整数の性質を証明するアルゴリズム

M2010MM046 安江彰悟
指導教員：佐々木克巳

1　はじめに

学習指導要領の改訂により, 2012 年度入学生から高等学校数学Aに選択分野として「整数の性質」が新たに追加された. 整数に関する問題はパターンが多く, 解法も様々である場合が多い. そのため, 整数に関する問題はかなり難しい.

だが, 最大公約数に関する等式・不等式を証明する問題については, その証明法をある程度限定することができる. 本研究の目的は, 最大公約数に関する等式・不等式の証明問題の解法を分類・分析し, 証明のアルゴリズムを作成することである.

修士論文では, [1, 3–8] から最大公約数に関する問題を収集し, 問題の形によって (S1) から (S12) に分類した. そして各分類毎に, 一番使いやすいと判断した証明法を選び, 選んだ証明法のアルゴリズムを示した. その際, (S2),(S4),(S6) から (S8) では, 性質 5.4 を用いずに証明する方法 (P1) と, 用いて証明する方法 (P2) に分けてそれぞれ証明のアルゴリズムを作成した. 本稿では, このうちの (S3),(S4)(P1) における証明のアルゴリズムを示す. 以下の 2 節でシークエント体系 SNK を定義する. 3,4 節では, 一般の文献における問題と証明を分類・分析し, 6 節でそれらの証明のアルゴリズムを作成する. 5 節は 6 節の準備である.

なお, 本稿ではローマ小文字は断りがない限り自然数 $(1, 2, \cdots)$ を表す. また, 本稿では便宜上, 以下の表 1 で示した表記を用いる.

表 1　本稿で用いる表記法

表記	意味
$a \mid b$	a は b の約数である
$\mathrm{CD}(a_1, \cdots, a_n)$	$a_1, \cdots, a_n$ の公約数全体の集合
$\mathrm{GCD}(a_1, \cdots, a_n)$	$a_1, \cdots, a_n$ の最大公約数

2　シークエント体系 SNK の導入

この節では, シークエント体系 SNK を定義する. 本稿で用いる体系 SNK は, [2] で用いている体系に, 以下の定義, 定理を追加したものである.

2.1　追加する推論規則

追加する推論規則は以下の通りである.
まず, 変数の消去に関する推論規則を定義する.

変数の消去に関する推論規則

$$\frac{d = t, \Gamma \longrightarrow d = u}{\Gamma \longrightarrow t = u}\ (\text{変数E})$$

つぎに, 代入に関する推論規則を定義する.

代入に関する推論規則

t, u を項とするとき, 代入の推論規則を以下のように定義する.

$$\frac{t = u, P(u), \Gamma \longrightarrow Q}{t = u, P(t), \Gamma \longrightarrow Q}\ (\text{代入})$$

つぎに, 証明図を実際の証明に近付けるために, 定理 (公理) の適用に関する推論規則を定義する. いずれも [2] で定義している推論規則を用いて証明可能である.

定理, 公理に関する推論規則 1

定理 (または公理)

$$R$$

に対し,

$$\frac{R, \Gamma \longrightarrow Q}{\Gamma \longrightarrow Q}\ (\text{定理のラベル})$$

を推論規則に追加する.

定理, 公理に関する推論規則 2

m を自然数とする. 定理 (または公理)

$$\forall a_1 \cdots \forall a_m (P \supset R)$$

に対し,

$$\frac{R[u_1/a_1, \cdots, u_m/a_m], \Gamma \longrightarrow Q}{P[u_1/a_1, \cdots, u_m/a_m], \Gamma \longrightarrow Q}\ (\text{定理のラベル})$$

$$\frac{\Gamma \longrightarrow P[u_1/a_1, \cdots, u_m/a_m]}{\Gamma \longrightarrow R[u_1/a_1, \cdots, u_m/a_m]}\ (\text{定理のラベル})$$

を推論規則に追加する.

上の二つの推論規則における「定理のラベル」とは, 定理 (または公理) である $R, \forall a_1 \cdots \forall a_m (P \supset R)$ の名前やラベルのことである. 例えば, 5 節の「性質 5.1」や「性質 5.3」を定理のラベルとして用いている.

最後に, SNK 公理, Def に関する推論規則を追加する. 追加する SNK 公理, Def に関する推論規則は以下の表 2, 表 3 の通りである. ただし, n は 2 以上の自然数である.

N.D.1 prop は, 自然数 (Natural number) の世界において, 1 の約数 (Divisor) は 1 しかないことを表す.

表 2 Def 推論規則

ラベル名	論理式
公約数 Def	$d \mid s_1 \ \wedge \ \cdots \ \wedge \ d \mid s_n$ $\Longleftrightarrow \ d \in \mathrm{CD}(s_1, \cdots, s_n)$ $d = \mathrm{GCD}(s_1, \cdots, s_n)$ $\Longrightarrow \ d \mid s_1 \ \wedge \ \cdots \ \wedge \ d \mid s_n$

表 3 SNK 公理

ラベル名	論理式
N.D.1 prop	$d \mid 1 \implies d = 1$

3 一般の文献での問題の扱われ方

一般の文献 [1,3–8] において, 最大公約数に関する等式・不等式を証明する問題は, 表 4 にまとめたとおりである. [7] p.87 節末問題 12(1) は 「ユークリッド互助法」に関する特別な問題であるから, 一般の問題に直してある. 「ユークリッド互助法」(およびそれに関する特別な問題) は [7] だけでなく, [1,3–8] で紹介されている. それらをまとめて etc としてある. ただし, Γ は「「最大公約数に関する仮定」以外の仮定」を並べた列である. α, β, f_1 は 2 以上の自然数である. 各 $i \in \{1, \cdots, f_1\}$ に対し, β_i は 2 以上の自然数である. 各 $j \in \{1, \cdots, f_{2,1}\}$ に対し, α_j は 2 以上の自然数である. 各 $k \in \{1, \cdots, f_{2,2}\}$ に対し, γ_k は 2 以上の自然数である.

表 4 最大公約数に関する等式・不等式を証明する問題

証明するシークエントの形		該当する問題
仮定	Γ	[3] p.103 Q3
結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$	
仮定	$\Gamma, \mathrm{GCD}(a_1, \cdots, a_\beta) = 1$	[3] p.103 Q4(2), Q7
結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$	
仮定	$\Gamma, \mathrm{GCD}(a_1, \cdots, a_\beta) = 1$	[3] p.103 Q4(1)
結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) \leq e_2$	
仮定	$\Gamma, \bigwedge_{i=1}^{f_1} (\mathrm{GCD}(a_{i,1}, \cdots, a_{i,\beta_i}) = 1)$	[3] p.199 T7-10
結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$	
仮定	Γ	[7] p.87 節末問題 12(1), [3] p.87 T3-5(2), p.88 2 行目, etc.
結論	$\prod_{j=1}^{f_{2,1}} \mathrm{GCD}(s_{j,1}, \cdots, s_{j,\alpha_j}) = \prod_{k=1}^{f_{2,2}} \mathrm{GCD}(t_{k,1}, \cdots, t_{k,\gamma_k})$	
仮定	$\Gamma, \bigwedge_{i=1}^{f_1} (\mathrm{GCD}(a_{i,1}, \cdots, a_{i,\beta_i}) = 1)$	[3] p.100 T3-16, p.134 Q4(1)
結論	$\prod_{j=1}^{f_{2,1}} \mathrm{GCD}(s_{j,1}, \cdots, s_{j,\alpha_j}) = \prod_{k=1}^{f_{2,2}} \mathrm{GCD}(t_{k,1}, \cdots, t_{k,\gamma_k})$	

4 一般の文献における証明の分類・分析

この節では, 表 4 で示した問題の証明を分類・分析する. (S3) は他の問題に比べると簡単に証明できる (詳細は 6.1 節で説明する). それ以外の問題のうち,「最大公約数が等しいこと」以外を示す問題の証明は, 性質 5.4 を用いない方法 (P1) と用いる方法 (P2) がある. 「最大公約数が等しいこと」を示す問題の証明は, (i) 公約数全体の集合が一致することを示す方法, (ii) ユークリッド互助法を用いる方法, (iii) 素因数分解を用いる方法の三つに分類できる. 詳細は割愛する.

5 6 節の準備

つぎの 6 節で証明のアルゴリズムを作成する. この節では, そのために必要な基本的な性質を述べる.

性質 5.1

$m_1, \cdots, m_n$ を任意の整数とする. このとき, 以下が成立する.

$$\bigwedge_{i=1}^{n} (c \mid a_i) \implies c \ \Big| \ \sum_{i=1}^{n} m_i a_i$$

性質 5.1 の証明は n に関する帰納法で行う (ここでは割愛する).

定理 5.2

n を 2 以上の自然数とする. このとき, 以下が成立する.

$\sum_{i=1}^{n} s_i x_i = 1$ を満たす整数 $x_1, \cdots, x_n$ が存在する
$\Longleftrightarrow$ $s_1, \cdots, s_n$ が互いに素

本稿では ($\Longleftarrow$) の証明は割愛する.

定理 5.2($\Longrightarrow$) の証明

$\sum_{i=1}^{n} s_i x_i = 1$ を満たす整数組 $x_1, \cdots, x_n$ が存在すると仮定する. そこで, そのような整数解を

$$(x_1, \cdots, x_n) = (u_1, \cdots, u_n)$$

とする. よって, $\sum_{i=1}^{n} s_i u_i = 1$ である. ここで, $s_1, \cdots, s_n$ の最大公約数を d とする. このとき, $d = 1$ を示せばいい. d は $s_1, \cdots, s_n$ の公約数であるから, $d \mid s_1, \cdots, d \mid s_n$ である. これらと性質 5.1 より, $d \ \Big| \ \sum_{i=1}^{n} s_i u_i$ である. これと $\sum_{i=1}^{n} s_i u_i = 1$ より, $d \mid 1$ である. 1 の約数は 1 だけであるから, $d = 1$ である. 以上で題意は示された.

性質 5.3

n を 2 以上の自然数とする. このとき,

$$d \in \mathrm{CD}(s_1, \cdots, s_n) \iff d \mid \mathrm{GCD}(s_1, \cdots, s_n)$$

である.

性質 5.3 の証明は n に関する帰納法で行う (ここでは割愛する).

性質 5.4

p を素数とするとき, 以下が成立する.

$$p \mid ab \iff p \mid a \text{ または } p \mid b$$

$$p \mid a^n \iff p \mid a$$

性質 5.4 の証明は割愛する.

6 証明のアルゴリズム

ここで対象とする証明は, 3 節の冒頭で示した文であるが, それらの文は, その形から表 5 に示した六つの形に分類される. ただし, Γ などの記号の意味は表 4 と同じである.

表 5 表 4 の問題における形による分類

分類	証明する文	
(S3)	仮定	Γ
	結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$
(S4)	仮定	$\Gamma, \mathrm{GCD}(a_1, \cdots, a_\beta) = 1$
	結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$
(S6)	仮定	$\Gamma, \mathrm{GCD}(a_1, \cdots, a_\beta) = 1$
	結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) \leq e_2$
(S7)	仮定	$\Gamma, \bigwedge_{i=1}^{f_1} (\mathrm{GCD}(a_{i,1}, \cdots, a_{i,\beta_i}) = 1)$
	結論	$\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$
(S11)	仮定	Γ
	結論	$\prod_{j=1}^{f_{2,1}} \mathrm{GCD}(s_{j,1}, \cdots, s_{j,\alpha_j}) = \prod_{k=1}^{f_{2,2}} \mathrm{GCD}(t_{k,1}, \cdots, t_{k,\gamma_k})$
(S12)	仮定	$\Gamma, \bigwedge_{i=1}^{f_1} (\mathrm{GCD}(a_{i,1}, \cdots, a_{i,\beta_i}) = 1)$
	結論	$\prod_{j=1}^{f_{2,1}} \mathrm{GCD}(s_{j,1}, \cdots, s_{j,\alpha_j}) = \prod_{k=1}^{f_{2,2}} \mathrm{GCD}(t_{k,1}, \cdots, t_{k,\gamma_k})$

修士論文では (S5),(S8),(S9),(S10) をそれぞれ追加して議論しているが, 本稿では詳細を割愛する.

6.1 (S3) の証明のアルゴリズム

(S3) の証明のアルゴリズムを考える. (S3) を示すポイントは,

$$\sum_{i=1}^{\alpha} s_i x_i = 1 \tag{1}$$

を満たす整数組 $(x_1, \cdots, x_\alpha)$ を仮定 Γ を用いて一組見つけることである. (1) を満たす整数組 $(x_1, \cdots, x_\alpha) = (u_1, \cdots, u_\alpha)$ が一組見つかれば, 定理 5.2($\Longrightarrow$) より, (S3) を示すことができる.

したがって, (S3) の証明は, 以下のように行うことができる.

(S3) を証明するアルゴリズム (通常,SNK)

step1 : (1) を満たす整数組

$$(x_1, \cdots, x_\alpha) = (u_1, \cdots, u_\alpha)$$

を見つける.
step2 : 定理 5.2($\Longrightarrow$) の証明をたどる. SNK を用いる場合, 証明図 R_1 を作成する. 終了.

R_1 は以下の通りである.

$$\dfrac{\dfrac{\dfrac{\vdots\ R_{1,1} \qquad \vdots\ R_{1,2}}{\Gamma \longrightarrow \Delta \qquad \Delta, \Psi \longrightarrow d = 1}}{\Psi, \Gamma \longrightarrow d = 1}\ (\mathrm{cut})}{d = \mathrm{GCD}(s_1, \cdots, s_\alpha), \Gamma \longrightarrow d = 1}\ (\text{公約数 } Def)$$
$$\dfrac{}{\Gamma \longrightarrow \mathrm{GCD}(s_1, \cdots, s_\alpha) = 1}\ (\text{変数E})$$

ただし, Δ, Ψ は, それぞれ以下を表す.

$$\Delta \ :\ s_1 u_1 + \cdots + s_\alpha u_\alpha = 1$$
$$\Psi \ :\ d \mid s_1, \cdots, d \mid s_\alpha$$

step1 より, $\Gamma \longrightarrow \Delta$ に至る証明図 $R_{1,1}$ はすでに見つかっている.

$R_{1,2}$ は以下の通りである.

$$\dfrac{\dfrac{\dfrac{}{d = 1 \longrightarrow d = 1}\ (\text{N.D.1 prop})}{d \mid 1 \longrightarrow d = 1}\ (\text{代入})}{\sum_{i=1}^{\alpha} s_i u_i = 1, d \mid \sum_{i=1}^{\alpha} s_i u_i \longrightarrow d = 1}\ (\text{性質 5.1})$$
$$\sum_{i=1}^{\alpha} s_i u_i = 1, \Psi \longrightarrow d = 1$$

6.2 (S4) の証明のアルゴリズム

(S4) の証明のアルゴリズムを考える. (S4) が (P1), (P2) のどちらに分類されるかを見分けるには,

$$\sum_{i=1}^{\alpha} s_i x_{1,i} = a_1, \cdots, \sum_{i=1}^{\alpha} s_i x_{\beta,i} = a_\beta \tag{2}$$

を満たす整数組

$$\mathbf{x_1} = (x_{1,1}, \cdots, x_{1,\alpha})^{\mathbf{T}} = (u_{1,1}, \cdots, u_{1,\alpha})^{\mathbf{T}}, \cdots,$$
$$\mathbf{x}_\beta = (x_{\beta,1}, \cdots, x_{\beta,\alpha})^{\mathbf{T}} = (u_{\beta,1}, \cdots, u_{\beta,\alpha})^{\mathbf{T}}$$

が Γ を用いたときに存在するか否かを調べればいい. もしそのような整数組が $a_1, \cdots, a_\beta$ に依存せず具体的に見つかれば, (P1) に分類される. 整数組が具体的に見つからない場合は, (P2) に分類される.

(S4) が (P1) に分類される場合, (2) を満たす整数組 $\mathbf{x_1} = \mathbf{u_1}, \cdots, \mathbf{x}_\beta = \mathbf{u}_\beta$ が存在することを用いて, 以下のように (S4)(P1) を証明することができる.

定理 6.1

$\mathrm{GCD}(a_1, \cdots, a_\beta) = 1$ と仮定する. 整数組

$$\mathbf{x_1} = (x_{1,1}, \cdots, x_{1,\alpha})^{\mathbf{T}} = (u_{1,1}, \cdots, u_{1,\alpha})^{\mathbf{T}}, \cdots,$$
$$\mathbf{x}_\beta = (x_{\beta,1}, \cdots, x_{\beta,\alpha})^{\mathbf{T}} = (u_{\beta,1}, \cdots, u_{\beta,\alpha})^{\mathbf{T}}$$

が (2) を満たすとき, すなわち

$$\sum_{i=1}^{\alpha} s_i u_{1,i} = a_1, \cdots, \sum_{i=1}^{\alpha} s_i u_{\beta,i} = a_\beta \qquad (3)$$

のとき, $\mathrm{GCD}(s_1, \cdots, s_\alpha) = 1$ である.

定理 6.1 の証明

$\mathrm{GCD}(a_1, \cdots, a_\beta) = 1$ と仮定する. $s_1, \cdots, s_\alpha$ の最大公約数を e とおく. このとき, $e = 1$ を示せばいい. e は $s_1, \cdots, s_\alpha$ の公約数であるから, $e \mid s_1, \cdots, e \mid s_\alpha$ である. これらと性質 5.1 より, $e \mid \sum_{i=1}^{\alpha}(s_i u_{1,i}), \cdots, e \mid \sum_{i=1}^{\alpha}(s_i u_{\beta,i})$ である. これらと (3) より, $e \mid a_1, \cdots, e \mid a_\beta$ である. よって, $e \in \mathrm{CD}(a_1, \cdots, a_\beta)$ である. これと性質 5.3 より, $e \mid \mathrm{GCD}(a_1, \cdots, a_\beta)$ である. これと最初の仮定より, $e \mid 1$ である. 1 の公約数は 1 しかないので, $e = 1$ である. 以上で題意は示された.

(S4) の証明のアルゴリズム (通常,SNK)

step1 : Γ を用いたとき, (2) を満たし, かつ $a_1, \cdots, a_\beta$ に依存しない具体的な整数組

$$\mathbf{x_1} = (x_{1,1}, \cdots, x_{1,\alpha})^{\mathbf{T}} = (u_{1,1}, \cdots, u_{1,\alpha})^{\mathbf{T}}, \cdots,$$
$$\mathbf{x}_\beta = (x_{\beta,1}, \cdots, x_{\beta,\alpha})^{\mathbf{T}} = (u_{\beta,1}, \cdots, u_{\beta,\alpha})^{\mathbf{T}}$$

が存在するか否かを調べる. もし存在すれば (P1) に分類されるので, step2.1 へ. 存在しなければ, (P2) に分類される. この場合のアルゴリズムは割愛する.
step2.1 : 定理 6.1 の証明をたどる. SNK を用いる場合, 証明図 R_2 を作成する. 終了.

R_2 は以下の通りである.

$$\dfrac{\begin{array}{cc}\vdots\ R_{2,1} & \vdots\ R_{2,2}\\ \Gamma \longrightarrow \Delta & \Delta, \Psi_2, \Phi \longrightarrow d = 1\end{array}}{\dfrac{\dfrac{\Psi_2, \Gamma, \Phi \longrightarrow d = 1}{\Psi_1, \Gamma, \Phi \longrightarrow d = 1}\ (\text{公約数 } Def)}{\Gamma, \Phi \longrightarrow \mathrm{GCD}(s_1, \cdots, s_\alpha) = 1}\ (\text{変数E})}\ (\text{cut})$$

ただし, $\Delta, \Phi, \Psi_1, \Psi_2$ は, それぞれ以下を表す.

$$\Delta \ :\ \sum_{i=1}^{\alpha} s_i u_{1,i} = a_1, \cdots, \sum_{i=1}^{\alpha} s_i u_{\beta,i} = a_\beta$$
$$\Phi \ :\ \mathrm{GCD}(a_1, \cdots, a_\beta) = 1$$
$$\Psi_1 \ :\ d = \mathrm{GCD}(s_1, \cdots, s_\alpha)$$
$$\Psi_2 \ :\ d \mid s_1, \cdots, d \mid s_\alpha$$

step1 より, $\Gamma \longrightarrow \Delta$ に至る証明図 $R_{2,1}$ はすでに見つかっている.

$R_{2,2}$ は以下の通りである.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{d = 1 \longrightarrow d = 1}{d \mid 1 \longrightarrow d = 1}\ (\text{N.D.1 prop})}{d \mid \mathrm{GCD}(a_1, \cdots, a_\beta), \Phi \longrightarrow d = 1}\ (\text{代入})}{d \in \mathrm{CD}(a_1, \cdots, a_\beta), \Phi \longrightarrow d = 1}\ (\text{性質 5.3})}{\Psi_4, \Phi \longrightarrow d = 1}\ (\text{公約数 } Def)}{\Delta, \Psi_3, \Phi \longrightarrow d = 1}\ (\text{代入})}{\Delta, \Psi_2, \Phi \longrightarrow d = 1}\ (\text{性質 5.1})$$

ただし, Ψ_3, Ψ_4 は, それぞれ以下を表す.

$$\Psi_3 \ :\ d \left| \sum_{i=1}^{\alpha} s_i u_{1,i}, \cdots, d \right| \sum_{i=1}^{\alpha} s_i u_{\beta,i}$$
$$\Psi_4 \ :\ d \mid a_1, \cdots, d \mid a_\beta$$

参考文献

[1] 岡本和夫 ほか 10 名:『数学A』. 実教出版, 東京, 2012.

[2] 佐々木 克巳 :「シークエント体系の証明図から実証明を作る方法」, 『アカデミア 情報理工編 第 11 巻』. 2011, pp.35-54

[3] 芹沢 正三 :「素数入門 計算しながら理解できる」. 講談社, 東京, 2013.

[4] 高橋陽一郎 ほか 33 名 :『詳説 数学A』. 啓林館, 大阪, 2011.

[5] チャート研究所 :『新課程 チャート式 基礎からの数学 I + A』. 数研出版, 東京, 2012.

[6] 坪井俊 ほか 13 名 :『数学A』. 数研出版, 東京, 2012.

[7] 長谷川考志 ほか 20 名 :『数学A』. 第一学習社, 広島, 2012.

[8] 俣野博・河野俊丈 ほか 27 名 :『数学A』. 東京書籍, 東京, 2013.