1. HPS 5.12: Elliptic Curve Pollard ρ

Read the abstraction of Pollard ρ given in HPS 4.5 and how it can be used to solve the Discrete Log Problem on $\mathbb{F}_p$. Adapt this material to create a Pollard ρ algorithm to solve the ECDLP.

2. HPS 5.27: Well-Definedness of the Weil Pairing

Here, we will show that the Weil pairing is well-defined! Let E/F be an elliptic curve over a field F such that $char(F)$ does not divide m, and let $P, Q \in E[m]$.

(a) Prove that $e_m(P, Q)$ is independent of the choice of rational functions f_P and f_Q.

(b) Prove that $e_m(P, Q)$ is independent of the auxiliary point S. (Hint: Fix P and Q and consider the quantity

$$F(S) = \frac{f_P(Q+S)}{f_P(S)} \bigg/ \frac{f_Q(P-S)}{f_Q(S)}$$

as a function of S. Compute the divisor of F and use the fact that every nonconstant function on E has at least one zero.)

3. The Tate-Lichtenbaum Pairing

Let $E/\mathbb{F}_p$ be an elliptic curve. One shortcoming of the Weil pairing on $E[m]$ is that it can be somewhat cumbersome to work with computationally (as will be explored in lecture). An alternative for it is the **Tate-Lichtenbaum Pairing**, which is defined as follows:

Let ℓ be prime not equal to p, let $P \in E[\ell]$, and let $Q \in E(\mathbb{F}_p)$. Choose a rational function f_P on E such that $div(f_P) = \ell[P] - \ell[O]$. Then, the Tate-Lichtenbaum Pairing of P and Q is

$$\tau(P, Q) = \frac{f_P(Q+S)}{f_P(S)} \in \mathbb{F}_p^\times$$

where S is any point such that $f_P(Q+S)$ and $f_P(S)$ are well-defined and non-zero.

(a) Show that the Tate Pairing is well-defined using a method similar to problem 2 parts a) and b).

(b) Show that there is the following relationship between the Tate-Lichtenbaum Pairing and the Weil Pairing, assuming $Q \in E[\ell]$:

$$e_\ell(P, Q) = \frac{\tau(P, Q)}{\tau(Q, P)}$$

Hence, we can recover the Weil Pairing from the Tate-Lichtenbaum Pairing! This is helpful since the Tate-Lichtenbaum pairing is easier to calculate (cf. Silverman XI.9).

EXTRA CREDIT: The following problems build some key theory of elliptic curves that we did not have time to discuss in class. It is reliant on some detailed and difficult concepts that are too time-consuming for the general problem set. Do/think about these if you want a fun extra challenge or are generally interested!

4. Inverse Limits and Adic Completions

Let $(J, \leq)$ be a directed set with partial order $\leq$. By this, we mean that for every $i, j \in J$, there exists some k such that $i \leq k$ and $j \leq k$. We say that a set of algebraic objects $\{S\}_{j\in J}$ (groups, abelian groups, rings, etc.) indexed by J forms an **inverse system** if for every S_i and S_k such that $i \leq k$, there exists a morphism $f_{ki} : S_k \to S_i$ such that $f_{ki} = f_{ji} \circ f_{kj}$ for all $i \leq j \leq k$. We form the **inverse limit** as

$$\varprojlim_j S_j = \{(s_j)_j \mid f_{ki}(s_k) = s_i\} \subseteq \prod_j S_j$$

Here, we are requiring a condition that going down in indexing via the maps f_{ki} is equivalent to going down in indexing in the natural way.

(a) Show that inverse limits are functorial: for two inverse systems of groups or rings $(\{A_i\}_{i\in I}, f_{ij}), (\{B_i\}_{i\in I}, g_{ij})$ indexed by the same indexing set I, show that if there exists a homomorphism $\phi_i : A_i \to B_i$ for all i such that $f_{ij} \circ \phi_j = \phi_i \circ g_{ij}$, there exists a unique morphism $\varprojlim \phi : \varprojlim A_i \to \varprojlim B_i$.

(b) Show that on a general ring R and an ideal I, there is a natural topology whose basis is given by $x + I^n R$ for each $x \in R$.

(c) We define R's **I-adic completion** to be the inverse limit

$$\hat{R} = \varprojlim_n \; R/I^n.$$

with respect to the inverse system induced by the natural projections $R/I^{n+1} \to R/I^n$. Show that $\hat{R}$ is complete in the topology that R's I-adic topology induces on it (Hint: how can you relate this construction to Cauchy sequences?).

(d) Let $R[x]$ be the polynomial ring of R. Exhibit an explicit isomorphism between the (x)-adic completion of $R[x]$ and the ring of formal power series $R[|x|]$.

(e) Choose a prime number p. We define the **p-adic integers** $\mathbb{Z}_p$ to be the completion of $\mathbb{Z}$ at the prime ideal (p) with fraction field $\mathbb{Q}_p$, the **p-adic numbers**. Show that $\mathbb{Q}_p$ is locally compact and totally disconnected with respect to the p-adic topology (Hint: can you find a connection between $\mathbb{Q}_p$ and the Cantor set?).

5. Direct Limits, Algebraic Closure, and the Absolute Galois Group

Let J be a directed set as in Problem 2. We say that a set of algebraic $\{S\}_{j\in J}$ indexed by J forms a **directed system** if for every S_i and S_k such that $i \leq k$, there exists a morphism $f_{ik} : S_i \to S_k$ such that $f_{ik} = f_{jk} \circ f_{ij}$ for all $i \leq j \leq k$. This extends to any other category that is built upon sets (topological spaces, vector spaces, abelian groups, etc.), substituting maps of sets with the appropriate morphisms.

For any directed system, we can form its **direct limit** as

$$\varinjlim_j S_j = \bigsqcup_j S_j / \sim$$

where two elements $(s_j, S_j) \sim (s_i, S_i)$ if and only if there exists some $i, j \leq k$ such that $f_{jk}(s_j) = f_{ik}(s_i)$. Essentially, we are quotienting out by a condition that elements are "eventually equal" in a larger element of the ordering.

(a) Let F be a perfect field, and choose an algebraic closure $\widetilde{F}$. Show that the set of finite subextensions $\widetilde{F}/K/F$ form a directed system with respect to inclusion (Hint: compositum!).

(b) Show that $\widetilde{F}$ can be identified with the direct limit $\varinjlim K$, where K ranges over the finite subextensions of $\widetilde{F}/F$ as defined in part a). Note that here we replace the disjoint union in the definition of disjoint union with the compositum of field extensions.

(c) Show that $Gal(\widetilde{F}/F) \cong \varprojlim Gal(K/F)$, where $Gal(K/F)$ ranges over the finite extensions of F with respect to the natural restrictions (Hint: contravariance of the Galois correspondence and how it acts on compositums).

6. Profinite Groups and the Profinite Topology

A group G is called **profinite** if it can be written as

$$G = \varprojlim_{i} \; H_i$$

where H_i are finite groups. Any finite group is obviously profinite. We saw in the last problem that $Gal(\widetilde{F}/F)$ for a field F is a nontrivial example of a profinite group!

(a) Show that a profinite group G has a natural topology with basis given by finite index normal subgroups. We call this topology the **profinite topology**.

(b) Show that $Gal(\widetilde{\mathbb{F}}_p/\mathbb{F}_p)$ is topologically generated by the arithmetic Frobenius

$$\mathrm{Frob}_{\widetilde{\mathbb{F}}_p} = (1, \mathrm{Frob}_{\mathbb{F}_{p^2}}, \mathrm{Frob}_{\mathbb{F}_{p^3}}, \mathrm{Frob}_{\mathbb{F}_{p^4}}, ...)$$

where $\mathrm{Frob}_{\mathbb{F}_{p^n}}$ is the Frobenius generator of $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. By this, we mean that the closure of the subgroup $\langle \mathrm{Frob}_{\widetilde{\mathbb{F}}_p} \rangle$ is isomorphic to $Gal(\widetilde{\mathbb{F}}_p/\mathbb{F}_p)$. We say that $Gal(\widetilde{\mathbb{F}}_p/\mathbb{F}_p)$ is a **pro-cyclic group**.

(c) (OPTIONAL CHALLENGE:) Show that any profinite group with the profinite topology is compact, Hausdorff, and totally disconnected (you will need some technical knowledge of topological groups!).

7. Galois representations: The l-adic Tate Module

Trying to flesh out the structure of $Gal(\widetilde{F}/F)$ for perfect fields F is one of the main objectives of algebraic number theory and arithmetic geometry. The best course of action is to study **Galois representations**, i.e. continuous group homomorphisms

$$Gal(\widetilde{F}/F) \longrightarrow GL_n(K)$$

for some topological field K, or a continuous action of $Gal(\widetilde{F}/F)$ on some topological K-vector space V. In this problem, we will explore why $\mathbb{Q}_\ell$ for some prime ℓ is a good choice for a base field, and how we can generate these representations from elliptic curves!

(a) Show that any complex Galois representation $Gal(\widetilde{\mathbb{Q}}/\mathbb{Q}) \to GL_n(\mathbb{C})$ must necessarily factor through a map $Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C})$ with $K/\mathbb{Q}$ a finite extension (Hint: what can you say about the kernel given the respective topologies of $GL_n(\mathbb{C})$ and $Gal(\widetilde{\mathbb{Q}}/\mathbb{Q})$?). Hence, a complex Galois representation is simply a representation of a finite group! We call these representations **Artin representations**.

(b) Let E be an elliptic curve defined over a perfect field F, and let ℓ be a prime number not equal to the characteristic of F. Show that the natural action of $Gal(\widetilde{F}/F)$ on $F[\ell^n](\widetilde{F})$ gives rise to a $\mathbb{Z}_\ell$-module with a natural action of $Gal(\widetilde{F}/F)$. Show that this forms a Galois representation upon tensoring with $\mathbb{Q}_\ell$. We call the associated vector space the **ℓ-adic Tate module** and denote it $V_\ell(E)$.

(c) Recall in lecture that we discussed the Frobenius map of an elliptic curve $E/\mathbb{F}_p$, which was defined as

$$\mathrm{Frob}_p : E(\widetilde{\mathbb{F}}_p) \to E(\widetilde{\mathbb{F}}_p), (x, y) \to (x^p, y^p).$$

Show that this is gives a well-defined endomorphism on $E[\ell^n](\widetilde{\mathbb{F}}_p)$, inducing a linear map $V_\ell(E) \to V_\ell(E)$. How can you interpret this in terms of the Galois action given what we know about $Gal(\widetilde{\mathbb{F}}_p/\mathbb{F}_p)$?

(d) Read Silverman V.1 and V.2 and understand why the quantity $a = p + 1 - \#E(\mathbb{F}_p)$ is the trace of the above Frobenius map.