講義資料 (6): 1 次不定方程式

6.1　1 次不定方程式

本節は，教科書 3.2 節の冒頭 (pp.117–123) に対応する．

定義 6.1 一般に，整数係数を持つ整数変数についての方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

を，1 次の**不定方程式** (indeterminate equation)，または 1 次の**ディオファントス方程式** (Diophantine equation) という．また，方程式を満たすような整数の組 $x_1, \ldots, x_n$ を求めることを方程式を**解く** (solve) といい，その組のことを方程式の**整数解** (integer solution)，または単に**解** (solution) と言う．□

NOTE: ディオファントスは 3 世紀に (現エジプトの) アレクサンドリアで活躍した数学者．著書の『算術』 ("Arithmetica") が有名．「代数学の父」と呼ばれることもある．

NOTE: フェルマーが，かの有名なフェルマーの大定理 (フェルマー予想) と共に「私は真に驚くべき証明を見つけたが，この余白はそれを書くには狭すぎる」と余白に書き込んだ本がこの『算術』である．

NOTE: "代数学" の英語名である "Algebra" の語源は，ディオファントス等の古代ギリシア数学を継承したアラビア数学を代表する一人であるアル＝フワーリズミーの著書『hisāb al-jabr wa'l muqābara (約分と消約の計算の書)』の "al-jabr" です．なお，"jabr" は「バラバラのものを再結合する」という意味であり，"al" は……，良く分からないです．知ってる人がいたら教えてください．
なお，アル＝フワーリズミーは 9 世紀前半にアッバース朝時代のバグダードで活躍した数学者．フワーリズミーの名は「ホラズム (現在のウズベキスタンとトルクメニスタンの辺り) 出身の人」を意味する．また，彼の名はアルゴリズム (algorithm) の語源にもなっている．これは彼の著書『インドの数の計算法』のラテン語訳の冒頭が Algoritmi dicti (アル＝フワーリズミーに曰く) となっていた事に由来する．

例 6.2 不定方程式 $8x + 3y = 5$ は $x = -2, y = 7$ や $x = 1, y = -1$ など複数の整数解を持つ．また，不定方程式 $2x + 6y = 3$ は整数解を一つも持たない．□

定理 6.3 不定方程式 $ax + by = c$ が整数解を持つ $\iff (a, b)|c$

証明 $d = (a, b)$ とする．

($\Leftarrow$) 定理 4.10 より，ある整数 x', y' が存在して $ax' + by' = d$．ここで，$d|c$ を考えて $c = kd$ とすると，$ax'k + by'k = dk = c$．よって整数解 $x = x'k, y = y'k$ を持つ．

(⇒) 不定方程式 $ax+by=c$ が整数解 $x=u, y=v$ を持つとする．このとき $au+bv=c$ が成立．この等式の左辺は d の倍数なので，右辺 c も d の倍数．すなわち，$d|c$．□

さて，解をどのように求めるのか，というのは自然な欲求であると思われる．不定方程式の解法には次に紹介する拡張ユークリッドの互除法が重要な役割を担う．

アルゴリズム 6.4 (拡張ユークリッドの互除法 (extended Euclidean algorithm))
入力として整数 a, b をとり，$ax+by=d=(a,b)$ となる整数 x, y, d を (一組だけ) 出力．

$(d, d') := (a, b)$; $(x, x') := (1, 0)$; $(y, y') := (0, 1)$;
while $d' \neq 0$ **do**
  $q := d \text{ div } d'$;
  $(d, d') := (d', d \bmod d')$;
  $(x, x') := (x', x - qx')$;
  $(y, y') := (y', y - qy')$;
end while
x, y, d の値を出力

□

命題 6.5 拡張ユークリッドの互除法は，任意の入力 a, b に対し，$ax+by=d=(a,b)$ となる整数 x, y, d を有限時間で必ず出力する．

証明 変数 d, d' のみに注目すると拡張ユークリッドの互除法はユークリッドの互除法に完全に対応する．よって，拡張ユークリッドの互除法は有限時間で停止し，出力 d は $d=(a,b)$ の関係を満たす．
出力までに k 回 while ループが実行されたとする．任意の i $(0 \leq i \leq k)$ に対し，i 回 while ループが実行された時点での変数 x, x', y, y', d, d' の値を $x_i, x'_i, y_i, y'_i, d_i, d'_i$ とする．このとき，各 i $(0 \leq i \leq k)$ で，$ax_i+by_i=d_i$ かつ $ax'_i+by'_i=d'_i$ が成立していることを示せば十分．i に関する帰納法で示す．

Basis $i=0$ の場合は，$ax_0+by_0=a*1+b*0=a=d_0$ かつ $ax'_0+by'_0=a*0+b*1=b=d'_0$ となり成立．

I.S. $i>0$ とする．帰納法の仮定より $ax_{i-1}+by_{i-1}=d_{i-1}$ かつ $ax'_{i-1}+by'_{i-1}=d'_{i-1}$ が成立．よって，$ax_i+by_i=ax'_{i-1}+by'_{i-1}=d'_{i-1}=d_i$．ここで，$q=d_{i-1} \text{ div } d'_{i-1}$ とする．$d'_i=d_{i-1} \bmod d'_{i-1}$ なので $d_{i-1}=qd'_{i-1}+d'_i$．よって，$d_{i-1}-qd'_{i-1}=d'_i$．よって，$ax'_i+by'_i=a(x_{i-1}-qx'_{i-1})+b(y_{i-1}-qy'_{i-1})=ax_{i-1}+by_{i-1}-q(ax'_{i-1}+by'_{i-1})$ $=d_{i-1}-qd'_{i-1}=d'_i$. □

アルゴリズム 6.6

入力: 整数 a, b, c (ただし $ab \neq 0$)
出力: 不定方程式 $ax+by=c$ の一般解 (パラメータ t を用いるとする)

(1) 拡張ユークリッドの互除法を用いて
  $(a,b)=d$ となる整数 d と，$au+bv=d$ となる整数 u, v を一組求める．
(2) $d \not| c$ ならば，解を持たないと判定し終了．そうで無い場合は (3) に進む．
(3) $a'=a \text{ div } d$, $b'=b \text{ div } d$, $c'=c \text{ div } d$ を求め，
  $x=b't+uc'$ と $y=-a't+vc'$ を出力．(t は媒介変数)

□

命題 6.7 アルゴリズム 6.6 は仕様を満たす，すなわち，任意の入力 a, b, c $(ab \neq 0)$ に対し有限時間で終了し，さらに，不定方程式 $ax + by = c$ が解を持つならばその一般解を出力し，解を持たないならば解を持たないと判定する．

証明 有限時間で停止するのは，拡張ユークリッドの互除法が有限時間で終了することより明らか．
(1) で求めた d は $(a, b) = d$ となっているので，定理 6.3 より，$d \not| c$ のときは解を持たない．よって，解を持たないときには解を持たないと判定している．
$d|c$ の場合を考える．このとき，$a(b't + uc') + b(-a't + vc') = (ab't - ba't) + (auc' + bvc')$ $= (a'db't - b'da't) + (au + bv)c' = (au + bv)c' = dc' = c$．よって，$x = b't + uc', y = -a't + vc'$ は解を与える．
最後に，$d|c$ の場合の出力が一般解を与えることを示す．このとき，$d \neq 0$ より $ax + by = c$ の解の全体と $a'x + b'y = c'$ の解の全体は一致するので，$x = b't + uc', y = -a't + vc'$ が不定方程式 $a'x + b'y = c'$ の一般解を与える事を示せば十分．具体的には，$a'x + b'y = c'$ の任意の解 $x = x_0, y = y_0$ に対し，ある整数 t が存在して $x_0 = b't + uc', y_0 = -a't + vc'$ となることを示す．
今，$x = uc', y = vc'$ が不定方程式 $a'x + b'y = c'$ の解であるので $a'(uc') + b'(vc') = c' = a'x_0 + b'y_0$．よって，$a'(x_0 - uc') = b'(vc' - y_0)$ なので $a'|b'(vc' - y_0)$．$(a', b') = 1$ より $a'|(vc' - y_0)$．よって，ある整数 t が存在して $a't = vc' - y_0$ となり $y_0 = -a't + vc'$ となる．また，$a'(x_0 - uc') = b'(vc' - y_0)$ より，$a'uc' = a'(-b't + x_0)$．$a' \neq 0$ なので，$x_0 = b't + uc'$ を得る． □

さて，アルゴリズム 6.6 を用いてどのように不定方程式の解を得るか例で見てみよう．

例 6.8 不定方程式 $8x + 3y = 5$ を考える．最初に拡張ユークリッドの互除法を用いて $8u + 3v = d = (8, 3)$ となる整数 u, v, d を求める．

d	d'	x	x'	y	y'	q
8	3	1	0	0	1	
3	2	0	1	1	−2	2
2	1	1	−1	−2	3	1
1	0	−1	3	3	−8	2

以上より，$u = -1, v = 3, d = 1$ を得る．$d|5$ なので整数解が存在する．ここで，$d = 1$ なので $a' = 8, b' = 3, c' = 5$．よって，一般解 $x = 3t - 5,\ y = -8t + 15$ を得る．なお，例題 6.2 で提示した解は $t = 1, 2$ の場合に対応する． □

なお，本節では簡単のために 2 変数の場合のみを議論したが本節の内容は任意個数の変数の場合でも成立する．最後に，定理 6.3 の一般形を紹介しておく (証明は割愛)．

定理 6.9 1 次不定方程式 $a_1x_1 + \cdots + a_nx_n = c$ が整数解を持つ $\iff$ $(a_1, \ldots, a_n)|c$ □

NOTE: 定理 6.9 を用いると，1 次不定方程式が整数解を持つかどうかを容易に判定することができる．では高次の項も含む一般の不定方程式の整数解が存在するかどうかを判定できる一般的な手法は存在するだろうか? 実は，このような手法が本質的に存在しない

ことが証明されているのである．これが，かの有名な『ヒルベルトの第 10 問題』と，その否定的解決である．ちなみに，非常に微妙な話ではあるが，実数解が存在するかどうかは判定可能であり，有理数解の存在判定が行えるかどうかは未だ分かっていない……，難しい．

NOTE: 我々はどれほど頑張ろうとも有限の時間に有限の記号に対して有限の操作を行うことしか出来ない．そのために，ある種の限界を本質的に所有する．ヒルベルトの第 10 問題などがその例である．このような，どう頑張ろうとも決して判定できない問題のことを『決定不能問題』と呼ぶ．他の有名な決定不能問題としては『プログラムの停止性問題』がある．すなわち，プログラムが停止するかどうかを判定できる汎用的な手段は存在しないのである．この辺りの話は現在『計算可能性の理論』として計算機科学や数理論理学の重要な分野に育っている．

NOTE: 1900 年にパリで開かれた国際数学者会議において，ヒルベルト (Hilbert) は 20 世紀の数学が解決すべきであるという 23 の問題を提出した．この中には未だ解かれていない『リーマン予想』も含まれている．

NOTE: ヒルベルトの第 10 問題は，1970 年に旧ソ連の若冠 22 才の青年マティヤセヴィッチ (Matiyasevich) によって否定的に解決された．この証明はフィボナッチ数が指数関数的に増加することを利用した非常に巧妙な証明である．

NOTE: その後マティヤセヴィッチは素数表現多項式，すなわち，変数に適当な自然数を代入することで全ての素数を表現し，かつ値が正になるときはいつでも素数になる多項式を発見した．最初に (1971 年に) 彼が発見した素数表現多項式は 24 変数 37 次多項式であったと言う (英訳された彼の論文では 21 変数 21 次多項式に改良されていた)．以下に，P.Jones, D.Sato, H.Wada, D.Wiens が 1976 年に発見した 26 変数 25 次の素数表現多項式を紹介しておく．これは，(私が知る限り) 唯一の紙面に載せることが可能なサイズの素数表現多項式である．

$$
\begin{aligned}
(k+2)\{1 &- [wz+h+j-q]^2 \ - \ [(gk+2g+k+1)(h+j)+h-z]^2 \\
&- [2n+p+q+z-e]^2 \ - \ [16(k+1)^3(k+2)(n-1)^2+1-f^2]^2 \\
&- [e^3(e+2)(a+1)^2+1-o^2]^2 \ - \ [(a^2-1)y^2+1-x^2]^2 \\
&- [16r^2y^4(a^2-1)+1-u^2]^2 \ - \ [n+l+v-y]^2 \\
&- [((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x-cu)^2]^2 \\
&- [(a^2-1)l^2+1-m^2]^2 \ - \ [ai+k+1-l-i]^2 \\
&- [p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\
&- [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
&- [z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}
$$

6.2 連立不定方程式

本節は，教科書 3.2 節の最後 (pp.126–127) に対応する．

連立の 1 次不定方程式も一般解のパラメータ表示を繰り返し求めることによって解くことができる.

例 6.10 連立 1 次不定方程式

$$\begin{cases} 3x - 5y &= 1 \\ 5y - 7z &= 1 \end{cases}$$

を考える．アルゴリズム 6.6 を不定方程式 $3x - 5y = 1$ に適用することにより，$x = 2 - 5s,\ y = 1 - 3s$ を得る．$y = 1 - 3s$ を $5y - 7z = 1$ に代入して不定方程式 $7z + 15s = 4$ を得る．再び，この方程式にアルゴリズム 6.6 を適用することにより，$s = 4 - 7t,\ z = 15t - 8$ を得る．よって連立方程式の解が以下のように得られる．

$$\begin{cases} x &= 2 - 5s = 35t - 18 \\ y &= 1 - 3s = 21t - 11 \\ z &= 15t - 8 \end{cases}$$

□

例 6.11 以下のような問題を考えてみよう.

3 で割ると 1 余り，5 で割ると 2 余り，7 で割ると 3 余る最小の正整数 n を求めよ.

このような問題の解法に連立不定方程式は有効である．実際に連立不定方程式を用いてこの問題を解いてみよう．この問題を数式で書き下すと

$$n = 3x + 1 = 5y + 2 = 7z + 3$$

を満たす最小の正整数 n を求める問題になる．ここで，$3x + 1 = 5y + 2 = 7z + 3$ は二つの不定方程式 $3x - 5y = 1$ と $5y - 7z = 1$ に帰着できる．例 6.10 で見たようにこの連立不定方程式の解は $x = 35t - 18,\ y = 21t - 11,\ z = 15t - 8$ となる．すなわち，$n = 105t - 53$ とパラメーター表示できる．ここで，n は $105t - 53$ で表される最小の正整数なので，求める解は $t = 1$ のとき，すなわち $n = 105 \cdot 1 - 53 = 52$ を得る． □

6.3 1 次不定方程式の正整数解と自然数解

本節は，教科書 3.2 節の中程 (pp.123–126) に対応する.
1 次不定方程式が正整数解を持つかどうか，自然数解を持つかどうかは非常に判定しにくい問題である．本節では比較的取り扱いやすい 2 変数の 1 次不定方程式に対する判定法を学ぶ.

定理 6.12 $(a, b) = 1$ とする．不定方程式 $ax + by = c$ に関して以下の事実が成立.

(1) $ab < 0$ ならば，この方程式は正の整数解を持つ.

(2) $a, b > 0$ ならば以下の事実が成立.

(2.1) $c > ab$ ならば，この方程式は正の整数解を持つ.

(2.2) $c = ab$ ならば，この方程式は正の整数解を持たない.

(2.3) $c = a + b$ ならば，この方程式は正の整数解を持つ．

(2.4) $c < a + b$ ならば，この方程式は正の整数解を持たない．

証明

(1) 一般性を失う事なく $b < 0 < a$ かつ $c \geq 0$ とする ($c < 0$ の場合は両辺に -1 を掛けてやれば良い)．$(a, b) = 1$ なので，定理 6.3 より $ax + by = c$ は整数解を持つ．整数解の一つを $x = u, y = v$ とする．剰余定理より，ある整数 q', r' が存在して $v = q'a + r'$ $(0 \leq r' < a)$．よって，ある整数 q, r が存在して $v = qa + r$ $(0 < r \leq a)$．$x = u + bq,\ y = r$ とすると，

$$ax + by = a(u + bq) + br = au + b(qa + r) = au + bv = c$$

であるので，$x = u + bq,\ y = r$ は整数解となる．ここで，$y = r > 0$ は明らか．また，$b < 0$ と $0 \leq c$ より $ax = c - by > 0$．よって，$a > 0$ なので $x > 0$．すなわち，$x = u + bq,\ y = r$ は正の整数解．

(2.1) $a, b > 0$ かつ $c > ab$ とする．(1) と同様にして，$ax+by = c$ の整数解 $x = u+bq,\ y = r$ $(0 < r \leq a)$ を得る．ここで，$y = r > 0$ は明らか．$c > ab$ と $r \leq a$ より

$$a(u + bq) = c - br \geq c - ab > ab - ab = 0$$

よって，$a > 0$ なので $u + bq > 0$．すなわち，$x = u + bq,\ y = r$ は正の整数解．

(2.2) $a, b > 0$ かつ $c = ab$ とする．正の整数解 $x = u, y = v$ が存在したと仮定する．このとき，$au = ab - bv = b(a - v)$．$au > 0$ より $b(a - v) > 0$．よって，$v > 0$ も考えて $0 < a - v < a$．ここで，$a | b(a - v)$ なので，$a | a - v$ となり矛盾．よって，この場合は正の整数解が存在しない．

(2.3) 明らかに不定方程式の解 $x = y = 1$ が存在．

(2.4) $a, b > 0$ より，如何なる正整数 x, y に対しても $ax + by \geq a + b > c$ となるので，不定方程式 $ax + by = c$ は正の整数解を持たない． □

この定理は，$a, b < 0$ の場合と $a, b > 0$ かつ $a + b < c$ かつ $c < ab$ の場合については言及していない．前者の場合は不定方程式の両辺に -1 を掛けてから議論すれば良い．後者の場合も，探索空間が有限 ($1 \leq x \leq (c - b) \text{ div } a$ かつ $1 \leq y \leq (c - a) \text{ div } b$) であるので，地道に探せば正の解の存在判定を行うことができる．また，一般に $(a, b) = d$ の場合にも，不定方程式 $ax + by = c$ の両辺を d で割ってから議論すれば良い (定理 6.3 より，$d \nmid c$ の場合には，そもそも解を持たない事に注意)．
さて，正の整数解の存在判定の議論をしてきたが，自然数解に関しては状況が微妙に異なる．最後に，自然数解の判定条件も紹介しておく．なお，証明は初等的に行えるが，少々長くなるので割愛する．

定理 6.13 $(a, b) = 1$ とする．不定方程式 $ax + by = c$ に関して以下の事実が成立．

(1) $ab < 0$ ならば，この方程式は自然数解を持つ．

(2) $a, b > 0$ ならば以下の事実が成立.

(2.1) $a = 1$ または $b = 1$ の場合は，$c \geq 0$ のときのみ自然数解を持つ.

(2.2) $a, b \geq 2$ かつ $c > ab - (a + b)$ ならば自然数解を持つ.

(2.3) $a, b \geq 2$ かつ $c = ab - (a + b)$ ならば自然数解を持たない. □

演習課題

問 6.1 拡張ユークリッドの互除法を用いて $936x+102y = d = (936, 102)$ となる整数 x, y, d を一組求めよ.

問 6.2 2 で割ると 1 余り，3 で割ると 2 余り，4 で割ると 3 余る最小の正整数 n を求めよ.

問 6.3 以下の不定方程式が正の整数解を持つかどうか，また，自然数解を持つかどうかを判定せよ．なお，判定の理由も記しておくこと.

(i) $5x + 7y = 37$　　(ii) $7x - 11y = 77$　　(iii) $14x + 35y = 28$

問 6.4 以下の，所謂 “郵便切手問題” に理由を添えて答えよ.
「3 セント切手と 5 セント切手を組み合わせることによっては支払うことの出来ない郵便料金を全て挙げよ.」