ZETA FUNCTIONS. NO.6

YOSHIFUMI TSUCHIMOTO

6.1. **Legendre symbol.**

DEFINITION 6.1. Let p be an odd prime. Let a be an integer which is not divisible by p. Then we define the **Legendre symbol** $\left(\frac{a}{p}\right)$ by the following formula.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } (X^2 - a) \text{ is irreducible over } \mathbb{F}_p \\ -1 & \text{otherwise} \end{cases}$$

We further define

$$\left(\frac{a}{p}\right) = 0 \text{ if } a \in p\mathbb{Z}.$$

LEMMA 6.2. *Let p be an odd prime. Then:*

(1) $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

We note in particular that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

DEFINITION 6.3. Let p, ℓ be distinct odd primes. Let λ be a primitive ℓ-th root of unity in an extension field of $\mathbb{F}_p$. Then for any integer a, we define a **Gauss sum** τ_a as follows.

$$\tau_a = \sum_{t=1}^{\ell-1} \left(\frac{t}{\ell}\right) \lambda^{at}$$

τ_1 is simply denoted as τ.

LEMMA 6.4. (1) $\tau_a = \left(\frac{a}{\ell}\right)\tau$.

(2) $\sum_{a=0}^{l-1} \tau_a \tau_{-a} = \ell(\ell - 1)$.

(3) $\tau^2 = (-1)^{(\ell-1)/2}\ell$ *($= \ell^*$ (say)).*

(4) $\tau^{p-1} = (\ell^*)^{(p-1)/2}$.

(5) $\tau^p = \tau_p$.

THEOREM 6.5.

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

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

$\left(\frac{2}{\ell}\right) = (-1)^{(\ell^2-1)/8}$

6.2. **On congruent zeta of elliptic curves.** Cosider a curve E : $y^2 = x(x-1)(x-\lambda) \qquad (\lambda \in \mathbb{F}_q)$. then:

$$\#E(\mathbb{F}_{q^r}) = \sum_{x \in \mathbb{F}_{q^r}} ((x(x-1)(x-\lambda))^{\frac{q-1}{2}} + 1) + 1$$
$$= q + 1 + \sum_{x \in \mathbb{F}_{q^r}} x^{\frac{q-1}{2}} ((x-1)(x-\lambda^{\frac{q-1}{2}}$$

We have on the other hand:

LEMMA 6.6.

$$\sum_{x \in \mathbb{F}_{q^r}} x^k = \begin{cases} -1 & \text{if } (q-1)|k \text{ and } k \neq 0. \\ 0 & \text{otherwise.} \end{cases}$$

$$\#E(\mathbb{F}_{q^r}) = q + 1 - \operatorname{coeff}\left(((x-1)(x-\lambda))^{\frac{q-1}{2}}, x^{\frac{q-1}{2}}\right)$$

Further computations are found in Clemens: "A scrapbook of complex curve thery". Students that are interested in this subject are advised to read the book.