

# CONGRUENT ZETA FUNCTIONS. NO.1

YOSHIFUMI TSUCHIMOTO

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

existence of finite fields.

For a good brief account of finite fields, consult Chapter I of a book [1] of Serre.

LEMMA 1.1. *For any prime number  $p$ ,  $\mathbb{Z}/p\mathbb{Z}$  is a field. (We denote it by  $\mathbb{F}_p$ .)*

Funny things about this field are:

LEMMA 1.2. *Let  $p$  be a prime number. Let  $R$  be a commutative ring which contains  $\mathbb{F}_p$  as a subring. Then we have the following facts.*

(1)

$$\underbrace{1 + 1 + \cdots + 1}_{p\text{-times}} = 0$$

*holds in  $R$ .*

(2) *For any  $x, y \in R$ , we have*

$$(x + y)^p = x^p + y^p$$

We would like to show existence of “finite fields”. A first thing to do is to know their basic properties.

LEMMA 1.3. *Let  $F$  be a finite field (that means, a field which has only a finite number of elements.) Then we have,*

(1) *There exists a prime number  $p$  such that  $p = 0$  holds in  $F$ .*

(2)  *$F$  contains  $\mathbb{F}_p$  as a subfield.*

(3)  *$q = \#(F)$  is a power of  $p$ .*

(4) *For any  $x \in F$ , we have  $x^q - x = 0$ .*

(5) *The multiplicative group  $(F_q)^\times$  is a cyclic group of order  $q - 1$ .*

The next task is to construct such field. An important tool is the following lemma.

LEMMA 1.4. *For any field  $K$  and for any non zero polynomial  $f \in K[X]$ , there exists a field  $L$  containing  $L$  such that  $f$  is decomposed into polynomials of degree 1.*

To prove it we use the following lemma.

LEMMA 1.5. *For any field  $K$  and for any irreducible polynomial  $f \in K[X]$  of degree  $d > 0$ , we have the following.*

- (1)  $L = K[X]/(f(X))$  is a field.
- (2) Let  $a$  be the class of  $X$  in  $L$ . Then  $a$  satisfies  $f(a) = 0$ .

Then we have the following lemma.

LEMMA 1.6. *Let  $p$  be a prime number. Let  $q = p^r$  be a power of  $p$ . Let  $L$  be a field extension of  $\mathbb{F}_p$  such that  $X^q - X$  is decomposed into polynomials of degree 1 in  $L$ . Then*

- (1)
 
$$L_1 = \{x \in L; x^q = x\}$$
 is a subfield of  $L$  containing  $\mathbb{F}_p$ .
- (2)  $L_1$  has exactly  $q$  elements.

Finally we have the following lemma.

LEMMA 1.7. *Let  $p$  be a prime number. Let  $r$  be a positive integer. Let  $q = p^r$ . Then we have the following facts.*

- (1) *There exists a field which has exactly  $q$  elements.*
- (2) *There exists an irreducible polynomial  $f$  of degree  $r$  over  $\mathbb{F}_p$ .*
- (3)  *$X^q - X$  is divisible by  $f$ .*
- (4) *For any field  $K$  which has exactly  $q$ -elements, there exists an element  $a \in K$  such that  $f(a) = 0$ .*

In conclusion, we obtain:

THEOREM 1.8. *For any power  $q$  of  $p$ , there exists a field which has exactly  $q$  elements. It is unique up to an isomorphism. (We denote it by  $\mathbb{F}_q$ .)*

The relation between various  $\mathbb{F}_q$ 's is described in the following lemma.

LEMMA 1.9. *There exists a homomorphism from  $\mathbb{F}_q$  to  $\mathbb{F}_{q'}$  if and only if  $q'$  is a power of  $q$ .*

EXERCISE 1.1. Compute the inverse of 113 in the field  $\mathbb{F}_{359}$ .