CHAPTER 7

DISTRIBUTION OF FROBENIUS ANGLES

Let $C/\mathbb{F}_q$ be a smooth projective curve over a finite field $\mathbb{F}_q$. As we have seen earlier, the (complex) zeroes of the zeta functions $Z(C/\mathbb{F}_q, T)$ are all on the circle of radius $|T| = q^{-1/2}$. For various purposes it is important to know more about how those zeroes are distributed on the circle. In this chapter, we give a very basic result about the distribution of zeroes of zeta functions of curves.

7.1. "Frobenius angles" of curves

Let C be a smooth projective curve of genus $g = g(C)$ defined over a finite field $\mathbb{F}_q$. We have seen that we can associate to C a set of $\alpha_j \in \mathbb{C}$, with $j = 1, \dots, 2g$. The functional equation tells us that the set $\{\alpha_1, \dots, \alpha_{2g}\}$ is stable under the map $\alpha \mapsto q/\alpha$. Moreover, by the Riemann Hypothesis of curves, we know that $|\alpha_j| = \sqrt{q}$. Thus, we can fix "angles" $\theta_j(C) \in]-\pi, \pi]$ such that

$$\forall j = 1, \dots, 2g, \qquad \alpha_j = \sqrt{q} \cdot \mathrm{e}^{i\theta_j(C)}.$$

The set $\{\theta_j(C)\}_{j=1,\dots,2g(C)}$ is called the set of Frobenius angles of C (note that we allow elements to have a multiplicity, so it would be better to speak of the multiset of Frobenius angles). The functional equation implies that the set $\{\theta_1(C), \dots, \theta_{2g}(C)\}$ is symmetric around 0 (*i.e.* stable under the map $\theta \mapsto -\theta$).

In this chapter, we are interested in proving more properties of this set of angles. Recall that

$$\sum_{j=1}^{2g} \mathrm{e}^{i\theta_j(C)} = q^{1/2} + q^{-1/2} - \frac{\#C(\mathbb{F}_q)}{q^{1/2}}.$$

Consequently, if we had more information about the arguments of vectors $\mathrm{e}^{i\theta_j(C)} \in \mathbb{C}$, we could deduce a good bound on the left-hand side and thus we could have a better control on $\#C(\mathbb{F}_q)$. On one extreme, if the angles $\theta_j(C)$ are all very close to 0, say, then the sum $\sum_j \mathrm{e}^{i\theta_j(C)}$ (which is a real number) is big (*i.e.* close to $2g$) so that C has very few $\mathbb{F}_q$-rational points (not much more than $q + 1 - 2g\sqrt{q}$). If, on the other extreme, the angles are "almost randomly chosen" in $]-\pi, \pi]$, the sum $\sum_j \mathrm{e}^{i\theta_j(C)}$ is rather small (*i.e.* much smaller than g) so that C has about $q+1$ rational points over $\mathbb{F}_q$.

Obviously, this is very vague, but it shows that results on the distribution of the angles $\theta_j(C)$ can lead to theorems on number of rational points on curves.

7.2. Equidistribution

Let us first give a precise definition for what it means for a set of points (or rather a sequence of sets) to be equidistributed in an interval.

Definition 7.1. — Let $(X_N)_{N\geq 1}$ be a sequence of finite subsets $X_N \subset [0, 2\pi]$, with $\#X_N = N$. We say that the sets X_N become equidistributed in $[-\pi, \pi]$ if and only if, for any interval $[a, b] \subset [-\pi, \pi]$,

$$\lim_{N\to\infty} \frac{\#\{x \in X_N \ : \ x \in [a, b]\}}{\#X_N} = \frac{b-a}{2\pi}.$$

(Note that we here allow elements of X_N to have multiplicities, so maybe it would be better to speak of X_N as a finite sequence of elements of $[0, 2\pi]$). In other words, the sequence X_N becomes equidistributed if (in the limit $N \to \infty$) an interval $[a, b] \subset [-\pi, \pi]$ contains the right proportion of elements of X_N.

Example 7.2. — For any $N \geq 1$, consider the set $X_N := \{-\pi + 2k\pi/N, k \in \{0, \dots, N-1\}\}$. The elements of X_N are "evenly" distributed in $[-\pi, \pi]$. It can be checked that $(X_N)_{N\geq 1}$ becomes equidistributed in $[-\pi, \pi]$ as $N \to \infty$.

The usual way of proving that a sequence (X_N) becomes equidistributed is to use the following criterion:

***Theorem 7.3* (Weyl's criterion)**. — *A sequence $(X_N)_{N\geq 1}$ becomes equidistributed in $[-\pi, \pi]$ if and only if:*

$$\forall k \in \mathbb{Z}_{\geq 1}, \qquad \lim_{N\to\infty} \frac{1}{\#X_N} \sum_{x\in X_N} \mathrm{e}^{ik\cdot x} = 0.$$

The criterion is very useful because it reduces the question of equidistribution to proving bounds about exponential sums. We don't go into the proof of Weyl's criterion, the reader can easily find one.

Example 7.4. — Let $\alpha \in [-\pi, \pi] \smallsetminus \{0\}$. For any $N \geq 1$, consider the set $X_N := \{k\alpha, \ k \in \{1, \dots, N\}\}$ of multiples of α (where $k\alpha$ is to be understood modulo 2π so that $k\alpha \in [-\pi, \pi]$ for all k).

With the help of Weyl's criterion, you can show that (X_N) becomes equidistributed in $[-\pi, \pi]$ if and only if α is not a rational multiple of π.

7.3. Gonality of curves

In the following section, we prove a theorem of equidistribution for the Frobenius angles of some special families of curves. To define them, we introduce a new invariant of curves:

If $f \in \mathbb{F}_q(C)$ is a nonconstant function on a curve C, the field extension $\mathbb{F}_q(C)/\mathbb{F}_q(f)$ is a finite extension (since both fields have transcendance degree 1 over $\mathbb{F}_q$, the extension is at least algebraic; the detailed proof of the finiteness is to be found in [**NX09**, Chap. 3]). So, for all nonconstant rational functions $f \in \mathbb{F}_q(C)$, one can define the degree of f, denoted by $\deg f$, to be the degree of the field extension $[\mathbb{F}_q(C) : \mathbb{F}_q(f)]$.

Definition 7.5. — Let $C/\mathbb{F}_q$ be a smooth projective curve over $\mathbb{F}_q$. The gonality of C, denoted by $\gamma_q(C)$, is the smallest degree of a nonconstant rational function on C:

$$\gamma_q(C) := \min\{\deg f, \ f \in \mathbb{F}_q(C) \smallsetminus \mathbb{F}_q\}.$$

Another point of view on the gonality is the following. A nonconstant rational function $f \in \mathbb{F}_q(C)$ induces an algebraic map $f : C \to \mathbb{P}^1$ (also denoted by f) defined over $\mathbb{F}_q$, which is actually surjective. And $\deg f$ is the the degree of f as a morphism. This means that, for all points $t \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, the preimage $f^{-1}(t) = \{P \in C(\overline{\mathbb{F}_q}) : \ f(P) = t\}$ is nonempty and finite, it has cardinality $\leq d$, and the cardinality is actually $= d$ for almost all t's (*i.e.* for all t except at most finitely many, "the ramification points of f").

For example, $\mathbb{P}^1$ has gonality 1 and a hyperelliptic curve has gonality 2.

With assumption of bounded gonality, one can prove upper bounds on the number of rational points on a curve, without any reference to its genus. We give here two bounds, which are certainly very far from optimal, but more than sufficient for our purpose.

Lemma 7.6. — *Let $C/\mathbb{F}_q$ be a smooth projective curve defined over $\mathbb{F}_q$, whose gonality $\gamma_q(C)$ is less than γ. For all $k \geq 1$, one has*

$$\#C(\mathbb{F}_{q^k}) \leq 2\gamma \cdot q^k.$$

Proof. — Assume that a curve C has gonality γ, and fix a nonconstant rational function $f \in \mathbb{F}_q(C)$ of degree γ. Then, as was mentioned above, the corresponding map $f : C \to \mathbb{P}^1$ is surjective and has finite fibers, each of cardinality $\leq \deg f = \gamma$. The fibers are disjoint, and since f is defined over $\mathbb{F}_q$, the fibers above $t \in \mathbb{P}^1(\mathbb{F}_{q^k})$ cover the whole of $C(\mathbb{F}_{q^k})$. Thus, for all $k \geq 1$:

$$\#C(\mathbb{F}_{q^k}) \leq \sum_{t \in \mathbb{P}^1(\mathbb{F}_{q^k})} \#f^{-1}(t) \leq \gamma \cdot \#\mathbb{P}^1(\mathbb{F}_{q^k}) = \gamma(q^k + 1) \leq 2\gamma \cdot q^k.$$

□

7.4. Equidistribution of Frobenius angles of curves

We can now prove the aforementioned equidistribution theorem.

Theorem 7.7. — *Let $(C_n)_{n\geq 1}$ be a sequence of smooth projective curves over a given finite field $\mathbb{F}_q$, such that their genus $g(C_n) = g_n$ tend to infinity when $n \to \infty$, and that the curves C_n have bounded gonality, i.e. $\exists\ B > 0$ such that $\gamma_q(C_n) \leq B$ for all $n \geq 1$.*

Then the Frobenius angles $\{\theta_j(C_n)\}_{1\leq j\leq 2g_n}$ become equidistributed in $[-\pi, \pi]$ when $n \to \infty$.

Proof. — We use Weyl's criterion to prove equidistribution: let C_n be a curve in the sequence, and $\{\theta_j(C_n)\}$ be its Frobenius angles. To show equidistribution, we need to prove that the exponential sums:

$$\sigma_k(C_n) := \frac{1}{2g_n} \sum_{j=1}^{2g_n} \mathrm{e}^{ik\cdot\theta_j(C_n)}$$

tend to zero when $n \to \infty$, for all integers $k \geq 1$. We have a nice interpretation of $\sigma_k(C_n)$: recall that, for a given $k \in \mathbb{Z}_{\geq 1}$,

$$\sum_{j=1}^{2g_n} \mathrm{e}^{ik\cdot\theta_k(C_n)} = q^{-k/2} \sum_{j=1}^{2g_n} \alpha_j(C_n)^k = \frac{q^k + 1}{q^{k/2}} - \frac{\#C_n(\mathbb{F}_{q^k})}{q^{k/2}}.$$

This identity can be seen as a variant of explicit formula (it gives a link between the zeroes of the zeta function of C_n and the number of $\mathbb{F}_{q^k}$-rational points on C_n). By the triangle inequality

$$|\sigma_k(C_n)| \leq \frac{q^{k/2} + q^{-k/2}}{2g_n} + \frac{\#C_n(\mathbb{F}_{q^k})}{2g_n \cdot q^{k/2}}.$$

For a given (fixed) $k \geq 1$, the first term tends to 0 when $n \to \infty$ (this is true for any sequence of smooth projective curves whose genera $\to \infty$). Now, under one of the assumptions in the theorem, we can use one of Lemmas 7.6 and get an upper bound on $\#C_n(\mathbb{F}_{q^k})$ of the form:

$$\forall k \geq 1,\ \forall n \geq 1, \qquad \#C_n(\mathbb{F}_{q^k}) \leq c(k),$$

where $c(k)$ is a certain function of k, depending on $\gamma_q(C_n) \leq B$ (the main point being that $c(k)$ is entirely independent of the genus of C_n). From this we deduce that

$$\forall k \geq 1, \quad |\sigma_k(C_n)| \leq o(1) + \frac{c(k) \cdot q^{-k/2}}{2g_n} = o(1) \quad (\text{when } n \to \infty).$$

So that, for any integer $k \geq 1$, the exponential sums $\sigma_k(C_n)$ have limit 0 when $n \to \infty$ (under assumption (1) or (2)). Weyl's criterion for equidistribution is thus satisfied, and we can conclude that the theorem holds. □

Example 7.8. — Let us give an example of situation where this theorem applies. Let $(f_n)_{n\geq 1}$ be a sequence of polynomials in $\mathbb{F}_q[x]$. We assume that, for all $n \geq 1$, $f_n(x)$ is monic and squarefree. Suppose that, as $n \to \infty$, we have $\deg f_n \to \infty$.

For all $n \geq 1$, consider the smooth projective hyperelliptic curve $C_n/\mathbb{F}_q$ defined by the affine equation $y^2 = f_n(x)$ (see Homework #2). Then, as $n \to \infty$, the genus of C_n (which is roughly $(\deg f_n)/2$) tends to infinity. And, as was noted above, $\gamma_q(C_n) = 2$ for all n because the rational function $C_n \to \mathbb{P}^1$ extending the function $(x, y) \mapsto x$ has degree 2.

This theorem is obviously a very basic result about the distribution of Frobenius angles. The goal was only to illustrate uses of the explicit formulas and their variants.

CHAPTER 8

FURTHER BOUNDS ON NUMBER OF POINTS

In this chapter, we give two improved bounds on the number of $\mathbb{F}_q$-rational points on curves over $\mathbb{F}_q$.

As a direct consequence of the Riemann Hypothesis for curves (Weil's theorem), we have already stated the so-called "Hasse-Weil bound". More precisely, if $C/\mathbb{F}_q$ is a smooth projective curve of genus g over a finite field $\mathbb{F}_q$, we have

$$-2g \cdot \sqrt{q} \leq \#C(\mathbb{F}_q) - (q+1) \leq 2g \cdot \sqrt{q},$$

or, equivalently,

$$|\#C(\mathbb{F}_q) - (q+1)| \leq \lfloor 2g \cdot \sqrt{q} \rfloor . \tag{14}$$

Here, $\lfloor x \rfloor$ denotes the integral part of a real number x (floor function).

For almost thirty years, there has been close to no investigation as to whether the Hasse-Weil bound is sharp or not (*i.e.* given a curve C of some genus g over a finite field $\mathbb{F}_q$, how close to the upper or lower bound in the Hasse-Weil inequality can $\#C(\mathbb{F}_q) - (q+1)$ actually get?). In the 1980's, new applications of curves over finite fields (to coding theory, to cryptography, etc) were found and they required more precise bounds on the number of rational points. In particular, for various applications, it is important to find curves over $\mathbb{F}_q$ with many $\mathbb{F}_q$-rational points and a moderate genus g. That is to say, given a finite field $\mathbb{F}_q$ and an integer $g \geq 1$, we would like to find a curve a (smooth projective) curve C of genus g defined over $\mathbb{F}_q$ with $\#C(\mathbb{F}_q)$ as big as is allowed by the Hasse-Weil bound, or at least to know if such a curve can exist at all.

8.1. Serre's bound

We start by stating a slight improvement on (14), proven by Jean Pierre Serre around 1982:

***Theorem 8.1* (Serre's bound).** — *Let $\mathbb{F}_q$ be a finite field, and $C/\mathbb{F}_q$ a smooth projective curve of genus g. Then, for all $n \geq 1$,*

$$|\#C(\mathbb{F}_{q^n}) - (q^n+1)| \leq g \cdot \left\lfloor 2q^{n/2} \right\rfloor . \tag{15}$$

As usual, we denote by $L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ the numerator of the zeta function of $C/\mathbb{F}_q$, and we fix complex numbers α_j such that $L(C/\mathbb{F}_q, T) = \prod_{j=1}^{2g}(1 - \alpha_j \cdot T)$. Note that we may (and will) assume that $g > 0$, since there is nothing to prove if $g = 0$. We make two preliminary observations:

Lemma 8.2. — *It is possible to choose a numbering of the α_j's such that*

$$\text{for all } j = 1, \ldots, g, \quad \alpha_{j+g} = \overline{\alpha_j} = \frac{q}{\alpha_j}.$$

In the following, we will assume that such an ordering has been chosen.

Proof. — First note that, by the Riemann hypothesis, $\alpha_j \cdot \overline{\alpha_j} = |\alpha_j|^2 = q$ for all $j = 1, \dots, 2g$ (here, the bar denotes complex conjugation).

There is an even number $2g$ of α_j's, and we basically need to show that we can pair them up. Given $j \in \{1, \dots, 2g\}$, either α_j is real or it is distinct from its complex conjugate $\overline{\alpha_j}$. When α_j is real, since $|\alpha_j| = \sqrt{q}$, it has to be $\pm\sqrt{q}$. If $\alpha_j \notin \mathbb{R}$, we pair it with $\overline{\alpha_j}$. Among the remaining even number of α_j, which are real, we need to show that there is an even number of "$+\sqrt{q}$" and an even number of "$-\sqrt{q}$". By construction of the α_j's, we know that $\prod_{j=1}^{2g} \alpha_j$ is the leading coefficient of $L(C/\mathbb{F}_q, T)$, which is $= q^g$ by the functional equation. In particular, there has to be an even number of $\alpha_j = -\sqrt{q}$ (otherwise, the product $\prod_{j=1}^{2g} \alpha_j$ would be negative). So we have proved that, among the α_j which are real, there is an even number of $-\sqrt{q}$ and thus, an even number of $+\sqrt{q}$. In other words, the orders of vanishing of $T \mapsto L(C/\mathbb{F}_q, T)$ at $T = \sqrt{q}$ and at $T = -\sqrt{q}$ are even.

This proves that there exists a way of numbering the α_j's such that the desired property holds. □

Lemma 8.3. — *For all $j = 1, \dots, g$, the number α_j is an algebraic integer.*

Proof. — Write $L(C/\mathbb{F}_q, T) = \sum a_i \cdot T^i \in \mathbb{Z}[T]$, and let $f(T) = T^{2g} \cdot L(C/\mathbb{F}_q, 1/T)$. A straightforward computation shows that

$$f(T) = \sum_{i=0}^{2g} a_{2g-i} \cdot T^i = T^{2g} + a_1 \cdot T^{2g-1} + \cdots + a_{2g-1} \cdot T + q^g.$$

In particular, $f(T)$ is a nonzero monic polynomial with integer coefficients. By definition of $f(T)$, each α_j is a root of $f(T)$.

In other words, for $j \in \{1, \dots, 2g\}$, there exists a nonzero monic polynomial with integer coefficients (namely $f(T)$) which vanishes at α_j. This is exactly saying that α_j is an algebraic integer. □

Proof of Theorem 5.1. — We can now give the proof of Serre's bound. We assume that $g > 0$, and we arrange the α_j's such that $\alpha_{j+g} = q/\alpha_j$ for $j = 1, \dots, g$. We put $M := \lfloor 2\sqrt{q} \rfloor \in \mathbb{Z}_{\geq 1}$ and, for any $j = 1, \dots, g$,

$$x_j := \alpha_j + \alpha_{j+g} + M + 1 \in \mathbb{C}.$$

Then x_j is a real number, because it is invariant under complex conjugation. Moreover, by the Riemann Hypothesis for curves,

$$x_j \geq M + 1 - |\alpha_j + \alpha_{j+g}| \geq M + 1 - 2\sqrt{q} > 0.$$

Now define $X := \prod_{j=1}^{g} x_j$: by the above, X is a real positive number. Actually, I claim that X is an integer. Assuming that claim for the time being, let us prove that it yields the Theorem. Since X is a positive integer, it has to be ≥ 1. Now, by the inequality between the arithmetic and geometric means, one has

$$\frac{1}{g} \sum_{j=1}^{g} x_j \geq \left(\prod_{j=1}^{g} x_j \right)^{1/g} = X^{1/g} \geq 1.$$

This implies that

$$M + 1 - \frac{1}{g} \left(\#C(\mathbb{F}_q) - q - 1 \right) = \frac{1}{g} \sum_{j=1}^{g} x_j \geq 1.$$

And reordering the terms, we obtain one half of the Theorem:

$$\#C(\mathbb{F}_q) - q - 1 \leq g \cdot M.$$

To prove the corresponding lower bound, we repeat the same argument with the x_j's replaced by

$$y_j := M + 1 - (\alpha_j + \alpha_{j+g}), \qquad \forall j = 1, \dots, g,$$

and we deduce that

$$M + 1 + \frac{1}{g}\left(\#C(\mathbb{F}_q) - q - 1\right) = \frac{1}{g}\sum_{j=1}^{g} y_j \geq 1,$$

which yields the other half of the Theorem: $\#C(\mathbb{F}_q) - q - 1 \geq -g \cdot M$.

Now it remains to prove the claim that X is an integer. Note first that each x_j is an algebraic integer (since it is defined as a sum of algebraic integers), so their product X is also an algebraic integer. Now, seen as an algebraic number, $X \in \overline{\mathbb{Q}}$ is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so X must be a rational number. But an algebraic integer which is rational is an element of $\mathbb{Z}$! So $X \in \mathbb{Z}$, as was to be shown. □

More generally, the samed sort of argument would give the following fact (left as an exercise):

Lemma 8.4. — *Let $S = \{\alpha_1, \dots, \alpha_s\}$ a set of s algebraic integers, such that there exists an odd integer ω for which $|\alpha_i| = p^{\omega/2}$ for all i. We assume that S is stable under the action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then, s is even and*

$$|\alpha_1 + \cdots + \alpha_s| \leq \frac{s}{2} \cdot \left\lfloor 2p^{\omega/2} \right\rfloor.$$

8.2. Ihara's bound

We now state and prove an improvement on Serre's bound:

***Theorem 8.5* (Ihara)**. — *Let $\mathbb{F}_q$ be a finite field, and $C/\mathbb{F}_q$ a smooth projective curve of genus g. Then,*

$$\#C(\mathbb{F}_q) \leq q + 1 + g \cdot \left(\sqrt{2q} - \frac{1}{2}\right). \tag{16}$$

This bound is based on the simple observation that, for a curve C defined over $\mathbb{F}_q$, one has $C(\mathbb{F}_q) \subset C(\mathbb{F}_{q^2})$, so that $\#C(\mathbb{F}_q) \leq \#C(\mathbb{F}_{q^2})$. Note that (16) provides only an upper bound, whereas (14) and (15) also gave lower bounds (but see the end of the proof).

Proof. — Consider a smooth projective curve C of genus g defined over $\mathbb{F}_q$. Let $N = \#C(\mathbb{F}_q)$ and denote by $\{\alpha_j\}_{j=1,\dots,2g}$ the set of inverse roots of $L(C/\mathbb{F}_q, T)$ (numbered as before). As was observed earlier, one has:

$$N = \#C(\mathbb{F}_q) \leq \#C(\mathbb{F}_{q^2}) = q^2 + 1 - \sum_{j=1}^{2g} {\alpha_j}^2 = q^2 + 1 - \sum_{j=1}^{g} ({\alpha_j}^2 + \overline{\alpha_j}^2). \tag{17}$$

Since $\alpha_j \cdot \overline{\alpha_j} = q$, one has ${\alpha_j}^2 + \overline{\alpha_j}^2 = (\alpha_j + \overline{\alpha_j})^2 - 2q$, for all $j = 1, \dots, g$. By the Cauchy-Schwarz inequality,

$$\left(\sum_{j=1}^{2g} \alpha_j\right)^2 = \left(\sum_{j=1}^{g} (\alpha_j + \overline{\alpha_j})\right)^2 \leq g \cdot \sum_{j=1}^{g} (\alpha_j + \overline{\alpha_j})^2 = g \cdot \left(2q \cdot g + \sum_{j=1}^{g} ({\alpha_j}^2 + \overline{\alpha_j}^2)\right).$$

Plugging this inequality into (17), and remembering that $\sum_{j=1}^{2g} \alpha_j = q + 1 - N$, we obtain that

$$N \leq q^2 + 1 - 2g \cdot q - \frac{1}{g} \cdot (q + 1 - N)^2,$$

which can be rewritten as

$$\phi(N) := N^2 + (g - 2q - 2) \cdot N + (q + 1)^2 + 2g^2 \cdot q - g(q^2 + 1) \leq 0.$$

Now the map $x \mapsto \phi(x)$ is a quadratic polynomial in $x \in \mathbb{R}$ and has a positive leading coefficient. Let $z_- < z_+$ be the roots of ϕ in $\mathbb{R}$. Since $\phi(N) \leq 0$, N is in the interval $[z_-, z_+] \subset \mathbb{R}$. Writing out explicitely the values of z_- and z_+ in terms of g and q, we obtain that

$$N - (q+1) \leq z_+ - (q+1) = \frac{1}{2}\left(-g + \sqrt{(8q+1)g^2 - 4g \cdot q(q-1)}\right).$$

And straightforward inequalities imply that

$$\frac{1}{2}\left(-g + \sqrt{(8q+1)g^2 - 4g \cdot q(q-1)}\right) \leq g \cdot \left(\sqrt{2q} - \frac{1}{2}\right).$$

Note that one could also get a lower bound on N by working out the value of z_- (exercise). □

Remark 8.6. — Ihara's bound is finer than the Hasse-Weil bound when

$$g > \frac{\sqrt{q}(\sqrt{q}-1)}{2},$$

as follows from a simple computation. That is to say, (16) gives a better upper bound on $\#C(\mathbb{F}_q)$ than (14) when the genus is big with respect to q. This means that (16) is interesting only in the "large genus limit".

As an explicit example, let $q = 2$ and $g = 100$. The Hasse-Weil bound gives $N_2(100) \leq 285$, Serre's bound gives $N_2(100) \leq 203$ and Ihara's gives $N_2(100) \leq 150$. Knowing only the Hasse-Weil bound, we could start looking for a curve of genus 100 over $\mathbb{F}_2$ with, say, 151 rational points. But Ihara's bound tells us that such a curve can not exist!