

\mathbb{Z}_p : 楕円曲線 $\xrightarrow{\text{完備}}$ 解析

\mathbb{Z}_p : \mathbb{Z} の p -進数 \mathbb{Z}_p に \mathbb{Z} を完備化

\cup
 $p\mathbb{Z}_p$

$$\mathbb{Z}_p \text{ の } \bar{\mathbb{Z}} = [0, * * * * -]_p$$

$$p\mathbb{Z}_p \text{ の } \bar{\mathbb{Z}} = [0, 0 * * * * -]_p = m$$

$\mathbb{Z}_p \setminus \underbrace{p\mathbb{Z}_p}_{m}$ は必ず可逆

$$\mathbb{Z}_p \setminus m \ni [0, \underbrace{a_1}_{\neq 0}, a_2, \dots]_p$$

a_1 を $\mathbb{Z}/p\mathbb{Z}$ の inv とし

逆元をとる

$$[0, b_1, b_2, \dots]_p$$

完備局所環 (解析学)

Zorn の補題

環には必ず極大 ideal がある

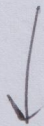
ideal をとる



さらに大なるものがあれば
それをとる



くりかえす



極大なものがある

PZ (P: 素数) 極大 ideal

の

$\mathbb{Z}_p \supset \underbrace{p\mathbb{Z}_p}_{\substack{\text{ideal} \\ \parallel}} \quad \mathbb{Z}_p \setminus m \text{ の元は可逆}$

$\mathbb{Z}_p \setminus m$

① m は 極大 ideal.

② m は \mathbb{Z}_p の 唯一 の 極大 ideal

① $\exists I \supset m \quad \text{とすると,}$
 $\underbrace{I}_{\substack{\text{ideal} \\ \subsetneq \mathbb{Z}_p}}$

$I \ni \exists x \text{ s.t. } x \notin m$

x は可逆 $\text{i.e. } x^{-1} \in \mathbb{Z}_p$

$\underbrace{1}_{\in \mathbb{Z}_p} = \underbrace{x}_{\in I} \cdot \underbrace{x^{-1}}_{\in \mathbb{Z}_p} \in I \quad \Rightarrow \quad \mathbb{Z}_p$
 $I = \mathbb{Z}_p$
 矛盾.

② m' : \mathbb{Z}_p の m 以外の 極大 ideal と仮定

$m' \neq m$ と仮定

$\exists x \in m' \text{ s.t. } x \notin m$

$(\exists x \text{ s.t. } x \notin m \text{ ならば } m' \subset m)$

x : 可逆

$\rightarrow m' = \mathbb{Z}_p$ 矛盾

$x \in \mathbb{Z}_p$ とし. $x \notin p\mathbb{Z}_p$ とし.

$y \in \mathbb{Z}_p$ と $xy = 1$ となる y を

$$x \cdot y_1 = 1 + (p\mathbb{Z}_p \text{ の } \bar{c})$$

と y_1 が存在.

$$x \cdot y_1 = 1 + pc = 1 - pc_1 \quad (c_1 = -c)$$

この $\{ \bar{c}, \bar{c}_1 \}$ は?
Z

$$x \cdot y_1 \cdot z = (1 + pc)z = 1$$

↓
 x の逆元がある.

$(1 + pc)$ の逆元は $1 - pc + (pc)^2 + \dots$

||
 $(1 - pc_1)$

$1 + pc_1 + (pc_1)^2 + (pc_1)^3 + \dots$

$(1 - t)^{-1} = 1 + t + t^2 + \dots \quad (t: |t| < 1)$

収束

$t = 0.1$

Key)

~~位相空間~~ X が完備 $\Leftrightarrow X$ がコンパクト
かつ全界

\mathbb{Z}_p での方程式の解法例

\mathbb{Z}_7 での $x^2=2$ の解法

$\mathbb{Z}/7\mathbb{Z}$ であれば

$$3^2 = 9 = 2 \quad (\text{in } \mathbb{Z}/7\mathbb{Z})$$

$$([0.3 \text{ *** }]_7)^2 = [0.2 \text{ * - * }]_7$$

$$[0.3]_7^2 = [0.2 \text{ 10000 }]_7$$

$$9 = 7 + 2$$

$$([0.3]_7 + d)^2 = [0.21]_7 + 3d$$

$$(3+d)^2 = 9 + 6d + d^2 = 2 + (7 + 6d + d^2)$$

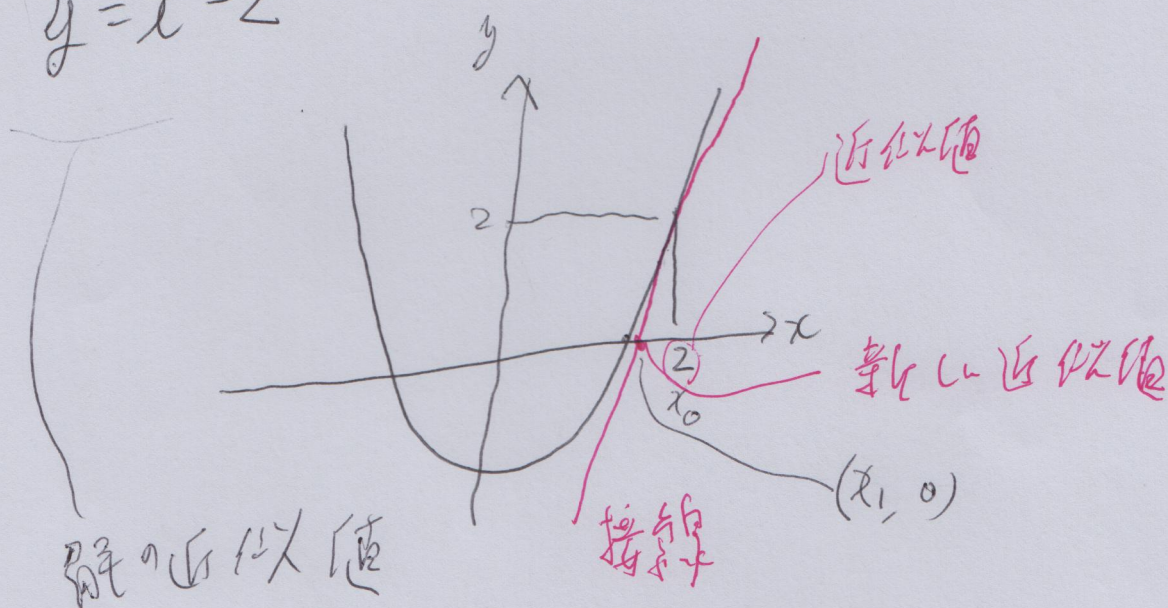
$$(3+7d_1)^2 = 2 + 7(1 + 6d_1 + 7d_1^2)$$

7 の倍数に等しい
とれる。

ニュートン法

- ・ 解の近似値を求めろ。
- 近似を高めろ。

$$y = x^2 - 2$$



x_0
接線

$$y - (x_0^2 - 2) = 2x_0(x - x_0)$$

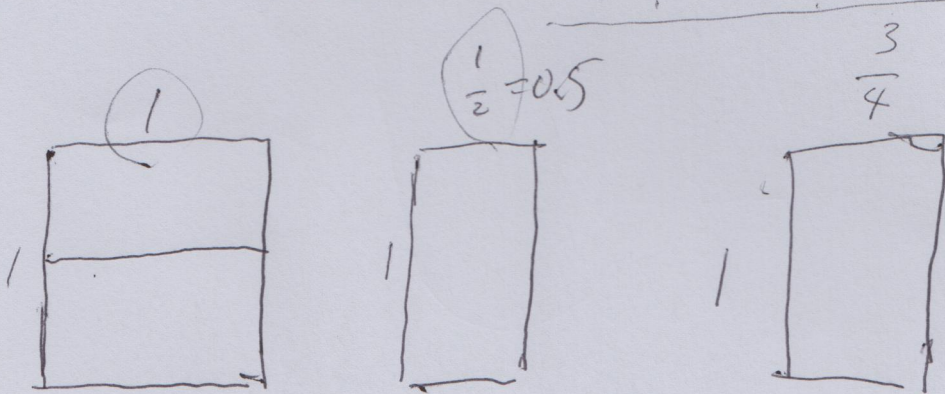
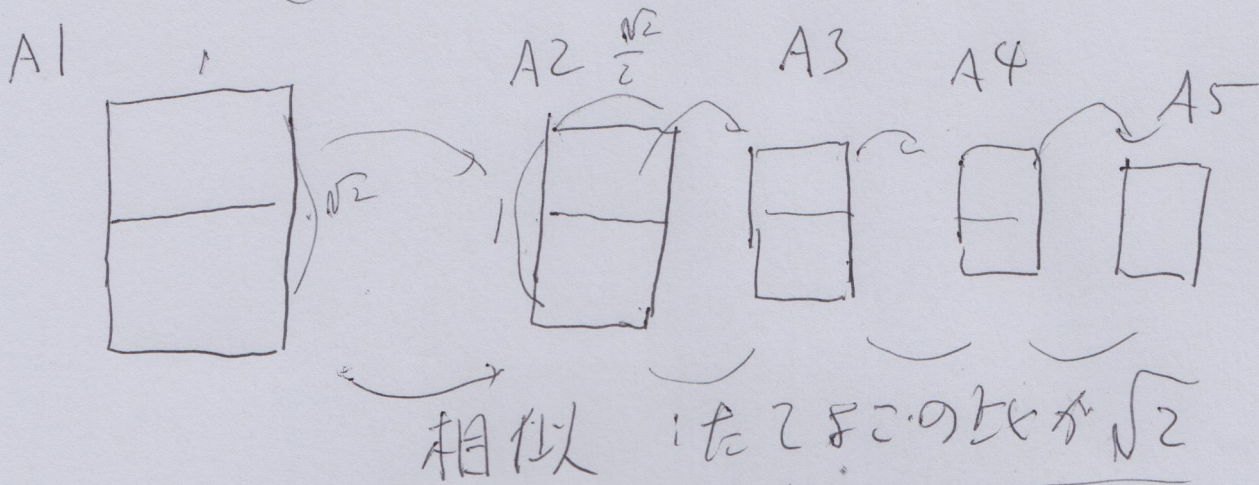
$$0 - (x_0^2 - 2) = 2x_0(x_1 - x_0)$$

$$x_1 = x_0 + \frac{2 - x_0^2}{2x_0}$$

$$= \cancel{x_0} + \frac{2 + x_0^2}{2x_0} = \left(\frac{1}{x_0}\right) + \left(\frac{x_0}{2}\right)$$

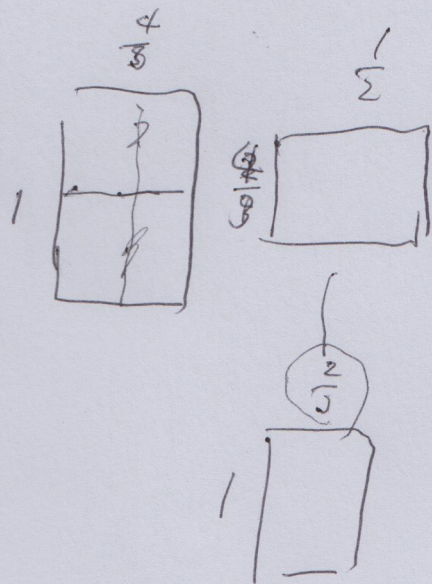
$$\text{平均} \left(\frac{1}{2x_0} \text{ と } \frac{x_0}{4} \right)$$

余談 $\sqrt{2}$



$$\frac{1 + \frac{1}{2}}{2} = \frac{3}{4}$$

$$\frac{4}{3} = 1.333\dots$$



exercise 4A

$$x^2 = 3 \quad \text{in } \mathbb{Z}_{13} \quad \text{is it?}$$

$$\left[\begin{array}{c} 4 \\ 0 \cdot \underbrace{***} \end{array} \right]_{13} \quad \text{is it?}$$