CONGRUENT ZETA FUNCTIONS. NO.2

YOSHIFUMI TSUCHIMOTO

In this lecture we define and observe some properties of conguent zeta functions.

existence of finite fields II.

Proof of Lemma 1.3 (5). We prove the following more general result

LEMMA 2.1. *Let K be a field. Let G be a finite subgroup of $K^\times$ (=multiplicative group of K). Then G is cyclic.*

PROOF. We first prove the lemma when $|G| = \ell^k$ for some prime number ℓ. In such a case Euler-Lagrange theorem implies that any element g of G has an order ℓ^s for some $s \in \mathbb{N}$, $s \leq k$. Let $g_0 \in G$ be an element which has the largest order m. Then we see that any element of G satisfies the equation

$$x^m = 1.$$

Since K is a field, there is at most m solutions to the equation. Thus $|G| \leq m$. So we conclude that the order m of g_0 is equal to $|G|$ and that G is generated by g_0.

Let us proceed now to the general case. Let us factorize the order $|G|$.

$$|G| = \ell_1^{k_1} \ell_2^{k_2} \dots \ell_t^{k_t} \qquad (\ell_1, \ell_2, \dots, \ell_t: \text{ prime number}, k_1, k_2, \dots, k_t \in \mathbb{Z}_{>0}).$$

Then G may be decomposed into product of p-subgroups

$$G = G_1 \times G_2 \times \dots \times G_t \qquad (|G_j| = \ell_j^{k_j} (j = 1, 2, 3, \dots, t)).$$

By using the first step of this proof we see that each G_j is cyclic. Thus we conclude that G is also a cyclic group. □

EXERCISE 2.1. Let G be a finite abelian group. Assume we have a decomposition $|G| = m_1 m_2$ of the order of G such that m_1 and m_2 are coprime. Then show the following:

(1) Let us put

$$H_j = \{g \in G; g^{m_j} = e_G\} \qquad (j = 1, 2)$$

Then H_1, H_2 are subgroups of G.

(2) $|H_j| = m_j$ $(j = 1, 2)$.

(3) We have

$$G = H_1 H_2.$$

EXERCISE 2.2. Let G_1, G_2 be finite cyclic groups. Assume $|G_1|$ and $|G_2|$ are coprime. Show that $G_1 \times G_2$ is also cyclic.