The Mathematics Student,
Vol. 76, Nos. 1-4 (2007), 203-211

RECENT DEVELOPMENTS IN FUNCTION FIELD ARITHMETIC

DINESH S. THAKUR

(Received: 29-01-2008)

Notation

$$\begin{array}{rcl}
\mathbb{Z} & = & \{\text{integers}\} \\
\mathbb{Q} & = & \{\text{rational numbers}\} \\
\mathbb{R} & = & \{\text{real numbers}\} \\
\mathbb{C} & = & \{\text{complex numbers}\} \\
\mathbb{Z}_+ & = & \{\text{ positive integers}\} \\
q & = & \text{a power of a prime } p \\
\mathbb{F}_q & = & \text{A Finite field with } q \text{ elements} \\
A & = & \mathbb{F}_q[t] \\
A_+ & = & \{\text{monics in } A\} \\
K & = & \mathbb{F}_q(t) \\
K_\infty & = & \mathbb{F}_q((1/t)) = \text{completion of } K \text{ at } \infty \\
C_\infty & = & \text{completion of algebraic closure of } K_\infty \\
[n] & = & t^{q^n} - t \\
d_n & = & \prod_{i=0}^{n-1}(t^{q^n} - t^{q^i}) \\
\ell_n & = & \prod_{i=1}^{n}(t - t^{q^i}) \\
\deg & = & \text{function assigning to } a \in A \text{ its degree in } t
\end{array}$$

The purpose of this expository talk is to describe some fascinating recent developments in the Function Field Arithmetic and hopefully get some bright students working in this rapidly developing subject area. Though this name 'Function Field Arithmetic' of the subject

This is the text of Invited Talk delivered at the Centenary year 73^{rd} Annual Conference of Indian Mathematical Society, held at the University of Pune, Pune-411007 during December 27-30, 2007.

might be unfamiliar to some, in fact, we all know the subject at some level.

Let us look a little closely (and perhaps a little simplistically) at how the concept of numbers and arithmetic evolves in school. In school, we first learn the concept of and manipulations with the 'counting numbers'. Then we see that many simple day-to-day problems can be formulated into linear equations involving counting numbers and to solve these it is helpful to introduce zero, negative numbers and fractions (i.e. rational numbers). But once we introduce the unknown or variable 'x', just as starting from zero, one and addition, subtraction, multiplication leads us to ring of integers $\mathbb{Z}$ and with division, the field of rational numbers $\mathbb{Q}$, adding x to zero and one, we are led to the polynomial ring and the field of rational functions (say with $\mathbb{Q}$-coefficients to start with). In addition to dealing with polynomial equations with unknown etc., we also learn to manipulate with polynomials and rational functions on equal footing with the integers and rational functions: Arithmetic operations, multiplication and division algorithms, factorizations into primes or irreducible polynomials respectively, greatest common divisors and so on. This is the introduction everybody has to the Function Field Arithmetic at its simplest level.

Soon, either through the geometric concept of length or the calculus concept of limits, we are introduced to real numbers and calculus also leads to power series and Laurent series through Taylor series developments.

Finally, we get the best analogies when we take the coefficient field of polynomials, rational functions or Laurent series to be a finite field, rather than say $\mathbb{Q}$ or $\mathbb{R}$ etc. for the simple reason that when we divide an integer by another non-zero integer n say, there are finitely many possibilities for the remainder, i.e. non-negative integers smaller than $|n|$, but when you divide by a non-zero polynomial n, a remainder can be any polynomial of smaller degree and hence there are infinitely many possibilities, unless the coefficient field is finite.

(While function fields with complex coefficients are also very useful sources of analogies with connections to Riemann surfaces and complex analysis techniques, for number theory, finite field coefficient are better for the reason explained).

In summary, we have the basic analogies:

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C}\ \iff\ A=\mathbb{F}_q[t],\ K=\mathbb{F}_q(t),\ K_\infty=\mathbb{F}_q((1/t)),\ C_\infty$$

where we have replaced x by more traditional choice t in this subject.

For usual numbers, the notion of the size is the usual absolute value while for rational functions it is the absolute value coming through 'degree', which is 'non-archimedean', in the sense that degree of the addition is at most the maximum of the degrees of the terms added, which is stronger than the usual 'triangle inequality'. But the difference in the two cases is not so huge once we realize that, in fact, in addition to these notions of 'size at infinite prime', there are notions of sizes for numbers and functions for each prime and irreducible polynomials respectively and all these so-called p-adic absolute values are non-archimedean. There is moreover a 'product formula' $\prod |k| = 1$ where the product is over all the absolute values suitably normalized.

A famous theorem of Artin-Whaples says roughly that any field with notions of sizes linked by the product formula is a finite extension of $\mathbb{Q}$ (i.e. a number field) or of $k(x)$ (i.e., a function field) for some field k. Thus (with k finite, as explained above) these fields, called global fields, are studied together in number theory. A nice parallel treatment of basic algebraic number theory and even the class field theory (i.e. theory of abelian extensions) was given for both global number and function fields in the first half of the last century.

Important success during that period is the proof, due to Hasse and Weil, of the Riemann hypothesis for function fields (for its higher dimensional generalization, Deligne got the 1978 Fields medal), for the zeta function defined by Artin by following an analogy with Riemann and Dedekind zeta functions. Namely, we associate a zeta function to a global field by the Euler product

$$\zeta(s)=\prod(1-\mathrm{Norm}(\wp)^{-s})^{-1},$$

where the product is over all 'non-archimedean primes' $\wp$ and the norm of a prime is number of residue (remainder) classes it has. This zeta function converges in certain half plane and can be continued to the whole complex plane. But it is a complex-valued (not C_∞-valued) simple rational function in q^{-s} for function fields over $\mathbb{F}_q$ and thus looses rich transcendental nature of Riemann zeta and special values involving π etc.

Work of Carlitz in 1930's and work of Drinfeld in 1970's brought in a new type of analogies introducing C_∞-valued analogs of exponential and zeta. We will give quick introduction, but refer to the literature mentioned below for motivation and more properties and analogies.

The Carlitz exponential is

$$e(z) = \sum z^{q^i} / \prod_{j=0}^{i-1} (t^{q^i} - t^{q^j}) = \sum z^{q^i}/d_i$$

For $a \in A$, define the polynomial $C_a(z)$ as follows: Put

$$C_1(z) = z, \quad C_t(z) := tz + z^q, \quad C_{t^n}(z) := C_{t^{n-1}}(C_t(z))$$

and extend by $\mathbb{F}_q$-linearity in a. Then the exponential satisfies for $a \in A$, a functional equation $e(az) = C_a(e(z))$ analogous to classical $e^{nz} = (e^z)^n$, for $n \in \mathbb{Z}$. This leads to analogous situation

$$a \to z \mapsto C_a(z) : A \to \text{End } G_a \quad \Longleftrightarrow \quad n \to (z \mapsto z^n) : \mathbb{Z} \to \text{End } G_m,$$

where G_a and G_m are the additive and multiplicative group respectively.

Just as the usual exponential has a period lattice $2\pi i\mathbb{Z}$, the Carlitz exponential has period lattice: $\tilde{\pi}A$ for some $\tilde{\pi} \in C_\infty$. With this analogs of e and $2\pi i$, we have analogs of 'a-th roots of unity':

$$\{e(\tilde{\pi}b/a) : b \in A\}$$

indexed by $a \in A$. Adjoing these to K gives an abelian extension of K with Galois group $(A/(a))^*$. (Note that these are just the roots of the 'cyclotomic polynomials' $C_a(z)$, by the functional equations above).

This cyclotomic theory was developed into an explicit class field theory for K and general function fields by work of Drinfeld and Hayes in 1970's and 1980's. In fact, generalizations (using similar objects with more general function fields and rank n period lattices) due to Drinfeld and many others eventually established Langlands correspondence between n-dimensional Galois representations and automorphic representations of Gl_n in the function field case. This led to the Fields medal to Drinfeld in 1990 for $n = 2$ case and to Lafforgue in 2002 for the general case.

In this talk, we focus instead on the arithmetic nature of special values of functions that come up in these new analogies. We focus on logarithms, Gamma (two of them) and Zeta. Let us introduce them. (Look at the references below for more details, motivation and properties).

The logarithm is the (multivalued) inverse function to the exponential and a simple branch is concretely given as

$$\log(z) = \sum_{n=0}^{\infty} \frac{z^{q^n}}{\ell_n}$$

Comparison of the Taylor series of the Carlitz exponential with the usual one shows that d_i should be analog of $q^i!$. More generally, Carlitz-Goss factorial is defined by (where we divide by appropriate power of t's to make infinite product convergent to make an interpolation)

$$n! := \prod (d_i/t^{deg(d_i)})^{n_i} \in K_\infty, \text{ where } n = \sum n_i q^i \in \mathbb{Z}_p, \ 0 \leq n_i < q$$

Another Gamma function, with poles at $-A_+ \cup \{0\}$, is defined by

$$\Gamma(z) = \frac{1}{z} \prod_{a \in A+} (1 + \frac{z}{a})^{-1} \in C_\infty, \quad z \in C_\infty$$

Both have nice functional equations in (different) analogies with the classical case, analogs of $(-1/2)! = \sqrt{\pi}$ have interpolations at finite primes with special values of these connecting with algebraic Gauss sums analogs.

Finally the Carlitz Zeta values are defined by

$$\zeta(s) = \sum_{a \in A_+} \frac{1}{a^s} \in K_\infty, \qquad s \in \mathbb{Z}_+.$$

Carlitz' analog of Euler theorem is

$$\zeta(s)/\tilde{\pi}^s \in K \text{ for } s \text{ 'even', i.e multiple of } q-1$$

Finally we can state the recent strong transcendence and algebraic independence results:

Theorem 1. *The logarithms of algebraic quantities, if linearly independent over K, are algebraically independent over $\overline{K}$.*

Theorem 2. *All algebraic monomials in factorial values at fractions are the known ones.*

Theorem 3. *Only algebraic relations for Γ-values at proper fractions are those explained by functional equations.*

Theorem 4. *Only algebraic relations among the zeta values together with $\tilde{\pi}$ come from the Carlitz-Euler relation and $\zeta(ps) = \zeta(s)^p$.*

For complete statements and proofs we again refer to literature below.

Let us see comparison with what is known in the classical case as well the underlying structures involved and techniques used.

In the number fields case, in place of Theorem 1, Baker's famous theorem, for which he got Fields medal in 1970, proved 'linear' independence over $\overline{\mathbb{Q}}$ of logarithms of algebraic numbers, given the linear independence over $\mathbb{Q}$.

Theorem 1 proved by Matt Papanikolas uses the strong motivic machinery developed by Greg Anderson, which reduces algebraic dependency which is linear dependency of monomials to linear dependency questions by use of tensor powers of motives to make required monomials. The linear dependency techniques of Baker, Wustholz etc. were used and similar theorems were proved in the function field case by Jing Yu earlier.

Theorem 3 proved was proved earlier by Anderson, Brownawell and Papanikolas by similar techniques, using description of gamma values at fractions in terms of 'periods' of Anderson t-motives, to which Greg Anderson, his student Sinha and the author contributed. This algebraic incarnation of transcendental gamma values was achieved by method of 'solitons' and 'Fermat motives'.

For comparison with Theorem 2 and 3, it should be noted that classically even transcendence of individual gamma values at proper fractions (except for denominators 2, 3, 4, 6) is not known, let alone the algebraic independence.

For the factorial function of Theorem 2, the techniques of periods led to results in close analogy with the classical case mentioned above, so the Theorem 2 was proved by the author by a different technique called 'finite state automata' using a theorem of Christol that a power/Laurent series $\sum f_n t^{-n}$ in K_∞ is algebraic over K if and only if there a finite state q-automata which on input n gives output f_n.

For comparison with Theorem 4, note that classically we know $\zeta(3)$ is irrational, but not whether it is transcendental, and we do not know what happens at other odd integers, neither do we know whether $\zeta(3)/\pi^3$ is rational or irrational/transcendental.

The Theorem 4 was proved by Chieh-Yu Chang and Jing Yu using the techniques of Anderson-Brownawell-Papanikolas and Papanikolas and using the earlier result due to Anderson and the author which gave again algebraic incarnation of these transcendental zeta values in terms of Anderson's t-motives (which are higher dimensional generalizations of Carlitz module we looked at, in the sense that we looked at certain embeddings $A \to \text{End } G_a^d$).

Some of this may look too advanced, because it may be unfamiliar, so we end with mentioning a remarkable continued fraction formula, which can be proved by only high-school level mathematics, for $e = e(1)$.

Write $[a_0, a_1, a_2, \cdots]$ as a short-form for the continued fraction $a_0 + 1/a_1 + (1/a_2 + \cdots)$.

Let us start by remarking that continued fraction expansion is unique and canonical, with no need for choice of a base. Its truncations give best possible approximations for their complexity. We understand them well for rational and quadratic irrationals, but we do not know a pattern for a single higher degree algebraic number or say for π.

On the other hand, Euler proved for Euler's e the following exact formula:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \cdots].$$

In our case, we have completely different pattern (and proof). For simplicity, we specialize to $A = \mathbb{F}_2[t]$ example. Write $[n] = t^{2^n} - t$. Then

$$e = [1, [1], [2], [1], [3], [1], [2], [1], [4], \cdots],$$

where the pattern of block duplication
(whole block $[1].[2].[1], [3], [1], [2], [1]$ is repeated after [4], followed by [5] and so on) continues.

Here is another descriptions of the same pattern:
$a_n = [$ position of first 1 in n base 2$] = [\mathrm{ord}_2(2n)]$.

References and Guide to the literature: In our simplistic version here, we have, of course, omitted to mention many important contributions. Two books giving the background material are [6, 10], where you will find references and history. (This particular subject area started with [4]). Another nice book going at more relaxed pace is [9]. In particular, [10, 2.1] gives quick motivated introduction to many objects we are considering such as exponential, zeta and gamma, which are then developed in detail later; and the chapter 10 there explains automata technique and the proof of Theorem 2.

For proofs of other main results, see the original articles listed below and expository accounts in the books as well [8] and [11].

Note added in the galley proofs(14th July 2008): Chang, Papanikolas, Thakur and Yu proved that all the algebraic relations between factorial values at proper functions together with zeta values are the known ones.

Chang, Papanikolas, Yu proved similar statement for Γ-values and zeta values. The proofs again use the breakthrough criterion of [2] and [7]. Pellarin gave a simpler proof of Theorem 1 using ideas of Denis(together with those of Anderson and Papanikolas).

Acknowledgments: This paper is the written version of the invited talk with the same title that I delivered at the Centenary meeting of Indian Mathematical Society in Pune in December 2007. I would like to thank the organizers for the invitation as well as their hospitality.

I would also like thank the Ellentuck Fund and the von Neumann Fund for their support during my stay at the Institute for Advanced study, Princeton, where this paper was written.

References

[1] G. W. Anderosn, *t-motives.* Duke Math. J. **53**1985, 457-502.

[2] G. W. Anderson, W. D. Brownawell, M. A. Papanikolas, *Determination of the algebraic relations among special* Γ*-values in positive characteristic.* Ann. of Math. (2) **160**(2004), 237–313.

[3] G. W. Anderson and D. S. Thakur, *Tensor powers of the Carlitz module and zeta values*, Ann. of Math. (2) **132** (1990), 159–191.

[4] L. Carlitz, *On certain functions connected with polynomials in a Galois field,*Duke Math. J. **1** (1935), 139–158.

[5] C.Y. Chang and J. Yu, *Determination of algebraic relations among special zeta values in characteristic p*, Advances in Mathematics 216(2007), 321-345.

[6] D. Goss, *Basic structures of function field arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], **35**, Springer-Verlag, Berlin, 1996.

[7] M. Papanikolas, *Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms*, Invent. Math. 171 (2008), 123-174.

[8] F. Pellarin, *Aspects d'lindependance algebriques in caracteristique non nulle, d'Apres Anderson, Brownawell, Denis, Papanikolas, Thakur, Yu*, Seminaire Bourbaki, no. 973, March 2007

[9] M. Rosen, *Number theory in function fields*, Springer 2002.

[10] D. Thakur, *Function Field Arithmetic,*World Scientific Pub., 2004.

[11] D. Thakur, *Diophantine approximation and transcendence in finite characteristic*, Diophantine equations, pp. 265-278, Edited by N. Saradha, Published for Tata Institute of Fundamental Research by Narosa Pub. 2007.

[12] J. Yu, *Transcendence and special zeta values in characteristic p,* Ann. of Math. (2) 134 (1991), no. 1, 1–23.

[13] J. Yu, *Analytic homomorphisms into Drinfeld modules,* Ann. of Math. (2) 145 (1997), no. 2, 215–233.

Dinesh S. Thakur
University of Arizona, Tucson, AZ 85721 and
Institute for Advanced Study, Princeton, NJ 08540
E-mail address: `thakur@math.arizona.edu, thakur@math.ias.edu`