# Part I: Examples

presentation rather closely especially in the proof we give of The Main Lemma in Part III. Most of this article was prepared while the author visited the IHES (1979-80). The present version was presented in three seminars at the University of Illinois in the Spring of 1981.

## PART I: EXAMPLES

§1. THE ZETA FUNCTION OF THE PROJECTIVE LINE. Let $\mathbf{F}_q$ be the finite field of $q$ elements and let $A = \mathbf{F}_q[x]$ be the ring of polynomials with coefficients in $\mathbf{F}_q$. The set of closed points on the projective line $\mathbf{P}^1$ can be identified with the set of monic irreducible polynomials in $A$ plus the rational function $\frac{1}{x}$ which corresponds to the point at infinity on $\mathbf{P}^1$. If $P$ is a polynomial in $A$ of degree $d$, we put

$$NP = q^d .$$

The zeta function of the affine line $\mathbf{A}^1 = \mathbf{P}^1 - \{\infty\}$ is defined, for $s$ a complex number, by

$$Z(s, \mathbf{A}^1) = \sum_a Na^{-s} ,$$

where $a$ runs over all monic polynomials in $A$ including $a = 1$. Since

$$\#\{a \in A \mid a \text{ monic, } \deg(a) = n\} = q^n ,$$

it follows that

$$Z(s, \mathbf{A}^1) = \sum_{n=0}^{\infty} q^{n-ns} = \frac{1}{1 - q^{1-s}} ;$$

hence $Z(s, \mathbf{A}^1)$ is an absolutely convergent series for $R(s) > 1$. Furthermore, since $A$ is a unique factorization domain, we have an Euler product expansion

$$Z(s, \mathbf{A}^1) = \prod_P \frac{1}{1 - NP^{-s}} ,$$

where $P$ runs over all monic irreducible polynomials in $A$ of degree $\geqslant 1$. If we include in this Euler product the factor $(1-q^{-s})^{-1}$, which corresponds to the rational function $P_\infty = \frac{1}{x}$, we obtain the zeta function of the projective line

$$Z(s, \mathbf{P}^1) = \prod_P \frac{1}{1 - NP^{-s}}$$

$$= \frac{1}{1 - q^{-s}} \cdot \frac{1}{1 - q^{1-s}}.$$

To study $Z(s, \mathbf{A}^1)$ we can also proceed in a slightly different way. First we recall that a fundamental lemma in the arithmetic of the ring $A$ is Gauss' result that for any positive integer $n \geqslant 1$

$$x^{q^n} - x = \prod_{d|n} F_d(x),$$

where $F_d(x)$ is the product of all monic irreducible polynomials in $A$ of degree $d$. By comparing the degrees on both sides of this identity we obtain

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

where $N_d$ is the number of monic irreducible polynomials in $A$ of degree $d$. In the Euler product for $Z(s, \mathbf{A}^1)$ we collect those polynomials $P$ of degree $d$ and use the last equality to obtain

$$Z(s, \mathbf{A}^1) = \prod_{d=1}^{\infty} \left( \frac{1}{1 - q^{-ds}} \right)^{Nd}.$$

By taking the logarithm of both sides we get

$$\log Z(s, \mathbf{A}^1) = \sum_{d=1}^{\infty} N_d \sum_{k=1}^{\infty} q^{-sdk}/k$$

$$= \sum_{m=1}^{\infty} \frac{1}{m} q^{-sm} \sum_{d|m} dN_d$$

$$= \sum_{m=1}^{\infty} \frac{1}{m} (q^{1-s})^m$$

$$= \log \frac{1}{1 - q^{1-s}};$$

this agrees with the expression obtained earlier for $Z(s, \mathbf{A}^1)$. Three observations are in order at this point:

(1.1) $Z(s, \mathbf{P}^1)$ is meromorphic in the region $R(s) \geqslant 1$ and has a simple pole at $s = 1$; this implies that

(1.2) The Euler product expansion of $Z(s, \mathbf{P}^1)$ has an infinite number of local factors (Euler's proof of the infinitude of primes!)

(1.3) $Z(1 + it, \mathbf{P}^1) \neq 0$ for all real values of $t$.

§2. GAUSS SUMS. If $x \in \mathbf{C}$ and if $m$ is an integer $\geqslant 1$, we put

$$e_m(x) = e^{2\pi i x/m}.$$

Let $p$ denote a prime number. If $x \in \mathbf{Z}$, and $\mu_p$ denotes the group of $p$-th roots of unity, then the map $x \to e_p(x)$ defines by passage to the quotient an isomorphism

$$e_p : \mathbf{Z}/p\mathbf{Z} \to \mu_p .$$

Let $k = \mathbf{F}_q$ denote the finite field with $q = p^a$ elements. For $x \in \mathbf{F}_q$ we put

$$\mathrm{Tr}_k(x) = x + x^p + \ldots + x^{p^{a-1}};$$

since $\mathrm{Tr}_k(x)$ belongs to $\mathbf{Z}/p\mathbf{Z}$, the map

$$\mathbf{F}_q \to \mu_p$$

given by $\psi_k(x) = e_p(\mathrm{Tr}_k(x))$ is a non-trivial additive character of $\mathbf{F}_q$. Any other additive character $\psi'$ of $\mathbf{F}_q$ has the form $\psi'(x) = \psi_k(cx)$ for some $c \in \mathbf{F}_q$. Let $\mathbf{F}_q^* = \mathbf{F}_q - \{0\}$ be the multiplicative group of $\mathbf{F}_q$. With each of the $q - 1$ characters $\chi$ of $\mathbf{F}_q^*$ there is associated a Gauss sum

$$g(\chi, \psi) = \sum_{x \in \mathbf{F}_q} \chi(x)\psi(x);$$

The one corresponding to the trivial character $\chi_0 \equiv 1$ has the value $g(\chi_0, \psi) = -1$. A well known property of $g(\chi, \psi)$ with $\chi$ a non-trival character is $|\, g(\chi, \psi)\,|^2 = q$.

For a monic polynomial in the ring $A = \mathbf{F}_q[x]$

$$a = x^n + a_1 x^{n-1} + \ldots + a_n$$

we put

$$\Lambda(a) = \chi(a_n)\psi(a_1);$$

if $b$ is another monic polynomial

$$b = x^m + b_1 x^{m-1} + \ldots + b_m,$$

Then

$$a \cdot b = x^{m+n} + (a_1 + b_1)x^{m+n-1} + \ldots + a_n b_m;$$

from this it follows easily that

$$\Lambda(a \cdot b) = \Lambda(a)\Lambda(b).$$

We can thus form the zeta function

$$Z(s, \mathscr{L}_\chi) = \sum_a \Lambda(a) N a^{-s}$$

$$= \prod_P \frac{1}{1 - \Lambda(P) N P^{-s}},$$

where the product runs over all irreducible monic polynomials in $A$. From the

properties of $Z(s, \mathbf{A}^1)$ it follows easily that $Z(s, \mathscr{L}_\chi)$ is absolutely convergent for $R(s) > 1$. The Dirichlet series $Z(s, \mathscr{L}_\chi)$ is also expressible in the form

$$Z(s, \mathscr{L}_\chi) = 1 + \sum_{d=1}^{\infty} q^{-ds} S_d ,$$

where

$$S_d = \sum_a \Lambda(a)$$

and the sum runs over all monic polynomials of degree $d$. As all monic polynomials of degree 1 in $A$ are of the form $a = x + c$ with $c \in \mathbf{F}_q$, and since $\Lambda(x+c) = \chi(c)\psi(c)$, we obtain for $d = 1$ the Gauss sum $S_1 = g(\chi, \psi)$. Also all irreducible monic polynomials in $A$ of degree 2 have the form $a = x^2 + bx + c$, $b, c \in \mathbf{F}_q$; for these we have

$$\begin{aligned} S_2 &= \sum_a \Lambda(x^2 + bx + c) \\ &= \sum_b \sum_c \chi(c)\psi(b) \\ &= \sum_c \chi(c) \left(\sum_b \psi(b)\right) = 0 . \end{aligned}$$

A similar argument shows that for all $d \geqslant 3$ we have $S_d = 0$. Hence we obtain

$$Z(s, \mathscr{L}_\chi) = 1 + g(\chi, \psi) q^{-s} .$$

This representation proves that $Z(s, \mathscr{L}_\chi)$, defined for $R(s) > 1$ has a holomorphic continuation to all values of the complex variable $s$; from the fact $| g(\chi, \psi) | = q^{\frac{1}{2}}$ it also follows that the zeros of $Z(s, \mathscr{L}_\chi)$ are all located on the line $R(s) = \frac{1}{2}$. The trivial fact $| g(\chi, \psi) | < q$ would suffice to show that $Z(1 + it, \mathscr{L}_\chi) \neq 0$ for all real values of $t$.

§3. KLOOSTERMAN SUMS. Let $\varphi$ be an additive character of $\mathbf{F}_q$. For a monic polynomial in $A$ of the form

$$a = x^n + a_1 x^{n-1} + \ldots + a_n , \qquad a_n \neq 0 ,$$

we define a function

$$\Lambda(a) = \psi(a_1)\varphi(a_{n-1}\bar{a}_n) , \qquad a_n \bar{a}_n = 1 ,$$

with the proviso that

$$\Lambda(x+c) = \psi(c)\varphi(c^{-1}) .$$

If $b \in A$ is another polynomial of the form

$$b = x^m + b_1 x^{m-1} + \ldots + b_m ,$$

we have

$$ab = x^{m+n} + (a_1+b_1)x^{m+n-1} + \ldots + (a_nb_{m-1}+b_ma_{n-1})x + b_nb_m .$$

By noting that $(a_nb_{m-1}+b_ma_{n-1})\bar{a}_n\bar{b}_m = b_{m-1}\bar{b}_m + a_{n-1}\bar{a}_n$ we obtain

$$\Lambda(a\cdot b) = \Lambda(a)\Lambda(b) .$$

Thus we can define a new zeta function by putting

$$\begin{aligned} Z(s, Kl) &= \sum_a \Lambda(a)Na^{-s} \\ &= \prod_P \frac{1}{1 - \Lambda(P)NP^{-s}} , \end{aligned}$$

where the sum is taken over the set of monic polynomials $a$ in $A$ with non-zero constant term including the polynomial $a = 1$, and the product is taken only over the subset of those which are irreducible.

By grouping together terms in the Dirichlet series $Z(s, Kl)$ corresponding to polynomials of the same degree we obtain

$$Z(s, Kl) = 1 + \sum_{d=1}^{\infty} q^{-ds}S_d ,$$

where

$$S_d = \sum_a \Lambda(a) ,$$

and the sum runs over all monic polynomials $a$ in $A$ of degree $d$ with non-zero constant term. Let us look more closely at the sums $S_d$ for small $d$. For $d = 1$ all the monic polynomials in $A$ are of the form $x + c$ with $c \in \mathbf{F}_q$, and

$$\begin{aligned} S_1 &= \sum_{c\in\mathbf{F}_q^*} \Lambda(x+c) \\ &= \sum_{c\in\mathbf{F}_q^*} \psi(c)\varphi(c^{-1}) ; \end{aligned}$$

since $\varphi(x) = \psi(bx)$ for some $b \in \mathbf{F}_q^*$, we obtain then that

$$S_1 = \sum_{c\in\mathbf{F}_q^*} \psi(c+bc^{-1}) .$$

If $\mathbf{F}_q = \mathbf{Z}/\mathbf{Z}_p$, then $S_1$ reduces to the well known Kloosterman sum

$$Kl(p) = \sum_{c\in\mathbf{F}_p^*} e^{\frac{2\pi i}{p}(ac+bc^{-1})} .$$

In the following we denote $S_1$ by $-K(\varphi)$. All monic polynomials of degree 2 with non-zero constant term are given by $a = x^2 + cx + b$, with $c \in \mathbf{F}_q$, $b \in \mathbf{F}_q^*$, and hence

$$S_2 = \sum_a \Lambda(x^2+cx+b),$$
$$= \sum_{c\in\mathbf{F}_q} \sum_{b\in\mathbf{F}_q^*} \psi(c)\varphi(cb^{-1})$$
$$= \sum_{b\in\mathbf{F}_q^*} \sum_{c\in\mathbf{F}_q} \psi_b(c),$$

where $\psi_b(c) = \psi(c(1+\bar{b}a_0))$, and $\varphi(c) = \psi(a_0c)$. Now $\psi_b(c) \equiv 1$ if and only if $1 + \bar{b}a_0 = 0$ and this occurs only once when $b = -a_0$. For this particular value of $b$, the inner sum is equal to $\#\mathbf{F}_q = q$. If $b \neq -a_0$, then $\psi_b$ is a non-trivial additive character and the inner sum has the value zero. Therefore we have $S_2 = q$. For $d = 3$ we have from the definition of $\Lambda$ that

$$S_3 = \sum_b \sum_c \sum_d \Lambda(x^3+bx^2+cx+d),$$

with $b, c, d \in \mathbf{F}_q$ and $d \neq 0$, and hence

$$S_3 = \sum_c \sum_d \varphi(c\bar{d}) \sum_{b\in\mathbf{F}_q} \psi(b) = 0.$$

For similar reasons we also obtain $S_d = 0$ for $d \geqslant 3$. We can now write

$$Z(s, Kl) = \prod_P \frac{1}{1 - \Lambda(P)NP^{-s}}$$
$$= 1 - K(\varphi)q^{-s} + q^{1-2s}.$$

This shows that the function $Z(s, Kl)$ is holomorphic for all complex values of $s$. It is clear that $Z(s, Kl) \neq 0$ for $R(s) > 1$; the simple observation $|K(\varphi)| < q$ would also give that

$$Z(1+it, Kl) \neq 0$$

for all real values of $t$. Let us pretend for a moment that we do not know this fact and show how it can be derived, in an unnecessarily complicated way, from the method of Hadamard and de la Vallée-Poussin. Suppose then that $1 + it_0$ is a zero of multiplicity $m$. For $\sigma > 1$ and $Z(s, Kl) = Z(s, \Lambda)$ we have

$$-\frac{Z'}{Z}(\sigma+it, \Lambda) = \sum_{\substack{P \\ n>0}} (\log NP)NP^{-n\sigma}(NP^{-it}\Lambda(P))^n.$$

If we put $\lambda_P = NP^{-it_0}\Lambda(P)$, then clearly $\lambda_P \cdot \bar{\lambda}_P = 1$ and

$$R\left\{-6\frac{Z'}{Z}(\sigma, 1) - 8\frac{Z'}{Z}(\sigma+it_0, \Lambda) - 2\frac{Z'}{Z}(\sigma+2it_0, \Lambda^2)\right\}$$
$$= \sum_{\substack{P \\ n>0}} (\log NP)NP^{-n\sigma}\{2 + \lambda_P^n + \bar{\lambda}_P^n\}^2 > 0.$$

On the other hand for $\sigma > 1$ and close to 1 we have

$$-\frac{Z'}{Z}(\sigma, 1) = \frac{1}{\sigma - 1} + f_1(\sigma),$$

$$\frac{Z'}{Z}(\sigma + it_0, \Lambda) = \frac{m}{\sigma - 1} + f_2(\sigma),$$

where $f_i$ remains finite as $\sigma \to 1$. We thus obtain

$$\frac{6}{\sigma - 1} - \frac{8m}{\sigma - 1} \gg 1.$$

But this is false for $\sigma$ sufficiently close to 1 unless $m = 0$ in which case $Z(s, Kl)$ does not vanish on the line of absolute convergence. It is a simple matter to obtain, say via a Tauberian argument, that

$$\sum_{NP \leqslant x} \Lambda(P) = \delta_\Lambda x + o(x),$$

where $\delta_\Lambda = 0$, unless $\Lambda \equiv 1$ in which case $\delta_\Lambda = \frac{1}{\log q}$. This circle of ideas has been introduced by Kornblum (*Math. Zeitschr.* Vol. 5 (1919), p. 100) in order to establish an analogue of Dirichlet's Theorem on arithmetic progressions for the ring $A = \mathbf{F}_q[x]$; they were later developed more fully and systematically by Artin in the second part of his thesis ([1], II). It is a consequence of Weil's proof of the Riemann Hypothesis for curves over finite fields that the zeros of $Z(s, \Lambda)$ are all located on the critical line $R(s) = \frac{1}{2}$. This gives the much sharper estimate $\delta_\Lambda x + O(x^{\frac{1}{2}})$ for the above sum. The equality $Z(s, Kl) = 1 - K(\varphi)q^{-s} + q^{1-2s}$ also implies $| K(\varphi) | \leqslant 2q^{\frac{1}{2}}$, an estimate which is best possible.

§4. EQUIDISTRIBUTION OF THE ARGUMENTS OF GAUSS SUMS. Let $\mathbf{F}_p$ be the finite field of $p$ elements; let $\psi : \mathbf{F}_p \to \mathbf{C}^*$ be a fixed non-trivial additive character of $\mathbf{F}_p$ as in §2. With each of the $p - 1$ characters $\chi$ of the multiplicative group $\mathbf{F}_p^* = \mathbf{F}_p - \{0\}$ we define a Gauss sum

$$g(\chi, \psi) = \sum_{x \in \mathbf{F}_q^*} \chi(x)\psi(x).$$

If $\chi$ is one of the $p - 2$ non-trivial multiplicative characters of $\mathbf{F}_p^*$, we have $| g(\chi, \psi) | = p^{\frac{1}{2}}$, and hence

$$g(\chi, \psi) = p^{\frac{1}{2}} e^{2\pi i \theta_p(\chi)},$$

with $\theta_p(\chi) \in [0, 1)$. For each prime $p$, and for a fixed choice of additive character $\psi$ we consider the sequence of $p - 2$ angles

$$\Theta_p = \{\theta_p(\chi_j)\}_{1 \leq j \leq p-2},$$

which result from all the non-trivial characters of $\mathbf{F}_p^*$. As $p$ ranges over the primes in increasing order we obtain a triangular array

$$\Theta = \{\Theta_p \mid p \quad \text{a prime}\}$$

of points in $[0, 1)$. For a prime $p$ and a subinterval $J$ in $[0, 1)$, we denote by $A(p, J)$ the number of angles $\theta_p(\chi_j)$, $1 \leqslant j \leqslant p - 2$ which belong to $J$, $| J |$ is the length of $J$. The sequence $\Theta$ is uniformly distributed in $[0, 1)$; in fact it can be shown that (Smith [10]),

$$\operatorname*{Sup}_J | (p-2)^{-1} A(p, J) - | J | | \ll p^{-\frac{1}{4}}.$$

In particular one obtains the estimate

$$A(p, J) = | J | p + O(p^{\frac{3}{4}}).$$

To establish these results we put, for $h$ a non-zero integer,

$$S_p(h) = \frac{1}{p-2} \sum_{\chi}{}' e^{2\pi i h \theta_p(\chi)},$$

where the sum runs over the non-trivial characters of $\mathbf{F}_p^*$. The Erdös-Turan inequality [1]) gives, for any integer $m \geqslant 1$

$$\operatorname*{Sup}_J | (p-2)^{-1} A(p, J) - | J | | \leqslant \frac{4}{m+1} + \frac{4}{\pi} \sum_{h=1}^{m} \frac{1}{h} | S_p(h) |.$$

To get an estimate for $S_p(h)$, we observe that since $g(\chi, \psi) = p^{\frac{1}{2}} e^{2\pi i \theta_p(\chi)}$, we have

$$\begin{aligned} \sum_{\chi}{}' g(\chi, \psi)^h &= p^{h/2} \sum_{\chi}{}' e^{2\pi i h \theta_p(\chi)} \\ &= p^{h/2}(p-2) S_p(h). \end{aligned}$$

On the other hand we have the combinatorial identity

$$\sum_{\chi}{}' g(\chi, \psi)^h = (-1)^{h+1} + (p-1) \sum_{x_i} \psi(x_1 + \ldots + x_h), \tag{4.1}$$

[1]) H. Montgomery has obtained a conceptually simple proof of this inequality along the lines of his article in *Bull. A.M.S.* vol. 84 (1978), 546-567.

where the sum on the right hand side is taken over all the $h$-tuples $(x_1, ..., x_h) \in (\mathbf{F}_p)^h$ which satisfy $x_1 \cdot x_2 \cdot ... \cdot x_h = 1$. The sum

$$Kl_h(p) = \sum_{x_i} \psi(x_1 + ... + x_h)$$

is usually called a hyper Kloosterman sum. As a generalization of the function $Z(s, Kl)$ considered in §3 it is natural to consider a function $Z(s, Kl_h)$ defined by the following Euler product

$$Z(s, Kl_h)^{(-1)^{h+1}} = \prod_{P \in |X_0|} \frac{1}{1 - \Lambda(P) NP^{-s}},$$

where $X_0$ is the affine variety defined over $\mathbf{F}_p$ by $x_1 ... x_h = 1$, $|X_0|$ is the set of closed points on $X_0$ and $\Lambda : |X_0| \to \mathbf{C}^*$ is a function which takes the value

$$\Lambda(P) = \psi(a_1 + ... + a_n),$$

when $P$ is the closed point $(a_1, ..., a_n) \in X_0(\mathbf{F}_p)$ defined by the maximal ideal $(x_1 - a_1, ..., x_h - a_n)$ in $\mathbf{F}_p[x_1, ..., x_h]$. The function $Z(s, Kl_h)$ can be shown to be a polynomial of degree $h$ in $p^{-s}$, where the coefficient of $p^{-s}$ is the hyper Kloosterman sum $Kl_h(p)$. It is a consequence of Deligne's proof of the Weil conjecture that the zeros of $Z(s, Kl_h)$ are all located on the line $R(s) = \dfrac{h-1}{2}$. This implies in particular that

$$|Kl_h(p)| \leqslant hp^{(h-1)/2}. \tag{4.2}$$

The weaker result $|Kl_h(p)| \leqslant hp^{\frac{h}{2} - \delta}$, for some $\delta > 0$ would follow from the non-vanishing of $Z(s, Kl_h)$ on the line $R(s) = \dfrac{h}{2}$; this would be enough to establish the equidistribution of the angles of the Gauss sums.

From Deligne's estimate (4.2) and the combinatorial identity we obtain that

$$\begin{aligned} S_p(h) &= \frac{1}{p-2} \sum_{\chi}{}' e^{2\pi i h \theta_p(\chi)} \\ &= \frac{1}{p-2} \cdot p^{-\frac{h}{2}} \sum_{\chi}{}' g(\chi, \psi)^h \\ &= (p-2)^{-1} p^{-\frac{h}{2}} \{(-1)^{h+1} + (p-1) Kl_h(p)\}, \end{aligned}$$

and hence

$$|S_p(h)| < 2hp^{-\frac{1}{2}}.$$

When this estimate is substituted into the Erdös-Turan inequality with $m = [p^{\frac{1}{4}}]$, we get

$$\operatorname*{Sup}_J |(p-2)^{-1}A(p, J) - |J|| \leqslant \frac{1}{m+1} + \frac{8}{\pi} mp^{-\frac{1}{2}} \ll p^{-\frac{1}{4}}.$$

This establishes the result. A comparison of the estimate $A(p, J) = p|J| + O(p^{\frac{3}{4}})$ with some of the classical prime number theorems suggests that perhaps the stronger result

$$A(p, J) = p|J| + O(p^{\frac{1}{2}+\varepsilon})$$

should be true.

## Part II: Statement of the theorem

§1.1. Introduction. In the statement of Deligne's theorem there appear certain Euler products which are generalizations of the Artin-Grothendieck $L$-functions and which satisfy some rather natural growth conditions; these conditions are stated below in §2 as Axioms A and B. In order to elucidate the applicability of the theorem, to introduce some relevant concepts from representation theory, and to prepare the notation that goes into the statement of the theorem, we now give two examples one of a geometric nature, the other of an arithmetic nature. The expert will realize that both examples are intimately connected, say via the Selberg-trace Formula.

§1.2. Geometric example. As in Part I, let $\mathbf{F}_q$ be the finite field of $q$ elements and let $A = \mathbf{F}_q[T]$ be the coordinate ring of the affine line $\mathbf{A}^1$. For technical reasons and to simplify our presentation, we assume the characteristic of $\mathbf{F}_q$ is not 2 or 3. The closed points on the affine line $\mathbf{A}^1$ are in one-to-one correspondence with the irreducible monic polynomials in $A$. Now if $P = P_v$ is such an irreducible polynomial in $A$, then the image of $T$ under the reduction map

$$A \to A/(P) = \mathbf{F}_{q_v}$$
$$T \to t_v,$$

gives an element $t_v$ in the finite field $\mathbf{F}_{q_v}$ with $q_v = q^{\deg(P)}$ elements. We can now consider the elliptic family