有限体

1. 定義

- 集合 U に対して $a \in U$, $b \in U$ となる要素 a, b が存在する.
  このとき $a+b \in U$, $a \cdot b \in U$ であるとき, 閉じているという.
- $a + 0 = a$ となる 0 が存在する. 0 のことを **加法単位元** という.
- $a \cdot 1 = a$ となる 1 が存在する. 1 のことを **乗法単位元** という.
- a に対して $a + (-a) = 0$ を満たす値として定義できる $-a$ がその集合内に存在する
  $-a$ を **加法逆元** という.
- a に対して $a \cdot a^{-1} = 1$ を満たす値として定義できる a^{-1} がその集合内に存在する
  a^{-1} を **乗法逆元** という.

集合の大きさ : **位数**

モジュロ演算

$a \% b$: a を b で割ったときの余り.

$r_i = a_i \% b$ [$i = 1, 2, \cdots n$ とする]

加算

$$\sum_{i=1}^{n} r_i = (a_1 + a_2 + \cdots + a_n) \% b$$
$$= (a_1 \% b + a_2 \% b + \cdots + a_n \% b) \% b$$

減算

$$2r_1 + \sum_{i=1}^{n} -r_i = (a_1 - a_2 - \cdots - a_n) \% b$$
$$= (2a_1 \% b - a_1 \% b - a_2 \% b - \cdots - a_n \% b) \% b$$

乗算

$$\pi\ r_i = (a_1 \cdot a_2 \cdot \cdots \cdot a_n) \% b$$

除算

$$div\ r_i$$

これだけ特殊なので1つ1つみていく

→結論をいうと $k^{-\alpha} \% p = k^{p-1-\alpha} \% p$ を繰り返し乗算に帰着させる.

$(2/7) \% 19$

→ これは $(3 \cdot 7) \% 19$ より 3

つまりこの乗算の形が前提となっている

そのまま計算するのは非効率

ここで使われるのがフェルマーの小定理 $a^{p-1} \% p = 1$

a と p が互いに素である. という条件でである集合 A がある.

同じサイズにする上で重要

$A = \{1, 2, \cdots, p-1\}$

この集合 A に a をかけたとき

$A' = \{a \cdot 1, a \cdot 2, \cdots, a(p-1)\}$

要素が0のときも

$0 \% p = 0 \cdot a \% p$

となり定理に適する

ここで A と A' の集合は同じ値を持つ.

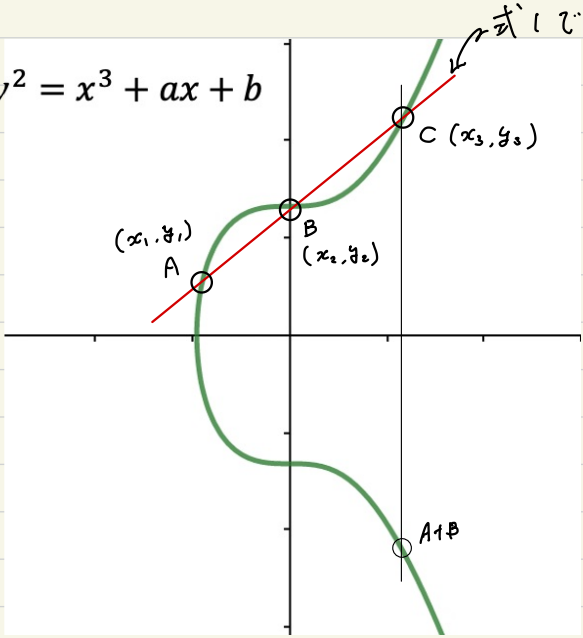
ということは. 集合の各要素の乗算結果は等しくなる.

$$(1 \cdot 2 \cdot \cdots \cdot (p-1)) \% p = (a \cdot 2a \cdots (p-1)a) \% p$$

$$(p-1)! \% p = a^{p-1} \cdot (p-1)! \% p$$

$$(p-1)! \% p = (a^{p-1} \% p \cdot (p-1)! \% p) \% p$$

$$1 = a^{p-1} \% p$$



ロードマップ

A+Bを求めたい．使えるのは AとBの座標 (x_1, y_1), (x_2, y_2)

→ Cを求める

1. A, Bを通る直線の傾きを利用
2. 楕円曲線の式に代入
   → そのままとくのは非効率なので
   解と係数の関係を利用
   → なんやかんやで Cのx座標が求まる
3. Cが判明し、x軸に対称なA+Bも求まる

式1.

AとB，BとC，CとAを通るそれぞれの直線の傾きは同じ

Aのy座標　Bのy

$$\begin{cases} S_{AB} = \dfrac{y_2 - y_1}{x_2 - x_1} \\ S_{BC} = \dfrac{y_3 - y_2}{x_3 - x_2} \\ S_{CA} = \dfrac{y_1 - y_3}{x_1 - x_3} \end{cases}$$

← S_{AB}は定数における

$$S_{AB} = S_{BC}$$

$$\frac{y_3 - y_2}{x_3 - x_2} = S_{AB}$$

$$y_3 = S_{AB}(x_3 - x_2) + y_2 \quad \cdots ①$$

この式と $y_3^2 = x_3^3 + 5x_3 + 7$ で連立方程式をそのままといてもいいけど
非効率なので式2をつくります．

式2

式1を一般化すると

$$y = s_{AB}(x - x_1) + y_1 = s_{AB}(x - x_2) + y_2 \quad \cdots ①'$$

では $y^2 = x^3 + ax + b$ に代入する。（結局代入するが、色々と手を加えます）

$$(\underbrace{s_{AB}x - (s_{AB}x_1 - y_1)}_{s_{AB}(x - x_1) + y_1})^2 = x^3 + ax + b$$

$$0 = x^3 - s_{AB}^2 x^2 + (a + 2s_{AB}(s_{AB}x_1 - y_1))x + (b - (s_{AB}x_1 - y_1)^2) \quad \cdots ②$$

ここで2つポイント

1. 方程式②の解は (x_1, y_1), (x_2, y_2), (x_3, y_3) である（1ページ前のグラフから自明）
2. 解と係数の関係（詳細は各自で調べてもらって、分からなかったら聞いて下さい）

⇓

教科書によせてかくと

1. $(x - x_1)(x - x_2)(x - x_3) = 0$
2. $s_{AB}^2 = x_1 + x_2 + x_3$ 使うのはこれだけ（これによって x_3 が計算可能）

$$a + 2s_{AB}(s_{AB}x_1 - y_1) = x_1x_2 + x_2x_3 + x_3x_1$$

$$b - (s_{AB}x_1 - y_1)^2 = x_1x_2x_3$$

$$x^3 + (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x + x_1x_2x_3 = 0 \quad \cdots ②'$$

よって

$$s_{AB}^2 = x_1 + x_2 + x_3$$

$$x_3 = s_{AB}^2 - (x_1 + x_2) \quad \cdots ③$$

①と③より

$$y_3 = s_{AB}(x_3 - x_2) + y_2 \quad \cdots ①, \quad x_3 = s_{AB}^2 - (x_1 + x_2) \quad \cdots ③$$

$\therefore$ A+Bの座標 $(s_{AB}^2 - (x_1 + x_2), \underbrace{-s_{AB}(x_3 - x_2) - y_2}_{-y_3})$ ←−にするのを忘れない