2023/07/19-ver13

離散数学 課題集 2023 年度

宮地 充子

大阪大学大学院

Email: ta-dismath-23@crypto-cybersec.comm.eng.osaka-u.ac.jp

概 要

本講義は Flipping 講義を導入し，講義の内容を事前にクイズで挑戦できるようになっています．クイズの解答は講義の中で実施します．解答に挙手した学生は出席カウントを実施します．本講義の教科書は「代数学から学ぶ暗号理論」宮地充子（日本評論社）です．課題は教科書に未記載の課題が多いので，教科書の課題を解くと，違った観点で学習ができ，理解が深まります．講義のスケジュールに各回の講義のキーワードが記載されています．教科書の予習に活用してください．前半 4 回は代数学の抽象的な内容，後半 2 回は前半の内容を実際に整数の上で再現します．前半がわからなくても，後半でわかるようになるので，最後まで続けてください．DX の基礎となるディジタルの世界は，数学という法律で秩序づけられています．ディジタルの世界を数学から見てみましょう．

整数論，セキュリティの科学としての面白さに，数字で現象を確認できることがあります．さらに，数字で確認した現象から，一般的に成り立つ条件を想定し，その条件を証明するというスタイルも研究の一つです．本課題では講義の内容を理解するとともに，具体例から一般化を試み，その証明をすることも学習します．受講者一人一人，見つける現象は違うことがあります．自分なりに一般的に成り立つケースを考えてみましょう．私の講義では毎年，研究の流行を反映した新しい課題が入ります．課題の裏に隠れた研究の旬を感じてもらえればと思います．研究を行うのに最も大切な，発想の思考方法も伝わればと思います．問題を解くときは，習った知識を前提に解きましょう．現象を見て，その次の講義でその現象を定理として証明する場合があります．まずは現象を手で実感することが大切です．
本講義は情報通信工学演習も兼ねています．情報通信工学演習の課題は † を付けます．情報通信工学演習を受講しない学生で，† の課題を提出した場合，加点します．†† は発展問題です．できる人は挑戦しましょう．

目 次

1 群 1 回目：群，部分群

なぜ，群や演算という概念を考えるのでしょうか? 数をデータのように扱うとそれは無秩序な集まりです．演算を定義することで，数に秩序と意味を与えることができます．生成元の概念を用いて，群を最小限の元で表すと，群の構造も解析しやすくなります．

問 1.1. *4* 次の置換 σ とは $\{1,2,3,4\}$ から $\{1,2,3,4\}$ への全単射写像である．$S_4 \ni \sigma, \tau$ に対して，$\sigma\tau$ を自然な写像の合成で定義する．例えば，$S_4 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ に対して，

$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ となる．このとき，*4* 次の置換からなる集合 S_4 は群となり，*4* 次置換群と呼ぶ[1]．
特に *2* つの元を入れ替える置換 (i, j) を互換と呼ぶ．S_4 の部分集合で，偶数個の互換の積からなる集合を A_4 とあらわす．この時，以下の問いに答えよ

(1) S_4 の元の個数を求めよ．

(2) S_4 から位数 *4* の部分群を全て構成してみよう．

(3) S_4 の部分集合で $\{1, 2, 3\}$ の置換の集合 H を考える．つまり $S_4 \supset H = \left\{ f \mid f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(1) & f(2) & f(3) & 4 \end{pmatrix} \right\}$ は S_4 の部分群であることを示せ．

(4) S_4 の元の最大位数を求めて，その位数をもつ元を一つ求めよ．

問 1.2. † ζ_6*: 1* の原始 *6* 乗根 *(6* 乗して初めて *1* になる数*)* とし，$G = \langle \zeta_6 \rangle$ とする．G の全ての部分群は一つの生成元で表されることを以下のステップで証明しましょう[2]．

(1) G の元をすべて求めよ．（集合として元を記載する．）

(2) 異なる部分群 $H_i = \langle \zeta_6^i \rangle$ のみを列挙せよ．*(*重複のない部分群を列挙する）

(3) $G \ni \zeta_6^i, \zeta_6^j$ で生成される部分群 $H_{i,j} = \langle \zeta_6^i, \zeta_6^j \rangle$ を考える．このとき，$\langle \zeta_6^i, \zeta_6^j \rangle = \langle \zeta_6^k \rangle$ となる k を求めよ．*(*任意の部分群が一つの元で生成できることを証明する．*)*

(5) (1)-(4) を用いて，「G の全ての部分群 H を一つの生成元で表せ．また，それら以外に部分群がないこと」を証明しましょう．論理に抜けがないか確認して記載しましょう．

問 1.3. †† *3* 次の置換 σ とは $\{1, 2, 3\}$ から $\{1, 2, 3\}$ への全単射写像である．S_3 は問 *1.1* のように群となる．このとき，以下の問いに答えよ．

(1) S_3 の元の個数を求めよ．

(2) S_3 に位数 *6* の元が存在しないことを示せ．(存在すると矛盾することを示すとよい．)

2 群 2 回目：剰余類，正規部分群，剰余群

本章では，数学的な割るという概念（同値類を一つと考える），2 個以上の生成元を持つ群と 1 つの元で生成される群の違い，$U(\mathbb{Z}/n\mathbb{Z})$ と $\langle \zeta_n \rangle$ の群としての違いも理解しましょう．正規部分群は非可換な群の中に可換な性質を作ることができます．Lagrange の定理は部分群が群の元の個数で決定できるという定理です．数学の概念は使うことによって理解が深まります．いくつかの事例で定理を使ってみましょう．

問 2.1. 正整数 m に対して，ζ_m*: 1* の原始 m 乗根 *(*m 乗して初めて *1* になる数*)* とし，$G = \langle \zeta_m \rangle$ とする．このとき 以下の問いに答えよ．

(1) $m = 2, \cdots, 20$ とする．G の全ての部分群の個数が最大となる m を求め，その理由を述べよ．

(2) m は任意の正整数とする．G の全ての部分群の個数が *3* となる最小の m を求めよ．また，その m が最小となる理由を述べよ．さらに，その G の各部分群の生成元を ζ_m を用いて記述せよ．

問 2.2. $1 \leq n$ を正整数とし，ζ_n を 1 の原始 n 乗根 *(*n 乗して初めて 1 になる数*)* とする．$\mathbb{Z}/8\mathbb{Z}$ 上の演算は乗算とし，$H_8 = U(\mathbb{Z}/8\mathbb{Z}) = \{\mathbb{Z}/8\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/8\mathbb{Z}\}$ 及び $G_2 = \langle \zeta_2 \rangle$, $G = G_2 \times G_2$ を考える．ここで，G は G_2 の直積群と呼ばれ，直積群の演算はそれぞれの群の演算で定義する．つまり，$G \ni (x_1, y_1), (x_2, y_2)$ に対して，$G \ni (x_1 x_2, y_1 y_2) = (x_1, y_1) \cdot (x_2, y_2)$ で定義する．この時，以下の問に答えよ．*(* 元の個数が同じ群の構造について理解する．*)*

1. H_8 の位数を求めて，生成元の集合を *1* 組求めよ．なお，生成元の集合は最小数の元で生成できる集合をさす．
2. H_8 の部分群をすべて求めて，その生成元を挙げよ．また，それがすべてであることを示せ．
3. G の位数を求めて，生成元を求めよ．
4. G の部分群をすべて求めて，その生成元を挙げよ．また，それがすべてであることを示せ．

[1] 対称群とも言う．
[2] 本問題は G の部分群と生成元がどのような関係になるか，手で解きながら，現象を理解することが目標です．その現象を一般的に記述することが，数学の定理の一歩となります．

問 2.3. † *3*次の置換 σ とは $\{1,2,3\}$ から $\{1,2,3\}$ への全単射写像である．$S_3 \ni \sigma, \tau$ に対して，$\sigma\tau$ を自然な写像の合成で定義する．順序は τ を行ってから σ を実施する，例えば，$S_3 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ に対して，$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ となる．このとき，*3*次の置換からなる集合 S_3 は群となり，*3*次置換群と呼ぶ．特に *2*つの元を入れ替える置換 (i,j) を互換と呼ぶ．例えば，τ は置換となり，$\tau = (2.3)$ で表される．

(1) $H = \langle\sigma\rangle$ とするとき，H の元をすべて列挙し，元の個数を求めよ．

(2) $K = \langle\sigma\rangle$ が S_3 の正規部分群になることを証明せよ．

(3) $L = \langle\tau\rangle$ が S_3 の正規部分群にならないことを証明せよ．

問 2.4. 群 $H = U(\mathbb{Z}/16\mathbb{Z}) = \{\mathbb{Z}/16\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/16\mathbb{Z}\}$ 及び H の部分群 $K = \langle 5\rangle$ に対して，以下の問に答えよ．この時，以下の問に答えよ．

(1) H/K の完全代表系を示せ．

(2) H/K は剰余群になる．このとき $H/K \ni a, b$ に対して，$H/K \ni a \cdot b$ を完全代表系同士の乗算結果を表に表せ．

3 準同形写像，環，零因子，イデアル

ギリシャ時代から数学が使われていた伝統から，ξ などのギリシャ記号が利用されます．日本人には見慣れませんが，記号を通してギリシャ文字にも慣れましょう．正規部分群や剰余群，Lagrange の定理は写像でも利用します．講義の課題に具体例を入れますので，その中で理解を深めてください．定義では，定義が機能するか，定義が矛盾しないか?を確認する必要があります．例えば，写像では 1 つの元が 1 つの元に写ることの確認も well defined に相当します．本講義では，準同型写像の定義，準同形定理などを学びます．群 G が g で生成されるとき，つまり，$G = \langle g\rangle$ であるとき，G 上の準同形写像 ϕ は　g の行き先　$\phi(g)$ を決めると決定できます．生成元は群の構造を決めるとともに，写像の定義とも関係します．今年も有限群の母と呼ばれる置換群に注目してます．置換群にも慣れてみましょう．

問 3.1. $1 \leq n$ を正整数とし，ζ_n を 1 の原始 n 乗根 *(*n 乗して初めて 1 になる数*)* とする．$G_4 = \langle\zeta_4\rangle$，$H_8 = U(\mathbb{Z}/8\mathbb{Z}) = \{\mathbb{Z}/8\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/8\mathbb{Z}\}$，及び *4*次の置換群　$S_4 = \left\{\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}\right\}$ を考える．H_8 の演算は乗算を考える．この時，以下の問に答えよ．

1. H_8 の位数を求めて，生成元の集合を *1*組求めよ．
2. 単射準同型写像 $\phi_1 : H_8 \longrightarrow S_4$ を構築せよ．
3. ϕ_1 が単射準同型写像になることを示せ．
4. G_4 の位数を求めて，生成元の集合を *1*組求めよ．
5. 単射準同型写像 $\phi_2 : G_4 \longrightarrow S_4$ を構築せよ．
6. ϕ_2 が単射準同型写像になることを示せ．

問 3.2. † $H_{16} = U(\mathbb{Z}/16\mathbb{Z}) = \{\mathbb{Z}/16\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/16\mathbb{Z}\}$，を考える．$H_{16}$ の演算は乗算を考える．$G = H_{16}$，G から G への自己準同形写像からなる集合を $End(G) = \{\phi : G \longrightarrow G$ 準同形写像 $\}$ とする．このとき以下の問に答えよ．

(1) G から G への写像 ϕ で　$Ker(\phi) = \langle 3\rangle = \{1,3,9,11\}$ となる準同型写像を構成せよ．

(2) (1) の写像 ϕ の像 $Im(\phi)$ を求めよ．

(3) $End(G) \ni \phi$ で恒等写像とは異なる全単射写像 ϕ を一つ求めよ．ここで，恒等写像 $\phi : G \longrightarrow G$ とは $\phi(a) = a \quad (\forall a \in G)$ となる写像である．

問 3.3. 整数環 $\mathbb{Z}$ に対して，その直積集合に対して，*2*種類の演算を考える．$\mathbb{Z}\times\mathbb{Z} = \{(h,k) | h \in \mathbb{Z}, k \in \mathbb{Z}\}$ には自然な直積演算を考える．つまり，$\mathbb{Z} \times \mathbb{Z} \ni (h_1,k_1),(h_2,k_2)$ に対し，

$$(h_1,k_1) + (h_2,k_2) \quad \leftarrow \quad (h_1 + h_2, k_1 + k_2) \text{ 成分毎の和.}$$
$$(h_1,k_1) \cdot (h_2,k_2) \quad \leftarrow \quad (h_1 \cdot h_2, k_1 \cdot k_2) \text{ 成分毎の積.}$$

一方，$A = \{(a,b) : \mathbb{Z} \ni a, b\}$ に対して，乗法，加法を以下で定義する．

$$\begin{aligned}(a,b)+(c,d) &\leftarrow (a+c, b+d)\\ (a,b)\cdot(c,d) &\leftarrow (ac, ad+bc)\end{aligned}$$

このとき以下の問に答えよ．

(1) $\mathbb{Z}\times\mathbb{Z}$ の零因子をすべて求めよ．

(2) A の零因子をすべて求めよ．

(3) $\mathbb{Z}\times 3\mathbb{Z}$ は $\mathbb{Z}\times\mathbb{Z}$ のイデアルになることを示せ．

(4) $\mathbb{Z}\times 3\mathbb{Z}$ は A のイデアルにならないことを示せ．

4　イデアル，剰余環，体

一つの事象を Global に考える，あるいは， Local に考えることは整数論では頻繁に行います．Global に成り立つ事実は Local でも成り立ちます．逆に Global でわからないことを Local で検証し，Global の結果に持ち上げます．Local の場合，元の個数が小さいので検証が容易だからです．準同形写像はローカルとグローバルの変換を可能にします．ここでは特に $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ を用います．準同形写像は不要な元の性質を落とすことにも利用できます．多項式が既約，可約であるという概念も演習で学習します．

問 4.1. 多項式環を考える．

$$\begin{aligned}\mathbb{Z}[X] &= \{f(X) = \sum a_i X^i | a_i \in \mathbb{Z}\}\\ \mathbb{Z}/p\mathbb{Z}[X] &= \{g(X) = \sum b_i X^i | b_i \in \mathbb{Z}/p\mathbb{Z}\}\end{aligned}$$

$\mathbb{Z}[X] \ni f(X)$ が $\mathbb{Z}$ 上で可約とは，$\mathbb{Z}[X] \ni g(X)$ の次数を $deg(g(X))$ とするとき，

$$f(X) = g(X)\cdot h(X)\ (1 \le deg(g(X)) < deg(f(X)), h(X) \in \mathbb{Z}[X])$$

を満たす $g(X)$ が存在することである．$f(X)$ が可約でないとき，既約という．

素数 p に対して，*2* つの多項式環の写像を以下で定義する．

$$\begin{aligned}\pi_p : \mathbb{Z}[X] &\longrightarrow \mathbb{Z}/p\mathbb{Z}[X]\\ \sum a_i X^i &\longmapsto \sum a_i \pmod p X^i\end{aligned}$$

この時，以下の問に答えよ．

(1) $\mathbb{Z}[X]$ から $\mathbb{Z}/p\mathbb{Z}[X]$ への写像が環準同型写像になることを示せ．

$$\pi_p\colon \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$$

$$f(X) = \sum a_i X^i \longmapsto f(X) = \sum a_i \pmod p X^i$$

(2) $f(x) = x^4 + x^3 + 1$ が $\mathbb{Z}/3\mathbb{Z}$ 上で可約であることを示せ．

(3) $f(x) = x^4 + x^3 + 1$ が既約になる剰余環 $\mathbb{Z}/p\mathbb{Z}$ で最小の p を求めよ．

(4) *(3)* を用いて $f(x)$ が $\mathbb{Z}$ 上既約となることを示せ．

問 4.2. † 剰余環 $\mathbb{Z}/16\mathbb{Z}$ とその正則元からなる群 $G = U(\mathbb{Z}/16\mathbb{Z})$ 上の自己準同形写像からなる集合を考える．

$$End(G) = \{f : \quad G \quad \longrightarrow \quad G\}$$

この時，以下の問に答えよ．

1. $End(G)$ が写像の乗法 $f\circ g$ においてモノイドになることを証明せよ．

$$\begin{aligned}f\circ g : \quad G &\longrightarrow G\\ f\circ g(x) &\longmapsto f(g(x))\end{aligned}$$

2. $U(\mathbb{Z}/16\mathbb{Z})$ の生成元を $\langle a, b\rangle$ 求めよ．ただし，a の位数は b の位数以上とする．
3. $|Im(f)|$ が最大になる恒等写像とは異なる準同型写像 $f \in End(G)$ を構築し，準同型であることを示せ．恒等写像とは $f(x) = x\ (\forall x \in G)$ である．
4. 位数 2 となる写像 $f \in End(G)$ で上の課題で構成した写像とは異なる写像を構成せよ．また f が準同型になること，さらに位数が 2 となることを示せ．

5 素数，合成数

$\mathbb{Z}$ で証明した定理の多くが多項式環 $\mathbb{Q}[X]$ についても成り立ちます．素数，合成数という概念は既約多項式，可約多項式という概念になり，素因数分解は規約多項式の分解に対応します．整数環で成り立つ定理を多項式環 $\mathbb{Q}[X]$ に置き直すことを演習では学習します．置き換えに必要な概念が多項式の次数 $\deg(f(X))$ です．次数も整数の上への写像と考えることができます．ここで $\mathbb{Q}[X] \setminus \{0\} \ni f(X) = a_nX^n + \cdots a_1X + a_0 (\mathbb{Q} \ni a_i, a_n \neq 0)$ に対して，$\deg(f(X)) = n$ とし，$f(X) = 0$ に対して，$\deg(f(X)) = -\infty$ とする．写像の位数とは $\phi^n = \mathrm{id}$ となる最小の正整数あるいは ∞ です．また群 G の生成元の個数が 2 個とは $G = \langle a_1, a_2\rangle$ となるが，任意の $a \ni G$ に対して，$G \neq \langle a\rangle$ であることを言います．準同形写像の構築は全ての生成元の行き先を決定するとできます．整数環で構築する剰余環の元の位数は乗算で考えます．

問 5.1. 正整数 n に対して，$H_n = U(\mathbb{Z}/n\mathbb{Z}) = \{\mathbb{Z}/n\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/n\mathbb{Z}\}$ を考える．この時，$8 < n$ で生成元の個数が 4 となる最小の n を求めよ．ここで生成元の個数が 4 とは $G = \langle a_1, a_2, a_3, a_4\rangle$ となるが，任意の $a_1, a_2 \ni G$ に対して，$G \neq \langle a_1\rangle$ かつ $G \neq \langle a_1, a_2\rangle$ かつ $G \neq \langle a_1, a_2, a_3\rangle$ であることを言う．また，求め方を記載せよ．

問 5.2. † 整数 $\mathbb{Z}$ に $\sqrt{-2}$ を付加した環　$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b, \in \mathbb{Z}\}$ にも整数環と同じ性質が成り立つ．なお，$\mathbb{Z}[\sqrt{-2}]$ における乗法と加法は自然な乗法と加法を考える．$\mathbb{Z}[\sqrt{-2}]$ から $\mathbb{N} \cup \{0\}$ への写像を

$$\begin{array}{rcl} \phi : \mathbb{Z}[\sqrt{-2}] & \longrightarrow & \mathbb{N} \cup \{0\} \\ a + b\sqrt{-2} & \longmapsto & a^2 + 2b^2 \end{array}$$

このとき，$\sqrt{-2}$ 上でも除法の原理と同様の原理が成り立つことを証明せよ．つまり，$\mathbb{Z}[\sqrt{-2}] \ni a + b\sqrt{-2}, c + d\sqrt{-2} \neq 0$ に対して，

$$\begin{array}{rcl} a + b\sqrt{-2} & = & (c + d\sqrt{-2}) \cdot (e + f\sqrt{-2}) + g + h\sqrt{-2} \\ 0 & \leq & \phi(g + h\sqrt{-2}) < \phi(c + d\sqrt{-2}) \end{array}$$

となる $\mathbb{Z}[\sqrt{-2}] \ni (e + f\sqrt{-2}), (g + h\sqrt{-2})$ が存在する．

問 5.3. 有限体　$\mathbb{F}_p$ 上の多項式環　$\mathbb{F}_p[X] = \{f(X) = \sum a_iX^i \mid a_i \in \mathbb{F}_p\}$ と $\mathbb{F}_p[X]$ から $\mathbb{F}_p[X]$ への写像 ϕ に対して，以下の問いに答えよ．

$$\begin{array}{rcl} \phi : \mathbb{F}_p[X] & \longrightarrow & \mathbb{F}_p[X] \\ f(X) = \sum a_iX^i & \longmapsto & (f(X))^p = \left(\sum a_iX^i\right)^p \end{array}$$

1. $f(X) = \sum a_iX^i$ に対して，$\phi(f(X))$ の各係数を明示的に記載せよ．$(\phi(f(X)) = \sum b_iX^i$ のような記載を行う．$)$
2. ϕ が多項式環上の加法と乗法に関して準同形になることを示せ．
3. ϕ に関して，$\{f(X) \in \mathbb{F}_p[X] \mid \phi((f(X))) = 1\}$ となる $\mathbb{F}_p[X]$ の部分群を求めよ．

問 5.4. 除法の原理で最大公約数を求めたが，除法の原理では，毎回のステップで除算が発生する．除算は非常に重いため，減算と偶数の場合，2 で割れる因子部分を削除する（2 の除算）で求める方法がある．

- *(G0)* $a = 2^ta'$,$b = 2^sb'$ $(a', b'$ はともに奇数$)$ とし，$t \leq s$ とするとき，$GCD(a, b) = 2^t\,GCD(a', b')$
- *(G1)* $GCD(a, b) = GCD(a - b, b)(a > b)$

($G0$) から，最大公約数の偶数部分は最初に決定できるので，a', b' の最大公約数を求めれば，全体の最大公約数が決定する．簡単のため，このとき，奇数 $a_i = b'$，$a_{i-1} = a'(a_i > a_{i-1})$ とする．このとき，以下が成り立つことを証明せよ．

1. $a_{i+1} = a_i - a_{i-1}$ とするとき，a_{i+1} は偶数である．
2. $a_{i+1} = a'_{i+1}2^t$ (a'_{i+1} は奇数とするとき，$GCD(a_i, a_{i-1}) = GCD(a'_{i+1}, a_{i-1})$.

問 5.5. †　整数 $\mathbb{Z}$ に対して，2 行 2 列の行列 $M_2(\mathbb{Z})$ の部分集合である正則行列からなる群とその部分集合，さらに $GL_2(\mathbb{Z})$ から有理数環 $\mathbb{Z}$ の単数群への写像を考える．

$$
\begin{aligned}
GL_2(\mathbb{Z}) &= \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}, det(A) = ad - bc = \pm 1 \right\} \\
SL_2(\mathbb{Z}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}, det(A) = 1 \right\} \\
det : GL_2(\mathbb{Z}) &\longrightarrow \mathbb{Z}^* \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto ad - bc
\end{aligned}
$$

このとき $SL_2(\mathbb{Z})$ が $GL_2(\mathbb{Z})$ の正規部分群になることを以下のステップで示せ．

1. det が乗法に関して準同型になることを示せ．
2. det が全射になることを示せ．
3. det の核 Ker を求めよ．
4. $SL_2(\mathbb{Z})$ が $GL_2(\mathbb{Z})$ の正規部分群になることを示せ．

6　不定方程式，合同式，中国人の剰余定理

Lagrange の定理，剰余群，位数，中国人の剰余定理などの考え方を学習します．中国人の剰余定理は，中国の算術書『孫子算経』に「3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 2 余る数は何か」と書かれていたことが由来です．105 の余りを求めるのは大変なので，3，5，7 の余りを求めて，105 で割ったあまりを求めたそうです．一般的な数学の理論を実学に応用することを学ぶことも本講義の目的です．ここでは中国人の剰余定理の重要さを実感してもらうために手計算で可能な値を利用しています．通常，べき乗演算 a^k の計算は，教科書の 13 章に記載されたバイナリ法利用しますが，本課題では，計算量が法と位数でどのように変わるのかを考えますので，k を 2 進展開で考えなくてよいです．

問 6.1. $G = U(\mathbb{Z}/n\mathbb{Z}) = \{\mathbb{Z}/n\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/n\mathbb{Z})\}$ とし，$1 < n \leq 20$ において考える．この時，以下の問に答えよ．

(1) G の部分群の個数が 4 個になる最小の n を求めよ．さらに，その部分群と生成元を全て挙げよ．

(2) G の部分群の個数が 3 個になる時の n の条件の一つを一般的に求めよ．

(3) G が 2 つの元で生成される最大の n を求めよ．G が 2 つの元で生成される n の条件の一つを一般的に求めよ．(あるいはならない一般的な条件を考えてみよう．)

問 6.2. 2^{13} の計算を中国人の剰余定理を応用して，次のステップに沿って求めよ．

1. 2^{13} より大きな合成数 m として，$m = 32 * 25 * 11$ を選ぶ．$p_1 = 32$, $p_2 = 25$, $p_3 = 11$ とする．次に，$2^{13} \pmod{p_i}$ $(i = 1, 2, 3)$ を求める．
2. 拡張 ECD から不定方程式を解く．$(i, j, k \in \{1, 2, 3\})$

$$x_i p_i + y_{j,k} p_j p_k = 1$$

3. 上述の結果を用いて，$i, j, k \in \{1, 2, 3\}$ に対して

$$s_i \equiv 1 \pmod{p_i}, s_i \equiv 0 \pmod{p_j p_k},$$

$2^{13} \pmod{p_1 * p_2 * p_3}$ をもとめる．

4. 上述の結果を用いて，$X \equiv 2^{13} \pmod{p_1 * p_2 * p_3}$ をもとめる．
5. $2^{13} < m$ を用いて， 2^{13} を出力する．

問 6.3. † $X \equiv 293^{13} \pmod{4536}$ の解法に中国人の剰余定理を用いることを考える．$4536 = 2^3 \times 3^4 \times 7$ より，利用できる法は複数ある．どのような法による分解が計算量削減につながるか考えたい．そこで，$X \equiv 293^{13} \pmod{4536}$ の計算量が少なくなる解法の方針を次のステップで求めよう．

1. *4536* を互いに素な同程度の大きさの二つの数 p_1, q_1 *(*$p_1 \approx q_1$*)* にわけて，求める．
2. *4536* を互いに素な大きさの異なる二つの数 p_2,q_2 *(*$p_1 \ll q_1$*)* にわけて，求める．
3. *4536* を互いに素な上記と異なる三つの数 p_3,q_3,r_3 にわけて，求める．
4. *3*つのケースを議論し，分割により計算量が変わる場合，計算量が少なくなる分割の方針を考えてみよう．