RELATIONS TO NUMBER THEORY IN PHILIPPE FLAJOLET'S WORK

Dedicated to the memory of Philippe Flajolet

Michael Drmota

Institute of Discrete Mathematics and Geometry

Vienna University of Technology

A 1040 Wien, Austria

michael.drmota@tuwien.ac.at

http://www.dmg.tuwien.ac.at/drmota/

Quebec 1987 ...

... at a number theory conference: comments on talk on the sum

$$\sum_{k<n} Q^{\nu(k)}$$

($Q > 0$, $\nu(k)$ ... binary sum-of-digits function = nb. of 1's in bin. exp.)

Actually we have (also thanks to Philippe's work):

$$\sum_{k<n} Q^{\nu(k)} \sim \Phi(\log_2(n))\, n^{\alpha},$$

where $\Phi(t)$ is a continuous and periodic function.

Philippe's comments dealt with (as far as I remember)

- digital sum
- Mellin transform, zeta-function
- asymptotics with the help of complex analysis

Contents

- Number Theory and Philippe Flajolet
- Riemann Zeta-function
- Random Polynomials over Finite Fields [Daniel Panario]
- Borrowed Techniques

Not in this talk

- Analysis of the Euclidean Algorithm [$\rightarrow$ previous talk]

What is Number Theory ?

(according to MSC 2010)

11 **Number theory**

11A Elementary number theory
11B Sequences and sets
11C Polynomials and matrices
11D Diophantine equations
11E Forms and linear algebraic groups
11F Discontinuous groups and automorphic forms
11G Arithmetic algebraic geometry (Diophantine geometry)
11H Geometry of numbers
11J Diophantine approximation, transcendental number theory
11K Probab. theory: distr. modulo 1; metric theory of algorithms

11L Exponential sums and character sums for finite fields
11M Zeta and L-functions: analytic theory
11N Multiplicative number theory
11P Additive number theory; partitions
11R Algebraic number theory: global fields For complex multiplication
11S Algebraic number theory: local and p-adic fields
11T Finite fields and commutative rings (number-theoretic aspects)
11U Connections with logic
11Y Computational number theory
11Z Miscellaneous applications of number theory

Number Theory in Philippe Flajolet's Work (following MathSciNet)

11A **Elementary number theory**

11A55 Continued fractions

11A63 Radix representation; digital problems

11B **Sequences and sets**

11B37 Recurrences

11B83 Special sequences and polynomials

11J **Diophantine approximation, transc. number theory**

11J70 Continued fractions and generalizations

11K **Probab. theory: distr. modulo 1; metric theory of algorithms**

11K06 General theory of distribution modulo 1

11K16 Normal numbers, radix expansions, Pisot numbers etc.

11K38 Irregularities of distribution, discrepancy
11K50 Metric theory of continued fractions
11K55 Metric theory of other algorithms and expansions; measure and Hausdorff dimension

11M **Zeta and L-functions: analytic theory**

11M06 $\zeta(s)$ and $L(s, \chi)$
11M41 Other Dirichlet series and zeta functions

11N **Multiplicative number theory**

11N25 Distribution of integers with specified multiplicative constraints

11T **Finite fields and commutative rings**

11T06 Polynomials

11Y **Computational number theory**

11Y16 Algorithms; complexity
11Y60 Evaluation of constants
11Y65 Continued fraction calculations

Analytic Combinatorics and Analytic Number Theory

Analytic combinatorics: *power series* (= **Laplace** transform)
(product rule based on **additive structure**)

$$\sum_{n\geq 0} a_n e^{-sn} = s\int_0^\infty \left(\sum_{n\leq t} a_n\right) e^{-st}\,dt \qquad (z=e^{-s})$$

Analytic number theory: *Dirichlet series* (= **Mellin** transform)
(product rule based on **multiplicative structure**)

$$\sum_{k\geq 1} \frac{a_k}{k^s} = s\int_0^\infty \left(\sum_{k\leq t} a_k\right) t^{-s-1}\,dt$$

$\boxed{\text{Laplace transform} = \text{Mellin transform}}$

"$\Longrightarrow$" $\boxed{\textbf{analytic combinatorics} = \textbf{analytic number theory}}$

Riemann Zeta-Function

$$\boxed{\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}}$$

Euler product (relation to **primes**):

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}}$$

Analytic properties of $\zeta(s)$ are closely related to the **distribution of primes**, in particular to the **prime number theorem**:

$$\pi(x) = \#\{p \in \mathbb{P} : p \leq x\} \sim \frac{x}{\log x}$$

References for the Riemann zeta-function

[116] Philippe Flajolet, Peter Grabner, Peter Kirschenhofer, Helmut Prodinger, and Robert Tichy. *Mellin transforms and asymptotics: Digital sums.* Theoretical Computer Science, 123(2):291-314, 1994.

[120] Philippe Flajolet, Xavier Gourdon, and Philippe Dumas. *Mellin transforms and asymptotics: Harmonic sums.* Theoretical Computer Science, 144(1-2):3-58, June 1995.

[125] Philippe Dumas and Philippe Flajolet. *Asymptotique des récurrences mahleriennes: le cas cyclotomique.* Journal de Théorie des Nombres de Bordeaux, 8(1):1-30, June 1996.

[143] Philippe Flajolet and Bruno Salvy. *Euler sums and contour integral representations.* Experimental Mathematics, 7(1):15-35, 1998.

References for the Riemann zeta-function

[157] Philippe Flajolet and Brigitte Vallée. *Continued fractions, comparison algorithms, and fine structure constants.* In Michel Théra, editor, Constructive, Experimental, and Nonlinear Analysis, volume 27 of Canadian Mathematical Society Conference Proceedings, pages 53-82, Providence, 2000. American Mathematical Society.

[197] Philippe Flajolet and Linas Vepstas. *On differences of zeta values.* Journal of Computational and Applied Mathematics, 220(1-2):58-73, 2008.

[199] Y. K. Cheung, Philippe Flajolet, Mordecai Golin, and C. Y. James Lee. *Multidimensional divide and-conquer and weighted digital sums* (extended abstract). In Proceedings of the Fifth Workshop on Analytic Algorithmics and Combinatorics (ANALCO) , pages 58-65. SIAM Press, 2009.

[207] Philippe Flajolet, Stefan Gerhold, and Bruno Salvy. *Lindelöf representations and (non-)holonomic sequences.* Electronic Journal of Combinatorics, 17(1)(R3):1-28, 2010.

The Riemann zeta-function appears as/in ...

- Dirichlet series, digital sums, Mellin transforms:
  analytic properties of $\zeta(s)$ are used: meromorphic continuation, growth properties, ...

- values of $\zeta(s)$, harmonic numbers, non-holonomicity:
  analytic properties of $\zeta(s)$ as well as properties of special values of $\zeta(s)$ are applied.

Zeta-function 1

Digital sums (related to divide-and-conquer recurrences)

Delange-type results [116]

$\nu_2(n)$ ... binary sum-of-digits function

$$\boxed{S(n) = \sum_{k<n} \nu_2(k) = \frac{1}{2} n \log_2 n + n F_0(\log_2 n)},$$

where the Fourier coefficients of F_0 are given by

$$f_k = -\frac{1}{\log 2} \frac{\boxed{\zeta(\chi_k)}}{\chi_k(\chi_k + 1)}, \quad \chi_k = \frac{2\pi i k}{\log 2}$$

($\nu_2(k)$ denotes the binary sum-of-digits function)

Zeta-function 1

Proof uses the Dirichlet series

$$\sum_{k\geq 1} \frac{\nu_2(k)}{k^s} = \frac{\zeta(s)}{2^s - 1}$$

and the integral representation

$$\frac{1}{n}S(n) - \frac{n-1}{2} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{\zeta(s)}{2^s - 1} n^s \frac{ds}{s(s+1)}$$

Generalizations: analysis of Gray code with the help of the Hurwitz zeta-function (and many others).

Zeta-function 1

Weighted Digital sums [199]

$$n = \sum_{k \ge 0} \varepsilon_k 2^k \qquad (\varepsilon_k \in \{0,1\} \text{ binary digits})$$

$$S_M(n) = \sum_{k \ge 0} j(j+1)\cdots(j+M-1)\varepsilon_k 2^k \qquad \text{weighted sum}$$

$$\sum_{n \ge 1} \frac{S_M(n) - S_M(n-1)}{n^s} = M!\frac{2^{(M-1)(s-1)}}{(2^{s-1}-1)^M}\zeta(s)$$

Explicit represenatation for the average (Delange type result)

$$\frac{1}{n}\sum_{k<n} S_M(k) = \frac{n}{2}(\log_2 n)^M + n\sum_{d=0}^{M-1} F_{M,d}(\log_2 n)(\log_2 n)^d + (-1)^{M+1}M!$$

Zeta-function 2

Mellin transforms [120]

$$\mathcal{M}[f(x);s] = \int_0^\infty f(x)x^{s-1}\,dx = f^*(s)$$

Then

$$\mathcal{M}\left[\sum_{k\geq 1} f(kx);s\right] = f^*(s)\zeta(s)$$

$$\mathcal{M}\left[\sum_{k\geq 1} f(\sqrt{k}x);s\right] = f^*(s)\zeta(s/2)$$

and in general (harmonic sums):

$$\boxed{\mathcal{M}\left[\sum_{k\geq 1} \lambda_k f(\mu_k x);s\right] = f^*(s)\sum_{k\geq 1}\lambda_k\mu_k^{-s}}$$

Such sums appear in analysis of several algorithms (like divide and conquer etc.)

Zeta-function 3

Asymptotics of sequences [125]

The Mahlerian sequence f_n is defined by

$$\sum_{n\geq 0} f_n z^n = \prod_{k=0}^{\infty} \frac{1}{1+z^{2^k}+z^{2^{k+1}}}.$$

Its asymptotic expansion includes periodic functions of the form

$$P(v) = \frac{1}{2\log 2} \sum_{k\neq 0} \Gamma(\chi_{2k})\zeta(1+\chi_{2k})(3^{-\chi_{2k}}+1)\exp(-4ki\pi v)$$

(A proper saddle point analysis is used.)

Zeta-function 4

Euler sums and multiple zeta values [143]

$$H_n^{(r)} = \sum_{j=1}^{n} \frac{1}{j^r}$$

Then we have (for example)

$$\sum_{n\geq 1} \frac{H_n}{n^2} = 2\zeta(3)$$

$$\sum_{n\geq 1} \frac{(H_n)^2}{n^5} = 6\zeta(7) - \zeta(2)\zeta(5) - \frac{5}{2}\zeta(3)\zeta(4)$$

$$\sum_{n\geq 1} \frac{H_n^{(2)}}{n^5} = 5\zeta(2)\zeta(5) + 2\zeta(2)\zeta(3) - 10\zeta(7)$$

Zeta-function 4

Many formulas like that are well known (by Borwein et al. etc.)

In [143] systematic study by using contour integral representations and residue computations is given. In this general context multiple zeta values appear, too.

These multiple zeta values appear also in the comparision of continued fraction algoithms [157]. The analysis there relies (also) on analytic properties of the zeta (and related) functions.

Zeta-function 5

$\zeta(s)$ **represented by Newton interpolation series** [197]

$$\zeta(s) - \frac{1}{s-1} = \sum_{n \geq 0} (-1)^n b_n \binom{s}{n}$$

with

$$b_n = n(1 - \gamma - H_{n-1}) - \frac{1}{2} + \sum_{k=2}^{n} \binom{n}{k} (-1)^k \zeta(k)$$

Precise asymptotic estimates for b_n can be derived, too (they are of size $\approx e^{-c\sqrt{n}}$ and leads to fast convergenc).

Zeta-function 5

Non-holonomicity [207]

The sequence $\dfrac{1}{\zeta(n+2)}$ is **non-holonomic**
(it does not satisfy a linear recurrence with polynomial coefficients).

The proof relies on then Lindelöf integral representation

$$\sum_{n\geq 1} \frac{1}{\zeta(n+2)}(-z)^n = -\frac{1}{2\pi i}\int_{1/2-\infty}^{1/2+\infty} \frac{1}{\zeta(s+2)} z^s \frac{\pi}{\sin(\pi s)}\, ds$$

Infinitely many zeros of $\zeta(s)$ lead to infinitely poles of $1/\zeta(s+2)$ and consequently to an asymptotic behaviour that is impossible for holonomic sequences.

Polynomials over Finite Fields

Analogy to integers $(K = \mathbb{F}_q)$

integers	$\leftrightarrow$	polynomials over K
prime numbers	$\leftrightarrow$	irreducible polynomials
rational numbers	$\leftrightarrow$	Laurent series
prime number theorem	$\leftrightarrow$	number of irred. polynomials
...	$\leftrightarrow$	...

References for polynomials over finite fields

[88] Philippe Flajolet and Michèle Soria. *Gaussian limiting distributions for the number of components in combinatorial structures.* Journal of Combinatorial Theory, Series A, 53:165-182, 1990.

[127] Philippe Flajolet, Xavier Gourdon, and Daniel Panario. *Random polynomials and polynomial factorization.* In F. Meyer auf der Heide and B. Monien, editors, Automata, Languages, and Programming, number 1099 in Lecture Notes in Computer Science, pages 232-243, 1996. Proceedings of the 23rd ICALP Conference, Paderborn, July 1996.

[145] Daniel Panario, Xavier Gourdon, and Philippe Flajolet. *An analytic approach to smooth polynomials over finite fields.* In J. P. Buhler, editor, Algorithmic Number Theory Symposium (ANTS), volume 1423 of Lecture Notes in Computer Science, pages 226-236. Springer Verlag, 1998.

[163] Philippe Flajolet, Xavier Gourdon, and Daniel Panario. *The complete analysis of a polynomial factorization algorithm over finite fields.* Journal of Algorithms, 40(1):37-81, 2001.

Analytic Combinatorics

Power set construction $\mathcal{P}$ of a combinatorial structure $\mathcal{C}$
(Objects of $\mathcal{P}$ can be decomposed into objects of $\mathcal{C}$.)

Labelled structure (exponential generating functions):

$$\widehat{P}(z) = \exp(\widehat{C}(z))$$

Unlabelled structures (ordinary generating functions):
multi set and power set construction

$$P(z) = \exp\left(\sum_{k\geq 1} \frac{1}{k} C(z^k)\right)$$

$$S(z) = \exp\left(\sum_{k\geq 1} \frac{(-1)^{k-1}}{k} C(z^k)\right)$$

Analytic Combinatorics

Power set construction $\mathcal{P}$ of a combinatorial structure $\mathcal{C}$

u "marks" the number of components.

Labelled structure

$$\widehat{P}(z,u) = \exp(u\widehat{C}(z))$$

Unlabelled structures:

$$P(z,u) = \exp\left(\sum_{k\geq 1} \frac{u^k}{k} C(z^k)\right)$$

$$S(z,u) = \exp\left(\sum_{k\geq 1} (-1)^{k-1} \frac{u^k}{k} C(z^k)\right)$$

A Central Limit Theorem

Theorem [88]

Suppose that the generating function of the combinatorial class $\mathcal{C}$ is a logarithmic function, that is,

$$C(z) = a \log \frac{1}{1 - z/\rho} + K + o(1)$$

in a Delta-domain.

Then the number of components of $\mathcal{C}$ in a power set construction satisfies a **central limit theorem** with mean and variance $\boxed{\sim a \log n}$.

Example. Cycles in permutations: $\widehat{P}(z,u) = \exp\left(u \log \frac{1}{1-z}\right)$

Polynomials over a finite field $\mathbb{F}_q$

GF of monic polynomials (I_k ... number of irreducible monic pol.)

$$P(z) = \frac{1}{1-qz} = \exp\left(\sum_{k\ge 1}\frac{1}{k}I(z^k)\right)$$
$$= \prod_{k\ge 1}\left(\frac{1}{1-z^k}\right)^{I_k}$$

GF for irreducible (monic) polynomials

$$I(z) = \sum_{k\ge 1}\frac{\mu(k)}{k}\log\frac{1}{1-qz^k} = \log\frac{1}{1-qz} + K + o(1)$$

"Prime number theorem" for polynomials over finite fields:

$$I_k = [z^k]I(z) \sim \frac{q^k}{k}$$

Erdős-Kac Type Theorem

By applying the above theorem for

$$P(z,u) = \exp\left(\sum_{k\geq 1} \frac{u^k}{k} I(z^k)\right)$$

one obtains

Theorem [88]

The number of irreducible factors in a random polynomial over a finite field satisfies a **central limit theorem** with mean and variance $\boxed{\sim \log n}$.

Theorem (for integers) [Erdős-Kac]

The number of prime factors in random integer $\leq n$ satisfies a **central limit theorem** with mean and variance $\boxed{\sim \log\log n}$.

Smooth Polynomials

A polynomial is m-smooth if all irreducible factors have degrees $\leq m$.

Theorem [145]

The number $N_q(n,m)$ of m-smooth polynomials of degree n over $\mathbb{F}_q$ satisfies

$$N_q(n,m) = q^n \rho(n/m)\left(1 + O\left(\frac{\log n}{m}\right)\right),$$

where $\rho(u)$ denotes the **Dickmann function**

$$\begin{array}{ll} \rho(u) = 1 & \text{for } 0 \leq u \leq 1 \\ u\rho'(u) = -\rho(u-1) & \text{for } u \geq 1 \end{array}$$

Smooth Polynomials

Proof uses the GF for m-smooth polynomials

$$N_q(n,m) = [z^n]\, S_m(z) = [z^n]\, \frac{1}{1-qz} \prod_{k>m} (1-z^k)^{I_k}$$

and a proper contour integration.

This result generalizes previously known results (by Odlyzko etc.)

Largest Irreducible Factor

Theorem [145]

The largest degree D_n among the irreducible factors of a random polynomial of degree n over $\mathbb{F}_q$ satisfies

$$\mathbb{P}(D_n = m) = \frac{1}{m} f(m/n) + O\left(\frac{\log n}{m^2}\right)$$

where $f(u) = \rho(1/u1)$.

Proof is a precise analysis of $L_m(z) = S_m(z) - S_{m-1}(z)$.

Extensions: joint Distribution of the Two Largest Degrees of Factors etc.

Smooth Integers and Largest Prime Factor

A positive integer n is y-smooth if all prime factors are $\leq y$.

Theorem (for integers)

- The number $\Psi(x, y)$ of y-smooth integers $\leq x$ is given by

$$\Psi(x, y) = x \cdot \rho(\log x / \log y) + O\left(\frac{x}{\log y}\right)$$

- The largest prime factor D_n of an integer $\leq x$ satisfies

$$\mathbb{P}(D_n \leq n^{\alpha}) \sim \rho(1/\alpha)$$

Average Case Analysis of Factorization Algorithm

A factorization algorithm in $\mathbb{F}_q[x]$ consists (usually) of three steps:

- ERF: elimination of repeated factors: $O(n^2)$
- DDF: distinct degree factorizationon, produces polynomials where all irreducible factors have same degree: $O(n^3)$
- EDF: equal degree factorization: $O(n^2)$

Theorem [127 163]

The expected costs for ERF, DDF and EDF are asymptotically given by

$$E_n[ERF] \sim c_1 n^2, \quad E_n[DDF] \sim c_1 n^3, \quad E_n[EDF] \sim c_3(1+\xi_n)n^2,$$

where the constants c_1, c_2, c_3 depend on q and $|\xi_n| \le 1/3$.

Average Case Analysis of Factorization Algorithm

Proof uses proper generating functions (such as)

$$P(z,u) = \prod_{n\ge 1}\left(1+\frac{z^n}{1-u^n z^n}\right)^{I_n},$$

or

$$P_k(z,u) = \prod_{j<k}\left(\frac{1}{1-z^j}\right)^{I_j}\prod_{j\ge k}\left(1-u^j\frac{z^j}{1-z^j}\right)^{I_j}$$

and a *careful analysis*.

Borrowed techniques

- continued fractions (usually used in *Diophantine approximation*) [$\rightarrow$ Viennot's talk]

- elliptic (and other special) functions (usually used in *Algebraic geometry*)

This is not number theory but important concepts from number theory are adopted to handle (analytic) combinatorial problems.

References for continued fractions and elliptic functions

[22] Philippe Flajolet. *Combinatorial aspects of continued fractions.* Annals of Discrete Mathematics, 8:217-222, 1980. Extended abstract. Proceedings of "Colloque Franco-Canadien de Combinatoire", Montreal, 1979.

[32] Philippe Flajolet. *On congruences and continued fractions for some classical combinatorial quantities.* Discrete Mathematics, 41:145-153, 1982.

[77] Philippe Flajolet and Jean Franon. *Elliptic functions, continued fractions and doubled permutations.* European Journal of Combinatorics, 10:235-241, 1989.

[87] Philippe Flajolet and René Schott. *Non-overlapping partitions, continued fractions, Bessel functions and a divergent series.* European Journal of Combinatorics, 11:421-432, 1990.

References for continued fractions and elliptic functions

[184] Philippe Flajolet, Stefan Gerhold, and Bruno Salvy. *On the non-holonomic character of logarithms, powers, and the nth prime function.* Electronic Journal of Combinatorics, 11(2)(A1):1-16, 2005.

[186] Eric van Fossen Conrad and Philippe Flajolet. *The Fermat cubic, elliptic functions, continued fractions, and a combinatorial excursion.* Séminaire Lotharingien de Combinatoire, 54(B54g):1-44, 2006.

[203] Roland Bacher and Philippe Flajolet. *Pseudo-factorials, elliptic functions, and continued fractions.* Ramanujan Journal, 21:71-97, 2010.

Thanks!