CHAPTER 5

FURTHER BOUNDS ON THE NUMBER OF RATIONAL POINTS

In this chapter, we give various 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 in the previous chapter), 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,

$$|\#C(\mathbb{F}_q) - (q+1)| \leq \lfloor 2g \cdot \sqrt{q} \rfloor . \tag{12}$$

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.

5.1. Serre's bound

We start by stating a slight improvement on (12), proven by Jean Pierre Serre around 1982:

***Theorem 5.1* (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 $n \geq 1$,*

$$|\#C(\mathbb{F}_{q^n}) - (q^n+1)| \leq g \cdot \left\lfloor 2q^{n/2} \right\rfloor . \tag{13}$$

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 5.2. — *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 5.3. — *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 5.4. — *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*

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

5.2. Two new quantities

Let $\mathbb{F}_q$ be a finite field, we introduce two quantities, that are meant to measure the quality of the upper bounds on the number of $\mathbb{F}_q$-rational points on a curve.

First, for an integer $g \geq 1$, let us define

$$N_q(g) := \max_C \#C(\mathbb{F}_q),$$

the max being taken on all smooth projective curves C of genus g defined over $\mathbb{F}_q$. Upper bounds on the number of $\mathbb{F}_q$-rational points on curves of a given genus g can be turned into an upper bound on $N_q(g)$.

Definition 5.5. — Let $\mathbb{F}_q$ be a finite field. One says that a smooth projective curve $C/\mathbb{F}_q$ of genus g is maximal (resp. minimal) if $\#C(\mathbb{F}_q)$ is maximal (resp. minimal) among the number of $\mathbb{F}_q$-rational points on curves of genus g defined over $\mathbb{F}_q$. In other words, C is maximal if and only if

$$\#C(\mathbb{F}_q) = N_q(g) = \max\left\{\#C'(\mathbb{F}_q),\ C'/\mathbb{F}_q \text{ curve of genus } g\right\}.$$

Secondly, we introduce an asymptotic invariant:

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

As a concrete example of the meaning of this definition, assume that, for some $\mathbb{F}_q$, we have proved an equality $A(q) = a > 0$: this would mean that there is an infinite sequence of genera $(g_i)_{i \geq 1}$ (with $g_i \to \infty$ as $i \to \infty$) and an infinite sequence of smooth projective curves $(C_i)_{i \geq 1}$ defined over $\mathbb{F}_q$, with $C_i/\mathbb{F}_q$ of genus g_i, and such that

$$\#C_i(\mathbb{F}_q) \sim a \cdot g_i \qquad (\text{as } i \to \infty).$$

For example, the Hasse-Weil bound implies that

$$\forall g \geq 1, \quad N_q(g) \leq q + 1 + 2g \cdot \sqrt{q}, \quad \text{ and thus, } A(q) \leq 2\sqrt{q}.$$

And Serre's bound yields the (slightly) better bound $A(q) \leq \left\lfloor 2\sqrt{q} \right\rfloor$, which improves on the previous upper bound when q is not a square.

5.3. Ihara's bound

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

***Theorem 5.6* (Ihara).** — *Let $\mathbb{F}_q$ be a finite field, and $C/\mathbb{F}_q$ a smooth projective curve of genus g. Then, for all $n \geq 1$,*

$$\#C(\mathbb{F}_{q^n}) - (q^n + 1) \leq g \cdot \left(\sqrt{2} \cdot q^{n/2} - \frac{1}{2}\right). \tag{14}$$

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 (14) provides only an upper bound, whereas (12) and (13) also gave lower bounds. In any case, (14) implies that

$$A(q) \leq \sqrt{2q} - \frac{1}{2}.$$

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:

$$N = \#C(\mathbb{F}_q) \leq \#C(\mathbb{F}_{q^2}) = q^2 + 1 - \sum_{j=1}^{2g} {\alpha_j}^2 = q^2 + 1 - \sum_{j=1}^{g} ({\alpha_j}^2 + \overline{\alpha_j}^2). \tag{15}$$

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 (15), 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 5.7*.** — 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, (14) gives a better upper bound on $\#C(\mathbb{F}_q)$ than (12) when the genus is big with respect to q. This means that (14) is interesting only in the "large genus limit". For instance, this is precisely the asymptotic setting for the definition of $A(q)$.

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!

5.4. Drinfeld-Vladuts' bound

In the proof of the previous theorem, instead of using that $\#C(\mathbb{F}_{q^2}) \geq \#C(\mathbb{F}_q)$, we could have remarked that, for all $k \geq 1$, one has $\#C(\mathbb{F}_{q^k}) \geq \#C(\mathbb{F}_q)$. Working out the details leads to the more general theorem:

***Theorem 5.8* (Drinfeld - Vladuts).** — *Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g. Then, for all $k \geq 1$,*

$$\#C(\mathbb{F}_q) \leq 1 + \frac{g + \sum_{j=1}^{k} \left(1 - \frac{j}{k+1}\right) \cdot q^{j/2}}{\sum_{j=1}^{k} \left(1 - \frac{j}{k+1}\right) \cdot q^{-j/2}}. \tag{16}$$

This theorem is also more flexible than the previous one. Indeed, we have a parameter $k \geq 1$ that we can choose to optimize the right-hand side.

For example, again with $q = 2$ and $g = 100$, it appears that $k = 8$ gives the best possible upper bound: (16) leads to $N_2(100) \leq 77$ (which is almost 4 times as small as the Hasse-Weil bound!).

***Corollary 5.9*.** — *Given a finite field $\mathbb{F}_q$, one has*

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

This follows easily from (16). Note the drastic improvement on the bound we started from: Hasse-Weil only gives that $A(q) \leq 2\sqrt{q}$.

It turns out that this upper bound is optimal in a sense: it is attained when q is a square. Indeed, Ihara has proved that, if q is a square, $A(q) = \sqrt{q} - 1$. This theorem was reproved in 1995 by Garcia and Stichtenoth in a completely explicit manner. They exhibited an explicit sequence of curves $C_i/\mathbb{F}_q$ (indexed by $i \in \mathbb{Z}_{\geq 1}$), with unbounded genus (*i.e.* $g(C_i) \to \infty$ as $i \to \infty$) such that

$$\frac{\#C_i(\mathbb{F}_q)}{g(C_i)} \longrightarrow \sqrt{q} - 1 \qquad (\text{as } i \to \infty).$$

5.5. Explicit formulas

Before we give the proof of Theorem 5.8, we introduce a new tool.

***Remark 5.10*.** — In the theory of the classical zeta function $\zeta(s)$, an "explicit formula" is a relation between

- a weighted sum over prime numbers,
- a weighted sum over zeroes of $\zeta(s)$.

Below, we give a similar relation in the setting of curves over finite fields. The analytic difficulties almost entirely disappear in the case of zeta functions of curves, because their analytic behaviour is much better.

Let $C/\mathbb{F}_q$ be a smooth projective curve of genus $g \geq 1$ defined over a finite field $\mathbb{F}_q$. For all $n \geq 1$, we put $N_n := \#C(\mathbb{F}_{q^n})$. As before, we denote by $\alpha_1, \ldots, \alpha_{2g}$ the inverse roots of the

L-function $L(C/\mathbb{F}_q, T)$ of $C/\mathbb{F}_q$. Then, for all $n \geq 1$, we have

$$N_n = \#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{2g} {\alpha_j}^n.$$

Dividing by $q^{n/2}$ yields

$$\frac{N_n}{q^{n/2}} = q^{n/2} + q^{-n/2} - \sum_{j=1}^{2g} \left(\frac{\alpha_j}{\sqrt{q}}\right)^n.$$

Now, by the Riemann Hypothesis for curves, we can pick "angles" $\theta_j \in [0, \pi]$ $(j = 1, \ldots, g)$ such that

$$\alpha_j = \sqrt{q} \cdot \mathrm{e}^{i\theta_j}, \quad \text{and} \quad \alpha_{j+g} = \overline{\alpha_j} = \sqrt{q} \cdot \mathrm{e}^{-i\theta_j}.$$

Writing the previous relations in terms of these angles leads to:

$$\forall n \geq 1, \qquad \frac{N_n}{q^{n/2}} = q^{n/2} + q^{-n/2} - 2 \cdot \sum_{j=1}^{g} \cos(n\theta_j). \tag{17}$$

We now take a "weighted sum" of these equalities for various $n \geq 1$. More precisely, given a polynomial $F(t) = \sum_n c_n t^n \in \mathbb{R}[t]$ with real coefficients, we define a trigonometric polynomial f by:

$$\forall \theta, \quad f(\mathrm{e}^{i\theta}) := 1 + F(\mathrm{e}^{i\theta}) + F(\mathrm{e}^{-i\theta}) = 1 + 2 \cdot \sum_n c_n \cdot \cos(n\theta).$$

For each n, we multiply (17) by c_n, then we sum the resulting identities over n: we obtain the following result.

***Proposition 5.11* (Explicit formulas).** — *To any polynomial $F(t) = \sum c_n t^n \in \mathbb{R}[t]$, associate a trigonometric polynomial $f(\mathrm{e}^{i\theta})$ as above. Then*

$$\sum_{n \geq 1} c_n \cdot \frac{\#C(\mathbb{F}_{q^n})}{q^{n/2}} = F(q^{1/2}) + F(q^{-1/2}) + g - \sum_{j=1}^{g} f(\mathrm{e}^{i\theta_j}). \tag{18}$$

This explicit formula is a very useful tool, because it relates the number of rational points on C on various extensions of $\mathbb{F}_q$ to the "angular" distribution of zeroes of $Z(C/\mathbb{F}_q, T)$. It is also very flexible because one can still choose various polynomials $F(t)$ best adapted to our purpose.

***Example 5.12*.** — Let us start by giving a "trivial example" of use for Proposition 5.11. Choose $F(t) = t$: then $f(\mathrm{e}^{i\theta}) = 1 + 2\cos\theta$ and formula (18) reads

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

Using that $|\cos\theta| \leq 1$ for all $\theta \in [0, \pi]$, we deduce that

$$\left| \frac{\#C(\mathbb{F}_q)}{q^{1/2}} - q^{1/2} - q^{-1/2} \right| \leq 2g,$$

which is exactly... the Hasse-Weil bound. One might hope that a more clever choice of $F(t)$ leads to a better bound on $\#C(\mathbb{F}_q)$. And indeed, we will see that the Drinfeld-Vladuts bound follows from Proposition 5.11 when applied to a good $F(t)$.