２元１次不定方程式特殊解の簡便法による求め方

～互除法を用いたシミュレート(順行)簡便法について

札幌旭丘高校　中村文則

ユークリッドの互除法は，最大公約数を求める高速アルゴリズムである．応用として簡便法を用い二元一次不定方程式の特殊解を求められることはよく知られている．その解法は，互除法により最大公約数を求める過程で生成される余りからシミュレートしていくものであるが，計算が煩雑であることも指摘される．そこで，シミュレートを効率的に求める方法(簡便法)を考えてみよう．

■互除法による最大公約数の求め方

ユークリッドの互除法は自然数に関する次の性質を用いたものである．

> 自然数a,bについて，aをbで割った余りをrとすると，
> aとbの最大公約数はbとrの最大公約数に等しい．　　$\Rightarrow \quad (a,b)=(b,r)$

※rは，$a=bq+r$と変形できる数であり，必ずしも余りである必要はない．

例えば，２つの自然数546と247の最大公約数は，次のように求められる．

$$546=247\times2+52$$
$$247=52\times4+39$$
$$52=39\times1+13$$
$$39=13\times3+0$$

すなわち，$(546,247)=(247,52)=(52,39)=(39,13)=13$

これより，最大公約数は13であることが分かる．

この計算(アルゴリズム)は次の簡便法により効率的に求めることができる．

簡便法Ａ

	546	247	
2	494	208	4
	52	39	
1	39	39	3
	13	0	

簡便法Ｂ-1

3	1	4	2
13) 39	) 52	) 247	) 546
39	39	208	494
0	13	39	52

簡便法Ｂ-2

```
          2
247 ) 546
      494     4
       52 ) 247
            208     1
             39 ) 52
                 39     3
                 13 ) 39
                      39
                       0
```

互除法により求められた最大公約数は，余りを絞り込んでいったものであるが，これを右図のように逆にたどっていく．

$$13=52-39\times1$$
$$=52-(247-52\times4)\times1$$
$$=-247-52\times5$$
$$=-247-(546-247\times2)\times5$$
$$=-546\times5+247\times11$$

これから，不定方程式

$$546x+247y=13$$

の特殊解，$x=-5,\ y=11$が浮かび上がってくる．

一般に次の性質が成立する．

> 自然数$a,\ b$の最大公約数がcであるとき，
> $ax+by=c$
> となる整数$x,\ y$が存在する．

ここで，$ax+by=c$を１次のディオファントス方程式という．

なお，先ほどの例では，$(546,247)=13$であることから，不定方程式の両辺を最大公約数の13で割ると，

$$42x+19y=1$$

この不定方程式の特殊解も $x=-5, y=11$ である．

ディオファントス方程式において，その最大公約 c で両辺を割ると，次の性質が得られる．

> 互いに素である自然数 a, b が与えられたとき，
> $ax+by=1$
> となる整数 x, y が存在する．

これを用いると互いの素である 2 数を x, y の係数とする二元一次不定方程式は，互除法により特殊解を求めることが可能になる．

■互除法による二元一次不定方程式の特殊解の求め方

不定方程式　$501x+217y=1$ の特殊解を求めてみよう．

$$501=217\times2+67$$
$$217=67\times3+16$$
$$67=16\times4+3$$
$$16=3\times5+1$$

↓

余りに関して解く

⇒

$$67=-217\times2+501$$
$$16=-67\times3+217$$
$$3=-16\times4+67$$
$$1=-3\times5+16$$

↑

互除法の計算で得られた剰余の結果を余りに関して解き，逆順にシミュレートしながら，商を積み上げていく．

しかしその計算は商と余りが同じ数になることもあり非常に煩雑である．

そこで，$a=501$，$b=217$ と置き換える．

すなわち，不定方程式を $ax+by=1$ とする．

そうすると，剰余の関係式の部分では，

$$67=-2b+a,\quad 16=-67\times3+b$$

となり見やすくなる．そこで，右のように計算をしていくと，

$$-68a+157b=1$$

と表される．これから，不定方程式 $ax+by=1$ と比較すると，特殊解，

$$x=-68,\ y=157$$

が得られる．

$$\begin{aligned}1&=-3\times5+16\\&=-(-16\times4+67)\times5+16\\&=21\times16-5\times67\\&=21\times(-67\times3+b)-5\times67\\&=-68\times67+21b\\&=-68\times(-2b+a)+21b\\&=-68a+157b\end{aligned}$$

■簡便法による逆順シミュレート(逆行)

H25 年秋に発行された数研通信№78 号(数研出版)で，小島一義氏は

2 元 1 次不定方程式の特殊解の新しい求め方　ーユークリッド互除法の逆行ー

を発表した．

氏は，ユークリッドの互除法の簡便法Aの計算を逆順にシミュレートすることで特殊解が求められることを示している．その計算方法については数研通信で確認いただきたい．

簡単に述べると，互除法の計算手順をその結果からすべて逆試行する．すなわち

商である数　⇒　負の数
割り算　⇒　掛け算
引き算　⇒　足し算

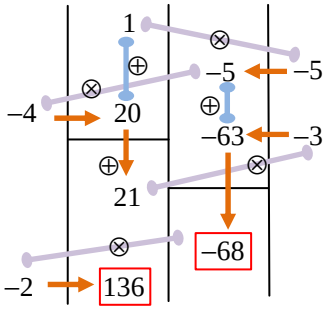
とし，計算過程を遡っていく．いわばビデオの巻き戻し再生である．

この演算により，高速計算で特殊解が求められるのである．

	501	217	
2	434	201	3
	67	16	
4	64	15	5
	3	1	

最後の部分から巻き戻していく

⇒



さらにH26年春に発行された数研通信№79では，臼井達哉氏は「互除法の逆行」の記法の改良を試みている．

氏の互除法の逆行は非常に面白い簡便法ではあり，前述の互除法から絞り込んだ余りを逆に辿る方法をアルゴリズム化したものである．ただ「思考の逆回転」はなかなか馴染みにくいようにも思う．そこで，逆行ではなく，順行で簡便化ができないか考えてみよう．

■簡便法による正順シミュレーション(順行)

再び，不定方程式　$501x+217y=1$ を例にとろう．

互除法の利用では，$a=501$，$b=217$ として，ディオファントス方程式 $ax+by=1$ の特殊解を求めるが，これを結果に代入するのではなく，a,b のままで互除法計算をしてみよう．

例の場合，その商は，

$$2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 5$$

の順に求められる．数 a,b を文字とみて商の順に割り，簡便法を実行していくのである．

	501	217	
2	434	201	3
	67	16	
4	64	15	5
	3	1	

$a=501,$ $b=217$ → 同じ商で割っていく

	a	b	
2	$2b$	$3a-6b$	3
	$a-2b$	$-3a+7b$	
4	$-12a+28b$	$65a-150b$	5
	$13a-30b$	$-68a+157b$	

正順シミュレーションの結果得られた整式は $-68a+157b$ であり，もともとの互除法で得られた余り 1 に対応しているわけだから，

$$-68a+157b=1$$

これより，特殊解 $x=-68,\ y=157$ が得られるのである．さらに面白いのは，互除法とそのシミュレーションの対応する位置にある数は等しいから，例えば左下にある余りの数を比較すると，

$$13a-30b=3$$

これは，$501x+217y=3$ の特殊解が $x=13,\ y=-30$ であることを示している．

■簡便法による正順シミュレーション(順行)の改良

正順シミュレーションで文字 a,b の計算を追っていくと，次のことが分かる．

「a と b の係数は連動しているわけではなく，それぞれ独立に生成される」

文字の四則演算であるわけだから当然である．正確にはもともとの 2 数は連動して商と余りが求められており，その連動性が商「$2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 5$」の並びに凝縮されてしまい，$a,b$ の計算では独立しているようにみえるのである．

このことを利用すると，正順シミュレートはさらに簡便化することができる．

正順シミュレーションから a だけを取り出した表を作ってみよう．ここで，b だけの式については $0a$ と考える．剰余の計算のアルゴリズムは保たれていることが分かるだろう．次に，余りの部分の係数だけを抜き出し順に下右図のように書いていこう．なお，1 行目は，初期値としての余りとみなす．したがって，1 行，3 行，5 行…のように奇数行を抜き出すことになる．そして商を表のように生成する順に並べる．

2	$1a+0b$ $0a+2b$	$0a+1b$ $3a-6b$	3
4	$a-2b$ $-12a+28b$	$-3a+7b$ $65a-150b$	5
	$13a-30b$	$-68a+157b$	

a だけを取り出す →

2	$1a$ $0a$	$0a$ $3a$	3
4	$1a$ $-12a$	$-3a$ $65a$	5
	$13a$	$-68a$	

奇数行の係数を縦に書き抜く →

	1	
2	0	$1-2\times0$
3	1	$0-3\times1$
4	-3	$1-4\times(-3)$
5	13	$-3-5\times13$
	-68	

こうして抜き出された係数から，互除法計算のアルゴリズムは，

［n 行の係数］＝［$(n-2)$ 行の係数］－［$(n-1)$ 行の係数×商］

となることが分かる．

すなわちこのことは，初期値と互除法により生成された商が分ければ a の係数が順次求められるということである．互除法を利用した高速のシミュレーションが可能になるのである．また，a と b は連動していないわけだから，特殊解のひとつが求められれば，不定方程式に代入することにより残りの解は得られる．ただ，b についても a と同様に係数を抜き出し，右表のように，並列しておけば，直接求めることは容易である．

	a	b
	1	0
2	0	1
3	1	−2
4	−3	7
5	13	−30
	−68	157

引き算の部分のミスは心配されるが，その場合は商の値を，$-2 \Rightarrow -3 \Rightarrow -4 \Rightarrow -5$ として足し算に変えてしまうといいだろう．

いくつか例を示して，正順シミュレート法(順行法)を使い方の練習とし，締めくくろう．

なお，不定方程式の特殊解は，合同式によりさらに容易に得られる．だから本当は不定方程式の解法に重きがおかれるべきではなく，ユークリッドの互除法およびその簡便法の原理をしっかりと理解し，そのあるアルゴリズムの面白さに主眼がおかれるべきなのであろう．

(1) $2059x+812y=29$

互除法の簡便法により，$(2059,812)=29$ である．

したがって，正順シミュレート法で求めた値を29倍したものが特殊解になる．

特殊解は，$x=-13\times 29=377$，$y=33\times 29=952$

	2059	812	
2	1624	435	1
	435	377	
1	377	348	6
	58	29	
2	58		
	0		

⇒

	a	b
	1	0
2	0	1
1	1	−2
1	−1	3
6	2	−5
	−13	33

(2) $2101x+3011y=1$

自然数 a,b とする．不定方程式 $ax\pm by=1$ において，$a<b$ の場合は，a と b の初期値は $a=0,\ b=1$ である．

特殊解は，$x=1393,\ y=-972$ である．

	2101	3011	
2	1820	2101	1
	281	910	
4	268	843	3
	13	67	
6	12	65	5
	1	2	

⇒

	a	b
	0	1
1	1	0
2	−1	1
3	3	−2
4	−10	7
5	43	−30
6	−225	157
	1393	−972