}{2\pi i} \int_{1-in\pi}^{1+in\pi} \frac{e^{-E(\mu h)}}{h} e^h \, dh.$$

The Laplace transform $\widehat{\rho}(s)$ of the Dickman function satisfies $s\,\widehat{\rho}(s) = e^{-E(s)}$. Therefore, it can be shown that

$$\rho(u) = \frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\left(\frac{e^{-E(v)}}{v}\right)e^{uv}\,dv.$$

Finally,

$$\begin{aligned}
\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(\mu h)}}{h}e^{h}\,dh &= \frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\left(\frac{e^{-E(v)}}{v/\mu}\right)e^{v/\mu}\,\frac{dv}{\mu}\\
&= \frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\left(\frac{e^{-E(v)}}{v}\right)e^{vn/m}\,dv\\
&= \rho\left(\frac{n}{m}\right).
\end{aligned}$$

□

Theorem. The largest degree $D_n^{[1]}$ among the irreducible factors of a random polynomial of degree n over $\mathbb{F}_q$ satisfies

$$\Pr(D_n^{[1]} = m) = \frac{1}{m} f\left(\frac{m}{n}\right) + O\left(\frac{\log n}{m^2}\right),$$

where $f(\mu) = \rho(1/\mu - 1)$ is a related to the Dickman function:

$$f(\mu) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h)}}{h} \, e^{(1-\mu)h} \, dh.$$

Proof (Sketch). Similar to the previous proofs but considering $S_m(z) - S_{m-1}(z)$ in the role of $S_m(z)$. □

The study of the largest and second largest degree of a random polynomial is relevant for average–case analysis of factoring algorithms.

Theorem. The two largest degrees $D_n^{[1]}$ and $D_n^{[2]}$ of the distinct factors of a random polynomial of degree n over $\mathbb{F}_q$ satisfy

(i) for $0 \le m \le n$,

$$\Pr(D_n^{[1]} = m, D_n^{[2]} \le m/2) = \frac{1}{m} g_1\left(\frac{m}{n}\right) + O\left(\frac{\log n}{m^2}\right),$$

where $g_1(\mu)$ is expressed in terms of the exponential integral E as

$$g_1(\mu) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h/2)}}{h}\, e^{(1-\mu)h}\, dh;$$

(ii) for $0 \le m_2 < m_1 \le n$,

$$\Pr(D_n^{[1]} = m_1, D_n^{[2]} = m_2) = \frac{1}{m_1 m_2} g_2\left(\frac{m_1}{n}, \frac{m_2}{n}\right) + O\left(\frac{\log n}{m_1 m_2^2}\right),$$

where $g_2(\mu_1, \mu_2)$ is

$$g_2(\mu_1, \mu_2) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu_2 h)}}{h}\, e^{(1-\mu_1-\mu_2)h}\, dh.$$

Similar results to the above theorems hold for the joint distribution of the jth largest distinct irreducible factors.

Related decomposition of irreducible factors results

The smallest irreducible factor

The Buchstab function is the unique continuous solution of the difference-differential equation

$$\begin{aligned} u\omega(u) &= 1 \qquad && 1 \le u \le 2, \\ (u\omega(u))' &= \omega(u-1) \qquad && u > 2. \end{aligned}$$

Theorem. The smallest degree S_n among the irreducible factors of a random polynomial of degree n over $\mathbb{F}_q$ satisfies

$$Pr(S_n \ge m) = \begin{cases} \frac{1}{m}\,\omega\left(\frac{n}{m}\right) + O\left(\frac{1}{m^2}\right) & \text{if } m = O(\frac{n}{\log n}), \\ \frac{1}{m}\,\omega\left(\frac{n}{m}\right) + O\left(\frac{\log n}{mn}\right) & \text{otherwise.} \end{cases}$$

As for largest degree irreducible factors, there are similar results for the joint distribution of the jth smallest distinct irreducible factors.

Free of small and large degree irreducible factor

Friedlander (1976) studies numbers free from small and large primes.

Let $N_q(n, m_1, m_2)$ be the number of polynomials of degree n over $\mathbb{F}_q$ with all irreducible factors of degree bigger than m_2 and less than m_1.

Using the well-known estimate for the Dickman function (see, for example, Tenenbaum 1996)

$$\rho(u) = e^{-(1+o(1))u \log u}, \qquad u = \frac{n}{m},$$

one can prove estimates for $N_q(n, m_1, m_2)$ when m_2 is constant, and when m_2 varies with n (and always m_1 tending to infinity with n).

Free of small and large degree irreducible factor (cont.)

Theorem. The number $N_q(n, m_1, m_2)$ of monic polynomials of degree n over $\mathbb{F}_q$ with all irreducible factors with degree between m_2 and m_1, with m_2 fixed and $\log n \ll m_1 \ll n$, satisfies

$$N_q(n, m_1, m_2) = q^n e^{-(1+o(1))\frac{n}{m_1} \log \frac{n}{m_1}}.$$

Theorem. The number $N_q(n, m_1, m_2)$ with $m_1, m_2 \to \infty$, $m_1 e^{-n/m_1} \ll m_2 \leq c m_1$ for any constant $c < 1$, and $2(\log n)^2 \leq m_1 \ll n$, satisfies

$$N_q(n, m_1, m_2) = q^n e^{-(1+o(1)) u_1 \log u_1},$$

where $u_1 = n/m_1$.

Random decomposable combinatorial structures

Random decomposable combinatorial structures

We presented here results for the decomposition of polynomials over finite fields into irreducible factors. Analytic combinatorics can be used to study general properties of decomposable combinatorial structures like

- permutations;
- polynomials over finite fields;
- some combinatorial problems like children's yards;
- random mappings (functional digraphs, patterns);
- some classes of graphs (2-regular graphs);
- and so on.

These problems have generating functions that can be expressed in the so-called exp–log class.

Generating functions

Let $C(z)$ be the GF for the components, and

$$L(z) = \sum_n L_n \frac{z^n}{n!}, \qquad U(z) = \sum_n U_n z^n$$

the EGF and the OGF for the labelled and unlabelled structures. Then, $L(z) = \exp(C(z))$, and

$$U(z) = \exp\left(C(z) + \frac{C(z^2)}{2} + \frac{C(z^3)}{3} + \cdots \right).$$

For instance, we get for $U(z)$

$$\prod_{k=1}^{\infty} (1 + z^k + z^{2k} + \cdots)^{C_k} = \prod_{k=1}^{\infty} \left(\frac{1}{1 - z^k} \right)^{C_k}$$

$$= \exp\left(\sum_k \log\left(1 - z^k\right)^{-C_k} \right) = \exp\left(\sum_k C_k z^k + \sum_k C_k \frac{z^{2k}}{2} + \cdots \right).$$

Examples

- Cycles in permutations

$$\exp\left(\log\frac{1}{1-z}\right).$$

- Random mappings (functional digraphs)

$$\exp\left(\frac{1}{2}\log\frac{1}{1-ez} + H\left((1-ez)^{1/2}\right)\right).$$

where $H(v)$ is analytic at $v = 0$ with $H(0) = 0$.

- 2-regular graphs

$$\frac{e^{-z/2-z^2/4}}{(1-z)^{1/2}} = \exp\left(\frac{1}{2}\log\frac{1}{1-z} - \frac{z}{2} - \frac{z^2}{4}\right).$$

- Irreducible factors of polynomials over a finite field $\mathbb{F}_q$

$$\frac{1}{1-qz} = \exp\left(\log\frac{1}{1-qz}\right).$$

Asymptotic analysis

Definition. Let $\Delta(\nu, \theta)$ be the region $|z| \leq 1 + \nu$ minus the region $|\arg(z-1)| \leq \theta$, with $\nu > 0$ and $0 < \theta < \pi/2$. $C(z)$ is of **logarithmic type** with multiplicity constant $a > 0$ if

$$C(z) = a \log\left(\frac{1}{1 - z/\rho}\right) + R(z),$$

$R(z)$ analytic in $\Delta(\nu, \theta)$, and as $z \to \rho$ in $\Delta(\nu, \theta)$

$$R(z) = K + O\left((1 - z/\rho)^{\alpha}\right)$$

with $0 < \alpha < 1$ and K a complex constant.

$H(z)$ is in the **exp-log class** if $H(z) = \exp(C(z))$ and $C(Z)$ is of logarithmic type.

Asymptotic analysis (cont.)

Hence,

$$H(z) = \frac{e^{R(z)}}{(1-z/\rho)^a} = \frac{e^K}{(1-z/\rho)^a} + O\left(\left(\frac{1}{1-z/\rho}\right)^{a-\alpha}\right).$$

Flajolet & Odlyzko's singularity analysis entails

$$[z^n]H(z) = \frac{1}{\rho^n}\,\frac{e^K}{\Gamma(a)}\,n^{a-1}\,(1+O(n^{-\alpha})),$$

$$[z^n]C(z) = \frac{1}{\rho^n}\,\left(\frac{a}{n} + O\left(\frac{1}{n^{1+\alpha}}\right)\right).$$

General results

Results have been provided for the probability that of the jth size component, for expectation, variance and higher moments of the jth size component, for the probability that the jth size component of an object of size n be equal to m, $1 \leq m \leq n$, for joint distributions, etc.

- Goncharov (1942, 1962): cycle distribution in permutations;
- Stepanov (1969): distributions in random mappings;
- Knuth & Trabb-Pardo (1976): permutations and numbers;
- Flajolet & Soria (1990, 1993): number of components;
- Arratia, Barbour, Stark & Tavaré (1990's): probabilistic approach;
- Gourdon, Flajolet, Panario (1996): largest size of components;
- Panario and Richmond (2001): smallest size of components.

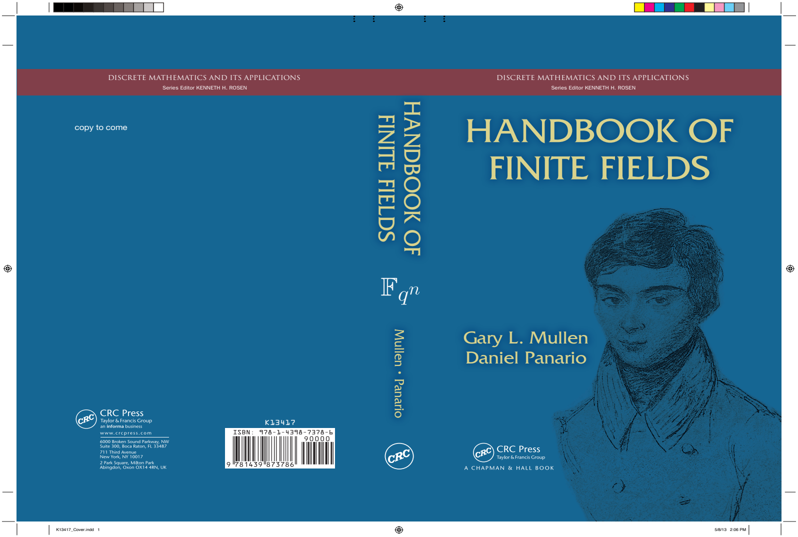
Other relations between integers and polynomials

Other relations between integers and polynomials

Several classical number theoretic problems have been translated to polynomials. For example,

- primes and irreducibles in arithmetic progression,
- twin primes and irreducibles,
- generalized Riemann hypothesis,
- Goldbach problems over finite fields,
- Waring problem over finite fields.

Advances have happened on these problems. For a precise account and references see the Chapter 13.1 in the book of the next slide (shameless advertisement coming...)



DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

copy to come

CRC Press
Taylor & Francis Group
an informa business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K13417

ISBN: 978-1-4398-7378-6
90000
9 781439 873786

HANDBOOK OF FINITE FIELDS

$\mathbb{F}_{q^n}$

Mullen • Panario

CRC

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

HANDBOOK OF FINITE FIELDS

Gary L. Mullen
Daniel Panario

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

K13417_Cover.indd 1

5/8/13 2:06 PM

Some important advances

Asymptotic uniform distribution in arithmetic progression have been known in some case (like prescribed first and last coefficients).

The twin primes conjecture has been proved for all finite fields of order bigger than 2. Also, generalizations (to more than 2 irreducibles, or to irreducible not as close as possible) have not been proved yet.

There have been some results about additive properties for polynomials related to Goldbach conjecture like the generalization to sum of three irreducibles, but there are open problems.

Several recent results in number theory have not been fully translated into polynomials over finite fields yet, including studies of divisors, irreducibles in small gaps, digital functions for polynomials; etc.

Some References

References on Analytic Combinatorics

Fundamental references:

- Ph. Flajolet, R. Sedgewick. “Analytic Combinatorics”, Cambridge University Press, 2009.
- Ph. Flajolet and A. Odlyzko. “Singularity analysis of generating functions”, SIAM J. Discrete Mathematics, 3, 216-240, 1990.

Other references:

- Ph. Flajolet, E. Fusy, X. Gourdon, D. Panario, N. Pouyanne, “A hybrid of Darboux’s method and singularity analysis in combinatorial asymptotics”, The Electronic Journal of Combinatorics, 13, R103, 2006.
- Ph. Flajolet, M. Soria, “Gaussian limiting distributions for the number of components in combinatorial structures”, Journal of Combinatorial Theory, Ser. A, 53, 165-182, 1990.
- D. Panario, B. Richmond, “Smallest components in decomposable structures: Exp-log class”, Algorithmica, 29, 205-226, 2001.

References on analisis of algorithms for polynomials

Random polynomial picture survey:

- D. Panario, "What do random polynomials over finite fields look like?", Finite Fields: Theory, Applications, and Algorithms, G.L. Mullen, A. Poli and H. Stichtenoth (eds), Springer, 89-108, 2004.

Gcd computations:

- Z. Gao and D. Panario. "Degree distribution of the greatest common divisor of polynomials over $\mathbb{F}_q$", Random Structures and Algorithms, 29, 26-37, 2006.

Discrete logarithm problem:

- A. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", Lecture Notes in Computer Science 209, 224-314 1985.
- D. Panario, X. Gourdon, Ph. Flajolet, "An analytic approach to smooth polynomials over finite fields", Lecture Notes in Computer Science, 1423, 226-236, 1998.
- M. Drmota, D. Panario, "A rigorous proof of the Waterloo algorithm for the discrete logarithm problem", Designs, Codes and Cryptography, 26, 229-241, 2002.

References on analisis of algorithms for polynomials (cont)

Irreducibility tests for polynomials:

- D. Panario, B. Richmond, “Analysis of Ben-Or’s polynomial irreducibility test”, Random Structures and Algorithms, 13, 439-456, 1998.
- D. Panario, B. Pittel, B. Richmond and A. Viola, “Analysis of Rabin’s irreducibility test for polynomials over finite fields”, Random Structures and Algorithms, 19, 525-551, 2001.

Polynomial factorization:

- Ph. Flajolet, X. Gourdon, D. Panario, “Random polynomials and polynomial factorization”, Lecture Notes in Computer Science, 1099, 232-243, 1996.
- Ph. Flajolet, X. Gourdon, D. Panario, “The complete analysis of a polynomial factorization algorithm over finite fields”, Journal of Algorithms, 40, 37-81, 2001.
- J. von zur Gathen, D. Panario, B. Richmond, “Interval partitions and polynomial factorization”, Algorithmica, 63, 363-397, 2012.
- G. Matera, M. Pérez, M. Privitelli, “Factorization patterns on nonlinear families of univariate polynomials over a finite field”, J. of Algebraic Combin., 51, 103-153, 2020.

References on matrices over finite fields

Enumeration of groups of matrices over finite fields:

- J. Fulman, P. Neumann, C. Praeger, "A generating function approach to the enumeration of matrices in classical groups over finite fields", Memoirs of the AMS, vol. 830, 2005.

Characteristic polynomial of a random matrix over finite fields:

- R. Stong, "Some asymptotic results on finite vector spaces", Advances in Applied Mathematics, 9, 167-199, 1988.
- J. Hansen, E. Schmutz, "How random is the characteristic polynomial of a random matrix?", Mathematical Proceedings of the Cambridge Philosophical Society, 114, 507-515, 1993.

References on expected splitting degree

Expected order of a random permutation and a random matrix:

- W. Goh, E. Schmutz, "The expected order of a random permutation", Bulletin London Mathematical Society 23, 34-42, 1991.
- R. Stong, "The average order of a matrix", Journal of Combinatorial Theory, Ser. A, 64, 337-343, 1993.
- R. Stong, "The average order of a permutation", Electronic Journal of Combinatorics, 5, R41, 1998.

Expected splitting degree of a polynomial over a finite field:

- J. Dixon, D. Panario, "The degree of the splitting field of a random polynomial over a finite field", Electronic Journal of Combinatorics, 11, R70, 2004.
- E. Schmutz, "Splitting fields for characteristic polynomials of matrices with entries in a finite field", Finite Fields and Applications, 14, 250-257, 2008.

References on mappings over finite fields

- Ph. Flajolet and A. Odlyzko. “Random mapping statistics”, Lecture Notes in Computer Science, 434, 329-354, 1990.
- T.Rogers. “The graph of the square mapping on the prime fields”. Disc.Math 148, 317-324, 1996.
- A.Peinado, F.Montoya, J.Muñoz, A.Yuste. “Maximal periods of $x^2 + c$ in $\mathbb{F}_q$”. LNCS 2227, 219-228, 2001.
- T.Vasiga, J.Shallit. “On the iteration of certain quadratic maps over GF(p)”. Disc.Math 227, 219-240, 2004.
- W.-S.Chou, I.E.Shparlinski. “On the cycle structure of repeated exponentiation modulo a prime”. Journal of Number Theory 107, 345-356, 2004.
- S.Ugolini. “Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic three and five”. Journal of Number Theory 133, 1207-1228, 2013.
- T.Gassert. “Chebyshev action on finite fields”. Disc.Math 315-316, 83-94, 2014.
- C.Qureshi, D.Panario. “Rédei actions on finite fields and multiplication map in cyclic groups”. SIAM Journal on Discrete Mathematics 29, 1486-1503, 2015.

References on mappings over finite fields (cont)

- R.Martins, D.Panario. “On the heuristic of approximating polynomials over finite fields by random mappings”. International Journal of Number Theory, 12, 1987-2016, 2016.
- C.Qureshi, D.Panario. “The graph structure of the Chebyshev polynomial over finite fields and applications”, Designs, Codes and Cryptography, 87, 393-416, 2019.
- C.Qureshi, L.Reis. “Dynamics of the *a*-map over residually finite Dedekind domains and applications. Journal of Number Theory, 204, 134-154, 2019.
- D.Panario, L.Reis. “The functional graph of linear maps over finite fields and applications”, Designs, Codes and Cryptography, 87, 437-453, 2019.
- L.Reis, Q.Wang. “The dynamics of permutations on irreducible polynomials”, Finite Fields and Applications, 64, 101664, 2020.
- R.Martins, C.Qureshi, D.Panario, E.Schmutz. “Periods of iterations of mappings over finite fields with restricted preimage sizes”, ACM Trans. on Algorithms, 16, Article 30, 2020.
- R. Martins, D. Panario, C. Qureshi. “A survey on iterations of mappings over finite fields”, Radon Series on Computational and Applied Mathematics, de Gruyter, 23, 135-172, 2019.