Math 620 Home Work Assignment 3

1. Let K be an imaginary quadratic field. For every $z \in K$ with $\mathrm{Im}(z) > 0$, let L_z be the lattice $\mathbb{Z} + \mathbb{Z} \cdot z \subset \mathbb{C}$, and let E_z be the elliptic curve $\mathbb{C}/L_z$. Denote by $j(z) = j(E_z)$ the j-invariant of E_z.

   (i) The ring of endomorphisms $\mathrm{End}(E_z)$ of E_z is an order of $\mathcal{O}_K$, necessariy equal to $\mathbb{Z}+f\mathcal{O}_K$ for a unique $f \in \mathbb{N}_{>0}$. Show that $K(j(z))$ is the ring class field of K with conductor f, i.e. the abelian extension of K which corresponds to the subgroup

   $$\big((\mathbb{Z} + f\mathcal{O}_K) \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}\big)^\times \cdot (K_\infty^\times \cdot K^\times)/(K_\infty^\times \cdot K^\times) \;\subset\; \mathbb{A}_K^\times/(K_\infty^\times \cdot K^\times)$$

   under class field theory.

   (ii) Let $K^\dagger$ be the extension field of K generated by $\mathbb{Q}^{\mathrm{cycl}}$ and all elements of the form $j(z)$, with $z \in K$, $\mathrm{Im}(z) > 0$. Describe the abelian extension $K^\dagger$ of K using class field theory, and show that $\mathrm{Gal}(K^{\mathrm{ab}}/K^\dagger)$ is a product of groups of order 2.

2. Let k be an number field. Denote by ${}^k\mathfrak{S}$ the quotient of $\underline{k^\times} = \mathrm{Res}_{k/\mathbb{Q}}\mathbb{G}_{\mathrm{m}}$ such that

   $$X^*({}^k\mathfrak{S}) = \big\{\, \chi \in X^*(\underline{k^\times}) \mid (1-\sigma)(1+\iota)\,\chi = (1+\iota)(1-\sigma)\,\chi = 0, \quad \forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \,\big\}$$

   where ι denotes a complex conjugation. Prove that there exists a subgroup $\Gamma \subset \mathcal{O}_K^\times$ of finite index such that for every subgroup $\Gamma_1 \subset \Gamma$ of finite index, the quotient of $\underline{k^\times}$ by the Zariski closure of Γ_1 is equal to ${}^k\mathfrak{S}$.

3. Let k be a number field. Recall that a $\mathbb{C}^\times$-valued algebraic Hecke character

   $$\psi : \mathbb{A}_k/k^\times \to \mathbb{C}^\times$$

   is a continuous character such that the restriction

   $$\psi_{\infty,+} : k_{\infty,+}^\times = (k \otimes_{\mathbb{Q}} \mathbb{R})_+^\times \to \mathbb{C}^\times$$

   of ψ to the neutral component $k_{\infty,+}$ of $k_\infty = k \otimes_{\mathbb{Q}} \mathbb{R}$ coincides with the restriction to $k_{\infty,+}$ of a character χ_ψ of $\underline{k^\times}$ defined over $\mathbb{C}$; sometimes χ_ψ is called the *infinity type* of ψ. Use the problem 2 above to show the following.

   (i) For every algebraic Hecke character ψ of $\mathbb{A}_k^\times$, the infinity component ψ_∞ factors through the quotient $\underline{k^\times} \twoheadrightarrow {}^k\mathfrak{S}$.

   (ii) If two algebraic Hecke characters ψ, ψ' have the same infinity component, then $\psi' \cdot \psi^{-1}$ has finite order.

   (iii) Every character of ${}^k\mathfrak{S}$ is the infinity component of an algebraic Hecke character of $\mathbb{A}_k^\times$.

4. We use the geometric normalization for the reciprocity law
$$\mathrm{rec}_{\mathbb{Q}} : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})\,.$$
Let $\chi_{\mathrm{cyc}} : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to (\widehat{\mathbb{Z}})^{\times}$ be the cyclotomic character coming describing the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ on the torsion points of $\mathbb{G}_{\mathrm{m}}$.

   (i) Show that $\chi_{\mathrm{cyc}} \circ \mathrm{rec}_{\mathbb{Q}}$ can be uniquely extended to an algebraic Hecke character
   $$\psi_{\mathrm{cyc}} : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to \widehat{\mathbb{Z}}^{\times} \times \mathbb{R}^{\times} \subset \mathbb{A}_{\mathbb{Q}}^{\times}$$
   such that ψ_{cyc} is the product of a continuous homomorphism $c : \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{Q}^{\times}$ and a homomorphism $\mathbb{G}_{\mathrm{m}}(\mathbb{A}_{\mathbb{Q}}) \to \mathbb{G}_{\mathrm{m}}(\mathbb{A}_{\mathbb{Q}})$ coming from a character χ of $\mathbb{G}_{\mathrm{m}}$.

   (ii) Show that the restriction of ψ_{cyc} to $\mathbb{Q}_p^{\times}$ is
   $$\psi_{\mathrm{cyc}}|_{\mathbb{Q}_p^{\times}} : a \mapsto \big(p^{-\mathrm{ord}_p(a)}, p^{-\mathrm{ord}_p(a)}a, p^{-\mathrm{ord}_p(a)}\big) \in \big(\textstyle\prod_{\ell\neq p} \mathbb{Z}_{\ell}^{\times}\big) \times \mathbb{Z}_p^{\times} \times \mathbb{R}^{\times}$$
   and the restriction of ψ_{cyc} to $\mathbb{R}^{\times}$ is
   $$\psi_{\mathrm{cyc}}|_{\mathbb{R}^{\times}} : a \mapsto \big(\mathrm{sgn}(a), |a|\big) \in \widehat{\mathbb{Z}}^{\times} \times \mathbb{R}^{\times}$$

5. (This problem is due to Shimura-Taniyama.) Let C be the projective completion of the affine curve over $\mathbb{Q}$ given by the equation $y^2 = x^p - 1$, where p is an odd prime number. Let $\mathbb{Q}(\mu_p)$ be the cyclotomic field generated by the p-th roots of unity, and let $\mathbb{Z}[\mu_p] = \mathcal{O}_{\mathbb{Q}(\mu_p)}$. There is an action of μ_p on C defined over $\mathbb{Q}_p$, given by
$$\zeta_p : (x, y) \to (\zeta_p\, x, y)$$
where ζ_p is a primitive p-th root of unity. This action gives an action of $\mathbb{Z}[\mu_p]$ on the Jacobian $\mathrm{Jac}(C) =: A$ of C, so that A is an abelian variety with CM by $\mathbb{Z}[\mu_p]$.

   (i) Prove that the genus of C is $g = \frac{p-1}{2}$.

   (ii) Show that for $i =, 1, \ldots, g)$, the meromorphic differential forms $\omega_i = \frac{x^{i-1}\,dx}{y}$ extends to regular differnetial forms on C and form a basis of $\mathrm{H}^0(C, K_C)$.

   (iii) The Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}$ is canonicallly isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\times}$, and consists of elements
   $$\sigma_i : \zeta_p \mapsto \zeta_p^i, \qquad i \in (\mathbb{Z}/p\mathbb{Z})^{\times}$$
   Show that the CM-type of A is equal to $\{\sigma_1, \ldots, \sigma_g\}$ and that the reflex field is equal to $\mathbb{Q}(\mu_p)$.

   (iv) Deduce from the theory of complex multiplication that for every ideal $\mathfrak{a} \subset \mathbb{Z}[\mu_p]$, there exists an element $x \in \mathbb{Q}(\mu_p)$ such that $N\mu(\mathfrak{a}) = (x)$ and $\mathbf{N}(\mathfrak{a}) = x\bar{x}$, where $N\mu$ denotes the reflex type norm. Note that this is a special case of the Stickelberger relation, see Lang's *Algebraic Number Theory*, Chap. 4, §4, Theorem 11.