TCC Galois Representations 2025 - Assignment

Problem 1. Let $K = \mathbb{Q}(i, \sqrt{17})$.

(1) Show that for every prime number $p \neq 2, 17$, either -1 or 17 or -17 is a square modulo p (possibly all 3).
(2) Show that $p = 17$ splits in $\mathbb{Q}(i)$ and that $p = 2$ splits in $\mathbb{Q}(\sqrt{17})$.
(3) Deduce that every prime p of $\mathbb{Q}$ splits into 2 or 4 primes of K, and consequently $\zeta_K(s)$ has every local polynomial $F_p(T)$ of the form $G_p(T)^2$ for some (usually quadratic) $G_p(T) \in \mathbb{Z}[T]$.

NB. In other words, just looking at the local factors, $\zeta_K(s)$ looks like a square of some reasonable function. But it certainly isn't! It has a simple pole at $s = 1$, so whatever $\prod_p G_p(p^{-s})^{-1}$ is, it does not have a meromorphic continuation to $\mathbb{C}$. (This gives some indication that meromorphic continuation is a subtle business, and we cannot expect it for any function with reasonable arithmetic coefficients.

Problem 2. Let p^n be a prime power and $F = \mathbb{Q}(\zeta)$, $\zeta = \zeta_{p^n}$, the p^nth cyclotomic field. It is a standard fact that the ring of integers of K is $\mathbb{Z}[\zeta]$, and that $\pi = 1 - \zeta$ generates the unique ideal above p,

$$(\pi)^{\phi(p^n)} = (p).$$

(1) Determine the decomposition group $D = D_p = D_\pi$, the inertia group $I = I_p = I_\pi$ in $\mathrm{Gal}(F/\mathbb{Q}) = (\mathbb{Z}/p^n\mathbb{Z})^\times$, and its filtration by the higher ramification groups
$$\{1\} = I_k \lhd \cdots I_2 \lhd I_1 \lhd I_0 = I.$$
(2) Let χ be a primitive character of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, that is of modulus p^n. Prove, by definition of the conductor, that the associated 1-dimensional Galois representation ρ_χ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ has conductor $N(\rho) = p^n$.

Hint: $\sigma \equiv \mathrm{id} \bmod \pi^k \iff v_\pi(\zeta - \sigma(\zeta)) \geq k$.

NB. The same argument, with a bit more notation, can be used to show that conductor=modulus for any Dirichlet character.

Problem 3. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 1/4$.

(1) On any elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}$ the x-coordinates of the 8 non-trivial 3-torsion points are roots of the 3-division polynomial $x^4 + 2ax^2 + 4bx - a^2/3$. Use this to find $E[3]$.
(2) Find a basis of $E[3]$ in which $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[3]$ as $\sigma \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi(\sigma) \end{smallmatrix}\right)$, where χ is the non-trivial irreducible representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$.
(3) Considering the 3-adic Tate module T_3E, show that for every prime p at which E has good reduction, the local factor of $L(E/\mathbb{Q}, s)$
$$F_p(T) = \det\left(1 - \mathrm{Frob}_p^{-1} T \mid V_3E^*\right) = 1 - aT + pT^2$$
has $a \equiv 2 \mod 3$ if $p \equiv 1 \mod 3$ and $a \equiv 0 \mod 3$ if $p \equiv 2 \mod 3$.