

**FINITE GROUPS AND EQUATIONS OVER FINITE  
FIELDS**  
**A PROBLEM SET FOR ARIZONA WINTER SCHOOL**  
2016

PREPARED BY SHABNAM AKHTARI

**Introduction and Notations**

The problems in Part I are related to Andrew Sutherland's lectures. We follow the notations and definitions in the lecture notes [6], as well as Serre's book [4]. Following Serre [4] (and Bourbaki's notation), we will denote the  $n$ -dimensional projective space by  $\mathbf{P}_n$  (and not by  $\mathbf{P}^n$ ). The problems are in different levels of difficulty. Some are there to ensure that the students understand the basic definitions, others are to motivate thinking and discussing some relevant mathematical ideas. There is some overlap between the set of problems here and those in the lecture notes [6].

The problems in Part II are related to Harald Helfgott's lectures and we follow the notations and definitions in the lecture notes [2]. Indeed, most of the problems in Part II are designed by Professor Helfgott. The students benefit from refreshing their background in Basic Group Theory before trying to solve these problems. There is a large overlap between the set of problems here and those in the lecture notes [2]. The students are strongly encouraged to understand the lecture notes in detail and have the notes by their sides while working on this problem set.

## 1. PART I, EQUATIONS OVER FINITE FIELDS

**Definition of  $N_X(p^e)$ .**

Let  $f_\alpha(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$  be a family of polynomials with integer coefficients. If  $p$  is a prime number let  $N_f(p^e)$  be the number of solutions of the equations  $f_\alpha = 0$  in a finite field of order  $p^e$ , with  $e$  a positive integer.

**1.1.** Let  $f_\alpha$  be a family of polynomials with integer coefficients. Let  $(f_\alpha)$  be the ideal of  $\mathbb{Z}[X_1, \dots, X_n]$  generated by the polynomials  $f_\alpha$ . Write the above definitions of  $N_X(p)$  and  $N_X(p^e)$  in the language of commutative algebra by corresponding the points  $x \in (\mathbb{F}_p)^n$  with  $f_\alpha(x) = 0$  to the maximal ideals of  $\mathbb{Z}[X_1, \dots, X_n]/(f_\alpha)$  with residue field  $\mathbb{F}_p$ .

**1.2.** Let  $X$  be a scheme of finite type over  $\mathbb{Z}$ . Write the above definitions of  $N_X(p)$  and  $N_X(p^e)$  in the scheme setting.

**1.3.** For polynomials  $f$  of degree  $d = 3$  there is a one-to-one correspondence between subgroups of  $S_d$  and distributions of  $N_f(p)$ . This is not true for  $d \geq 4$ . Give an example of a polynomial of degree 3 and show the above mentioned correspondence. Give an example of a polynomial of degree 4 and show that there is not such a correspondence.

**The zeta function**

**1.4.** The zeta function of the scheme  $X$  is defined by the infinite product

$$\zeta_X(s) = \prod_{x \in \underline{X}} \frac{1}{1 - |x|^{-s}},$$

where  $x$  runs through the set  $\underline{X}$  of closed points of  $X$  and  $|x|$  is the number of elements of the residue field  $\kappa(x)$ . The product converges absolutely for  $\text{Re}(s) > \dim X$ .

**1.5.** Write an Euler product for the Dirichlet's series  $\zeta_X(s)$ .

**1.6.** Let  $a_n$  be the coefficients of  $\zeta_{X,p}(s)$ . We have the following identity:

$$N_X(p)t + N_X(p^2)\frac{t^2}{2} + \dots = \log(1 + a_p t + a_{p^2} t^2 + \dots).$$

Express  $N_X(p)$ ,  $N_X(p^2)$ ,  $N_X(p^3)$  and  $N_X(p^4)$  in terms of  $a_n$ 's.

**1.7.** Let  $X$  be the reduction of a non-singular variety  $Y$  defined over a number field  $K$ . Assume that

$$Z_X(T) = \frac{P_1(T) \dots P_{2n-1}(T)}{P_0(T) \dots P_{2n}(T)},$$

where  $P_i \in \mathbb{Z}[T]$  and  $P_i(0) = 1$ . Show that the degree of  $P_i$  is equal to the Betti number  $b_i$  of  $Y(\mathbb{C})$ .

**1.8.** Show that if  $q$  is a prime power then the Fermat curve of degree  $q + 1$  has  $q^3 + 1$  rational points.

**1.9.** Show that for every matrix  $A \in \text{GL}_d(\mathbb{C})$  we have

$$\exp\left(\sum_{r=1}^{\infty} \text{tr} A^r \frac{T^r}{r}\right) = \det(1 - AT)^{-1}$$

( $T$  is a variable).

### Computing $N_X(p^e)$ .

**1.10.** Let  $X$  be given by the equation  $x^2 + y^2 = 0$ . Compute  $N_X(p^e)$  for every prime number  $p$ .

**1.11.** Let  $N \pmod{p^e}$  be the number of solutions of  $x^2 + y^2 = 0$  in the ring  $\mathbb{Z}/p^e\mathbb{Z}$ . Show that

(i)  $N \pmod{2^e} = 2^e$ .

(ii) If  $p \equiv 1 \pmod{4}$ , then  $N \pmod{p^e} = (e + 1)p^e - ep^{e-1}$ .

(iii) If  $p \equiv 3 \pmod{4}$ , then  $N \pmod{p^e} = p^e$  if  $e$  is even and  $N \pmod{p^e} = p^{e-1}$  if  $e$  is odd.

**1.12. (An Example of Genus 0)**

Let  $X$  be the conic in the projective plane  $\mathbf{P}_2$  defined by the equation

$$x^2 + y^2 + z^2 = 0.$$

Compute  $N_X(p)$ .

*Remark.* The easy way is to use Weil's Bound. Try not to use Weil's bound and give a direct argument.

**1.13.** Let  $X$  be the conic in the projective plane  $\mathbf{P}_2$  defined by the equation

$$x^2 + y^2 + z^2 = 0.$$

Show that

$$\zeta_X(s) = \zeta(s)\zeta(s-1).$$

**1.14. (An Example of Genus 1 with Complex Multiplication)**

Let  $X$  be the elliptic curve in  $\mathbf{P}_2$  given by the affine equation

$$y^2 = x^3 - x.$$

Compute  $N_X(p)$ .

**1.15.** Let  $X$  be the elliptic curve in  $\mathbf{P}_2$  given by the affine equation

$$y^2 - y = x^3 - x^2.$$

Show that this curve has good reduction outside  $p = 11$ . What is the conductor of  $y^2 - y = x^3 - x^2$  ?

**1.16. (Genus 1 without Complex Multiplication)** Let  $X$  be the elliptic curve in  $\mathbf{P}_2$  given by the equation

$$y^2 - y = x^3 - x^2.$$

Find the zeta function of  $X$ .

**1.17.** Let  $X$  be the curve in the previous problem. Let  $N_X(\text{mod } p)$  be the number of points of the projective curve  $X$  in the ring  $\mathbb{Z}/p^e\mathbb{Z}$ . Show that

- (i)  $N_X(\text{mod } p) = p^{e-1}N_X(p)$  if  $p \neq 11$ .
- (ii)  $N_X(\text{mod } p) = p^e - p^{e-1}$  if  $p = 11$  and  $e > 1$ .

**1.18.** Let  $X$  be the quadratic in  $\mathbf{P}_3$  defined by the homogeneous equation

$$ax^2 + by^2 + cz^2 + dt^2 = 0$$

where  $a, b, c, d$  are non-zero integers. Compute  $N_X(p^e)$ .

### The Hasse-Witt Matrix

**Definition.** Let  $\overline{C}/\mathbb{F}_p$  be a hyperelliptic curve of genus  $g$  defined by an equation of the form  $y^2 = f(x)$ . Let  $n = \frac{p-1}{2}$  and let  $f_k^n$  denote the coefficient of  $x^k$  in the polynomial  $f(x)^n$ . The Hasse-Witt matrix of  $\overline{C}$  is the  $g \times g$  matrix  $W_p : [w_{i,j}]$  over  $\mathbb{F}_p$ , where

$$w_{i,j} := f_{ip-j}^n \quad (1 \leq i, j \leq g).$$

It is known that the characteristic polynomial  $\chi$  of the Frobenius endomorphism of  $\text{Jac}(\overline{C})$  satisfies

$$\chi(\lambda) \equiv (-1)^g \lambda^g \det(W_p - \lambda I) \pmod{p}.$$

**1.19.** Show that

$$\text{tr} W_p \equiv t_p \pmod{p},$$

where

$$(1) \quad t_p := p + 1 - \#\overline{C}(\mathbb{F}_p).$$

**Definition.**  $t_p$  defined in (1) is called the trace of Frobenius.

**1.20.** Use Weil's bound to obtain an upper bound for  $t_p$  in the previous Exercise.

**1.21.** Does the trace of  $W_p$  uniquely determine the integer  $t_p$ .

**1.22.** Find the Hasse-Witt matrix of  $y^2 = ax^d + bx^e$ .

**1.23.** Prove that in each row of the Hasse-Witt matrix of  $y^2 = ax^d + bx^e$  there is at most one non-zero entry.

### Weil Conjectures

**1.24.** Let  $f \in \mathbb{Z}[x]$  be a non-constant squarefree polynomial. Prove that the average value of  $N_f(p)$  over  $p \leq B$  converges to the number of factors of  $f$  in  $\mathbb{Z}[x]$  as  $B \rightarrow \infty$ .

**1.25.** Let  $f_p \in \mathbb{F}_p$  denote a squarefree polynomial of degree  $d > 0$  and let  $L_p(T)$  denote the denominator of the zeta function  $Z_{f_p}(T)$ . We know that the roots of  $L_p(T)$  lie on the unit circle in the complex plane; show that each is in fact an  $n$ -th root of unity for some  $n \leq d$ . Give a one-to-one correspondence between (1) cycle-types of degree  $d$  permutations, (2) possible factorization patterns of  $f_p$  in  $\mathbb{F}_p[x]$ , and (3) the possible polynomials  $L_p(T)$ . Explain why non-conjugate elements of  $\rho_f(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$  may have the same characteristic polynomial (give an explicit example)

**1.26.** Construct a (not necessarily irreducible) quintic polynomial  $f \in \mathbb{Z}[x]$  with no roots in  $\mathbb{Q}$  for which  $f_p(x)$  has a root in  $\mathbb{F}_p$  for every prime  $p$ .

### Equidistribution

**1.27.** Let  $X$  be a compact Hausdorff space. Show that the only set  $S \subseteq X$  that are  $\mu$ -quarrable for every measure on  $X$  are the sets that are both open and closed.

**1.28.** Let  $(x_i)$  be a  $\mu$ -equidistributed sequence in  $X$  and  $S$  a  $\mu$ -quarrable set in  $X$ . Show that

$$\mu(S) = \lim_{n \rightarrow \infty} \frac{\#\{x_i \in S : i \leq n\}}{n}.$$

**1.29.** Let  $G$  be a compact commutative Lie group (written multiplicatively) containing an element  $z$  such that the set  $\{z^n : z \in \mathbb{N}\}$  is dense in  $G$ . Show that the sequence  $(z, z^2, z^3, \dots)$  is equidistributed with respect to the Haar measure on  $G$ .

**1.30.** Compute the trace moment sequence for  $\text{SU}(2)$ .

## 2. PART II, GROUPS

**2.1.** Let  $K = \mathbb{Z}/p\mathbb{Z}$ . Show that the group

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in K \right\}$$

is nilpotent.

**2.2.** Let  $K = \mathbb{Z}/p\mathbb{Z}$ . Show that the group

$$\left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in K \right\} \quad (\text{Heisenberg group})$$

is nilpotent, but not abelian.

**2.3.** Let  $G$  be a group. Let  $H < G$ ,  $g \in G \setminus H$  and  $A = H \cup \{g\}$ . Then  $|A^2| < 3|A|$ , but  $A^3 \supset HgH$ , and  $HgH$  may be much larger than  $A$ . Give an example with  $G = \text{SL}_2(\mathbb{Z}/p\mathbb{Z})$ .

**2.4.** Let  $G$  be a group. Prove that

$$\frac{|(A \cup A^{-1} \cup \{e\})^3|}{|A|} \leq \left( 3 \frac{|A^3|}{|A|} \right)^3$$

for every finite subset  $A$  of  $G$ . Show as well that, if  $A = A^{-1}$  (i.e., if  $g^{-1} \in A$  for every  $g \in A$ ), then

$$\frac{|A^k|}{|A|} \leq \left( \frac{|A^3|}{|A|} \right)^{k-2}.$$

for every  $k \geq 3$ . Conclude that

$$\frac{|A^k|}{|A|} \leq 3^{k-2} \left( \frac{|A^3|}{|A|} \right)^{3(k-2)}$$

for every  $A \subset G$  and every  $k \geq 3$ .

**2.5.** [Orbit-stabilizer theorem for sets] Let  $G$  be a group acting on a set  $X$ . Let  $x \in X$ , and let  $A \subseteq G$  be non-empty. Show that

$$|(A^{-1}A) \cap \text{Stab}(x)| \geq \frac{|A|}{|Ax|}.$$

Moreover, for every  $B \subseteq G$ ,

$$|BA| \geq |A \cap \text{Stab}(x)||Bx|.$$

**2.6.** Let  $G$  be a group acting on a set  $X$ . Let  $x \in X$ , and let  $A \subseteq G$  be non-empty and  $B \subseteq G$ . Show that

$$|BA| \geq |A \cap \text{Stab}(x)||Bx|.$$

**2.7.** Let  $G$  be a group and  $H$  a subgroup of  $G$ . Let  $A \subset G$  be a non-empty set with  $A = A^{-1}$ . Prove that, for any  $k > 0$ ,

$$|A^{k+1}| \geq \frac{|A^k \cap H|}{|A^{-1}A \cap H|}|A|.$$

**2.8.** Let  $G$  be a group and  $H$  a subgroup of  $H$ . Let  $A \subset G$  be a non-empty set. Then

$$|A^{-1}A \cap H| \geq \frac{|A|}{r},$$

where  $r$  is the number of cosets of  $H$  intersecting  $A$ .

**2.9.** Give an example of a group  $G$  and  $A \subset G$  such that  $|A+A| < 2|A|$ .

**2.10.** Let  $G$  be an abelian group, and  $A \subset G$  of bounded size. Show that  $|A|^k \leq \binom{|A|+k-1}{|A|-1}$ . Then conclude that for  $|A|$  fixed,  $|A^k|$  grows polynomially on  $k$ . What Can you say about the degree of this polynomial?

**2.11.** Modify the previous problem for the special case  $G = \mathbb{Z}$ .



**2.12.** Let  $A = \{a_1, a_2\}$  or  $A = \{a_1, a_2, a_3\}$  be a set of generators of the Heisenberg group

$$H(K) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in K \right\}$$

with  $K = \mathbb{Z}/p\mathbb{Z}$ . Our task, given any element  $g$  of  $H(K)$ , is to find a word of length  $O(p^{3/2}) = O(\sqrt{|H(K)|})$  on  $A$  equal to  $g$ . Show that this can be done in time polynomial on  $\log p$ . (Note that inverting an element of  $(\mathbb{Z}/p\mathbb{Z})^*$  takes time linearly on  $\log p$ , by the Euclidean algorithm.)

**2.13.** Let  $X \subset \mathbb{F}_p$ ,  $Y \subset \mathbb{F}_p^*$  be given with  $X = -X$ ,  $0 \in X$ ,  $1 \in Y$ . Show that

$$|6Y^2X| \geq \frac{1}{2} \min(|X||Y|, p).$$

**2.14.** Use the previous problem to show that for any  $A \subset \mathbb{F}_p^*$  with  $C < |A| < p^{1-\epsilon}$ ,  $\epsilon > 0$ , we have

$$\max(|A \cdot A|, |A + A|) > |A|^{1+\delta},$$

where  $C > 0$  and  $\delta > 0$  depend only on  $\epsilon$ .

**2.15.** For any  $\lambda_1, \dots, \lambda_k \in \mathbb{Z}$ , and any  $\epsilon > 0$ , prove that there is a constant  $C$  such that, for every prime  $p > C$ , there is a set  $S \cap \mathbb{F}_p$ ,  $0 < |S| \leq p/2$ , such that

$$(2) \quad |S \cup (S+1) \cup \lambda_1 S \cup \dots \cup \lambda_k S| \leq (1+\epsilon)|S|.$$

**2.16.** Let  $\lambda \geq 2$  be an integer. Define the *Baumslag-Solitar group*  $BS(1, \lambda)$  by

$$BS(1, \lambda) = \langle a_1, a_2 | a_1 a_2 a_1^{-1} = a_2^\lambda \rangle.$$

(1) A group  $G$  with generators  $a_1, \dots, a_\ell$  is called *amenable* if, for every  $\epsilon > 0$ , there is a finite  $S \subset G$  such that

$$|F \cup a_1 F \cup \dots \cup a_\ell F| \leq (1+\epsilon)|F|.$$

Show that  $BS(1, \lambda)$  is amenable.

- (2) Express the subgroup of the affine group over  $\mathbb{F}_p$  generated by the set

$$A = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

as a quotient of  $\text{BS}(1, \lambda)$ , i.e., as the image of a homomorphism  $\pi_p$  defined on  $\text{BS}(1, \lambda)$ .

- (3) Displace or otherwise modify your sets  $F$  so that, for each of them,  $\pi_p|_F$  is injective for  $p$  larger than a constant. Conclude that  $S = \pi_p(F)$  satisfies (2).

**2.17.** Let  $\lambda_0 \geq 2$  be an integer. Let  $\lambda = \lambda_0 \bmod p$ , which lies in  $\mathbb{F}_p^*$  for  $p > \lambda_0$ . Show that the diameter of the graph  $\Gamma_p$  defined above is  $O(\lambda_0 \log p)$ .

**2.18.** Let  $G_p = \text{SL}_2(\mathbb{Z}/p\mathbb{Z})$ . Prove that the diameter of  $G_p$  with respect to any set of generators  $A$  is  $(\log |G_p|)^{O(1)}$ .

## REFERENCES

- [1] F. Fité and A.V. Sutherland, Sato-Tate groups of  $y^2 = x^8 + c$  and  $y^2 = x^7 - cx$ , in Frobenius Distributions on Curves, Contemporary Mathematics, AMS, to appear.
- [2] H.A. Helfgott, Growth and expansion in groups of Lie type, Notes for the Arizona Winter School 2016.
- [3] H.A. Helfgott, Growth in groups: ideas and perspectives, To appear in Bull. Am. Math. Soc.
- [4] J.P. Serre, Lectures on  $N_X(p)$ , Research Notes in Mathematics 11, CRC Press, 2012.
- [5] S. Lang and H. Trotter, Frobenius distributions in  $GL_2$ -extensions, Lecture Notes in Mathematics 504 (1976), Springer.
- [6] A.V. Sutherland, Sato-Tate distribution, Notes for the Arizona Winter School 2016.