Analytic Theory of Function Fields.

Trevor D. Wooley, Fall 2024, Purdue University.

§1. Introduction to function fields.

We first need to introduce the concept of a function field as it pertains to this class. We shall need:

(a) $\mathbb{F}_p$, the finite field having p elements (for prime p), which we may choose to think of as being $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$.

(b) $\mathbb{F}_q$, the finite field having q elements, with $q = p^h$ for some prime p and $h \in \mathbb{N}$.

Recall that all finite fields having q elements are isomorphic to one another, so we may speak of "the" finite field of q elements.

We will make use of the standard properties of finite fields from basic courses in abstract algebra and Galois theory, though often explicitly recalling these properties. In particular, it is often useful to recall that the units of a finite field $\mathbb{F}_q$, which is to say the non-zero elements $\mathbb{F}_q^*$, form a multiplicative group generated by a single element (a <u>primitive root</u>), so

$$\mathbb{F}_q^* = \langle c \rangle \quad \text{for some } c \in \mathbb{F}_q^*.$$

(c) $\mathbb{F}_q[t]$, the ring of <u>polynomials</u> over the field $\mathbb{F}_q$,

$$\mathbb{F}_q[t] = \Big\{ \sum_{i=0}^{n} a_i t^i : a_i \in \mathbb{F}_q, \ n \geqslant 0 \Big\}.$$

As we learn in abstract algebra, the ring $\mathbb{F}_q[t]$ is a PID (Principal Ideal Domain), and hence also a UFD (Unique Factorisation Domain). It

has the finite unit group $\mathbb{F}_q^\times$, and shares many properties — not just these — in common with $\mathbb{Z}$ (the ring of integers).

This is our first analogy

Analogy 1: $\mathbb{F}_q[t] \longleftrightarrow \mathbb{Z}$.

A little experimentation reveals that a notion of positivity can be obtained by insisting that we consider lead coefficients restricted to be 1

Analogy 2: $\mathbb{F}_q[t]^+ \longleftrightarrow \mathbb{N}$

$\{f \in \mathbb{F}_q[t] : f \text{ monic}\} \quad \{1, 2, \dots\}$.

(d) $\mathbb{F}_q(t)$, the field of rational functions over the field $\mathbb{F}_q$.

This is our first example of a function field!

$\mathbb{F}_q(t)$ = field of fractions of $\mathbb{F}_q[t]$ (as defined in abstract algebra)

$= \left\{ \frac{f}{g} : f, g \in \mathbb{F}_q[t], \ g \neq 0 \right\}$.

Here, of course, we implicitly make use of an equivalence relation acting so that $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ if and only if $f_1 g_2 = f_2 g_1$.

Examples of elements of $\mathbb{F}_q(t)$: $\frac{1}{t}$, $\frac{1}{t^2+2}$, $\frac{t^3+3t+2}{t+5}$, t^3+1.

Analogy 3: $\mathbb{F}_q(t) \longleftrightarrow \mathbb{Q}$

(e) $\mathbb{F}_q((1/t))$, the field of formal Laurent series over the field $\mathbb{F}_q$.

This may be a new definition for the reader:

$$\mathbb{F}_q((1/t)) = \left\{ \sum_{n=N}^{\infty} \frac{a_n}{t^n} : a_n \in \mathbb{F}_q, \ N \in \mathbb{Z} \right\}.$$ (Note: N may be negative!)

The addition and multiplication relations work in the expected way, so that when $N \geq M$, one has

$$\sum_{n=N}^{\infty} \frac{a_n}{t^n} + \sum_{m=M}^{\infty} \frac{b_m}{t^m} = \sum_{\ell=N}^{\infty} \frac{c_\ell}{t^\ell},$$

where

$$c_\ell = \begin{cases} a_\ell, & \text{when } M < \ell \leq N, \\ a_\ell + b_\ell, & \text{when } \ell \leq M. \end{cases}$$

Also,

$$\left(\sum_{n=N}^{\infty} \frac{a_n}{t^n}\right)\left(\sum_{m=M}^{\infty} \frac{b_m}{t^m}\right) = \sum_{\ell=N+M}^{\infty} \frac{c_\ell}{t^\ell},$$

where

$$c_\ell = \sum_{\substack{n \geq N \\ m \geq M \\ n+m=\ell}} a_n b_m.$$

One can check the field axioms for this set equipped with these definitions for addition and multiplication. In particular, if $u \in \mathbb{F}_q((1/t)) \setminus \{0\}$, then $u^{-1} \in \mathbb{F}_q((1/t)) \setminus \{0\}$. (See Problem Sheet 1).

It follows that there is a copy of $\mathbb{F}_q(t)$ (and also $\mathbb{F}_q[t]$) inside $\mathbb{F}_q((1/t))$.

Analogy 4: $\mathbb{F}_q((1/t)) \longleftrightarrow \mathbb{R}$

A justification of this analogy requires a consideration of Cauchy sequences, and the introduction of a distance function, for $\mathbb{F}_q((1/t))$.

Notions of size: We are familiar with the degree of a polynomial

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \in \mathbb{F}_q[t],$$

namely $\deg(f) = \max\{ i \in \mathbb{Z}_{\geq 0} : a_i \neq 0 \}$. By convention, $\deg(0) = -\infty$.

A related quantity is the <u>absolute value</u> of $f \in \mathbb{F}_q[t]$

$$|f| = q^{\deg f} \qquad (\text{with } |0| = 0).$$

<u>Analogy 5 :</u>

$A := \mathbb{F}_q[t]$

$f \in \mathbb{F}_q[t]$.

$$\begin{array}{ccc} |f| = q^{\deg f} & \longleftrightarrow & |n| \qquad (n \in \mathbb{N}) \\ \| & & \| \\ |A/fA| & & |\mathbb{Z}/n\mathbb{Z}| \,. \end{array}$$

More generally, when $f/g \in \mathbb{F}_q(t)$, we define

$$\operatorname{ord}(f/g) = \deg f - \deg g, \qquad (\text{can be negative!})$$

and

$$|f/g| = q^{\operatorname{ord}(f/g)} = q^{\deg f - \deg g}.$$

Even more generally, when

$$\alpha = \sum_{n=N}^{\infty} \frac{a_n}{t^n} \in \mathbb{F}_q((1/t)), \qquad \text{with } a_n \in \mathbb{F}_q,$$

we define

$$\operatorname{ord}(\alpha) = \max\{-n \in \mathbb{Z} : a_n \neq 0\}$$

and

$$|\alpha| = q^{+\operatorname{ord}(\alpha)}.$$

One can check that $|\cdot|$ forms a valuation on $\mathbb{F}_q((1/t))$. Thus, we have

(i) $|\alpha| = 0$ if and only if $\alpha = 0$;

(ii) $|\alpha\beta| = |\alpha| \cdot |\beta|$, for $\alpha, \beta \in \mathbb{F}_q((1/t))$;

(iii) $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$ for $\alpha, \beta \in \mathbb{F}_q((1/t))$. [ultrametric inequality]

One can check that Cauchy sequences in $\mathbb{F}_q((1/t))$ converge to a limit

lying inside $\mathbb{F}_q((1/t))$. Moreover, one sees that $\mathbb{F}_q((1/t))$ is the completion of $\mathbb{F}_q(t)$ with respect to $|\cdot|$. This is analogous to $\mathbb{R}$ being the completion of $\mathbb{Q}$ with respect to the ordinary absolute value.

(f) $\mathbb{P}_q[t]$, the set of monic irreducible polynomials lying in $\mathbb{F}_q[t]$ (note the non-standard notation here!), sometimes called prime polynomials.

Analogy 6: $\pi \in \mathbb{P}_q[t]$ $\longleftrightarrow$ prime number in $\mathbb{N}$.

In the classical world of $\mathbb{Z}$, we have the famous Prime Number Theorem first proved by Hadamard and de la Vallée Poussin in 1896:

$$\pi(x) := \sum_{\substack{p \le x \\ p \text{ prime}}} 1 = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

In the function field world of $\mathbb{F}_q[t]$, we have Gauss' formula:

$$\sum_{\substack{\pi \in \mathbb{P}_q[t] \\ \deg(\pi) = n}} 1 = \frac{1}{n} \sum_{d \mid n} \mu(n/d)\, q^d = \frac{q^n}{n} + O\left(q^{n/2}/n\right),$$

in which $\mu(\cdot)$ denotes the Möbius function, defined by

$$\mu(n) = \begin{cases} (-1)^k, & \text{when } n \text{ is squarefree and a product of } k \text{ distinct primes;} \\ 0, & \text{when } n \text{ is not squarefree.} \end{cases}$$

Analogy 7: $\displaystyle\sum_{\substack{\pi \in \mathbb{P}_q[t] \\ \deg(\pi) = n}} 1 \sim \frac{q^n}{n}$ $\longleftrightarrow$ $\displaystyle\pi(x) \sim \frac{x}{\log x}$

Recall/ Note: $x \longleftrightarrow q^n$, $\log x \longleftrightarrow n$ $\Big\}$ $\displaystyle\frac{x}{\log x} \longleftrightarrow \frac{q^n}{n}$.

We shall see a proof of the Prime Number Theorem in function fields later. In this course, our goal is to understand, generalise, and make use of these analogies, especially as they relate to phenomena in analytic number theory (and discrete harmonic analysis).

§2. Polynomial equations and inequalities in function fields.

Certain equations and inequalities are easy to investigate in $\mathbb{F}_q[t]$ by virtue of the graded structure available. We spend a little time in this section to record such results, since no analogue is readily available in the "number field" setting.

We begin with a classical result on solubility in finite fields.

Theorem 2.1. (Chevalley–Warning, 1936) Let k be a finite field of characteristic p, and suppose that $f_1, \dots, f_r \in k[x_1, \dots, x_s]$, where $\deg(f_i) = d_i$ $(1 \le i \le r)$. Let $N(\underline{f})$ denote the number of solutions of the system of equations

$$f_i(\underline{x}) = 0 \quad (1 \le i \le r),$$

with $\underline{x} \in k^s$. Then, whenever $s > d_1 + \dots + d_r$, one has $p \mid N(\underline{f})$.

Proof. (Ax, 1964) Suppose that k has q elements (so that $q = p^h$ for some prime p). Then, for each $\underline{x} \in k^s$, and for $1 \le i \le r$, one has

$$1 - f_i(\underline{x})^{q-1} = \begin{cases} 1, & \text{when } f_i(\underline{x}) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Notice that, implicitly in the last statement, we regard $1 - f_i(\underline{x})^{q-1}$ as an element of k. Write $\bar{N}(\underline{f})$ for the element of k

corresponding to the residue class of $N(\underline{f})$ modulo p (under the canonical mapping). Then

$$\overline{N}(\underline{f}) = \sum_{\underline{x} \in k^s} \prod_{i=1}^{r} \left(1 - f_i(\underline{x})^{q-1} \right). \qquad (2\cdot1)$$

On expanding the latter product, a typical term takes the shape

$$\sum_{\substack{(\alpha_1,\dots,\alpha_s) \in \mathbb{Z}_{\geq 0}^s \\ \alpha_1+\dots+\alpha_s \leq (q-1)(d_1+\dots+d_r)}} c(\underline{\alpha})\, x_1^{\alpha_1} \dots x_s^{\alpha_s}, \qquad (2\cdot2)$$

where the $c(\underline{\alpha})$ are suitable elements of k, the precise definition of which need not detain us, save that $c(\underline{0}) = 1$ when all f_i have no constant terms.

Plainly, the term with $\underline{\alpha} = \underline{0}$ contributes to (2·1) an amount

$$c(\underline{0}) \sum_{\underline{x} \in k^s} 1 = c(\underline{0}) q^s = 0 \quad (\text{in } k).$$

Note that, since $s > d_1+\dots+d_r$ and $\alpha_1+\dots+\alpha_s \leq (q-1)(d_1+\dots+d_r)$, then each s-tuple $\underline{\alpha}$ occurring in the sum (2·2) satisfies the condition that, either

(i) $\alpha_j = 0$ for some j, or

(ii) $(q-1) \nmid \alpha_j$ for some j.

Let j be any such value, and consider the sum

$$\sum_{\underline{x} \in k^s} x_1^{\alpha_1} \dots x_s^{\alpha_s} = \left(\sum_{x_j \in k} x_j^{\alpha_j} \right) \prod_{i \neq j} \sum_{x_i \in k} x_i^{\alpha_i}. \qquad (2\cdot3)$$

Recalling that there exists some generator $c \in k^\times$ with $k^\times = \langle c \rangle$, we see that

$$\sum_{x_j \in k} x_j^{\alpha_j} = \begin{cases} \displaystyle\sum_{l=0}^{q-2} (c^l)^{\alpha_j} = \frac{(c^{\alpha_j})^{q-1} - 1}{c^{\alpha_j} - 1} = 0, & \text{when } (q-1) \nmid \alpha_j \\ 0, & \text{when } \alpha_j = 0. \end{cases}$$

On substituting this conclusion into (2·3), and thence into (2·2) and (2·1), we conclude that $\bar{N}(\underline{f}) = 0$ in k, whence $p \mid N(\underline{f})$. This completes the proof of the theorem. //

Corollary 2.2. Under the hypotheses of Theorem 2.1, if each f_i has no constant term, then $N(\underline{f}) \geq p$.

Proof. Note that $f_i(\underline{0}) = 0 \quad (1 \leq i \leq r)$, so $N(\underline{f}) \geq 1$. But $p \mid N(\underline{f})$, and hence $N(\underline{f}) \geq p$. //

This conclusion shows that when each f_i has no constant term, and in particular, when each f_i is homogeneous of positive degree, then the system of equations $f_i(\underline{x}) = 0 \quad (1 \leq i \leq r)$, has a solution $\underline{x} \in k^s \setminus \{\underline{0}\}$. (a non-trivial solution).

One can say more by working harder with exponential sums.

Theorem. (Katz, 1971). Let $f_1, \dots, f_r \in k[x_1, \dots, x_s]$ with k a finite field of characteristic p and cardinality q. Define

$$\mu = \left\lceil \frac{s - (d_1 + \cdots + d_r)}{\max d_i} \right\rceil,$$

where $d_i = \deg(f_i)$. Also, denote by $N(\underline{f})$ the number of solutions of the system of equations $f_i(\underline{x}) = 0 \quad (1 \leq i \leq r)$, with $\underline{x} \in k^s$. Then

$$q^{\mu} \mid N(\underline{f}).$$

The concept of C_i-fields. (a concept introduced by Lang in his thesis of 1952).

In this definition, and henceforth, we use the term form to refer to a homogeneous polynomial in one or more variables.

Definition 2.3. Let K be a field, and let $i \in \mathbb{Z}_{\geq 0}$. Suppose that for any form $f \in K[x_1, \ldots, x_s]$ of degree d with $s > d^i$, the equation $f(\underline{x}) = 0$ has a non-trivial solution $\underline{x} \in K^s \setminus \{\underline{0}\}$. Then the field K is called C_i.

It follows that a field K is C_0 if and only if K is algebraically closed. To see this, consider a binary form $g(x_1, x_2)$ lying in $K[x_1, x_2]$. The equation $g(x_1, x_2) = 0$ has a non-trivial solution provided that one of the equations $g(t, 1) = 0$ or $g(1, t) = 0$ has a solution $t \in K$, and the desired conclusion follows.

Theorem 2.4. Let k be a finite field. Then k is C_1.

Proof. It follows from the Chevalley-Warning theorem that when $f \in k[x_1, \ldots, x_s]$ is a form of degree d with $s > d$, then $f(\underline{x}) = 0$ has a non-trivial solution (see Corollary 2.2). Thus k is C_1. //

Building on earlier work of Tsen, Lang (in his thesis of 1952) showed that:

(i) When K is a C_i field, then whenever $f_1, \ldots, f_r \in K[x_1, \ldots, x_s]$ are forms of degree d with $s > r d^i$, then the equations

$$f_i(\underline{x}) = 0 \quad (1 \leq i \leq r)$$

have a simultaneous non-trivial solution $\underline{x} \in K^s \setminus \{\underline{0}\}$.

(ii) When K is a C_i field, and E is an algebraic extension of K, then E is a C_i field.

(iii) When K is a C_i field, and F is an extension of K having transcendence degree j, then F is a C_{i+j} field. In particular, when $t_1, \ldots, t_j$ are independent transcendental elements over K, then $K(t_1, \ldots, t_j)$ is a C_{i+j} field.

We aim to avoid some of the complications of the Lang-Nagata approach, and seek instead a conclusion more narrowly focused on function fields.

Definition 2.5. Let K be a field, and let $i \in \mathbb{Z}_{\geqslant 0}$. Suppose that for any polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_s]$ having no constant terms, of respective degrees $d_1, \ldots, d_r$, and with $s > d_1^i + \ldots + d_r^i$, the equations $f_1(\underline{x}) = \ldots = f_r(\underline{x}) = 0$ have a non-trivial solution $\underline{x} \in K^s \setminus \{\underline{0}\}$. Then the field K is called strongly C_i.

It follows from elimination theory (or algebraic geometry) that an algebraically closed field K is strongly C_0.

Theorem 2.6. Let k be a finite field. Then k is strongly C_1.

Proof: This follows directly from the Chevalley-Warning theorem. //

Theorem 2.7. Let K be a strongly C_i field. Then the field of rational functions $K(t)$ is a strongly C_{i+1} field.

Proof. Let $L = K(t)$, and suppose that $f_\ell \in L[x_1, \ldots, x_s]$ is

a polynomial with no constant term of degree d_ℓ, for $1 \le \ell \le r$, with $s > d_1^{i+1} + \dots + d_r^{i+1}$ variables. By clearing denominators of the coefficients of $f_1, \dots, f_r$, we may suppose without loss of generality that each coefficient lies in $K[t]$, and has degree at most h.

We take n to be a sufficiently large positive integer, and for $1 \le i \le s$ we put

$$x_i = y_{i0} + y_{i1} t + \dots + y_{in} t^n, \qquad (2.4)$$

where we consider the y_{ij} to be variables. Then

$$f_\ell(\underline{x}) = f_{\ell,0}(\underline{y}) + f_{\ell,1}(\underline{y})\, t + \dots + f_{\ell, d_\ell n + h}(\underline{y})\, t^{d_\ell n + h},$$

for suitable polynomials $f_{\ell,m}(\underline{y})$ in the $s(n+1)$ variables y_{ij} $(0 \le j \le n,\ 1 \le i \le s)$, all having no constant term, and having coefficients in K.

We seek a non-trivial solution $\underline{y} \in K^{s(n+1)} \setminus \{\underline{0}\}$ to the system of equations

$$f_{\ell,m}(\underline{y}) = 0 \qquad (1 \le \ell \le r,\ 0 \le m \le d_\ell n + h),$$

since in view of (2.4), this provides a solution $\underline{x} \in K(t)^s \setminus \{\underline{0}\}$ to the system of equations $f_\ell(\underline{x}) = 0$ $(1 \le \ell \le r)$. Since K is a strongly C_i field, such a solution exists provided that

$$s(n+1) > \sum_{\ell=1}^{r} \sum_{m=0}^{d_\ell n + h} \left(\deg(f_{\ell,m})\right)^i.$$

But $\deg(f_{\ell,m}) \le \deg(f_\ell) = d_\ell$, so this is assured provided that

$$s(n+1) > \sum_{\ell=1}^{r} (d_\ell n + h + 1)\, d_\ell^{\,i} = (n+1) \sum_{\ell=1}^{r} d_\ell^{\,i+1} + \sum_{\ell=1}^{r} (1 + h - d_\ell)\, d_\ell^{\,i}.$$

If we take n large enough, then this condition is satisfied whenever

$$s > \sum_{\ell=1}^{r} d_\ell^{\,i+1},$$

and thus $K(t)$ is a strongly C_{i+1} field. //

Corollary 2.8. The field $\mathbb{F}_q(t)$ is a strongly C_2 field.

One can apply the same ideas to handle algebraic and more general transcendental extensions.

Theorem 2.9. Let K be a strongly C_i field, and suppose that L is an extension of K which is of transcendence degree j over K. Then L is a strongly C_{i+j} field.

Proof. If L has transcendence degree j over K, then L is algebraic over $K(t_1, \dots, t_j)$ for some elements $t_1, \dots, t_j$ transcendental over K. Applying Theorem 2.7 inductively, we see that $K(t_1, \dots, t_j)$ is a strongly C_{i+j} field. It therefore suffices to show that whenever E is an algebraic extension of a strongly C_m field F, then E is strongly C_m.

Let E be an algebraic extension of F, and suppose that $f_\ell \in E[x_1, \dots, x_s]$ is a polynomial with no constant term of degree d_ℓ, for $1 \le \ell \le r$, with $s > d_1^m + \dots + d_r^m$ variables. The coefficients of the polynomials f_ℓ are all contained in a subfield E_0, algebraic over F and with $[E_0 : F] < \infty$. Let $\{\omega_1, \dots, \omega_n\}$ be an F-basis

for E_0. For $1 \le i \le s$, we put

$$x_i = y_{i1} w_1 + \cdots + y_{in} w_n, \qquad (2.5)$$

where we consider the y_{ij} to be variables. Then for suitable polynomials $f_{l,h}(\underline{y})$ in the sn variables y_{ij} $(1 \le j \le n, 1 \le i \le s)$, all having no constant term, and having coefficients in F.

We seek a non-trivial solution $\underline{y} \in \mathbf{F}^{sn} \setminus \{\underline{0}\}$ to the system of equations

$$f_{l,h}(\underline{y}) = 0 \qquad (1 \le l \le r, \ 1 \le h \le n),$$

noting that from (2.5), we then have a solution $\underline{x} \in E_0^s \setminus \{\underline{0}\}$ to the system $f_l(\underline{x}) = 0$ $(1 \le l \le r)$. Since F is a strongly C_m field, such a solution exists provided that

$$sn > \sum_{l=1}^{r} \sum_{h=1}^{n} \deg(f_{l,h})^m.$$

But $\deg(f_{l,h}) \le \deg(f_l) = d_l$, so this is assured provided that

$$sn > \sum_{l=1}^{r} n d_l^m = n \sum_{l=1}^{r} d_l^m.$$

This condition is satisfied whenever $s > \sum_{l=1}^{r} d_l^m$, and thus E is strongly C_m. //

Thus, any algebraic extension of $\mathbb{F}_q[t_1, \ldots, t_r]$ is strongly C_{r+1}. We note that whenever $f(x_1, \ldots, x_s)$ is a polynomial of degree d with coefficients in $\mathbb{F}_q(t)$, having no constant term, then it has a non-trivial solution $\underline{x}$ to $f(\underline{x}) = 0$ provided that $s > d^2$. However, it may be that fewer variables may ensure that a solution exists. Such issues can be addressed via modifications of the Hardy-Littlewood (circle) method.

We now turn to the topic of inequalities.

Theorem 2.10 (Dirichlet's approximation theorem).
Let $r \in \mathbb{N}$ and $\alpha \in \mathbb{F}_q((1/t))$. Then there exist unique polynomials $a, g \in \mathbb{F}_q[t]$ with g monic, $0 \leq \deg(g) \leq r$, $(a, g) = 1$, and

$$|g\alpha - a| < q^{-r}.$$

Proof. Let

$$\alpha = \sum_{i \leq I} \alpha_i t^i = \alpha_I t^I + \alpha_{I-1} t^{I-1} + \cdots \in \mathbb{F}_q((1/t)), \text{ with } \alpha_i \in \mathbb{F}_q,$$

and put

$$g = \sum_{j=0}^{r} g_j t^j, \quad \text{with } g_j \in \mathbb{F}_q. \qquad (2.6)$$

Then

$$g\alpha = \sum_{l \leq I+r} c_l t^l,$$

where

$$c_l = \sum_{\substack{i \leq I \\ i+j=l}} \sum_{0 \leq j \leq r} \alpha_i g_j. \qquad (2.7)$$

By applying linear algebra, the equations

$$\sum_{\substack{0 \leq j \leq r \\ l-j \leq I}} \alpha_{l-j} g_j = 0 \quad (-r \leq l \leq -1) \qquad (2.8)$$

have a non-trivial solution $g \in \mathbb{F}_q^{r+1} \setminus \{0\}$. Fix any one such solution, define g via (2.6), and suppose $d = \deg(g)$. We have $g_d \neq 0$, and we may replace g by $g_d^{-1} g$ to suppose without loss of generality that g is monic.

In view of (2.8), we find from (2.7) that $c_l = 0$ for $(-r \leq l \leq -1)$. Put $a = c_0 + c_1 t + \cdots + c_{I+r} t^{I+r}$ when $I + r \geq 0$, and 0 otherwise. Then

$$g\alpha = a + \sum_{l \leq -r-1} c_l t^l,$$

whence

$$|g\alpha - a| \leq q^{-r-1}.$$

Putting $g' = g/(g,a)$ and $a' = a/(g,a)$, we find that $|g'\alpha - a'| < q^{-r}$ with $(g',a') = 1$, giving the upper bound claimed in the statement.

It remains to establish the uniqueness of a, g subject to the hypotheses of the statement of the theorem. Suppose then that

$$|g_1\alpha - a_1| < q^{-r} \quad \text{and} \quad |g_2\alpha - a_2| < q^{-r},$$

with $0 \le \deg(g_i) \le r$, g_i monic and $(a_i, g_i) = 1$ $(i = 1,2)$. Then we have

$$|g_2 a_1 - g_1 a_2| \le \underbrace{|g_2(g_1\alpha - a_1) - g_1(g_2\alpha - a_2)|}_{\le \max\{|g_2||g_1\alpha - a_1|,\ |g_1||g_2\alpha - a_2|\}} < q^r \cdot q^{-r} = 1.$$

Thus $g_2 a_1 = g_1 a_2$, and since $(a_1, g_1) = (a_2, g_2) = 1$, it follows that $g_1 = g_2$ & $a_1 = a_2$, proving uniqueness. //

Notice that the graded structure of $\mathbb{F}_q((1/t))$ allows us to reduce this Diophantine approximation problem to a problem in linear algebra. By adapting these ideas, one can prove analogous conclusions for polynomials (see HW 1). When $\theta \in \mathbb{F}_q((1/t))$, define

$$\|\theta\| = \min_{a \in \mathbb{F}_q[t]} |\theta - a|.$$

Then one can show by using ideas from this section (note especially the Chevalley–Warning theorem) that when $\alpha \in \mathbb{F}_q((1/t))$, one has

$$\min_{0 \le \deg(n) \le N} \|\alpha n^k\| < q^{-N/k} \qquad (k \ge 1).$$

§ 3. The arithmetic of function fields.

We review some features of the arithmetic of the polynomial ring $A = \mathbb{F}_q[t]$, where $q = p^h$, with p prime and $h \in \mathbb{N}$.

Recall that there is a division algorithm, so given $u, v \in A$, with $v \neq 0$, there exist $g, r \in A$ with $u = gv + r$ satisfying either (a) $r = 0$ and $v \mid u$, or (b) $0 \leq \deg(r) < \deg(v)$ (with $r \neq 0$). Moreover, the polynomials g and r are uniquely defined with these properties.

This property allows us to consider congruences modulo v, for $v \in A \setminus \{0\}$, and the quotient ring

$$A/vA = \{ \bar{r} + vA : 0 \leq \deg(r) < \deg(v) \}.$$

Notice that $|A/vA| = q^{\deg(v)} = |v|$, since the representatives r of congruence classes modulo v are given by

$$r_0 + r_1 t + \cdots + r_V t^V \quad \text{where } V = \deg(v) - 1.$$

Two elements $f, g \in A$ are relatively prime if no polynomial $d \in A$ with $\deg(d) \geq 1$ satisfies $d \mid f$ and $d \mid g$.

There is an analogue of the Chinese Remainder Theorem, so if $m_1, \ldots, m_r \in A$ are pairwise coprime (pairwise relatively prime), and $m = m_1 \cdots m_r$, then

$$A/mA \cong A/m_1 A \oplus \cdots \oplus A/m_r A.$$

If $x_i \in A/m_i A$ $(1 \leq i \leq r)$, put $n_j = m/m_j$, $b_j \equiv n_j^{-1} \pmod{m_j}$,

$$x = n_1 b_1 x_1 + \cdots + n_r b_r x_r.$$

Then $x \equiv x_i \pmod{m_i}$ $(1 \leq i \leq r)$.

Now we consider multiplicative structure.

Theorem 3.1. Let $\pi \in A$ be a prime polynomial. Then $(A/\pi A)^\times$ is a cyclic group having $|\pi|-1$ elements.

Proof. Observe that $A/\pi A$ is a field having $|\pi|$ elements, so that $(A/\pi A)^\times = \langle c \rangle$, some $c \in (A/\pi A)^\times$. //

In particular, if $\deg(\pi) = d$ (and π is monic irreducible) then $|(A/\pi A)^\times| = q^d - 1$, and for each $a \in (A/\pi A)^\times$, one has

$$a^{q^d-1} \equiv 1 \pmod{\pi}. \qquad \text{(analogue of Fermat's Little Theorem)}$$

$$\| \qquad\qquad \text{Moreover, there exist elements of maximal order } |\pi|-1.$$

$$a^{|\pi|-1}$$

What about congruences modulo prime powers? The situation over $\mathbb{Z}$ is quite elegant:

(a) When p is an odd prime, then $(\mathbb{Z}/p^h\mathbb{Z})^\times$ is cyclic, with a single generator g known as a primitive root. Moreover, a primitive root g modulo p^2 is also primitive modulo p^h for all $h \geq 2$. (and also $h=1$!)

(b) When $h = 1$ or 2, $(\mathbb{Z}/2^h\mathbb{Z})^\times$ is cyclic, and when $h \geq 3$, one has $(\mathbb{Z}/2^h\mathbb{Z})^\times \cong (\mathbb{Z}/2) \oplus (\mathbb{Z}/2^{h-2}\mathbb{Z})$.

$$\| \qquad\qquad \|$$

$$\langle -1 \rangle \qquad \langle 5 \rangle$$

So $(\mathbb{Z}/2^h\mathbb{Z})^\times$ is close to being cyclic.

The situation is more complicated in the setting of $A = \mathbb{F}_q[t]$, where we recall that $q = p^h$.

Theorem 3.2. Suppose that $\pi \in A = \mathbb{F}_q[t]$ is a monic irreducible polynomial of degree d. Let $m \in \mathbb{N}$, and write l for the least positive integer with $p^l \geq m$. Then, for all $a \in (A/\pi^m A)^\times$, one has

$$a^{p^l(|\pi|-1)} \equiv 1 \pmod{\pi^m}.$$

Proof. Observe that

$$a^{|\pi|-1} \equiv 1 \pmod{\pi},$$

whence

$$a^{|\pi|-1} = 1 + \pi b,$$

for some $b \in A$. But then

$$(a^{|\pi|-1})^{p^l} = (1+\pi b)^{p^l} = 1 + \pi^{p^l} b^{p^l} \equiv 1 \pmod{\pi^{p^l}}.$$

Since $p^l \geq m$, we have shown that

$$a^{p^l(|\pi|-1)} \equiv 1 \pmod{\pi^m}. \quad //$$

Were it the case that $(A/\pi^m A)^\times$ be cyclic, then there would exist $a \in (A/\pi^m A)^\times$ having the property that

$$a^{p^l(|\pi|-1)} \equiv 1 \pmod{\pi^m}$$

only when

$$|\pi|^{m-1}(|\pi|-1) \mid p^l(|\pi|-1),$$

which is to say $(p^h)^{d(m-1)} \mid p^l$, or equivalently, $l \geq hd(m-1)$.

But $p^{h+1} \leq m$, so this is possible only when

$$p^{hd(m-1)} \leq pm.$$

One can see that this allows the possibilities (a) $m = 1$, (b) $m = 2$ and $h = d = 1$, or $p = 2$ and $hd = 2$, (c) $m = 3$, $p = 3$, $h = d = 1$.

We note that Theorem 3.2 provides a stronger conclusion than the function field analogue of Euler's theorem. In order to state this precisely, we define the analogue of Euler's function, for $v \in A$, namely

$$\phi(v) = |v| \prod_{\pi | v} (1 - 1/|\pi|),$$

where here, and throughout, we reserve π to denote a monic irreducible element of A (a prime polynomial).

Suppose that

$$v = v_0 \pi_1^{a_1} \cdots \pi_r^{a_r},$$

where $v_0 \in \mathbb{F}_q^\times$ and $a_i \in \mathbb{N}$, with π_i a prime polynomial. Then, in view of the Chinese Remainder Theorem, we have

$$(A/vA)^\times \cong (A/\pi_1^{a_1}A)^\times \otimes \cdots \otimes (A/\pi_r^{a_r}A)^\times,$$

so

$$|(A/vA)^\times| = \prod_{i=1}^{r} |(A/\pi_i^{a_i}A)^\times| = \prod_{i=1}^{r} |\pi_i|^{a_i - 1}(|\pi_i| - 1)$$

$$= \phi(v).$$

Theorem 3.3. Let $v \in A$ have degree at least 1. Then, for all $a \in (A/vA)^\times$, one has $a^{\phi(v)} \equiv 1 \pmod{v}$. //

From this theorem, we have $a^{|\pi|^{m-1}(|\pi|-1)} \equiv 1 \pmod{\pi^m}$, which as noted above is rarely as strong as Theorem 3.2.

§4. Prime polynomials.

We return to the topic of the analogue of the Prime Number Theorem in function fields:

$$\Pi_q(n) := \sum_{\substack{\pi \in A \\ \deg(\pi)=n}} 1 = \frac{1}{n} \sum_{d \mid n} \mu(n/d) q^d = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

There is an algebraic approach, which we do not pursue here, which begins by noting that if $\pi \in A$ has degree n, then the splitting field of π over $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_{q^n}$. One can now apply basic Galois Theory to study subfields of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$ to identify monic irreducible elements of various degrees and corresponding subfields.

We opt instead for an approach involving a zeta function.

Definition 4.1. The zeta function of $A = \mathbb{F}_q[t]$ is defined for $\mathrm{Re}(s) > 1$ by the infinite series

$$\zeta_A(s) = \sum_{\substack{u \in A \\ u \text{ monic}}} |u|^{-s}.$$

Thus, we have

$$\zeta_A(s) = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots = \frac{1}{1 - q^{1-s}}.$$

This function is analytic for $\mathrm{Re}(s) > 1$, and extends by analytic continuation to the whole complex plane to give a function meromorphic on $\mathbb{C}$ except for a simple pole at $s = 1$.

Putting

$$\xi_A(s) = q^{-s}(1 - q^{-s})^{-1} \zeta_A(s),$$

we find that

$$\xi_A(s) = q^{-s}(1-q^{-s})^{-1}(1-q^{1-s})^{-1} = (q^s-1)^{-1}(q^{s-1}-1)^{-1}q^{s-1} = \xi_A(1-s).$$

This gives an analogue of the functional equation for the classical zeta function $\xi(s) = \xi(1-s)$, where

$$\xi(s) = \tfrac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Euler Product: Recall that each monic polynomial can be uniquely written as a product of prime polynomials (since A is a UFD). Thus, when $\mathrm{Re}(s)>1$, we have

$$\zeta_A(s) = \sum_{\substack{u\in A\\ u \text{ monic}}} |u|^{-s} = \prod_{\substack{\pi\in A\\ \pi \text{ prime}}} \sum_{h=0}^{\infty} |\pi^h|^{-s} = \underbrace{\prod_{\substack{\pi\in A\\ \pi \text{ prime}}} (1-|\pi|^{-s})^{-1}}_{\text{Euler product representation.}}$$

We have exchanged an infinite sum for an infinite product here, and this requires some justification. Just observe that

$$\left| \sum_{\substack{u\in A\\ u \text{ monic}}} |u|^{-s} - \prod_{\substack{\pi\in A\\ \pi \text{ prime}\\ \deg(\pi)\le N}} (1-|\pi|^{-s})^{-1} \right| \le \sum_{\substack{u\in A\\ u \text{ monic}\\ \deg(u)>N}} |u|^{-s}$$

$$\le \frac{q^{N+1}}{q^{(N+1)s}} + \cdots$$

$$\le q^{(N+1)(1-s)}(1-q^{1-s})^{-1}$$

$$\longrightarrow 0 \quad \text{as} \quad N\to\infty. \qquad \square.$$

We are now equipped to give a simple proof of the prime number theorem in function fields.

Theorem 4.2. (Gauss, Dedekind) One has

$$\Pi_q(n) := \sum_{\substack{\pi \in \mathbb{A} \\ \deg(\pi)=n}} 1 = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d .$$

Proof. For the sake of convenience, we write $u = q^{-s}$, and then see that

$$\zeta_{\mathbb{A}}(s) = \frac{1}{1-qu} = \prod_{d=1}^{\infty} (1-u^d)^{-a_d},$$

by using the Euler product, and writing a_d for the number of monic irreducibles in $\mathbb{A}$ of degree d. Thus

$$-\log(1-qu) = -\sum_{d=1}^{\infty} a_d \log(1-u^d),$$

and by differentiating with respect to u,

$$\frac{q}{1-qu} = \sum_{d=1}^{\infty} \frac{d\, a_d\, u^{d-1}}{1-u^d} .$$

$$\Rightarrow \sum_{n=1}^{\infty} (qu)^n = \sum_{d=1}^{\infty} d\, a_d \sum_{m=1}^{\infty} (u^d)^m = \sum_{n=1}^{\infty} \left(\sum_{d|n} d\, a_d \right) u^n \quad \text{(using } n=md\text{)}$$

Comparing coefficients of u^n, we therefore deduce that

$$\sum_{d|n} d\, a_d = q^n ,$$

whence, by Möbius inversion,

$$n\, a_n = \sum_{d|n} \mu(n/d)\, q^d .$$

Thus, we have

$$\Pi_q(n) = a_n = \frac{1}{n} \sum_{d|n} \mu(n/d)\, q^d . \qquad //$$

Corollary 4.3. One has

$$\Pi_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Proof. We have

$$\Pi_q(n) = \frac{1}{n}\sum_{d|n} \mu(n/d)\, q^d = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right),$$

since if $d|n$ and $1 \le d < n$, then $d \le n/2$. //

Notice that

$$\sum_{\substack{\pi \in \mathbb{A} \\ \deg(\pi) \le n}} 1 = \sum_{m=0}^{n} \Pi_q(m) = \underbrace{\frac{q^n}{n} + \frac{q^{n-1}}{n-1} + \cdots + 1}_{\text{the discrete analogue of } li(x) = \int_2^x \frac{dt}{\log t}} + O\left(\frac{q^{n/2}}{n}\right)$$

Some basic consequences of the Prime Number Theorem:

In the classical setting ($\mathbb{Z}$), one has some useful consequences of the Prime Number Theorem

$$\sum_{p \le x} 1 \sim \frac{x}{\log x}$$

that can be derived with care:

$$\sum_{p \le x} \frac{1}{p} = \log\log x + O(1)$$

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} \sim C \log x \quad , \text{ with } C = e^{\gamma} \text{ and } \gamma = 0.577\ldots$$

In the function field setting, one has analogues of these results, though the proofs are made easier because one sums over <u>all</u> polynomials of each fixed degree up to some bound. This has algebraic significance, and summing over subsets of such sets of

polynomials leads to more difficult problems better resembling the classical analogue. We now illustrate ~~these~~ ideas.

Example 4.4. One has

$$\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg u \le n}} \frac{1}{|u|} = \sum_{d=0}^{n} \frac{q^d}{q^d} = n+1$$

(Note: monic polynomials)

[Compare $\sum_{n \le x} \frac{1}{n} \sim \log x$ with $x = q^n$].

Example 4.5. One has

$$\sum_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n}} \frac{1}{|\pi|} = \sum_{d=1}^{n} \frac{1}{q^d} \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right)\right)$$

$$= \sum_{d=1}^{n} \frac{1}{d} + O\left(\sum_{d=1}^{n} \frac{q^{-d/2}}{d} \right)$$

$$= \log n + O(1).$$

[Compare $\sum_{p \le x} \frac{1}{p} \sim \log\log x + O(1)$ with $x = q^n$].

Example 4.6. One has

$$-\log\left(\prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n}} \left(1 - \frac{1}{|\pi|}\right)\right) = -\log\left(\prod_{d=1}^{n} \prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi = d}} \left(1 - \frac{1}{|\pi|}\right)\right)$$

$$= -\sum_{d=1}^{n} \log\left(1 - 1/q^d\right) \cdot \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right)\right)$$

$$= \sum_{d=1}^{n} \left(\frac{1}{q^d} + \frac{1}{2q^{2d}} + \cdots\right)\left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right)\right)$$

$$= \sum_{d=1}^{n} \frac{1}{d} + O(1) = \log n + O(1).$$

A more careful examination here shows, in fact, ~~that~~ ~~there exists~~ a constant $C = C(q)$ having the ~~property that~~

$$-\log\left(\prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n}} \left(1 - \frac{1}{|\pi|}\right)\right) = \log n + C + o(1), \text{ as } n \to \infty.$$

Thus

$$\prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n}} \left(1 - \frac{1}{|\pi|}\right)^{-1} \sim e^{C} n \quad \text{as} \quad n \to \infty.$$

[Compare $\prod_{p \le x} (1 - \frac{1}{p})^{-1} \sim e^{\gamma} \log x$, with $x = q^n$].

---

§5. Arithmetic functions and Dirichlet Series.

Definition 5.1. (a) We say that a function $f : \mathbb{F}_q[t] \setminus \{0\} \to \mathbb{C}$ is an arithmetic function.

(b) An arithmetic function f is called multiplicative if

(i) $f(a) = 1$ for all $a \in \mathbb{F}_q^*$, and

(ii) $f(uv) = f(u)f(v)$ whenever $(u,v) = 1$.

Suppose that $u \in \mathbb{F}_q[t]^*$ has prime polynomial factorization

$$u = u_0 \pi_1^{a_1} \cdots \pi_r^{a_r},$$

with $u_0 \in \mathbb{F}_q^*$, and π_i monic irreducible, $a_i \in \mathbb{N}$. Then

$$f(u) = f(\pi_1^{a_1}) \cdots f(\pi_r^{a_r}),$$

just as in the analogous classical theory.

Writing $a^h \| b$ when $a^h | b$ but $a^{h+1} \nmid b$, we then have

$$f(u) = \prod_{\pi^h \| u} f(\pi^h)$$

as shorthand for the previous statement.

We shall usually restrict attention to arithmetic (and multiplicative) functions defined on the monic polynomials $\mathbb{F}_q[t]^+$.

Convolutions. The (Dirichlet) convolution of two arithmetic functions f and g is defined for $u \in \mathbb{F}_q[t]^+$ by defining

$$(f*g)(u) = \sum_{\substack{d|u \\ d \in \mathbb{F}_q[t]^+}} f(d)\, g(u/d).$$

Exercise: Confirm that when f and g are multiplicative functions, then so too is $f*g$.

Familiar arithmetic functions:

$$1_{\mathbb{A}}(u) = \begin{cases} 1, & \text{when } u \in \mathbb{F}_q[t]^+ \\ \end{cases} \qquad \text{(multiplicative)}$$

$$\tau(u) = \sum_{\substack{d|u \\ d \in \mathbb{F}_q[t]^+}} 1 = 1_{\mathbb{A}} * 1_{\mathbb{A}}(u) \qquad \text{(multiplicative)}.$$

$$\tau_k(u) = \underbrace{(1_{\mathbb{A}} * 1_{\mathbb{A}} * \cdots * 1_{\mathbb{A}})(u)}_{k\text{-fold convolution}} \qquad \text{(multiplicative)}$$

$$\phi(u) = |u| \prod_{\pi | u} \left(1 - 1/|\pi|\right) \qquad \text{(multiplicative)}.$$

Note: $(\phi * 1_{\mathbb{A}})(u) = |u|$ (multiplicative).

$$\sigma(u) = \sum_{\substack{d | u \\ d \in \mathbb{F}_q[t]^+}} |d| = (1_{\mathbb{A}} * |\cdot|) \qquad \text{(multiplicative)}.$$

$$\mu(u) = \begin{cases} (-1)^k, & \text{when } u = \pi_1 \dots \pi_k \text{ is a product of } k \text{ distinct prime polynomials.} \\ 0, & \text{otherwise.} \end{cases} \qquad \text{(multiplicative)}$$

Then $(\mu * 1_{\mathbb{A}})(u) = \begin{cases} 1, & \text{when } u = 1 \\ 0, & \text{otherwise.} \end{cases}$

$\omega(u) = \sum_{\pi | u} 1$ = the number of distinct prime polynomial divisors of u

$\Omega(u) = \sum_{\pi^h \| u} h$ = total number of prime divisors of u, counted with multiplicity.

Exercise: Check that $\mu(u)^2$, $2^{\omega(u)}$ and $\mu(u)^2(-1)^{\omega(u)}$ are all multiplicative functions.

Connection with Dirichlet series. Given an arithmetic function $f : \mathbb{F}_q[t]^+ \to \mathbb{C}$, one can define the Dirichlet series

$$D_f(s) = F(s) := \sum_{u \in \mathbb{F}_q[t]^+} f(u) |u|^{-s}.$$

If one has $|f(u)| \le |u|^B$ for all $u \in \mathbb{F}_q[t]^+$, then this series converges absolutely for $\mathrm{Re}(s) > 1 + B$.

Note: One has $D_1(s) = \sum_{u \in \mathbb{F}_q[t]^+} |u|^{-s} = \zeta_A(s)$

$= 1/(1-q^{1-s})$.

Connection with convolution: Suppose that f and g are arithmetic functions, and the associated Dirichlet series $D_f(s)$ and $D_g(s)$ both converge absolutely in the half-plane $\mathrm{Re}(s) > \sigma_0$. Then one has

$$D_f(s) D_g(s) = \left(\sum_{u \in \mathbb{F}_q[t]^+} f(u) |u|^{-s} \right) \left(\sum_{v \in \mathbb{F}_q[t]^+} g(v) |v|^{-s} \right)$$

$$= \sum_{w \in \mathbb{F}_q[t]^+} \left(\sum_{\substack{u | w \\ u \text{ monic}}} f(u) g(w/u) \right) |w|^{-s}$$

$$= \sum_{w \in \mathbb{F}_q[t]^+} (f * g)(w) \cdot |w|^{-s} = D_{f*g}(s),$$

provided that $\mathrm{Re}(s)$ is sufficiently large.

Examples: $D_\tau(s) = \zeta_A(s)^2$, since $\tau = 1_A * 1_A$

$\zeta_A(s) D_\mu(s) = 1$

$\dfrac{\zeta_A(s-1)}{\zeta_A(s)} = D_\mu(s) \zeta_A(s-1) = D_\phi(s)$

} Exercises.

The sizes of arithmetic functions and their average values:

Just as in the classical situation over $\mathbb{Z}$, one can apply multiplicative structure to bound multiplicative functions by

making use of prime (polynomial) factorisations. Some basic examples follow:

Theorem 5.2. Let $\varepsilon > 0$. Then there exists a positive number $C(\varepsilon)$ having the property that, whenever $u \in \mathbb{F}_q[t]^+$, one has

$$\tau(u) \leq C(\varepsilon) |u|^{\varepsilon}.$$

Proof. The basic observation is that, whenever

$$u = \prod_{\pi^h \| u} \pi^h,$$

one has

$$\tau(u) = \prod_{\pi^h \| u} \tau(\pi^h) = \prod_{\pi^h \| u} (h+1).$$

Consequently, one has

$$\frac{\tau(u)}{|u|^{\varepsilon}} = \prod_{\pi^h \| u} \frac{h+1}{|\pi|^{h\varepsilon}}.$$

Examine the function $(h+1)/q^{dh\varepsilon}$ as a function of d. One has

$$\frac{h+1}{|\pi|^{h\varepsilon}} \leq \frac{h+1}{2^{dh\varepsilon}}.$$

Provided that $d \geq \frac{1}{\varepsilon} \frac{\log_2(h+1)}{h}$, it follows that $\frac{h+1}{|\pi|^{h\varepsilon}} \leq 1$ (with $\operatorname{ord}(\pi) = d$). But $\frac{\log_2(h+1)}{h} \leq \frac{\log_2(1+1)}{1} = 1$, so one has $\frac{h+1}{|\pi|^{h\varepsilon}} \leq 1$ whenever $d \geq 1/\varepsilon$. Meanwhile, for smaller values of d, we see that $(h+1)/|\pi|^{h\varepsilon}$ achieves its maximum either at $h = 1$, or (by taking logarithms and differentiating) at

the integer nearest to the solution of

$$\frac{1}{h+1} = \varepsilon \log |\pi| \quad \Rightarrow \quad \frac{h+1}{|\pi|^{h\varepsilon}} \le \frac{1 + 1/(\varepsilon \log |\pi|)}{e^{(h-1)/h}} < 1 + \frac{2}{\varepsilon}.$$

Then in either case we have

$$\frac{h+1}{|\pi|^{h\varepsilon}} < 2 + 2/\varepsilon,$$

whence

$$\frac{\tau(u)}{|u|^{\varepsilon}} \le \prod_{\substack{\pi^h \| u \\ \deg(\pi) < 1/\varepsilon}} (2 + 2/\varepsilon) \le (2 + 2/\varepsilon)^{q^{1/\varepsilon}}.$$

Put $C(\varepsilon) = (2 + 2/\varepsilon)^{q^{1/\varepsilon}}$, and we conclude that $\tau(u) \le C(\varepsilon) |u|^{\varepsilon}$. //

Theorem 5.3. There is a positive constant $C = C(q)$ having the property that, whenever $u \in \mathbb{F}_q[t]^+$ has large enough degree, then

$$\phi(u) \ge C |u| / \log_q \log_q |u|.$$

Proof. We have

$$\phi(u) = |u| \prod_{\pi | u} (1 - 1/|\pi|).$$

This quantity is smallest when u is a product of the smallest possible prime polynomials. Motivated by this observation, we consider

$$\Omega_n := \prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n}} \pi,$$

and consider the largest natural number n such that $|\Omega_n| \le |u|$.

Observe that

$$\log_q |\mathcal{U}_n| = \sum_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n}} \log_q |\pi| = \sum_{d=1}^{n} d \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d} \right) \right) = \frac{q^{n+1}-1}{q-1} + O(q^{n/2}).$$

Thus $n = \log_q \log_q |\mathcal{U}_n| + O(1) \le \log_q \log_q |u| + O(1)$, and we see that

$$\phi(u) \ge |u| \prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \le n+1}} \left(1 - 1/|\pi|\right) \sim |u| / e^{C_1 (n+1)},$$

where C_1 is the constant obtained in our analogue of Mertens' theorem. Hence

$$\phi(u) \ge C(q) |u| / \log_q \log_q |u|,$$

for a suitable positive constant $C(q)$. //

Averages of arithmetic functions.

One can, of course, proceed by analogy with classical treatments to determine averages of arithmetic functions. Thus, for example, one may consider the average of $\tau(n)$ via a divisor sum

$$\frac{1}{x} \sum_{1 \le n \le x} \tau(n) = \frac{1}{x} \sum_{1 \le n \le x} \sum_{d \mid n} 1 = \frac{1}{x} \sum_{1 \le d \le x} \sum_{m \le x/d} 1$$

$$= \frac{1}{x} \sum_{1 \le d \le x} \left(\frac{x}{d} + O(1) \right) = x \sum_{1 \le d \le x} \frac{1}{d} + O(x)$$

$$= x \log x + O(x).$$

Indeed, one can obtain sharper conclusions by considering the ranges $1 \le d \le x^{1/2}$ and $d > x^{1/2}$ separately. One may imitate this approach in the function field setting, but another idea is available.

(32) Example 5.4.

Observe that

$$D_\tau(s) = \zeta_A(s)^2 = (1-q^{1-s})^{-2}$$

$$\| $$

$$\sum_{u\in \mathbb{F}_q[t]^+} \tau(u)\,|u|^{-s} = \sum_{d=0}^{\infty} \Big(\sum_{\substack{u\in \mathbb{F}_q[t]^+ \\ \deg(u)=d}} \tau(u) \Big) q^{-ds} .$$

One may therefore evaluate

$$T_q(d) := \sum_{\substack{u\in \mathbb{F}_q[t]^+ \\ \deg(u)=d}} \tau(u) ,$$

by comparing coefficients on left and right hand sides of the above relation, noting that absolute convergence is assured for $\mathrm{Re}(s)$ large enough.

We have (writing $w = q^{-s}$) the expansion

$$(1-qw)^{-2} = \sum_{n=0}^{\infty} (n+1)(qw)^n \qquad \Big(\text{consider } \frac{d}{dw}(1-qw)^{-1} \Big).$$

Thus

$$\sum_{n=0}^{\infty} (n+1)(qw)^n = \sum_{d=0}^{\infty} T_q(d)\, w^d ,$$

whence

$$T_q(d) = (d+1)q^d \qquad (d \geq 0) .$$

Consequently,

$$\sum_{\substack{u\in \mathbb{F}_q[t]^+ \\ \deg(u)\leq n}} \tau(u) = (n+1)q^n + nq^{n-1} + \cdots + 1 .$$

Note that this argument works so well (compared with the classical arguments) because $T_q(d)$ corresponds to an algebraic object

counting points in $\mathbb{F}_q$ on a variety.

Example 5.5. Observe that with $f(u) = \varphi(u)/|u|$, one has

$$D_f(s) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{\varphi(u)}{|u|^{s+1}} = \prod_{\pi} \left(1 + \sum_{h=1}^{\infty} \frac{\varphi(\pi^h)}{|\pi|^{h(s+1)}} \right)$$

$$= \prod_{\pi} \left(1 + \frac{|\pi|-1}{|\pi|} \frac{1}{|\pi|^s - 1} \right)$$

$$= \prod_{\pi} \left(\frac{|\pi|^{s+1} - 1}{|\pi|^{s+1} - |\pi|} \right) = \prod_{\pi} \left(\frac{1 - |\pi|^{-1-s}}{1 - |\pi|^{-s}} \right)$$

$$= \zeta_A(s) / \zeta_A(s+1).$$

Write $w = q^{-s}$. Then $\zeta_A(s) = (1 - qw)^{-1}$, whence

$$D_f(s) = \frac{1-w}{1-qw},$$

and we obtain

$$\frac{1-w}{1-qw} = D_f(s) = \sum_{d=0}^{\infty} \left(\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) = d}} \frac{\varphi(u)}{|u|} \right) w^{+d}$$

$$\| $$

$$(1-w)(1+qw+q^2w^2+\cdots) = 1 + (q-1)w + (q^2-q)w^2 + \cdots$$

Hence

$$\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) = d}} \frac{\varphi(u)}{|u|} = q^d(1 - 1/q) = q^d / \zeta_A(2).$$

This may be compared with the classical asymptotic formula

$$\sum_{1 \le n \le x} \frac{\varphi(n)}{n} \sim \frac{6}{\pi^2} x. \qquad //$$

§6. Additive characters and Fourier series.

We have in mind proving an analogue of a (quantitative) version of Dirichlet's theorem concerning primes in arithmetic progression. This entails a consideration of multiplicative characters. A concrete approach to such matters entails a consideration of additive characters, and the associated temptation to introduce Fourier series in the function field setting.

We must first introduce an analogue of the exponential function relevant for our purposes. We suppose as usual that $q = p^h$ and consider $A = \mathbb{F}_q[t]$, so that A has characteristic p.

(a) First we define an additive character on $\mathbb{F}_p$. When $a \in \mathbb{F}_p$, we identify a with an element of $\{0, 1, 2, \dots, p-1\}$, and define

$$e_p(a) = e^{2\pi i a/p}.$$

Thus $e_p(\cdot) : \mathbb{F}_p \longrightarrow \mathbb{C}^\times$ (the multiplicative group of complex numbers with unit modulus).

This function satisfies

$$e_p(a+b) = e_p(a)\, e_p(b),$$

and defines an injective homomorphism.

We also have an orthogonality relation.

Lemma 6.1. One has

$$\frac{1}{p} \sum_{u \in \mathbb{F}_p} e_p(ua) = \begin{cases} 1, & \text{when } a = 0, \\ 0, & \text{when } a \in \mathbb{F}_p \setminus \{0\}. \end{cases}$$

Proof: When $a = 0$ the desired conclusion is self-evident. Meanwhile,

when $a \neq 0$, the map $u \mapsto au$ permutes the elements of $\mathbb{F}_p$, and one sees that

$$\sum_{u \in \mathbb{F}_p} e_p(ua) = \sum_{k=0}^{p-1} e^{2\pi i k/p} = 0,$$

by summing the geometric progression.

(b) Next we extend this definition to define an additive character

$$e_q(\cdot) : \mathbb{F}_q \longrightarrow \mathbb{C}^\times.$$

This involves the <u>trace</u> of an element $a \in \mathbb{F}_q$, which we may define via the relation

$$tr(a) = a + a^p + \cdots + a^{p^{k-1}}.$$

Recall that the Galois group $Gal(\mathbb{F}_q : \mathbb{F}_p)$ is generated by the Frobenius homomorphism $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $u \longmapsto u^p$, so (as should be the case) the trace of a is the sum of all the Galois conjugates of a. In particular, we have $tr(a) \in \mathbb{F}_p$. We then define

$$e_q(a) = e_p(tr(a)) = e^{2\pi i\, tr(a)/p}.$$

We again have a homomorphism $e_q : \mathbb{F}_q \longrightarrow \mathbb{C}^\times$ satisfying the property

$$e_q(a+b) = e_q(a)\, e_q(b),$$

by virtue of the additive property of the trace function. Moreover, we have an orthogonality relation once again.

Lemma 6.2. One has

$$\frac{1}{q}\sum_{u\in\mathbb{F}_q} e_q(ua) = \begin{cases} 1, & \text{when } a=0, \\ 0, & \text{when } a\in\mathbb{F}_q\setminus\{0\}. \end{cases}$$

Proof. When $a=0$, one has $e_q(ua)=1$, and the conclusion is clear. Meanwhile, when $a\neq 0$, the map $u\mapsto au$ permutes the elements of $\mathbb{F}_q$, and one sees that

$$\sum_{u\in\mathbb{F}_q} e_q(ua) = \sum_{v\in\mathbb{F}_q} e_q(v) = \sum_{v\in\mathbb{F}_q} e_p(\mathrm{tr}(v)). \qquad (6.1)$$

For each $c\in\mathbb{F}_p$, the number of solutions of the equation $\mathrm{tr}(v)=c$, which is to say

$$v + v^p + \dots + v^{p^{h-1}} = c,$$

with $v\in\mathbb{F}_q$, is at most p^{h-1}. Since every $v\in\mathbb{F}_q$ satisfies some one of these equations, for one of the p values $c\in\mathbb{F}_p$, we see that the number of solutions is precisely p^{h-1} for each $c\in\mathbb{F}_p$. Here, we recalled that $\mathrm{card}(\mathbb{F}_q) = p^h$. Thus

$$\sum_{v\in\mathbb{F}_q} e_p(\mathrm{tr}(v)) = p^{h-1}\sum_{c\in\mathbb{F}_p} e_p(c) = 0.$$

The desired conclusion is now immediate from (6.1). //

(c) Finally, we extend the definition of $e_q(\cdot)$ to define an additive character on $\mathbb{F}_q((1/t))$. Here, we take the opportunity to abbreviate $\mathbb{F}_q(t)$ to K and $\mathbb{F}_q((1/t))$ to K_∞.

When $\alpha\in K_\infty$, say

$$\alpha = \sum_{i \le N} \alpha_i t^i ,$$

with $\alpha_i \in \mathbb{F}_q$ and $N \in \mathbb{Z}$, we define the residue of α to be $\operatorname{res}(\alpha) = \alpha_{-1}$. The latter is just the coefficient of t^{-1}.

Then, we define $e : \mathbb{K}_\infty \longrightarrow \mathbb{C}^\times$ by defining

$$e(\alpha) = e_q(\operatorname{res}(\alpha)) . \qquad (6.2)$$

One can now define integrals of functions defined on $\mathbb{K}_\infty$ by making use of the natural (Haar measure) defined by letting

$$\alpha + \left(\frac{1}{t}\right)^n \{ \beta \in \mathbb{K}_\infty : |\beta| < 1 \} \quad \text{have measure } q^{-n},$$

uniformly for $\alpha \in \mathbb{K}_\infty$. In particular, if

$$T = \left\{ \sum_{i \le -1} \alpha_i t^i : \alpha_i \in \mathbb{F}_q \ (i \le -1) \right\},$$

then the measure of T is 1 and one sees that T is the analogue of the unit interval.

Now suppose that one has a function $F : \mathbb{K}_\infty \longrightarrow \mathbb{C}$. If $I \subseteq \mathbb{K}_\infty$ is a Haar-measurable set, one can define the integral

$$\int_I F(\alpha)\, d\alpha$$

to be equal to

$$\lim_{M \to \infty} q^{-M} \sum_{\alpha_N \in \mathbb{F}_q} \sum_{\alpha_{N-1} \in \mathbb{F}_q} \cdots \sum_{\alpha_{-M} \in \mathbb{F}_q} F(\alpha_N t^N + \cdots + \alpha_{-M} t^{-M}) ,$$

$$\alpha_N t^N + \cdots + \alpha_M t^{-M} + t^{-M} T \subseteq I$$

provided that this limit exists.

We have an orthogonality relation.

Lemma 6.3. One has

$$\int_{\mathbb{T}} e(u\alpha)\, d\alpha = \begin{cases} 0, & \text{when } u \in \mathbb{A}\setminus\{0\}, \\ 1, & \text{when } u = 0. \end{cases}$$

Proof. When $u=0$, one has

$$\int_{\mathbb{T}} e(u\alpha)\, d\alpha = \int_{\mathbb{T}} e(0)\, d\alpha = \int_{\mathbb{T}} d\alpha$$

$$= \lim_{M\to\infty} q^{-M} \sum_{\alpha_{-1}\in\mathbb{F}_q} \cdots \sum_{\alpha_{-M}\in\mathbb{F}_q} 1 \qquad = 1.$$

$$\alpha_{-1}t^{-1} + \cdots + \alpha_{-M}t^{-M} \in t^M\mathbb{T} \subseteq \mathbb{T}$$

Suppose, meanwhile, that $u \in \mathbb{F}_q[t]\setminus\{0\}$. Thus,

$$u = u_d t^d + \cdots + u_1 t + u_0,$$

for some $u_i \in \mathbb{F}_q$ with $u_d \in \mathbb{F}_q^*$. When $\alpha \in \mathbb{T}$, we may write

$$\alpha = \alpha_{-1}t^{-1} + \cdots + \alpha_{-r}t^{-r} + \cdots,$$

with $\alpha_i \in \mathbb{F}_q$, and then

$$\alpha u = \beta_{d-1}t^{d-1} + \cdots + \beta_{-r}t^{-r} + \cdots,$$

where

$$\beta_j = \sum_{l=0}^{d} \sum_{\substack{m\le -1 \\ l+m=j}} u_l \alpha_m \qquad (j \le d-1).$$

It follows that

$$\operatorname{res}(u\alpha) = \beta_{-1} = u_d\alpha_{-d-1} + \cdots + u_0\alpha_{-1},$$

whence

$$\lim_{M\to\infty} q^{-M} \sum_{\alpha_{-1}\in\mathbb{F}_q} \cdots \sum_{\alpha_{-M}\in\mathbb{F}_q} e\left(u\left(\alpha_{-1}t^{-1}+\cdots+\alpha_{-M}t^{-M}\right)\right)$$

$$\alpha_{-1}t^{-1}+\cdots+\alpha_{-M}t^{-M}+t^{-M}\mathbb{T}\subseteq\mathbb{T}$$

$$= q^{-d-1} \sum_{\alpha_{-1}\in\mathbb{F}_q} \cdots \sum_{\alpha_{-d-1}\in\mathbb{F}_q} e_q\left(u_d\alpha_{-d-1}+\cdots+u_0\alpha_{-1}\right)$$

$$= \prod_{j=1}^{d+1} \left(q^{-1} \sum_{\alpha_{-j}\in\mathbb{F}_q} e_q\left(u_{j-1}\alpha_{-j}\right)\right)$$

$$= \begin{cases} 0, & \text{when } u_{j-1}\in\mathbb{F}_q\setminus\{0\} \text{ for some } 1\le j\le d+1, \\ 1, & \text{when } u_{j-1}=0 \text{ for all } 1\le j\le d+1. \end{cases}$$

We thus conclude that

$$\int_{\mathbb{T}} e(u\alpha)\,d\alpha = \begin{cases} 0, & \text{when } u_0,\dots,u_d \text{ are not all } 0, \\ 1, & \text{when } u_0,\dots,u_d \text{ are all } 0. \end{cases}$$

$$= \begin{cases} 0, & \text{when } u\in\mathbb{F}_q[t]\setminus\{0\}, \\ 1, & \text{when } u=0. \end{cases} //$$

This orthogonality relation enables us to develop Fourier analysis for functions defined on $K_\infty = \mathbb{F}_q((1/t))$, and in particular for functions defined on $K_\infty/A = \mathbb{F}_q((1/t))/\mathbb{F}_q[t] \cong \mathbb{T}$.

Additive characters modulo g, for $g\in\mathbb{F}_q[t]^+$.

One has an orthogonality relation for the function

$$e(\cdot/g) : A/gA \longrightarrow \mathbb{C}^\times.$$

Lemma 6.4. Suppose that $g \in \mathbb{F}_q[t] \setminus \{0\}$ and $u \in \mathbb{F}_q[t]$. Then

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a|<|g|}} e\left(\frac{a}{g} u\right) = \begin{cases} 1, & \text{when } g \mid u, \\ 0, & \text{when } g \nmid u. \end{cases}$$

Proof. Suppose first that $g \mid u$. Then $u/g \in \mathbb{F}_q[t]$, and hence for each summand on the left hand side, one has

$$\frac{a}{g} u \in \mathbb{F}_q[t].$$

Then $\operatorname{res}\left(\frac{a}{g} u\right) = 0$, whence $e\left(\frac{a}{g} u\right) = e_q\left(\operatorname{res}\left(\frac{a}{g} u\right)\right) = e_q(0) = 1$.

We thus find that

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a|<|g|}} e\left(\frac{a}{g} u\right) = \frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a|<|g|}} 1 = \frac{|g|}{|g|} = 1. \quad \square$$

Now consider the situation in which $g \nmid u$. Let $d = (g, u)$, and then write $u_1 = u/d$ and $g_1 = g/d$. By considering the residues a modulo g_1, we see that

$$\sum_{\substack{a \in \mathbb{F}_q[t] \\ |a|<|g|}} e\left(\frac{a}{g} u\right) = \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a|<|g|}} e\left(\frac{a}{g_1} u_1\right) = \frac{|g|}{|g_1|} \sum_{\substack{b \in \mathbb{F}_q[t] \\ |b|<|g_1|}} e\left(\frac{b}{g_1} u_1\right).$$

Noting that the map $b \mapsto b u_1 \pmod{g_1}$ permutes the residues modulo g_1, since $(u_1, g_1) = 1$, we infer that

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a|<|g|}} e\left(\frac{a}{g} u\right) = \frac{1}{|g_1|} \sum_{\substack{c \in \mathbb{F}_q[t] \\ |c|<|g_1|}} e\left(c/g_1\right).$$

Now suppose that $g_1 = \gamma_0 + \gamma_1 t + \cdots + \gamma_r t^r$, with $\gamma_r \in \mathbb{F}_q^\times$ and $\gamma_i \in \mathbb{F}_q$ $(0 \le i < r)$. Then

$$\sum_{\substack{c \in \mathbb{F}_q[t] \\ |c| < |g_1|}} e\left(\frac{c}{g_1}\right) = \sum_{c_0, \dots, c_{r-1} \in \mathbb{F}_q} e\left(\frac{c_0 + c_1 t + \cdots + c_{r-1} t^{r-1}}{\gamma_0 + \gamma_1 t + \cdots + \gamma_r t^r}\right)$$

$$\boxed{c = c_0 + c_1 t + \cdots + c_{r-1} t^{r-1}}$$

$$= \sum_{c_0, \dots, c_{r-1} \in \mathbb{F}_q} e\Big(\underbrace{(c_0 + c_1 t + \cdots + c_{r-1} t^{r-1}) \cdot \frac{1}{\gamma_r t^r} \Big(1 + \frac{\gamma_{r-1}}{\gamma_r} \cdot \frac{1}{t} + \cdots + \frac{\gamma_0}{\gamma_r t^r}\Big)^{-1}}_{\frac{c_{r-1}}{\gamma_r} \cdot \frac{1}{t^r} + \cdots} \Big)$$

$$= \sum_{c_0, \dots, c_{r-2} \in \mathbb{F}_q} \sum_{c_{r-1} \in \mathbb{F}_q} e_q(c_{r-1}/\gamma_r)$$

$$= 0.$$

Hence

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g} u\right) = 0 \qquad \text{when } g \nmid u. \quad \square \quad //$$

Suppose now that $f : \mathbb{A} \to \mathbb{C}$ is an arithmetic function that is periodic with period g, for some $g \in \mathbb{A}$. Thus $f(u+g) = f(u)$ for all $u \in \mathbb{A}$. We define the <u>finite Fourier transform</u> $\hat{f} : \mathbb{A} \to \mathbb{C}$ by means of the relation

$$\hat{f}(k) = \frac{1}{|g|} \sum_{a \bmod g} f(a) e(-ka/g). \qquad (6.3)$$

A Fourier representation of f is then given by applying the orthogonality relation embodied in Lemma 6.4. Thus

$$f(b) = \sum_{a \bmod g} f(a) \cdot \frac{1}{|g|} \sum_{k \bmod g} e\left(\frac{k(b-a)}{g}\right)$$

$$= \sum_{k \bmod g} e\left(\frac{kb}{g}\right) \cdot \frac{1}{|g|} \sum_{a \bmod g} f(a)\, e\left(-\frac{ka}{g}\right),$$

whence

$$f(b) = \sum_{k \bmod g} \hat{f}(k)\, e(kb/g). \qquad (6.4)$$

Observe that we have an analogue of Parseval's identity / Plancherel's identity. Thus,

$$\sum_{b \bmod g} |f(b)|^2 = \sum_{b \bmod g} \Big| \sum_{k \bmod g} \hat{f}(k)\, e(kb/g) \Big|^2$$

$$= \sum_{b \bmod g} \sum_{k_1 \bmod g} \sum_{k_2 \bmod g} \hat{f}(k_1)\overline{\hat{f}(k_2)}\, e(b(k_1-k_2)/g),$$

so

$$\sum_{b \bmod g} |f(b)|^2 = |g| \sum_{k \bmod g} |\hat{f}(k)|^2. \qquad (6.5)$$

Equivalently,

$$\frac{1}{|g|} \sum_{b \bmod g} |f(b)|^2 = \sum_{k \bmod g} |\hat{f}(k)|^2.$$

Similar ideas may be developed, mimicking classical Fourier theory, for functions $f : \underset{\mathbb{K}_\infty/\mathbb{A}}{\Pi} \longrightarrow \mathbb{C}$ and their Fourier series.

§7. Multiplicative (Dirichlet) Characters.

By analogy with the classical setting (of $\mathbb{Z}$), we next consider characters on the multiplicative group $(\mathbb{A}/m\mathbb{A})^\times$, for $m \in \mathbb{A}$ with $\deg(m) \geq 1$.

Definition 7.1. Let $m \in \mathbb{A}$ have positive degree. A Dirichlet character modulo m is a totally multiplicative function $\chi : \mathbb{A} \to \mathbb{C}$, supported on the reduced residue classes a modulo m, having period m.

[By convention, we impose $\chi(a) = 0$ for $(a,m) \neq 1$.]

Thus, if χ is a Dirichlet character modulo m, then:

(a) $\chi(a + \ell m) = \chi(a)$, for all $a, \ell \in \mathbb{A}$;

(b) $\chi(ab) = \chi(a)\chi(b)$, for all $a, b \in \mathbb{A}$;

(c) $\chi(a) \neq 0$ if and only if $(a,m) = 1$.

By restricting χ to reduced residues modulo m, we may interpret χ as a function of $(\mathbb{A}/m\mathbb{A})^\times$ with

$$1 = \chi(1) = \chi(a^{\phi(m)}) = \chi(a)^{\phi(m)}, \quad \text{for } (a,m) = 1,$$

so that $\chi(a) \in \mathbb{C}^\times$. Thus

$$\chi : (\mathbb{A}/m\mathbb{A})^\times \longrightarrow \mathbb{C}^\times$$

defines a group homomorphism. Conversely, one sees that every group homomorphism from $(\mathbb{A}/m\mathbb{A})^\times$ into $\mathbb{C}^\times$ defines a Dirichlet character.

Some basic properties of Dirichlet characters modulo m:

(d) The principal character χ_0 is the character taking the value 1 on $(\mathbb{A}/m\mathbb{A})^\times$.

(e) Note that every Dirichlet character χ satisfies

$$\chi(1)^2 = \chi(1), \quad \text{whence} \quad \chi(1) = 1.$$

(f) As we observed above, one has for all $a \in (A/mA)^\times$ the relation

$$\chi(a)^{\phi(m)} = \chi(a^{\phi(m)}) = \chi(1) = 1,$$

so characters take values which are $\phi(m)$-th roots of unity.

(g) If χ_1 and χ_2 are two Dirichlet characters modulo m, then $\chi_1\chi_2$ is a Dirichlet character modulo m (check (a), (b), (c)).

Here, $\chi_1\chi_2(a) := \chi_1(a)\chi_2(a)$ whenever $a \in (A/mA)^\times$.

(h) When χ is a Dirichlet character modulo m, then so too is the conjugate character $\bar{\chi}$. Moreover, for each $a \in (A/mA)^\times$, one has $1 = \chi(a)\bar{\chi}(a) = \chi\bar{\chi}(a)$, so that $\bar{\chi}$ is the multiplicative inverse of χ.

(i) The set of Dirichlet characters modulo m, which we will call $X(m)$, forms a group under multiplication of characters.

Note that since the values of each character on $(A/mA)^\times$ are $\phi(m)$-th roots of unity, the value set is finite, and hence $|X(m)| < \infty$.

We will prove that $|X(m)| = \phi(m) = |(A/mA)^\times|$, and give an explicit description of each of these characters.

Our argument depends on a more general treatment of characters on finite abelian groups. When G is a finite abelian group, we consider the group $\hat{G}$ of homomorphisms $\chi : G \to \mathbb{C}^\times$. Note that if $|G| = n$,

then $\chi(g)$ is an n-th root of unity for all $g \in G$.

Lemma 7.2. Suppose that G is cyclic of order n, so that $G = \langle g \rangle$ for some $g \in G$. Then $\hat{G}$ consists of exactly n characters

$$\chi_k : G \longrightarrow \mathbb{C}^\times$$

$$\chi_k(g^m) = e^{2\pi i km/n} \qquad (1 \le k \le n).$$

Thus $\hat{G} = \langle \chi_1 \rangle$ is cyclic.

Proof. Consider the generator g of G. Given $\chi \in \hat{G}$, we have $\chi(g) = e^{2\pi i k/n}$ for some $1 \le k \le n$. Then $\chi(g^m) = \chi(g)^m = e^{2\pi i km/n}$, which defines this character for all elements of G. In particular, if $\chi \in \hat{G}$, then $\chi = \chi_1^m$ for some $1 \le m \le n$, so $\hat{G} = \langle \chi_1 \rangle$. //

Corollary 7.3. Suppose G is cyclic of order n. Then for each $\chi \in \hat{G}$, one has

$$\sum_{a \in G} \chi(a) = \begin{cases} n, & \text{when } \chi = \chi_0, \\ 0, & \text{otherwise,} \end{cases}$$

and for $a \in G$, we have

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} n, & \text{when } a = id, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. With notation as in the lemma, we may suppose that $\chi = \chi_1^k$ for some $1 \le k \le n$, whence

$$\sum_{a \in G} \chi(a) = \sum_{r=1}^{n} e^{2\pi i rk/n} = \begin{cases} 0, & \text{when } 1 \le k < n, \\ n, & \text{when } k = n, \end{cases}$$

and this delivers the first conclusion. For the second, we may suppose that $a = g^l$ for some $1 \le l \le n$, whence

$$\sum_{\chi \in \hat{G}} \chi(a) = \sum_{r=1}^{n} e^{2\pi i rl/n} = \begin{cases} 0, & \text{when } 1 \le l < n, \\ 1, & \text{when } l = n, \end{cases}$$

and again we obtain the desired conclusion. //

Next, we address direct products of abelian groups, with an inductive strategy in mind.

Lemma 7.4 Suppose that G_1 and G_2 are finite abelian groups, and $G = G_1 \otimes G_2$, so for each $g \in G$ we have $g = (g_1, g_2)$ for some $g_i \in G_i$ $(i=1,2)$.

(a) Suppose that $\chi_i \in \hat{G}_i$ $(i=1,2)$. Then the function

$$\chi : G \longrightarrow \mathbb{C}^\times$$
$$\chi(g) := \chi_1(g_1)\,\chi_2(g_2)$$

defines a character, so $\chi \in \hat{G}$.

(b) Suppose that $\chi \in \hat{G}$. Then there exist $\chi_i \in \hat{G}_i$ $(i=1,2)$ with $\chi(g) = \chi_1(g_1)\chi_2(g_2)$ $(g = (g_1, g_2) \in G)$.

Proof. (a) is self-evident. □

(b) We have $g = (g_1, g_2) = (g_1, id)(id, g_2)$,

so $\chi(g) = \chi((g_1, id))\,\chi((id, g_2))$.

Then if we define

$$\chi_1(g_1) = \chi((g_1, id)) \quad \& \quad \chi_2(g_2) = \chi((id, g_2)),$$

for each $g_i \in G_i$ $(i=1,2)$, then the conclusion follows. □//

This lemma shows that $\hat{G} \cong \hat{G}_1 \otimes \hat{G}_2$.

Theorem 7.5. Let G be a finite abelian group. Then $\hat{G} \cong G$.

Proof. Any finite abelian group is (by the classification theorem) isomorphic to a direct product of cyclic groups, so

$$G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_r,$$

for suitable cyclic groups G_i $(1 \le i \le r)$. Now apply Lemmata 7.2

and 7.4 inductively to obtain the desired conclusion. //

$$\hat{G} \cong \hat{G}_1 \otimes \hat{G}_2 \otimes \cdots \otimes \hat{G}_r .$$

Corollary 7.6. One has $X(m) \cong (\mathbb{A}/m\mathbb{A})^\times$, and, in particular

$$|X(m)| = \phi(m).$$

Proof. $|X(m)| = |(\mathbb{A}/m\mathbb{A})^\times| = \phi(m)$. //

Corollary 7.7. Suppose that G is an abelian group. Then for each $\chi \in \hat{G}$, one has

$$\sum_{a \in G} \chi(a) = \begin{cases} |G| , & \text{when } \chi = \chi_0, \\ 0 , & \text{otherwise}, \end{cases}$$

and for $a \in G$, we have

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} |G| , & \text{when } a = id, \\ 0 , & \text{otherwise}. \end{cases}$$

Proof. Use the decomposition into cyclic groups $G = G_1 \otimes \cdots \otimes G_r$, and associated characters $\chi_i \in \hat{G}_i$ with $\chi \in G$ so that $\chi = \chi_1 \cdots \chi_r$.

$$\chi(g) = \chi_1(g_1) \cdots \chi_r(g_r) \quad \text{when} \quad g = (g_1, \cdots, g_r).$$

Thus, making use of Corollary 7.3, we have

$$\sum_{a \in G} \chi(a) = \Big(\sum_{g_1 \in G_1} \chi_1(g_1)\Big) \cdots \Big(\sum_{g_r \in G_r} \chi_r(g_r)\Big)$$

$$= \begin{cases} |G_1| \cdots |G_r| , & \text{when } \chi_i = \chi_0 \quad (1 \le i \le r) \\ 0 , & \text{when } \chi_i \neq \chi_0 \text{ some } 1 \le i \le r. \end{cases}$$

Since $|G| = |G_1| \cdots |G_r|$, the first conclusion follows. Similarly,

$$\sum_{\chi \in \hat{G}} \chi(g) = \Big(\sum_{\chi_1 \in \hat{G}_1} \chi_1(g_1)\Big) \cdots \Big(\sum_{\chi_r \in \hat{G}_r} \chi_r(g_r)\Big)$$

$$= \begin{cases} |G_1| \cdots |G_r|, & \text{when } g_i = id \ (1 \le i \le r), \\ 0, & \text{when } g_i \ne id \text{ some } 1 \le i \le r, \end{cases}$$

$$= \begin{cases} |G|, & \text{when } g = (g_1, \dots, g_r) = id, \\ 0, & \text{when } g \ne id, \end{cases}$$

and again the desired conclusion follows. //

For our purposes, it is useful to record the special case given below.

Corollary 7.8. For each $\chi \in X(m)$, one has

$$\sum_{a \in (\mathbb{A}/m\mathbb{A})^\times} \chi(a) = \begin{cases} \phi(m), & \text{when } \chi = \chi_0, \\ 0, & \text{otherwise.} \end{cases}$$

Also, if $a \in \mathbb{A}$ satisfies $(a, m) = 1$, then

$$\sum_{\chi \in X(m)} \chi(a) = \begin{cases} \phi(m), & \text{when } a \equiv 1 \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

As previously noted, we adopt the convention that $\chi(a) = 0$ when $(a, m) \ne 1$, and thus

$$\sum_{\substack{a \in \mathbb{A} \\ |a| < |m|}} \chi(a) = \begin{cases} \phi(m), & \text{when } \chi = \chi_0, \\ 0, & \text{otherwise,} \end{cases}$$

and for all $a \in \mathbb{A}$,

$$\sum_{\chi \in X(m)} \chi(a) = \begin{cases} \phi(m), & \text{when } a \equiv 1 \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

It is not too difficult to construct the characters $\chi \in X(m)$ explicitly.

Recall that when π is a monic irreducible element of $\mathbb{A}$, then $(\mathbb{A}/\pi\mathbb{A})^\times$ is cyclic, and

$$\{ a^{|\pi|-1} : a \in (\mathbb{A}/\pi^m\mathbb{A})^\times \} \cong \underset{\|}{C_{p^{a_1}}} \otimes \cdots \otimes \underset{\|}{C_{p^{a_r}}},$$
$$\langle g_1 \rangle \qquad\qquad \langle g_r \rangle$$

for suitable positive integers $a_i = a_i(\pi)$ $(1 \le i \le r = r(\pi))$, with

$$|\pi|^{m-1} = p^{a_1 + \cdots + a_r}$$

(see Theorem 3.1 and HW2, a1). Thus $(\mathbb{A}/\pi^m\mathbb{A})^\times$ can be written as an internal direct product

$$(\mathbb{A}/\pi^m\mathbb{A})^\times = \{ g_0^{b_0} g_1^{b_1} \cdots g_r^{b_r} : 0 \le b_0 < |\pi|-1,\ 0 \le b_j < a_j\ (1 \le j \le r) \},$$

for suitable elements $g_0, \ldots, g_r$ of $(\mathbb{A}/\pi^m\mathbb{A})^\times$. The characters of $(\mathbb{A}/\pi^m\mathbb{A})^\times$ therefore take the shape

$$\chi_{\underline{k}}(a) = \exp\left(2\pi i \left(\frac{k_0 b_0}{|\pi|-1} + \frac{k_1 b_1}{p^{a_1}} + \cdots + \frac{k_r b_r}{p^{a_r}} \right)\right),$$

when $a = g_0^{b_0} g_1^{b_1} \cdots g_r^{b_r}$, where $0 \le k_0 < |\pi|-1$, $0 \le k_j < p^{a_j}$ $(1 \le j \le r)$.
$\in (\mathbb{A}/\pi^m\mathbb{A})^\times$

We can determine the characters of $(\mathbb{A}/u\mathbb{A})^\times$, when $u \in \mathbb{A}$ has degree at least 1, by using the relation

$$(\mathbb{A}/u\mathbb{A})^\times \cong \bigotimes_{\pi^m \| u} (\mathbb{A}/\pi^m\mathbb{A})^\times,$$

available via the Chinese Remainder Theorem. In this case, the general character of $(\mathbb{A}/u\mathbb{A})^\times$ takes the shape

$$\chi_{\underline{k}}(a) = \exp\left(2\pi i \sum_{\pi^m \| u} \left(\frac{k_0 b_0}{|\pi|-1} + \frac{k_1 b_1}{p^{a_1}} + \cdots + \frac{k_r b_r}{p^{a_r}} \right)\right),$$

when $a = \prod_{\pi^m \| u} g_0^{b_0} g_1^{b_1} \cdots g_r^{b_r}$, in which we have adopted the convention that throughout, $a_i = a_{i,\pi}$, $b_i = b_{i,\pi}$, $k_i = k_{i,\pi}$, $r = r_\pi$, and where

$$0 \le k_{0,\pi} < |\pi| - 1 \quad , \quad 0 \le k_{j,\pi} < p^{a_{j,\pi}} \quad (1 \le j \le r_\pi) .$$

Observe in this last formula that $\chi_{\underline{k}}(a)$ is indeed a character modulo u. For certainly $b_{i,\pi}$ depends only on a modulo u. Moreover, when we consider the map $b_{0,\pi} \mapsto b_{0,\pi} + (|\pi| - 1)$, $b_{j,\pi} \mapsto b_{j,\pi} + p^{a_{j,\pi}}$ $(1 \le j \le r_\pi)$, it follows that (in the obvious sense) each $g_i^{b_i} \mapsto g_i^{b_i}$.

Finally, we observe that while <u>totally</u> multiplicative functions f on $\mathbb{A}$ having period m, and with $f(a) = 0$ whenever $(a, m) \ne 1$, are Dirichlet characters modulo m, the same is true in the absense of the condition "totally".

<u>Theorem 7.9.</u> Suppose that $f : \mathbb{A} \to \mathbb{C}$ is a multiplicative function satisfying:

(a) $f(a) = 0$ whenever $(a, m) \ne 1$, and

(b) $f(a + lm) = f(a)$ for all $a, l \in \mathbb{A}$.

Then f is a Dirichlet character modulo m.

<u>Proof.</u> We need show only that $f(ab) = f(a) f(b)$ for all $a, b \in \mathbb{A}$. When $(ab, m) \ne 1$, one has either $(a, m) \ne 1$ or $(b, m) \ne 1$, and hence $f(ab) = 0 = f(a) f(b)$.

Now suppose that $(ab, m) = 1$, whence $(a, m) = (b, m) = 1$.

Since $(a, m) = 1$, there exists $\ell \in A$ with $\ell m \equiv 1-b \pmod{a}$, whence $(a, b+\ell m) = 1$. Hence

$$\begin{aligned} f(ab) &= f(a(b+\ell m)) \\ &= f(a) f(b+\ell m) \\ &= f(a) f(b). \end{aligned}$$

This proves the total multiplicativity of f, confirming that f is a Dirichlet character. //

§8. Prime polynomials in arithmetic progression.

We now seek an analogue of Dirichlet's Theorem on primes in arithmetic progression – first proved in the function field setting by Kornblum (as described by Landau).

Definition 8.1. Let χ be a Dirichlet character modulo m. The **Dirichlet L-function** associated with χ is

$$L(s, \chi) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{\chi(u)}{|u|^s}.$$

By comparison with $\zeta_A(s) = \sum_{u \in \mathbb{F}_q[t]^+} |u|^{-s}$, we see that $L(s, \chi)$ converges absolutely for $\mathrm{Re}(s) > 1$, and moreover

$$L(s, \chi) = \prod_{\pi} \left(1 - \frac{\chi(\pi)}{|\pi|^s}\right)^{-1}. \qquad (\mathrm{Re}(s) > 1).$$

We therefore see, in particular, that

$$\begin{aligned} L(s, \chi_0) &= \prod_{\pi} \left(1 - \frac{\chi_0(\pi)}{|\pi|^s}\right)^{-1} \\ &= \prod_{\pi \nmid m} \left(1 - \frac{1}{|\pi|^s}\right)^{-1} = \prod_{\pi} \left(1 - \frac{1}{|\pi|^s}\right)^{-1} \cdot \prod_{\pi \mid m} \left(1 - \frac{1}{|\pi|^s}\right) \end{aligned}$$

Thus, the principal character χ_0 modulo m satisfies the property that

$$L(s,\chi_0) = \prod_{\pi \nmid m} (1 - |\pi|^{-s})\, \zeta_A(s). \qquad (8.1)$$

Recall that $\zeta_A(s) = (1-q^{1-s})^{-1}$. Then we see from (8.1) that $L(s,\chi_0)$ can be analytically continued throughout $\mathbb{C}$, save for a simple pole at $s=1$. (by using the corresponding analytic continuation for $\zeta_A(s)$).

Moreover, one has $|\pi|^{-s} = q^{-ds}$, where $d = \deg(\pi)$. Then $L(s,\chi_0)$ takes the shape:

$$L(s,\chi_0) = \frac{P_k(w)}{1-qw}, \qquad (8.2)$$

where $w = q^{-s}$ and $P_k(w) \in \mathbb{Z}[u]$ has degree $\leq$ equal to the degree of m. The situation is different for $L(s,\chi)$ when $\chi \neq \chi_0$.
[Notice: $(1-qw) \nmid P_k(w)$].

Theorem 8.2. Let χ be a Dirichlet character modulo m with $\chi \neq \chi_0$. Write $w = q^{-s}$. Then $L(s,\chi)$ is a polynomial in w of degree at most $\deg(m) - 1$.

Proof. We have

$$L(s,\chi) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{\chi(u)}{|u|^s} = \sum_{n=0}^{\infty} A(n,\chi)\, q^{-ns},$$

where

$$A(n,\chi) = \sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) = n}} \chi(u).$$

When $n \geq \deg(m)$, we find that

$$A(n,\chi) = q^{n-\deg(m)} \sum_{|a|<|m|} \chi(a) = 0 \quad \text{(by orthogonality)},$$

and hence

$$L(s,\chi) = \sum_{n=0}^{\deg(m)-1} A(n,\chi)\, w^n \qquad (\text{with } w = q^{-s}),$$

which is a polynomial of degree at most $\deg(m)-1$. //

Corollary 8.3. When χ is a non-principal Dirichlet character modulo m, the function $L(s,\chi)$ has an analytic continuation to the whole of $\mathbb{C}$.

The classical proof of the Prime Number Theorem (in arithmetic progressions, over $\mathbb{Z}$) rests on proving that $L(1,\chi) \neq 0$ for all $\chi \neq \chi_0$. We can pursue this approach also in the function field setting, with a similar dichotomy dividing real and complex characters.

Lemma 8.4. Let $m \in \mathbb{F}_q[t]^+$ have degree at least one. Then for each $\pi \nmid m$, there exist integers e_π and f_π with $e_\pi f_\pi = \phi(m)$, such that

$$\prod_{\chi \in X(m)} L(s,\chi) = \prod_{\pi \nmid m} \left(1 - |\pi|^{-f_\pi s}\right)^{-e_\pi}. \qquad (8.3)$$

Proof. We observe that for each prime polynomial π with $\pi \nmid m$, the map

$$\nu : X(m) \longrightarrow \mathbb{C}^\times$$
$$\chi \longmapsto \chi(\pi)$$

is a group homomorphism. Let the order of π in $(A/mA)^\times$ be f_π. Then for every $\chi \in X(m)$ one has

$$\chi(\pi)^{f_\pi} = \chi\Big(\pi^{f_\pi}\Big) = \chi(1) = 1,$$
$$\text{(} 1 \pmod m \text{)}$$

so that $\chi(\pi)$ is an f_π-th root of unity. We claim that there exists $\chi \in X(m)$ for which $\chi(\pi)$ is a primitive f_π-th root of unity. In order to confirm this assertion, let d be the least common multiple of the orders of the $\chi(\pi)$ as roots of unity, for $\chi \in X(m)$. Then by considering the group structure of $\nu(X(m))$, we see that there

exists $\chi \in X(m)$ with $\chi(\pi)$ of order d. But then, for all $\chi \in X(m)$, one has $1 = \chi(\pi)^d = \chi(\pi^d)$, so that $\pi^d \equiv 1 \pmod m$. Thus $f_\pi \mid d$, and so $d = f_\pi$.

Since for every $\chi \in X(m)$, one has that $\chi(\pi)$ is an f_π-th root of unity; and there exists $\chi_1 \in X(m)$ with $\chi_1(\pi) = \zeta_{f_\pi}$ a primitive f_π-th root of unity, we see that

$$\nu\left(X(m)\right) = \langle \chi_1(\pi) \rangle \quad \text{is cyclic, of order } f_\pi,$$

whence

$$|\ker(\nu)| = |X(m)| \,/\, |\nu(X(m))| = \varphi(m)/f_\pi = e_\pi, \text{ say}.$$

We thus deduce that for each prime polynomial π with $\pi \nmid m$, one has

$$\prod_{\chi \in X(m)} \left(1 - \chi(\pi)|\pi|^{-s}\right)^{-1} = \prod_{j=1}^{f_\pi} \left(1 - \zeta_{f_\pi}^j |\pi|^{-s}\right)^{-e_\pi} = \left(1 - |\pi|^{-f_\pi s}\right)^{-e_\pi}.$$

Hence,

$$\prod_{\chi \in X(m)} L(s,\chi) = \prod_{\pi} \prod_{\chi \in X(m)} \left(1 - \chi(\pi)|\pi|^{-s}\right)^{-1}$$

$$= \prod_{\pi \nmid m} \prod_{\chi \in X(m)} \left(1 - \chi(\pi)|\pi|^{-s}\right)^{-1}$$

$$= \prod_{\pi \nmid m} \left(1 - |\pi|^{-f_\pi s}\right)^{-e_\pi}. \quad //$$

It is relatively easy to show that when χ is complex (i.e. not real) then $L(1,\chi) \neq 0$.

<u>Lemma 8.5.</u> Suppose that χ is a complex Dirichlet character modulo m. Then $L(1,\chi) \neq 0$.

Proof. By expanding each term $(1 - |\pi|^{-f_\pi s})^{-e_\pi}$, one sees that each of these factors has the shape $\sum_{k=0}^{\infty} c_k |\pi|^{-ks}$, with $c_k = 1$ and $c_k \geq 0$. Thus

$$\prod_{\pi \nmid m} (1 - |\pi|^{-f_\pi s})^{-e_\pi} = \sum_{u \in \mathbb{F}_q[t]^+} \frac{C(u)}{|u|^s},$$

for suitable coefficients $C(u) \geq 0$ with $C(1) = 1$, and thus the Dirichlet series on the right hand side of (8.3), say $D(s)$, satisfies the property that $D(s) > 1$ when s is a real number with $s > 1$.

Suppose, if possible, that χ is a complex character with $L(1, \chi) = 0$. Then by complex conjugation, we have also $L(1, \bar{\chi}) = 0$. Then $L(s, \chi) L(s, \bar{\chi})$ has a double zero at $s = 1$. In the product $\prod_{\chi \in X(m)} L(s, \chi)$, we also have the factor $L(s, \chi_0)$ which has a simple pole at $s = 1$, and all other factors are analytic at $s = 1$. Then $\prod_{\chi \in X(m)} L(s, \chi)$ has a zero at $s = 1$, and is (recall) analytic when $s \neq 1$. But then one cannot have

$$\prod_{\chi \in X(m)} L(s, \chi) > 1 \quad \text{when } s \text{ is real with } s > 1,$$

as was proved above. We are therefore forced to conclude that $L(1, \chi) \neq 0$ for complex χ. //

The case of real-valued characters is more complicated.

Lemma 8.6. Suppose that $\chi \neq \chi_0$ is a real-valued Dirichlet character modulo m. Then $L(1,\chi) \neq 0$.

Proof. If χ is real-valued, then $\chi(n) = \pm 1$ whenever $(n,m)=1$, whence $\chi^2(n) = 1$. So $\chi^2 = \chi_0$. We again seek to obtain a Dirichlet series with non-negative coefficients, on this occasion examining the function

$$D(s) = \frac{L(s,\chi^2)L(s,\chi)}{L(2s,\chi^2)} = \frac{L(s,\chi_0)L(s,\chi)}{L(2s,\chi_0)}.$$

$$= \prod_{\pi \nmid m} \frac{(1-|\pi|^{-s})^{-1}(1-\chi(\pi)|\pi|^{-s})^{-1}}{(1-|\pi|^{-2s})^{-1}}$$

$$= \prod_{\substack{\pi \nmid m \\ \chi(\pi)=1}} \frac{(1-|\pi|^{-s})^{-2}}{(1-|\pi|^{-2s})^{-1}} \cdot \prod_{\substack{\pi \nmid m \\ \chi(\pi)=-1}} \frac{(1-|\pi|^{-s})^{-1}(1+|\pi|^{-s})^{-1}}{(1-|\pi|^{-2s})^{-1}}$$

$$= \prod_{\substack{\pi \nmid m \\ \chi(\pi)=1}} \frac{1+|\pi|^{-s}}{1-|\pi|^{-s}} = \prod_{\substack{\pi \nmid m \\ \chi(\pi)=1}} \left(1 + 2|\pi|^{-s} + 2|\pi|^{-2s} + \dots\right).$$

Thus $D(s)$ is a Dirichlet series with non-negative coefficients.

It is helpful to simplify the factors $L(s,\chi_0)$ and $L(2s,\chi_0)$ in this conclusion so that we reduce the dependence on m. Observe that

$$\frac{L(s,\chi_0)}{L(2s,\chi_0)} = \prod_{\pi \mid m} \frac{(1-|\pi|^{-s})}{(1-|\pi|^{-2s})} \cdot \frac{\zeta_A(s)}{\zeta_A(2s)}$$

$$= \prod_{\pi \mid m} (1+|\pi|^{-s})^{-1} \cdot \frac{1-q^{1-2s}}{1-q^{1-s}}.$$

Thus,

$$\frac{1-q^{1-2s}}{1-q^{1-s}} L(s,\chi) = \prod_{\pi \mid m} (1+|\pi|^{-s}) \cdot D(s) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{a(u)}{|u|^s},$$ say,

is a Dirichlet series with non-negative coefficients, with $a(1) = 1$.

The proof that $L(1,\chi)$ is non-zero is made easier by converting the problem into one about rational functions. To this end, put $W = q^{-s}$, and write $L(s,\chi) = P(W,\chi)$, a polynomial in W (by Theorem 8.2). Then

$$\frac{1-qW^2}{1-qW} P(W,\chi) = \sum_{d=0}^{\infty} \underbrace{\left(\sum_{|u|=q^d} a(u) \right)}_{\| \; A(d)} W^d,$$

where $A(d)$ is non-negative for $d \geq 0$, and $A(0) = 1$. Notice that $L(s,\chi)$ converges for $\mathrm{Re}(s) > 1$, whence $\sum_{u \in \mathbb{F}_q[t]^+} \frac{a(u)}{|u|^s}$ converges for $\mathrm{Re}(s) > 1$. Consequently, one sees that $\sum_{d=0}^{\infty} A(d) W^d$ converges for $|W| < q^{-1}$.

Goal: Prove that $L(1,\chi) \neq 0$, or equivalently, that $P(q^{-1},\chi) \neq 0$.

Suppose that $P(q^{-1},\chi) = 0$, and seek a contradiction. Then

$$(1-qW) \mid P(W,\chi),$$

so that $\frac{1-qW^2}{1-qW} P(W,\chi)$ is a polynomial in W. Then $\sum_{d=0}^{\infty} A(d) W^d$ is a polynomial in W with non-negative coefficients and constant term 1 with a zero at $W = 1/\sqrt{q}$. But this is impossible, because such a polynomial has no positive roots. #

We conclude that $P(q^{-1}, \chi) \neq 0 \Rightarrow L(1, \chi) \neq 0$. //

Theorem 8.7. When $\chi \in X(m)$ and $\chi \neq \chi_0$, one has $L(1, \chi) \neq 0$.

Proof. Just combine the conclusions of Lemmata 8.5 and 8.6. //

We are now equipped to prove an analogue of Dirichlet's theorem concerning the infinitude of primes in arithmetic progressions. This will provide only weak quantitative information without further input. We begin with a definition of Dirichlet density.

Definition 8.8. Suppose that $\mathcal{S}$ is a set of prime polynomials in A. The Dirichlet density of $\mathcal{S}$ is defined to be

$$\delta(\mathcal{S}) = \lim_{s \to 1+} \frac{\sum_{\pi \in \mathcal{S}} |\pi|^{-s}}{\sum_{\pi \in A} |\pi|^{-s}},$$

provided that this limit exists.

Notice that when $s > 1$, one has

$$\sum_{\pi \in \mathcal{S}} |\pi|^{-s} < \infty \quad \text{and} \quad \sum_{\pi \in A} |\pi|^{-s} < \infty.$$

Moreover, using the analogue of the Prime Number Theorem,

$$\sum_{|\pi| \leq q^n} |\pi|^{-1} = \sum_{d=1}^{n} q^{-d} \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d} \right) \right)$$

$$= \log n + O(1).$$

So, morally speaking, one may regard $\mathcal{S}$ as having Dirichlet density δ when $\sum_{\substack{|\pi| \leq q^n \\ \pi \in \mathcal{S}}} |\pi|^{-1} = \delta \log n + O(1)$.

Even more heuristically, the set $\mathcal{S}$ contains a proportion δ of the set of prime polynomials.

Goal: We aim to show that when $(a,m)=1$, then the Dirichlet density of the set of prime polynomials π satisfying $\pi \equiv a \pmod m$ is $1/\varphi(m)$.

We begin by connecting the quantities employed in Definition 8.8 to zeta and L-functions.

Lemma 8.9. As $s \to 1+$, one has

$$\sum_{\pi \in \mathbb{A}} |\pi|^{-s} = \log \zeta_{\mathbb{A}}(s) + O(1)$$

$$= \log\left(\frac{1}{s-1}\right) + O(1).$$

Proof. Using the Euler product representation of $\zeta_{\mathbb{A}}(s)$, we have

$$\log \zeta_{\mathbb{A}}(s) = -\sum_{\pi} \log\left(1 - |\pi|^{-s}\right)$$

$$= \sum_{\pi} \sum_{k=1}^{\infty} \frac{|\pi|^{-ks}}{k}$$

$$= \sum_{\pi} |\pi|^{-s} + O\Big(\underbrace{\sum_{u \in \mathbb{F}_q[t]^+} |u|^{-2s}}_{=O(1)} \Big).$$

This confirms the first assertion of the lemma. □

In order to establish the second assertion, observe that

$$\log \zeta_{\mathbb{A}}(s) = -\log\left(1 - q^{1-s}\right) = -\log\left(1 - \exp\left(-(s-1)\log q\right)\right).$$

Thus, as $s \longrightarrow 1+$, one has

$$\log \zeta_{\mathbb{A}}(s) = -\log\left((s-1)\log q + O((s-1)^2)\right)$$

$$= \log\left(\frac{1}{s-1}\right) - \log\log q + O(s-1).$$

This confirms the second assertion of the lemma. //

Lemma 8.10. As $s \longrightarrow 1+$, one has

$$\sum_{\pi \in \mathbb{A}} \chi(\pi) |\pi|^{-s} = \log L(s,\chi) + O(1).$$

Moreover,

$$\log L(s,\chi) = \begin{cases} \log\left(\frac{1}{s-1}\right) + O(1), & \text{when } \chi = \chi_0, \\ O(1), & \text{when } \chi \neq \chi_0. \end{cases}$$

Proof. Again, using the Euler product representation, we see that

$$\log L(s,\chi) = -\sum_{\pi} \log\left(1 - \chi(\pi)|\pi|^{-s}\right) = \sum_{\pi} \chi(\pi)|\pi|^{-s} + O(1).$$

On recalling (8.1), we see that

$$\log L(s,\chi_0) = \log \zeta_{\mathbb{A}}(s) + \sum_{\pi | \mathfrak{m}} \log\left(1 - |\pi|^{-s}\right)$$

$$= \log \zeta_{\mathbb{A}}(s) + O(1),$$

whence

$$\log L(s,\chi_0) = \log\left(\frac{1}{s-1}\right) + O(1).$$

Meanwhile, when $\chi \neq \chi_0$, one has $L(1,\chi) \neq 0$ and $L(s,\chi)$ is analytic throughout $\mathbb{C}$. Thus, as $s \longrightarrow 1+$, one has

$$\log L(s,\chi) = \log L(1,\chi) + O(s-1) = O(1).$$

This completes the proof of the lemma. //

Theorem 8.11. Suppose that $a, m \in \mathbb{A}$ satisfy $(a, m) = 1$ and $\deg(m) \geq 1$. Then the Dirichlet density of the set of primes

$$\mathbb{P}_{a,m} = \{ \pi \in \mathbb{A} : \pi \equiv a \pmod{m} \}$$

satisfies

$$\delta(\mathbb{P}_{a,m}) = 1/\varphi(m).$$

In particular, there are infinitely many prime polynomials π with $\pi \equiv a \pmod{m}$.

Proof. We use the orthogonality of Dirichlet characters to detect the arithmetic progression a modulo m. Thus, when $s > 1$, one has

$$\sum_{\pi \in \mathbb{P}_{a,m}} |\pi|^{-s} = \frac{1}{\varphi(m)} \sum_{\pi \in \mathbb{A}} |\pi|^{-s} \underbrace{\sum_{\chi \in X(m)} \chi(\pi) \bar{\chi}(a)}_{= 0 \text{ unless } \pi a^{-1} \equiv 1 \pmod{m}}$$

$$= \frac{1}{\varphi(m)} \sum_{\chi \in X(m)} \bar{\chi}(a) \sum_{\pi \in \mathbb{A}} \chi(\pi) |\pi|^{-s}$$

$$= \frac{1}{\varphi(m)} \sum_{\chi \in X(m)} \bar{\chi}(a) \left(\log L(s, \chi) + O(1) \right),$$

as $s \to 1+$.

By applying Lemma 8.10, we see that

$$\sum_{\pi \in \mathbb{P}_{a,m}} |\pi|^{-s} = \frac{1}{\varphi(m)} \log L(s, \chi_0) + \frac{1}{\varphi(m)} \sum_{\substack{\chi \neq \chi_0 \\ \chi \in X(m)}} \bar{\chi}(a) \log L(s, \chi) + O(1)$$

$$= \frac{1}{\varphi(m)} \log\left(\frac{1}{s-1}\right) + O(1).$$

Thus, on recalling Lemma 8.9, we see that

$$\lim_{s \to 1+} \frac{\sum_{\pi \in \mathbb{P}_{a,m}} |\pi|^{-s}}{\sum_{\pi \in \mathbb{A}} |\pi|^{-s}} = \lim_{s \to 1+} \frac{\frac{1}{\varphi(m)} \log\left(\frac{1}{s-1}\right) + O(1)}{\log\left(\frac{1}{s-1}\right) + O(1)} = \frac{1}{\varphi(m)}.$$

This confirms that the Dirichlet density of $\mathbb{P}_{a,m}$ is equal to $\frac{1}{\varphi(m)}$. //

§9. Prime polynomials in arithmetic progressions and the Riemann Hypothesis.

We are able to sharpen the conclusion above to give an asymptotic formula comparable in strength to the Prime (polynomial) theorem.

Theorem 9.1 Whenever $a, m \in \mathbb{A}$ satisfy $(a, m) = 1$ and $\deg(m) \geq 1$, one has

$$\sum_{\substack{\pi \in \mathbb{A} \\ \pi \equiv a \pmod m \\ \deg(\pi) = N}} 1 = \frac{1}{\phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Compare:

$$\sum_{\substack{\pi \in \mathbb{A} \\ \deg(\pi) = N}} 1 = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

In order to prove this assertion, motivated by classical treatments, the natural line of attack is to investigate the logarithmic derivatives

$$\frac{L'}{L}(s,\chi) = \frac{d}{ds}\log L(s,\chi)$$

$$= -\frac{d}{ds}\sum_{\pi}\log\left(1-\chi(\pi)|\pi|^{-s}\right)$$

$$= -\sum_{\pi}\frac{\log|\pi|\ \chi(\pi)|\pi|^{-s}}{1-\chi(\pi)|\pi|^{-s}},$$

since we obtain

$$-\frac{L'}{L}(s,\chi) = \log q \sum_{d=1}^{\infty} d \sum_{\substack{\pi\in\mathbb{F}_q[t]\\ \deg(\pi)=d}} \frac{\chi(\pi)}{|\pi|^s} + \text{lower order terms}.$$

The right hand side here is a Dirichlet series with coefficients counting the number of prime polynomials of degree d, counted with weight $d\chi(\pi)$ (compare $\sum_{p\le x}(\log p)\chi(p)$).

We simplify matters by substituting $w = q^{-s}$, make use of our first secret weapon ($L(s,\chi) = P(w,\chi)$ is a polynomial when $\chi \neq \chi_0$), and then make use of the remarkable fact that the Riemann Hypothesis holds in function fields, owing to work of Weil, 1948.

Let us now put this sketch into better order. Let χ be a Dirichlet character modulo m. Then $L(s,\chi) = P(w,\chi)$, where $w = q^{-s}$ and P is a polynomial of degree at most $M-1$, where $M = \deg(m)$. Thus, for suitable complex numbers $\alpha_i(\chi)$ $(1 \le i \le M-1)$, one has

$$P(w,\chi) = \prod_{i=1}^{M-1}(1-\alpha_i(\chi)w). \qquad (9.1)$$

Alternatively, making use of the Euler product decomposition, one has

$$P(w,\chi) = L(s,\chi) = \prod_{\pi \nmid m} \left(1 - \chi(\pi)\,|\pi|^{-s}\right)^{-1}$$

$$= \prod_{d=1}^{\infty} \prod_{\substack{\pi \nmid m \\ \deg(\pi)=d}} \left(1 - \chi(\pi)\, q^{-ds}\right)^{-1}$$

$$= \prod_{d=1}^{\infty} \prod_{\substack{\pi \nmid m \\ \deg(\pi)=d}} \left(1 - \chi(\pi)\, w^{d}\right)^{-1}. \qquad (9.2)$$

In order to assist in computing the logarithmic derivative, observe that

$$\frac{d}{dw} \log\left(1 - \alpha w^d\right) = \frac{-d\alpha w^{d-1}}{1-\alpha w^d} = -\frac{d}{w} \sum_{k=1}^{\infty} (\alpha w^d)^k. \qquad (|w| < 1/|\alpha|).$$

Then, on recalling (9.1), we find that when $\chi \neq \chi_0$, one has.

$$w \frac{d}{dw} \log(P(w,\chi)) = w \frac{d}{dw} \sum_{i=1}^{M-1} \log\left(1 - \alpha_i(\chi) w\right)$$

$$= -\sum_{i=1}^{M-1} \sum_{k=1}^{\infty} \left(\alpha_i(\chi) w\right)^k$$

$$= \sum_{k=1}^{\infty} c_k(\chi)\, w^k,$$

where

$$c_k(\chi) = -\sum_{i=1}^{M-1} \alpha_i(\chi)^k. \qquad (9.3)$$

When $\chi = \chi_0$, we instead use the relation

$$L(s,\chi_0) = \prod_{\pi \mid m} \left(1 - |\pi|^{-s}\right) \zeta_{\mathbb{A}}(s).$$

Then

$$P(w,\chi_0) = \left(\prod_{\pi \mid m} \left(1 - w^{\deg(\pi)}\right)\right)(1 - qw)^{-1},$$

whence

$$w \frac{d}{dw} \log\left(P(w,\chi_0)\right) = -w \frac{d}{dw} \log(1 - qw) + w \frac{d}{dw} \sum_{\pi \mid m} \log\left(1 - w^{\deg(\pi)}\right)$$

$$= \sum_{k=1}^{\infty} q^k w^k - \sum_{\pi \mid m} \sum_{k=1}^{\infty} w^{k \deg(\pi)}$$

$$= \sum_{k=1}^{\infty} C_k(\chi_0)\, w^k,$$

where

$$C_k(\chi_0) = q^k + O_m(1). \qquad (9.4)$$

It is useful at this point to recall the Riemann Hypothesis for function fields over a finite field, proved in sufficient generality for our purposes by A. Weil in 1948. This shows that the roots of L-functions of the shape $P(w, \chi)$ are $\frac{1}{2}$-integral powers of q, and in this instance $|\alpha_i(\chi)| = 1$ or $\sqrt{q}$ for each i when $\chi \neq \chi_0$. Note that $|w| = 1/|\alpha_i(\chi)| = 1/\sqrt{q}$ corresponds to $\mathrm{Re}(s) = 1/2$ (via $w = q^{-s}$). Observe, in particular, from (9.3) that $|C_k(\chi)| \leq (M-1) q^{k/2}$ $(\chi \neq \chi_0)$.

Revert now to the Euler product formulation (9.2), and proceed in like manner. We find that

$$w \frac{d}{dw} \log |P(w,\chi)| = -\sum_{d=1}^{\infty} \sum_{\substack{\pi \nmid m \\ \deg(\pi) = d}} w \frac{d}{dw} \log(1 - \chi(\pi) w^d)$$

$$= \sum_{d=1}^{\infty} \sum_{\deg(\pi) = d} \sum_{k=1}^{\infty} d \left(\chi(\pi) w^d\right)^k$$

$$= \sum_{n=1}^{\infty} \left(\sum_{d \mid n} \sum_{\deg(\pi) = d} d\, \chi(\pi)^{n/d} \right) w^n$$

Comparing coefficients of power series, one sees that when $\chi \neq \chi_0$,

$$\sum_{n=1}^{\infty} c_n(\chi)\, w^n = \sum_{n=1}^{\infty} \left(\sum_{d \mid n} \sum_{\deg(\pi)=d} d\ \chi(\pi)^{n/d} \right) w^n,$$

whence

$$c_n(\chi) = \sum_{d \mid n} \sum_{\deg(\pi)=d} d\ \chi(\pi)^{n/d}$$

$$= n \sum_{\deg(\pi)=n} \chi(\pi) + O\left(\sum_{d \leq n/2} d \cdot q^{d/d} \right).$$

Thus

$$n \sum_{\deg(\pi)=n} \chi(\pi) = c_n(\chi) + O(q^{n/2})$$

$$= O(q^{n/2}).$$

Meanwhile, in the case $\chi = \chi_0$, we have

$$n \sum_{\deg(\pi)=n} \chi_0(\pi) = c_n(\chi_0) + O(q^{n/2})$$

$$= q^n + O(q^{n/2}).$$

Thus, when $(a,m)=1$, we find that

$$\sum_{\substack{\deg(\pi)=n \\ \pi \equiv a \pmod m}} 1 = \sum_{\deg(\pi)=n} \frac{1}{\phi(m)} \sum_{\chi \in X(m)} \chi(\pi)\, \bar{\chi}(a)$$

$$= \frac{1}{\phi(m)} \sum_{\chi \in X(m)} \bar{\chi}(a) \sum_{\deg(\pi)=n} \chi(\pi)$$

$$= \frac{1}{\phi(m)} \left(\frac{1}{n} \underbrace{\left(q^n + O(q^{n/2}) \right)}_{\chi = \chi_0} + \frac{1}{n} \sum_{\chi \neq \chi_0} O_m(q^{n/2}) \right).$$

We ~~therefore~~ conclude ~~that~~

$$\sum_{\substack{\deg(\pi)=n \\ \pi \equiv a \pmod m}} 1 = \frac{1}{\phi(m)} \left(\frac{q^n}{n} + O_M\left(\frac{q^{n/2}}{n}\right)\right).$$

This completes the proof of Theorem 9.1. //

Before leaving this section, we provide an application of Theorem 9.1 of which we have use later on.

Theorem 9.2. Suppose ~~that~~ $a, g \in \mathbb{F}_q[t]$ with g monic and $(a,g) = 1$. Then one has

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g}\pi\right) = \frac{\mu(g)}{\phi(g)} \frac{q^N}{N} + O_g\left(\frac{q^{N/2}}{N}\right).$$

Proof. We break the sum on the left hand side into arithmetic progressions modulo g. Thus, one has

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g}\pi\right) = \sum_{\substack{|r|<|g| \\ (r,g)=1}} \sum_{\substack{\pi \equiv r \pmod g \\ |\pi| \leq q^N}} e\left(\frac{a\pi}{g}\right) + O_g(1)$$

↑ accounts for π with $\pi \mid g$.

Note the condition $(r,g) = 1$ comes from the irreducibility of π. Thus,

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g}\pi\right) = \sum_{\substack{|r|<|g| \\ (r,g)=1}} e\left(\frac{ar}{g}\right) \sum_{\substack{\pi \equiv r \pmod g \\ |\pi| \leq q^N}} 1 + O_g(1).$$

$$= \sum_{\substack{|r|<|g| \\ (r,g)=1}} e\left(\frac{ar}{g}\right) \cdot \left(\frac{1}{\varphi(g)} \frac{q^N}{N} + O_g\left(\frac{q^{N/2}}{N}\right)\right) + O_g(1)$$

$$= \frac{1}{\varphi(g)} \frac{q^N}{N} \sum_{\substack{|r|<|g| \\ (r,g)=1}} e(ar/g) + O_g\left(\frac{q^{N/2}}{N}\right).$$

We now make use of our formula for Ramanujan's sum (in the function field setting) from Problem Set 3, Q6. Thus

$$\sum_{\substack{|r|<|g| \\ (r,g)=1}} e(ar/g) = \frac{\mu(g/(g,a))}{\varphi(g/(g,a))} \cdot \varphi(g)$$

$$= \mu(g), \quad \text{since } (g,a)=1.$$

Then

$$\sum_{|\pi|=q^N} e\left(\frac{a}{g}\pi\right) = \frac{\mu(g)}{\varphi(g)} \frac{q^N}{N} + O_g\left(\frac{q^{N/2}}{N}\right). \quad //$$

---

§10. Equidistribution: uniform distribution in function fields.

As an analogue of the unit interval $[0,1)$ considered as the additive group $\mathbb{R}/\mathbb{Z}$, define

$$\mathbb{T} = \mathbb{F}_q((1/t)) / \mathbb{F}_q[t] = \mathbb{K}_\infty / \mathbb{A},$$

and recall that we write

$$\{\alpha\} = \alpha - \lfloor \alpha \rfloor,$$

where $\lfloor \alpha \rfloor$ is the polynomial part of α. Thus, we have

$$\{\alpha\} \in \mathbb{T},$$

and one can consider $\mathbb{T}$ to be the analogue of the unit interval $[0,1)$, or indeed $\mathbb{R}/\mathbb{Z}$. Notice that, with respect to the Haar measure introduced earlier, one has

$$\text{mes}(\mathbb{T}) = \int_{\mathbb{T}} d\alpha = 1.$$

We now define analogues of intervals in $\mathbb{T}$. When $N \in \mathbb{N}$, we fix $I = (c_1, \dots, c_N) \in \mathbb{F}_q^N$, and then put

$$\mathcal{C}_I = \Big\{ \sum_{i \leq -1} a_i t^i \in \mathbb{T} : a_i = c_{-i} \ (-N \leq i \leq -1) \Big\}.$$

Thus, the cylinder set $\mathcal{C}_I$ satisfies

$$\text{mes}(\mathcal{C}_I) = q^{-N}.$$

Definition 10.1 (Carlitz, 1952) Let $(a_x)_{x \in \mathbb{F}_q[t]}$ be a sequence of elements $a_x \in \mathbb{F}_q((1/t))$. We say that $(a_x)_{x \in \mathbb{F}_q[t]}$ is *equidistributed* in $\mathbb{T}$ if, for any cylinder set $\mathcal{C} \subseteq \mathbb{T}$, we have

$$\lim_{N \to \infty} q^{-N} \, \text{card} \Big\{ x \in \mathbb{F}_q[t]_{\deg \leq N} : \{a_x\} \in \mathcal{C} \Big\} = \text{mes}(\mathcal{C}).$$

Theorem 10.2. Suppose that $F : \mathbb{T} \to \mathbb{C}$ is integrable. Then

$$\lim_{M \to \infty} q^{-M} \sum_{\substack{m \in \mathbb{F}_q[t] \\ \deg(m) < M}} F(a_m) = \int_{\mathbb{T}} F(\alpha) \, d\alpha$$

for all equidistributed sequences $(a_x)_{x \in \mathbb{F}_q[t]}$.

Proof. This is an exercise in basic analysis. //

We now establish an analogue for Weyl's criterion for equidistribution.

Lemma 10.3. The sequence $(a_x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ if and only if, for all $h \in \mathbb{F}_q[t] \setminus \{0\}$, one has

$$\lim_{M \to \infty} q^{-M} \Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h a_x) \Big| = 0. \qquad (10.1)$$

Proof. We first show that the validity of (10.1) implies that (a_x) is equidistributed in $\mathbb{T}$. Let $\mathcal{C}$ be a cylinder set, so that for some natural number N, one has

$$\mathcal{C} = {}^{c}\beta + t^{-N}\mathbb{T},$$

where $\beta = c_{+1}t^{-1} + \dots + c_{+N}t^{-N}$, for some fixed $c_1, \dots, c_N \in \mathbb{F}_q$.

Given $\varepsilon > 0$, the validity of (10.1) shows that for $M \geq M(\varepsilon, h)$, one has

$$\Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h a_x) \Big| < \varepsilon q^M.$$

Thus, for each fixed $k \in \mathbb{N}$, we have

$$\sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)) = q^M + \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)),$$

whence for $M \geq M'(\varepsilon, k)$, one has

$$\Big| \sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)) - q^M \Big| \leq q^k \max_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h a_x) \Big|$$

$$< \varepsilon q^{k+M}.$$

On the other hand, by HW3, QB4, one has

$$\sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} e\left(h(a_x - \beta)\right) = \begin{cases} q^k, & \text{when } \|a_x - \beta\| < q^{-k}, \\ 0, & \text{when } \|a_x - \beta\| \geq q^{-k} \end{cases}.$$

Thus, on writing $N_k(M)$ for the number of a_x with $x \in \mathbb{F}_q[t]$ and $\deg(x) < M$ for which $\|a_x - \beta\| < q^{-k}$, we have

$$\sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} \sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} e\left(h(a_x - \beta)\right) = q^k N_k(M).$$

Combining these conclusions, we see

$$\left| q^k N_k(M) - q^M \right| < \varepsilon q^{k+M}$$

$$\Rightarrow \quad \left| q^{-M} N_k(M) - q^{-k} \right| < \varepsilon.$$

Now take $k = N$. We see that

$$\left| q^{-M} \operatorname{card} \{x \in \mathbb{F}_q[t]_{\deg < M} : \{a_x\} \in \mathcal{C}\} - \operatorname{mes}(\mathcal{C}) \right| < \varepsilon.$$

Since this relation holds for any $\varepsilon > 0$, we conclude that

$$\lim_{M \to \infty} q^{-M} \operatorname{card} \{x \in \mathbb{F}_q[t]_{\deg < M} : \{a_x\} \in \mathcal{C}\} = \operatorname{mes}(\mathcal{C}),$$

and hence $\{a_x\}$ is equidistributed in $\mathbb{T}$. □

In the other direction, if (a_x) is equidistributed in $\mathbb{T}$, then for any cylinder set $\mathcal{C} = \beta + t^{-N}\mathbb{T}$, and any $\varepsilon > 0$,

there exists $M_0 = M_0(\varepsilon, \mathcal{C})$ such that whenever $M \geq M_0(\varepsilon, \mathcal{C})$,

$$\left| q^{-M} \operatorname{card} \{ x \in \mathbb{F}_q[t]_{\deg < M} : \{a_x\} \in \mathcal{C} \} - \operatorname{mes}(\mathcal{C}) \right| < \varepsilon .$$

It follows as in the first case that with $k = N$, one has

$$\left| q^k N_k(M) - q^M \right| < \varepsilon q^{k+M},$$

and hence

$$\left| \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)) \right| < \varepsilon q^{k+M}.$$

This shows that (take $\beta = \ell / t^k$ and sum over ℓ), for any $g \in \mathbb{F}_q[t]$, when $M \geq M_0'(\varepsilon, k)$,

$$\left| \sum_{\substack{\ell \in \mathbb{F}_q[t] \\ \deg(\ell) < k}} e(g\ell/t^k) \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \ell/t^k)) \right| < \varepsilon q^{2k+M}$$

$$= \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \left(\sum_{\substack{\ell \in \mathbb{F}_q[t] \\ \deg(\ell) < k}} e(\ell (g-h)/t^k) \right) \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h a_x)$$

$$= \begin{cases} q^k, & \text{when } g \equiv h \pmod{t^k} \\ 0, & \text{when } g \not\equiv h \pmod{t^k}. \end{cases}$$

Thus, for each $g \in \mathbb{F}_q[t]$ with $\deg(g) < k$, one finds that

$$\left| q^k \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \right| < \varepsilon q^{2k+M},$$

whence

$$\Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \Big| < (\varepsilon q^k)\, q^M,$$

which is to say that

$$\limsup_{M \to \infty} \; q^{-M} \Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \Big| < \varepsilon q^k.$$

Since $\varepsilon > 0$ is arbitrary, it follows that for every $g \in \mathbb{F}_q[t] \setminus \{0\}$, one has

$$\lim_{M \to \infty} \; q^{-M} \Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \Big| = 0.$$

□

An immediate application of Weyl's inequality shows that the sequence $(\theta x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ whenever θ is irrational.

Theorem 10.4. Suppose that $\theta \in \mathbb{K}_\infty$ is irrational. Then $(\theta x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.

Proof. Suppose that $\theta \in \mathbb{K}_\infty$ is irrational. Then, for any $h \in \mathbb{F}_q[t] \setminus \{0\}$, one sees that $\alpha := h\theta$ is also an irrational element of $\mathbb{K}_\infty$. But if $\operatorname{ord}\{h\theta\} = -N$, we find that whenever $N > M$ one has

$$\sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < N}} e(h\theta x) = \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < N}} e(\alpha x) = \begin{cases} q^N, & \text{when } \|\alpha\| < q^{-N}, \\ 0, & \text{when } \|\alpha\| \geqslant q^{-N}, \end{cases}$$

$$= 0, \qquad \text{since} \quad \|h\theta\| = q^{-M} > q^{-N}.$$

We therefore conclude that, for each $h \in \mathbb{F}_q[t] \setminus \{0\}$, one has

$$\lim_{N\to\infty} q^{-N} \Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < N}} e\big(h(\theta x)\big) \Big| = 0,$$

which ensures that $(\theta x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$. //

As we shall see, this conclusion generalises to polynomials

$$\theta_k x^k + \theta_{k-1} x^{k-1} + \cdots + \theta_1 x,$$

provided that one at least of the coefficients θ_i is irrational, so long as we are not too ambitious concerning the degree k of the leading order term. To see that problems may occur when $k \geq p$, we provide an example of Golitz (1952).

Example 10.5. When $\alpha = \sum_{i \leq n} \alpha_i t^i \in \mathbb{K}_\infty$, consider the map defined by

$$T(\alpha) = \alpha_{-1} t^{-1} + \alpha_{-p-1} t^{-2} + \alpha_{-2p-1} t^{-3} + \cdots.$$

Then T is a linear map from $\mathbb{K}_\infty$ to $\mathbb{T}$. Let

$$\mathcal{Z} = \{ \alpha \in \mathbb{K}_\infty : \alpha_{-1} = \alpha_{-p-1} = \cdots = \alpha_{-rp-1} = \cdots = 0 \}.$$

Then a countability argument shows that there exists an irrational element $\alpha \in \mathbb{K}_\infty$ with $T(\alpha) = 0$ (i.e. $\alpha \in \mathcal{Z}$). Given such an irrational element $\alpha \in \mathcal{Z}$, it follows that whenever $x \in \mathbb{F}_q[t]$, say $x = \sum_{i=0}^{m} x_i t^i$, the coefficient of t^{-1}

in αx^p is equal to

$$\operatorname{res}\left(\alpha\left(x_0^p + x_1^p t^p + \dots + x_m^p t^{mp}\right)\right) = \alpha_{-1} x_0^p + \alpha_{-p-1} x_1^p + \dots + \alpha_{-mp-1} x_m^p$$
$$= 0.$$

Hence, the sequence $(\alpha x^p)_{x \in \mathbb{F}_q[t]}$ has the property that $|\{\alpha x^p\}| \leq q^{-2}$ for every $x \in \mathbb{F}_q[t]$. In particular, one sees that the cylinder $\frac{1}{t} + t^{-N}\mathbb{T}$ contains no points of the sequence (αx^p) modulo 1 whenever $N \geq 1$. This contradicts equidistribution in $\mathbb{T}$, and thus $(\alpha x^p)_{x \in \mathbb{F}_q[t]}$ is not equidistributed in $\mathbb{T}$ for any (irrational) element $\alpha \in \mathcal{B}$.

---

§11. Equidistribution: Weyl's inequality.

In order to investigate the equidistribution of polynomials $\alpha_k x^k + \dots + \alpha_1 x$ of degree $k > 1$, we shall need a version of Weyl's inequality. The idea here is to estimate the exponential sum

$$f(\underline{\alpha}) = \sum_{\deg(x) < X} e\left(\alpha_k x^k + \dots + \alpha_1 x\right)$$

by repeated application of Cauchy's inequality. Thus

$$|f(\alpha)|^2 = f(\alpha) f(-\alpha)$$
$$= \sum_{\deg(x) < X} \sum_{\deg(y) < X} e\left((\alpha_k x^k + \dots + \alpha_1 x) - (\alpha_k y^k + \dots + \alpha_1 y)\right)$$
$$= \sum_{\deg(h) < X} \sum_{\substack{\deg(x) < X \\ y = x+h}} e\left((\alpha_k((x+h)^k - x^k) + \dots + \alpha_1 h)\right).$$

Notice that since $(x+h)^j - x^j = jhx^{j-1} + \dots$, it follows that the argument here may be treated as a polynomial of degree $k-1$. By iterating this process, we are ultimately left with an average of degree 1 polynomials, and geometric progressions.

We require an auxiliary lemma.

Lemma 11.1. Suppose that $\alpha \in \mathbb{K}_\infty$, and $a, g \in A$ satisfy $(a,g) = 1$, g monic, $a \neq 0$, and $|\alpha - a/g| < 1/|g|^2$.

Then one has, for all $\beta \in \mathbb{K}_\infty$,

$$\sum_{|x| < q^X} \min\{q^Y, \|\alpha x + \beta\|^{-1}\} \ll q^{X+Y}\left(|g|^{-1} + q^{-X} + q^{-Y} + |g| q^{-X-Y}\right).$$

Proof. We divide up the range of summation into subintervals of the shape

$$I = \{z + f : \deg(f) < \deg(g)\},$$

with $z \in A$ satisfying $\deg(z) < X$. There are $q^{X - \deg(g)}$ possible choices for z. Suppose that x_1, x_2 are distinct elements of a common subinterval I. Then one has

$$\|(\alpha x_1 + \beta) - (\alpha x_2 + \beta)\| = \|\alpha(x_1 - x_2)\|$$

$$= \left\|\left(\frac{a}{g} + \gamma\right)(x_1 - x_2)\right\|,$$

where we write $\gamma = \alpha - a/g$, so that $|\gamma| < 1/|g|^2$. Notice that $|\gamma(x_1 - x_2)| < 1/|g|$ and, since $(a,g) = 1$, one has $\left\|\frac{a}{g}(x_1 - x_2)\right\| \geq \left\|\frac{1}{g}\right\| = \frac{1}{|g|}$. Thus

$$\left\|\left(\frac{a}{g} + \gamma\right)(x_1 - x_2)\right\| = \left\|\frac{a}{g}(x_1 - x_2)\right\|.$$

Hence, we deduce that

$$\sum_{x \in I} \min\{q^Y, \|\alpha x + \beta\|^{-1}\} \leq q^Y + \sum_{0 \leq \deg(r) < \deg(g)} \left\|\frac{r}{g}\right\|^{-1}$$

$$= q^Y + q|g|(1 + 1/q + \cdots)$$

$$\ll q^Y + |g|.$$

Adding the contributions from all such intervals I, we conclude that

$$\sum_{|x| < q^X} \min\{q^Y, \|\alpha x + \beta\|^{-1}\} \ll (q^Y + |g|)(1 + q^X/|g|)$$

$$= q^{X+Y}(|g|^{-1} + q^{-X} + q^{-Y} + |g| q^{-X-Y}).$$

//

Next, we introduce some standard notation that facilitates the discussion of Weyl differencing. When $\psi : K_\infty \to K_\infty$, we denote by Δ_1 the forward difference operator

$$\Delta_1(\psi(x); h) := \psi(x+h) - \psi(x).$$

We then define Δ_j for $j \geq 2$ recursively by means of the relation

$$\Delta_j(\psi(x); \underline{h}) = \Delta_j(\psi(x); h_1, \ldots, h_j)$$

$$= \Delta_1(\Delta_{j-1}(\psi(x); h_1, \ldots, h_{j-1}); h_j).$$

By convention, we take $\Delta_0(\psi(x); h) = \psi(x)$.

One may verify that when $1 \leq j \leq k$, one has

$$\Delta_j(x^k; \underline{h}) = h_1 \cdots h_j \, p_j(x; h_1, \ldots, h_j),$$

where P_j is a polynomial in x of degree $\leq k-j$ with (leading) coefficient of x^{k-j} equal to $k!/(k-j)!$. Notice here that when $\mathrm{char}(\mathbb{F}_q) < k$, then this coefficient may be 0. By the linearity of the operator Δ_j, one sees that

$$\Delta_j(a_k x^k + \dots + a_1 x; \underline{h}) = \sum_{i=1}^{k} a_i \Delta_j(x^i; \underline{h}),$$

so one may infer the structure of $\Delta_j(p(x); \underline{h})$ easily for general polynomials p. Note that in all cases, when $j > \deg(p)$, one has $\Delta_j(p(x); \underline{h}) = 0$.

Lemma 11.2. (Weyl differencing) Let $\psi : \mathbb{K}_\infty \to \mathbb{K}_\infty$ be any function on $\mathbb{K}_\infty$, and put

$$F(\psi) = \sum_{\deg(x) < X} e(\psi(x)).$$

Then for each natural number j, one has

$$|F(\psi)|^{2^j} \ll (q^X)^{2^j - j - 1} \sum_{\deg(h_1) < X} \dots \sum_{\deg(h_j) < X} \sum_{\deg(x) < X} e(\Delta_j(\psi(x); \underline{h})).$$

Proof. We proceed by induction. When $j = 1$, one has

$$|F(\psi)|^2 = \sum_{\deg(x) < X} \sum_{\deg(y) < X} e(\psi(y) - \psi(x))$$

$$= \sum_{\deg(x) < X} \sum_{\deg(h_1) < X} e(\psi(x + h_1) - \psi(x))$$

$$= \sum_{\deg(h_1) < X} \sum_{\deg(x) < X} e(\Delta_1(\psi(x); h_1)),$$

(with $y = x + h_1$).

Suppose now that the desired conclusion has been established for $1 \le j < J$. Then by Cauchy's inequality, one has

$$|F(\psi)|^{2^J} = \left(|F(\psi)|^{2^{J-1}}\right)^2$$

$$\ll ((q^X)^{2^{J-1}-J})^2 \Big(\underbrace{\sum_{\deg(h_1)<X} \cdots \sum_{\deg(h_{J-1})<X}}_{=(q^X)^{J-1}} 1 \Big) Z(\psi),$$

where

$$Z(\psi) = \sum_{\deg(h_1)<X} \cdots \sum_{\deg(h_{J-1})<X} \Big| \sum_{\deg(x)<X} e\big(\Delta_{J-1}(\psi(x); \underbrace{\underline{h}}_{(h_1,\dots,h_{J-1})})\big)\Big|^2.$$

But

$$\Big| \sum_{\deg(x)<X} e\big(\Delta_{J-1}(\psi(x);\underline{h})\big)\Big|^2 = \sum_{\deg(h_J)<X} \sum_{\deg(x)<X} e\big(\Delta_1(\Delta_{J-1}(\psi(x);\underline{h});h_J)\big)$$

$$= \sum_{\deg(h_J)<X} \sum_{\deg(x)<X} e\big(\Delta_J(\psi(x);\underbrace{\underline{h}}_{(h_1,\dots,h_J)})\big).$$

Thus

$$|F(\psi)|^{2^J} \le (q^X)^{2^J-2J} \cdot (q^X)^{J-1} \sum_{\deg(h_1)<X} \cdots \sum_{\deg(h_J)<X} \Big| \sum_{\deg(x)<X} e\big(\Delta_J(\psi(x);\underline{h})\big)\Big|,$$

and the proof follows by induction. //

Note that, if we apply this Weyl differencing lemma ($k-1$ times) to the exponential sum

$$f(\alpha) = \sum_{\deg(x)<X} e(\alpha x^k),$$

then we find that

$$|f(\alpha)|^{2^{k-1}} \leq (q^X)^{2^{k-1}-k} \sum_{\deg(h_1)<X} \cdots \sum_{\deg(h_{k-1})<X} \sum_{\deg(x)<X} e\Big(\overbrace{k!\alpha h_1 \cdots h_{k-1}(x+\tfrac{1}{2}(h_1+\cdots+h_{k-1}))}^{\Delta_{k-1}(\alpha x^k; h_1,\ldots,h_{k-1})}\Big).$$

Lemma 11.3. (Weyl's inequality) Let $k \geq 2$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{K}_\infty$. Suppose that $a, g \in \mathbb{F}_q[t]$, and $(a,g)=1$, g is monic and $|\alpha_k - a/g| \leq |g|^{-2}$. Then, provided that $\mathrm{char}(\mathbb{F}_q) > k$, one has

$$\sum_{\deg(x)<X} e(\alpha_k x^k + \cdots + \alpha_1 x) \ll (q^X)^{1+\varepsilon}\left(|g|^{-1} + q^{-X} + |g|(q^X)^{-k}\right)^{2^{1-k}}.$$

Proof. Write $\psi(x) = \alpha_k x^k + \ldots + \alpha_1 x$ and

$$F(\underline{\alpha}) = \sum_{\deg(x)<X} e(\psi(x)).$$

We apply the Weyl differencing lemma with $j = k-1$ to obtain the bound

$$|F(\underline{\alpha})|^{2^{k-1}} \ll (q^X)^{2^{k-1}-k} \sum_{\deg(h_1)<X} \cdots \sum_{\deg(h_{k-1})<X} \Upsilon(\underline{h}),$$

where

$$\Upsilon(\underline{h}) = \sum_{\deg(x)<X} e\big(\Delta_{k-1}(\psi(x); \underline{h})\big).$$

Since $\Delta_{k-1}(\psi(x); \underline{h}) = k! h_1 \cdots h_{k-1} x \alpha_k + \gamma$, where γ is independent of x, it follows from HW3, QB4 and Lemma 11.1 that

$$\Upsilon(\underline{h}) = \begin{cases} q^X, & \text{when } \|k! h_1 \cdots h_{k-1} \alpha_k\| < q^{-X}, \\ 0, & \text{when } \|k! h_1 \cdots h_{k-1} \alpha_k\| \geq q^{-X}, \end{cases}$$

whence

$$|F(\alpha)|^{2^{k-1}} \ll (q^X)^{2^{k-1}-k} \sum_{\deg(h_1)<X} \cdots \sum_{\deg(h_{k-1})<X} \min\left\{q^X, \|k! h_1 \cdots h_{k-1} \alpha_k\|^{-1}\right\}$$

$$\leq (q^X)^{2^{k-1}-k}\left(\sum_{0 \leq \deg(g) < (k-1)X} \tau_k(g)\ \min\left\{q^X, \|g\alpha_k\|^{-1}\right\} + \underbrace{(q^X)^{k-1}}_{g=0}\right)$$

$(\#\, h_1, \dots, h_{k-1} \text{ s.t. } h_1 \dots h_{k-1} = 0)$

provided that $p = \mathrm{char}(\mathbb{F}_q) > k$.

$$\overset{\text{Theorem 5.2}}{\ll} (q^X)^{2^{k-1}-k+\varepsilon}\left(\sum_{0 \leq \deg(g) < (k-1)X} \min\left\{q^X, \|g\alpha_k\|^{-1}\right\} + (q^X)^{k-1}\right)$$

$$\overset{\text{Lemma 11.1}}{\ll} (q^X)^{2^{k-1}-k+\varepsilon} \cdot q^X \cdot q^{(k-1)X}\left(|g|^{-1} + q^{-X} + q^{-(k-1)X} + |g| q^{-kX}\right).$$

Hence

$$|F(\alpha)| \ll (q^X)^{1+\varepsilon}\left(|g|^{-1} + q^{-X} + q^{-(k-1)X} + |g| q^{-kX}\right)^{2^{1-k}}. \quad //$$

§12. Equidistribution: rational approximations.

We next recall the basic theory of continued fractions as it relates to the function field setting. For any irrational element $\alpha \in \mathbb{K}_\infty$, we can write α as an infinite continued fraction in the form

$$\alpha = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots}} := [b_0; b_1, b_2, \dots],$$

with $b_i \in \mathbb{F}_q[t]$ and $\deg(b_i) > 0$ $(i \geq 1)$. When α is a rational element of $\mathbb{K}_\infty$, on the other hand, one can write α as a finite continued fraction of the shape

$$\alpha = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots + \cfrac{1}{b_n}}} = [b_0; b_1, \dots, b_n],$$

with $b_i \in \mathbb{F}_q[t]$ and $\deg b_i > 0$ $(1 \leq i \leq n)$.

Note that continued fraction expansions in $\mathbb{K}_\infty$ are uniquely defined.

One defines two sequences $(a_n)_{n\geq -2}$ and $(g_n)_{n\geq -2}$ in $\mathbb{F}_q[t]$ recursively by putting

$$a_{-2} = 0\,,\ g_{-2} = 1\,,\quad a_{-1} = 1\,,\ g_{-1} = 0,$$

and for $n \geq 0$,

$$a_n = b_n a_{n-1} + a_{n-2} \quad \text{and} \quad g_n = b_n g_{n-1} + g_{n-2}.$$

Then for all $n \geq 0$, we have

$$g_n a_{n-1} - g_{n-1} a_n = (-1)^n \quad \text{and} \quad [b_0; b_1, \dots, b_n] = a_n/g_n.$$

The fractions a_n/g_n $(n \geq 0)$ are called the convergents of α. An inductive argument shows that the sequence $(\deg(g_n))_{n\geq 0}$ is strictly increasing.

We record some simple consequences of these definitions.

Lemma 12.1. Suppose that $\alpha \in \mathbb{K}_\infty$. Then the convergents a_n/g_n $(n \geq 0)$ of α satisfy the following properties:

(a) one has $\operatorname{ord}(g_n \alpha - a_n) = -\operatorname{ord} g_{n+1}$ $(n \geq 0)$;

(b) if $a, g \in \mathbb{F}_q[t]$ satisfy $\operatorname{ord}(g\alpha - a) < -\operatorname{ord} g$, then a/g is a convergent of α;

Proof: These are easy exercises. //

Lemma 12.2. Let $\alpha \in \mathbb{K}_\infty$. Suppose that there exists a constant $\varkappa > 1$ such that, for all sufficiently large $N \in \mathbb{N}$, there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$ with $\operatorname{ord}(g\alpha - a) \leq -\varkappa N$ and

$\operatorname{ord} g < N$. Then α is rational.

Proof. Suppose that α is irrational and a_n/g_n $(n \geq 0)$ are the convergents of α. Since α is irrational, we have $\lim_{n\to\infty} \deg(g_n) = +\infty$. We take n sufficiently large and put $N = \operatorname{ord} g_n$.

By hypothesis, we have that there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$ such that $\operatorname{ord}(g) < N$ and

$$\operatorname{ord}(g\alpha - a) \leq -N < -\operatorname{ord} g_n = -N < -\operatorname{ord} g. \quad -(12.1)$$

Then from Lemma 12.1 (b), we see that a/g is a convergent of α. But $\operatorname{ord} g < N = \operatorname{ord} g_n$, and $(\deg(g_n))_{n\geq 0}$ is strictly increasing, so there exists $m \in \mathbb{N} \cup \{0\}$ with $m < n$ such that $a = a_m$ and $g = g_m$. But then from Lemma 12.1 (a),

$$\operatorname{ord}(g\alpha - a) = \operatorname{ord}(g_m\alpha - a_m) = -\operatorname{ord}(g_{m+1}) \geq -\operatorname{ord} g_n.$$

This contradicts (12.1), and so we are forced to conclude that α is rational. //

We shall apply this conclusion in combination with a consequence of Weyl's inequality. Again we suppose that $\operatorname{char}(\mathbb{F}_q) > k$ and we suppose k to be fixed.

Theorem 12.3. There exist positive constants c and C having the following property. Let $\varepsilon > 0$ and let N be sufficiently large in terms of k, ε. Suppose that $\psi(x) = \alpha_k x^k + \cdots + \alpha_1 x$ is a polynomial with coefficients in $\mathbb{K}_\infty$ satisfying the bound

$$\left| \sum_{\deg(x) < N} e(\psi(x)) \right| \geq q^{N-\eta},$$

large enough

for some positive number η with $\eta \le cN$. Then there exist $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ having the property that

$$\operatorname{ord}(g\alpha_u - a) < -kN + \varepsilon N + C\eta \quad \text{and} \quad \deg(g) \le \varepsilon N + C\eta.$$

Proof. Suppose that for some positive number η with $\eta \le cN$ one has

$$\Big| \sum_{\deg(x)<N} e(\psi(x)) \Big| \ge q^{N-\eta}.$$

Suppose that $a, g \in \mathbb{F}_q[t]$ satisfy $(a,g)=1$, g monic, $\deg(g) \le kN - 2^{k-1}\varepsilon N - 2^k\eta$ and $|g\alpha_k - a| < q^{-kN + 2^{k-1}\varepsilon N + 2^k\eta} \le |g|^{-1}$. Such polynomials exist as a consequence of Dirichlet's approximation theorem. By Weyl's inequality (Lemma 11.3), we have

$$\Big| \sum_{\deg(x)<N} e(\psi(x)) \Big| \ll (q^N)^{1+\varepsilon} \Big(|g|^{-1} + q^{-N} + |g| q^{-kN} \Big)^{2^{1-k}}$$

$$\ll (q^N)^{1+\varepsilon} \big(|g|^{-1} + q^{-N} \big)^{2^{1-k}} + q^{N-2\eta}.$$

Thus, when N is large, we deduce that

$$q^{N-\eta} \ll (q^N)^{1+\varepsilon} \big(|g|^{-1} + q^{-N} \big)^{2^{1-k}} + q^{N-2\eta}$$

$$\Downarrow$$

$$|g| \ll \big(q^{N\varepsilon + \eta} \big)^{2^{k-1}} \qquad \text{(provided } \eta \le 2^{-k}N \text{, say)}.$$

Thus, we have

$$\operatorname{ord}(g\alpha_u - a) < -kN + \varepsilon' N + C\eta \quad \text{and} \quad \deg(g) \le \varepsilon' N + C\eta,$$

with $\varepsilon' = 2^{k-1}\varepsilon$. The conclusion follows on relabelling ε. ∎

Now we show that when the lower bound in Theorem 12.3 holds too often, then α_k must be rational.

Lemma 12.4. Suppose that $\psi(x) = \alpha_k x^k + \dots + \alpha_1 x$ is a polynomial with coefficients in $\mathbb{K}_\infty$ with α_k irrational. Then for any fixed $\eta > 0$, there exists $N_0 \in \mathbb{N}$ having the property that for any $b \in \mathbb{F}_q[t]$, one has

$$\Big| \sum_{\deg(x) < N_0} e\big(\psi(x+b)\big) \Big| < q^{N_0 - \eta}.$$

Proof. Suppose that $\eta > 0$. Suppose further that for any $N \in \mathbb{N}$, if possible, one has the existence of $b_N \in \mathbb{F}_q[t]$ such that

$$\Big| \sum_{\deg(x) < N} e\big(\psi(x+b_N)\big) \Big| \geqslant q^{N-\eta}. \qquad (12.2)$$

Applying Theorem 12.3 with $\varepsilon = 1/3$, we see that there exists a constant $C > 0$ such that, for N sufficiently large, there exists $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ having the property that

$$\operatorname{ord}(g\alpha_k - a) < -kN + \tfrac{1}{3}N + C\eta \quad \text{and} \quad \deg(g) < \tfrac{N}{3} + C\eta.$$

For each sufficiently large $M \in \mathbb{N}$, we apply these inequalities with $N = \lfloor 3(M - C\eta) \rfloor$. Then

$$\operatorname{ord}(g\alpha_k - a) \leqslant -(3k-1)M + (3kC\eta + k - \tfrac{1}{3}) \leqslant -3M/2$$

and

$$\deg(g) < M.$$

Since these inequalities hold for all large $M \in \mathbb{N}$, we conclude from Lemma 12.2 that α_k is rational. ⁂ This contradiction

shows that (12.2) cannot hold, and hence the conclusion of the lemma follows. //

Theorem 12.5. Suppose that $p = \mathrm{char}(\mathbb{F}_q) > k$, and that one at least of $\alpha_1, \dots, \alpha_k \in \mathbb{K}_\infty$ is irrational. Then $(\alpha_k x^k + \dots + \alpha_1 x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.

Proof. We suppose that j is the largest index with j irrational. We then put $\alpha_l = a_l / g_l$, with $a_l, g_l \in \mathbb{F}_q[t]$, g_l monic and $(a_l, g_l) = 1$, for $j < l \le k$. Finally, put

$$g = \begin{cases} \mathrm{lcm}\{g_{j+1}, \dots, g_k\}, & \text{when } j < k, \\ 1, & \text{when } j = k. \end{cases}$$

We may now largely remove the influence of the rational coefficients from the discussion by breaking down a summation over polynomials $x \in \mathbb{F}_q[t]$ into arithmetic progressions modulo g. We aim to apply Weyl's criterion, so fix $h \in \mathbb{F}_q[t] \setminus \{0\}$. We have, for large X,

$$\sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < X}} e\left(h\left(\alpha_k x^k + \dots + \alpha_1 x\right)\right) = \sum_{\substack{r \in \mathbb{F}_q[t] \\ \deg(r) < \deg(g)}} \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < X - \deg(g)}} e\left(h\left(\alpha_k (yg + r)^k + \dots + \alpha_1 (yg + r)\right)\right).$$

Since $g \alpha_l \in \mathbb{F}_q[t]$ for $j < l \le k$ and $h \alpha_k r^k + \dots + \alpha_1 r$ is independent of y, we find that

$$\Big| \sum_{y \in \mathbb{F}_q[t]} e\big(h(\alpha_k(yg+r)^k + \cdots + \alpha_1(yg+r))\big) \Big|$$

$$\deg(y) < X - \deg(g)$$

$$= \Big| \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < X - \deg(g)}} e\big(h(\beta_j y^j + \cdots + \beta_1 y)\big) \Big|,$$

where $\beta_l = \beta_l(g, r; \underline{\alpha})$ $(1 \le l \le r)$ and $\beta_j = \alpha_j g^j$. Notice, in particular, since α_j is irrational, then so is $h\beta_j$.

Thus

$$q^{-X} \Big| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < X}} e\big(h(\alpha_k x^k + \cdots + \alpha_1 x)\big) \Big| \le \sum_{\substack{r \in \mathbb{F}_q[t] \\ \deg(r) < \deg(g)}} q^{\deg(g) - X} \Big| \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < X - \deg(g)}} e\big(h(\beta_j y^j + \cdots + \beta_1 y)\big) \Big|.$$

By Weyl's criterion, the sequence $(\alpha_k x^k + \cdots + \alpha_1 x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ if and only if, for each h, the left hand side converges to 0 as $X \to \infty$. This is ensured if, for each of the (finitely many) choices for r, one has that for each h,

$$\lim_{Y \to \infty} q^{-Y} \Big| \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < Y}} e\big(h(\beta_j y^j + \cdots + \beta_1 y)\big) \Big| = 0. \quad -(12.2)$$

Then we seek a contradiction. Suppose, if possible, that this assertion fails. Given any $\eta > 0$, it follows that there are infinitely many (large) natural number N for which

$$\Big| \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < N}} e\big(h(\beta_j y^j + \cdots + \beta_1 y)\big) \Big| \ge q^{N - \eta}.$$

But Lemma 12.4 shows that there exists $N_0 \in \mathbb{N}$ having the property that for any $b \in \mathbb{F}_q[t]$, one has

$$\left| \sum_{\deg(y) < N_0} e\left(h(\beta_j y^j + \cdots + \beta_1 y)\right) \right| < q^{N_0 - \eta}.$$

Hence, whenever $N > N_0$, one has

$$\left| \sum_{\deg(y) < N} e\left(h(\beta_j y^j + \cdots + \beta_1 y)\right) \right| \leq q^{N-N_0} \max_{b \in \mathbb{F}_q[t]} \left| \sum_{\deg(z) < N_0} e\left(h(\beta_j (z+b)^j + \cdots + \beta_1 (z+b))\right) \right|$$

by writing $y = z + t^{N_0} w$, some $w \in \mathbb{F}_q[t]$ with $\deg(w) \leq N - N_0$.

$$\leq q^{N-N_0} \cdot q^{N_0 - \eta} = q^{N-\eta}.$$

This yields a contradiction. Thus we conclude that (12.2) does in fact hold, and hence

$$\lim_{X \to \infty} q^{-X} \left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < X}} e\left(h(\alpha_k x^k + \cdots + \alpha_1 x)\right) \right| = 0.$$

Then $(\alpha_k x^k + \cdots + \alpha_1 x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ by Weyl's criterion. //

§13. An introduction to the circle method in function fields: Waring's problem.

The classical version of Waring's problem, posed by Edward Waring in 1770, seeks to determine the least positive integer $s = s(k)$ having the property that all large enough integers n have a representation

$$n = x_1^k + \dots + x_s^k,$$

with $x_i \in \mathbb{N} \cup \{0\}$. Thus, as was famously shown by Lagrange in 1770, all positive integers are the sum of at most 4 integral squares. By convention, the least such integer s is denoted by $G(k)$, and so one has $G(2) = 4$ (the implicit lower bound here is seen by considering integers of the shape $8m+7$, for example).

One has $G(4) = 16$, but aside from the cases $k = 2, 4$, no other values of $G(k)$ have been determined. The sharpest known upper bounds are:

$G(3) \leq 7$ (Linnik, 1942).
$G(5) \leq 17$ (Vaughan & W., 1995)
$G(6) \leq 24$ (Vaughan & W., 1994)
$\vdots$
$G(k) \leq \lceil k(\log k + 4.20032) \rceil$ (Brüdern & W., 2023).

It is conjectured that $G(k) \leq 4k$ in all cases, and that $G(k) \leq k+1$ unless there is a congruential obstruction.

We consider the analogue in function fields — but first we must decide what this analogue should be!

Let k be an integer with $k \geq 2$, let $s \in \mathbb{N}$, and consider a polynomial m in $\mathbb{F}_q[t]$.

Goal: Determine when m has a representation.

$$m = x_1^k + \cdots + x_s^k,$$

with $x_i \in \mathbb{F}_q[t]$ $(1 \le i \le s)$

Observations: (a) It is possible that a representation of a given m fails to exist for all $s \ge 1$. Thus, for example, if $p \mid k$, then

$$x_1^k + \cdots + x_s^k \in \mathbb{F}_q[t^p]$$

(Note: $(x_0 + x_1 t + \cdots + x_l t^l)^p = x_0^p + x_1^p t^p + \cdots + x_l^p t^{lp}$).

Then m can be represented as a sum of k-th powers only when $m \in \mathbb{F}_q[t^p]$.

(b) If we are aiming for an analogue of Waring's problem, then we should perhaps insist that each x_i belongs to $\mathbb{F}_q[t]^+$. This has its problems. Suppose, for example, that $\mathrm{char}(\mathbb{F}_q) = p$ and $\deg(m) = pl+1$. Then at least one of the x_i must have degree $\ge l+1$. But then enough cancellation amongst the degree $k(l+1)$ terms in

$$x_1^k + \cdots + x_s^k$$

can occur only when $s \ge p$. Since p might be very large compared to k, this seems like an unnecessarily restrictive condition.

If one does not restrict the x_i at all, on the other hand, then the x_i might have degree arbitrarily large in terms of $\deg(m)$. This is the approach of Paley (1933), who aims to show that there are polynomials $x_1, \ldots, x_s$ with

$$x_1^k + \cdots + x_s^k = t.$$

One then finds that

$$x_1(m(t))^k + \cdots + x_s(m(t))^k = m(t).$$

(c) It could be that the set of all sums of kth powers of elements of $\mathbb{F}_q[t]$ is a proper subring of $\mathbb{F}_q[t]$. Take $k = q^2 - 1$ and π a quadratic irreducible monic polynomial in $\mathbb{F}_q[t]$. Then, when $(x, \pi) = 1$, one has

$$x^k = x^{\varphi(\pi)} \equiv 1 \pmod{\pi}.$$

Then it follows that, whenever $s \in \mathbb{N}$, one has

$$x_1^k + \dots + x_s^k \equiv s' \pmod{\pi},$$

with $0 \le s' \le s$, and hence

$$x_1^k + \dots + x_s^k \equiv t \pmod{\pi}$$

is insoluble. We therefore deduce that no polynomial of the shape $\lambda\pi + t$ is represented as the sum of k-th powers in $\mathbb{F}_q[t]$, for any $\lambda \in \mathbb{F}_q[t]$.

For these reasons, it is customary to consider the <u>additive</u> <u>doorme of k-th powers</u> in $\mathbb{F}_q[t]$, a ring denoted by

$$\mathbb{J}_q^k[t] := \{ x_1^k + \dots + x_s^k : x_i \in \mathbb{F}_q[t] \text{ and } s \in \mathbb{N} \cup \{0\} \}.$$

We say that m is an <u>exceptional element</u> of $\mathbb{J}_q^k[t]$ when its leading coefficient lies in $\mathbb{F}_q \setminus \mathbb{J}_q^k$, and in addition $k \mid \deg(m)$. The strongest constraints on the degrees of the variables x_i that might still permit a representation $m = x_1^k + \dots + x_s^k$ is

$$\deg(x_i) \le \lceil (\deg m)/k \rceil \qquad (1 \le i \le s).$$

We define $P = P_k(m) := \lceil (\deg m)/k \rceil$ when m is not exceptional, and when m is exceptional we put

$$P = P_k(m) := \deg(m)/k + 1.$$

This prevents the obstruction that the lead coefficient of m is not an element of $\mathbb{J}_q^k$ in circumstances wherein $\mathbb{J}_q^k \neq \mathbb{F}_q$.

and $k \mid \deg(m)$.

Notice that when m is not exceptional, then P is the unique integer with $k(P-1) < \deg(m) \leq kP$.

Definition 13.1.(a) We say that m admits a strict representation as a sum of s k-th powers when, for some $x_i \in \mathbb{F}_q[t]$ with $\deg(x_i) \leq P_k(m)$ $(1 \leq i \leq s)$, one has

$$x_1^k + \cdots + x_s^k = m.$$

with $q \geq 2$

(b) When k, q are natural numbers exceeding 1, we define $G_q(k)$ to be the least integer s_0 satisfying the property that, whenever $s \geq s_0$ and $m \in \mathbb{F}_q^k[t]$ has sufficiently large degree (in terms of k, s and q), then m admits a strict representation of the shape $m = x_1^k + \cdots + x_s^k$.

Our goal will be a quantitative version of the following theorem.

Theorem 13.2. Suppose that $\mathrm{char}(\mathbb{F}_q) > k$. Then one has

$$G_q(k) \leq 2^k + 1.$$

This is a theorem first proved, more or less simultaneously, by K. R. Matthews (1967), M. Car (1972), R. M. Kubota (1971),

---

Yu-Ru Liu & W. (2010): $G_q(k) \leq Ak(\log k + \log\log k + 2 + O(\log\log k / \log k))$,

whenever $p \nmid k$, where

$$A = \begin{cases} 1, & \text{when } \mathrm{ch}(\mathbb{F}_q) > k, \\ (1 - 2^{-\gamma_q(k)})^{-1}, & \text{when } \mathrm{ch}(\mathbb{F}_q) < k. \end{cases}$$

Here,

$$\gamma_q(k) = a_0 + a_1 + \cdots + a_n \quad \text{when} \quad k = a_0 + a_1 p + \cdots + a_n p^n \text{ in base } p.$$

We apply the Hardy–Littlewood (circle) method to investigate

$$R(m) = \#\{x_1, \dots, x_s \in \mathbb{F}_q[t] : \deg(x_i) \le P \text{ and } x_1^k + \dots + x_s^k = m\},$$

where $P = P_k(m)$. The starting point is to introduce the exponential sum

$$f(\alpha; P) = \sum_{\deg(x) \le P} e(\alpha x^k), \qquad (13.1)$$

and observe that by orthogonality, one has

$$R(m) = \int_{\mathbb{T}} f(\alpha; P)^s e(-m\alpha)\, d\alpha. \qquad (13.2)$$

$$\sum_{\deg(x_1) \le P} \cdots \sum_{\deg(x_s) \le P} e\big(\alpha(x_1^k + \dots + x_s^k - m)\big).$$

In order to analyse the integral (13.2), we follow the idea of Hardy and Littlewood from 1920, introducing so-called major and minor arcs. Thus, we take W to be a parameter with $1 \le 2W < kP$. Given polynomials $a, g \in \mathbb{F}_q[t]$ with $(a,g) = 1$ and g monic, we define the Farey arc

$$\mathfrak{M}(g,a) = \mathfrak{M}(g,a;W)$$

centred on a/g by putting

$$\mathfrak{M}(g,a;W) = \{\alpha \in \mathbb{K}_\infty : |g\alpha - a| < q^W (q^P)^{-k}\}.$$

The set of major arcs $\mathfrak{M}(W)$ is then defined to be the union of the sets

$$\mathfrak{M}(g,a;W) \quad \text{with}$$

$a, g \in \mathbb{F}_q[t]$, g monic, $0 \le |a| < |g| \le q^W$ and $(a,g) = 1$.

Thus, we have $\mathfrak{M}(W) \subseteq \mathbb{T}$.

We then define the set $\mathfrak{m}(W) = \mathbb{T} \setminus \mathfrak{M}(W)$, the so-called minor arcs in the Hardy-Littlewood decomposition.

One can check that the arcs $\mathfrak{M}(g,a;W)$ comprising $\mathfrak{M}(W)$ are disjoint. Our goal is to show that the contribution of the poorly approximated points $\alpha \in \mathfrak{m}(W)$ is small, so that for an appropriate choice of $W \to \infty$ as $P \to \infty$, one has

$$\left| \int_{\mathfrak{m}} f(\alpha;P)^s e(-n\alpha)\, d\alpha \right| = o\left((q^P)^{s-k}\right) \quad \text{as } P \to \infty.$$

Here we continue the assumption $s \ge 2^k + 1$. If we can also obtain an asymptotic formula of the shape

$$\int_{\mathfrak{M}} f(\alpha;P)^s e(-n\alpha)\, d\alpha \sim C_{s,k,q}(n)\,(q^P)^{s-k},$$

with $C_{s,k,q}(n)$ bounded away from 0 appropriately, then we conclude that

$$\int_{\mathbb{T}} f(\alpha;P)^s e(-n\alpha)\, d\alpha = \int_{\mathfrak{M}} f(\alpha;P)^s e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} f(\alpha;P)^s e(-n\alpha)\, d\alpha$$

$$= C_{s,k,q}(n)\,(q^P)^{s-k} + o\left((q^P)^{s-k}\right)$$

$$\longrightarrow \infty \quad \text{as} \quad P \to \infty.$$

In particular, we shall have shown that $R(n) \ge 1$ for large $\deg(n)$.

§14. The contribution of the minor arcs.

We begin by establishing a non-trivial estimate for the generating function $f(\alpha; P)$ valid uniformly for $\alpha \in \mathfrak{m}(W)$. Throughout, we assume that $1 \leq W \leq P$.

Lemma 14.1. Suppose that $k \geq 2$ and $\mathrm{char}(\mathbb{F}_q) > k$. Then one has

$$\sup_{\alpha \in \mathfrak{m}(W)} |f(\alpha; P)| \ll (q^P)^{1+\varepsilon} (q^W)^{-2^{1-k}}.$$

Proof. We apply Weyl's inequality. Suppose that $\alpha \in \mathfrak{m}(W)$. By applying Dirichlet's approximation theorem, we find that there exist $a, g \in \mathbb{F}_q[t]$ with $(a, g) = 1$, g monic, $1 \leq |g| \leq q^{kP-W}$ and $|g\alpha - a| < (q^W)(q^P)^{-k}$. If one were to have $|g| \leq q^W$, then we would have $\alpha \in \mathfrak{N}(W)$, contradicting our hypothesis that $\alpha \in \mathfrak{m}(W) = \mathbb{T} \setminus \mathfrak{M}(W)$. Then we are forced to conclude that $|g| > q^W$.

We now deduce from Weyl's inequality (Lemma 11.3) that

$$\sum_{\deg(x) \leq P} e(\alpha x^k) \ll (q^P)^{1+\varepsilon} \left(|g|^{-1} + q^{-P} + |g|(q^P)^{-k} \right)^{2^{1-k}}$$

$$\ll (q^P)^{1+\varepsilon} \left(q^{-W} + q^{-P} + q^{kP-W}(q^P)^{-k} \right)^{2^{1-k}}$$

$$\ll (q^P)^{1+\varepsilon} (q^W)^{-2^{1-k}}. \quad //$$

Let us consider the representation problem

$$x_1^k + \dots + x_s^k = m,$$

with $\deg(x_i) \leqslant P$. We have $x_i = x_{i0} + x_{i1}t + \dots + x_{iP}t^P$ with $x_i \in \mathbb{F}_q$, so by comparing coefficients of powers of t on left and right hand sides, we see that there are

$$kP+1 \quad \text{equations of degree } k \text{ over } \mathbb{F}_q.$$

We expect the number of solutions here to be

$$\approx (q^{P+1})^s / q^{kP+1}$$

(q^{P+1}: # choices for $x_1, \dots, x_s$; q^{kP+1}: constraint from $kP+1$ equations)

$$\approx q^{s-1} \cdot (q^P)^{s-k}.$$

If we are able to take $W = \mathfrak{P}$ and $s > k2^{k-1}$, then it follows from Lemma 14.1 that

$$\left| \int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-\alpha m)\, d\alpha \right| \leq \int_{\mathfrak{m}(W)} |f(\alpha;P)|^s \, d\alpha$$

$$\leqslant \Big(\sup_{\alpha \in \mathfrak{m}(W)} |f(\alpha;P)| \Big)^s \operatorname{mes}(\mathfrak{m}(W))$$

$$\ll \left((q^P)^{1+\varepsilon-2^{1-k}} \right)^s \cdot 1$$

$$\ll (q^P)^{s-k} \cdot (q^P)^{s\varepsilon - 2^{1-k}}.$$

Thus, we find that $\displaystyle\int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-\alpha m)\, d\alpha = o\left((q^P)^{s-k}\right)$,

which suffices for our purposes. We can do better by using an idea of Hua (1938).

Lemma 14.2. Suppose that $k \geq 2$ and $\mathrm{char}(\mathbb{F}_q) > k$. Then, whenever $1 \leq j \leq k$, one has

$$\int_{\mathfrak{m}} |f(\alpha; P)|^{2^j} \, d\alpha \ll (q^P)^{2^j - j + \varepsilon}.$$

Proof. We take an inductive approach. When $j = 1$, one finds by orthogonality that

$$\int_{\mathfrak{m}} |f(\alpha; P)|^2 \, d\alpha = \int_{\mathfrak{m}} f(\alpha; P) f(-\alpha; P) \, d\alpha$$

$$= \#\{x, y \in \mathbb{F}_q[t] : \deg(x) \leq P, \deg(y) \leq P, \text{ and } x^k = y^k\}$$

$$\leq k q^{P+1}.$$

This confirms the desired conclusion when $j = 1$. □

Now suppose that the conclusion of the lemma has been established for $1 \leq j \leq J$ with some J satisfying $1 \leq J < k$. By applying the Weyl differencing lemma (Lemma 11.2), we find that

$$|f(\alpha; P)|^{2^J} \leq (q^{P+1})^{2^J - J - 1} \sum_{|h_1| \leq q^P} \cdots \sum_{|h_J| \leq q^P} \sum_{|x| \leq q^P} e(\alpha \Delta_J(x^k; \underline{h})).$$

Thus,

$$\int_{\mathfrak{m}} |f(\alpha; P)|^{2^{J+1}} \, d\alpha = \int_{\mathfrak{m}} f(\alpha)^{2^{J-1}} f(-\alpha)^{2^{J-1}} |f(\alpha)|^{2^J} \, d\alpha$$

$$\leq (q^{P+1})^{2^J - J - 1} T,$$

where

$$T = \sum_{|h_1| \leq q^P} \cdots \sum_{|h_J| \leq q^P} \sum_{|x| \leq q^P} \int_{\mathfrak{m}} f(\alpha)^{2^{J-1}} f(-\alpha)^{2^{J-1}} e(\alpha \Delta_J(x^k; \underline{h})) \, d\alpha.$$

By orthogonality, the expression T counts the number of solutions of the equation

$$\sum_{i=1}^{2^{J-1}} (u_i^k - v_i^k) = \Delta_J(x^k; \underline{h}),$$

with $\deg(u_i)$, $\deg(v_i) \le P$, $\deg(x) \le P$ and $\deg(h_\ell) \le P$ $(1 \le \ell \le J)$.
The solutions counted by T are of two types. First, there are solutions with

$$\sum_{i=1}^{2^{J-1}} (u_i^k - v_i^k) = 0.$$

The number of possible choices for $\underline{u}$ and $\underline{v}$ here is, by orthogonality,

$$\int_{\mathfrak{N}} |f(\alpha; P)|^{2^J} d\alpha \ll (q^P)^{2^J - J + \varepsilon}.$$

(inductive hypothesis)

For each such choice of $\underline{u}, \underline{v}$, one has $\Delta_J(x^k; \underline{h}) = 0$, whence

$$h_1 \cdots h_J \left(\frac{k!}{(k-J)!} x^{k-J} + \cdots \right) = 0.$$

Then either $h_\ell = 0$ for some $1 \le \ell \le J$, or else x satisfies a polynomial equation (with coefficients depending only on $h_1, \dots, h_J$) of degree $k-J$. Then the total number of choices for x and $h_1, \dots, h_J$ is $O((q^P)^J)$. It therefore follows that the total contribution from this class of solutions, say T_1, satisfies

$$T_1 \ll (q^P)^J \cdot (q^P)^{2^J - J + \varepsilon} \ll (q^P)^{2^J + \varepsilon}.$$

The remaining solutions counted by T satisfy the condition that

$$\sum_{i=1}^{2^{J-1}} (u_i^k - v_i^k) = w,$$

say, with $w \neq 0$. There are at most $(q^{P+1})^{2^J}$ possible choices

for $\underline{u}, \underline{v}$ generating such solutions. Given any one such choice, one has

$$h_1 \cdots h_J \left(\frac{k!}{(k-J)!} x^{k-J} + \cdots \right) = W,$$

with $|W| \leq (q^P)^k$. It follows that $h_1, \ldots, h_J$ and

$$\frac{k!}{(k-J)!} x^{k-J} + \cdots$$

are all divisors of the non-zero polynomial W. There are $O(|W|^\varepsilon)$ possible choices for such divisors (Theorem 5.2), and hence $O\left((q^P)^{k\varepsilon}\right)$ possible choices for $h_1, \ldots, h_J$ and x. It therefore follows that the total contribution from this class of solutions, say T_2, satisfies

$$T_2 \ll (q^P)^{k\varepsilon} \cdot (q^{P+1})^{2^J} \ll (q^P)^{2^J + k\varepsilon}.$$

We have shown that $T = T_1 + T_2 \ll (q^P)^{2^J + k\varepsilon}$,

whence

$$\int_{\mathfrak{m}} |f(\alpha; P)|^{2^{J+1}} d\alpha \ll (q^P)^{2^J - J - 1} \cdot (q^P)^{2^J + k\varepsilon}$$
$$\ll (q^P)^{2^{J+1} - J - 1 + k\varepsilon}.$$

This confirms the conclusion of the lemma when $j = J+1$, and hence the desired conclusion follows by induction on J. //

Notice that when $J \geq k$, one has $\Delta_J(x^k; \underline{h})$ independent of x (and indeed this expression is 0 when $J > k$). Thus, we cannot expect the conclusion of this lemma to remain valid when $j > k$. Moreover, when $\mathrm{char}(\mathbb{F}_q) \leq k$, the lead coefficient of $\Delta_J(x^k; \underline{h})$

vanishes when $J \geq 1$, and this also clearly limits the values of j for which the conclusion of Lemma 14.2 can be valid.

By combining Lemmata 14.1 and 14.2, we obtain a satisfactory upper bound for the contribution of the minor arcs $\mathfrak{m}(W)$.

Lemma 14.3. Suppose that $k \geq 2$ and that $(\mathbb{F}_q) > k$. Then, whenever $s > 2^k$, one has

$$\left| \int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-n\alpha)\,d\alpha \right| \ll (q^P)^{s-k+\varepsilon} (q^W)^{-2^{1-k}}.$$

Proof. By the triangle inequality, one finds that

$$\int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-n\alpha)\,d\alpha \leq \Big(\sup_{\alpha \in \mathfrak{m}(W)} |f(\alpha;P)| \Big)^{s-2^k} \int_{\mathbb{T}} |f(\alpha;P)|^{2^k} d\alpha .$$

Then by Lemmata 14.1 and 14.2, we conclude that

$$\begin{aligned} \int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-n\alpha)\,d\alpha &\ll \big((q^P)^{1+\varepsilon} (q^W)^{-2^{1-k}} \big)^{s-2^k} \cdot (q^P)^{2^k - k + \varepsilon} \\ &\ll (q^P)^{s-k+s\varepsilon} (q^W)^{-2^{1-k}} . \end{aligned}$$

//

§15. Major arc approximations to exponential sums.

We turn now to consider the contribution of the major arcs $\mathfrak{M}(W)$ to $R(n)$.

Lemma 15.1 Suppose that $\alpha \in \mathbb{T}$, and that $\alpha = a/g + \beta$, with $a, g \in \mathbb{F}_q[t]$, $0 \leq |a| < |g| \leq q^P$, g monic and $|\beta| < |g|^{-1} (q^P)^{1-k}$. Then one has

$$f(\alpha; P) = |g|^{-1} S(g,a) f(\beta; P),$$

where

$$S(g,a) = \sum_{0 \le |r| < |g|} e(ar^k/g).$$

Proof. We break the summands in the sum

$$f(\alpha; P) = \sum_{|x| \le q^P} e(\alpha x^k)$$

into arithmetic progressions modulo g. Thus, we write

$$x = gy + r,$$

with $|y| \le q^P/|g|$ and $|r| < |g|$, noting ~~that~~ this uniquely defines y and r. It follows ~~that~~ one then has

$$e\left(\frac{a}{g} x^k\right) = e\left(\frac{a}{g}(gy+r)^k\right) = e\left(\frac{a}{g} r^k\right),$$

whence

$$f\left(\beta + \frac{a}{g}; P\right) = \sum_{|x| \le q^P} e\left(\frac{a}{g} x^k + \beta x^k\right)$$

$$= \sum_{|y| \le q^P/|g|} \sum_{|r| < |g|} e\left(\frac{a}{g} r^k\right) e\left(\beta (gy+r)^k\right)$$

$$= \sum_{|r| < |g|} e\left(\frac{a}{g} r^k\right) \sum_{|y| \le q^P/|g|} e\left(\beta (gy+r)^k\right). \quad \text{— (15.1)}$$

In order to handle the inner sum over y, we observe that when $|\beta| < |g|^{-1}(q^P)^{1-k}$, one has

$$|\beta(gy+r)^k - \beta(gy)^k| \leqslant |\beta|\,|r|\,|gy|^{k-1} \qquad (\text{for } y \neq 0)$$

$$< \left(|g|^{-1}(q^P)^{1-k}\right)\cdot\left(q^{-1}|g|\cdot(q^P)^{k-1}\right)$$

$$= q^{-1}.$$

Thus

$$\operatorname{ord}\left(\beta(qy+r)^k - \beta(gy)^k\right) < -1,$$

so that

$$e\left(\beta(gy+r)^k - \beta(gy)^k\right) = 1.$$

This enables us to conclude that

$$e\left(\beta(gy+r)^k\right) = e\left(\beta(gy)^k\right),$$

whence

$$\sum_{|y|\leq q^P/|g|} e\left(\beta(gy+r)^k\right) = \sum_{|y|\leq q^P/|g|} e\left(\beta(gy)^k\right).$$

Moreover, this same relation shows that

$$\sum_{|r|<|g|}\ \sum_{|y|\leq q^P/|g|} e\left(\beta(gy+r)^k\right) = |g| \sum_{|y|\leq q^P/|g|} e\left(\beta(gy)^k\right),$$

$$\Vert$$

$$\sum_{|x|\leq q^P} e(\beta x^k)$$

so that

$$\sum_{|y|\leq q^P/|g|} e\left(\beta(gy+r)^k\right) = \frac{1}{|g|}\sum_{|x|\leq q^P} e(\beta x^k) = \frac{1}{|g|} f(\beta;P).$$

By substituting into (15.1), we conclude that

$$f(\alpha;P) = f(\beta+\tfrac{a}{g};P) = \sum_{|r|<|g|} e(ar^k/g)\cdot\frac{1}{|g|}f(\beta;P)$$

$$= \frac{1}{|g|}S(g,a)f(\beta;P). \qquad //$$

This relation allows us very nearly to separate local contributions in the major arc analysis. Observe that

$$\int_{\mathfrak{M}(W)} f(\alpha;P)^s e(-m\alpha)\,d\alpha = \sum_{\substack{1\le|g|\le q^W\\ g\text{ monic}}}\sum_{\substack{0\le|a|<|g|\\ (a,g)=1}}\int_{|\beta|<|g|^{-1}q^W(q^P)^{-k}} f(\beta+a/g)^s e(-m(\beta+\tfrac{a}{g}))\,d\beta$$

$$= \sum_{\substack{1\le|g|\le q^W\\ g\text{ monic}}}\sum_{\substack{0\le|a|<|g|\\ (a,g)=1}} |g|^{-s}S(g,a)^s e(-ma/g)\; I_s(g;W),$$

where

$$I_s(g;W) = \int_{|\beta|<|g|^{-1}q^W(q^P)^{-k}} f(\beta;P)^s e(-m\beta)\,d\beta.$$

Further analysis requires that we provide pointwise bounds for $S(g,a)$ and $f(\beta;P)$.

§16. A transference principle.

Rather than provide sharper estimates for the auxiliary functions $S(q,a)$ and $f(\beta;P)$, we take a short-cut offered by a transference principle.

Lemma 16.1. Let θ, X, Y, Z be positive real numbers. Suppose that $\Psi : K_\infty \longrightarrow \mathbb{C}$ satisfies the property that whenever $a \in \mathbb{F}_q[t]$, $g \in \mathbb{F}_q[t]^+$ satisfy $(a,g) = 1$ and $|\alpha - a/g| < 1/|g|^2$, then

$$\Psi(\alpha) \ll X\left(|g|^{-1} + Y^{-1} + |g|Z^{-1}\right)^\theta. \qquad (16.1)$$

Then, whenever $b \in \mathbb{F}_q[t]$ and $r \in \mathbb{F}_q[t]^+$ satisfy $(b,r) = 1$, one has

$$\Psi(\alpha) \ll X\left(\lambda^{-1} + Y^{-1} + \lambda Z^{-1}\right)^\theta, \qquad (16.2)$$

where $\lambda = |r| + Z|r\alpha - b|$.

Proof. Suppose that $b \in \mathbb{F}_q[t]$ and $r \in \mathbb{F}_q[t]^+$ satisfy $(b,r) = 1$. By Dirichlet's approximation theorem, there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t]^+$ with $1 \leqslant |g| \leqslant |r|$ and $|g\alpha - a| < |r|^{-1}$. Suppose in the first instance that $a/g \neq b/r$. Then

$$\frac{1}{|gr|} \leqslant \left|\frac{a}{g} - \frac{b}{r}\right| \leqslant \max\left\{\left|\alpha - \frac{b}{r}\right|, \left|\alpha - \frac{a}{g}\right|\right\}$$

$$\leqslant \max\left\{\left|\alpha - \frac{b}{r}\right|, q^{-1} \cdot \frac{1}{|gr|}\right\}$$

Hence $|g|^{-1} \leqslant |r\alpha - b|$, and so we deduce from (16.1) that

$$\Psi(\alpha) \ll X\left(|r\alpha - b| + Y^{-1} + |r|Z^{-1}\right)^\theta$$

$$\ll X(Y^{-1} + \lambda Z^{-1})^{\theta}.$$

This confirms the estimate (16.2) in this case.

Now suppose that $a/g = b/r$. Since $(a,g) = (b,r) = 1$, we see that $g = r$ and $a = b$, and hence $|r\alpha - b| < |r|^{-1}$. If $\alpha = b/r$, then $\lambda = |r|$ and the desired conclusion (16.2) is immediate from (16.1). So we may suppose that $0 < |\alpha - b/r| \leq 1/|r|^2$. In this situation, we may again apply Dirichlet's approximation theorem. Thus, there exist $a' \in \mathbb{F}_q[t]$ and $g' \in \mathbb{F}_q[t]^+$ with $1 \leq |g'| \leq |r\alpha - b|^{-1}$ such that

$$|g'\alpha - a'| < |r\alpha - b| \leq |g'|^{-1}.$$

If one were to have $a'/g' = b/r$, then since $(a',g') = (b,r) = 1$, one finds that $g' = r$ and $a' = b$, and so $|g'\alpha - a'| = |r\alpha - b|$, yielding a contradiction. Thus $a'/g' \neq b/r$, and one has

$$\frac{1}{|g'r|} \leq \left| \frac{a'}{g'} - \frac{b}{r} \right| \leq \max\left\{ \left|\alpha - \frac{b}{r}\right|, \left|\alpha - \frac{a'}{g'}\right| \right\}$$

$$\leq \max\left\{ \left|\alpha - \frac{b}{r}\right|, q^{-1}|r\alpha - b|/|g'| \right\}$$

$$\leq \max\left\{ |\alpha - b/r|, q^{-1} \cdot \frac{1}{|rg'|} \right\}.$$

We therefore see that $|r\alpha - b| \geqslant |g'|^{-1}$, and hence we deduce from (16.1) that

$$\Psi(\alpha) \ll X\left(|g'|^{-1} + Y^{-1} + |g'|Z^{-1} \right)^{\theta}$$

$$\ll X\left(|r\alpha - b| + Y^{-1} + (Z|r\alpha - b|)^{-1} \right)^{\theta}.$$

Alternatively, since $|\alpha - b/r| \leq 1/|r|^2$, one may apply (16.1) to give

$$\Psi(\alpha) \ll X\left(|r|^{-1} + Y^{-1} + rZ^{-1}\right)^{\theta}.$$

Thus, in any case, one obtains the bound

$$\Psi(\alpha) \ll X\left(\lambda^{-1} + Y^{-1} + \lambda Z^{-1}\right)^{\theta},$$

where $\lambda = |r| + Z|r\alpha - b|$. This completes the proof of the lemma. //

This general principle (which basically amounts to an equivalence between real and p-adic behaviours in the classical context) yields directly a consequence of Weyl's inequality (Lemma 11.3).

Lemma 16.2 Let $k \geq 2$ and $\alpha \in \mathbb{K}_\infty$. Then, whenever $a, g \in \mathbb{F}_q[t]$ satisfy g monic and $(g,a) = 1$, one has (provided $\mathrm{char}(\mathbb{F}_q) > k$),

$$f(\alpha; P) \ll (q^P)^{1+\varepsilon}\left(\lambda^{-1} + q^{-P} + \lambda(q^P)^{-k}\right)^{2^{1-k}},$$

where $\lambda = |g| + (q^P)^k |g\alpha - a|$.

Proof. It follows from Weyl's inequality that whenever $b, r \in \mathbb{F}_q[t]$, and r is monic, $(b,r) = 1$ and $|\alpha - b/r| < |r|^{-2}$, then, provided $\mathrm{char}(\mathbb{F}_q) > k$, one has

$$|f(\alpha; P)| \ll (q^P)^{1+\varepsilon}\left(|r|^{-1} + q^{-P} + |r|(q^P)^{-k}\right)^{2^{1-k}}.$$

Then, applying the transference principle with $X = (q^P)^{1+\varepsilon}$, $Y = q^P$, $Z = (q^P)^k$, $\theta = 2^{1-k}$, the desired conclusion follows. //

Corollary 16.3. Suppose that $\mathrm{char}(\mathbb{F}_q) > k$ and $|\beta| < (q^P)^{1-k}$. Then one has

$$f(\beta; P) \ll (q^P)^{1+\varepsilon} \left(1 + (q^P)^k |\beta|\right)^{-2^{1-k}}.$$

Proof. We apply Lemma 16.2 with $\alpha = \beta$, $a = 0$ and $g = 1$. Thus we find that $\lambda = 1 + (q^P)^k |\beta|$ and

$$f(\beta; P) \ll (q^P)^{1+\varepsilon} \left((1 + (q^P)^k |\beta|)^{-1} + q^{-P} + |\beta|\right)^{2^{1-k}}.$$

Since we assume that $|\beta| < (q^P)^{1-k}$, we have

$$1 + (q^P)^k |\beta| < 1 + (q^P),$$

whence

$$\left(1 + (q^P)^k |\beta|\right)^{-1} \geqslant q^{-P}.$$

Likewise, we have $|\beta| < (q^P)^{1-k} \leq q^{-P}$. Hence we conclude that

$$f(\beta; P) \ll (q^P)^{1+\varepsilon} \left(1 + (q^P)^k |\beta|\right)^{-2^{1-k}},$$

as desired. //

Corollary 16.4. Whenever $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t]^+$ satisfy $(a, g) = 1$, one has

$$S(g, a) \ll |g|^{1 - 2^{1-k} + \varepsilon}.$$

Proof. We have

$$S(g,a) = f\left(\frac{a}{g}; \deg(g)\right)$$
$$\ll |g|^{1+\varepsilon}\left(|g|^{-1} + |g|^{-1} + |g|\cdot|g|^{-k}\right)^{2^{1-k}}$$
$$\ll |g|^{1-2^{1-k}+\varepsilon}$$

//

We note that with greater effort, one can prove an analogue of Corollary 16.3 showing that when $|\beta| < (q^P)^{1-k}$, one has

$$f(\beta; P) \ll (q^P)\left(1 + (q^P)^k|\beta|\right)^{-1/k}.$$

Similarly, one can establish an analogue of Corollary 16.4 yielding the bound

$$S(g,a) \ll |g|^{1-1/k+\varepsilon},$$

whenever $(a,g) = 1$.

Before further analysis of the major arc contribution, we pause to investigate the consequences of our new estimates for $I_s(g;W)$. We extend the range of integration to define

$$I_s(\mathfrak{P}) = \int_{|\beta| < (q^{P+1})^{1-k}} f(\beta; P)^s\, e(-m\beta)\, d\beta.$$

Thus we find that

$$|I_s(\mathfrak{P}) - I_s(g;W)| = \left|\int_{|g|^{-1}q^W(q^P)^{-k} \le |\beta| < (q^{P+1})^{1-k}} f(\beta;P)^s\, e(-m\beta)\, d\beta\right|$$

$$\leq \int_{|g|^{-1}q^W(q^P)^{-k} \leq |\beta| < (q^P)^{1-k}} |f(\beta;P)|^s \, d\beta .$$

Consequently, when $s > 2^k + 1$ and $|g| \leq q^W$, we see that

$$|I_s(\phi) - I_s(g;W)| \ll (q^P)^{s+\varepsilon} \int_{|g|^{-1}q^W(q^P)^{-k} \leq |\beta| < (q^P)^{1-k}} \left((q^P)^k |\beta|\right)^{-2-2^{1-k}} d\beta$$

$$\ll (q^P)^{s-2k+\varepsilon} \left(\frac{q^W}{|g|}\right)^{-2^{1-k}} \int_{|\beta| \geq (q^P)^{-k}} |\beta|^{-2} \, d\beta .$$

We can calculate the integral by examining the elements β with $\operatorname{ord} \beta = -h$. Thus

$$\int_{|\beta| \geq (q^P)^{-k}} |\beta|^{-2} \, d\beta = \sum_{h \geq -kP} q^{-2h} \cdot \int_{|\beta| = q^h} d\beta$$

$$= \sum_{h \geq -kP} q^{-2h} \cdot (q-1)q^h \ll q^{kP} .$$

Hence

$$|I_s(\phi) - I_s(g;W)| \ll (q^P)^{s-k+\varepsilon} \left(\frac{q^W}{|g|}\right)^{-2^{1-k}} .$$

We thus deduce that

$$\left| \int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-m\alpha) \, d\alpha - I_s(P) \sum_{1 \leq |g| \leq q^W \atop g \text{ monic}} \sum_{0 \leq |a| < |g| \atop (a,g)=1} |g|^{-s} S(g,a)^s e(-ma/g) \right|$$

$$\ll \sum_{\substack{1 \le |g| \le q^W \\ g \text{ monic}}} \sum_{\substack{0 \le |a| < |g| \\ (a,g)=1}} |g|^{-s} |S(g,a)|^s \, |I_s(P) - I_s(g;W)|$$

$$\ll (q^P)^{s-k+\varepsilon} \sum_{\substack{1 \le |g| \le q^W \\ g \text{ monic}}} \phi(g) |g|^{-s} \left(|g|^{1-2^{1-k}+\varepsilon}\right)^s \left(\frac{q^W}{|g|}\right)^{-2^{-k}}.$$

Since we assume that $s \ge 2^k$, this error term is

$$\ll (q^P)^{s-k+\varepsilon} \sum_{\substack{1 \le |g| \le q^W \\ g \text{ monic}}} |g|^{1-s2^{1-k}+s\varepsilon+2^{-k}} (q^W)^{-2^{-k}}$$

$$\ll (q^P)^{s-k+\varepsilon} (q^W)^{-2^{-k}} \underbrace{\sum_{\substack{1 \le |g| \le q^W \\ g \text{ monic}}} |g|^{-1-2^{-1-k}}}_{\| \; O(1)}$$

Thus

$$\int_{\mathfrak{M}(W)} f(\alpha;P)^s e(-m\alpha)\, d\alpha = I_s(P) \sum_{\substack{1 \le |g| \le q^W \\ g \text{ monic}}} \sum_{\substack{0 \le |a| < |g| \\ (a,g)=1}} |g|^{-s} S(g,a)^s e(-ma/g) + O\left((q^P)^{s-k+\varepsilon} (q^W)^{-2^{-k}}\right).$$

Hence the error term here is $o\left((q^P)^{s-k}\right)$ provided only that $W \ge \delta P$ for a fixed positive number δ.

We summarise this conclusion in the form of a lemma. Here, we write

$$\mathfrak{S}(m;W) = \sum_{\substack{1\le|g|\le q^W \\ g \text{ monic}}} \sum_{\substack{0\le|a|<|g| \\ (a,g)=1}} |g|^{-s} S(g,a)^s e(-ma/g).$$

Lemma 16.5. Suppose that $s \ge 2^k+1$ and $\mathrm{char}(\mathbb{F}_q) > k$. Then one has

$$\int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-m\alpha)\,d\alpha = I_s(P)\mathfrak{S}(m;W) + O\big((q^P)^{s-k+\varepsilon}(q^W)^{-2^k}\big).$$

Note that, as before, we assume in this statement that $1 \le W \le P$.

---

§17. The singular integral.

By analogy with the classical treatments, we refer to the quantity $I_s(P)$ as the singular integral.

Suppose that the leading coefficient of the polynomial m is $c(m)$. We define $b = b(m)$ by putting

$$b(m) = \begin{cases} c(m), & \text{when } k \mid \deg(m) \text{ and } m \text{ is not exceptional}, \\ 0, & \text{otherwise}. \end{cases}$$

Also, we define $J_\infty(m) = J_\infty(m;q)$ by

$$J_\infty(m) := \mathrm{card}\{\underline{a} \in \mathbb{F}_q^s \setminus \{0\} : a_1^k + \cdots + a_s^k = b\}.$$

Lemma 17.1. Whenever $s \ge 2^{k-1}+1$, one has

$$I_s(P) = J_\infty(m)(q^P)^{s-k}.$$

Proof. We take a constructive approach which essentially applies an

argument reminiscent of Hensel's lemma, but in concrete form. We begin by observing that when $n \geqslant 0$, one has

$$\int_{\operatorname{ord}\alpha < -n} e(N\alpha)\, d\alpha = \begin{cases} q^{-n}, & \text{when } \operatorname{ord} N < n, \\ 0, & \text{otherwise.} \end{cases}$$

When $n = 0$, this follows by our previous orthogonality arguments, and when $n > 0$ one proves this in similar fashion (see HW).

We therefore find that

$$I_s(P) = \int_{|\beta| < (q^{P+1})^{1-k}} f(\beta; P)^s\, e(-m\beta)\, d\beta$$

$$= \int_{|\beta| < (q^{P+1})^{1-k}} \sum_{\substack{x_1, \dots, x_s \\ \operatorname{ord}(x_i) \leqslant P}} e\left(\beta\left(x_1^k + \dots + x_s^k - m\right)\right) d\beta$$

$$= \sum_{\substack{x_1, \dots, x_s \\ \operatorname{ord}(x_i) \leqslant P \\ \operatorname{ord}(x_1^k + \dots + x_s^k - m) < (k-1)(P+1)}} q^{-(k-1)(P+1)}.$$

It therefore remains to count the number $I(m)$ of solutions of the inequality

$$\operatorname{ord}(x_1^k + \dots + x_s^k - m) < (k-1)(P+1), \qquad (17.1)$$

with $x_i \in \mathbb{F}_q[t]$ and $\deg(x_i) \leqslant P$ $(1 \leqslant i \leqslant s)$.

For each i we write

$$x_i = x_{i0} + x_{i1} t + \dots + x_{iP} t^P,$$

with $x_{ij} \in \mathbb{F}_q$, and likewise we put

$$m = m_0 + m_1 t + \dots + m_{kP} t^{kP}.$$

Here, we adopt the convention that $m_j = 0$ when $j > \deg(m)$. We are at liberty to suppose that $\deg(m)$ is large, whence P is also large enough that $(k-1)(P+1) < \deg(m)$. The condition (17.1) therefore implies that one must have

$$x_{1P}^k + \cdots + x_{sP}^k - m_{kP} = 0$$

(by examining the coefficient of t^{kP}). The number of solutions of this equation is $J_\infty(m)$. Moreover, if $J_\infty(m) = 0$ then the relation (17.1) has no solutions, and hence $I_s(P) = J_\infty(m)(q^P)^{s-k}$ for trivial reasons. So we may suppose that $J_\infty(m) \geq 1$ and hence that $x_{iP} \neq 0$ for some index i. Without loss of generality, we may rearrange variables to suppose that $i = 1$ in the rest of our argument. So we fix a solution $\underline{x}_P$ counted by $J_\infty(m)$, and rearrange indices so that $x_{1P} \neq 0$.

We now work on solving for the remaining variables. We make an arbitrary choice of $x_2(t), \ldots, x_s(t)$ satisfying the condition that $x_{2P}, \ldots, x_{sP}$ take the values already fixed. There are $(q^P)^{s-1}$ such choices. Now we seek to solve

$$\operatorname{ord}\left(x_1^k - \left(m - x_2^k - \cdots - x_s^k\right)\right) < (k-1)(P+1)$$

noting that the right hand side here is fixed, say

$$m - x_2^k - \cdots - x_s^k = y_0 + y_1 t + \cdots + y_{kP} t^{kP}.$$

Owing to our choice of $x_{1P}, \ldots, x_{sP}$, we may assume that $x_{1P}^k = y_{kP}$, and moreover $x_{1P} \neq 0$.

Observe that the multinomial expansion of x_1^k takes the form

$$x_1^k = (x_{1P}t^P + \cdots + x_{11}t + x_{10})^k$$

$$= c_{kP}(x_{1P},\ldots,x_{10})t^{kP} + \cdots + c_1(x_{1P},\ldots,x_{10})t + c_0(x_{1P},\ldots,x_{10}),$$

where $c_\ell(x_{1P},\ldots,x_{10})$ are polynomials in the x_{ij}, having coefficients in $\mathbb{F}_q$, and having the form

$$c_{kP-\ell}(x_{1P},\ldots,x_{10}) = \binom{k}{k-1} x_{1P}^{k-1} x_{1,P-\ell} + d_{kP-\ell}(x_{1P},\ldots,x_{10}), \quad (1 \le \ell < P),$$

in which $d_{kP-\ell}(x_{1P},\ldots,x_{10})$ depends at most on $x_{1,P-\ell+1},\ldots,x_{1P}$. This follows by examining powers of t above. Moreover, the lead coefficient here, namely

$$k\, x_{1P}^{k-1}$$

is non-zero, such that $(\mathbb{F}_q) > k$ and $x_{1P} \neq 0$. Then the equation

$$c_{kP-1}(x_{1P},\ldots,x_{10}) = y_{kP-1}$$

has the solution $x_{1,P-1} = (y_{kP-1}(k x_{1P}^{k-1})^{-1}$ $\underbrace{\quad}_{d_{kP-1}(x_{1P},\ldots,x_0)}$. Fixing this value, the equation

$$c_{kP-2}(x_{1P},\ldots,x_{10}) = y_{kP-2}$$

has the solution $x_{1,P-2} = (y_{kP-2} - \underbrace{d_{kP-2}(x_{1P},\ldots,x_{10})}_{\text{fixed}})(k x_{1P}^{k-1})^{-1}$. We may proceed inductively, solving successively for the values

$$x_{1,P-\ell} = (y_{kP-\ell} - \underbrace{d_{kP-\ell}(x_{1P},\ldots,x_{10})}_{\text{fixed}})(k x_{1P}^{k-1})^{-1}.$$

When $1 \le \ell \le P-k+1$. We have then determined the coefficients of $t^{kP-\ell}$ for $0 \le \ell \le P-k+1$, and exhausted the constraints provided by the relation

$$\operatorname{ord}(x_1^k - (m - x_2^k - \cdots - x_s^k)) < kP - (P-k+1) = (k-1)(P+1).$$

The coefficients $x_{1,P-\ell}$ may be chosen freely when $P-k+2 \le \ell \le P$.

The total number of solutions counted here is

$$\mathfrak{X}(m) = J_\infty(m)\,(q^P)^{s-1}\cdot q^{k-1}$$

$$= J_\infty(m)\,(q^P)^s\cdot q^{k-1-P},$$

and hence

$$I_s(P) = \mathfrak{X}(m)\; q^{-(k-1)(P+1)}$$

$$= J_\infty(m)(q^P)^s\; q^{k-1-P}\cdot q^{-kP}\cdot q^{P-(k-1)}$$

$$= J_\infty(m)\,(q^P)^{s-k}. \quad //$$

On substituting this conclusion into Lemma 16.5, we see that when $s \geqslant 2^k+1$ and $\mathrm{char}(\mathbb{F}_q) > k$, one has

$$\int_{\mathfrak{m}(W)} f(\alpha;P)^s\, e(-n\alpha)\,d\alpha = J_\infty(m)\,\mathfrak{S}(m;W)\,(q^P)^{s-k} + O\big((q^P)^{s-k}(q^W)^{-\frac{k}{2}}\big).$$

It now remains only to analyse the singular series $\mathfrak{S}(m;W)$ and the density $J_\infty(m)$.

In order to compute $J_\infty(m)$, we may again apply exponential sum estimates. Put

$$g(u) = \sum_{a\in\mathbb{F}_q} e_q(ua^k) \qquad (u\in\mathbb{F}_q),$$

and note that with the notation in play, one has

$$J_\infty(m) = \frac{1}{q} \sum_{u \in \mathbb{F}_q} g(u)^s e_q(-bu) - \nu \qquad \text{(where } \nu = 0 \text{ when } b \neq 0, \text{ and } \nu = 1 \text{ when } b = 0\text{)}$$

As a consequence of HW3, Q7, one has

$$|g(u)| \leqslant (k-1) q^{\frac{1}{2}} \qquad (u \neq 0).$$

To see this, one could either run the argument of that question directly, or else just take $\pi = t$. Thus one finds that

$$J_\infty(m) = q^{-1} \cdot \underbrace{q^s}_{u=0} + \left(q^{-1} \cdot \sum_{u \in \mathbb{F}_q^\times} g(u)^s e_q(-bu) \right) - \nu$$

Whence

$$|J_\infty(m) - q^{s-1}| \leqslant q^{-1}(q-1) \cdot ((k-1) q^{1/2})^s + 1$$

$$\leqslant (k-1)^s q^{s/2}.$$

Then provided that

$$q^{s-1} > (k-1)^s q^{s/2},$$

we conclude that $J_\infty(m) \geqslant 1$. In such circumstances, one also has $J_\infty(m) \leqslant 2q^{s-1}$. We may summarise these deliberations in the form of a lemma.

Lemma 17.2. Suppose that $s \geqslant 3$ and $q > (k-1)^4$. Then one has

$$1 \leqslant J_\infty(m) \leqslant 2q^{s-1}.$$

Proof. We have taken a crude approach to obtain a simple-to-state conclusion in summarising our argument above. One could of course take a more precise route. //

We remark that an argument of similar type shows that independently of $\mathrm{char}(\mathbb{F}_q)$, provided that s is sufficiently large, then one also has $1 \le J_\infty(m) \le 2q^{s-1}$. In order to confirm this observation, note that when $u \neq 0$, one has $\mathrm{Tr}(ua^k) \neq 0$ for some $a \in \mathbb{F}_q$. The argument here is similar to that applied above — $\mathrm{Tr}(\xi) = 0$ defines an equation of degree p^{k-1} in ξ (where $q = p^{k-1}$), so has at most q/p solutions. Thus

$$\Big| \sum_{a \in \mathbb{F}_q} e_q(ua^k) \Big| \le |(q-1) + e^{2\pi i/p}|$$

$$\le q - \delta,$$

for a positive number δ. But then one has

$$|J_\infty(m) - q^{s-1}| \le q^{-1}(q-1)(q-\delta)^s + 1$$

$$< q^s (1 - \delta/q)^s + 1$$

$$\le q^s e^{-\delta s/q} + 1.$$

If we take $s > 2\frac{q}{\delta}\log q$, then we find that

$$|J_\infty(m) - q^{s-1}| \le q^s e^{-2\log q} + 1 \le 2q^{s-2},$$

whence

$$1 \le J_\infty(m) \le 2q^{s-1}.$$

§ 18. The singular series.

Now we turn to the analysis of the singular series

$$\mathfrak{S}(m) = \sum_{g \in \mathbb{F}_q[t]^+} \sum_{\substack{0 \le |a| < |g| \\ (a,g)=1}} |g|^{-s} S(g,a)^s e(-ma/g).$$

We begin by noting here that, by virtue of the estimate

$|S(g,a)| \ll |g|^{1-2^{1-k}+\varepsilon}$ provided by Corollary 16.4, one has

$$|\mathfrak{S}(m) - \mathfrak{S}(m;W)| = \Big| \sum_{\substack{g \in \mathbb{F}_q[t]^+ \\ |g| > q^W}} \sum_{\substack{0 \le |a| < |g| \\ (a,g)=1}} |g|^{-s} S(g,a)^s e(-ma/g) \Big|$$

$$\ll \sum_{\substack{g \in \mathbb{F}_q[t]^+ \\ |g| > q^W}} |g| \cdot |g|^{-s2^{1-k}+\varepsilon}.$$

Thus, when $s \ge 2^k + 1$, we find that

$$|\mathfrak{S}(m) - \mathfrak{S}(m;W)| \ll \sum_{\substack{g \in \mathbb{F}_q[t]^+ \\ |g| > q^W}} |g|^{-1-2^{-k}}$$

$$\ll \sum_{d=W+1}^{\infty} q^d \cdot \left(q^{d+1}\right)^{-1-2^{-k}}$$

$$< \sum_{d \ge W+1} q^{-d2^{-k}} \ll \left(q^W\right)^{-2^{-k}}.$$

A similar argument shows that $\mathfrak{S}(m)$ converges absolutely.

Lemma 18.1. Suppose that $\mathrm{char}(\mathbb{F}_q) > k$ and $s \ge 2k+1$. Then the

singular series $\mathfrak{S}(m)$ converges absolutely, one has

$$|\mathfrak{S}(m) - \mathfrak{S}(m;W)| \ll (q^W)^{-4}.$$

Moreover, one has

$$\int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-m\alpha)\,d\alpha = J_\infty(m)\mathfrak{S}(m)(q^P)^{s-4} + O((q^P)^{s-4+\varepsilon}(q^W)^{-2^{-4}}).$$

Proof. We have established the first two ~~statements~~. For the final one, we apply Lemma 16.5 and Lemmata 17.1. Thus,

$$|I_s(P)| \ll (q^P)^{s-4},$$

whence

$$\left|\int_{\mathfrak{m}(W)} f(\alpha;P)^s e(-m\alpha)\,d\alpha - J_\infty(m)\mathfrak{S}(m)(q^P)^{s-4}\right|$$
$$\le |I_s(P)| \cdot |\mathfrak{S}(m;W) - \mathfrak{S}(m)| + O((q^P)^{s-4+\varepsilon}(q^W)^{-2^{-4}})$$
$$\ll (q^P)^{s-4+\varepsilon}(q^W)^{-2^{-4}}. \quad //$$

The analysis of $\mathfrak{S}(m)$ makes use of ~~the~~ arithmetic of $\mathbb{F}_q[t]$. We ~~begin with the~~ quasimultiplicative property of $S(g,a)$.

Lemma 18.2. Suppose that $(a_1,g_1) = (a_2,g_2) = (g_1,g_2) = 1$. Then

$$S(g_1g_2, a_1g_2 + a_2g_1) = S(g_1,a_1)S(g_2,a_2).$$

Proof. Each residue class b modulo g_1g_2 is uniquely represented in the form $u_1g_2 + u_2g_1$ with $|u_1| < |g_1|$ and $|u_2| < |g_2|$. Thus

$$S(g_1g_2, a_1g_2 + a_2g_1) = \sum_{|u_1|<|g_1|} \sum_{|u_2|<|g_2|} e\left(\frac{(a_1g_2 + a_2g_1)(u_1g_2 + u_2g_1)^k}{g_1g_2}\right)$$
$$= \sum_{|u_1|<|g_1|} \sum_{|u_2|<|g_1|} e\left(\frac{a_1(u_1g_2)^k}{g_1} + \frac{a_2(u_2g_1)^k}{g_2}\right)$$

$$= \sum_{|u_1'|<|g_1|} \sum_{|u_2'|<|g_2|} e\left(\frac{a_1(u_1')^k}{g_1}\right) \cdot e\left(\frac{a_2(u_2')^k}{g_2}\right)$$

$$= S(g_1, a_1) S(g_2, a_2). \quad //$$

We may now introduce the function

$$S(g) = \sum_{\substack{|a|<|g| \\ (a,g)=1}} |g|^{-s} S(g,a)^s e(-ma/g),$$

so that

$$\tilde{G}(m) = \sum_{g \in \mathbb{F}_q[t]^+} S(g).$$

Lemma 18.3. The function $S(g)$ is multiplicative.

Proof. Suppose that $(g_1, g_2) = 1$. Then by Lemma 18.2, one has

$$S(g_1 g_2) = \sum_{\substack{|a_1|<|g_1| \\ (a_1,g_1)=1}} \sum_{\substack{|a_2|<|g_2| \\ (a_2,g_2)=1}} |g_1 g_2|^{-s} S(g_1 g_2, a_1 g_2 + a_2 g_1)^s \times e\left(-m(a_1 g_2 + a_2 g_1)/(g_1 g_2)\right),$$

using the Chinese Remainder Theorem in disguise. Thus

$$S(g_1, g_2) = \sum_{\substack{|a_1|<|g_1| \\ (a_1,g_1)=1}} \sum_{\substack{|a_2|<|g_2| \\ (a_2,g_2)=1}} |g_1|^{-s} S(g_1, a_1)^s e(-ma_1/g_1) \times |g_2|^{-s} S(g_2, a_2)^s e(-ma_2/g_2)$$

$$= S(g_1) S(g_2). \quad //$$

For each monic irreducible $\pi \in \mathbb{F}_q[t]$, we now define

$$T(\pi) = \sum_{\ell=0}^{\infty} S(\pi^\ell).$$

Lemma 18.4. Suppose that $s \geq 2^k+1$. Then $T(\pi)$ converges absolutely, so does $\prod_\pi T(\pi)$, and

$$\mathfrak{S}(m) = \prod_\pi T(\pi).$$

Further, there is a positive integer C_0 having the property that

$$\tfrac{1}{2} < \prod_{\deg(\pi) \geq C_0} T(\pi) < 3/2,$$

with C_0 depending at most on s, k and q.

Proof. We have already seen that $|S(\pi^\ell)| \ll |\pi|^{-1-2^{-k}}$, and thus $\sum_{\ell=0}^{\infty} |S(\pi^\ell)|$ converges. So $T(\pi)$ converges absolutely.

Furthermore, one has

$$\sum_\pi \log T(\pi) = \sum_\pi \log\Big(1 + \underbrace{\sum_{\ell \geq 1} S(\pi^\ell)}_{O(|\pi|^{-1-2^{-k}})}\Big),$$

and hence $\prod_\pi T(\pi)$ converges absolutely, because

$$\sum_\pi \Big|\sum_{\ell \geq 1} S(\pi^\ell)\Big| \ll \sum_\pi |\pi|^{-1-2^{-k}}$$

$$\ll \sum_{d=1}^{\infty} \frac{q^d}{d} \cdot (q^d)^{-1-2^{-k}} < \infty.$$

The absolute convergence of $\prod_\pi T(\pi)$ confirms that we may rearrange the terms in the product. Thus, by unique factorisation and the multiplicative property of $S(g)$, one has

$$\prod_\pi T(\pi) = \prod_\pi \sum_{\ell=0}^{\infty} S(\pi^\ell) = \sum_{g \in \mathbb{F}_q[t]} S(g) = \mathfrak{S}(m).$$

Observe next — that our previous estimates show that there is a positive number $c_1 = c_1(s, k, q)$ for which

$$|T(\pi) - 1| \leq c_1 |\pi|^{-1-2^{-k}}.$$

Thus, when $\deg(\pi)$ is sufficiently large, one has

$$|T(\pi) - 1| \leq |\pi|^{-1-2^{-1-k}},$$

Whence there exists $c_0 = c_0(s, k, q)$ such that

$$\left| \prod_{\deg(\pi) \geq c_0} T(\pi) \right| \leq \left| \prod_{\deg(\pi) \geq c_0} (1 + |\pi|^{-1-2^{-1-k}}) \right| < \frac{3}{2}$$

and

$$\left| \prod_{\deg(\pi) \geq c_0} T(\pi) \right| \geq \left| \prod_{\deg(\pi) \geq c_0} (1 - |\pi|^{-1-2^{-1-k}}) \right| > \frac{1}{2}.$$

But $T(\pi)$ is real, since $S(g) = \overline{S(g)}$, by noting that

$$S(g) = \sum_{\substack{|a| < |g| \\ (a,g)=1}} |g|^{-s} S(g,a)^s e(-ma/g) = \sum_{\substack{|a| < |g| \\ (a,g)=1 \\ a \leftrightarrow -a.}} |g|^{-s} S(g,-a)^s e(ma/g)$$

$$= \overline{S(g)}.$$

Hence

$$\frac{1}{2} < \prod_{\deg(\pi) \geq c_0} T(\pi) < \frac{3}{2}.$$

//

We next relate the quantity $T(\pi)$ to a limiting density of the number of solutions of congruences modulo π^h as $h \to \infty$. Define

$$M_s(g,m) = \#\{(x_1,\dots,x_s) \in \mathbb{F}_q[t]^s : \deg(x_i) < \deg(g),\ x_1^k + \dots + x_s^k \equiv m \pmod g\}.$$

Lemma 18.5. One has

$$M_s(g,m) = |g|^{s-1} \sum_{\substack{u \mid g \\ u \text{ monic}}} S(g/u).$$

Proof. By orthogonality, one has

$$M_s(g,m) = |g|^{-1} \sum_{|a|<|g|} \sum_{|x_1|<|g|} \cdots \sum_{|x_s|<|g|} e\left(\frac{a}{g}(x_1^k + \dots + x_s^k - m)\right)$$

$$= |g|^{-1} \sum_{d \mid g} \sum_{\substack{|a_1|<|g_1| \\ (a_1,g_1)=1}} \sum_{|x_1|<|g|} \cdots \sum_{|x_s|<|g|} e\left(\frac{a_1}{g_1}(x_1^k + \dots + x_s^k - m)\right)$$

$\boxed{(a,g)=d}$

$a_1 = a/g,\ g_1 = g/d$

$$= |g|^{-1} \sum_{d \mid g} \sum_{\substack{|a_1|<|g_1| \\ (a_1,g_1)=1}} \left(\frac{|g|}{|g_1|} S(g_1,a_1)\right)^s e(-ma_1/g_1).$$

Thus

$$M_s(g,m) = |g|^{s-1} \sum_{d \mid g} \underbrace{\sum_{\substack{|a_1|<|g_1| \\ (a_1,g_1)=1}} |g_1|^{-s} S(g_1,a_1)^s e(-ma_1/g_1)}_{S(g_1)}.$$

The conclusion here can be rewritten as $M_s(g,m) = |g|^{s-1} \sum_{\substack{u \mid g \\ u \text{ monic}}} S(u)$,

using the duality of divisors.

An important consequence of this conclusion relates $M_s(g,m)$ to $T(\pi)$. Thus, when π is a monic irreducible polynomial, we have

$$\sum_{l=0}^{H} S(\pi^l) = \sum_{\substack{u \mid \pi^H \\ u \text{ monic}}} S(u) = (|\pi^H|^{s-1})^{-1} M_s(\pi^H, m),$$

Whence

$$T(\pi) = \lim_{H\to\infty} \sum_{l=0}^{H} S(\pi^l) = \lim_{H\to\infty} (\pi^H)^{1-s} M_s(\pi^H, m).$$

One might heuristically expect that

$$M_s(\pi^H, m) = \#\{\underline{x} \in \mathbb{A}^s : x_1^k + \cdots + x_s^k \equiv m \pmod{\pi^H},\ |x_i| < |\pi|^H\}$$

should grow roughly like $(\pi^H)^{s-1}$, since by fixing all but one variable, the final one is more or less determined.

Thus we should expect $M_s(\pi^H, m) \asymp |\pi^H|^{s-1}$, and we see that

$$(\pi^H)^{1-s} M_s(\pi^H, m)$$

should remain bounded as $H \to \infty$. In fact, it is implicit in the conclusions of Lemma 18.4 that $(\pi^H)^{1-s} M_s(\pi^H, m) \to 1$ when $h \to \infty$ and $\deg(\pi) \to \infty$.

This justifies the statement that $T(\pi)$ is a π-adic density of solutions of the equation $x_1^k + \cdots + x_s^k = m$.

§19. Associated congruences.

We may now concentrate on the solubility of the congruence

$$x_1^k + \dots + x_s^k \equiv m \pmod{g},$$

with $\deg(x_i) < \deg(g)$, in which $g = \pi^l$ for a given monic irreducible polynomial π. We begin with a special case having the flavour of Hensel's Lemma that facilitates an induction on l.

Lemma 19.1. Suppose that $\mathrm{char}(\mathbb{F}_q) \nmid k$, that π is monic and irreducible, and $\pi \nmid u$. Suppose also that $\nu \in \mathbb{N}$ and

$$y_0^k \equiv u \pmod{\pi^\nu}.$$

Then, whenever $\mu \geqslant \nu$, there exists $y_\mu \in \mathbb{F}_q[t]$ having the property that

$$y_\mu^k \equiv u \pmod{\pi^\mu} \quad \text{and} \quad y_\mu \equiv y_0 \pmod{\pi^\nu}.$$

Proof. We establish the desired conclusion by induction, noting that the case $\nu = \mu$ is trivial on setting $y_\nu = y_0$. Suppose then that the conclusion has already been established when $\mu = m$ with $m \geqslant \nu$. Thus $y_m^k \equiv u \pmod{\pi^m}$ and $y_m \equiv y_0 \pmod{\pi^\nu}$. Define w via the relation

$$y_m^k = u + w\pi^m,$$

and take z to be a variable, putting $y_{m+1} = y_m + z\pi^m$. Then we have

$$y_{m+1}^k = y_m^k + k(z\pi^m)y_m^{k-1} + \binom{k}{2}(z\pi^m)^2 y_m^{k-2} + \dots$$

$$\equiv (u + w\pi^m) + kzy_m^{k-1}\pi^m \pmod{\pi^{m+1}}.$$

Then we have $y_{m+1}^k \equiv u \pmod{\pi^{m+1}}$ provided that we choose z with

$$k y_m^{k-1} \cdot z \equiv -w \pmod{\pi}.$$

Notice that $k \neq 0$ in $\mathbb{F}_q$ and $(\pi, y_m) = 1$ (since $\pi \nmid u$ and $y_m^k \equiv u \pmod{\pi^m}$). Then the element $k y_m^{k-1}$ has a multiplicative inverse $(k y_m^{k-1})^{-1}$ modulo π, and we have

$$z \equiv -w (k y_m^{k-1})^{-1} \pmod{\pi}.$$

Take z_m to be any element of $\mathbb{F}_q[t]$ with $z_m \equiv -w(k y_m^{k-1})^{-1} \pmod{\pi}$.

Then put $y_{m+1} = y_m + z_m \pi^m$, and we have

$$y_{m+1}^k \equiv u \pmod{\pi^{m+1}} \quad \text{and} \quad y_{m+1} \equiv y_m \pmod{\pi^m}$$
$$\equiv y_0 \pmod{\pi^r}.$$

This shows that the desired conclusion holds with $\mu = m+1$, and so the conclusion of the lemma follows by induction. //

One can apply Lemma 19.1 to obtain a lower bound for $M_s(\pi^h, u)$ by fixing $s-1$ variables, and solving for the final variable.

Lemma 19.2. Suppose that $\mathrm{char}(\mathbb{F}_q) \nmid k$ and that π is monic and irreducible. Suppose also that $\nu \in \mathbb{N}$ and

$$v_1^k + \dots + v_s^k \equiv m \pmod{\pi^\nu},$$

for some polynomials $v_i \in \mathbb{F}_q[t]$ with $|v_i| < |\pi|^\nu$ and $\pi \nmid v_1$.

Then whenever $\mu \geq \nu$, the number T_μ of s-tuples $(w_1, \dots, w_s) \in \mathbb{F}_q[t]^s$ with

$|w_i| < |\pi^\mu|$, and $w_i \equiv v_i \pmod{\pi^\nu}$ $(1 \le i \le s)$,

and satisfying

$$w_1^k + \dots + w_s^k \equiv m \pmod{\pi^\mu},$$

has the property that

$$T_\mu \geqslant |\pi|^{(\mu-\nu)(s-1)}.$$

Proof. We put $w_i = v_i + z_i \pi^\nu$ with $|z_i| < |\pi|^{\mu-\nu}$, so that $|w_i| < |\pi|^\mu$, for $1 \le i \le s$. We then seek to solve the congruence

$$w_1^k \equiv m - w_2^k - \dots - w_s^k \pmod{\pi^\mu}. \qquad (19.1)$$

Fixing $z_2, \dots, z_s$, we see that there are $|\pi|^{(\mu-\nu)(s-1)}$ choices for the right hand side here, in each of which one has

$$\begin{aligned} w_1^k &\equiv m - w_2^k - \dots - w_s^k \pmod{\pi^\nu} \\ &\equiv m - v_2^k - \dots - v_s^k \pmod{\pi^\nu} \\ &\equiv v_1^k \pmod{\pi^\nu}. \end{aligned}$$

Moreover, one has $\pi \nmid v_1$, so $\pi \nmid v_1^k$. We therefore see from Lemma 19.1 that a solution w_1 exists to the congruence (19.1), since such a solution exists for each fixed choice of $w_2, \dots, w_s$, we see that

$$T_\mu \geq |\pi|^{(\mu-\nu)(s-1)}. \qquad //$$

We have reduced the problem of obtaining a lower bound for $M_s(\Pi^l, m)$ to that of bounding $M_s(\pi, m)$ from below, since we have (not quite!) a lower bound of the shape

$$M_s(\pi^l, m) \geqslant |\pi|^{(l-1)(s-1)} M_s^*(\pi, m).$$

Here the asterisk indicates that we should restrict a variable to be coprime with π.

Lemma 19.3. Suppose that π is monic and irreducible, $s \geqslant k+1$, and m is congruent modulo π to a (finite) sum of k-th powers. Then there exist $w_1, \dots, w_s \in \mathbb{F}_q[t]$ with $|w_i| < |\pi|$, and such that $\pi \nmid w_1$, having the property that

$$w_1^k + \cdots + w_s^k \equiv m \pmod{\pi}. \qquad (19.2)$$

Proof. If $\pi \mid m$, then we put $w_s = 1$ and consider the congruence

$$w_1^k + \cdots + w_{s-1}^k \equiv m-1 \pmod{\pi},$$

with $\pi \nmid (m-1)$ and $s-1 \geqslant k$. Thus, we may suppose in (19.2) that $\pi \nmid m$ and $s \geqslant k$.

Let $t = t(m)$ be the least natural number having the property that

$$w_1^k + \cdots + w_t^k \equiv m \pmod{\pi} \qquad (19.3)$$

is soluble. We define an equivalence relation on polynomials $m \in \mathbb{F}_q[t]$ with $\pi \nmid m$, by declaring $m_1 \sim m_2$ if and only if $t(m_1) = t(m_2)$. We now consider the number of equivalence classes of such polynomials. Note that when $\pi \nmid v$, then $t(m) = t(mv^k)$. For given a representation (19.3), we have

$$(vw_1)^k + \cdots + (vw_t)^k \equiv mv^k \pmod{\pi},$$

so $t(mv^k) \leqslant t(m)$. Meanwhile, if

$$w_1^k + \cdots + w_t^k \equiv mv^k \pmod{\pi},$$

then

$$(v^{-1}w_1)^k + \cdots + (v^{-1}w_t)^k \equiv m \pmod{\pi},$$

so that $t(m) \leqslant t(mv^k)$. Hence, indeed, one has $t(m) = t(mv^k)$.

But the number of distinct choices for $v^k \pmod{\pi}$ with $\pi \nmid v$ is $\dfrac{|\pi|-1}{(k, |\pi|-1)}$, so that each equivalence class contains at least $\dfrac{|\pi|-1}{(k, |\pi|-1)}$ distinct polynomials. Thus, the number of equivalence classes can be at most $(k, |\pi|-1) \le k$.

We claim that the values $\{t(m): m \in \mathbb{F}_q[t] \text{ and } \pi \nmid m\}$ form a set of consecutive integers. To see this, consider any polynomial m_0 with $t(m_0) = \max\{t(m): m \in \mathbb{F}_q[t] \text{ and } \pi \nmid m\}$. Let $l = t(m_0)$, so that for some polynomials $w_1, \dots, w_{l_0} \in \mathbb{F}_q[t]$, one has

$$w_1^k + \dots + w_{l_0}^k \equiv m_0 \pmod{\pi}.$$

The polynomial $m_0 - w_{l_0}^k$ cannot be represented as the sum of fewer than $l_0 - 1$ k-th powers modulo π, for this would contradict our hypothesis that $t(m_0) = l_0$. Hence $t(m_0 - w_{l_0}^k) = l_0 - 1$. Similarly, one has $t(m_0 - w_{l_0}^k - w_{l_0-1}^k) = l_0 - 2$, and so on. So we find that

$$\{t(m): m \in \mathbb{F}_q[t] \text{ and } \pi \nmid m\} = \{1, 2, \dots, l_0\}.$$

Since there are at most k equivalence classes, it follows that $l_0 \le k$, and the conclusion of the lemma follows. //

The conclusion of Lemma 19.3 shows that when $m \in \mathbb{F}_q^k[t]$, so that there is no obstruction to the solubility of (19.2) arising from congruences modulo π, then for each monic irreducible π there is a solution of (19.2) whenever $s \ge k+1$. Moreover, such a solution exists

with $\pi \nmid w_1$. But then we may apply Lemma 19.2 to see that

$$M_s(\pi^H, m) \geq |\pi|^{(H-1)(s-1)} \cdot 1,$$

whence

$$T(\pi) = \lim_{H \to \infty} (\pi^H)^{1-s} M_s(\pi^H, m) \geq |\pi|^{1-s}.$$

It follows that

$$\mathfrak{S}(m) = \prod_{\pi} T(\pi) \gg \prod_{\deg(\pi) \geq C_0} T(\pi) > \tfrac{1}{2}.$$

We can say something more definitive concerning the structure of $\mathbb{F}_q^k[t]$ modulo π when $\operatorname{char}(\mathbb{F}_q) > k$.

Lemma 19.4. Suppose that π is monic and irreducible with $\operatorname{char}(\mathbb{F}_q) > k$. Then for all $m \in \mathbb{F}_q[t]$, for some $n \in \mathbb{N}$ one has that there exist $w_1, \dots, w_n \in \mathbb{F}_q[t]$ for which $w_1^k + \dots + w_n^k \equiv m \pmod{\pi}$.

Proof. We use the structure of the ring $\mathbb{A}/\pi\mathbb{A}$ (where $\mathbb{A} = \mathbb{F}_q[t]$). Since π is irreducible, we find that $\mathbb{A}/\pi\mathbb{A}$ has the structure of a field, with $\mathbb{A}/\pi\mathbb{A} \cong \mathbb{F}_{q^d}$, with $d = \deg(\pi)$. Thus, if $q = p^h$, we have $\mathbb{A}/\pi\mathbb{A} \cong \mathbb{F}_{p^{dh}}$.

Now consider the ring

$$R = \{ x_1^k + \dots + x_\ell^k \pmod{\pi} : x_i \in \mathbb{F}_q[t], \ \ell \in \mathbb{N} \cup \{0\} \}.$$

The ring $R \subseteq \mathbb{F}_q[t]/(\pi\mathbb{F}_q[t])$ is closed under addition and multiplication, so forms a subring of $\mathbb{F}_q[t]/\pi\mathbb{F}_q[t]$. Thus $|R| \mid |\mathbb{A}/\pi\mathbb{A}|$, whence $|R| \mid p^{dh}$. So $|R| = p^r$, say, with $r \leq dh$. It follows that since $|R^\times|$ divides $|(\mathbb{A}/\pi\mathbb{A})^\times|$ also, then

$$(p^r - 1) \mid (p^{dh} - 1).$$

Finally, we observe that when g is a primitive root in $(A/\pi A)^\times$, then $g^k \in R$, whence

$$1 \equiv (g^k)^{|R|-1} \equiv (g^k)^{p^r - 1} \pmod{\pi},$$

so that $(p^{dh} - 1) \mid k(p^r - 1)$. But then, if R is a proper subring of $(A/\pi A)$, we have $r < dh$ and

$$p^{dh} - 1 \leq k(p^r - 1) < p(p^r - 1) \leq p^{dh} - p \quad \#.$$

$\operatorname{char}(\mathbb{F}_q) > k$

So we are forced to conclude that R is not a proper subring of $A/\pi A$, whence every polynomial $m \in \mathbb{F}_q[t]$ is a sum of k-th powers of elements of $\mathbb{F}_q[t]$. //

By combining the conclusions of Lemmata 19.3 and 19.4, we see that when $\operatorname{char}(\mathbb{F}_q) > k$ and $s \geq k+1$, then there exist $w_1, \dots, w_s \in \mathbb{F}_q[t]$ with $|w_i| < |\pi|$ and $\pi \nmid w_1$, such that

$$w_1^k + \cdots + w_s^k \equiv m \pmod{\pi}.$$

It then follows from Lemma 19.2 that

$$M_s(\pi^\mu, m) \geq T_\mu \geqslant |\pi|^{(\mu-1)(s-1)} \qquad (\mu \geq 1),$$

whence

$$T(|\pi|) = \lim_{H \to \infty} (\pi^H)^{1-s} M_s(\pi^H, m) \geqslant |\pi|^{1-s} \geqslant q^{(1-s)\deg(\pi)}.$$

Thus, as previously discussed, we conclude that

$$\mathfrak{S}(m) = \prod_{\pi} T(\pi) \geq \frac{1}{2} \prod_{\deg(\pi) \leq C_0(s,k,q)} q^{(1-s)\deg(\pi)} \gg_{s,k,q} 1 .$$

This is the last piece in the preparation for the proof of our asymptotic formula for

$$R(m) = \#\{(x_1,\dots,x_s) \in \mathbb{F}_q[t]^s : \deg(x_i) \leq P \text{ and } x_1^k + \dots + x_s^k = m\}.$$

We have

$$R(m) = \int_{\mathcal{T}} f(\alpha;P)^s e(-m\alpha)\,d\alpha$$

$$= \underbrace{\int_{\mathcal{M}} f(\alpha;P)^s e(-m\alpha)\,d\alpha}_{\text{Lemma 16.5}} + \underbrace{\int_{\mathfrak{m}} f(\alpha;P)^s e(-m\alpha)\,d\alpha}_{\text{Lemma 14.3}}$$

$$= I_s(P)\mathfrak{S}(m;W) + O\left((q^P)^{s-k+\varepsilon}(q^W)^{-2^{-k}}\right) \qquad (q^P)^{s-k+\varepsilon}(q^W)^{-2^{1-k}}$$

when $s \geq 2^k+1$ and $\mathrm{char}(\mathbb{F}_q) > k$ — when $s \geq 2^k+1$ and $\mathrm{char}(\mathbb{F}_q) > k$

$$= I_s(P)\mathfrak{S}(m;W) + O\left((q^P)^{s-k+\varepsilon}(q^W)^{-2^{-k}}\right).$$

$$= \underbrace{J_\infty(m)(q^P)^{s-k}}_{\text{Lemma 17.1}} \left(\underbrace{\mathfrak{S}(m) + O((q^W)^{-2^{-k}})}_{\text{Lemma 18.1}}\right) + O\left((q^P)^{s-k+\varepsilon}(q^W)^{-2^{-k}}\right)$$

$$= J_\infty(m)\mathfrak{S}(m)(q^P)^{s-k} + O\left((q^P)^{s-k-2^{-2-k}}\right)$$

when $W = \lfloor P/2 \rfloor$,

We have shown that whenever $m \in \mathbb{F}_q^k[t]$, then (when $s \geq 2^k+1$ and $\mathrm{char}(\mathbb{F}_q) > k$) one has $\mathfrak{S}(m) \gg 1$. Also, provided that $s \geq 3$ and

$q > (k-1)^4$, we have $J_\infty(m) \geq 1$. Moreover, such also holds

when $s > \frac{2q}{\delta} \log q$ (since $\delta = 1 - \cos(2\pi/p) \geq 1(1 - 4/p) = 4/p$.)

so if $q \leq (k-1)^4$, then this latter condition holds for

$$s > \frac{2q}{4/p} \log q \text{ , with } \frac{2q}{4/p} \log q \leq q^3 \leq (k-1)^{12}.$$

Then we may conclude that

$$R(m) \gg (q^p)^{s-k}$$

whenever $s \geqslant \max\{2^k + 1, (k-1)^{12}\}$.

§20. Generalisations and refinements.

In this section we explore the scope for generalisations and refinements of the Waring's problem treatment of §§13–19. What was shown in these sections is that when $\deg(m)$ is sufficiently large, then

$$R(m) = \#\{w_1^k + \cdots + w_s^k = m : \deg(w_i) \leq P\}$$

$$\sim \mathfrak{S}(m) J_\infty(m) (q^P)^{s-k} + o((q^P)^{s-k}),$$

valid when $s \geq 2^k + 1$ and $\mathrm{char}(\mathbb{F}_q) > k$. We discuss (without proof) what can be said about this asymptotic formula for smaller values of s, and with the constraint on the characteristic relaxed.

(a) Reducing the required number of variables.

The bound $G_q(k) \leq 2^k + 1$ is analogous to the classical bound $G(k) \leq 2^k + 1$ in the analogous theory over the integers. To improve this bound, one must replace the use of Weyl differencing by more efficient tools.

Vinogradov's mean value theorem: (Classical version — I.M. Vinogradov, 1935).

Theorem 20.1 (W., 2019) When $\mathrm{char}(\mathbb{F}_q) > k$, one has

$$\int_{\mathbb{T}} |f(\alpha; P)|^{2s} \, d\alpha \ll (q^P)^{2s - k + \varepsilon},$$

provided only that $s \geq k(k+1)/2$.

This represents a significant improvement on Hua's Lemma, which would give an analogous conclusion with $s = 2^{k-1}$ (superior for $k \geq 5$).

Corollary One has $G_q(k) \leq k^2 + k + 1$ when $\mathrm{char}(\mathbb{F}_q) > k$.

The underlying idea is to consider a system of equations superficially more complicated than that underlying Hua's lemma, which depends on

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k,$$

with $|x_i|, |y_i| \leq q^P$.

Instead, let $J_{s,k}(P)$ denote the number of solutions of the system

$$\left.\begin{aligned} x_1^k + \cdots + x_s^k &= y_1^k + \cdots + y_s^k \\ x_1^{k-1} + \cdots + x_s^{k-1} &= y_1^{k-1} + \cdots + y_s^{k-1} \\ &\vdots \\ x_1 + \cdots + x_s &= y_1 + \cdots + y_s \end{aligned}\right\} \quad \text{with} \quad |x_i|, |y_i| \leq q^P.$$

Then, by orthogonality, one has

$$J_{s,k}(P) = \int_{\mathbb{T}^k} \Big| \underbrace{\sum_{|x| \leq q^P} e(\alpha_1 x + \cdots + \alpha_k x^k)}_{f_k(\underline{\alpha}; P)} \Big|^{2s} d\alpha_1 \cdots d\alpha_k.$$

As a consequence of the nested efficient congruencing method (W., 2019), one has:

Theorem 2.2 (W. 2019). When $\mathrm{char}(\mathbb{F}_q) > k$, one has

$$\int_{\mathbb{T}^k} |f_k(\underline{\alpha}; P)|^{2s} d\underline{\alpha} \ll (q^P)^{2s - \frac{1}{2}k(k+1) + \varepsilon} + (q^P)^s.$$

The significance of the term $\frac{1}{2}k(k+1)$ in the exponent is that the sum of the degrees in this system of equations is $1 + 2 + \cdots + k = \frac{1}{2}k(k+1)$. The first theorem that we recorded is a direct consequence of this stronger statement.

Further refinement is possible by restricting variables further, which

loses the asymptotic formula for $R(m)$, replacing it with a corresponding lower bound.

In order to describe this kind of result, let the base p expansion of k be

$$k = a_0 + a_1 p + \cdots + a_n p^n,$$

say, where $0 \le a_i \le p-1$ $(0 \le i \le n)$ and $a_n \neq 0$. Then put

$$\gamma_q(k) = a_0 + a_1 + \cdots + a_n,$$

and

$$A_q(k) = \begin{cases} 1, & \text{when } \operatorname{char}(\mathbb{F}_q) > k, \\ (1 - 2^{-\gamma_q(k)})^{-1}, & \text{when } \operatorname{char}(\mathbb{F}_q) < k. \end{cases}$$

Finally, put

$$\hat{G}_q(k) = Ak(\log k + \log\log k + 2 + A\log\log k / \log k),$$

where

$$A = A_q(k).$$

(Y.-R. Liu & W., 2010)

Theorem 20.3. There is a constant C_1 (absolute) such that whenever k and q are natural numbers with $\operatorname{char}(\mathbb{F}_q) \nmid k$, then

$$G_q(k) \le \hat{G}_q(k) + C_1 k \sqrt{\log\log k} / \log k.$$

When $\operatorname{char}(\mathbb{F}_q) \mid k$, meanwhile, one has $G_q(k) = G_q(k/\operatorname{char}(\mathbb{F}_q))$.

Notice that one has $1 \le A \le 4/3$ for all $k > 1$ with $\operatorname{char}(\mathbb{F}_q) \nmid k$, because $\gamma_q(k) \ge 2$ whenever $p \nmid k$. Thus, independently of the characteristic of $\mathbb{F}_q$, one obtains a bound for $G_q(k)$ roughly

$$G_q(k) \lesssim 4/3\, k \log k.$$

This work shows that

$$R(m) \gg \mathfrak{S}(m) J_\infty(m) (q^P)^{s-k} \quad \text{when} \quad s \ge Ak(\log k + \cdots).$$

A key role is played by the set of "smooth" polynomials

$$\mathcal{A}(P,R) = \{ x \in \mathbb{F}_q[t] : |x| \le q^P \text{ and } \pi | x \Rightarrow |\pi| \le q^R \},$$

in which $R = \lfloor \eta P \rfloor$ with η a very small positive number. In such circumstances, it transpires that there is a positive number $c = c(\eta)$ having the property that

$$\operatorname{card}(\mathcal{A}(P,R)) = c(\eta) q^P + O(q^P / \log R),$$

as $P \to \infty$. Thus, the set $\mathcal{A}(P,R)$ has positive density amongst all polynomials of degree at most P. Using the efficient differencing machinery, one shows that when $r \in \mathbb{N}$, one has a mean value of the shape

$$\int_0^1 \Big| \sum_{x \in \mathcal{A}(P,R)} e(\alpha x^k) \Big|^{2r} d\alpha \ll (q^P)^{\lambda_r + \varepsilon},$$

when $\eta > 0$ is small enough in terms of ε, where

$$\lambda_r \le 2r - k + k e^{-(2-2^{1-r}) r/k}.$$

↑ exponential decay.

This mean value serves as a substitute for Hua's lemma. One then has the task of obtaining analogues of Weyl's inequality, and the treatment of the major arcs, in this new setting.

Notice, in particular, that the use of smooth numbers allows for useful conclusions without the constraint $\operatorname{char}(\mathbb{F}_q) > k$!

(b) Removing (as far as possible) the constraint $\dim(\mathbb{F}_q) > k$.

We have noted already in Theorem 20.3 that one can work subject to the constraint $\dim(\mathbb{F}_q) \neq k$, but this idea of using smooth polynomials does not deliver an asymptotic formula for $R(m)$. To obtain an asymptotic formula, one can instead resort to using variants once more of Vinogradov's mean value theorem. This has been all worked out in forthcoming work of Yu-Ru Liu & W. To illustrate ideas, we consider $G_8(13)$ (13^{th}-powers over $\mathbb{F}_8[t]$). The key idea is that we wish to obtain a translation-invariant system analogous to Vinogradov's system

$$\sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \quad (1 \leq j \leq k), \qquad (20.1)$$

relevant for $k = 13$. Here, when we consider the shift

$$x \longmapsto x + a,$$

a binomial expansion of $(x+a)^j$ reveals that the equations (20.1) remain valid with x_i replaced by $x_i + a$, y_i replaced by $y_i + a$.

Now, thanks to the homework exercise concerning non-vanishing of $\binom{k}{j}$ in characteristic p, we find that $\binom{13}{j}$ is non-vanishing in characteristic 2 precisely when

$$j = 13 = 2^3 + 2^2 + 1,$$

and $j = 2^3 + 2^2,\ 2^3 + 1,\ 2^3,\ 2^2 + 1,\ 2^2,\ 1,$

which is to say when

$$j \in \{13, 12, 9, 8, 5, 4, 1\} = J, \text{ say}.$$

Thus the system

$$\sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \qquad (j \in J)$$

has the necessary translation-invariance properties.

But if $2|j$, then

$$x_1^j + \cdots + x_s^j = (x_1^{j/2} + \cdots + x_s^{j/2})^2,$$

and thus the equation indexed by j holds if and only if the equation indexed by $j/2$ holds. Thus the equations of degree 8, 4 are equivalent to that of degree 1, and that of degree 12 is equivalent to one of degree 3. So we may replace J by

$$J' = \{13, 9, 5, 3, 1\}$$

One can show

$$\#\left\{ x, y \in A^s : |x_i|, |y_i| \le q^P \text{ and } \sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \quad (j \in J') \right\}$$

$$\ll (q^P)^{2s - (13+9+5+3+1)} + (q^P)^{s+\varepsilon}.$$

This yields an asymptotic formula for $R(m)$ in this situation when the number of variables is

$$\ge 2(13+9+5+3+1)+1 = 63,$$

in this situation of degree 13.

§21. Another application : solubility of diagonal equations.

As a consequence of the Lang - Tsen theorem (see Corollary 2.8), we know that whenever $k \in \mathbb{N}$ and $s > k^2$, then for any fixed coefficients $a_i \in \mathbb{F}_q(t)$ $(1 \le i \le s)$, the equation

$$a_1 x_1^k + \cdots + a_s x_s^k = 0 \qquad (21.1)$$

has a solution $\underline{x} \in \mathbb{F}_q[t]^s \setminus \{\underline{0}\}$. By clearing denominators of the a_i, of course, it is always possible to assume that in fact $a_i \in \mathbb{F}_q[t]$. This conclusion gives no quantitative information concerning the number of solutions — the circle method permits such quantitative results to be established.

Let $N_s(B; \underline{a})$ denote the number of solutions of the equation (1.1) with $\underline{x} \in \mathbb{F}_q[t]^s$ and $\operatorname{ord} x_i \le B$ $(1 \le i \le s)$.

Theorem 21.1. Let k and q be natural numbers with $\operatorname{char}(\mathbb{F}_q) > k$. Let $s > 2^k$ and $\underline{a} \in (\mathbb{F}_q[t] \setminus \{0\})^s$. Then one has

$$N_s(B; \underline{a}) \gg (q^B)^{s-k}.$$

Indeed, there is an asymptotic formula of the shape

$$N_s(B; \underline{a}) \sim \mathfrak{C}_{s,k}(\underline{a}) (q^B)^{s-k},$$

in which $\mathfrak{C}_{s,k}(\underline{a})$ is a product of local densities.

We sketch how to prove this result. First, define

$$f_i(\alpha; B) = \sum_{1 \le |x| \le q^B} e(a_i \alpha x^k),$$

Thus, with $f(\alpha; B) = \sum_{1 \le |x| \le q^B} e(\alpha x^k)$,

one has

$$f_i(\alpha; B) = f(a_i \alpha; B).$$

Then, by orthogonality, one has

$$N_s(B; \underline{a}) = \int_{\mathbb{T}} f_1(\alpha; B) \cdots f_s(\alpha; B)\, d\alpha.$$

We apply the Hardy–Littlewood method, taking $\mathfrak{M}(W)$ to be the union of the sets

$$\mathfrak{M}(g, a; W) = \{ \alpha \in \mathbb{K}_\infty : |g\alpha - a| < q^W (q^B)^{-k} \},$$

with

$$a, g \in \mathbb{F}_q[t],\ g \text{ monic},\ 0 \leq |a| < |g| \leq q^W \text{ and } (a, g) = 1.$$

We then put $\mathfrak{m}(W) = \mathbb{T} \setminus \mathfrak{M}(W)$.

A simple exercise shows that, whenever B is large enough in terms of $\operatorname{ord}(a_i)$, then whenever τ is a small positive number, then

$$a_i \alpha \in \mathfrak{M}(W - \tau B) \Rightarrow \alpha \in \mathfrak{M}(W - \tau B + \operatorname{ord} a_i) \subseteq \mathfrak{M}(W).$$

Thus, whenever $\alpha \in \mathfrak{m}(W)$, one has $a_i \alpha \in \mathfrak{m}(W - \tau B)$. On taking $W = \lfloor \frac{1}{2} B \rfloor$, we therefore deduce that

$$\begin{aligned} \sup_{\alpha \in \mathfrak{m}(W)} |f_i(\alpha)| &= \sup_{\alpha \in \mathfrak{m}(W)} |f(a_i \alpha; B)| \\ &\leq \sup_{\beta \in \mathfrak{m}(W - \tau B)} |f(\beta; B)| \\ &\ll (q^B)^{1+\varepsilon} \left(q^{W - \tau B} \right)^{-2^{1-k}} \\ &\ll (q^B)^{1 - 2^{-1-k}}. \end{aligned}$$

On the other hand, by Hua's Lemma, one finds that

$$\int_{\mathfrak{m}} |f_i(\alpha;B)|^{2^k}\,d\alpha = \#\Big\{\sum_{j=1}^{2^{k-1}} a_i(x_j^k - y_j^k) = 0 : |x_j|,|y_j| \le q^B\Big\}$$

$$= \#\Big\{\sum_{j=1}^{2^{k-1}} (x_j^k - y_j^k) = 0 : |x_j|,|y_j| \le q^B\Big\}$$

$$= \int_{\mathfrak{m}} |f(\alpha;B)|^{2^k}\,d\alpha \ll (q^B)^{2^k - k + \varepsilon}.$$

Thus, by Hölder's inequality, one has

$$\int_{\mathfrak{m}(W)} f_1(\alpha;B)\cdots f_s(\alpha;B)\,d\alpha \ll \prod_{i=1}^{s}\Big(\int_{\mathfrak{m}(W)} |f_i(\alpha;B)|^s\,d\alpha\Big)^{\frac{1}{s}}.$$

Here, one has

$$\int_{\mathfrak{m}(W)} |f_i(\alpha;B)|^s\,d\alpha \le \Big(\sup_{\alpha\in\mathfrak{m}(W)} |f_i(\alpha;B)|\Big)^{s-2^k} \int_{\mathfrak{m}} |f_i(\alpha;B)|^{2^k}\,d\alpha$$

$$\ll (q^B)^{(1-2^{-1-k})(s-2^k)} \cdot (q^B)^{2^k-k+\varepsilon}$$

$$\ll (q^B)^{s-k-2^{-2-k}}.$$

It remains to handle the major arcs $\mathfrak{M}(W)$. Let $A = \max_i \operatorname{ord}(a_i)$. Then it follows as in Lemma 15.1 that when $\alpha = a/g + \beta$ with $0 \le |a| < |g| \le q^B$, g monic and $|\beta| < |g|^{-1}(q^B)^{1-k}q^{-A}$, then

$$f(a;\alpha;B) = |g|^{-1} S(g,a;a) f(a;\beta;B).$$

Then

$$\int_{\mathfrak{m}(W)} f_1(\alpha;B)\cdots f_s(\alpha;B)\,d\alpha = \sum_{\substack{1\le|g|\le q^W \\ g \text{ monic}}} \sum_{\substack{0\le|a|<|g| \\ (a,g)=1}} \int_{|\beta|<|g|^{-1}q^W(q^B)^{-k}} \prod_{i=1}^{s} f_i(\beta + a/g;B)^s\,d\beta.$$

The truncation error in the integral is easily handled, and one arrives at the relation

$$\int_{\mathfrak{M}(W)} \prod_{i=1}^{s} f_i(\alpha;B)\,d\alpha = I_s(B;\underline{a})\mathfrak{S}(\underline{a};W) + O\big((q^B)^{s-k+\varepsilon}(q^W)^{-2^{-k}}\big),$$

where

$$I_s(B;\underline{a}) = \int_{|\beta| < (q^{B+1})^{1-k}} \prod_{i=1}^{s} f_i(\beta;B)\, d\beta$$

and

$$\mathfrak{S}(\underline{a};W) = \sum_{\substack{1 \le |g| \le q^W \\ g \text{ monic}}} \sum_{\substack{0 \le |a| < |g| \\ (a,g)=1}} |g|^{-s} \prod_{i=1}^{s} S(g,a;a_i).$$

The treatment of the singular integral follows that of §17. Thus, we find that

$$I_s(B;\underline{a}) = (q^{B+1})^{1-k} \#\{ \operatorname{ord}(a_1 x_1^k + \dots + a_s x_s^k) \le (k-1)(B+1) : \operatorname{ord}(x_i) \le B \}$$

But when $s > k^2$, the equation $a_1 x_1^k + \dots + a_s x_s^k = 0$ has a solution $\underline{x} \in \mathbb{F}_q[t]^s \setminus \{\underline{0}\}$, and so one finds that $I_s(B;\underline{a})$ converges with $(q^B)^{s-k} \ll I_s(B;\underline{a}) \ll (q^B)^{s-k}$. In fact, one again obtains an asymptotic formula of the shape $I_s(B;\underline{a}) = J_\infty(\underline{a})(q^B)^{s-k}$, but now $J_\infty(\underline{a})$ does not depend only on the equation of the shape $a_1 y_1^k + \dots + a_s y_s^k = 0$ with $y \in \mathbb{F}_q^s$.

The treatment of the singular series follows that of §18. We find that

$$|\mathfrak{S}(\underline{a};W) - \mathfrak{S}(\underline{a})| \ll (q^W)^{-2^{1-k}},$$

where

$$\mathfrak{S}(\underline{a}) = \sum_{g \in \mathbb{F}_q[t]^+} \sum_{\substack{0 \le |a| < |g| \\ (a,g)=1}} |g|^{-s} \prod_{i=1}^{s} S(g;a;a_i).$$

One sees that when $(a,g)=1$, one has

$$|S(g;a;a_i)| \ll |g|^{1-2^{1-k}+\varepsilon} |a_i|^{2^{1-k}},$$

and thus when $s > 2^4$, the singular series converges absolutely and one obtains

$$\mathfrak{S}(\underline{a}) = \prod_{\pi} T(\underline{a}; \pi),$$

where

$$T(\underline{a}; \pi) = \sum_{l=0}^{\infty} \sum_{\substack{|a| < |\pi|^l \\ (a,\pi)=1}} |\pi^l|^{-s} \prod_{i=1}^{s} S(\pi^l, a_i a)$$

$$= \lim_{H \to \infty} (|\pi|^H)^{1-s} M_s(\pi^H; \underline{a}),$$

where

$$M_s(\pi^H; \underline{a}) = \#\{ \underline{x} \in \mathbb{A}^s : a_1 x_1^4 + \cdots + a_s x_s^4 \equiv 0 \pmod{\pi^H}, \ |x_i| < |\pi|^H \}.$$

Again, we find that when $s > 2^4$, one has

$$|T(\underline{a}; \pi) - 1| \ll |\pi|^{-1-2^{-2}},$$

when $\deg(\pi)$ is large enough. Meanwhile, a Hensel's lemma argument shows that when $a_1 v_1^4 + \cdots + a_s v_s^4 \equiv 0 \pmod{\pi^\nu}$, then

$$T_\mu(\underline{a}) = \#\{ (w_1, \ldots, w_s) \in \mathbb{F}_q[t]^s : |w_i| < |\pi|^\mu \text{ and } w_i \equiv v_i \pmod{\pi^\nu} \text{ and } a_1 w_1^4 + \cdots + a_s w_s^4 \equiv 0 \pmod{\pi^\mu} \}$$

has the property $T_\mu(\underline{a}) \geq |\pi|^{(\mu-\nu)(s-1)}$.

Since $a_1 x_1^4 + \cdots + a_s x_s^4 \equiv 0 \pmod{\pi^\nu}$ has a solution with $(x_i, \pi) = 1$ for some i, as a consequence of the Lang-Tsen theorem (guaranteeing a solution of $a_1 x_1^4 + \cdots + a_s x_s^4 = 0$), we find

that $M_s(\pi^H; \underline{a}) \gg T_\mu(\underline{a}) \gg |\pi|^{(\mu - r)(s-1)}$ for a suitable $r \geq 1$,

Whence

$$T(\underline{a}; \pi) = \lim_{H \to \infty} (\pi^\#)^{1-s} M_s(\pi^H; \underline{a}) \gg |\pi|^{-r(s-1)}$$

$$\gg q^{r(1-s)\deg(\pi)}.$$

Hence $\mathfrak{S}(\underline{a}) \gg_{s,k,a,q} 1$. We thus deduce that

$$\int_{m(W)} \prod_{i=1}^{s} f_i(\underline{\alpha})\, d\underline{\alpha} = I_s(B; \underline{a})\mathfrak{S}(\underline{a}) + O((q^B)^{s-4-2^{-2-4}})$$

$$\gg (q^B)^{s-k}.$$

Consequently,

$$\#\{a_1 x_1^4 + \cdots + a_s x_s^4 = 0 : |x_i| \leq q^B\} \gg (q^B)^{s-4},$$

provided that $s > \max\{k^2, 2^4\}$. This gives the advertised strengthening of the Lang–Tsen theorem.

We remark that, as with work in the previous section, the condition $s > 2^4$ can be weakened to give $s > k^2 + k$ (and, with more work, only $s \geq k^2$ and even better can be achieved).