Core Program Week 0

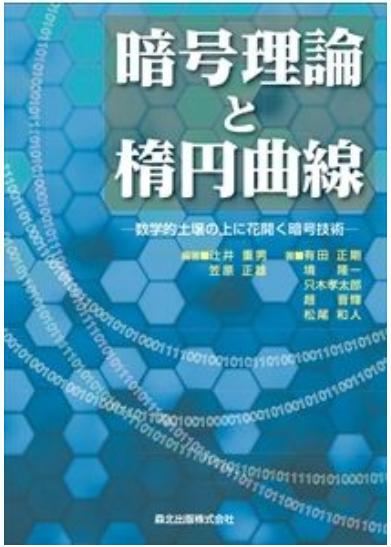
有限体と楕円曲線

ZK Tokyo

はじめに

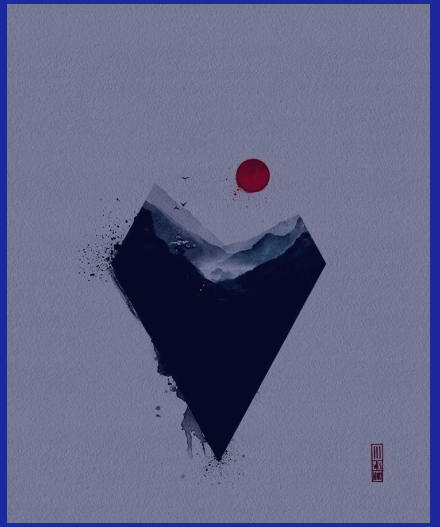
- Core Programで扱うゼロ知識証明に関する数学的前提を解説します
- 最低限の説明を目標としているため厳密な定義を省略している場合があります。以下の項目については余力があればご自身で確認されることを勧めます
  - 群、環、体の定義
  - 有限体の多項式表現
  - アフィン座標と射影座標

おすすめの書籍はこちら→



目次

mod演算と有限体



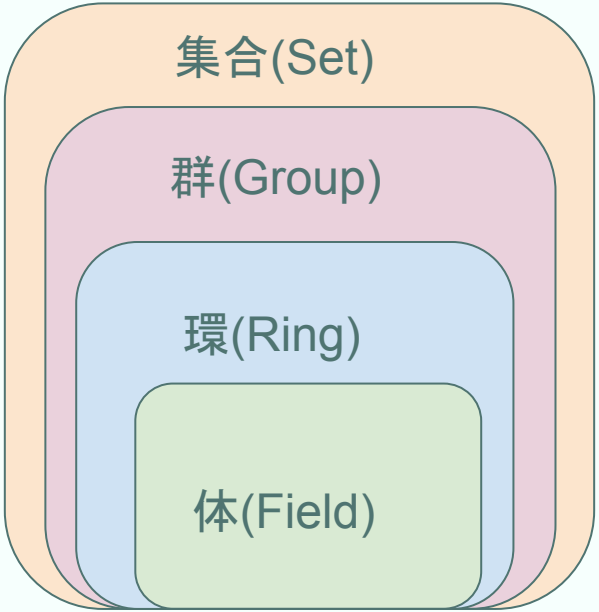
群・環・体

群：結合法則があり単位元・逆元を持つ

環：加法と乗法が定義され、分配法則を満たす

体：環であり、0以外の要素について乗法逆元

が存在する(除算が定義できる)



単位元 (identity element)とは？
ある集合 S と演算 * があるとき、要素 $e \in S$ が単位元であるとは、すべての $a \in S$ に対して次が成り立つこと

$$a * e = e * a = a$$

mod 演算とは？

- ある整数を別の整数(法: identity)で割った時の余りを求める操作

  $a \ mod \ p$は整数 aを素数 pで割った時の余りを意味する

- 演算結果は0から $p-1$の間の自然数になり、これらの要素を元と呼ぶ

p=5の例

1 mod 5= 1, 2 mod 5 = 2, 3 mod 5 = 3, 4 mod 5 = 4 , 0 mod 5 = 0

6 mod 5 = 1 ← ここで再び 1 に戻る。このような性質を巡回(cyclic)と呼び

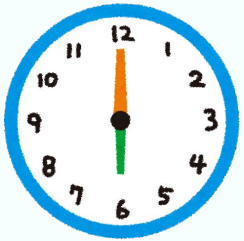
この0から $p-1$の整数集合を $\mathbb{Z}_p$と表す

なぜmod 演算を使うのか？

- 無限に大きな数字を扱うと計算効率が悪いが、mod 演算を用いると計算結果を有限範囲に収めることができる
- 例えば我々は数直線上の数字ではなく時計上の数字を扱うことで時間を操っている

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \in \mathbb{Z}_{13}$$

無限の要素を持つ整数の世界→有限個の要素を持つ有限体(Finite Field)の世界へ



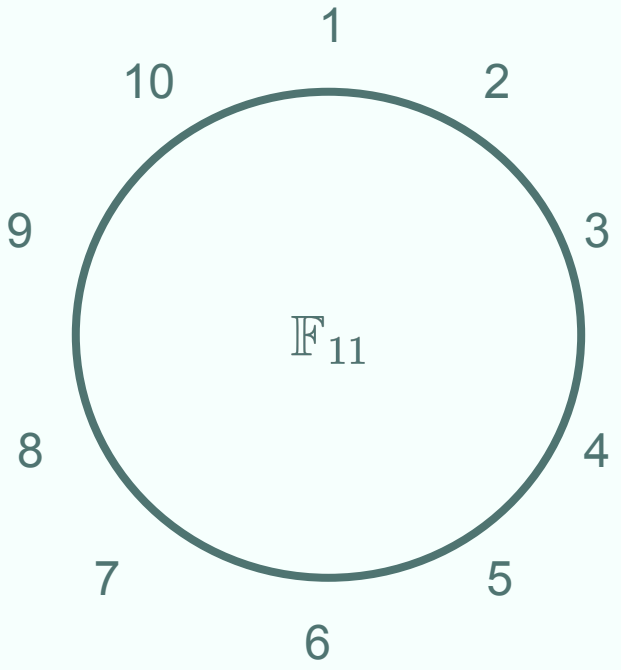
有限体：F_pとは？

- 有限体とは要素の数が有限で、四則演算が定義されている集合である
- 要素の個数 pをその体の位数(order)と呼び、有限体は $\mathbb{F}_p$表す
- 加法・乗法に対して、逆元が必ず存在する

  →減算と除算が定義できる

  つまり有限体は四則演算について閉じている

- 有限体の演算はmod演算として定義される



加算・乗算

整数どうしの加算・乗算を行い、結果を で割る

加算例

$$3 + 2 = 5 \equiv 0 (mod\, 5)$$

乗算例

$$4 \times 3 = 12 \equiv 2 (mod\, 5)$$

位数

位数：その有限体に含まれる要素の個数

位数の性質：有限体の位数は必ず「素数のベキ乗　p^n」の形になる

- p は素数
- n は正の整数

$\{0, 1\} \in \mathbb{F}_2$… 2で割った余りの世界(位数2)

$\{0, 1, 2\} \in \mathbb{F}_3$… 3で割った余りの世界(位数3)

$\{0, 1, \alpha, \alpha + 1\} \in \mathbb{F}_4$ … $\mathbb{F}_2$を拡大(後述)して作られる世界(位数4)

$\{0, 1, 2, 3, 4\} \in \mathbb{F}_5$ … 5で割った余りの世界(位数5)

逆元

- 単位元にある演算をすると1になる数のことを逆元(inverse element)と呼ぶ
- $3 + x = 1 (mod\, 5)$ の場合、加法逆元　3^{-1} は $x = 3$となる
- $3 \times y = 1 (mod\, 5)$ の場合、乗法逆元　3^{-1} は $y = 2$となる

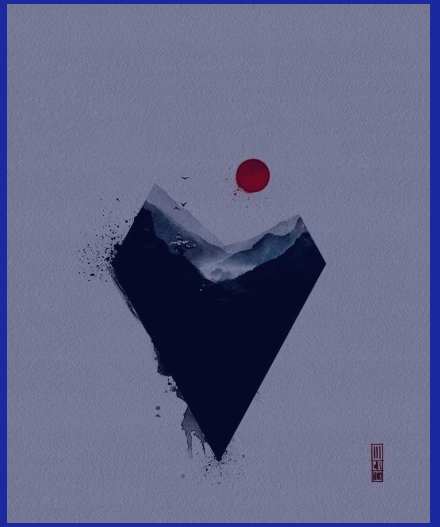
+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

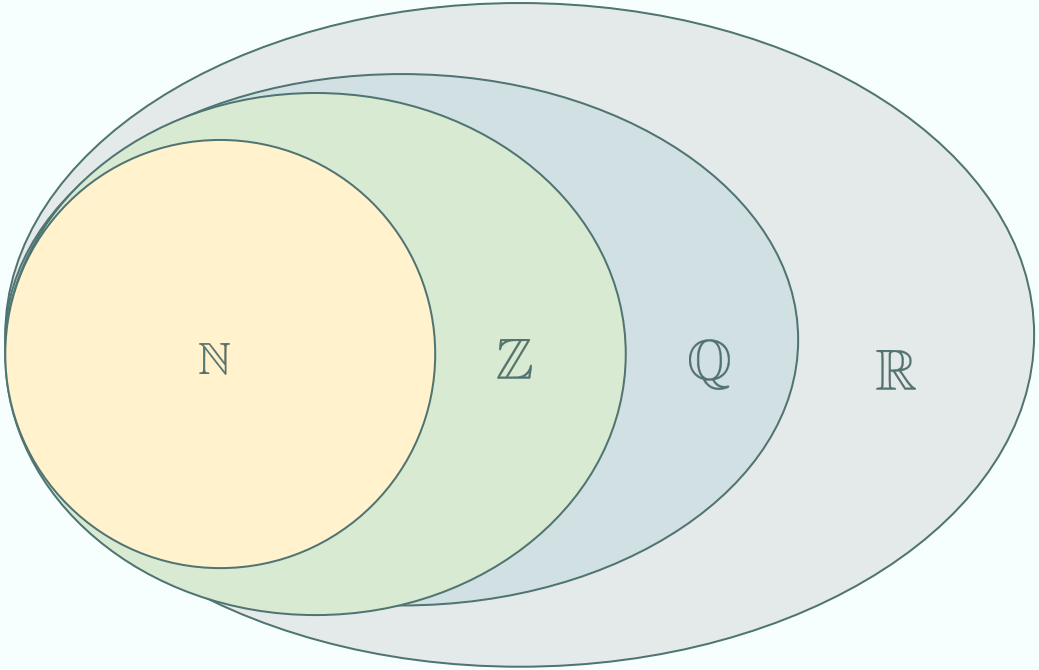
演習 1

1. 減算と除算の計算方法を調べ、それぞれ逆元に注目して説明してください
2. 拡張ユークリッド法について調べ、実装してください
3. $3 - 2 (mod\, 5)$を計算してください
4. $3 \div 2 (mod\, 5)$を計算してください
5. $(7 \times 5)^{-1} mod\, 13$ を計算してください

拡大体



数の集合のおさらい



1. **自然数** $\mathbb{N}$: 1,2,3,…
2. **整数** $\mathbb{Z}$: …,−2,−1,0,1,2,…
3. **有理数** $\mathbb{Q}$: qp の形で表せる数（p は整数、qはゼロではない整数）
4. **実数** $\mathbb{R}$: 有理数と無理数（2,π など）を合わせた数

これらの集合関係は以下のようになる

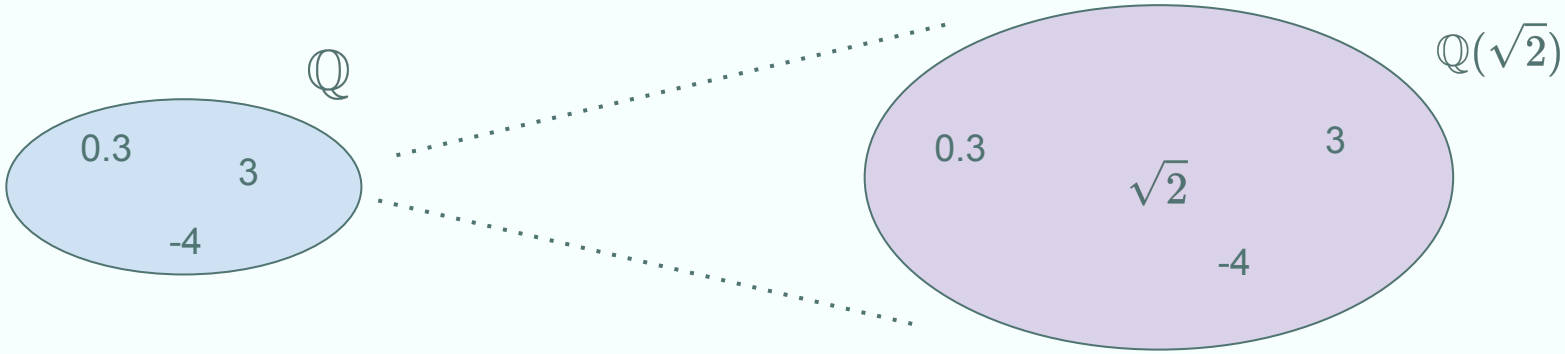
$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

拡大とは？

ある集合の中で解けなかった方程式の解を含めるために、より **大きな数の集合** を作ること

$x^2 = 2$ の解である $\sqrt{2}$ は含まれない

$\sqrt{2}$ を含んだ新しい数の集合 $\mathbb{Q}(\sqrt{2})$を考える



$\mathbb{Q}(\sqrt{2})$は $\mathbb{Q}$ の拡大体

有限体の拡大体

ある有限体 $\mathbb{F}_p$に元を追加して作られるより大きな有限体(Finite Field Extension)

もとの有限体の素数の冪乗で表現される。

$$\mathbb{F}_{p^n}$$

$\mathbb{Q}(\sqrt{2})$のように、もとの体における多項式の解として追加される

有限体では**既約多項式**(その有限体上で因数分解できない多項式)の**根**(多項式に代入したら0になる数)を追加することで構成される

根を追加するとは？
既約多項式を解けるような新しい数(記号)を導入する操作

既約多項式の例

$f(x) = x^3 + x + 1$

→因数分解できない

$\mathbb{F}_2 = \{0, 1\}$を代入してみる

$f(0) = 0 + 0 + 1 = 1$

$f(1) = 1 + 1 + 1 = 1 (mod\, 2)$

よって根は持たない

→既約多項式である
→ここに根を追加することで拡大体を構成する

$f(x) = x^2 + x = x(x + 1)$

→因数分解できる

$\mathbb{F}_2 = \{0, 1\}$を代入してみる

$f(0) = 0 + 0 = 0$

$f(1) = 1 + 1 = 0\, (mod\, 2)$

よって二つの根を持つ

→既約多項式ではない

拡大体と係数ベクトル

係数ベクトル $(a_n, a_{n-1}, \ldots, a_1)$ $a_i \in \mathbb{F}_p (i = 1, 2..n)$ であるとき

$$h(X) = a_n X^{n-1} + a_{n-1} X^{n-2} + \cdots + a_2 X + a_1$$

とすると $\mathbb{F}_2$ ではベクトル(多項式における係数部分)は0/1からなるので

例えば2次多項式は $X^2, X^2+1, X^2+X, X^2+X+1$ の四つになる

$X^2 \leftrightarrow (100)$ $X^2+1 \leftrightarrow (101)$ $X^2+X \leftrightarrow (110)$ $X^2+X+1 \leftrightarrow (111)$

$f(x)$が既約多項式である時、$h(x)$の剰余類は体となることが知られている。

また、その元の位数を q としたとき $\mathbb{F}_q$ を $\mathbb{F}_p$ の拡大体と呼ぶ

拡大体F_{2^3}の構成例

1. 既約多項式を選ぶ(ここでは $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ とする)
2. 根 αを追加する
   a. $p(x)$ の根 α を追加して拡大体 $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$ を構成する
   b. ここで $a^3 + a + 1 = 0$ と定義される

$$\mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

F_{2^3}の多項式表現とベクトル表現

多項式表現	ベクトル表現
$\alpha^0 = 1$	000
$\alpha^1 = \alpha$	001
$\alpha^2 = \alpha^2$	010
$\alpha^3 = \alpha + 1$	011
$\alpha^4 = \alpha \cdots \alpha^3 = \alpha^2 + \alpha$	100
$\alpha^5 = \alpha \cdots \alpha^4 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$	101
$\alpha^6 = \alpha \cdots \alpha^5 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$	110
$\alpha^7 = \alpha \cdots \alpha^6 = \alpha^3 + \alpha = 1$	111

既約多項式 $x^3 + x + 1 = 0$とすると　$x^3 = -x - 1 = x + 1 (mod\, 2)$から再帰的に求めることができる

拡大体の元をベクトルで表す利点

拡大体 $\mathbb{F}_{2^n}$ の元は、次数 nの多項式の係数ベクトルで表される。

これは、固定長 nビットの列として実装できるため、以下の利点がある：

- 加算・減算を各ビットの XOR演算だけで処理できるため、キャリーが不要であり、二進数に比べて高速
- 計算機での実装が容易で、暗号や誤り訂正で多用される

$\mathbb{F}_2$ においてa+a=0 であり-a=aなので

a-b=a+bが成り立つ

この特徴により加算と減算は XORで表現できる

例えば a = 101, b = 011 とすると

- a+b=110
- a-b=110

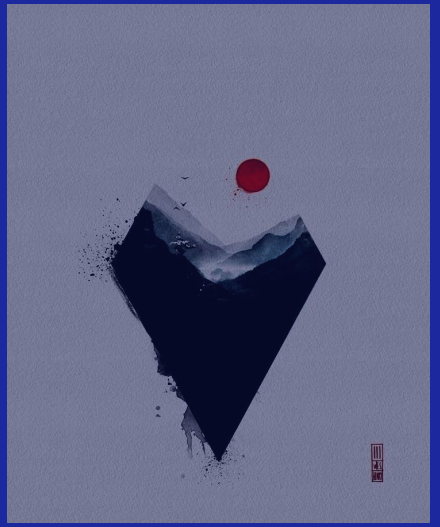
演習 2

1. $\mathbb{F}_2$で10110101-0110110を解いてください

2. $\mathbb{F}_{2^8}$で10110101-0110110を解いてください

3. $\mathbb{F}_{2^3}$における $x^3 + x + 1$以外の既約多項式を一つ見つけてください

離散対数問題



離散対数問題とは？

- $g^x \equiv h \, mod \, p$を満たす　xを求める問題
- 素数　pが大きくなると問題を解くことが困難になる
- これが暗号の安全性の前提になる問題として活用されている

例：Diffie-Hellman, ElGamal, DSA

例: $\mathbb{F}_{17}$で　$g = 3, h = 13$ のとき

$3^x = 13 mod \, 17$となる　x を求めたい

x	$3^x mod \, 17$
1	3
2	9
3	10
4	**13**

pが大きくなるとどうなる？

$p = 17$

→候補は16個なので手作業でも計算できる

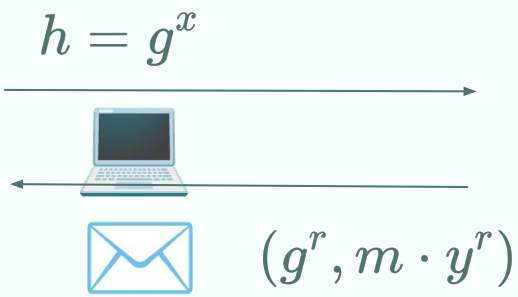
$p = 2^{256}$

→天文学的な数の候補がある

鍵の数が爆発的に増えることで総当たりで解くのは現実的に不可能になる！

離散対数問題はどのように安全性を提供するのか？

ElGamal暗号



$$m = c_2 \cdot (c_1^x)^{-1}$$

秘密鍵なしでは復号できない！

1. アリス:

- 秘密鍵 xを選ぶ

- 公開鍵 $h = g^x$をボブに渡す

2. ボブ:

- ランダム rを選ぶ

- 暗号文: $(c_1, c_2) = (g^r, m \cdot y^r)$

3. アリス:

- 秘密鍵 x を使って復号

$$m = c_2 \cdot (c_1^x)^{-1}$$

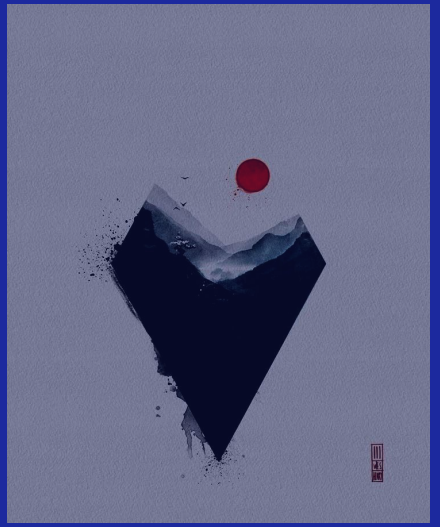
演習 3

- 離散対数問題以外で安全性仮定になっている数学的問題を2つ挙げてください。それぞれ、なぜ安全と言えるのか説明してください

- 離散対数問題を効率的に解くアルゴリズムを一つ調べ、なぜ効率的か説明してください

- $5^x \equiv 8 \pmod{23}$の離散対数 xを求めてください

楕円曲線



楕円曲線(elliptic curve)の特徴

- 短いビット長でも高い安全性を提供することができる

- 特定の楕円曲線で可能なペアリング演算がGroth16(week2)などの中核になっている

- 楕円曲線は楕円積分という分野から生まれたものであり、楕円形状になっているわけではない！

RSA

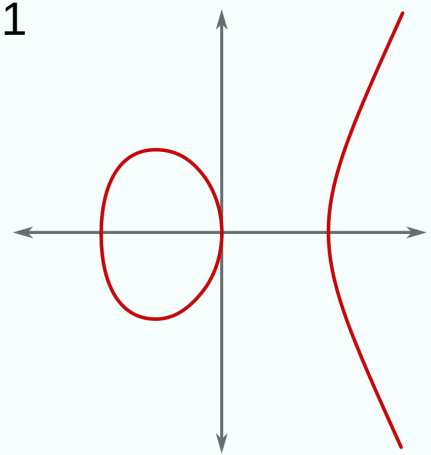
2048 bit

ECC

256 bit

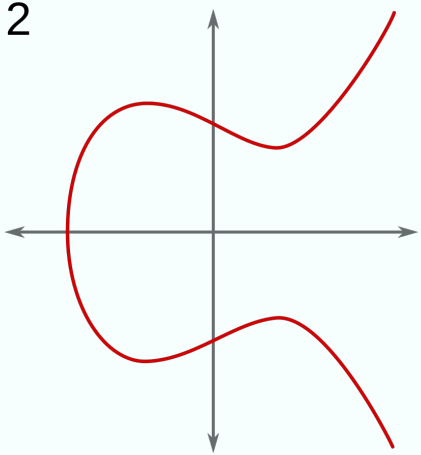
有限体上の楕円曲線の定義

1



$y^2 = x^3 - x$

2



$y^2 = x^3 - x + 1$

”実数体”上で表現した2つの楕円曲線の例

標準形: $y^2 = x^3 + ax + b\,(a, b \in \mathbb{F}_p)$

楕円曲線上の2点の加算やスカラー倍算が可能だが、加算を定義するために無限遠点(Point at inginity)を追加する

つまり楕円曲線上の点の集合　$E(\mathbb{F}p)$は正確には

無限遠点 Oと方程式を満たす有限個の点　(x, y)

から構成される　$E(\mathbb{F}_p) \cup O$と表される。

生成元G

- 楕円曲線上の特定の群のすべての点を、その点自身を繰り返し加算することで生成できる点

- 曲線上のすべての点 P は、ある整数 kを用いて $P = kG$（G を k回加算した点）と表すことができる

- $kG = O$となる最小の正の整数 kを位数と呼ぶ

例：secp256k1

$$p = 2^{256} - 2^{32} - 977$$

$$y^2 = x^3 + 7 \quad (a = 0, b = 7)$$

生成元 Gは、次の 16 進座標で定義される点：

G_x = 79BE667E F9DCBBAeC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

G_y = 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

無限遠点O

- 群を満たすために導入される点

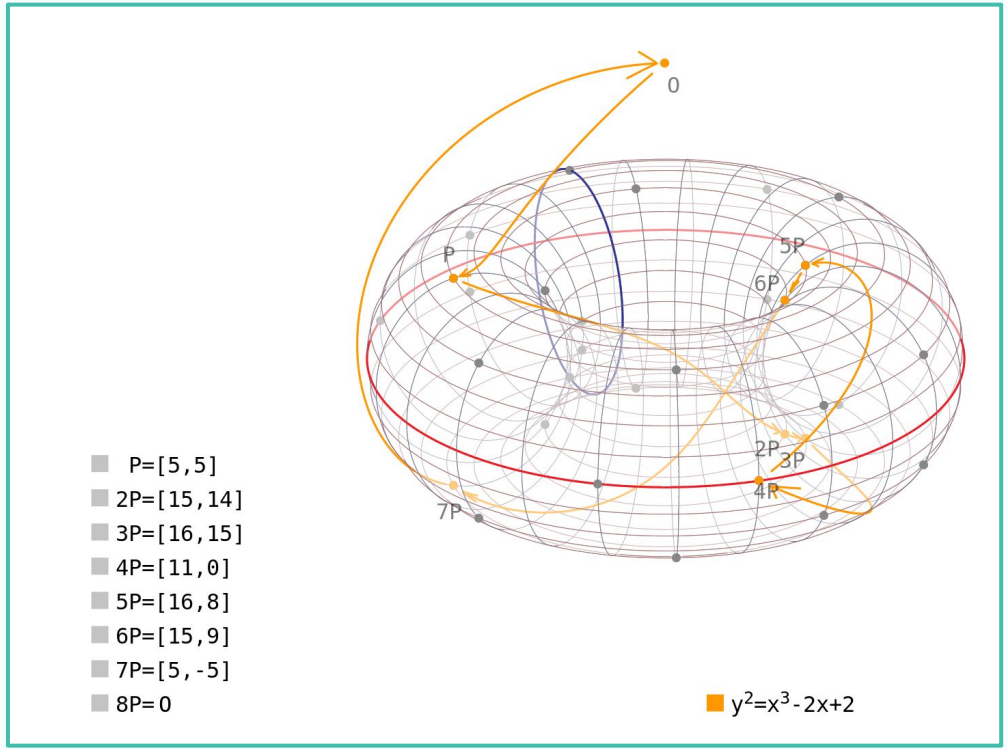
楕円曲線上の点の加算における単位元であり、加算の閉包性を保証するための仮想的な点

- 楕円曲線上の加法演算における単位元で、任意の点 P に対し、 $P + O$ が成り立つ

- 任意の点 $P = (x, y)$ に対して、その逆元は

$P' = (x, -y)$ であり、 $P + P' = O$ となる

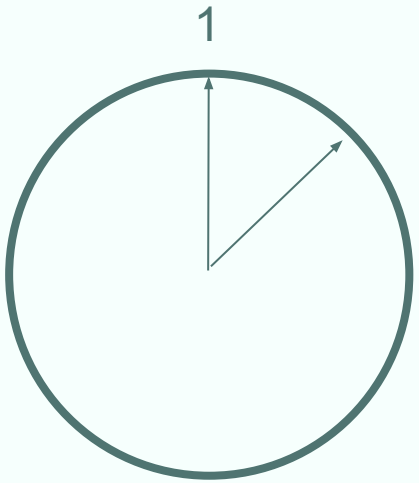
つまり、点とその逆元を加算すると無限遠点になる。



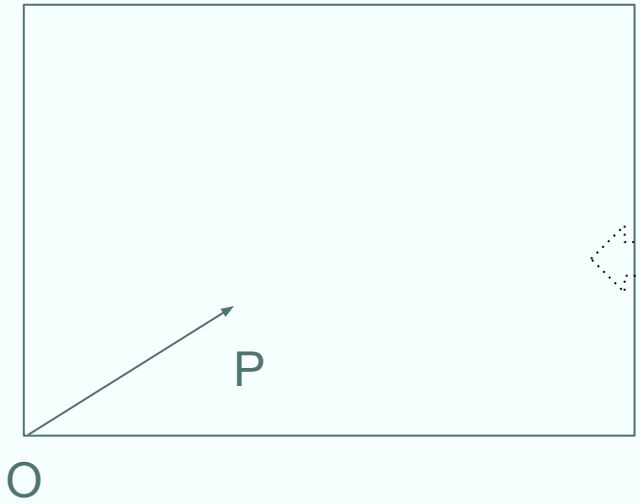
Elliptic curves: point at infinity

有限体F_p上の楕円曲線の形

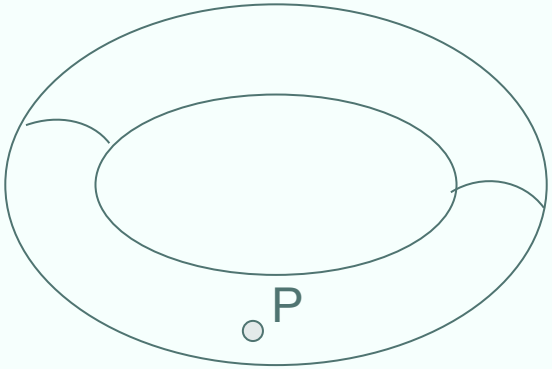
有限体(円周表現)



有限体上の楕円曲線
(二次元表現)



有限体上の楕円曲線
(三次元表現)



有限体上の楕円曲線は円周のように上下左右で閉じているので浮き輪 (トーラス)のような形になる

楕円曲線の加算

2点 $P_1 : (x_1 , y_1)$と $P_2 : (x_2 , y_2)$の加算 $P_3 : (x_3 , y_3) = P_1 + P_2$ を考える

(理解のために実際の有限体での加算に加え、実数体での加算も示す)

実数体

1. 2点を通る直線を引く
2. この直線と楕円曲線が交わる3つ目の点 P_3 を見つける
3. 点 P_3 をx軸に関して対称移動した点を

   $P_1 + P_2$とする

有限体

1. 直線の傾き $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ を計算する
2. $x_3 = \lambda^2 - x_1 - x_2 \mod p$
3. $y_3 = \lambda(x_3 - x_1) + y_1 \mod p$

それぞれシミュレータで試してみよう！

楕円曲線のスカラー倍算

- 楕円曲線上の点Pに対して、整数　n倍の点　nP

を計算する

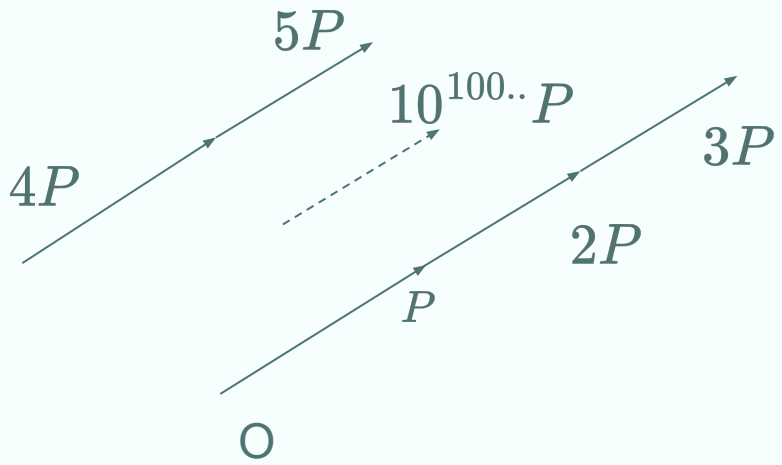
- 点　Pの加算をn回繰り返す演算になる

$$P + P + \cdots + P$$

楕円曲線上の離散対数問題: ECDLP

点　P　から点　nPを計算することは簡単だが、

逆は難しい



楕円曲線上の離散対数問題

楕円曲線上の離散対数問題の困難性もまた重要な暗号プリミティブの安全性に利用されている

1. Diffie-Hellman鍵共有プロトコルの楕円曲線版 (ECDH)
2. 楕円曲線デジタル署名アルゴリズム (ECDSA)
3. 楕円曲線ElGamal暗号など

脆弱な曲線を選ばないように注意深くパラメータを選定することが重要

ペアリング

BLS12-381など特定の楕円曲線上で定義される特殊な関数

$$e : G_1 \times G_2 \to G_T$$

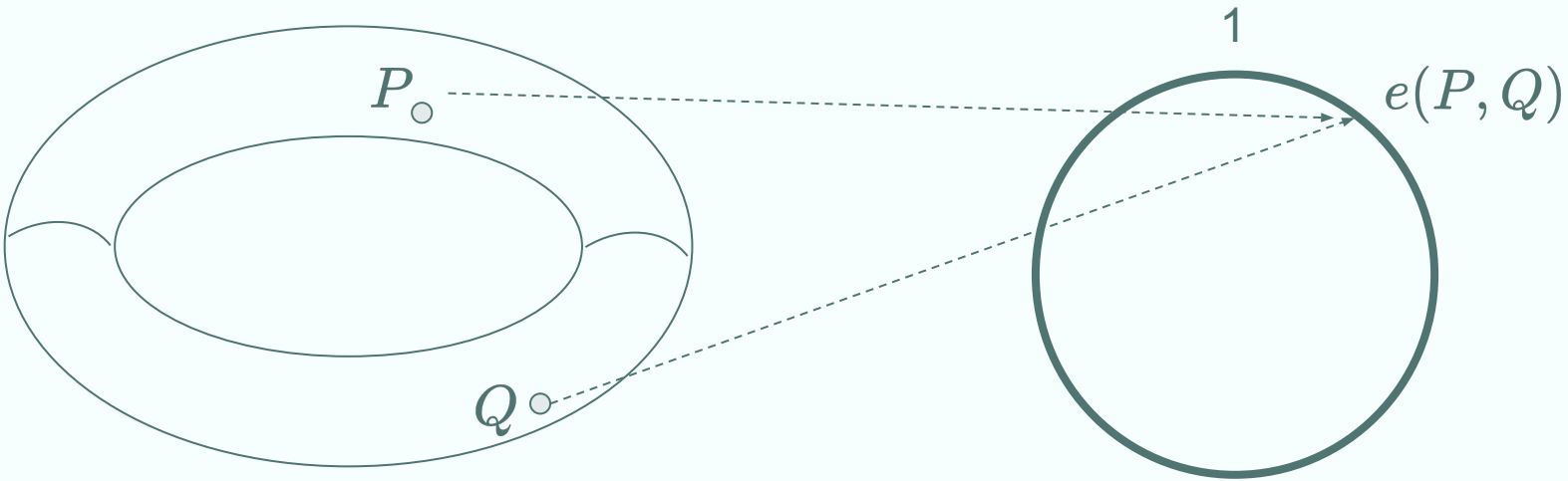
2つの楕円曲線上の点を、有限体上の乗法群に写像する双線形性(bilinearity property)が最大の特徴

$$e(aP, bQ) = e(P, Q)^{ab}$$

ゼロ知識証明の効率的な検証を実現するために重宝される

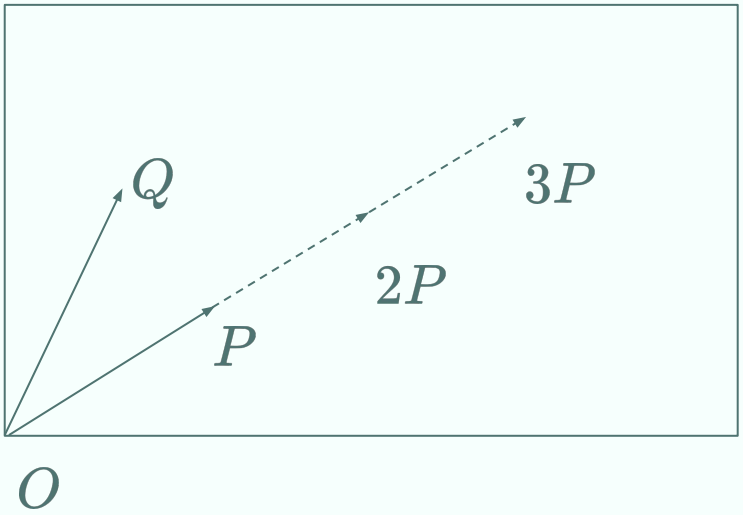
ペアリング写像のイメージ

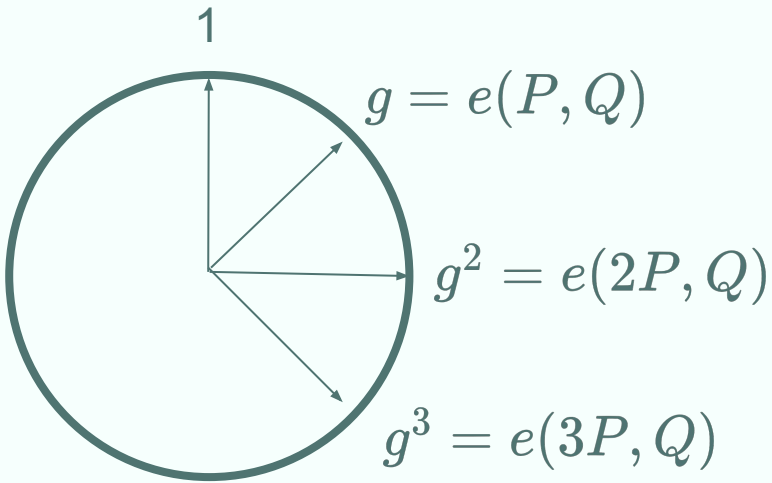
2点P, Qを入力とし、出力　$e(P, Q)$が決まるという関数



双線形性

楕円曲線上の点を2倍、3倍すると有限体上の点は2乗、3乗のところに進む





整数 a, b に対して $e(aP, bQ) = e(P, Q)^{ab}$ となる性質が双線形のポイント

演習 4

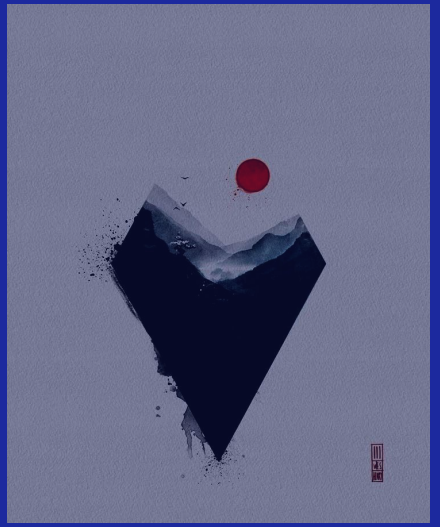
- ECDLPを効率的に計算するアルゴリズムをひとつ挙げてください
- スカラー倍算を効率的に計算するアルゴリズムをひとつ挙げてください
- ゼロ知識証明ライブラリ「Circom」で使われているデフォルトの楕円曲線を調べてください
- BLS12-381上の2点P(3,5),Q(5,3)の加算をシュミレータを使って計算してください

参考資料

- https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/
- https://andrea.corbellini.name/ecc/interactive/modk-mul.html
- https://trustica.cz/en/blog/2018/03/29/elliptic-curves-point-at-infinity/
- https://www.morikita.co.jp/books/mid/084751

ZK Tokyo

Thank you!



mod 演算とは？

- ある整数を別の整数(法)で割った時の余りを求める操作

  $a \ mod \ p$は整数 aを pで割った時の余りを意味する

- 演算結果は0から $p-1$ の間の自然数になる
- pで割った時の余りの整数集合を $\mathbb{Z}_p$と表す
- 各要素を元と呼ぶ

$$7 \ mod \ 5 = 2$$

$$10 \ mod \ 3 \ = 1$$