5.6. Proof of Theorem 5.8 and its Corollary

Before we give the proof, let us explain how explicit formulas lead to (upper) bounds on the number of rational points on curves.

Example 5.13. — Consider the trigonometric polynomial

$$f(\mathrm{e}^{i\theta}) := \frac{1}{2} \cdot (1 + \sqrt{2} \cdot \cos\theta)^2 = 1 + \sqrt{2} \cdot \cos\theta + \frac{1}{2} \cdot \cos(2\theta).$$

The second expression follows from the first by an esay computation involving some trigonometric identities. This map $f(\mathrm{e}^{i\theta})$ corresponds to

$$F(t) = \frac{1}{\sqrt{2}} \cdot t + \frac{1}{4} \cdot t^2.$$

We apply the explicit formula to this $F(t)$ (*i.e.* for the choice $c_1 = 1/\sqrt{2}$ and $c_2 = 1/4$). Recall that $\#C(\mathbb{F}_q) \leq \#C(\mathbb{F}_{q^2})$, so that

$$F(\sqrt{q}^{-1}) \cdot \#C(\mathbb{F}_q) \leq \frac{c_1}{\sqrt{q}} \cdot \#C(\mathbb{F}_q) + \frac{c_2}{q} \cdot \#C(\mathbb{F}_{q^2}) = \sum_{n\geq 1} \frac{c_n \cdot \#C(F_{q^n})}{q^{n/2}}.$$

Notice that, by construction, $f(\mathrm{e}^{i\theta}) \geq 0$ for all $\theta \in [0,\pi]$: this yields

$$g - \sum_{j=1}^{g} f(\mathrm{e}^{i\theta_j}) \leq g.$$

Together with these two bound, the explicit formula leads to

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

Plugging in the definition of $F(t)$, we get

$$\#C(\mathbb{F}_q) \leq 1 + \frac{4q \cdot g + q^2 + 1 + \sqrt{8q}(q+1)}{\sqrt{8q} + 1}.$$

If one assumes that $g \leq (q-1) \cdot \sqrt{q/2}$, this simplifies to

$$\#C(\mathbb{F}_q) \leq q^2 + 1.$$

We have thus obtained an upper bound on $\#C(\mathbb{F}_q)$, which is slightly better that the Hasse-Weil bound, when the genus is “not too big” with respect to q. In other words,

$$\text{If } g \leq (q-1) \cdot \sqrt{q/2}, \qquad N_q(g) \leq q^2 + 1.$$

In this range of g, the Hasse-Weil bound would only give that

$$N_q(g) \leq \frac{q^2}{\sqrt{2}} + q + 1.$$

Example 5.14. — With the same sort of arguments one could also prove the following upper bound:

$$\text{If } g \leq \frac{q-1}{2} \cdot \sqrt{q} \cdot \left(\sqrt{3(q-1)} + \sqrt{q}\right), \qquad N_q(g) \leq q^3 + 1.$$

The proof is left as an exercise. You may use the trigonometric polynomial

$$f(\mathrm{e}^{i\theta}) = \frac{1}{3} \cdot (\cos\theta)^2 \cdot \left(\sqrt{3} + 2 \cdot \cos\theta\right)^2.$$

In both examples above, we get a good bound on $N_q(g)$ when g is “not too big” compared to q. But to prove Theorem 5.8 (and especially its Corollary 5.9), we typically need to get rid of this constraint (since $A(q)$ is an asymptotic invariant defined “in the large genus limit”, *i.e.* when $g \to \infty$).

Lemma 5.15. — *Let $F(t) = \sum_{n\geq 1} c_n t^n \in \mathbb{R}[t]$ be a polynomial as above, and $f(\mathrm{e}^{i\theta})$ be the associated "trigonometric function". Assume that*

(1) $c_n \geq 0$ for all $n \geq 1$ *(2) $f(\mathrm{e}^{i\theta}) \geq 0$ for all $\theta \in [0, \pi]$.*

Then, any smooth projective curve $C/\mathbb{F}_q$ of genus g satisfies

$$\#C(\mathbb{F}_q) \leq N_q(g) \leq 1 + \frac{g + F(\sqrt{q})}{F(\sqrt{q}^{-1})}.$$

Proof. — Using assumption (1) and the "growth condition" $\#C(\mathbb{F}_{q^n}) \geq \#C(\mathbb{F}_q)$ (for all $n \geq 1$), we get that

$$F(\sqrt{q}^{-1}) \cdot \#C(\mathbb{F}_q) = \sum_{n\geq 1} \frac{c_n \cdot \#C(F_q)}{q^{n/2}} \leq \sum_{n\geq 1} \frac{c_n \cdot \#C(F_{q^n})}{q^{n/2}}.$$

On the right-hand side of the explicit formula, we use assumption (2):

$$g - \sum_{j=1}^{g} f(\mathrm{e}^{i\theta_j}) \leq g.$$

Using the explicit formula to link these two inequalities we obtain that

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

Which is exactly what we need (note that $F(\sqrt{q}^{-1}) > 0$). □

Lemma 5.16. — *Under assumptions (1) and (2) in the previous lemma, one has*

$$A(q) \leq \frac{1}{F(\sqrt{q}^{-1})}.$$

Proof. — By definition of $A(q)$, the lemma follows directly from the previous one, upon taking the limit when $g \to \infty$. □

It remains to find a "good" test function F. We want to find coefficients c_n such that F satisfies both (1) and (2), and such that the bounds in Lemmas 5.15 and 5.16 are as good as possible.

As a first observation, note that the bound in Lemma 5.16 is tighter when $F(\sqrt{q}^{-1})$ is bigger. So we need to choose the coefficients c_n as big as possible. However, note that assumption (2) implies:

$$1 - c_n = \frac{1}{\pi} \int_0^{\pi} f(\mathrm{e}^{i\theta}) \cdot (1 - \cos(n\theta))\mathrm{d}\theta \geq 0,$$

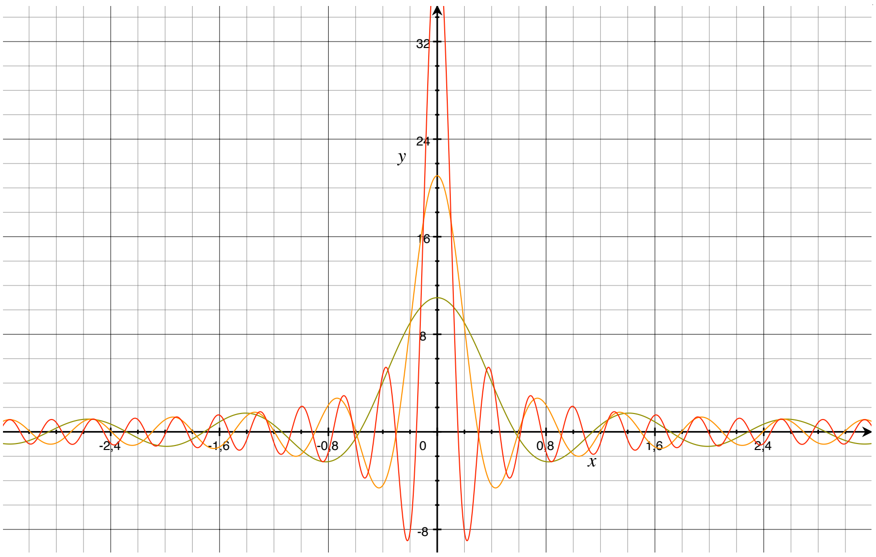
so that $0 \leq c_n \leq 1$, with (1). To maximize $F(\sqrt{q}^{-1})$, the best we can do is thus to choose $c_n = 1$ for all $n \geq 1$. But $F(t)$ has to be a polynomial, so we can not really do this because almost all c_n have to be 0. What we can do however, is to "cut-off" this first choice: let $c_n = 1$ for all $n = 1, \ldots, N$ and $c_n = 0$ for all $n > N$ (for some parameter $N \geq 1$). That is to say, choose

$$F_N(t) = \sum_{n=1}^{N} t^n = \frac{t(t^N - 1)}{t - 1}.$$

In that situation, a straightforward computation leads to

$$f_N(\mathrm{e}^{i\theta}) = \frac{\cos(N\theta) - \cos((N+1)\theta)}{1 - \cos\theta}.$$

Hypothesis (1) is satisfied in this case, but not (2)! Here are graphs of f_N on $[-\pi, \pi]$ for different values of N ($N = 5$ in green, $N = 10$ in orange and $N = 20$ in red):



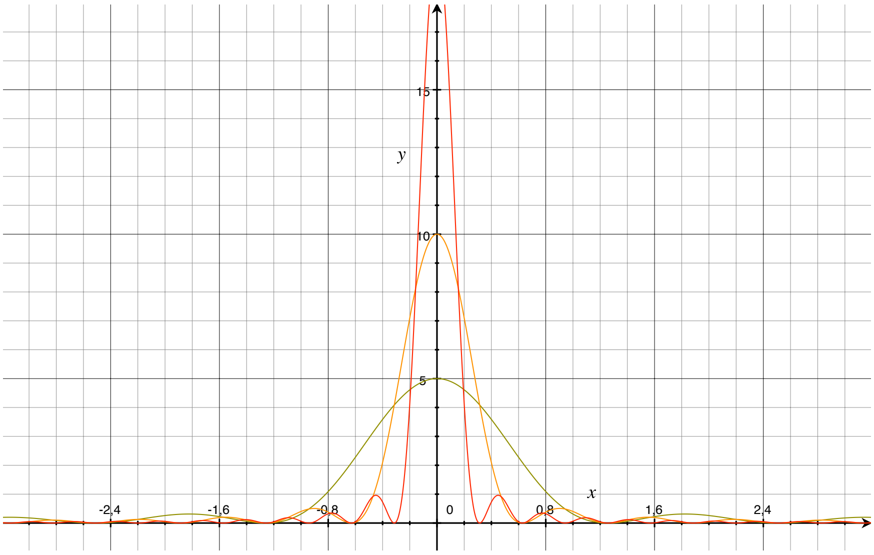
So we need to be somewhat more subtle in the choice of c_n. We choose the next best $F(t)$, which has coefficients that are "close to 1" but still satisfies (2). For a parameter $N \in \mathbb{Z}_{\geq 1}$, let

$$F_N(t) := \sum_{n=1}^{N} \left(1 - \frac{n}{N}\right) t^n.$$

Then, $F_N(t)$ satisfies (1), and a quick computation shows that

$$f_N(\mathrm{e}^{i\theta}) = \frac{1}{N} \cdot \frac{1 - \cos(N\theta)}{1 - \cos\theta},$$

which shows that assumption (2) is also satisfied here! You might recognize from Fourier analysis that f_N is essentially the Féjer kernel. For comparison, here are graphs of f_N on $[-\pi, \pi]$ for $N = 5, 10, 20$:



Using Lemma 5.15 with this choice of F_N gives that,

$$\forall N \geq 1, \qquad \#C(\mathbb{F}_q) \leq N_q(g) \leq 1 + \frac{F_N(\sqrt{q}) + g}{F_N(\sqrt{q}^{-1})}.$$

This bound is exactly the Drinfeld-Vladuts bound (for $N = k + 1$). To deduce Corollary 5.9, it suffices to take a limit as $N \to \infty$ after dividing by g. More precisely, the last displayed equation implies that

$$\forall N \geq 1, \qquad \frac{N_q(g)}{g} \leq \frac{1}{F_N(\sqrt{q}^{-1})} + \frac{1}{g} \cdot \left(1 + \frac{F_N(\sqrt{q})}{F_N(\sqrt{q}^{-1})}\right).$$

Now, remark that

$$\lim_{N\to\infty} F_N(\sqrt{q}^{-1}) = \frac{1}{\sqrt{q}-1}.$$

For any $\epsilon > 0$, choose N_0 such that

$$\forall N \geq N_0, \qquad F_N(\sqrt{q^{-1}})^{-1} \leq \sqrt{q} - 1 + \frac{\epsilon}{2}$$

and g_0 such that

$$\forall g \geq g_0, \qquad \frac{1}{g} \cdot \left(1 + \frac{F_{N_0}(\sqrt{q})}{F_{N_0}(\sqrt{q}^{-1})}\right) \leq \frac{\epsilon}{2}.$$

We have proved that, for all $\epsilon > 0$, there is a g_0 such that, for all $g \geq g_0$,

$$\frac{N_q(g)}{g} \leq \sqrt{q} - 1 + \epsilon.$$

This assertion is equivalent to

$$A(q) \leq \sqrt{q} - 1.$$

This concludes the proof of Corollary 5.9.

5.7. Another application of explicit formulas

To conclude this chapter and to illustrate how useful explicit formulas can be, let us give a very basic result about the distribution of zeroes of zeta functions of curves.

5.7.1. "Frobenius angles" of curves. — Let C be a smooth projective curve of genus g 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 $j = 1, \ldots, 2g$. The functional equation tells us that the set $\{\alpha_1, \ldots, \alpha_{2g}\}$ 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

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

Note that these angles are not quite the same as those we used before. The functional equation implies that the set $\{\theta_1(C), \ldots, \theta_{2g}(C)\}$ is symmetric around 0 (*i.e.* stable under the map $\theta \mapsto -\theta$).

In this section, 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 a lot of $\mathbb{F}_q$-rational points (almost $q + 1 + 2g\sqrt{q}$). 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 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.

5.7.2. 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 5.17. — 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 $[0, 2\pi]$ if and only if, for any interval $[a, b] \subset [0, 2\pi]$,

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

(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 $[a, b] \subset [0, 2\pi]$ contains the right proportion of elements of X_N.

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

***Theorem 5.18* (Weyl's criterion).** — *A sequence $(X_N)_{N\geq 1}$ becomes equidistributed in $[0, 2\pi]$ 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.

5.7.3. Two invariants of curves. — In the following subsection, we prove a theorem of equidistribution for the Frobenius angles of somes special families of curves. To define them, we introduce two new invariants for curves:

Definition 5.19. — Let $C/\mathbb{F}_q$ be a smooth projective curve over $\mathbb{F}_q$. The $\mathbb{F}_q$-dimension of C, denoted by $\mathcal{D}_q(C)$, is the smallest integer $m \geq 1$ such that there is an embedding $C \hookrightarrow \mathbb{P}^m$ defined over $\mathbb{F}_q$.

For example, $\mathcal{D}_q(\mathbb{P}^1) = 1$. For a less trivial example, consider the affine curve $C_0/\mathbb{F}_q$ defined by

$$C_0 \subset \mathbb{A}^2 : \qquad y^2 + y = x^3 + 1,$$

C_0 is smooth, and its projectivization $C \subset \mathbb{P}^2$ (see previous chapters) is also smooth. So that C can be embedded into $\mathbb{P}^2$ in a smooth manner, over $\mathbb{F}_q$. So $\mathcal{D}_q(C) = 2$. More generally, if C_0 is an affine plane curve $\subset \mathbb{A}^2$ (so C_0 is given by one equation) and if the projective closure $C \subset \mathbb{P}^2$ of C in $\mathbb{P}^2$ is smooth, then $\mathcal{D}_q(C) \leq 2$. Note that there are curves with larger $\mathbb{F}_q$-dimension.

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 5.20. — 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").

With assumption of bounded $\mathbb{F}_q$-dimension or 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 5.21. — *Let $C/\mathbb{F}_q$ be a smooth projective curve defined over $\mathbb{F}_q$, whose $\mathbb{F}_q$-dimension $\mathcal{D}_q(C)$ is less than M. For all $k \geq 1$, one has*

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

Proof. — Fix an embedding $C \subset \mathbb{P}^m$ (with $m \leq M$). Then $\#C(\mathbb{F}_{q^k}) \leq \#\mathbb{P}^m(\mathbb{F}_{q^k})$ and

$$\#C(\mathbb{F}_{q^k} \leq \frac{q^{mk}-1}{q^k-1} = q^{(m-1)k} + q^{(m-2)k} + \cdots + q^k + 1 \leq mq^{(m-1)k} \leq Mq^{Mk}.$$

□

Lemma 5.22. — *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 $k \geq 1$:

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

□

5.7.4. Equidistribution of Frobenius angles of curves. — We can now prove the aforementioned equidistribution theorem.

Theorem 5.23. — *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 $n \to \infty$. Assume one of the following:*

(1) either the curves C_n have bounded $\mathbb{F}_q$-dimension, i.e. $\exists\ M > 0$, $\mathcal{D}_q(C_n) \leq M$ for all $n \geq 1$.
(2) or the curves C_n have bounded gonality, i.e. $\exists\ \gamma > 0$ such that $\Gamma_q(C_n) \leq \gamma$ for all $n \geq 1$.

Then the Frobenius angles $\{\theta_j(C_n)\}_{1\leq j\leq 2g_n}$ become equidistributed 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 $k \geq 1$. Luckily, 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). So that, 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 5.21 or 5.22, 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 M or γ (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. □

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.