産学官連携・育成講座
『暗号のための数学』
ワークブック

兵庫県立大学・応用情報科学研究科
教授・申　吉浩

平成 26 年度

編纂方針

- 衒学的にならない。難しいことを易しく教える。
- 網羅的に教えるよりも、適切なトピックを選んで、数学を理解するこつ・面白さを体験してもらう。
- 詳細より目的を教える。何故必要なのか、何の役に立つのか、これが一番重要。詳細は誰でも忘れてしまうし、必要な時思い出せればばよい。
- キーワードを繰り返す。キーワードが耳になじめば、トラウマはなくなる。キーワードが分かれば、詳細は必要な時に調べることができる。
- 自分で計算してもらう。手を動かさないと、本当の理解は得られない。

Contents

1　法で遊ぼう！　4

2　群　28

3　離散対数問題　35

4　素数と RSA 暗号　41

1　法で遊ぼう！

- 記号 $a, b, c, d, x, y, \alpha, \beta$ 等の記号は全て整数を表し、必要がない限り特にことわらない。
- a が b を割り切る時、$a \mid b$ と表す。例えば、$2 \mid 6, 3 \mid 6$ が成り立つ。
- a と b の最大公約数を (a, b) と表す。例えば、$(12, 30) = 6$ である。
- $(a, b) = 1$ が成り立つ時、a と b は互いに素であるという。
- $\mathbb{Z}$ は整数（正も負も）全体の集合、$\mathbb{N}$ は正の整数全体の集合を表す。すなわち、

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$
$$\mathbb{N} = \{1, 2, 3, \dots\}$$

定義 1.1. x を n で割った余りを $x \bmod n$ と表す。

問 1.1. $(x+y) \bmod 6$ 及び $xy \bmod 6$ の計算表を完成させよ。

$(x+y) \bmod 6$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	
2	2					
3	3					
4	4					
5	5					

$xy \bmod 6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4			
3	0					
4	0					
5	0					

定義 1.2. (n を法とした合同)
x と y をそれぞれ n で割った余りは等しい。

$$x \equiv y \bmod n$$

問 1.2. 以下の数を 15 を法とする合同関係で仕分けせよ。

$$37, 45, 19, 78, 81, 30, 94, 22, 94, 33, 48$$

命題 1.3. $a \equiv b \bmod n$ が成り立つことと、適切な c に対して $a = b + cn$ が成り立つことは同値である。

問 1.3. 以下の問いに答えよ。

1. $34 \equiv 92 \bmod 29$ を確かめよ。
2. $a = 34, b = 92$ とする時、$a = b + 29c$ となる c を求めよ。
3. $a = 34, b = 93$ とする時、$a = b + 29c$ となる c は存在しないことを示せ。

命題 1.4. $a \equiv a' \bmod n$、$b \equiv b' \bmod n$ とする時、

$a + b \equiv a' + b' \bmod n$　及び　$ab \equiv a'b' \bmod n$

が成り立つ。

問 1.4. 各問いに答えよ。

1. 空欄をうめよ。

   519 を 7 で割った余りは$\square_1$、131 を 7 で割った余りは$\square_2$、519 + 131 =$\square_3$、それを 7 で割った余りは$\square_4$、519 × 131 =$\square_5$、それを 7 で割った余りは$\square_6$ となる。

   一方、$\square_1 + \square_2$ を 7 で割った余りは$\square_7$、$\square_1 \times \square_2$ を 7 で割った余りは$\square_8$ となる。

2. $((192 + 354) \times 552 \times 793) \bmod 5$ を求めよ。

3. $(99!) \bmod 5$ を求めよ。

1.5. $a = d_n d_{n-1} \ldots d_2 d_1 d_0$ を、10^i の桁の数字が d_i である $n+1$ 桁の十進数とする。例えば、$a = 123$ なら $d_2 = 1, d_1 = 2, d_0 = 3$。
a が3で割り切れることと、$d_n + d_{n-1} + \cdots + d_1 + d_0$ が3で割り切れることとは同値である。実際、

$$a = 10^n d_n + 10^{n-1} d_{n-1} + \cdots + 10^1 d_1 + 10^0 d_0$$

と $10 \bmod 3 = 1$ が成り立つので、下式を得る。

$$a \equiv 1^n d_n + 1^{n-1} d_{n-1} + \cdots + 1^1 d_1 + 1^0 d_0 \bmod 3$$

問 1.5. 以下の問いに答えよ。

1. $a = d_n d_{n-1} \ldots d_2 d_1 d_0$ が9の倍数となるための条件を求めよ。
2. $a = d_n d_{n-1} \ldots d_2 d_1 d_0$ が11の倍数となるための条件を求めよ。

定義 1.6. $ab \equiv ba \equiv 1 \bmod n$ を満たす b が存在する時、a を**法 n に関する可逆元**とよび、b を a の**法 n に関する逆元**と呼ぶ。

問 1.6. 下表は $xy \mod 15$ を与える。法 15 における可逆元を全て求めよ。また、可逆元それぞれについて、その逆元を求めよ。

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	1

定義 1.7. $\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}$ とする。

$\mathbb{Z}/(n)^\times = \{x \in \mathbb{Z}/(n) \mid x$ は法 n に関して可逆$\}$

を $\mathbb{Z}/(n)$ の**乗法群**と呼ぶ。

定理 1.8.

$$\mathbb{Z}/(n)^\times = \{x \in \mathbb{Z}/(n) \mid (x, n) = 1\}$$

定理 1.8 の理解を当面の目標とする。

問 1.7. 以下の問いに答えよ。

1. 問 1.6 で求めた可逆元は全て 15 と素であることを確かめよ。
2. 問 1.6 で可逆でないとされた元 x について、$xy \bmod 15 = 0$ となる $y \in \mathbb{Z}/(15)$ が存在することを確かめよ。

定理 1.9. 以下の二つの集合は一致する。

$$\{ma + nb \mid m, n \in \mathbb{Z}\} = \{n(a, b) \mid n \in \mathbb{Z}\}$$

特に、$\alpha a + \beta b = (a, b)$ を満たす α, β が存在する。

問 1.8. $a = 221, b = 119$ とし、$221\alpha + 119\beta$ を $\alpha = -4, -3, -2, -1, 0, 1, 2, 3, 4$（列）及び $\beta = -4, -3, -2, -1, 0, 1, 2, 3, 4$（行）に対して計算した。以下の問いに答えよ。

1. 最小の正の値 d を探せ。
2. ランダムに 5 個の値を選び、d の倍数になっていることを確かめよ。
3. $a = 221$ と $b = 119$ が表中に現れることから、d が 221 と 119 の約数であることを示せ。

	-4	-3	-2	-1	0	1	2	3	4
-4	-1360	-1139	-918	-697	-476	-255	-34	187	408
-3	-1241	-1020	-799	-578	-357	-136	85	306	527
-2	-1122	-901	-680	-459	-238	-17	204	425	646
-1	-1003	-782	-561	-340	-119	102	323	544	765
0	-884	-663	-442	-221	0	221	442	663	884
1	-765	-544	-323	-102	119	340	561	782	1003
2	-646	-425	-204	17	238	459	680	901	1122
3	-527	-306	-85	136	357	578	799	1020	1241
4	-408	-187	34	255	476	697	918	1139	1360

補題 1.10. 以下は互いに同値である。

1. a は法 n に関して可逆元
2. $\alpha a \equiv 1 \bmod n$ となる α が存在
3. $(a, n) = 1$

アルゴリズム 1.11. ユークリッド互除法
入力： $a > b$
出力： (a, b)

1. $x = a, y = b$ とする。
2. x を y で割った余りを計算し z とする。
3. $z = 0$ なら y を出力して終わり。
4. $x = y, y = z$ と置き換えて、ステップ２以下を繰り返す。

アルゴリズム 1.12. 拡張ユークリッド互除法
入力： a, b
出力： $(a, b) = \alpha a + \beta b$

1. $x = 1 \cdot a + 0 \cdot b, y = 0 \cdot a + 1 \cdot b$ とする。
2. $x = \alpha a + \beta b$ を $y = \alpha' a + \beta' b$ で割った余りを $z = (\alpha - q\alpha')a + (\beta - q\beta')b$ とする。但し、q は x を y で割った時の商。
3. $z = 0$ なら $y = \alpha' a + \beta' b$ を出力して終わり
4. $x = \alpha' a + \beta' b, y = (\alpha - q\alpha')a + (\beta - \beta')b$ と置き直して、ステップ２以下を繰り返す。

補題 1.13. $a > b$とする。aをbで割った余りをrとする時、$\frac{a}{2} > r$が成り立つ。

命題 1.14. $a > b$とし、更に、bはnビットの数であるとする。拡張ユークリッド互除法は高々$2n$回の割り算を実行する。

1.15. 計算量

アルゴリズムの実行可能性を考える時、計算量が非常に重要である。計算量はアルゴリズムの実行に必要な『ビット演算』の回数で測る。

例えば、m ビットの数 a を n ビットの数 b で割って商と余りを計算するには、最大で $(m-n+1)n$ 回のビット演算を行う。この計算量のオーダーを $O((m-n+1)n)$ と表す。

問 1.9. $88 = 1001110_{(2)}$ を $6 = 110_{(2)}$ で割る計算を二進法で行う。以下を完成させよ。また、ビット演算の実行回数を数えよ。

$$
\begin{array}{cccccccc}
1 & 0 & 0 & 1 & 1 & 1 & 0 & \\
1 & 1 & 0 & & & & & \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & 0 & (0) \\
 & 1 & 1 & 0 & & & & \\
\hline
 & & 1 & 1 & 1 & 1 & 0 & (1) \\
 & & 1 & 1 & 0 & & &
\end{array}
$$

1.16. 多項式時間アルゴリズム
アルゴリズムへの入力のビット数をnとする時、アルゴリズムの計算量がnの多項式で抑えられるならば、**多項式時間アルゴリズム**という。
例えば、割り算の計算量は$O((m+n)^2)$で抑えられるため、多項式時間である。

問 1.10. 命題 1.14 の結果を用い、ユークリッド互除法は多項式アルゴリズムであることを示せ。特に、入力のビット数$m+n$（aとbのビット数の和）に対して、ユークリッド互助法の計算量は$m+n$の何乗で抑えられるか？

1.17. 計算の実行可能性
多項式時間アルゴリズムで計算可能であることは、しばしば、計算が実行可能であることと同一視される。また、「効率的に計算できる」ことは、「多項式時間で計算できる」ことを意味する。

1.18. 指数時間アルゴリズム
アルゴリズムへの入力のビット数nに対して、アルゴリズムの計算量が指数関数e^{cn}で評価できる時、**指数時間アルゴリズム**という。

1.19. 法nに関する逆元の計算
法nに関する可逆元aの逆元は、拡張ユークリッド互除法により効率的に計算できる。
$\alpha a \equiv 1 \bmod n$を満足する$\alpha$が逆元であるから、$\alpha a = 1 + \beta n$、即ち、$\alpha a + (-\beta)n = 1 = (a, n)$を満たす$\alpha$を計算する。

問 1.11. 法 16361 に関する 256 の可逆元を求めよ。

定義 1.20. $a^k \equiv 1 \bmod n$ となる最小の正の整数 k を**法 n に関する位数（いすう)** と呼ぶ。

問 1.12. 以下の問いに答えよ。

1. a が位数をもつならば、a は可逆元である。何故か？
2. 法 7 に対する可逆元全てに対して位数を求めよ。
3. $3^{100} \bmod 7$ を計算せよ。

1.21. $a^k \bmod n$ を**冪乗剰余**とよぶ。RSA 暗号などの実用では、十進法で 600 桁程度の巨大な n, k に対して $a^k \bmod n$ を計算する必要があり、単純な方法では実用的には計算不可能である。
実用的な時間で冪乗剰余を計算するためには、特別な工夫が必要である。

問 1.13. 京コンピュータは一秒間に 10^{16} 回の浮動小数点計算を実行する能力がある。めちゃ過大評価して、京コンピュータは一秒間に 10^{16} 回の 600 桁の割り算ができると仮定する。n, k が十進法で 600 桁の数である時、$a \bmod n, a^2 \bmod n, a^3 \bmod n, \ldots,$ を順次計算して $a^k \bmod n$ を求めるとすると、何年がかかるか、概算せよ。「1 年 $\approx 32 \times 10^6$ 秒」としてよい。

アルゴリズム 1.22. 露西亞農奴法
入力： a, k, n
出力： $a^k \bmod n$

1. k を二進数 $b_\ell b_{\ell-1} \ldots b_1 b_0$ に展開する。
2. $c_0 = a^{2^0} \bmod n, c_1 = a^{2^1} \bmod n, \ldots, c_{\ell-1} = a^{2^{\ell-1}} \bmod n, c_\ell = a^{2^\ell} \bmod n$ を全て計算し、記憶しておく。
3. $b_i = 1$ となる i についてのみ、c_i を全て掛け合わせて、答えを出力する。

問 1.14. $59^{97} \bmod 103$ を露西亞農奴法で計算せよ。

1.23. 露西亞農奴法の計算量

乗算剰余 $xy \bmod n$ の回数で測る。a の二進表現を $b_\ell b_{\ell-1} \ldots b_1 b_0$ として、$a^k \bmod n$ を計算する。

- c_{i+1} は c_i から一回の乗算剰余で計算できる。

  $$c_{i+1} = a^{2^{i+1}} \bmod n = \left(a^{2^i}\right)^2 \bmod n = {c_i}^2 \bmod n$$

  $\{c_0, c_1, \ldots, c_\ell\}$ の計算には ℓ 回の乗算剰余

- $b_i = 1$ となる i について c_i を掛け合わせる。

  $$a^k \equiv \prod_{b_i=1} c_i \bmod n$$

$a^k \bmod n$ の計算に必要な乗算剰余の回数は：

$$\ell + (b_i = 1 \text{の個数})$$

定理 1.24. 中国剰余定理
m, nは互いに素であるとする。以下が成り立つ。

1. $x, y \in \mathbb{Z}/(mn)$について、$x \equiv y \bmod m, x \equiv y \bmod n$が成り立つ時、$x = y$である。
2. 任意の$a \in \mathbb{Z}/(m), b \in \mathbb{Z}/(n)$に対して、$x \equiv a \bmod m, x \equiv b \bmod n$を満たす$x \in \mathbb{Z}/(mn)$が（一意に）存在する。

問 1.15. $\mathbb{Z}/(15)$の元$x = 0, 1, 2, \ldots, 14$を下表に割振れ。$x \bmod 3$で行を決め、$x \bmod 5$で列を決める。

	0	1	2	3	4
0	0				
1		1			
2			2		

問 1.16. $\mathbb{Z}/(24)$の元$x = 0, 1, 2, \ldots, 11$を下表に割振れ。$x \bmod 4$で行を決め、$x \bmod 6$で列を決める。

	0	1	2	3	4	5
0	0					
1		1				
2			2			
3				3		

1.25. RSA暗号では、互いに異なる素数p, qに対して$n = pq$を定める。$e = 2^{2^4} + 1$と、任意の平文（ひらぶん）$x \in \mathbb{Z}/(n)$に対して、

$$E(x) = x^e \bmod n$$

により暗号化の関数を定める。
一方、$E_p(x) = x^e \bmod p, E_q(x) = x^e \bmod q$は$E(x)$に比べて、それぞれ$2^3 = 8$倍程度早く計算できる。従って、$E_p(x)$と$E_q(x)$を計算してから、

$$y \equiv E_p(x) \bmod p$$
$$y \equiv E_q(x) \bmod p$$

を満たす$y \in \mathbb{Z}/(n)$を効率的に計算できれば、$E(x) = y$とすれば効率がよい。中国剰余定理により、このようなyは一意に存在する。

1.26. m, n を互いに素とする。
任意の $a \in \mathbb{Z}/(m), b \in \mathbb{Z}/(n)$ に対して、

$$x \equiv a \bmod m \tag{1}$$
$$x \equiv b \bmod n \tag{2}$$

を満たす $x \in \mathbb{Z}/(mn)$ を以下のように計算する。
(1) より $x = my + a$ として、(2) に代入すると、$my + a \equiv b \bmod n$ を得る。m は法 n で可逆なので、$m'm \equiv 1 \bmod n$ なる逆元 $m' \in \mathbb{Z}/(n)$ が存在する。y は以下のように求められる。

$$y \equiv (m'm)y \equiv m'(my) \equiv m'(b - a) \bmod n$$

問 1.17. $x \equiv 4 \bmod 3, x \equiv 9 \bmod 5$ を満足する $x \in \mathbb{Z}/(6)$ を求めよ。

2　群

2.1. 動機付け
群は演算の抽象化である。
p を素数としよう。$px \equiv 0 \bmod p$ が成り立つことを示すのは難しくない。一方、$x^{p-1} \equiv 1 \bmod p$ が成り立つことはFermat（フェルマー）の定理として知られており、証明は自明ではない。
しかし、群の立場からは、どちらの性質もLagrange（ラグランジュ）の定理から導くことができる。
Fermatの定理はRSA暗号の基礎であり、ElGamal暗号やDSA署名は群の上に抽象的に定義されていて、適切な群を選ぶ自由度がある点がメリットである。

定義 2.2. Gを集合、$\bullet$をGの上で定義された (二項) 演算とする。即ち、任意のペア$(x, y) \in G \times G$に対して、$x \bullet y \in G$が定まる。
以下の条件を満足する時、$(G, \bullet)$を**群**と呼ぶ。

1. 任意の$x, y, z \in G$に対して、$(x \bullet y) \bullet z = x \bullet (y \bullet z)$が成り立つ。
2. $e \in G$が存在して、任意の$x \in G$に対して、$a \bullet e = e \bullet a = a$が成り立つ。
3. 任意の$x \in G$に対して$x' \in G$が存在して、$x \bullet x' = x' \bullet x = e$が成り立つ。

問 2.1. 以下を確かめよ。

1. $\mathbb{Z}/(n)$上で、$x + y = (x + y) \bmod n$と定める。$(\mathbb{Z}/(n), +)$は群である。
2. $\mathbb{Z}/(n)^\times$上で、$x \times y = (xy) \bmod n$と定める。$(\mathbb{Z}/(n)^\times, \times)$は群である。

定義 2.3. $(G, \bullet)$ を群とする。$x \in G$ について、$x^n = \underbrace{x \bullet \cdots \bullet x}_{n} = e$ を満たす最小の正の整数を x の**位数（いすう）**と呼び、$|x|$ で表す。

2.4. $x \in G$ は必ず位数を持つとは限らないが (全ての $n \in \mathbb{N}$ に対して $x^n \neq e$)、G が有限集合なら必ず位数をもつ。

定義 2.5. G が有限集合の時、$(G, \bullet)$ を**有限群**と呼ぶ。G の元の個数を G の**位数**と呼び、$|G|$ で表す。

定義 2.6. $x \in G$ の位数を n とする。$G_x = \{x, x^2, x^3, \ldots, x^n\}$ とする時、$(G_x, \bullet)$ は群となる。$(G_x, \bullet)$ を $\boldsymbol{x}$ **が生成する巡回部分群**と呼ぶ。

問 2.2. $(\mathbb{Z}/(21)^\times, \times)$ において 16 が生成する巡回部分群 H の元を求めよ。

定理 2.7. *Lagrange* の定理
$(G, \bullet)$ を有限群とする。任意の $x \in G$ に対して、
x の位数 $|x|$ は G の位数 $|G|$ の約数である。

問 2.3. $(\mathbb{Z}/(21)^{\times}, \times)$ において 16 が生成する巡回部分群を H とする。$x \in \mathbb{Z}/(21)^{\times}$ に対して、$x \times H = \{x \times y \mid y \in H\}$ とする。以下の問いに答えよ。

1. 下表では $1 \times H$ と $2 \times H$ の元に印をつけてみた。同様に、残りの $x \in \mathbb{Z}/(21)^{\times}$ について、$x \times H$ の元に印をつけよ。
2. 結果は 16 の位数が G の位数を割り切ることを示している。何故か？

	1	2	4	5	8	10	11	13	16	17	19	20
1	√		√						√			
2		√			√		√					
4												
5												
8												
10												
11												
13												
16												
17												
19												
20												

定理 2.8. *Fermat* の定理
p を素数とする。任意の $x \in \mathbb{Z}/(p)^{\times}$ に対して、
$x^{p-1} \equiv 1 \bmod p$ が成り立つ。

問 2.4. 以下の問いに答えよ。

1. $\mathbb{Z}/(5)^{\times}$ の各元の位数を求めよ。
2. 問 1.12 の結果も合わせ、$\mathbb{Z}/(5)^{\times}, \mathbb{Z}/(7)^{\times}$ の両方とも $\times$ に関して巡回群であることを確かめよ。

定理 2.9. 原始根定理
p を素数とする。$(\mathbb{Z}/(p)^{\times}, \times)$ は巡回群である。

定義 2.10. 位数が $p-1$ の元 $x \in \mathbb{Z}/(p)^{\times}$ を、**法 p に関する原始根**と呼ぶ。

定理 2.11. p, q を相異なる素数とする。任意の $x \in \mathbb{Z}/(pq)^\times$ に対して、$x^{\mathrm{lcm}(p-1,q-1)} \equiv 1 \bmod pq$ が成り立つ。

$\mathrm{lcm}(p-1, q-1)$ は $p-1$ と $q-1$ の最小公倍数。

問 2.5. $\mathbb{Z}/(35)^\times$ の各元 x の位数を調べる。列は $x \bmod 7$、行は $x \bmod 5$ の値に対応し、括弧内の数字は $\mathbb{Z}/(7), \mathbb{Z}/(5)$ での位数を示す。

1. $\mathbb{Z}/(35)^\times$ の各元を表中に割り振り、括弧内に $\mathbb{Z}/(35)^\times$ での位数を記せ。
2. x の $\mathbb{Z}/(35)$ 中の位数、$x \bmod 7$ の $\mathbb{Z}/(7)$ 中の位数、$x \bmod 5$ の $\mathbb{Z}/(5)$ 中の位数の間の関係について述べよ。

	1 (1)	2 (3)	3 (6)	4 (3)	5 (6)	6 (2)
1 (1)	1 (1)	( )	( )	( )	( )	6 ( )
2 (4)	( )	2 ( )	( )	( )	( )	( )
3 (4)	( )	( )	3 ( )	( )	( )	( )
4 (2)	( )	( )	( )	4 ( )	( )	34 (2)

3　離散対数問題

3.1. この節では、$(G, \bullet)$ を巡回群、$g \in G$ を生成元とする。即ち、g の位数 n に対して、$G = \{g, g^2, \ldots, g^n\}$ が成り立つものとする。

定義 3.2.　$y \in G$ が与えられて、

$$y = g^x = \underbrace{g \bullet \cdots \bullet g}_{x\text{回}}$$

を満足する $x \in \mathbb{N}$ を求める問題を**離散対数問題**という。

3.3. 実数 $g > 0, y > 0$ に対して、$y = g^x$ の実数解 x を求める問題は、$x = \log_g y = \frac{\log y}{\log g}$ とすることで、容易に解くことができる。解 x は関数電卓などで簡単に計算できる。これは、対数関数のテーラー展開から、

$$\log x = 2\left(\frac{x-1}{x+1} + \frac{1}{3}\left(\frac{x-1}{x+1}\right)^3 + \cdots + \frac{1}{2n+1}\left(\frac{x-1}{x+1}\right)^{2n+1} + \cdots\right)$$

が与えられているからである。$\left|\frac{x-1}{x+1}\right| < 1$ が成り立ち、上記の数列の無限和は収束する。計算機で計算する場合は、項の値が十分小さくなったところで計算を止めればよい。

3.4. 有限群Gの上の離散対数問題を効率的に解くことができるか否かは、Gに依存する。

問 3.1. nを自然数とし、以下の問に答えよ。

1. $g \in \mathbb{Z}/(n)$が$(\mathbb{Z}/(n), +)$の生成元となるための条件を求めよ。
2. gを$(\mathbb{Z}/(n), +)$の生成元とし、離散対数問題$y \equiv gx \bmod n$を解け。
3. $5 \in \mathbb{Z}/(13)$は$(\mathbb{Z}/(13), +)$の生成元である。離散対数問題$10 \equiv 5x \bmod 13$を解け。

3.5. 以下の有限群Gに対しては、離散対数問題を解くことは困難であると考えられており、暗号のベースに利用される。

- 素数pを法とする乗法群$(\mathbb{Z}/(p)^{\times}, \times)$
- 有限体$\mathbb{F}_{p^m}$上の楕円曲線

問 3.2. 以下の問に答えよ。

1. $2 \in \mathbb{Z}/(13)^{\times}$が$(\mathbb{Z}/(n)^{\times}, \times)$の生成元であることを確かめよ。
2. 離散対数問題$7 \equiv 2^x \bmod 13$を解け。

3.6. Diffie-Hellman 鍵交換

以下の手順で、Alice と Bob の間で秘密裏に鍵を交換する。有限巡回群 $(G, \bullet)$ と生成元 $g \in G$ は公開情報である。

1. Alice は乱数 $\alpha \in \mathbb{N}$ を生成し、$a = g^\alpha \in G$ を Bob に送る。
2. Bob は乱数 $\beta \in \mathbb{N}$ を生成し、$b = g^\beta \in G$ を Alice に送る。
3. Alice は $K = b^\alpha$ により、Bob は $K = a^\beta$ により、鍵 K を計算し、共有する。

$$b^\alpha = (g^\beta)^\alpha = g^{\alpha\beta} = (g^\alpha)^\beta = a^\beta$$

が成り立つので、Alice と Bob が計算する鍵 K は一致する。

一方、a と b は通信路上に現れる。もし、盗聴者が a から α を計算できれば、$K = b^\alpha$ を計算して鍵を得ることができてしまう。しかし、a から α を計算することは、$(G, \bullet)$ の離散対数問題を解くことにほかならないので、離散対数問題を解くことは困難であると仮定できれば、この攻撃は無効である。

3.7. 離散対数問題を解くアルゴリズム
任意の群の上で離散対数問題を解く万能のアルゴリズムとして、Pohlig-Hellmanアルゴリズムが知られているが、指数時間アルゴリズムである。

乗法群 $(\mathbb{Z}/(p)^{\times}, \times)$**：** 数体篩（ふるい）法によるアルゴリズムが現時点では最速であり、準指数時間アルゴリズムである。Pohlig-Hellmanアルゴリズムより高速であるが、大きなpに対しては実用的ではない。

その他の群： Pohlig-Hellmanアルゴリズムの他に離散対数問題を解くアルゴリズムは知られていない。

4　素数と RSA 暗号

4.1. RSA 暗号

秘密情報（秘密鍵）： p, q, d

p, q：互いに異なる素数

d：$ed \equiv 1 \bmod \mathrm{lcm}(p-1, q-1)$

公開情報（公開鍵）： n, e

n：$n = pq$

e：$(e, \mathrm{lcm}(p-1, q-1)) = 1$

暗号化関数： $E(x) = x^e \bmod n$

復号関数： $D(x) = x^d \bmod n$

4.2. p, q, e, d の生成法

p, q： 1000〜2000 ビット（十進表現で 300〜600 桁）の素数をランダムに生成。

e： Ferumat 素数 $2^{2^4}+1$ とすることが普通。暗号化関数 $E(x)$ の高速化が目的（1.23 参照）。

d： $ed \equiv 1 \bmod \mathrm{lcm}(p-1, q-1)$ を満足するよう拡張 Euclid 互除法（1.12 参照）を用いて計算（1.19 参照）。

問 4.1. $p = 11, q = 13$ の時、$e = 7$ と決めたとする。d を求めよ。

命題 4.3. $E(x)$ と $D(x)$ は互いに逆関数である。

4.4. 平文（ひらぶん）x を暗号化した暗号文は $E(x)$ であり、暗号文に復号関数を施すと平文 x に戻る。従って、

$$\begin{aligned} D(E(x)) &= (x^e \bmod n)^d \bmod n \\ &\equiv x^{ed} \bmod n \equiv x \bmod n \end{aligned}$$

が成り立つ必要がある。
$ed \equiv 1 \bmod \mathrm{lcm}(p-1, q-1)$ なので、命題 1.3 より、$ed = Q \cdot \mathrm{lcm}(p-1, q-1) + 1$ である。

$$\begin{aligned} x^{ed} &\equiv x^{Q\mathrm{lcm}(p-1,q-1)+1} \\ &\equiv \left(x^{\mathrm{lcm}(p-1,q-1)}\right)^Q \cdot x \bmod n \end{aligned}$$

定理 2.11 より、$x^{\mathrm{lcm}(p-1,q-1)} \equiv 1 \bmod n$ が成り立つので、$x^{ed} \equiv x \bmod n$ を得る。

問 4.2. 問 4.1 の p, q, e, d を仮定して、平文 $x = 2$ の暗号文 $E(2)$、及び、その復号 $D(E(2))$ を求めよ。

定理 4.5. 次の *2* 条件は同値である。

1. n, e から d を計算する効率のよい（多項式時間）アルゴリズムがある。
2. n を素因数分解する効率のよい (多項式時間) アルゴリズムがある。

4.6. 2 のアルゴリズムがあれば、p, q を効率的に得ることができる。拡張Euclid互除法により、p, q から d を効率的に求めることができる (4.2)。

4.7. 1 のアルゴリズムがあれば、$\mathrm{lcm}(p-1, q-1) \mid (ed-1)$ を満足する d を効率的に計算できる。$ed - 1 = 2^k a$ を満たす $k \in \mathbb{N}$ と奇数 a を計算し、確率的アルゴリズム 4.8 により n を素因数分解できる。

アルゴリズム 4.8.
入力： n, k, a
出力： n の素因数

1. $x \in \mathbb{Z}/(n)$ をランダムに選ぶ。
2. $y_i = x^{2^i \cdot a} \bmod n \ (i = 0, \ldots, k-1)$ を計算。
3. $(y_i - 1, n) \neq 1, n$ なら、$(y_i - 1, n)$ を出力。
4. 全て $(y_i - 1, n) = 1, n$ なら、1 に戻る。

問 4.3. $n = 221, e = d = 7$ とする。以下の問いに答えよ。

1. $ed - 1$ を素因数分解せよ。
2. $x = 21$ に対して、$(y_i - 1, n)$ を計算せよ。
3. $x = 5$ に対して、$(y_i - 1, n)$ を計算せよ。
4. 221 の素因数 p, q を求めよ。
5. $x = 21, 5$ に対して $(y_i - 1, p)$ 及び $(y_i - 1, q)$ を計算せよ。

4.9. RSA 暗号では、n は公開情報だが、その素因数 p, q は秘密情報である。実際、p, q がわかれば、拡張 Euclid 互除法により、秘密鍵 d が計算できてしまう。
即ち、RSA 暗号を安全に利用するためには、異なるユーザの間では異なる p, q を用いなければならず、膨大な数の素数を重複なく、かつ、効率的に生成する手段が必要である。

命題 4.10. 素数は無限に存在する。

4.11. 最大の素数が存在すると仮定し、それをpと表してみる。
素数全体を$2 = p_1 < p_2 < \cdots < p_n = p$とする時、$p^{\#} = p_1 \cdot p_2 \cdots p_n + 1$は$p_i$では割り切れない。
従って、$p^{\#}$はpより大きな素因数をもつこととなり、pが最大の素数とした仮定と矛盾する。

問 4.4. $2 \cdot 3 \cdot 5 + 1$を素因数分解せよ。

4.12. 素数の公式

Mersenne（メルセンヌ）と Fermat は次の形の素数を研究した。

$$M(n) = 2^n - 1$$
$$F(n) = 2^n + 1$$

命題 4.13. $M(n)$ が素数ならば、n は素数である。

命題 4.14. $F(n)$ が素数ならば、$n = 2^k$ である。

4.15. 次の因数分解の公式が鍵となる。

$$x^2 - 1 = (x-1)(x+1)$$
$$x^{2n+1} - 1 = (x-1)(x^{2n} + \cdots + x^i + \cdots + 1)$$
$$x^{2n+1} + 1 = (x+1)(x^{2n} + \cdots + (-1)^i x^i + \cdots + 1)$$

問 4.5. 次の問いに答えよ。

1. $2^6 - 1$ を素因数分解せよ。
2. $2^6 + 1$ を素因数分解せよ。