CHAPTER 6

SOME ARITHMETIC APPLICATIONS

In this chapter, we give another application of curves over finite fields. Namely, we give an example where the Riemann hypothesis for curves yields good bounds on exponential sums. And we use this fact to prove a theorem about the distribution of squares in $\mathbb{F}_p$.

6.1. Some exponential sums

6.1.1. Legendre symbol. — For all odd prime numbers p, we denote by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol modulo p. It is defined as follows:

$$\forall a \in \mathbb{Z}, \qquad \left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } a \equiv 0 \bmod p, \\ 1 & \text{if } a \not\equiv 0 \bmod p \text{ and } a \text{ is a square modulo } p, \\ -1 & \text{if } a \not\equiv 0 \bmod p \text{ and } a \text{ is not a square modulo } p. \end{cases}$$

Clearly, this map on $\mathbb{Z}$ induces a map on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ because $\left(\frac{a}{p}\right)$ only depends on the residue class of a modulo p. So the Legendre symbol detects the squares in $\mathbb{F}_p$. Moreover, it is not difficult to check that $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a character of $\mathbb{F}_p^\times$ (*i.e.* a group homomorphism). This provides a second interpretation of the Legendre symbol: $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is the only non trivial group homorphism whose square is the trivial homomorphism $x \mapsto 1$ (this group morphism is then extended to the whole of $\mathbb{F}_p$ by setting $\left(\frac{0}{p}\right) = 0$).

Proposition 6.1. — *Let p be an odd prime number. Then*

$$\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) = 0.$$

Proof. — Left as an exercise. Remember that the cyclic group $\mathbb{F}_p^\times$ (of order $p-1$) contains $(p-1)/2$ squares, and as many nonsquares. □

This proposition is basically a restatement of the fact that $\mathbb{F}_p$ contains as many squares as nonsquares. In particular, the map $\left(\frac{\cdot}{p}\right)$ takes the value 1 as many times as it takes the value -1. In other words, the probability that a "random" element of $\mathbb{F}_p^\times$ is a square (resp. a nonsquare) is $1/2$.

6.1.2. Character sums. — Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial in one variable. For all odd prime number p, let us define the following sum:

$$S(f;p) := \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right).$$

In a sense, $S(f;p)$ measures the probability that $f(x)$ is a square, given a random $x \in \mathbb{F}_p$.

Since $\left|\left(\frac{y}{p}\right)\right| \leq 1$ for all $y \in \mathbb{F}_p$, and since $S(f;p) \in \mathbb{R}$ is a sum of p terms, we have the trivial bound:

$$|S(f;p)| \leq p.$$

For many applications (see below) however, this bound is insufficient: one would like to find bounds of the form

$$|S(f,p)| \leq C_f \cdot p^{1-\epsilon} \qquad (?),$$

for a certain constant C_f (depending only on f, and not on p) and a certain exponent $\epsilon \in (0,1)$. Such a bound would lead to

$$\left|\frac{1}{p}\sum_{x\in\mathbb{F}_p}\left(\frac{f(x)}{p}\right)\right| \leq C_f \cdot p^{-\epsilon} \longrightarrow 0 \quad (p \to \infty).$$

In other words, in the "large p" limit, the polynomial $f \bmod p$ takes roughly as many square values as nonsquare values. As an example of this behaviour, see the Proposition above (in the case where $f(x) = x$).

Of course, one can not hope that such a bound holds for any given $f(x) \in \mathbb{Z}[x]$: we need to avoid trivial cases where the reasonning above fails. Say, for example, that $f(x) = x^2$: in this case, the polynomial $f \bmod p$ takes only square values (except where it vanishes) and

$$\frac{S(x^2;p)}{p} = \frac{1}{p}\sum_{x\in\mathbb{F}_p}\left(\frac{x^2}{p}\right) = \frac{1}{p}\sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)^2 = \frac{p-1}{p} = 1 + o(1) \quad (p \to \infty).$$

Nonetheless, the theorem below tells us that a strong bound on $S(f;p)$ exists, provided that one avoids this kind of "bad polynomials".

***Theorem 6.2* (Weil).** — *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. We assume that $f(x)$ has no multiple factors in $\mathbb{C}[x]$. For any odd prime number p such that $f(x) \bmod p \in \mathbb{F}_p[x]$ has no multiple factors in $\overline{\mathbb{F}_p}[x]$, one has:*

$$|S(f;p)| \leq (\deg f - 1) \cdot \sqrt{p}.$$

Proof. — Let p be as in the statement of the theorem. Note that

$$S(f;p) = -p + \sum_{x\in\mathbb{F}_p}\left(1 + \left(\frac{f(x)}{p}\right)\right).$$

But, for any $z \in \mathbb{F}_p$,

$$1 + \left(\frac{z}{p}\right) = \begin{cases} 1 & \text{if } z = 0, \\ 2 & \text{if } z \neq 0 \text{ and } z \text{ is a square in} \mathbb{F}_p^\times, \\ 0 & \text{if } z \neq 0 \text{ and } z \text{ is not a square in} \mathbb{F}_p^\times \end{cases} = \#\{y \in \mathbb{F}_p : \ y^2 = z\}.$$

In other words, the map $z \mapsto 1 + \left(\frac{z}{p}\right)$ counts the number of square roots of z in $\mathbb{F}_p$. Let $U \subset \mathbb{A}^2$ be the affine set over $\mathbb{F}_p$ defined by

$$U : \qquad y^2 = f(x).$$

With our assumptions on f and p, it is not hard to see that U is an affine curve, and that U is smooth. Moreover,

$$\#U(\mathbb{F}_p) = \#\{(x,y) \in \mathbb{F}_p^2 : \ y^2 = f(x)\} = \sum_{x\in\mathbb{F}_p} \#\{y \in \mathbb{F}_p : \ y^2 = f(x)\} = S(f,p) + p.$$

We would like to use the results about curves that we know. Unfortunately, U is not projective so we can not directly apply Weil's theorem... That being said, we have seen in Homework #1 how to construct (explicitly) a smooth projective C, defined over $\mathbb{F}_p$, which "completes" U.

(Remember that, in general, C is not the homoegenisation of U in $\mathbb{P}^2$, which might be singular). For our present purpose, it will be sufficient to know that:

- such a smooth projective curve C exists,
- one does not add too many $\mathbb{F}_p$-rational points on passing from U to C:

$$\#C(\mathbb{F}_p) - \#U(\mathbb{F}_p) = \begin{cases} 2 & \text{if } \deg f \text{ is even,} \\ 1 & \text{if } \deg f \text{ is odd.} \end{cases}$$

- the genus of C is given by

$$g = \left\lfloor \frac{\deg f - 1}{2} \right\rfloor = \begin{cases} \frac{\deg f - 2}{2} & \text{if } \deg f \text{ is even,} \\ \frac{\deg f - 1}{2} & \text{if } \deg f \text{ is odd.} \end{cases}$$

The Riemann hypothesis for curves implies that

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g \cdot \sqrt{p}.$$

From which one easily deduces that

$$|S(f;p)| = |\#U(\mathbb{F}_p) - p| \leq \begin{cases} (\deg f - 2) \cdot \sqrt{p} + 1 & \text{if } \deg f \text{ is even,} \\ (\deg f - 1) \cdot \sqrt{p} & \text{if } \deg f \text{ is odd.} \end{cases}$$

In both cases, one has

$$|S(f;p)| \leq (\deg f - 1) \cdot \sqrt{p},$$

as required. □

Remark 6.3. — Note that, even if $f \bmod p$ has multiple factors in $\overline{\mathbb{F}_p}[x]$, one can still prove a bound as in the Theorem:

$$|S(f;p)| \leq C_{f,p} \cdot \sqrt{p},$$

for a constant $C_{f,p}$. It turns out that $C_{f,p} \leq \deg f - 1$.

6.2. Distribution of quadratic residues

Let $r \geq 2$ be an integer, and $p > r$ be a prime number. In the sequence of integers

$$(1,\ 2,\ 3,\ \ldots,\ p-1)$$

we look for subsequences $(a+1, a+2, \ldots, a+r)$ of r consecutive integers (where $0 \leq a \leq p-r-1$) which are all quadratic residues modulo p. Do these subsequences exist at all? If so, how many are there? We are particularly interested in the setting where r is fixed and $p \to \infty$.

More generally, if we fix a sequence of signs $\boldsymbol{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r) \in \{\pm 1\}^r$, do there exist sequences $(a+1, a+2, \ldots, a+r)$ (with $0 \leq a \leq p-r-1$) of consecutive integers such that

$$\forall i = 1, \ldots, r, \qquad \left(\frac{a+i}{p}\right) = \varepsilon_i \quad ?$$

This problem was first considered (and solved) by Davenport in the 1930's. The proof we give here roughly follows the exposition in the book "Sommes exponentielles" by N. Katz (in French, see §1.4 there).

For any $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_r) \in \{\pm 1\}^r$, we let

$$N(\boldsymbol{\varepsilon}; p) := \#\left\{ a \in \{0, 1, \ldots, p-r-1\} :\ \left(\frac{a+i}{p}\right) = \varepsilon_i \text{ for all } i \right\}$$

be the number of "good sequences". We have $0 \leq N(\boldsymbol{\varepsilon}; p) \leq p - r$, and we want to know how $p \mapsto N(\boldsymbol{\varepsilon}; p)$ behaves when $p \to \infty$. The precise result, due to Davenport (and improved by Weil), is as follows:

Theorem 6.4. — *Let $r \geq 2$, and $\boldsymbol{\varepsilon} \in \{\pm 1\}^r$. Then, for all prime numbers $p > r$,*

$$\left| N(\boldsymbol{\varepsilon}; p) - \frac{p}{2^r} \right| \leq \frac{r-1}{2} + \left(1 - \frac{1}{2^r}\right)(r-1) \cdot \sqrt{p}.$$

From this theorem, one deduces the following result:

Corollary 6.5. — *Let $r \geq 2$, and $\boldsymbol{\varepsilon} \in \{\pm 1\}^r$. Then, for prime numbers $p \to \infty$,*

$$\frac{N(\boldsymbol{\varepsilon}; p)}{p - r} = \frac{1}{2^r} + O(p^{-1/2}),$$

where the constant in the $O(.)$ is explicit (and depends only on r).

Note that the quantity on the left measures the proportion of "good sequences" among the possible sequences $(a+1, a+2, \ldots, a+r)$ of r consecutive integers. Note also that the estimates in Theorem 7.4 and Corollary 7.5 are entirely independent on the choice of $\boldsymbol{\varepsilon} \in \{\pm 1\}^r$! There are 2^r choices for $\boldsymbol{\varepsilon}$: is this a coincidence that the proportion $\frac{N(\boldsymbol{\varepsilon};p)}{p-r}$ tends to $1/2^r$ when $p \to \infty$?

Proof of Theorem 7.4. — Note that, for all $a \in \{0, 1, \ldots, p-r-1\}$ and all $i \in \{1, \ldots, r\}$, one has

$$1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right) = \begin{cases} 2 & \text{if } \left(\frac{a+i}{p}\right) = \varepsilon_i, \\ 0 & \text{if } \left(\frac{a+i}{p}\right) \neq \varepsilon_i. \end{cases}$$

So that, given $a \in \{0, 1, \ldots, p-r-1\}$,

$$\prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right) = \begin{cases} 2^r & \text{if the sequence } (a+1, a+2, \ldots, a+r) \text{ is good,} \\ 0 & \text{otherwise.} \end{cases}$$

So, up to normalization by a constant, this map is the characteristic function for the set of "good" a's inside the set of all a's:

$$N(\boldsymbol{\varepsilon}; p) = \sum_{a \text{ "good"}} 1 = \sum_{a=0}^{p-r-1} \frac{1}{2^r} \prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right).$$

We "complete the sum" and remove the extra terms:

$$N(\boldsymbol{\varepsilon}; p) = \sum_{a=0}^{p-1} \frac{1}{2^r} \prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right) - \sum_{a=p-r}^{p-1} \frac{1}{2^r} \prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right).$$

We will treat these two sums separately.

Let us start by proving that the second sum gives an error-term. Note that, for $a \geq p-r$, there is one index $i \in \{1, \ldots, r\}$ such that $a + i = p$: for this index i, one has $1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right) = 1$ (and, for all other i's, this term is ≤ 2). Thus, for $a \in \{p-r, \ldots, p-1$,

$$\frac{1}{2^r} \prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right) \leq \frac{1 \cdot 2^{r-1}}{2^r} = \frac{1}{2}.$$

Thus the second sum satisfies:

$$S_2 := \sum_{a=p-r}^{p-1} \frac{1}{2^r} \prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right) \leq \frac{r-1}{2}.$$

We now estimate the first sum. Expanding the inner products, and exchanging the order of summation, we get

$$S_1 := \sum_{a=0}^{p-1} \frac{1}{2^r} \prod_{i=1}^{r} \left(1 + \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right) = \sum_{a=0}^{p-1} \frac{1}{2^r} \left(1 + \sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} \prod_{i \in I} \varepsilon_i \cdot \left(\frac{a+i}{p}\right)\right)$$

$$= \frac{1}{2^r} \sum_{a \in \mathbb{F}_p} \left(1 + \sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} \prod_{i \in I} \varepsilon_i \cdot \prod_{i \in I} \left(\frac{a+i}{p}\right)\right) = \frac{p}{2^r} + \sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} \prod_{i \in I} \varepsilon_i \cdot \left(\sum_{a \in \mathbb{F}_p} \prod_{i \in I} \left(\frac{a+i}{p}\right)\right).$$

Remembering that $\left(\frac{\cdot}{p}\right)$ is multiplicative, we obtain that

$$S_1 - \frac{p}{2^r} = \frac{1}{2^r} \sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} \prod_{i \in I} \varepsilon_i \cdot \left(\sum_{a \in \mathbb{F}_p} \left(\frac{\prod_{i \in I}(a+i)}{p}\right)\right).$$

Now we make use of the triangle inequality and we get

$$\left|S_1 - \frac{p}{2^r}\right| \leq \frac{1}{2^r} \sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} 1 \cdot \left|\sum_{a \in \mathbb{F}_p} \left(\frac{\prod_{i \in I}(a+i)}{p}\right)\right|.$$

For any subset $I \subset \{1, \dots, r\}$ (I non-empty), let us put

$$f_I(x) := \prod_{i \in I} (x+i) \in \mathbb{Z}[x].$$

Since $p > r$, this polynomial f_I clearly satisfies all the assumptions of Theorem 7.2 (as we know the factorization of $f_I(x)$). Thus, it results that,

$$\left|\sum_{a \in \mathbb{F}_p} \left(\frac{\prod_{i \in I}(a+i)}{p}\right)\right| = \left|\sum_{a \in \mathbb{F}_p} \left(\frac{f_I(a)}{p}\right)\right| \leq (\deg f_I - 1) \cdot \sqrt{p} = (\#I - 1) \cdot \sqrt{p}.$$

From which we deduce that

$$\left|S_1 - \frac{p}{2^r}\right| \leq \frac{\sqrt{p}}{2^r} \sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} (\#I - 1).$$

At this point, we are almost done: the remaining sum is easy to estimate and, in any case, the sum depends only on r (not on p) so that we don't need to be extra careful (improvements on the upper bound will only lead to better constants in the right-hand side of Theorem 7.4). As an example of upper bound, one has:

$$\sum_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} (\#I - 1) = \sum_{k=1}^{r} \binom{r}{k} (k-1) \leq \sum_{k=1}^{r} \binom{r}{k} (r-1) = (r-1)(2^r - 1).$$

In conclusion, we have proved that

$$\left|S_1 - \frac{p}{2^r}\right| \leq \left(1 - \frac{1}{2^r}\right)(r-1) \cdot \sqrt{p}.$$

And, putting everything together, we arrive at the desired result:

$$\left|N(\boldsymbol{\varepsilon}; p) - \frac{p}{2^r}\right| = \left|S_1 + S_2 - \frac{p}{2^r}\right| \leq \left|S_1 - \frac{p}{2^r}\right| + |S_2| \leq \frac{r-1}{2} + \left(1 - \frac{1}{2^r}\right)(r-1) \cdot \sqrt{p}.$$

Hence the theorem. Note that all our estimates are explicit and entirely independent of $\boldsymbol{\varepsilon}$: this means that, for a given $r \geq 2$ (and any $\boldsymbol{\varepsilon} \in \{\pm 1\}^r$), it should be possible to compute a bound $P_r > 0$ such that, for all primes $p > P_r$, one has $N(\boldsymbol{\varepsilon}; p) \geq 1$ (*i.e.* for all primes $p > P_r$, there is at least one sequence satisfying our requirements). □