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

No.04: $\boxed{\mathbb{Z}_p \text{ as a local ring.}}$

In this lecture, rings are assumed to be unital, associative and commutative unless otherwise specified.

DEFINITION 4.1. A (unital commutative) ring A is said to be a **local ring** if it has only one maximal ideal.

LEMMA 4.2. *Let A be a ring. Then the following conditions are equivalent:*

(1) *A is a local ring.*
(2) *$A \setminus A^\times$ forms an ideal of A.*

PROPOSITION 4.3. *$\mathbb{Z}_p$ is a local ring. Its maximal ideal is equal to $p\mathbb{Z}_p$.*

Recall that $\mathbb{Z}_p$ is compact. It is therefore a "complete local ring". We may do some "analysis" such as Newton's method to obtain some solution to algebraic equations.

Newton's method for approximating a solution of algebraic equation.

Let us solve an equation

$$x^2 = 2$$

in $\mathbb{Z}_7$. We first note that

$$3^2 \equiv 2 \quad (7)$$

hold. So let us put $x_0 = 3 = [0.3]_7$ as the first approximation of the solution. The Newton method tells us that for an approximation x of the equation $x^2 = 2$, a number x' calculated as

$$x' = \frac{1}{2}(x + \frac{2}{x})$$

gives a better approximation.

$$x_0' = \frac{1}{2}([0.3]_7 + [0.3\dot{2}]_7 = [0.3\dot{1}]_7$$

So $[0.3\dot{1}]_7$ is a better approximation of the solution. In order to make the calculation easier, let us choose $x_1 = [0.31]_7$ (insted of x_0') as a second approximation.

$$x_1' = \frac{1}{2}([0.31]_7 + 2/[0.31]_7) = \frac{1}{2}([0.31]_7 + [0.3\dot{1}45\dot{2}]_7) \fallingdotseq [0.312]_7$$

We choose $x_2 = [0.312]_7$ as a second approximation.

$$x_2' = \frac{1}{2}([0.312]_7 + 2/[0.3\dot{1}25340662\dot{2}]_7) \risingdotseq [0.31261]_7$$

We choose $x_3 = [0.31261]_7$ as a third approximation.

$$x_3' == \frac{1}{2}([0.31261]_7 + [0.3126142465066\ldots]_7) \risingdotseq [0.312612124...]_7$$

We choose $x_4 = [0.312612124]_7$ as a third approximation.

$$x_4' = \frac{1}{2}([0.312612124]_7 + [0.31261212456522042266221313 5351\ldots]_7)$$
$$\risingdotseq [0.3126121246621102]_7$$

Exercise 4.1. Compute $[0.5]_7/[0.11]_7$

Exercise 4.2. Find a solution to

$$x^3 \equiv 5 \pmod{11^5}$$

such that $x \equiv 3 \pmod{11}$.

$\boxed{\mathbb{Q}_p}$

Definition 4.4. We denote by $\mathbb{Q}_p$ the quotient field of $\mathbb{Z}_p$.

Lemma 4.5. *Every non zero element $x \in \mathbb{Q}_p$ is uniquely expressed as*

$$x = p^k u \qquad (k \in \mathbb{Z}, u \in \mathbb{Q}_p^\times).$$

We have so far constructed a ring $\mathbb{Z}_p$ and a field $\mathbb{Q}_p$ for each prime p.

Proposition 4.6. *Let p be a prime. Then:*

(1) *$\mathbb{Z}_p$ is a local ring with the unique maximal ideal $p\mathbb{Z}_p$.*

(2)
$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p(= \mathbb{Z}/p\mathbb{Z}).$$

(3) *$\mathbb{Z}_p$ is an integral domain whose quotient field $\mathbb{Q}_p$ is a field of characteristic zero.*

With $\mathbb{Q}_p$ and/or $\mathbb{Z}_p$, we may do some "calculus" such as:

Theorem 4.7. [1, corollary 1 of theorem 1] *Let $f \in \mathbb{Z}_p[X_1, X_2, \ldots, X_m], x \in \mathbb{Z}_p^m$, $n, k \in \mathbb{Z}$. Assume that there exists a natural number j such that $1 \le j \le m$,*

$$\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \pmod{p}.$$

Then there exists $y \in \mathbb{Z}_p^m$ *such that*

$$f(y) = 0 \tag{1}$$

$$y \equiv x \pmod{p} \tag{2}$$

See [1] for details.

References

[1] J. P. Serre, *Cours d'arithmétique*, Presses Universitaires de France, 1970.