Lecture 10 Quadratic Reciprocity and modular forms

Given an odd prime p, the Legendre symbol

$$\left(\frac{x}{p}\right) := \begin{cases} 1, & \text{if } \exists\, y \in \mathbb{Z} \text{ s.t. } y^2 \equiv x \pmod p \\ & \quad \& \; x \not\equiv 0 \pmod p \\ -1, & \text{if } \nexists\, y \in \mathbb{Z} \text{ s.t. } y^2 \equiv x \pmod p \\ & \quad \& \; x \not\equiv 0 \pmod p \\ 0 & \text{if } x \equiv 0 \pmod p \end{cases}$$

Prop 2 Let $F = \mathbb{F}_{p^d}$, p odd. We have a group homomorphism

$$F^\times \xrightarrow{\psi} F^\times$$
$$x \longmapsto x^{\frac{p^d-1}{2}}.$$

such that

(i) $\mathrm{Im}(\psi) = \{-1, 1\}$

(ii) $\mathrm{Ker}(\psi) = (F^\times)^2$

and $\forall\ a \in \mathbb{F}_p{}^\times$ we have $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Proof

For $a \in F^\times$ $\exists\ \alpha \in E$ s.t. $\underbrace{\alpha^2 = a}_{\star}$, so

$$a \in (F^\times)^2 \iff \alpha \in F^\times \iff \alpha^{p^d - 1} = 1$$

But each $a \in F^\times$ is a zero of the polynomial

$$X^{p^d-1} - 1 = \left(X^{\frac{p^d-1}{2}} - 1\right)\left(X^{\frac{p^d-1}{2}} + 1\right) \qquad *$$

$$\alpha^{p^d-1} \overset{(\star)}{=} \underbrace{a^{\frac{p^d-1}{2}}}_{=:\psi(a)} \overset{(*)}{=} \pm 1,$$

so $\mathrm{Im}(\psi) \subseteq \{-1, 1\}$ and also $\ker(\psi) = (F^\times)^2$.

But $F^\times$ is cyclic of even order. Hence $|F^\times/(F^\times)^2| = 2$,

so we have

$$\begin{array}{ccc} F^\times & \xrightarrow{\psi} & F^\times \\ & \overset{\hat{\psi}}{\nearrow} & \uparrow \\ \pi \downarrow & & \\ F^\times/(F^\times)^2 & \xrightarrow{\sim} & \{-1, 1\} \end{array}$$

and thus $\mathrm{Im}(\psi) = \{-1, 1\}$. In particular, for $F = \mathbb{F}_p$ we have $\forall\ a \in \mathbb{F}_p$

$$\left(\frac{a}{p}\right) = \psi(a) = a^{\frac{p-1}{2}} \qquad \square$$

Let p be an odd prime and pick a field F.

Let E be the splitting field of the polynomial $f_p(x) := X^p - 1$ over F and define

$$\mu_r := \{ x \in E : x^r = 1 \}$$

Assume that $\chi(F) \neq p$ so that μ_p has exactly p elements.

Since $\mu_p \subseteq E^\times$ and $|\mu_p| < \infty$, then $\exists\, \zeta \in \mu_p$ s.t. μ_p

Define the Gauss sum

$$S_p := \sum_{k \in \mathbb{F}_p} \left(\frac{k}{p}\right) \zeta^k \in E.$$

Lemma 3 Notation as above $S_p^2 = \left(\frac{-1}{p}\right) p$

Proof

$$S_p^2 = \left(\sum_j \left(\frac{j}{p}\right)\zeta^j\right)\left(\sum_k \left(\frac{k}{p}\right)\zeta^k\right) = \sum_j \sum_k \left(\frac{j}{p}\right)\left(\frac{k}{p}\right)\zeta^j\zeta^k =$$

perm. $(k \mapsto jk)$

$$\sum_j \sum_k \left(\frac{jk}{p}\right)\zeta^{j+k} = \sum_j \sum_k \left(\frac{j\,jk}{p}\right)\zeta^{j+jk} =$$

$$\sum_j \sum_k \left(\frac{j^2 k}{p}\right)\zeta^{j(1+k)} = \sum_j \sum_k \left(\frac{k}{p}\right)\zeta^{j(1+k)}$$

Hence

$$S_r^2 = \sum_j \sum_k \left(\frac{k}{p}\right) \zeta^{j(1+k)} =$$

$$\sum_j \sum_{k \neq -1} \left(\frac{k}{p}\right) \zeta^{j(1+k)} + \sum_j \left(\frac{-1}{p}\right) \zeta^0 =$$

$$\sum_{k \neq -1} \left(\frac{k}{p}\right) \underbrace{\sum_j \left(\zeta^{1+k}\right)^j}_{\| \; 0} + \sum_j \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) \sum_j 1 = \left(\frac{-1}{p}\right) r$$

[use Viète's formula.]

□

Lemma 4 Fix a prime $\ell \neq p$ and consider the Gauss sum S_p over $\mathbb{F}_\ell$. Then

$$S_p^{\ell} = \left(\frac{\ell}{p}\right) S_p$$

Proof

$$\left(k = r\ell^{-1}\right)$$

$$S_p^{\ell} = \left(\sum_{k \in \mathbb{F}_p} \left(\frac{k}{p}\right) \zeta^k\right)^{\ell} = \sum_{k} \left(\frac{k}{p}\right) \zeta^{k\ell} = \sum_{r} \left(\frac{r\ell^{-1}}{p}\right) \zeta^{r} =$$

$$\sum_{r} \left(\frac{r}{p}\right)\left(\frac{\ell^{-1}}{p}\right) \zeta^{r} = \sum_{r} \left(\frac{r}{p}\right)\left(\frac{\ell}{p}\right)^{-1} \zeta^{r} = \left(\frac{\ell}{p}\right) S_p \qquad \square$$

Thm (Gauss) If p and ℓ are distinct, odd primes then

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}$$

Proof

$$\left(\frac{\ell}{p}\right) = \left(S_p^{\,2}\right)^{\frac{\ell-1}{2}} = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{\ell-1}{2}} = \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}} p^{\frac{\ell-1}{2}} = \left((-1)^{\frac{p-1}{2}}\right)^{\frac{\ell-1}{2}} \left(\frac{p}{\ell}\right)$$

By Lemma 4 ↑ — By Lemma 3 ↓ — By Prop'n 2 ↓

$$= (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}} \left(\frac{p}{\ell}\right)$$

□

Let ℓ be a prime number > 2 and let $E := sf\, f(X) / \mathbb{F}_\ell$, where $f(X) = X^8 - 1$. Recall that

$$\mu_8 := \{ x \in E : x^8 = 1 \}$$

is a cyclic subgroup of $E^\times$. So let $\zeta \in \mu_8$ be a generator of μ_8.

We'll prove the following.

Propn 6 The element $\alpha := \zeta + \zeta^{-1}$ is s.t. $\alpha^2 = 2$.

Proof

Note that $f(X) = (X^4-1)(X^4+1)$. So the roots of the first factor are the elements of μ_4. So the primitivity of ζ implies that ζ is a root of the second factor $\Phi_8(X) = X^4+1$,

thus

$$\zeta^{-2}(\zeta^4+1) = 0$$

$$\zeta^2 + \zeta^{-2} = 0$$

and then

$$\alpha^2 = (\zeta+\zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2 \qquad \square$$

Prop 7 If we further assume that $\ell \equiv \pm 1 \pmod 8$, then

(a) $$\alpha^\ell = \alpha$$

(b) $$\left(\frac{2}{\ell}\right) = 1$$

Proof

Note that $\ell \equiv \pm 1 \pmod 8 \Rightarrow \zeta^\ell = \zeta^{8k \pm 1} = \zeta^{8k}\zeta^{\pm 1}$

$= (\zeta^8)^k \zeta^{\pm 1} = 1^k \zeta^{\pm 1} = \zeta^{\pm 1}$. Therefore

$$\alpha^\ell = \left(\zeta + \zeta^{-1}\right)^\ell = \zeta^\ell + \zeta^{-\ell} = \zeta^{\pm 1} + \zeta^{\mp 1} = \alpha$$

if $\ell \equiv \pm 1 \pmod 8$. Therefore

$$\left(\frac{2}{\ell}\right) = \left(\alpha^2\right)^{\frac{\ell-1}{2}} = \alpha^{\ell-1} = 1 \qquad \square$$

Prop 8 If $\ell \equiv \pm 3 \pmod 8$, then

(a) $$\alpha^{\ell} = -\alpha$$

(b) $$\left(\frac{2}{\ell}\right) = -1$$

Proof

[Ex]

Corollary For each odd prime ℓ we have $\left(\frac{2}{\ell}\right) = (-1)^{\frac{\ell^2-1}{8}}$.

Given any number field K, the Dedekind ζ-function $\zeta_K(s)$ is the Dirichlet series

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \text{ ideal of } \mathcal{O}_K} \mathcal{N}(\mathfrak{a})^{-s} =: \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s}$$

The fact that $\mathcal{O}_K$ is a Dedekind domain is equivalent to

$$\zeta_K(s) := \prod_{0 \neq \mathfrak{p} \text{ prime ideal of } \mathcal{O}_K} \left(1 - \mathcal{N}(\mathfrak{p})^{-s}\right)^{-1}.$$

Thm Let $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* := (-1)^{\frac{q-1}{2}} q$, where q is an odd prime. We have

$$\zeta_K(s) = \zeta(s) L(\chi, s)$$

where

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

and $\chi(n) := \left(\frac{n}{q}\right)$. Thus

$$r_K(n) = \sum_{0 < d \mid n} \chi(d)$$

for each $n \in \mathbb{Z}_{\geq 1}$.

Proof of this

We have $\chi(nn') \equiv (nn')^{\frac{q-1}{2}} \pmod q$,

$$\chi(nn') \equiv \chi(n)\chi(n') \pmod q,$$

$$\chi(nn') = \chi(n)\chi(n'),$$

$\forall\ n, n' \in \mathbb{Z}$. Therefore

$$L(\chi, s) = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})^{-1}$$

But $\forall$ prime ideal $p \neq 0 \subseteq \mathbb{Z}$, we have $N(p) = p^f$,

and $e f g = 2$, with $p\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_g$. Therefore

$$\zeta_K(s) = \prod_{\substack{p \text{ prime} \\ e_p = 2}} (1 - p^{-s})^{-1} \prod_{\substack{p \text{ prime} \\ g_p = 2}} (1 - p^{-s})^{-2} \prod_{\substack{p \text{ prime} \\ f_p = 2}} (1 - p^{-2s})^{-1}$$

$$= \prod (1 - p^{-s})^{-1} \prod (1 - p^{-s})^{-2} \prod (1 - p^{-s})^{-1} (1 + p^{-s})^{-1}$$

$\left(\frac{q^*}{p}\right) = 0$ $\qquad$ $\left(\frac{q^*}{p}\right) = 1$ $\qquad$ $\left(\frac{q^*}{p}\right) = -1$

$$= \zeta(s) \prod_{p \text{ prime}} \left(1 - \left(\frac{q^*}{p}\right) p^{-s}\right)^{-1} = \zeta(s) L(\chi, s), \text{ as}$$

the QRL says that

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

Indeed,

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) =$$

$$(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\left(\frac{q}{p}\right) \quad \square$$

We may define $r_k(0) \in \mathbb{Q}$ so that

$$f(\tau) = \sum_{n=0}^{\infty} r_k(n)\, q^n,$$

is the Fourier expansion of a modular form of weight $k = 1$, where

$q = e^{2\pi i \tau}$, and $\tau \in \mathcal{H} := \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$.

We shall express $r_k(0)$ in terms of some generalised Bernoulli numbers attached to Dirichlet characters, following Leopoldt and Kubota.