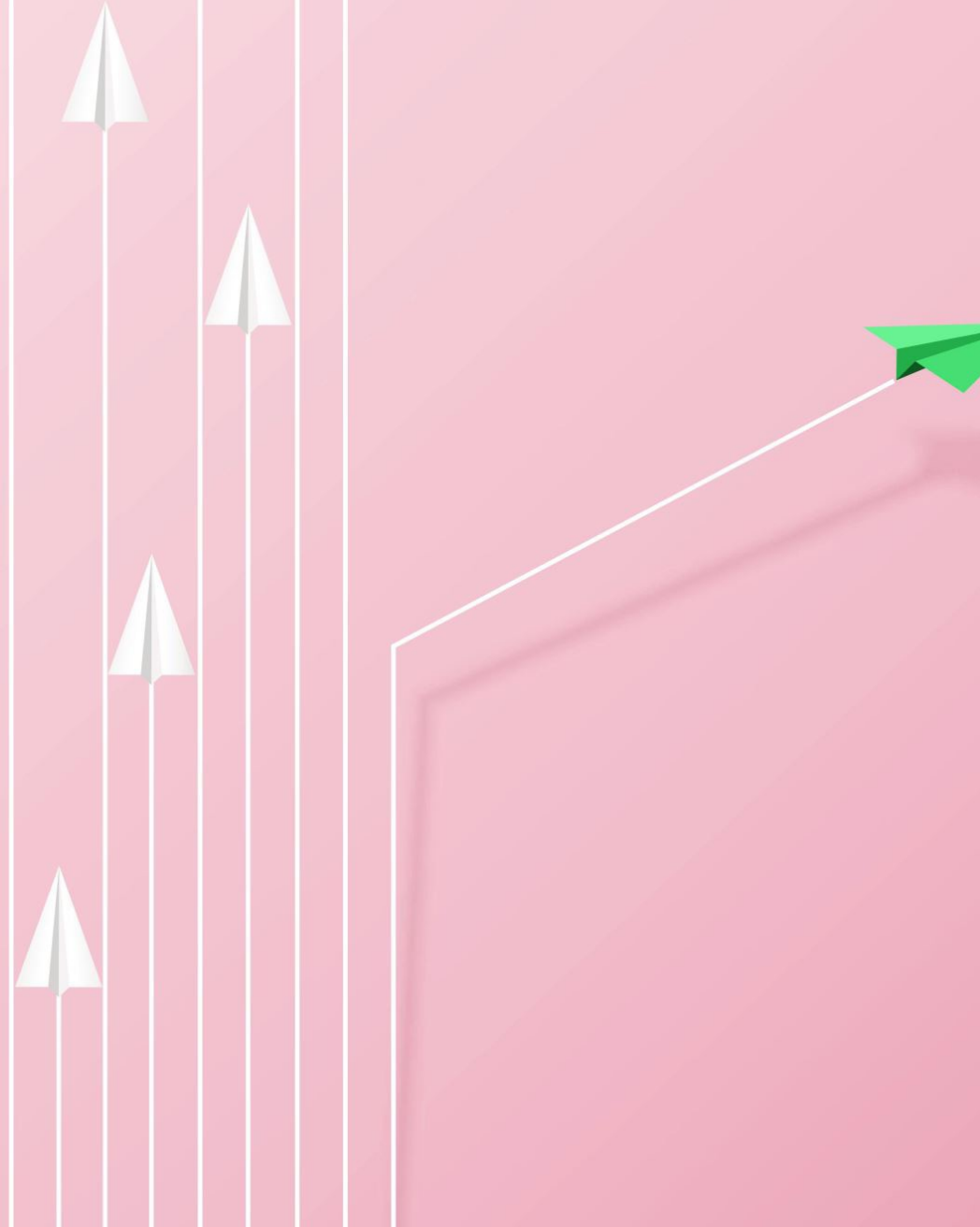# *The p-adic Numbers*

Uyen Tran

(University of Nebraska – Lincoln)

Why?

Polynomials Over $\mathbb{C}$

- Rational functions
$$f(x) = \frac{p(x)}{q(x)}, \qquad q(x) \neq 0$$

- Any polynomial over $\mathbb{C}$ can be written of a unique product of the form:
$$P(x) = c(x - \alpha_1) \dots (x - \alpha_m)$$

- We can consider $(x - \alpha)$ as a "prime" in the set of polynomials over $\mathbb{C}$.

- <u>Question:</u> We can rewrite any polynomials as a power series around $(x - \alpha)$. Can we do something like that with integers and prime numbers?

$$P(x) = a_0 + a_1 x + \dots + a_n x^n = \sum_{i \geq 0} b_i (x - \alpha)^i$$

Integers

- Rational numbers
$$q = \frac{a}{b}, \qquad a, b \in \mathbb{Z}, b \neq 0$$

- Any integer can be written as a product of prime numbers:
$$a = p_1 p_2 \dots p_n$$

- <u>Answer:</u> Yes!
$$321 = 3{\times}10^2 + 2{\times}10 + 1$$
$$321 = 6{\times}7^2 + 3{\times}7 + 6$$

p-adic number!

What are p-adic numbers?

Defn: Fix a prime number p. A **p-adic number** is a *formal sum* of the form:

$$a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots \qquad \text{where } a_i \in \{0, 1, \ldots, p-1\} \text{ for all } i.$$

Examples:

- $p = 3, \quad 1 + 2 \times 3$
- $p = 5, \quad 2 \times 5^{-1} + 1 \times 5$
- $p = 5, \quad 4 + 4 \times 5 + 4 \times 5^2 + 4 \times 5^3 + \cdots$

Notes:

- Formal sum: Don't try to put it into a calculator!
- n_0 can be zero, or a positive integer, or a negative integer.
- A p-adic number could be a finite or infinite expression.

Addition and Multiplication

Fix a prime number p. Given two p-adic numbers $x = \sum_{i \geq n_0} a_i p^i$, $y = \sum_{j \geq m_0} b_j p^j$.

- Addition:

$$x + y = \sum_{i \geq n_0} (a_i + b_i)\, p^i$$

- Multiplication:

$$xy = \sum_{k \geq n_0 + m_0} \left(\sum_{i+j=k} a_i b_j \right) p^k$$

- Example: Fix $p = 5$, $x = 1 + 3{\times}5$, $y = 2 + 1{\times}5$

$$x + y = (1 + 2) + (3 + 1){\times}5 = 3 + 4{\times}5$$

p-adic absolute value

Defn: Fix a prime number p. Given a p-adic number $x = a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \cdots$,

The **p-adic absolute value of x**, denoted $|x|_p$, is

$$|x|_p = \frac{1}{p^n}$$

where p^n is the first power of p that has a non-zero coefficient.

Examples:

- $p = 5$, $x = 2p + 4p^2 + 4p^6$, then $|x|_5 = \frac{1}{p}$.

- $p = 5$, $x = 1 + 3p + 3p^2$, then $|x|_5 = \frac{1}{p^0}$.

p-derivations

p-derivations

Fix a prime number p.

Let R be a ring where $p = 1 + \cdots + 1$ is not a zero-divisor.

A function $\delta: R \to R$ is a **p-derivation** if

- $\delta(1) = 0$
- $\delta(ab) = \delta(a)b^p + a^p\delta(b) + p\delta(a)\delta(b)$
- $\delta(a + b) = \delta(a) + \delta(b) + \frac{a^p + b^p - (a+b)^p}{p}$

Derivatives of polynomials

Recall that derivatives of polynomials also have a similar set of rules:

- $\frac{d}{dx}(1) = 0$
- $\frac{d}{dx}\big(f(x)g(x)\big) = g(x)\frac{d}{dx}\big(f(x)\big) + f(x)\frac{d}{dx}\big(g(x)\big)$
- $\frac{d}{dx}\big(f(x) + g(x)\big) = \frac{d}{dx}\big(f(x)\big) + \frac{d}{dx}\big(g(x)\big)$

p-derivations

p-derivations

- Following the rules, we find the unique p-derivation over the integers is the function delta $\delta: \mathbb{Z} \to \mathbb{Z}$ given by

$$\delta(n) = \frac{n - n^p}{p}$$

- If the highest power of p that divides n is greater than 0 , taking the p-derivation of n will decrease that higher power of p that divides n by 1.

- Example:

$$\text{Fix } p = 2, \delta(6) = \frac{6-36}{2} = -15$$

Derivatives of polynomials

- If the degree of a polynomial is not zero, taking the derivative of that polynomial will decrease the degree by one.

Thank You :)