$\mathbb{Z}_p$, $\mathbb{Q}_p$, AND THE RING OF WITT VECTORS

YOSHIFUMI TSUCHIMOTO

Playing with "digits in base n"

You should know that every positive integer may be written in decimal notation:

$$(531)_{10} = 5 \times 10^2 + 3 \times 10^1 + 1 \times 10^0.$$

Similarly, given any integer ("base") $b \geq 2$, we may write a number as a string of digits in base n. For example, we have

$$(531)_{10} = 1 \times 7^3 + 3 \times 7^2 + 5 \times 7 + 6 \times 1 = (1356)_7.$$

Similarly, we have

$$(531)_{10} = (1356)_7 = (1023)_8 = 1000010011_2 = (213)_{16}.$$

You may also probably know (repeating) decimal expresions of positive rational numbers.

$$(531.79)_{10} = 5 \times 10^2 + 3 \times 10^1 + 1 \times 10^0 + 7 \times 10^{-1} + 9 \times 10^{-2}.$$

$$(531.79)_{10} = (1356.\dot{5}34\dot{6})_7 = (1023.62\dot{4}365605075341217270\dot{2})_8$$

Now let us reverse the order of digits. Namely, we employ a notation like this[1]:

$$\begin{aligned} &[97.135]_{10} = (531.79)_{10} \\ &[0.135]_{10} = (531)_{10} \\ &[123.456]_{10} = (654.321)_{10} \\ &\dots \end{aligned}$$

Let us do some calculation with the above notation:

$$\begin{aligned} &[0.1]_{10} + [0.9]_{10} = [0.01]_{10} \\ &[0.1]_{10} \times [0.9]_{10} = [0.9]_{10} \\ &[0.01]_{10} \times [0.09]_{10} = [0.009]_{10} \end{aligned}$$

You may recognize curious rules of computations. This curious notation will lead you to a new world called "the world of addic numbers".

EXERCISE 0.1. Compute

$$[0.12345]_8 + [0.75432]_8$$

with our curious notation. Then do the same computation in the usual digital notation in base 10.

LEMMA 0.1. *For any prime number p, $\mathbb{Z}/p\mathbb{Z}$ is a field. (We denote it by $\mathbb{F}_p$.)*

LEMMA 0.2. *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]This is our private notation.

(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 0.3. *Let* F *be a finite field (that means, a field which has only a finite number of elements.) Then:*

(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 fields. An important tool is the following lemma.

LEMMA 0.4. *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 linear factors in* L.

To prove it we use the following lemma.

LEMMA 0.5. *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 0.6. *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 0.7. *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 the polynomial* f *as above.*
(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 0.8. *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* $\mathbb{F}_q$.*)*