NIKI MYRTO MAVRAKI

ABSTRACT. We introduce the Weil conjectures, concerning the problem of counting solutions to a system of polynomial equations over a finite field. The real aim in number theory is to count solutions to such a system over \mathbb{Z} or the ring of integers of a number field. However, this problem is much harder than counting the solutions over a finite field and the two problems are related via various local global principles. An object introduced to count certain objects of geometric, arithmetic and algebraic nature is zeta functions. We will introduce some zeta functions and state some related conjectures. Most of these notes are adapted from [Must, Introduction].

1. MOTIVATION WEIL CONJECTURES: THE RIEMANN ZETA FUNCTION

The prototypical example of a zeta function is the Riemann zeta function, first studied by Euler and later studied by Riemann who thought of it as a function on the whole complex plane and in this way was able to use complex analysis. The Riemann zeta function is defined as

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s}.$$

The unique factorization of an integer as a product of primes gives an expression for this *global* zeta functions as a product of *local* zeta functions, each corresponding to a single prime $p \in \mathbb{Z}$, as follows

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

Riemann's motivation to study this function was to understand the distribution of prime numbers. He showed that although a priori $\zeta(s)$ is defined (and is analytic) for $s \in \mathbb{C}$ with $\operatorname{Re}(s) > 1$, we can continue it meromorphically to the entire complex plane with a simple pole as s = 1. Moreover, he showed that $\zeta(s)$ satisfies a functional equation. More precisely he showed that if $\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s)$, then $\xi(s) = \xi(1-s)$. Last but not least, he conjectured what is referred to as the 'Riemann hypothesis', which states that the zeroes of $\zeta(s)$ all lie on the line $\operatorname{Re}(s) = \frac{1}{2}$, with the exception of the 'trivial zeroes' at -2n. Although this might seem like a really special conjecture about a rather special meromorphic function, these ideas gave birth to a more and more popular study of several zeta functions introduced to analyze the distribution of various objects of arithmetic or geometric interest. In the following we will introduce some of these zeta functions and state the Weil conjectures, which are the main subject of this seminar.

2. The Hasse-Weil zeta function

To state the Weil conjectures we will use the Hasse-Weil zeta function.

Definition 2.1. Let $X \subset \mathbb{A}_k^n$ be the common zero locus of the polynomials $f_1, \dots, f_n \in k[x_1, \dots, x_n]$, where $k = \mathbb{F}_q$ is a finite field. Let

$$N_m = |\{u \in X(\mathbb{F}_{q^m})\}| = |\{u \in \mathbb{F}_{q^m}^n : f_i(u) = 0, \text{ for all } i = 1, \cdots, r\}|.$$

The Hasse-Weil zeta function of X is

$$Z(X,t) = \exp\left(\sum_{m\geq 1} \frac{N_m}{m} t^m\right) \in \mathbb{Q}[[t]],$$

where $t = q^{-s}$. We write $Z(X, t) := \zeta(X, s)$.

2.1. Connection with the Riemann zeta function. To see how this zeta function is connected with the Riemann zeta function, consider $X_p \subset \mathbb{A}^1_{\mathbb{F}_p}$ be the zero locus of $f(x) = x \in \mathbb{F}_p[x]$. Then,

$$\zeta(X_p, s) = \exp\left(\sum_{m \ge 1} \frac{(p^{-s})^m}{m}\right) = \exp(-\log(1 - p^{-s})) = (1 - p^{-s})^{-1},$$

and the Riemann ζ function is the product of these Hasse-Weil zeta functions over all primes,

$$\zeta(s) = \prod_{p \text{ prime}} \zeta(X_p, s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

3. Weil conjectures

Weil made three conjectures regarding this zeta function, aiming to understand the number of solutions to a system of polynomial equations over a finite field. In the following we introduce these conjectures, namely the rationality conjecture, the functional equation and the Riemann hypothesis.

Conjecture 3.1. (rationality) Z(X,t) is a rational function.

The rationality conjecture was proved by Weil in the case of abelian varieties. The general case of a smooth projective curve, was proved by Dwork and also by Grothendieck who developed étale cohomology for this purpose. We point out here that the rationality of Z(X,t) is equivalent to the following fact regarding the number of \mathbb{F}_{q^m} -points of X, denoted by N_m .

Remark 3.2. There are algebraic numbers $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_{k'}$ for $k, k' \in \mathbb{N}$ such that $N_m = \alpha_1^m + \dots + \alpha_k^m - \beta_1^m - \dots - \beta_{k'}^m$, for all $m \in \mathbb{N}$.

The equivalence of the two statements follows from the following calculation.

$$\exp\left(\sum_{m\geq 1} (\alpha_1^m + \dots + \alpha_k^m - \beta_1^m - \dots - \beta_{k'}^m) \frac{t^m}{m}\right) = \prod_{i=1}^k \exp(-\log(1 - \alpha_i t)) \prod_{j=1}^{k'} \exp(\log(1 - \beta_j t))$$
$$= \frac{\prod_{i=1}^{k'} (1 - \beta_i t)}{\prod_{i=1}^k (1 - \alpha_i t)} = Z(X, t) = \exp\left(\sum_{m\geq 1} \frac{N_m}{m} t^m\right).$$

The second conjecture asserts that the Hasse-Weil zeta function satisfies a functional equation, much like the Riemann zeta function.

Conjecture 3.3. (functional equation) If $E = (\Delta^2) \in \mathbb{Z}$ is the self intersection number of the diagonal $\Delta \to X \times X$ and $n = \dim X$, then

$$Z\left(X,\frac{1}{q^n t}\right) = \pm q^{\frac{nE}{2}} t^E Z(X,t).$$

Finally, the third conjecture analogous to the Riemann hypothesis, predicts the modulus of the zeroes and poles of this (rational) zeta function.

Conjecture 3.4. (*Riemann hypothesis*) Let $n = \dim X$. One can write

$$Z(X,t) = \frac{P_1(t)P_3(t)\cdots P_{2n+1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)},$$

with $P_0(t) = 1 - t$, $P_{2n} = 1 - q^n t$ and for $1 \le i \le 2n - 1$, $P_i(t) = \prod_j (1 - \alpha_{i,j} t)$ with $\alpha_{i,j}$ algebraic integers such that $|a_{i,j}| = q^{i/2}$.

Remark 3.5. There is a connection between the polynomials P_i and the cohomology of X. In fact deg $(P_i) = b_i(X)$, the *i*-th Betti number of X and $E = \sum_{i=0}^{2n} (-1)^i b_i(X)$.

Remark 3.6. Conjecture 3.4 also implies that the algebraic numbers $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_{k'}$ in Remark 3.2 are in fact algebraic integers.

It is worth pointing out that the Hasse-Weil bounds for the number of \mathbb{F}_q -points on a curve X follow as a corollary of the Riemann hypothesis Conjecture 3.4.

Corollary 3.7. Let X be a curve of genus g. We have

$$||X(\mathbb{F}_q)| - 1 - q| \le 2gq^{\frac{1}{2}}$$

Proof. Let X be a curve of genus g. Then dim X = 1 and Remark 3.5 yields that deg $(P_1) = 2g$. Hence, Conjecture 3.4 yields

$$Z(X,t) = \frac{\prod_{i=1}^{2g} (1 - \alpha_i t)}{(1 - t)(1 - qt)},$$

where α_i are algebraic integers with $|\alpha_i| = q^{\frac{1}{2}}$. This in turn, in view of Remark 3.2, yields

$$N_m = |X(\mathbb{F}_{q^m})| = 1 + q^m - \alpha_1^m - \dots - \alpha_{2g}^m$$
, for all $m \in \mathbb{N}$.

In particular, for m = 1 we get that

$$|X(\mathbb{F}_q)| - 1 - q| = |-\alpha_1 - \dots - \alpha_{2g}|| \le 2gq^{\frac{1}{2}},$$

where in the last inequality we invoked the fact that $|\alpha_i| = q^{\frac{1}{2}}$ for all $i = 1, \ldots, 2g$.

4. The zeta function of an arithmetic variety

If $X \subset \mathbb{A}^n_{\mathbb{Z}}$ is defined by the ideal $(f_1, \dots, f_d) \subset \mathbb{Z}[x_1, \dots, x_n]$, we may consider it's reduction modulo p for any prime p. That is, for each prime $p \in \mathbb{Z}$, we consider $X_p \subset \mathbb{A}^n_{\mathbb{F}_p}$ be the \mathbb{F}_p -curve that is carved out by the reductions of f_i modulo p, denoted by $\bar{f}_1, \dots, \bar{f}_d$. Then, for each X_p we have the Hasse-Weil zeta function and we define

$$L_X(s) = \prod_{p \text{ prime}} Z(X_p, p^{-s}).$$

We already saw an example of such a zeta function in Section 2, when we considered X = Z(x) and got $L_X(s) = \zeta(s)$, the Riemann zeta function. Later in this course we will see that L_X is always defined in some half-plane $\{s \in \mathbb{C} : \operatorname{Re}(s) > \eta\}$. It is conjectured that when X is a smooth projective variety one can continue L_X meromorphically to the whole complex plane. Furthermore, it is conjectured that after a suitable normalization taking into account the primes of bad reduction of X, L_X also satisfies a functional equation. Both conjectures remain open in most cases. They are only known for \mathbb{P}^n , elliptic curves and some special varieties (toric varieties and flag varieties).

5. The Poincaré power series

Although most of this course will be about counting points of a variety over a finite field, it is worthwhile mentioning here the related problem of counting points of a variety with coordinates in $\mathbb{Z}/p^m\mathbb{Z}$. To tackle this problem, we introduce the Poincaré power series of $f \in \mathbb{Z}[x_1, \ldots, x_n]$. For each $m \in \mathbb{N}$ we let

$$c_m := \left| \{ u \in \left(\mathbb{Z} / p^m \mathbb{Z} \right)^n : f(u) = 0 \} \right|,$$

and we set $c_0 := 1$. The Poincaré series of f is defined to be

$$P_f(t) := \sum_{m \ge 0} c_m (tp^{-n})^m \in \mathbb{Q}[[t]].$$

Borevich conjectured that P_f is a rational function (recall here that the related Hasse-Weil zeta function Z(X, s) is a rational function). The method of p-adic integration allowed Igusa to prove this conjecture. In the next section we will introduce p-adic integration, used to defined another zeta function, the Igusa zeta function. We will see that the Igusa zeta function relates with the Poincarè power series in a way that the rationality of the one is equivalent to the rationality of the other.

6. INTEGRATION ON \mathbb{Q}_p .

Let G be a commutative topolical group, that is a group endowed with a topology which makes the group operation $G \times G \to G$, mapping $(g, h) \to gh$ and the inverse map $G \to G$ such that $g \to g^{-1}$ continuous. Such a group has a non-zero, translation invariant Borel measure which is unique up to multiplication by a non-zero constant. This measure is called the Haar measure.

For us G will be \mathbb{Q}_p with the addition operation, which is an abelian and locally compact group. We write $|\cdot|_p$ to denote the p-adic absolute value on \mathbb{Q}_p . We denote the Haar measure on $(\mathbb{Q}_p, +)$ by μ and we normalize it such that the unit ball in \mathbb{Q}_p , that is $\mathbb{Z}_p =$ $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, has measure equal to 1. That is,

$$\mu(\mathbb{Z}_p) = 1.$$

Some properties of the Haar measure are the following.

- $\mu(U) > 0$ for every non-empty open $U \subset \mathbb{Q}_p$.
- $\mu(K)$ is finite if and only if K is a compact subset of \mathbb{Q}_p .

We will compute some first integrals with respect to this measure below.

6.1. Examples of integrals.

Example 6.1. $\mu(p^m \mathbb{Z}_p) = p^{-m}$.

Proof. We write $\mathbb{Z}_p = \bigsqcup_{a \in \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}} a + p^m \mathbb{Z}_p$. Then we have

$$1 = \mu(\mathbb{Z}_p) = \sum_{a \in \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}} \mu(a + p^m \mathbb{Z}_p).$$

By the invariance of the Haar measure under translation, this yields that

$$1 = p^m \mu(p^m \mathbb{Z}_p).$$

Hence $\mu(p^m \mathbb{Z}_p) = p^{-m}$, as claimed.

Remark 6.2. The uniqueness of the Haar measure up to multiplication by a constant, together with our computation in example 6.1 imply that for any $a \in \mathbb{Q}_p^{\times}$ and any Borel set U, we have

$$\mu(aU) = |a|_p \mu(U).$$

In the following example we will see that points have Haar measure zero.

Example 6.3. $\mu(\mathbb{Z}_p \setminus \{0\}) = \mu(\mathbb{Z}_p) = 1.$

Proof. We write $\mathbb{Z}_p \setminus \{0\} = \bigsqcup_{j=0}^{\infty} p^j \mathbb{Z}_p^{\times}$. Then in view of Remark 6.2 we have

$$\mu(\mathbb{Z}_p \setminus \{0\}) = \sum_{j=0}^{\infty} p^{-j} \mu(\mathbb{Z}_p^{\times}) = \sum_{j=0}^{\infty} p^{-j} (\mu(\mathbb{Z}_p) - \mu(p\mathbb{Z}_p))$$
$$= \sum_{j=0}^{\infty} p^{-j} (1 - p^{-1}) = 1.$$

7. The Igusa zeta function

Having defined the Haar measure on $(\mathbb{Q}_p, +)$ we are now able to define the Igusa zeta function associated to a polynomial. The Igusa zeta function of $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$ is defined by

$$Z_f(s) := \int_{\mathbb{Z}_p^n} |f(x)|_p^s d^n \mu,$$

where $d^n \mu$ is the product measure $d\mu \times \cdots d\mu$.

Igus showed that Z_f is a rational function of $t = p^{-s}$; proving in this way Borevich's conjecture concerning the rationality of P_f . The connection between P_f is stated precisely in the following proposition.

Proposition 7.1. Let $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$. We have

$$P_f(t) = \frac{1 - Z_f(s)}{1 - t}$$
, where $t = p^{-s}$.

Proof. We have

$$Z_f(s) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s d^n \mu = \int_{\mathbb{Z}_p^n \setminus f^{-1}(\{0\})} |f(x)|_p^s d^n \mu.$$

If we write $F_i = \{x \in \mathbb{Z}_p^n : |f(x)|_p = p^{-i}\}$ so that $\mathbb{Z}_p^n \setminus f^{-1}(\{0\}) = \bigsqcup_{i=0}^{\infty} F_i$, we have

$$Z_f(s) = \sum_{i=0}^{\infty} p^{-is} \mu(F_i).$$

It remains to calculate $\mu(F_i)$. To this end, we write

$$F_i = \{x \in \mathbb{Z}_p^n : \operatorname{ord}_p(f(x)) \ge i\} \setminus \{x \in \mathbb{Z}_p^n : \operatorname{ord}_p(f(x)) \ge i+1\},\$$

and we calculate $\mu(\{x \in \mathbb{Z}_p^n : \operatorname{ord}_p(f(x)) \ge i\})$. Notice that and an application of the Taylor expansion yields that if $x_0 \in \mathbb{Z}_p^n$ satisfies $\operatorname{ord}_p(f(x_0)) \ge i$, then $\operatorname{ord}_p(f(x_0 + p^i \mathbb{Z}_p^n)) \ge i$. This in turn implies

$$\{x \in \mathbb{Z}_p^n : \operatorname{ord}_p(f(x)) \ge i\} = \bigsqcup_{f(x_0)=0 \mod p^i} x_0 + p^i \mathbb{Z}_p^n$$

Therefore, $\mu(\{x \in \mathbb{Z}_p^n : \operatorname{ord}_p(f(x)) \ge i\}) = c_i p^{-in}$, and

$$Z_f(s) = \sum_{i=0}^{\infty} c_i p^{-in-is} - c_{i+1} p^{-(i+1)n-is}$$
$$= \sum_{i=0}^{\infty} c_i (p^{-n}t)^i - t^{-1} \sum_{i=0}^{\infty} c_i (p^{-n}t)^i$$
$$= P_f(t) - t^{-1} (P_f(t) - 1).$$

The proposition follows.

7.1. Examples of Igusa zeta functions.

Example 7.2. In this example we compute the Igusa zeta function for $f(x) = x \in \mathbb{Z}_p[x]$. We will show that $Z_f(s) = \frac{1-p^{-1}}{1-p^{-(s+1)}}$. In particular $Z_f(s)$ has a meromorphic continuation to the entire complex plane as a rational function of p^{-s} .

Proof. We have

$$Z_f(s) = \int_{\mathbb{Z}_p \setminus \{0\}} |x|_p^s dx = \sum_{j=0}^\infty \int_{|x|_p = p^{-j}} |x|_p^s dx$$
$$= \sum_{j=0}^\infty p^{-js} \mu(p^j \mathbb{Z}_p^\times) = \sum_{j=0}^\infty p^{-j(s+1)} (1-p^{-1})$$
$$= \frac{1-p^{-1}}{1-p^{-(s+1)}},$$

as claimed.

Example 7.3. We will compute the Igusa zeta function for $f(x) = x^2 - 1 \in \mathbb{Z}_p[x]$, where $p \neq 2$. We will show that $Z_f(s) = (p-2)p^{-1} + 2p^{-1-s}\frac{1-p^{-1}}{1-p^{-(s+1)}}$, which as in the previous example is rational function of p^{-s} .

Proof. We have

$$Z_f(s) = \int_{\mathbb{Z}_p} |x^2 - 1|_p^s = \sum_{j=0}^{p-1} \int_{j+p\mathbb{Z}_p} |x^2 - 1|_p^s.$$

A change of variables setting x = j + py now yields

$$Z_f(s) = \sum_{j=0}^{p-1} p^{-1} \int_{\mathbb{Z}_p} |(j+py-1)(j+py+1)|_p^s dy.$$

7

Notice that for $j \notin \{1, -1\}$ we have $\int_{\mathbb{Z}_p} |(j + py - 1)(j + py + 1)|_p^s dy = 1$. Therefore,

$$\begin{aligned} Z(s) &= (p-2)p^{-1} + p^{-1} \int_{\mathbb{Z}_p} |py(2+py)|_p^s dy + p^{-1} \int_{\mathbb{Z}_p} |py(-2+py)|_p^s dy \\ &= (p-2)p^{-1} + 2p^{-1-s} \int_{\mathbb{Z}_p} |y|_p^s dy \\ &= (p-2)p^{-1} + 2p^{-1-s} \frac{1-p^{-1}}{1-p^{-(s+1)}}, \end{aligned}$$

where in the last equality we used Example 7.3.

We will finish this note by introducing some more zeta functions that arose in group theory.

8. Zeta functions in group theory

8.1. Subgroup growth zeta functions. Let G be a finitely generated group. For every $n \in \mathbb{N}$ we let

$$a_n(G) := |\{H \le G : [G:H] = n\}|.$$

The fact that G is finitely generated implies that $a_n(G)$ is a finite number for all $n \in \mathbb{N}$. To see this, let H be a subgroup of G of index n and denote by $\{g_1, \dots, g_n\}$ a set of coset representatives of G/H. We can associate to H the map $\theta_H : G \to S_n$ given by $g \to \sigma$, where σ is defined by $gg_iH = g_{\sigma(i)}H$. It is easy to see that if $H' \neq H$ then $\theta_{H'} \neq \theta_H$ and since G is finitely generated there are only finitely many maps $G \to S_n$. Therefore, $a_n(G) < +\infty$.

We can now define the subgroup growth zeta function associated to G.

$$\zeta_G(s) = \sum_{H \le G} [G:H]^{-s} = \sum_{n \ge 1} \frac{a_n(G)}{n^{-s}}.$$

 $\langle \alpha \rangle$

As an example, we compute the zeta function associated to $G = \mathbb{Z}^d$.

Proposition 8.1. We have $\zeta_{\mathbb{Z}^d}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1)$.

Proof. Recall that each finite index subgroup of \mathbb{Z}^d has the form $A\mathbb{Z}^d$, where A is a $d \times d$ matrix with integer entries that is invertible over \mathbb{Q} , $A \in M_d(\mathbb{Z}) \cap \operatorname{GL}_d(\mathbb{Q})$. The index $[\mathbb{Z}^d : A\mathbb{Z}^d] = |\det(A)|$. Moreover, two matrices $A, B \in M_d(\mathbb{Z}) \cap \operatorname{GL}_d(\mathbb{Q})$ give the same subgroup if and only if $AB^{-1} \in \operatorname{GL}_d(\mathbb{Q})$. Therefore,

$$\zeta_{\mathbb{Z}^d}(s) = \sum_{A \in T} |\det(A)|^{-s},$$

where T is a complete set of representatives of $M_d(\mathbb{Z}) \cap \operatorname{GL}_d(\mathbb{Q}) / \operatorname{GL}_d(\mathbb{Z})$. Such a set is given by lower triangular matrices $A = (a_{ij})_{1 \leq i,j \leq d}$, such that $a_{ii} \geq 1$ for all i and $0 \leq a_{ij} \leq a_{ii}$

when j < i. The determinant of such a matrix is $a_{11} \cdots a_{dd}$. Furthermore, the number of such matrices with diagonal (a_{11}, \cdots, a_{dd}) is $a_{22}a_{33}^2 \cdots a_{dd}^{d-1}$. Therefore,

$$\begin{aligned} \zeta_{\mathbb{Z}^d}(s) &= \sum_{A \in T} |\det(A)|^{-s} \\ &= \sum_{a_{11}=1}^{\infty} \cdots \sum_{a_{dd}=1}^{\infty} a_{22} a_{33}^2 \cdots a_{dd}^{d-1} (a_{11} \cdots a_{dd})^{-s} \\ &= \sum_{a_{11}=1}^{\infty} a_{11}^{-s} \cdots \sum_{a_{dd}=1}^{\infty} a_{dd}^{d-1-s} \\ &= \zeta(s)\zeta(s-1) \cdots \zeta(s-d+1). \end{aligned}$$

We mention here that Proposition 8.1 can be used to prove that

$$a_1(\mathbb{Z}^2) + \dots + a_N(\mathbb{Z}^d) \sim d^{-1}\zeta(d)\zeta(d-1)\cdots\zeta(2)N^d.$$

It is known that if the group G is solvable, then ζ_G is analytic in a half-plane $\{s \in \mathbb{C} : \operatorname{Re}(s) \geq \alpha(G)\}$. Moreover, if G is a nilpotent group the fact that G is a direct product of its p-Syllow subgroups allows us to decompose ζ_G as a product of local zeta functions, as

$$\zeta_G(s) = \prod_{p \text{ prime}} \zeta_{G,p}(s),$$

where

$$\zeta_{G_p}(s) = \sum_{n \ge 0} a_{p^n}(G) p^{-ns}.$$

Furthermore p-adic integral methods can be used to show that each $\zeta_{G,p}$ is a rational function in p^{-s} . It is an open problem to understand the behavior of $\zeta_{G,p}$ as p varies.

We finish this note by introducing one more zeta function, aimed to count the representations of a group G.

8.2. Zeta functions in representation theory. For a group G, we can let $r_n(G)$ be the number of equivalence classes of n-dimensional representations of G. We can then define the representation zeta function

$$\zeta_G^{\text{rep}}(s) = \sum_{n \ge 1} r_n(G) n^{-s}.$$

References

[Must] Mircea Mustata, Zeta functions in algebraic geometry, lecture notes.

[Popa] Mihnea Popa, Modern aspects of the cohomological study of varieties, lecture notes.

NIKI MYRTO MAVRAKI, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VAN-COUVER, BC V6T 1Z2, CANADA

E-mail address: myrtomav@math.ubc.ca