D-MATH HS 2018 Prof. Emmanuel Kowalski
Exponential sums over Finite Fields. Exercise Sheet 1

January 11, 2019

Exercise 1.

i) Let us write

$$\begin{aligned}
\frac{1}{p}\sum_{h\in\mathbb{F}_p} G(2,h;p)^3 e\Big(\frac{-ah}{p}\Big) &= \frac{1}{p}\sum_{h\in\mathbb{F}_p}\Big(\sum_{x\in\mathbb{F}_p} e\Big(\frac{x^2h}{p}\Big)\Big)^3 e\Big(\frac{-ah}{p}\Big)\\
&= \frac{1}{p}\sum_{h\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} e\Big(\frac{h(x^2+x^2+x^2-a)}{p}\Big)\\
&= \frac{1}{p}\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p}\sum_{h\in\mathbb{F}_p} e\Big(\frac{h(x^2+x^2+x^2-a)}{p}\Big).
\end{aligned}$$

Now, thanks to the orthogonality of additive characters, we have

$$\sum_{h\in\mathbb{F}_p} e\Big(\frac{h(x^2+x^2+x^2-a)}{p}\Big) = \begin{cases} 0 & \text{if } x^2+x^2+x^2-a\neq 0\\ p & \text{if } x^2+x^2+x^2-a=0,\end{cases}$$

and so we get the result.

ii) As in the part (*ii*) of the previous exercise, developing the product we have

$$|G(2,h;p)|^2 = \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} e\Big(\frac{x^2h}{p}\Big)e\Big(-\frac{y^2h}{p}\Big) = \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} e\Big(\frac{(x^2-y^2)h}{p}\Big).$$

Using now a change of variables $(s,t)=(x+y,x-y)$, $G(2,h;p)$ becomes

$$|G(2,h;p)|^2 = \sum_{s\in\mathbb{F}_p}\sum_{t\in\mathbb{F}_p} e\Big(\frac{4sth}{p}\Big) = p,$$

where in the last step we use, again, the orthogonality of the additive characters (assuming $h,4\neq 0 \mod p$).

iii) First observe that $G(2,0;p)=p$. Combining part (*i*) and part (*ii*) we get:

$$\begin{aligned}
N_{2,3}(a,p) &= p^2 + \frac{1}{p}\sum_{h\in\mathbb{F}_p^\times} G(2,h;p)^3 e\Big(\frac{-ah}{p}\Big)\\
&= p^2 + O(p^{\frac{3}{2}}).
\end{aligned}$$

iv) The same argument works for $s \geq 3$ getting:

$$|N_{2,s}(a,p)| = p^{s-1} + O(p^{\frac{s}{2}}).$$

Exercise 2.

i) Using the same argument as in exercise 2 we get

$$|N_{2,2}(a,p)| = p + O(p),$$

but this do not lead to an asymptotic formula for $|N_{2,2}(a,p)|$ because the remainder term has the same size as the main one.

ii) Because $\mathbb{F}_p$ is the finite field with p elements, any $a \in \mathbb{F}_p^\times$ satisfies $a^{p-1} = 1$ i.e. any $a \in \mathbb{F}_p^\times$ is a zero of the polynomial $f(x) = x^{p-1} - 1$, so one has

$$f(x) = x^{p-1} - 1 = \prod_{a \in \mathbb{F}_p^\times} (x - a).$$

Moreover $a \in \mathbb{F}_p^\times$ is a square modulo p if and only if $a^{\frac{p-1}{2}} = 1$, i.e. a is a zero of the polynomial $g(x) = x^{\frac{p-1}{2}} - 1$. On the other hand it is clear that $g|f$ and this implies that g has $\frac{p-1}{2}$ distinct zeros in $\mathbb{F}_p$. Now observing that

$$X := \{x^2 : x \in \mathbb{F}_p\} = |\{\text{root of } g\}| \cup \{0\},$$

one obtains that $|X| = \frac{p+1}{2}$. To conclude it is enough to observe that Y_a is just the set $-X$ shifted by a.

iii) Using the Inclusion–Exclusion principle we have

$$|X \cup Y_a| = |X| + |Y_a| - |X \cap Y_a|.$$

It is clear that $|X \cup Y_a| \leq p$ so

$$p \geq |X \cup Y_a| = |X| + |Y_a| - |X \cap Y_a| = p + 1 - |X \cap Y_a|,$$

and then

$$|X \cap Y_a| \geq 1.$$

Exercise 3.

i) If $x^2 + y^2 = 0$ and $x, y \neq 0$ then $(xy^{-1})^2 = -1$. It is a well known fact that -1 is a square modulo p if and only if $p \equiv 1 \mod 4$. Thanks to that it is clear that $N_2(0,p) = \{(0,0)\}$ if $p \equiv 3 \mod 4$. Instead, if $p \equiv 1 \mod 4$ we get

$$N_{2,2}(0,p) = \{(x, \pm ix) : x \in \mathbb{F}_p^\times\} \cup \{(0,0)\},$$

where we are denoting by i a square root of -1 in $\mathbb{F}_p$.

ii) Let $a, b \in \mathbb{F}_p^\times$ and consider $a^{-1}b$. By the previous exercise there exist $h, k \in \mathbb{F}_p$ such that $h^2 + k^2 = a^{-1}b$. Consider the change of variables $(x,y) = (hx + ky, kx - hy)$. For all $(x,y) \in \mathbb{F}_p^2$, one has

$$(hx + ky)^2 + (hx - ky)^2 = (h^2 + k^2)(x^2 + y^2) = a^{-1}b(x^2 + y^2).$$

Then it is clear that $\mathrm{Im}(N_{2,2}(a,p)) \subset N_{2,2}(b,p)$ and because the map we are considering is injective we conclude that $|N_2(a,p)| \leq |N_2(b,p)|$. Repeating this argument starting with ab^{-1} gives the inequality in the other direction.

iii) Using the previous part we have

$$p^2 = |\mathbb{F}_p^2| = \sum_{a \in \mathbb{F}_p} |(N_{2,2}(a,p)| = |(N_{2,2}(0,p)| + |(N_2(1,p)|(p-1).$$

Inserting the possible values of $|N_{2,2}(0,p)|$ we get the result.

Exercise 4.

i) Let us denote by $\mathbb{F}^{\times d}$ the set of d-powers in $\mathbb{F}^{\times}$. A charcter of order d ovver $\mathbb{F}^{\times}$ can be seen as a character over $\mathbb{F}^{\times}/\mathbb{F}^{\times d}$. Then (i) is just the orthogonal relation for characters over $\mathbb{F}^{\times}/\mathbb{F}^{\times d}$.

ii) Using (i), we rewrite

$$\begin{aligned} G(d,h;p) &= \sum_{z \in \mathbb{F}_p} e\Big(\frac{zh}{p}\Big) \cdot \Big(\sum_{\chi:\chi^d=1} \chi(z) \Big) \\ &= \sum_{\substack{\chi:\chi^d=1 \\ \chi \neq 1}} \sum_{z \in \mathbb{F}_p} e\Big(\frac{zh}{p}\Big) \chi(z) \\ &= \sum_{\substack{\chi:\chi^d=1 \\ \chi \neq 1}} \overline{\chi}(h) \tau_\chi \end{aligned}$$

then the result follows since $|\tau_\chi| = \sqrt{p}$ for any multiplicative character $\chi \neq 1$.

iii) If $p \not\equiv 1 \mod d$ then any element in $\mathbb{F}_p$ is a d-power. Thus

$$G(d,h;p) = \sum_{x \in \mathbb{F}_p} e\Big(\frac{x^d h}{p}\Big) = \sum_{z \in \mathbb{F}_p} e\Big(\frac{zh}{p}\Big).$$

Then

$$G(d,h;p) = \begin{cases} p & \text{if } h = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 5

As in Exercise 1 we have the equality

$$\begin{aligned} |N_{k,s}(a,p)| &= \frac{1}{p} \sum_{h \in \mathbb{F}_p} G(k,h;p)^s e\Big(\frac{-ah}{p}\Big) \\ &= p^{s-1} + \frac{1}{p} \sum_{h \in \mathbb{F}_p^{\times}} G(k,h;p)^s e\Big(\frac{-ah}{p}\Big). \end{aligned}$$

Then the result is a direct consequence of Exercise 4.

Exercise 5.

i) Let $N > 0$, and let us denote N' the larges integer such that $pN' \leq N$, then

$$\begin{aligned}\sum_{n\leq N}\chi(n) &= \sum_{n\leq pN'}\chi(n) + \sum_{pN'\leq n\leq N}\chi(n)\\ &= N'\sum_{0\leq n\leq p}\chi(n) + \sum_{0\leq n\leq N-pN'}\chi(n)\\ &= \sum_{0\leq n\leq N-pN'}\chi(n),\end{aligned}$$

where in the first step we used the periodicity of χ and in the second one the fact that χ is a non-trivial character. The results than follows since $0 \leq N - pN' \leq p$.

ii) It is enough to observe that

$$\frac{1}{p}\sum_{a\in\mathbb{F}_p} e\Big(\frac{a(h-n)}{p}\Big) = \begin{cases}1 & \text{if } h = n,\\ 0 & \text{otherwise.}\end{cases}$$

iii) We have

$$\begin{aligned}\sum_{n\leq N}\chi(n) &= \sum_{h\in\mathbb{F}_p}\chi(h)\cdot\Big(\frac{1}{p}\sum_{n\leq N}\sum_{a\in\mathbb{F}_p} e\Big(\frac{a(h-n)}{p}\Big)\Big)\\ &= \frac{1}{p}\sum_{h\in\mathbb{F}_p}\sum_{n\leq N}\sum_{a\in\mathbb{F}_p} e\Big(\frac{ah}{p}\Big)e\Big(-\frac{an}{p}\Big)\chi(h)\\ &= \frac{1}{p}\sum_{a\in\mathbb{F}_p}\sum_{n\leq N} e\Big(-\frac{an}{p}\Big)\sum_{h\in\mathbb{F}_p} e\Big(\frac{ah}{p}\Big)\chi(h)\\ &= \frac{1}{p}\sum_{a\in\mathbb{F}_p^\times}\sum_{n\leq N} e\Big(-\frac{an}{p}\Big)\overline{\chi}(a)\tau_\chi,\end{aligned}$$

as we wanted.

iv) For $0 < a < p$ this is just a geometric series, then we have

$$\sum_{n\leq N} e\Big(-\frac{an}{p}\Big) = \frac{1 - e\Big(-\frac{a(N+1)}{p}\Big)}{1 - e\Big(-\frac{a}{p}\Big)}.$$

On the other hand for $0 < a < p$ we have

$$\Big|1 - e\Big(-\frac{a}{p}\Big)\Big| \geq \frac{a}{p},$$

thus

$$\Big|\sum_{n\leq N} e\Big(-\frac{an}{p}\Big)\Big| \leq \frac{2p}{a}. \tag{1}$$

From part *(iii)* we have

$$\sum_{n\leq N}\chi(n) = \frac{\tau_\chi}{p}\sum_{a\in\mathbb{F}_p^\times}\overline{\chi}(a)\sum_{n\leq N} e\Big(-\frac{an}{p}\Big),$$

Then using (1) we have

$$\Big|\sum_{n\le N}\chi(n)\Big| \le \frac{\sqrt{p}}{p}\sum_{a\in\mathbb{F}_p^\times}\Big|\sum_{n\le N} e\Big(-\frac{an}{p}\Big)\Big|$$
$$\le \frac{1}{\sqrt{p}}\sum_{0<a<p}\frac{p}{a}$$
$$\le 3\sqrt{p}\log p,$$

as we wanted.

v) One repeats the same argument observing that

$$\begin{aligned}\sum_{h\in\mathbb{F}_p} e\Big(\frac{h^2\alpha+ah}{p}\Big) &= \sum_{h\in\mathbb{F}_p} e\Big(\frac{\alpha(h^2+a\overline{\alpha}h)}{p}\Big)\\ &= \sum_{h\in\mathbb{F}_p} e\Big(\frac{\alpha(h^2+a\overline{\alpha}h+(a\overline{2\alpha})^2-(a\overline{2\alpha})^2)}{p}\Big)\\ &= e\Big(\frac{-(a\overline{2})^2)}{p}\Big)\sum_{h\in\mathbb{F}_p} e\Big(\frac{\alpha(h+a\overline{2\alpha})^2}{p}\Big)\\ &= e\Big(\frac{-(a\overline{2})^2)}{p}\Big)G(2,\alpha;p).\end{aligned}$$

Exercise 6.

In the following we denote by $||\cdot||$ the norm in $\mathbb{R}^2$ and by

$$B_r^{+,+}(0) := \{(x,y)\in\mathbb{R}^2_{\ge 0} : ||(x,z)|| \le r\}$$

the quarter of the circle centered in 0 of radius r in the first quadrant. We start finding an asymptotic formula for

$$N_{+,+}(X) := |\{(a,b)\in\mathbb{N}^2 : a^2+b^2\le X\}|.$$

We can rewrite this as

$$N_{+,+}(X) := |\{(a,b)\in\mathbb{N}^2 : (a,b)\in B^{+,+}_{\sqrt{X}}(0)\}|.$$

The points $(a,b)\in\mathbb{N}^2$ are in one to one correspondence with squares $S_{a,b} := [a,a+1)\times[b,b+1)$. Moreover is it clear that $S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)\ne\emptyset$ if and only if $(a,b)\in B^{+,+}_{\sqrt{X}}(0)$. Indeed, if $(a,b)\in B^{+,+}_{\sqrt{X}}(0)$ then of course $S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)\ne\emptyset$. Let us do the other direction: if $(c,d)\in S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)$, then by definition $||(c,d)||\le\sqrt{X}$. On the other hand one has that $||(a,b)||\le||(c,d)||\le\sqrt{X}$, thus $(a,b)\in B^{+,+}_{\sqrt{X}}(0)$. We can conclude that

$$\begin{aligned}N_{+,+}(X) :&= |\{(a,b)\in\mathbb{N}^2 : (a,b)\in B^{+,+}_{\sqrt{X}}(0)\}|\\ &= |\{(a,b)\in\mathbb{N}^2 : S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)\ne\emptyset\}|\\ &= \text{Area}\Big(\bigcup_{S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)\ne\emptyset} S_{a,b}\Big).\end{aligned}$$

We claim that

$$B^{+,+}_{\sqrt{X}-\sqrt{2}}(0) \subset \bigcup_{S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)\neq\emptyset} S_{a,b} \subset B^{+,+}_{\sqrt{X}+\sqrt{2}}(0).$$

Let $(c,d) \in B^{+,+}_{\sqrt{X}-\sqrt{2}}(0)$, then there exists $(a,b) \in \mathbb{N}^2$ such that $(c,d) \in S_{a,b}$. Then $S_{a,b} \cap B^{+,+}_{\sqrt{X}}(0) \neq \emptyset$ since $(c,d) \in B^{+,+}_{\sqrt{X}-\sqrt{2}}(0) \subset B^{+,+}_{\sqrt{X}}(0)$. Thus $(c,d) \in \bigcup_{S_{a,b}\cap B^{+,+}_{\sqrt{X}}(0)\neq\emptyset} S_{a,b}$. Let $(c,d) \in S_{a,b}$ for some (a,b) such that $S_{a,b} \cap B^{+,+}_{\sqrt{X}}(0) \neq \emptyset$. Then

$$||(c,d)|| \leq ||(a,b)|| + ||(a-c,b-d)|| \leq \sqrt{X} + \sqrt{2}.$$

Hence, we conclude

$$\text{Area}(B^{+,+}_{\sqrt{X}-\sqrt{2}}(0)) \leq N_{+,+}(X) \leq \text{Area}(B^{+,+}_{\sqrt{X}+\sqrt{2}}(0)),$$

and then

$$N_{+,+}(X) = \frac{\pi}{4}X + O(\sqrt{X}).$$

Using the symmetries of the circle we finally get

$$N(X) = \pi X + O(\sqrt{X}).$$