1 群・環・体

$\mathbb{Z}$ = {整数} = {0, ±1, ±2 ··· }

$\mathbb{Q}$ = {有理数} = $\{ \frac{a}{b} \mid \mathbb{Z} \ni a, b \neq 0 \}$

演算：加法 +　　乗法 ×

$(\mathbb{Z}, +)$　　$(\mathbb{Z}, \times)$

① 演算について閉じる

$\mathbb{Z} \ni a, b$　　$a+b \in \mathbb{Z}$　　$a \times b \in \mathbb{Z}$

② 結合法則：$\mathbb{Z} \ni a, b, c$

$(a+b)+c = a+(b+c)$　　$(a \times b) \times c = a \times (b \times c)$

③ 単位元：演算結果を変えない元

$\mathbb{Z} \ni 2$　$2 + \square = \square + 2 = 2$　　$2 \times \square = \square \times 2 = 2$

$\square$ = 0　　$\square$ = 1

0が単位元 → 零元とも呼ぶ　　1が単位元

④ 逆元：単位元に戻す元

$\mathbb{Z} \ni 2$　$2 + \square = \square + 2 = 0$　　$2 \times \square = \square \times 2 = 1$

$\square$ = −2　　$\square \notin \mathbb{Z}$

$\mathbb{Z} \ni {}^{\forall}a$　$a + \square = \square + a = 0$　　（逆元のみる元を正則元という）

となる？ → OK

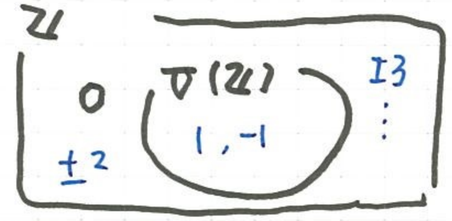
Def (群)
集合 S，演算 $*$ に対して ①演算に関して閉じる ②結合法則 ③単位元 $\in S$ ④ $S \ni {}^{\forall}x$ に対し x に逆元 $x^{-1} \in S$ となるとき，群という

$U(\mathbb{Z}) = \{ \mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z} \}$

$= \{ \mathbb{Z} \ni a \mid a$ は 可逆元 $\}$

$= \{ 1, -1 \}$

$\mathbb{Z} \setminus \{0\} \supsetneq U(\mathbb{Z})$



⊙ 目標　R (環)

$U(R) = \{R$の正則元$\}$

$= R \setminus \{0\}$

Def (環)
集合 R に 演算 (+, ×) が定義されていて 1)4) をみたすとき 環 という．

(加法) 群となる

(乗法) ・演算に関して閉じている．

・結合法則をみたす．

・単位元　$1 \in R$

(分配法則)　$R \ni a, b, c$ に対して

$(a+b) \times c = a \times c + b \times c$

$a \times (b+c) = a \times b + a \times c$

Example
・$\mathbb{Z}$ は 環，　$\mathbb{Q}$ は環，　$M_2(\mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \}$ は環

1.1 剰余 環

$\mathbb{Z} \ni m > 0$ に対して $\mathbb{Z}$ を m で割った余りの集合 $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \cdots, m-1\}$

(記号) $\mathbb{Z} \ni a, b$ に対し $\mathbb{Z} \ni m > 0$

$a-b$ を m で割った余りを

$a-b \pmod m$ と表わす.

$a \equiv b \pmod m \iff a$ と b の m で割った余りが同じ

$\iff a-b$ が m で割れる

$\mathbb{Z}/m\mathbb{Z} \ni a, b$ に対して

(加法) $a+b \equiv a+b \pmod m$

(乗法) $a \times b \equiv a \times b \pmod m$

Example $m=3$ $\mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/3\mathbb{Z} \ni 2$ の逆元は 2

$2 \times \square = \square \times 2 = 1$

$\cup(\mathbb{Z}/3\mathbb{Z}) = \{1,2\}$

$\cup(\mathbb{Z}/3\mathbb{Z}) = \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$

Def 環 R で $R \setminus \{0\} \ni a$ に対して 逆元が存在するとき

R を体という。

Example $\mathbb{Z}/3\mathbb{Z}$ は体.

$m=4$ のとき? $\mathbb{Z}/4\mathbb{Z}$

0

1 $\cup(\mathbb{Z}/4\mathbb{Z}) = \{1,3\}$

2 $\cap$

3 $\mathbb{Z}/4\mathbb{Z} \setminus \{0\}$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Theorem

$\mathbb{Z} \ni p$: 素数 のとき $\mathbb{Z}/p\mathbb{Z}$ は 体となる.

このとき p 個の元をもつ 有限体 と呼ばれて $\mathbb{F}_p$ とかく.

1. 3 逆元の求め方

(目標) $\mathbb{Z}/m\mathbb{Z} \ni a$ に逆元があるとき a^{-1} を求める

Euclid の互除法

入力 : $\mathbb{Z} \ni a, b \neq 0$ 出力 : $\gcd(a,b)$: a と b の最大公約数

除法の原理 : $\mathbb{Z} \ni a, b$ に対して

$a = bq + r$ q : 商 $\exists!$, r : 余り $\exists!$ $(|b| > r \geq 0)$

$\gcd(a,b) = \gcd(b,r)$

1. $a_0 \leftarrow a$, $a_1 \leftarrow b$, $q_1 \leftarrow q$, $a_2 \leftarrow r$ とする

$a_0 = a_1 q_1 + a_2$ $(|a_1| > a_2 \geq 0)$

$a_1 = a_2 q_2 + a_3$ $(|a_1| > a_2 > a_3 \geq 0)$

$\vdots$

$a_{i-1} = a_i q_i + a_{i+1}$ $(|a_1| > a_2 > \cdots > a_{i+1} = 0)$

$\gcd(a_i, 0) = a_i$

2. $\gcd(a_i, a_{i+1}) = a_i$ を出力

拡張 Euclid 互除法

入力 : $\mathbb{Z} \ni a, b \neq 0$, 出力 : $\gcd(a,b) = d$ のとき

$ax + by = d$ となる $x, y \in \mathbb{Z}$

Euclid の互除法 の数列 $\{a_i\}$

$$\begin{cases} a_{j-1} = a_j q_j + a_{j+1} \\ a_j = a_j \end{cases}$$

$$\Rightarrow \begin{bmatrix} a_{j-1} \\ a_j \end{bmatrix} = \begin{bmatrix} q_j & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_j \\ a_{j+1} \end{bmatrix}$$

（$= L_j$）　$\det(L_j) = -1 \neq 0$

$L_j^{-1} = M_j \in M_2(\mathbb{Z})$ (整数行列)

両辺に M_j をかけると

$$\begin{bmatrix} a_j \\ a_{j+1} \end{bmatrix} = M_j \begin{bmatrix} a_{j-1} \\ a_j \end{bmatrix} = M_j M_{j-1} \cdots M_1 \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

$$\begin{bmatrix} a_i \\ a_{i+1} \end{bmatrix} = M_i \cdots\cdots M_1 \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

（$a_i = d$, $a_{i+1} = 0$；$M_i \cdots M_1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ 整数行列）

$$\begin{bmatrix} d \\ 0 \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} ax + by \\ az + bw \end{bmatrix}$$

① $\mathbb{Z}/m\mathbb{Z} \ni a$, $\gcd(a, m) = 1$ に対して 拡張 ECD より

$ax + my = 1$ となる $x, y \in \mathbb{Z}$

$ax = 1 - my \equiv 1 \pmod{m}$

x は a の逆元

(1)べき乗演算　$\mathbb{Z} \ni g > 0$, $\mathbb{Z} \ni k > 0$, $\mathbb{Z} \ni p$：素数

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (体)

$g^k \pmod{p}$ の計算

$g^k = \underbrace{g \times \cdots \times g}_{k\text{コ}} \pmod{p}$

$k = 7$ とする．$7 = 111 = 1\cdot 2^2 + 1\cdot 2 + 1\cdot 2^0$

・$g^7 = g \times \cdots \times g$ ： 6回乗算

$g^{111} = (g^2 \cdot g)^2 \cdot g = g^{2^2} g^2 \cdot g$

1 ・ 1 　 1

2乗算 2回
乗算 2回
} 4回

$g^k \pmod{p}$

$g \times g = g^2$

↑ nビット　↑ nビット　↑ 2n bit

$g \to g^2 \times g \longrightarrow g^2 \pmod{p} \times g$ (2nビット)

nビット ⟼ 2nビット　　↑ nビット　↑ nビット

2. べき乗剰余

Fermat's 小定理　　$\forall a > 0$,　$\forall p$: 素数

$gcd(a,p)=1$ とする．このとき

$$a^{p-1} \equiv 1 \pmod p$$

proof

$\forall a, b$　　p: 素数

$$(a+b)^p = a^p + {}_pC_1 a^{p-1}b + {}_pC_2 a^{p-2}b^2 + \cdots + {}_pC_{p-1} ab^{p-1} + b^p$$

$$\equiv a^p + b^p \pmod p$$

一般に

$$(\underbrace{a_1 + \cdots + a_a}_{a\text{コ}})^p \equiv a_1^p + \cdots + a_a^p \pmod p$$

$a_i = 1$ とする

$$(1 + \cdots + 1)^p \equiv 1 + \cdots + 1 \pmod p$$

$$a^p \equiv a \pmod p$$

$$a(a^{p-1} - 1) \equiv 0 \pmod p$$

$gcd(a,p)=1$ より　　$a^{p-1} \equiv 1 \pmod p$

Fermat's 小定理を逆元に用いる．

$$a^{p-1} \equiv 1 \pmod p$$

$$a^{p-2} \cdot a \equiv 1 \pmod p$$

$\square \cdot a \equiv 1 \pmod p \Rightarrow \square$ は逆元

$a^{-1} \equiv a^{p-2}$ で求められる．

2.1 DH鍵共有法

・AとBが公開のNWを用いて秘密鍵を共有する．

・DLP (Discrete Logarithm Problem)

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (有限体) と $\mathbb{F}_p^\times = U(\mathbb{F}_p)$ の g, y に対して

$$y = g^x = g \times \cdots \times g$$

となる x を存在すれば… 求める問題を離散対数問題という

(設定)　$\mathbb{F}_p$ と $\mathbb{F}_p^\times$ の g と　$ord(g) = \ell$ (位数) を共有する

(def)　G: 群．　G の g に対して
$g^\ell = g \times \cdots \times g = 1$ となる最小の
$\exists \ell > 0$ が ω を g の位数という。

(注)　$\mathbb{F}_p$ の a に対して a の位数は $p-1$ の約数となる．

(Fermatの小定理)

2019.07.13 ⑤

A

1. 秘密 $a \in [1, l-1]$ を取る

$y_a = g^a \pmod p$

2. $(y_b)^a \equiv g^{ab} \pmod p$

$\equiv k_{ab}$

3. 共有 key を k_{ab} とする

公開NW

B

1 秘密 $b \in [1, l-1]$

$y_b \equiv g^b \pmod p$

2. $(y_a)^b \equiv g^{ab} \pmod p$

$\equiv k_{ab}$

3. 共有 key を k_{ab} とする.

- moodle に 自分の公開鍵 をおく
- TA と key 共有する.
- チームの 共有 key の個数を 競争する.

3. ElGamal暗号

公開鍵暗号 = (鍵生成, 暗号化, 復号)

(公開鍵, 秘密鍵)

鍵生成

1 有限体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, \cdots, p-1\}$, $\mathbb{F}_p^\times$ (ベースポイントと呼ぶ) gの位数 $\mathrm{ord}(g) = \ell$ (素数)

2 $x \in \mathbb{Z}/\ell\mathbb{Z} \setminus \{0\} = [1, \cdots, \ell-1]$ に対応

$$y = g^x \pmod p$$

公開鍵 y. 秘密鍵 x

暗号化

平文 (plaintext) $m \in \mathbb{F}_p^\times$ (公開key y)

1 乱数 $r \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ に対応 $u = g^r \pmod p$

2. $c = y^r \cdot m \pmod p$ を計算 (同じ)

3. $(u, c) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ が暗号文

復号

暗号文 $(u, c) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ (秘密鍵 x)

1 $u^x = (g^r)^x = (g^x)^r = y^r \pmod p$

2 $c / u^x = (y^r \cdot m) / y^r = m \pmod p$

必要な演算

	べき演算	乗算	逆元
鍵生成	1 ◎		
暗号化	1 ◎	1 ◎	
復号	1 ◎	1 回	1 回

ElGamal暗号の特徴

準同型性 : $\varphi : G_1 \to G_2$ (G_1, G_2: 群) 準同型とは

G_1 内 x_1, x_2 $\quad \varphi(x_1 \cdot x_2) = \varphi(x_1) \odot \varphi(x_2)$

($\cdot$: G_1演算, $\odot$: G_2の演算)

$$\mathrm{Enc} : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times \times \mathbb{F}_p^\times$$
$$m \longmapsto (g^r, y^r \cdot m)$$

$$\mathrm{Enc}(m_1) \cdot \mathrm{Enc}(m_2) \overset{?}{=} \mathrm{Enc}(m_1 \cdot m_2)$$

$$\mathrm{Enc}(m_1) \cdot \mathrm{Enc}(m_2) = (g^{r_1}, y^{r_1} m_1) \cdot (g^{r_2}, y^{r_2} m_2)$$
$$= (g^{r_1} \cdot g^{r_2}, \; y^{r_1} m_1 \, y^{r_2} m_2)$$
$$= (g^{r_1 + r_2}, \; y^{r_1 + r_2} (m_1 m_2))$$

復号 $\longrightarrow$ $m_1 \cdot m_2 \pmod p$ となる

$\therefore \mathrm{Enc}(m_1) \cdot \mathrm{Enc}(m_2) = \mathrm{Enc}(m_1 \cdot m_2)$

※ 2つの暗号文の積で、復号せずに元の平文の積の暗号文が作れる。

(応用例) 暗号文を同じ平文で自動的に変更する方法

単位元は演算結果をかえない

みためは

$Enc(m) \rightarrow Enc(1) \cdot Enc(m) \neq Enc(m)$

$\parallel$

$Enc(1 \cdot m)$

$\parallel$

$Enc(m)$ → 復号すると m になる

確率暗号 (⇔ 確定的暗号)

同じ平文でも暗号文が異なる

$Enc(m) = (g^{r}, g^{r} \cdot m)$

r をおしすう

4 DSA署名

署名 = (鍵生成, 署名生成, 署名検証)

(公開鍵, 秘密鍵)

鍵生成 : $y = g^x \pmod p$ ←ElGamalと同じ

① $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\} \Rightarrow g$, $\mathrm{ord}(g) = \ell$ (素数)

② Hash func $H: \{0,1\}^* \to \{0,1\}^{|\ell|-1}$

署名生成 $m \in \{0,1\}^*$

① $H(m) = m'$ を計算

② 乱数 $r \in \mathbb{Z}_\ell \setminus \{0\}$ $\quad (\mathbb{Z}_\ell = \mathbb{Z}/\ell\mathbb{Z})$

$u_1 = g^r \pmod p$ 1,024 2048

$u \equiv u_1 \pmod \ell$ 160 bits 224

③ $v \equiv r^{-1}(m' + x u) \pmod \ell$ ←①(署名式)

$v = 0$ のとき Step② に戻る

④ 署名 $(u, v) \in (\mathbb{Z}/\ell\mathbb{Z})^\times \times (\mathbb{Z}/\ell\mathbb{Z})^\times$

(検証の考え方)

$vr \equiv (m' + x u) \pmod \ell$

$\Leftrightarrow g^{vr} \equiv g^{m'} \cdot g^{xu} \pmod p$

$\Leftrightarrow (g^r)^v \equiv g^{m'} \cdot y^u \pmod p$

$\Leftrightarrow u_1 \equiv g^{m'/v} \cdot y^{u/v} \pmod p$ ← 誰でも計算可

署名検証 $(m, (u, v))$ を検証

① $m' = H(m)$ を計算

② $t = 1/v \pmod \ell$ を計算

③ $u' = g^{m't} y^{ut} \pmod p$ を計算

④ $u \equiv u' \pmod \ell$ となることを検証

必要な演算

	べき乗	乗算	逆元
署名生成	1	2	1
署名検証	2 (1+α)	3	1

$g^a y^b$ を一挙に計算

$(a,b) = (1,1), (0,0), (1,0), (0,1)$

$a = 1\,0\,1\,1\,1\,0\,0$ 1

$b = 1\,0\,0\,1\,0\,0\,1\ldots$

gy 1 g y

べき乗 = 固定点と任意点 でアルゴリズムを変えることができる

g^r と $g^{m't}, y^{ut}$