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

October 18, 2018

Exercise 1. Let $p > 2$ be a prime number and $\mathbb{F}_p$ be the finite field with p elements. For any $a \in \mathbb{F}_p$ we define

$$N_{2,3}(a,p) := \{(x,y,z) \in \mathbb{F}_p^3 : x^2 + y^2 + z^2 = a\}.$$

the aim of this exercise is to give an asymptotic formula for $|N_{2,3}(a,p)|$ for any $a \in \mathbb{F}_p$. Proceed stepwise as follows:

i) show that:

$$|N_{2,3}(a,p)| = \frac{1}{p} \sum_{h \in \mathbb{F}_p} G(2,h;p)^3 e\left(\frac{-ah}{p}\right),$$

where

$$G(2,h;p) := \sum_{x \in \mathbb{F}_p} e\left(\frac{x^2 h}{p}\right).$$

ii) For $h \neq 0$ prove that

$$|G(2,h;p)|^2 = p.$$

iii) Conclude the exercise by proving the formula:

$$|N_{2,3}(a,p)| = p^2 + O(p^{\frac{3}{2}}).$$

iv) What about a similar result for $|N_{2,s}(a,p)|$[1]?

Exercise 2. In this exercise we are going to show that $N_{2,2}(a,p) \neq \emptyset$ for all $a \in \mathbb{F}_p$.

i) Why would the same strategy adopted in Exercise 1 not work in the case $s = 2$?

ii) Consider the two sets $X := \{x^2 : x \in \mathbb{F}_p\}$ and $Y_a := \{-y^2 + a : y \in \mathbb{F}_p\}$. Show that

$$|X|, |Y_a| \geq \frac{p+1}{2}.$$

iii) Prove that $X \cap Y_a \neq \emptyset$ and conclude.

Exercise 3. Assume $p > 2$. Using the fact that $N_{2,2}(a,p) \neq \emptyset$ for all $a \in \mathbb{F}_p$, we are now going to give an explicit formula for its cardinality:

[1] $N_{2,s}(a,p)$ is defined as $N_{2,s}(a,p) := \{(x_1, ..., x_s) \in \mathbb{F}_p^3 : x_1^2 + ... + x_s^2 = a\}$

i) show that

$$|N_{2,2}(0,p)| = \begin{cases} 2p-1 & \text{if } p \equiv 1 \mod 4 \\ 1 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

ii) Let $a, b \in \mathbb{F}_p^\times$. Show that:

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

Hint: Consider $a^{-1}b$, by the previous exercise there exist $h, k \in \mathbb{F}_p$ such that $h^2 + k^2 = a^{-1}b$. Use then the change of variables $(s,t) = (hx + ky, kx - hy)$.

iii) Conclude the proof showing that for $a \in \mathbb{F}_p$

$$|N_{2,2}(a,p)| = \begin{cases} p-1 & \text{if } p \equiv 1 \mod 4 \\ p+1 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Exercise 4. Let $d \geq 2$ be an integer and let p be a prime number such that $p \equiv 1 \mod d$. The goal of this exercise is to prove that

$$G(d,h;p) := \sum_{x \in \mathbb{F}_p} e\Big(\frac{x^d h}{p}\Big) \tag{1}$$

satisfies $|G(d,h;p)| \leq (d-1)\sqrt{p}$.

i) Show that for any $a \in \mathbb{F}_p^\times$

$$\sum_{\chi : \chi^d = 1} \chi(a) = \begin{cases} d & \text{if } a \text{ is a } d\text{-power,} \\ 0 & \text{otherwise.} \end{cases}$$

ii) Conclude the exercise.

iii) Compute $G(d,h;p)$ when $p \not\equiv 1 \mod d$.

Exercise 5. Let p be a prime number and let $a \in \mathbb{F}_p$. For any k, s we define

$$N_{k,s}(a,p) := \{(x_1, ..., x_s) \in \mathbb{F}_p^s : x_1^k + \cdots + x_s^k = a\}.$$

Use Exercise 4 to prove that

$$N_{k,s}(a,p) = p^{s-1} + E(k,s;p),$$

where

$$E(k,s;p) = \begin{cases} O_k(p^{\frac{s}{2}}) & \text{if } p \equiv 1 \mod k, \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 6. Let p be a prime number and χ be a non trivial multiplicative character over $\mathbb{F}_p^\times$. The goal of this exercise is to prove the so called *Pólya-Vinogradov inequality*:

$$\Big|\sum_{n \leq N} \chi(n)\Big| = O(\sqrt{p}\log p)$$

for any $N > 0$.

i) Prove that we may assume $0 \leq N < p$.

ii) Show that for any N one has

$$\sum_{n\leq N}\chi(n)=\sum_{h\in\mathbb{F}_p}\chi(h)\cdot\Big(\frac{1}{p}\sum_{n\leq N}\sum_{a\in\mathbb{F}_p}e\Big(\frac{a(h-n)}{p}\Big)\Big).$$

iii) From (i) deduce that

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

where $\overline{\chi}$ denotes the inverse character of χ.

iv) Show that for any $0<a<p$ one has

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

and conclude.

v) With a similar argument, show that for any $\alpha\in\mathbb{F}_p^\times$ and for any $0<N<p$

$$\sum_{n\leq N}e\Big(\frac{n^2\alpha}{p}\Big)\ll\sqrt{p}\log p.$$

Exercise 7. For $X>0$, let

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

Try to guess what should be $N(X)$ approximately as $X\to\infty$. Try to either

i) check your guess numerically,

ii) prove your guess in the form

$$N(X)=N_0(X)+O(X^{1/2}).$$