CHAPTER 5

THE RIEMANN HYPOTHESIS FOR CURVES OVER FINITE FIELDS

We now turn to the statement and the proof of the main theorem in this course, namely the Riemann hypothesis for curves over finite fields.

More precisely, we prove the following theorem

Theorem 5.1 **(Weil)**. — *Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g, defined over a finite field $\mathbb{F}_q$. Denote by $L(C/\mathbb{F}_q, T)$ the numerator of its zeta function and write this polynomial as a product*

$$L(C/\mathbb{F}_q, T) = \prod_{j=1}^{2g} (1 - \alpha_j \cdot T).$$

Then $|\alpha_j| = \sqrt{q}$ for all $j = 1, \dots, 2g$.

The name "Riemann hypothesis" comes from the fact that this theorem can be translated into the following statement, which is reminiscent of the “classical” Riemann hypothesis:

Corollary 5.2 **(Riemann hypothesis)**. — *Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g, defined over a finite field $\mathbb{F}_q$. Then the zeroes of the zeta function $s \mapsto \zeta(C/\mathbb{F}_q, s) = Z(C/\mathbb{F}_q, q^{-s})$ all have real part $1/2$.*

5.1. Proof of Theorem 5.1

We now set out to prove the Theorem of Weil. To do so, we roughly follow a proof given by Stepanov in the 1970’s. His proof was subsequently simplified by Bombieri (see his Bourbaki talk). There are nice accounts of these proofs, among which: one by Schoof in lecture notes to a summer school in Abuja in 1990, a short proof by Hindry (in French) in conference proceedings to “Journées X/UPS”, and you can also have a look at [**NX09**, §4.2].

5.1.1. Preliminary reduction. — To prove Theorem 4.1, we start by making a few reductions. Let $C/\mathbb{F}_q$ be a smooth projective curve over a finite field. Assume that C has genus g and that its L-function factors as $L(C/F_q, T) = \prod_{j=1}^{2g}(1 - \alpha_j \cdot T)$.

Lemma 5.3. — *Let notations be as above, and let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite extension. Then*

$$L(C/\mathbb{F}_{q^m}, T) = \prod_{j=1}^{2g} (1 - \alpha_j^m \cdot T).$$

Proof. — Immediate from the definition of $L(C/\mathbb{F}_q, T)$ and the “base change formula” for $Z(C/\mathbb{F}_q, T)$ (see Proposition 2.36). □

The lemma above tells us that, given the L-function of $C/\mathbb{F}_q$ and a finite extension $\mathbb{F}_{q^m}/\mathbb{F}_q$, we can compute right away the "inverse zeroes" of the L-function of $C/\mathbb{F}_{q^m}$. But, since $|\alpha_j^m| = |\alpha_j|^m$ for all $j = 1, \dots, 2g$, this implies the following equivalence:

$$C/\mathbb{F}_q \text{ satisfies the RH for curves} \quad \Longleftrightarrow \quad C/\mathbb{F}_{q^m} \text{ does (for some } m).$$

So, given our curve $C/\mathbb{F}_q$, if will be enough to prove that $C/\mathbb{F}_{q^m}$ satisfies the Riemann Hypothesis (for *some* integer $m \geq 1$) to deduce that the original $C/\mathbb{F}_q$ does. We can thus "replace q by q^m" but, for simplicity of notation, we will just write q for q^m and assume that q is "big enough".

The second reduction step is the following:

Lemma 5.4. — *Hypothesese being as above. The following statements are equivalent:*

(i) $|\alpha_j| = \sqrt{q}$ *for all* $j = 1, \dots, 2g$,

(ii) $|\alpha_j| \leq \sqrt{q}$ *for all* $j = 1, \dots, 2g$,

(iii) For some $m \geq 1$, *there exists a constant* $\gamma_m > 0$ *such that, for all large enough* $n \geq n_0$, *one has*

$$\left|\#C(\mathbb{F}_{q^{2nm}}) - (q^{2nm} + 1)\right| \leq \gamma_m \cdot q^{mn}.$$

Proof. — See second homework assignment. □

This latter statement is seemingly weaker, but it will be enough to prove the full Riemann Hypothesis. We thus need to prove two inequalities: given a curve $C/\mathbb{F}_q$ with q "big enough" (*i.e.* up to replacing q by q^m, or q^{nm}, for some m), find constants $C_1 > 0$, $C_2 > 0$ such that

$$-C_1 \cdot q^{1/2} \leq \#C(\mathbb{F}_q) - (q + 1) \leq C_2 \cdot q^{1/2}.$$

We start by proving the corresponding upper bound, and we will then show the lower bound.

5.1.2. Proof of the upper bound. —

Lemma 5.5. — *Assume that* $q = q_0^2$ *is a square and that* $q > (g + 1)^4$. *Then*

$$\#C(\mathbb{F}_q) < q + 1 + 2g \cdot \sqrt{q}.$$

The idea behind the proof is simple enough. Assume that we can construct a rational function $z \in \mathbb{F}_q(C)^\times$ such that z vanishes to high order m at all the $\mathbb{F}_q$-rational points of C except possibly one, say $Q \in C(\mathbb{F}_q)$, where z has a pole of order $\leq n$. Then, we would deduce that

$$m \cdot (\#C(\mathbb{F}_q) - 1) \leq \# \{\text{zeroes of } z\} = \# \{\text{poles of } z\} \leq n,$$

and $\#C(\mathbb{F}_q) \leq \frac{n}{m} + 1$. And then, we need to choose the parameters m, n so that this upper bound is good enough for our purpose (and such that such a z exists).

Proof. — See Homework 2, Exercise 2. □

5.1.3. Proof of the lower bound. — We start by proving the required lower bound in a special case. The general case is given in the following subsection, for completeness (the idea is the same, but the details are slightly trickier and the general proof requires more technology than we developped so far).

The special case we consider is the following. Let $\mathbb{F}_q$ be a finite field of characteristic p. Let $f(x) \in \mathbb{F}_q[x]$ be a square-free polynomial of degree $e \geq 1$, and $d \geq 1$ be an integer, coprime to pe. Consider a smooth projective curve C over $\mathbb{F}_q$ with affine equation

$$C: \qquad y^d = f(x).$$

It turns out that C has only one point at infinity Q_∞ and that this point is $\mathbb{F}_q$-rational (*i.e.* when counting $\mathbb{F}_q$-rational points on C, except for this one point at infinity, we need only count solutions $(x, y) \in (\mathbb{F}_q)^2$ to the affine equation above). Note that C has genus $g = \lfloor (d-1)(e-1)/2 \rfloor$.

We assume (as we may) that q is a square, that $q > (g+1)^4$ and that, moreover, $\mu_d(\overline{\mathbb{F}_q}) \subset \mathbb{F}_q^\times$. This last condition that the d-th roots of unity are $\mathbb{F}_q$-rational is equivalent to $q - 1 \equiv 0 \bmod d$.

Now denote by $a_1 = 1, a_2, \dots, a_d$ a choice of representatives in $\mathbb{F}_q^\times$ of the quotient $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^d$ (the quotient of $\mathbb{F}_q^\times$ by the subgroup of d-th powers in $\mathbb{F}_q^\times$). In other words, one has

$$\mathbb{F}_q^\times = (\mathbb{F}_q^\times)^d \sqcup a_2 \cdot (\mathbb{F}_q^\times)^d \sqcup \dots \sqcup a_d \cdot (\mathbb{F}_q^\times)^d.$$

For all $a \in \mathbb{F}_q^\times$, consider the auxiliary affine curves $C_a \subset \mathbb{A}^2$ given by the equation

$$C_a : \qquad a \cdot y^d = f(x).$$

All these curves are smooth and have the same genus g as C. Of course, for $a = 1$, one has that $C_1 = C \smallsetminus \{Q_\infty\}$ is just the affine part of C. By the previous lemma, applied to C_a, we get:

$$\forall a \in \mathbb{F}_q^\times, \qquad \#C_a(\mathbb{F}_q) < q + 1 - 1 + 2g \cdot \sqrt{q} = q + 2g \cdot \sqrt{q}. \tag{9}$$

We now count rational points. Let $Z_0 = \{x \in \mathbb{F}_q \ : \ f(x) = 0\}$ be the zet of $\mathbb{F}_q$-rational zeroes of f, and put $Z = \{(x, 0), \ x \in Z_0\} \subset \mathbb{F}_q^2$. By definition, all the sets $C_a(\mathbb{F}_q)$ $(a \in \mathbb{F}_q^\times)$ contain Z since $(x, 0) \in \mathbb{A}^2(\mathbb{F}_q)$ satisfies the equation for C_a.

Now, if $x \in \mathbb{F}_q \smallsetminus Z_0$, then $f(x) \in \mathbb{F}_q^\times$ and there exists a unique $i \in \{1, \dots, d\}$ (depending on x) such that $f(x) \in a_i \cdot (\mathbb{F}_q^\times)^d$. Then the equation $f(x) = a_i \cdot y^d$ has exactly d solutions $y \in \mathbb{F}_q^\times$ (by construction, there is at least one, and at most d; but given one such y, you can construct $d-1$ others by multiplying y by non trivial d-th roots of unity). Thus, any $x \in \mathbb{F}_q \smallsetminus Z_0$ induces d distinct $\mathbb{F}_q$-rational points on exactly one of the C_{a_i} $(i \in \{1, \dots, d\})$. So

$$d \cdot \#(\mathbb{F}_q \smallsetminus Z_0) = \sum_{i=1}^{d} \#(C_{a_i}(\mathbb{F}_q) \smallsetminus Z).$$

Writing $r = \#Z_0 = \#W$, this point-count gives:

$$d \cdot (q - r) = -d \cdot r + \sum_{i=1}^{d} \#C_{a_i}(\mathbb{F}_q) = -d \cdot r + \#C(\mathbb{F}_q) - 1 + \sum_{i=2}^{d} \#C_{a_i}(\mathbb{F}_q).$$

Using the upper bound (9), we get

$$\#C(\mathbb{F}_q) - 1 = d \cdot q - \sum_{i=2}^{d} \#C_{a_i}(\mathbb{F}_q) \geq d \cdot q - (d-1) \cdot (q + 2g \cdot \sqrt{q})) \geq q - (d-1) \cdot 2g \cdot \sqrt{q}.$$

And this gives the lower bound:

$$\#C(\mathbb{F}_q) - (q+1) \geq -\gamma \cdot \sqrt{q},$$

for some constant γ which depends only on the genus of C.

This concludes the proof of the desired lower bound, and thus, of the Riemann hypothesis in this special case.

5.2. Bonus track: a proof of the lower bound in the general case

Let us prove the following estimate:

Lemma 5.6. — *Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g over a finite field $\mathbb{F}_q$. Assume that $q = q_0^2$ is a square, and that $q > (g+1)^4$. Then, for $k \geq 1$ large enough, one has*

$$\#C(\mathbb{F}_{q^k}) = q^k + O(q^{k/2}),$$

where the implicit constant in $O(.)$ depends only on $C/\overline{\mathbb{F}_q}$.

Proof. — Let $f \in \mathbb{F}_q(C)^\times$ be a non constant rational function. Then f induces a morphism of curves $f : C \to \mathbb{P}^1$, also denoted by f. The inclusion $\mathbb{F}_q(\mathbb{P}^1) \subset \mathbb{F}_q(C)$ induced by f, gives us an extension of function fields: let us put $K_0 = \mathbb{F}_q(\mathbb{P}^1)$ and $K = \mathbb{F}_q(C)$. This extension is finite but not necessarily Galois, but one can make a further finite extension L/K so that L/K_0 is Galois (*i.e.* take L to be the Galois closure of K/K_0 in $\overline{K}$). Something we haven't talked about so far is the fact that there is an equivalence of categories between function fields over $\mathbb{F}_q$ and smooth projective curves (see Chapter 2 in Silverman's book [**Sil09**]). This means that L is the function field of a certain smooth projective curve $Y/\mathbb{F}_q$ of genus g_Y, and that there is a morphism $g : Y \to \mathbb{P}^1$ extending f.

We denote by $G := \mathrm{Gal}(L/K_0)$ and $H := \mathrm{Gal}(L/K) \subset G$. For any integer $k \geq 1$, let $A_k \subset Y(\overline{\mathbb{F}_q})$ the set of unramified points for $g : Y \to \mathbb{P}^1$, whose image in $\mathbb{P}^1$ is $\mathbb{F}_{q^k}$-rational. Since $\#\mathbb{P}^1(\mathbb{F}_{q^k}) = q^k + 1$, we have first

$$(10) \qquad \forall k \geq 1, \quad \#A_k = \#G \cdot (q^k + 1) + O(1),$$

the $O(1)$ accounting for the finitely many ramification points of g (this $O(1)$ is independent of k).

For every point $P \in A_k$, the point $\mathrm{Fr}_q P$ maps to the same point in $\mathbb{P}^1$ under g (because g is "defined over $\mathbb{F}_q$"). So, by Galois theory, there exists a unique $\sigma \in G$ such that $\mathrm{Fr}_q P = \sigma(P)$ (some people call this σ the Frobenius substitution at P). This allows us to further partition A_k according to which σ is associated to points: for all $\sigma \in G$, let $A_{k,\sigma} := \{P \in A_k \ : \ \mathrm{Fr}_q P = \sigma(P)\}$. Then A_k is a disjoint union of the $A_{k,\sigma}$ for $\sigma \in G$.

For k large enough, one has $q^k > (g_Y + 1)^4$ (and q is a square, so q^k is one too) and we can argue as for the upper bound in Lemma 4.5, this time with $A_{k,\sigma}$ instead of C. Doing so, we obtain an upper bound

$$(11) \qquad \#A_{k,\sigma} \leq q^k + 1 + 2g_Y \cdot q^{k/2}.$$

Hence,

$$\#A_k = \sum_{\sigma \in G} \#A_{k,\sigma} = \#G \cdot (q^k + 1) + O(q^{k/2}).$$

Since $\#A_k = \#G \cdot (q^k + 1) + O(1)$, this means that, for all $\sigma \in G$, $\#A_k = q^k + O(q^{k/2})$.

By Galois theory, we have

$$\bigsqcup_{\sigma \in H} A_{k,\sigma} = \left\{P \in Y \ : \ \text{the image of } P \text{ in } X \text{ is } \mathbb{F}_{q^k}\text{-rational}\right\},$$

where the union is disjoint. Therefore,

$$\sum_{\sigma \in H} \#A_{k,\sigma} = \#H \cdot \#X(\mathbb{F}_{q^k}) + O(1) = \#H \cdot q^k + O(q^{k/2}),$$

by what we have proved. Dividing by $\#H$ and reordering terms, we have proved the claim. □

Again, the proof of this lemma finishes the proof of the Riemann hypothesis for curves over finite fields.

5.3. Consequences: Hasse-Weil inequality, etc.

Corollary 5.7. — *For all $n \geq 1$, one has the bound*

$$|\#C(\mathbb{F}_{q^n}) - q^n - 1| \leq 2g \cdot q^{n/2},$$

which is called the Hasse-Weil bound. In other words,

$$\forall n \geq 1, \qquad \#C(\mathbb{F}_{q^n}) = q^n + O(q^{n/2}),$$

where the implicit constant in the $O(.)$ depends only on the genus of C.

This corollary follows easily from Theorem 5.1 and relation (8).

Remark 5.8. — Write $L(C/\mathbb{F}_q, T) = \sum_{i=0}^{2g} a_i T^i$. The estimate $|\alpha_j| = \sqrt{q}$ allows us to deduce a bound on the coefficients a_i of $L(C/\mathbb{F}_q, T)$:

$$\forall i = 0, \dots, 2g, \quad |a_i| \leq \binom{2g}{i} q^{i/2}.$$

This is a simple exercise (use the relation between coefficients and roots of a polynomial).

Another interesting consequence of the Riemann hypothesis is a bound on the class-number of curves:

Corollary 5.9. — *Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g over a finite field $\mathbb{F}_q$. Then the class-number of C satisfies*

$$(\sqrt{q}-1)^{2g} \leq h(C) = \#\operatorname{Pic}^0(C) \leq (\sqrt{q}+1)^{2g}.$$

Proof. — Recall that $L(C/\mathbb{F}_q, 1) = h(C)$. In particular, $L(C/\mathbb{F}_q, 1)$ is a positive integer and $|L(C/\mathbb{F}_q, 1)| = L(C/\mathbb{F}_q, 1)$. Now, for all $j = 1, \ldots, 2g$, the triangle inequality implies that

$$\sqrt{q} - 1 = |\alpha_j| - 1 \leq |1 - \alpha_j| \leq 1 + |\alpha_j| = \sqrt{q} + 1.$$

The product over all j's of these inequalities yields

$$(\sqrt{q}-1)^{2g} \leq \prod_{j=1}^{2g} |1-\alpha_j| = |L(C/\mathbb{F}_q, 1)| \leq (\sqrt{q}+1)^{2g}.$$

□

5.4. Extra: further bounds on the number of rational points

As a direct consequence of the Riemann Hypothesis for curves (Weil's Theorem 5.1 above), 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.

In this short section, we will state and prove a slight improvement on (12), proven by Jean Pierre Serre around 1982:

***Theorem 5.10* (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 5.11. — *It is possible to choose a numbering of the α_j's such that*

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

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 5.12. — *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

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

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

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

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 5.13. — *Let $S = \{\alpha_1, \ldots, \alpha_s\}$ 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*

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