CONGRUENT 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 $\ell^* = (-1)^{(\ell-1)/2}\ell$)*

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

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

---

p-dependence of zeta functions is important topic. We are not going to talk about that in too much detail but let us explain a little bit.

Let us define the zeta function of a category $\mathcal{C}$ [**?**].

$$\zeta(s, \mathcal{C}) = \prod_{P \in P(\mathcal{C})} (1 - N(P)^{-s})^{-1}$$

where P runs over all finite simple objects.

- P: finite $\overset{\text{def}}{\iff}$ $N(P) \overset{\text{def}}{=} \#\operatorname{End}(P) < \infty$.
- P: simple $\overset{\text{def}}{\iff}$ $\operatorname{Hom}(P, Y) \setminus \{0\}$ consists of mono morphisms.

For any commutative ring A, an A-module M is simple if and only if $M \cong A/\mathfrak{m}$ for some maximal idea $\mathfrak{m}$ of A. We have thus:

$$\begin{aligned}
\zeta(s, (A\text{-modules})) &= \prod_{\substack{\mathfrak{m}\in \operatorname{Spm}(A) \\ \#(A/\mathfrak{m})<\infty}} (1 - \#(A/\mathfrak{m})^{-s})^{-1} \\
&= \prod_{p:\text{prime}} \prod_{\substack{\mathfrak{m}\in \operatorname{Spm}(A) \\ \mathbb{F}_p \subset A/\mathfrak{m} \\ [A/\mathfrak{m}:\mathbb{F}_p]<\infty}} (1 - \#(A/\mathfrak{m})^{-s})^{-1} \\
&= \prod_{p} \prod_{\substack{\mathfrak{m}\in \operatorname{Spm}(A/p) \\ \mathbb{F}_p \subset A/\mathfrak{m} \\ [(A/p)/\mathfrak{m}:\mathbb{F}_p]<\infty}} (1 - \#((A/p)/\mathfrak{m})^{-s})^{-1} \\
&= \prod_{p} \zeta(s, (A/p)\text{-modules}).
\end{aligned}$$

Let us take a look at the last line. It sais that the zeta is a product of zeta's on A/p. Let us fix a prime number p, put $\bar{A} = A/p$, and concentrate on $\bar{A}$ to go on further.

$$\zeta(s, (A/p)\text{-modules}) = \prod_{\substack{\mathfrak{m}\in \operatorname{Spm}(\bar{A}) \\ [\bar{A}/\mathfrak{m}:\mathbb{F}_p]<\infty}} (1 - \#(\bar{A}/\mathfrak{m})^{-s})^{-1}$$

$$\begin{aligned}
Z(\operatorname{Spec}(\bar{A})/\mathbb{F}_p, T) &= \exp\Big(\sum_{r=1}^{\infty} (\operatorname{Spec}(\bar{A})(\mathbb{F}_{p^r}), T)\Big) \\
&= \prod_{\mathfrak{m}\in \operatorname{Spm}(A)} \exp\Big(\sum_{r=1}^{\infty} (\operatorname{Spec}(\bar{A}/\mathfrak{m})(\mathbb{F}_{p^r}), T)\Big)
\end{aligned}$$

$$Z(\mathbb{F}_{q^e}/\mathbb{F}_q, T) = \exp\Big(\sum_{e|r} \frac{e}{r} T^r\Big) = (1 - T^e)^{-1}$$

$$\zeta(s, \mathbb{F}_{p^e}\text{-modules}) = Z(\operatorname{Spec}(\mathbb{F}_{p^e})/\mathbb{F}_p, p^s)$$

We conclude:

PROPOSITION 6.6. *Let A be a commutative ring. Then:*

(1) *We have a product formula.*

$$\zeta(s, (A\text{-modules})) = \prod_{p} \zeta(s, (A/p)\text{-modules})$$

(2) *ζ is obtained by substituting T in the congruent zeta function by p^s.*

$$\zeta(s, (A/p)\text{-modules}) = Z(\operatorname{Spec}(A/p)/\mathbb{F}_p, p^s)$$