CONGRUENT ZETA FUNCTIONS. NO.10

YOSHIFUMI TSUCHIMOTO

elliptic curves

There is diverse deep theories on elliptic curves.

Let k be a field of characteristic $p \neq 0, 2, 3$. We consider a curve E in $\mathbb{P}(k)$ of the following type:

$$y^2 = x^3 + ax + b \quad (a, b \in k, 4a^3 + 27b^2 \neq 0).$$

(The equation, of course, is written in terms of inhomogeneous coordinates. In homogeneous coordinates, the equation is rewritten as:

$$Y^2 = X^3 + aXZ^2 + bZ^3.)$$

Such a curve is called an **elliptic curve**. It is well known (but we do not prove in this lecture) that

THEOREM 10.1. *The set $E(k)$ of k-valued points of the elliptic curve E carries a structure of an abelian group. The addition is so defined that*

$$P + Q + R = 0 \iff P, Q, R \text{ are colinear.}$$

We would like to calculate congruent zeta function of E.

For the moment, we shall be content to prove:

PROPOSITION 10.2. *Let p be and odd prime. Let us fix $\lambda \in \mathbb{F}_p$ and consider an elliptic curve $E : y^2 = x(x-1)(x-\lambda)$. Then*

$$\#E(\mathbb{F}_p) = \text{the coefficient of } x^{\frac{p-1}{2}} \text{ in the polynomial expansion of } [(x-1)(x-\lambda)]^{\frac{p-1}{2}}.$$