

LECTURE NOTES: BASIC L-FUNCTIONS

GERGELY HARCOS

For motivation and guidance let us consider the following problems.

Problem 1. For a prime p and two intervals $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \dots, p-1\}$ how evenly are the products ab ($a \in \mathcal{A}, b \in \mathcal{B}$) distributed modulo p ?

Problem 2. For a fixed integer q how evenly are the primes distributed modulo q ?

These problems appear similar, but only on the surface. Yet, a deep connection can be identified through the language of L -functions. Namely, both problems can be formulated as counting problems where the error term can be expressed in terms of the zeros of certain L -functions.

For the first problem we can use harmonic analysis on $\mathbb{Z}/p\mathbb{Z}$. Let $e_p(k) := e^{2\pi i k/p}$ be the standard character on $\mathbb{Z}/p\mathbb{Z}$, and for a nonzero residue $x \bmod p$ let \bar{x} denote its multiplicative inverse mod p . For any $r \in \{1, 2, \dots, p-1\}$ we can prove the exact formula

$$\sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ ab \equiv r \pmod{p}}} 1 = |\mathcal{A}||\mathcal{B}| \frac{p+1}{p^2} + \frac{1}{p^2} \sum_{0 < m, n < p} S(m, n, p) \left(\sum_{a \in \mathcal{A}} e_p(ma) \right) \left(\sum_{b \in \mathcal{B}} e_p(nb\bar{r}) \right),$$

where

$$S(m, n, p) := \sum_{x=1}^{p-1} e_p(mx + n\bar{x})$$

is the so-called *Kloosterman sum*. The other two inner sums are finite geometric series, hence they are straightforward to evaluate and estimate. We obtain the elegant inequality

$$\left| \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ ab \equiv r \pmod{p}}} 1 - \frac{|\mathcal{A}||\mathcal{B}|}{p} \right| \leq 1 + (\log p)^2 \max_{0 < m, n < p} |S(m, n, p)|.$$

This shows that if the Kloosterman sums $S(m, n, p)$ are small in terms of p , then the products ab ($a \in \mathcal{A}, b \in \mathcal{B}$) are well-distributed modulo p . But how small are these sums? Kloosterman himself gave a nontrivial bound in 1926, but the essentially best possible answer came from Weil in 1948, as a result of his deep understanding of curves over finite fields and their L -functions. I will return to this matter at the end of the lecture.

For the second problem we can combine harmonic analysis on $(\mathbb{Z}/q\mathbb{Z})^\times$ with complex analysis. It is easier to count prime powers than primes alone, therefore we introduce

$$\Lambda(n) := \begin{cases} \log p & \text{if } n \text{ is a power of the prime } p; \\ 0 & \text{otherwise.} \end{cases}$$

We choose a reduced residue $r \bmod q$ and a smooth weight function $F : (0, \infty) \rightarrow (0, \infty)$ of compact support. We can prove the exact formula

$$\sum_{n \equiv r \pmod{q}} \Lambda(n) F(n) = \frac{1}{\varphi(q)} \hat{F}(1) - \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \bar{\chi}(r) \sum_{L(p, \chi)=0} \hat{F}(\rho),$$

where

$$\hat{F}(s) := \int_0^\infty F(x)x^{s-1} dx, \quad s \in \mathbb{C},$$

is the Mellin transform of F (it is an entire function), χ runs through the characters of $(\mathbb{Z}/q\mathbb{Z})^\times$ (their number is precisely $\varphi(q)$), and the last sum is over all zeros ρ of Dirichlet's L -function $L(s, \chi)$ counted with multiplicity. I will discuss these L -functions in a moment. The first term in the formula is the expected main term. The other terms are substantially smaller, because the corresponding ρ 's are known to have real part less than 1. The famous Riemann Hypothesis states that all zeros have real part $1/2$ or less. Currently we cannot exclude the possibility that these real parts get occasionally very close to 1, but nevertheless we can show that the main term dominates for typical weight functions, e.g. for those approximating the characteristic function of a long interval.

Dirichlet defined his L -functions in 1837 as follows. The character $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ can be extended to a periodic multiplicative function $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ by putting

$$\chi(n) := \begin{cases} \chi(n \bmod q), & (n, q) = 1; \\ 0, & (n, q) > 1. \end{cases}$$

Such a function is called a *Dirichlet character*. Then one can define the Dirichlet series

$$L(s, \chi) := \sum_{n=1}^\infty \frac{\chi(n)}{n^s}, \quad \Re s > 1,$$

and extend it meromorphically to the complex plane. If $\chi : \mathbb{Z} \rightarrow \mathbb{C}^\times$ is the trivial character, then $L(s, \chi)$ has a simple pole at $s = 1$ (this supplies the main term above!) and is holomorphic elsewhere; otherwise $L(s, \chi)$ is holomorphic everywhere. By multiplicativity, there is an *Euler product* decomposition over the primes:

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}, \quad \Re s > 1,$$

this is what makes Dirichlet L -functions so suitable for counting primes. For any Dirichlet character $\chi \bmod q$ there is a smallest divisor $q' | q$ such that χ agrees with a Dirichlet character $\chi' \bmod q'$ on integers coprime with q . The resulting χ' is called *primitive* and has many distinguished properties. First of all, χ being induced from χ' means analytically that

$$L(s, \chi) = L(s, \chi') \prod_{p|q} (1 - \chi'(p)p^{-s}),$$

whence $L(s, \chi)$ and $L(s, \chi')$ have the same zeros in the *critical strip* $0 < \Re s < 1$. Zeros outside this strip are well understood and are irrelevant for our counting problem.

Now let us assume that χ is primitive (i.e. $\chi' = \chi$), then we have the following beautiful functional equation, discovered by Riemann in 1860 for the case $q = 1$ (Riemann zeta function) and worked out for general q by Hurwitz in 1882:

$$q^{s/2} \Gamma_{\mathbb{R}}(s + \varepsilon) L(s, \chi) = \kappa q^{(1-s)/2} \Gamma_{\mathbb{R}}(1 - s + \varepsilon) L(1 - s, \bar{\chi}).$$

Here $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2} \Gamma(s/2)$, $\varepsilon \in \{0, 1\}$ such that $\chi(-1) = (-1)^\varepsilon$, and κ is an explicitly computable complex number of modulus 1. This shows that by attaching the $\Gamma_{\mathbb{R}}$ -factor to the L -function, the resulting completed L -function exhibits full symmetry with respect to $s \leftrightarrow 1 - s$. It follows that there are infinitely many zeros ρ with real part at least $1/2$; in fact it seems that all zeros in the critical strip have real part equal to $1/2$.

The two key features of Dirichlet L -functions are Euler product and functional equation. Generalizing these objects to an arbitrary number field K is far from obvious, and was not

done until 1918 when Hecke came upon the correct notion of *primitive Grössencharacter* whose associated L -function has analogous properties to the ones discussed above. The original definitions and proofs are complicated, but a clear picture arises by using the ring of *adeles* \mathbb{A}_K of K . This is a certain restricted direct product over the various non-equivalent completions of K . One takes a factor \mathbb{R} for each real embedding $K \rightarrow \mathbb{R}$, a factor \mathbb{C} for each conjugate pair of complex embeddings $K \rightarrow \mathbb{C}$, and a factor $K_{\mathfrak{p}}$ for each prime ideal \mathfrak{p} in the ring of integers of K . These factors gives rise to the product space $\prod_v K_v$, and the ring of adeles consists of those vectors (x_v) in this space for which $x_{\mathfrak{p}}$ is a \mathfrak{p} -adic integer for all but finitely many prime ideals \mathfrak{p} . The group K embeds diagonally into \mathbb{A}_K as a discrete subgroup with compact quotient. In particular, K^\times embeds into the group of *ideles* \mathbb{A}_K^\times . A character $\omega : \mathbb{A}_K^\times \rightarrow \mathbb{C}^\times$ determines a local character $\omega_v : K_v^\times \rightarrow \mathbb{C}^\times$ for each place v and one can associate a local L -function $L(s, \omega_v)$ as a certain shift of $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2)$ or $\Gamma_{\mathbb{C}}(s) := (2\pi)^{1-s}\Gamma(s)$ or $(1 - \mathcal{N}\mathfrak{p}^{-s})^{-1}$ depending on the type of v . One can then define the complete L -function as an Euler product

$$\Lambda(s, \omega) := \prod_v L(s, \omega_v), \quad \Re s > 1.$$

If ω is trivial on K^\times , then using Poisson summation for K within \mathbb{A}_K one can show that

$$(|D|_{\mathcal{N}\mathfrak{q}})^{s/2}\Lambda(s, \omega) = \kappa(|D|_{\mathcal{N}\mathfrak{q}})^{(1-s)/2}\Lambda(1-s, \bar{\omega}),$$

where D is the discriminant of K , \mathfrak{q} is a certain ideal depending on ω , and κ is a complex number of modulus 1. These are the basic L -functions for a number field K : they are associated with the characters of $\mathbb{A}_K^\times/K^\times$ and agree with the complete L -functions discovered by Hecke. The Riemann Hypothesis seems to be true for all these L -functions.

The above construction also works for a finite algebraic extension of the function field $\mathbb{F}_p(T)$. Such an extension K is the function field of some projective algebraic curve C over \mathbb{F}_p which can be studied by algebraic geometry. For example, places of K correspond to $\text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ -orbits in $C(\bar{\mathbb{F}}_p)$, positive divisors play the role of ideals in the number field setting etc. The functional equation for a basic L -function now reads

$$(p^{\deg \mathfrak{d}} p^{\deg \mathfrak{q}})^{s/2}\Lambda(s, \omega) = \kappa(p^{\deg \mathfrak{d}} p^{\deg \mathfrak{q}})^{(1-s)/2}\Lambda(1-s, \bar{\omega}),$$

where \mathfrak{d} is the canonical divisor of C , \mathfrak{q} is a certain positive divisor depending on ω , and κ is a complex number of modulus 1. This forces $\Lambda(s, \omega)$ to be special, e.g. if $\mathfrak{q} \neq 0$ then

$$\Lambda(s, \omega) = \prod_{j=1}^{\deg \mathfrak{d} + \deg \mathfrak{q}} (1 - \alpha_j p^{-s})$$

for some $\alpha_j \in \mathbb{C}$. The coefficient of p^{-s} on the right hand side is an interesting sum over $C(\mathbb{F}_p)$, e.g. for $K = \mathbb{F}_p(T)$ (so that $\deg \mathfrak{d} = -2$) and a certain ω with $\deg \mathfrak{q} = 4$ it is the Kloosterman sum discussed in Problem 1: $S(m, n, p) = -\alpha_1 - \alpha_2!$

The punch line is that for the function field case Weil proved in 1941 the analogue of the Riemann Hypothesis: all the zeros of $\Lambda(s, \omega)$ have real part equal to $1/2$. This means that the above α_j 's are of modulus $p^{1/2}$, therefore

$$\max_{0 < m, n < p} |S(m, n, p)| \leq 2p^{1/2}.$$

Going back to Problem 1, we can infer

$$\left| \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ ab \equiv r \pmod{p}}} 1 - \frac{|\mathcal{A}||\mathcal{B}|}{p} \right| \leq 1 + 2p^{1/2}(\log p)^2.$$

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, POB 127,
BUDAPEST H-1364, HUNGARY
E-mail address: `gharcos@renyi.hu`