ABELIAN VARIETIES OVER FINITE FIELDS

1. Introduction

1.1. **Goal.** In this series of lectures, we will study abelian varieties over finite fields. The main goal is to understand the Honda-Tate Theorem which classifies abelian varieties over $\mathbf{F}_q$ up to isogeny in terms of Weil q-numbers. The lectures will be broken down into the key results, which combine to give the purely algebraic proof of Honda-Tate by Chai–Oort. For background material, we refer to [3, 5, 4, 11] or Edixhoven, Moonen and van der Geer's book available at http://van-der-geer.nl/~gerard/AV.pdf. For the main results of Honda and Tate, we use the references [8, 9]. The expository notes [1, 6] can also be useful.

1.2. **Prerequisites.** We will assume some knowledge of third year algebra. But we will not assume any knowledge of abelian varieties. The main results from algebraic geometry will be treated as black boxes. We will strive to illustrate the theory with as many examples as possible, mainly using elliptic curves [7, 10].

2. Abelian varieties over finite fields

2.1. **Introduction to abelian varieties over finite fields.** Give the definition of abelian varieties over a field. Discuss isogenies, existence of dual abelian variety and polarisations.

2.2. **Endomorphism rings and Tate modules.** Study endomorphism rings and Tate modules of abelian varieties.

2.3. **Tate's isogeny theorem.** Define the geometric Frobenius and Verschiebung maps and explain their relation on the dual abelian variety. Give the main ideas in the proof of Tate's isogeny theorem: For an abelian variety $A/\mathbf{F}_q$ and a prime $\ell \neq p$, the map

$$\mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \to \mathrm{End}(T_\ell A)$$

is an isomorphism.

2.4. **The Weil conjecture.** Discuss the proof of Weil's theorem: For a simple abelian variety $A/\mathbf{F}_q$, the geometric Frobenius $\pi_A \in \mathrm{End}(A)$ is a Weil q-number, that is, it is an algebraic integer and for every complex embedding $\psi : \mathbf{Q}(\pi_A) \to \mathbf{C}$, we have $|\psi(\pi_A)| = q^{1/2}$.

2.5. **p-divisible groups, Dieudonné modules and Serre–Tate deformation theory.** Define p-divisible groups and give examples. State (without proofs) the main results on Dieudonné theory over perfect fields. State the main theorem relating the deformation of abelian varieties and their p-divisible groups and explain the proof.

2.6. **Proof of Honda-Tate's Theorem.** Honda-Tate's Theorem states that the map

$$\{\text{Simple abelian varieties over } \mathbf{F}_q\}/\text{isogeny} \to \{\text{Weil } q\text{-numbers}\}/\text{conjugation}$$
$$A \mapsto \pi_A$$

is a bijection. The fact that this map is well-defined and injective follows from previous lectures. We will show that the map is surjective by following the short algebraic proof given by Chai and Oort [2].

References

[1] Ching-Li Chai and Frans Oort, *Moduli of abelian varieties and p-divisible groups*, Arithmetic geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, pp. 441–536. MR 2498069

[2] Ching-Li Chai and Frans Oort, *An algebraic construction of an abelian variety with a given Weil number*, Algebr. Geom. 2 (2015), no. 5, 654–663. MR 3421786

[3] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR 861974

[4] J. S. Milne and W. C. Waterhouse, *Abelian varieties over finite fields*, Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64. MR 0314847

[5] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008, With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR 2514037

[6] Frans Oort, *Abelian varieties over finite fields*, Higher-dimensional geometry over finite fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, pp. 123–188. MR 2484079

[7] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, Grad. Texts in Math., 106 Springer, Dordrecht, 2009. xx+513 pp.

[8] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 13400144. MR 206004

[9] John Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini* (d'après T. Honda), Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 352, 95–110. MR 3077121

[10] W. Trappe and L. C. Washington, *Introduction to cryptography with coding theory*, Pearson Prentice Hall, Upper Saddle River, NJ, 2006, xiv+577 pp.

[11] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969), 521–560. MR 265369