CONGRUENT ZETA FUNCTIONS. NO.08

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 8.1. *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*

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

We would like to calculate congruent zeta function of E.

For the moment, we shall be content to prove:

PROPOSITION 8.2. *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*

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

See [1] for more detail and a further story.

The following proposition is a special case of the Weil conjecture. (It is actually a precursor of the conjecture)

PROPOSITION 8.3 (Weil). *Let E be an elliptic curve over $\mathbb{F}_q$. Then we have*

$$Z(E/\mathbb{F}_q, T) = \frac{1 - d_E T + qT^2}{(1-T)(1-qT)}.$$

where d_E is an integer which satisfies $|d_E| \leq 2\sqrt{q}$.

Note that for each E we have only one unknown integer d_E to determine the Zeta function. So it is enough to compute $\#E(\mathbb{F}_q)$ to compute the Zeta function of E. (When $q = p$ then one may use Proposition 8.2 to do that.)

$$\#E(\mathbb{F}_q) = 1 + q - d_E.$$

EXERCISE 8.1. compute the congruent zeta function $Z(E, T)$ for an elliptic curve $E : y^2 = x(x-1)(x+1)$.

REFERENCES

[1] C. H. Clemens, *A scrapbook of complex curve theory*, Graduate Sdudies in Mathematics, vol. 55, American Mathematical Society, 1980.