P-Adic Integers

October 16, 2015

1 Modular Arithmetic

1.1 well known number system

- $\mathbb{N}$= the NATURAL NUMBERS 0, 1, 2, 3, ...
- $\mathbb{Z}$= the INTEGERS . . ., -2, -1, 0, 1, 2, ...
- $\mathbb{Q}$= the RATIONAL NUMBERS $\frac{a}{b},\ a, b \in \mathbb{Z},\ b \neq 0$..
- $\mathbb{R}$= the REAL NUMBERS, e.g., $\pi := 3.1415926\ldots$.

$$\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\} <---------> \{Modular\ Arithmetic\}$$

1.2 integers mod n

2=0 !!!

When $n \geqslant 2$, there is a very small number system:

$$\mathbb{Z}/n\mathbb{Z} := \{0, 1, 2, \ldots, n-1\}.$$

For example

n=2, $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

n=3, $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$.

n=5, $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$.

2 Algorithm on Modular

Let us take the above example n=5 .

2.1 Addition

$3 + 4 = 7 \equiv 2(mod\ 5)$.

$8 + 4 = 12 \equiv 2(mod\ 5)$.

2.2 Subtraction(leave to you)

1-4 = ?

6-4 = ?

2.3 Multiplication

$2 \cdot 4 = 8 \equiv 3(mod\ 5)$.

$7 \cdot 4 = 28 \equiv 3(mod\ 5)$.

2.4 Division

Let n = 5, $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$.

• **Problem**

What is $\frac{1}{3}$?

The division may not exist!!!

let n = 6, $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$.

• **Problem**

Does there exist $\frac{1}{2}$?

• **Fact**

When n is a prime number, the division is always valid.

3 P expansion

{Real Numbers} < − − − > {Decimal Expansion} {P-adic Numbers}

We can express any real number as

$$C_n C_{n-1} \dots C_0 . C_{-1} C_{-2} \dots, \; 0 \le C_i \le 9,$$

which is called digit.

- **Example**

$\frac{1}{3} = 0.3333\dots,$

$\frac{4}{3} = 1.3333\dots,$

$\frac{1}{4} = 0.2500\dots,$

4 P-Adic Integers and its algorithm

Let p = 3.

$\mathbf{Z}_3$ consists of "formal" infinite sums

$$a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \dots, \; a_i \in \{0, 1, 2\}.$$

What is 22 in $\mathbf{Z}_3$?

- **Exercise**

Write down the similar expression of 37 for $\mathbb{Z}_5$.

4.1 Addition—why infinite sum need to be allowed

Let p=3,

$\alpha = 2 + 2 \cdot p + p^2.$

$\beta = 2 + p$.

$\alpha + \beta =$

- **Exercise**

Let p = 5

$\alpha = 2 + 2 \cdot p + p^2$.

$\beta = 4 + 3 \cdot p$.

$\alpha + \beta =$?

And check that the expression is exactly the expression of 56 for $\mathbb{Z}_5$.

• **Problem**

Let p = 3

$\beta = 2 + 2 \cdot p + 2 \cdot p^2 + 2 \cdot p^3 + \ldots.$

We have $\beta + 1 = 0$, in other words, the p-expansion of -1 is

$$2 + 2 \cdot p + 2 \cdot p^2 + 2 \cdot p^3 + \ldots.$$