

ユークリッドの互除法 あれこれ

栗野俊一 *

2006/06/08

1 ユークリッドの互除法 とは ?

二つの整数 m, n が与えられた時に、この二つの整数の最大公約数を求めるという問題を考える。

一般には、 m, n を素因数分解し、その中で共通な因数をかけ合せるという形を、中学で学んでいる。

それに対して、次のような形で、素因数分解せずに、最大公約数を求めるという方法がある。これが、ユークリッドの互除法 と呼ばれる方法である。

Step 0: m を「割られる数」、 n を「割る数」とする。

Step 1: 「割る数」が 0 であれば、最大公約数は、「割られる数」である (終了)。

Step 2: 「割られる数」を「割る数」で割った余りを「余り」とする。

Step 3: 新しい「割られる数」を今の「割る数」とし、新しい「割る数」を前 Step の「余り」とする。

Step 4: Step 1 に戻る。

講義では、これが、一変数の多項式の場合も利用できることを学んだ。

この内容を C 言語¹ 風に記述すると以下ようになる。

```
warareru = m;
waru = n;

while ( waru != 0 ) {          /* 割る数が 0 でない間、以下を繰り返し */
    amari = warareru % waru; /* % は C 言語で「余り」を計算する */
    warareru = waru;
    waru = amari;
}
```

*日本大学理工学部数学科 kurino@math.cst.nihon-u.ac.jp

¹2 学年生に配当されている「ソフトウェア概論」で学ぶ

}

/* warareru には、m と n の最大公約数が入っている */

例えば、16 と 12 の最大公約数を求める場合には、次のような手順となる。

Step 0: 「割られる数」は 16、「割る数」は 12 となる。

「割られる数」は 16、「割る数」は 12

1 - Step 1: 「割る数」は、現在 12 なので、0 でないから終了しない。

1 - Step 2: 「余り」は、16 を 12 割るので、4 となる。

「余り」は 4

1 - Step 3: 新しい「割られる数」は、元の「割る数」なので、12、新しい「割る数」は、「余り」なので、4 となる。

「割られる数」は 12、「割る数」は 4

1 - Step 4: Step 1 に戻る。

2 - Step 1: 「割る数」は、現在 4 なので、0 でないから終了しない。

2 - Step 2: 「余り」は、12 を 4 割るので、0 となる。

「余り」は 4

2 - Step 3: 新しい「割られる数」は、元の「割る数」なので、4、新しい「割る数」は、「余り」なので、0 となる。

「割られる数」は 4、「割る数」は 0

2 - Step 4: Step 1 に戻る。

3 - Step 1: 「割る数」は、現在 0 なので、終了。「割られる数」には、元の 16 と 12 の最大公約数である 4 が入っている。

上記の例では、長々と記述したが、普段、紙と鉛筆でやる場合は、次のようにもっと簡便な形で表現する。

1. $16 \div 12 = 1...4$

2. $12 \div 4 = 3...0$

3. 余りが 0 になったので、答は、最後に割った数である 4

2 何故？ ユークリッドの互除法

既に、中学校で学んだように、16 と 12 の最大公約数を求めたいのであれば、素因数分解を用いて、次のように解くこともできる。

$$\begin{aligned}16 &= 2^4 \\12 &= 2^2 \times 3 \\4 &= 2^2\end{aligned}$$

これは、16 と 12 をそれぞれ素因数分解を行い、その各々の素因数（上記の例では 2 と 3）の指数の小さい方（上記の例で、2 の指数は 2 の方、3 の指数は、一方にしかないので、考えない [あるいは 0 とする]）を選んで計算すればよい。

確かに、この方法は、分りやすいが、実は、ユークリッドの互除法に比較して、時間がかかるという問題がある。これは、素因数分解そのものが大変難しい² からである。

確かに、小さな数に関しては、直に素因数が思い付くかもしれないが、例えば、演習問題で出題した、 $2^{30} - 1, 2^{18} - 1$ など素因数分解をしようと思った日には、うんざりするかもしれない。

ましてや、多項式で、素因数分解を行うことが大変であることは言うまでもない。

ところが、ユークリッドの互除法は、割り算だけができればよく、これは、桁数の多い整数でも、多項式でも、それほど大変ではない。

ユークリッドの互除法が重要な理由は、これが、大変高速である からである。

上記の例でも、2 を敢て x に置き換えて、多項式 $x^{30} - 1, x^{18} - 1$ と考え、多項式の上での互除法を適用すれば、あっさりと、最大公約数（数といっても多項式だが..）が得られ、この式の x に 2 を代入することにより、元の数の最大公約数が得られる。

3 最大公約数の性質

最大公約数の重要な性質として次の性質があげられる。

定理 1 d が、自然数 m, n の最大公約数であれば、実は、ある整数 a, b が存在し、

$$am + bn = d$$

²実は、現在通信で利用される暗号技術の一つ RSA 暗号は、この素因数分解の困難性に基いて作られている。もし、素因数分解が簡単にできる方法が発見されれば、大変なことになる（程、価値があり、難しい問題ということ..）。

と表現できる。

例えば、16 と 12 の最大公約数 4 の場合は、 $4 = 1 \times 16 + (-1) \times 12$ となるので確かに、16 と 12 を用いて 4 を表現することができる。

これは、最大公約数の非常に特徴的な性質であり、 m, n には、複数の公約数がありえるが、それらの中で、このように、 m と n を利用して表現できるのは、最大公約数だけである³。

この性質は、最大公約数の特に極立った性質であるので、ついでに覚えておこう。

もちろん、断るまでもないが、これは多項式に対しても成立する（事は講義で学んでいる）。

即ち、次の定理が成立する

定理 2 $f(x), g(x) \in K[x]$ に対して、その最大公約数を $\phi(x)$ とする。この時、ある $u(x), v(x) \in K[x]$ が存在し、 $\phi(x) = u(x)f(x) + v(x)g(x)$ となる。

4 ユークリッドの互除法、再び

ある a, b が存在して m, n の最大公約数 d が、 $am + bn = d$ の形で記述できるとして、その a, b とは具体的には何か？ という疑問が自然に生れる。 $am + bn = d$ では、 m, n が与えられており、 d は、 m, n の最大公約数なので、上記のようにユークリッドの互除法で得ることができる。しかし、解るのはここまでで、未知の数は、 a, b の二つあり、式は一つだけである⁴ ももちろん、小さな整数の場合は、目のこで、 a, b の値を推測することもできるだろうが、 m, n が大きくなったり、あるいは、多項式の場合を考えると、そのような場当たりの方法では解決できない。

実は、ここでもユークリッドの互除法（の変形⁵）が利用できる。

例えば、上述のように 16 と 14 で互除法を適用すると以下ようになる。

1. $16 \div 12 = 1 \dots 4$

2. $12 \div 4 = 3 \dots 0$

これは、別の形は以下のように書き表すことができる。

1. $16 = 12 + 4$

2. $12 = 4 + 0$

³後で、述べるようにこのような形で m, n で表現できる数は、全て d の倍数になる。 d の倍数の中で最小のものが d 自身である。また、 d は m, n の公約数の最大なものであり、ようすに、 m, n で表現できるものと m, n の公約数の唯一の共通要素が、 d （最大公約数）である。

⁴なので、実は、このような a, b の組み合わせは、無限に存在することとなる。

⁵ユークリッドの互除法では、余りしか利用しないが以下の議論では商も利用する。

そして、これを、余りを求める式の形に変形すると、次のようになる。

1. $4 = 16 - 12 \times 1$

2. $0 = 12 - 4 \times 3$

ここで、注目すべきは、一つ目の式で、良くみるとこれは、 $4 = \dots$ の形、すなわち、16 と 12 の最大公約数である 4 を表す式であることが解る。

更に、その右辺をみると $16 - 12 \times 1$ であるが、これは、 $1 \times 16 + (-1) \times 12$ と考えれば、ようするに $a = 1, b = -1$ であることを表していることが解る。

これは余りにも話が旨いので、別の例を考えてみよう。例えば、34 と 21 の最大公約数を互除法で求めると次のようになる。

1. $13 = 34 - 21 \times 1$

2. $8 = 21 - 13 \times 1$

3. $5 = 13 - 8 \times 1$

4. $3 = 8 - 5 \times 1$

5. $2 = 5 - 3 \times 1$

6. $1 = 3 - 2 \times 1$

7. $0 = 2 - 1 \times 2$

8. 答は 1

この結果、34 と 21 の最大公約数は、1 である⁶ことが解る。

今度は、流石に一つ目の式に着目しても駄目であるが、良く観察すると次のような性質があることが解る。

- 最後の行は「 $0 = \dots$ 」の形である。
- 最後から二番目の行は「最大公約数 = ..」の形である。
- 一行目の左辺は、 m, n の式である。
- 二行目の左辺は、 n と、一行目の右辺からなる式である。
- n 行目の左辺は、 $n - 1$ 行目と $n - 2$ 行目の右辺からなる式である。

そこで、最初と二番目の 34, 21 を敢て、 m, n と書換え、更に、最後から二番目の左辺の 1 を d と書き換える。

1. $13 = m - n \times 1$

⁶このように最大公約数が、1 であるような数は、互いに素である と言う。

$$2. 8 = n - 13 \times 1$$

$$3. 5 = 13 - 8 \times 1$$

$$4. 3 = 8 - 5 \times 1$$

$$5. 2 = 5 - 3 \times 1$$

$$6. d = 3 - 2 \times 1$$

そして、上の式の左辺を、下の式の右辺に順番に代入してみる。

$$1. 13 = m - n \text{ — これは既に } m, n \text{ の式}$$

$$2. 8 = n - 13 \times 1 = n - (m - n) \times 1 = -m + 2n \text{ — } m, n \text{ の式になった}$$

$$3. 5 = 13 - 8 \times 1 = (m - n) - (-m + 2n) \times 1 = 2m - 3n \text{ — 一つ前だけでなく、二つ前の左辺も利用する。}$$

$$4. 3 = 8 - 5 \times 1 = (-m + 2n) - (2m - 3n) \times 1 = -3m + 5n \text{ — 以下同様}$$

$$5. 2 = 5 - 3 \times 1 = (2m - 3n) - (-3m + 5n) \times 1 = 5m - 8n \text{ — ...}$$

$$6. d = 3 - 2 \times 1 = (-3m + 5n) - (5m - 8n) \times 1 = -8m + 13n \text{ — } d \text{ が } m, n \text{ で表現できた}$$

実際に、 $-8 \times 34 + 13 \times 21 = -272 + 273 = 1$ となる。

もちろん、この手法が、多項式でも利用できることは言うまでもない。

なお、これによって、解 $(a, b \text{ の組})$ が一つしか得られないが、他の解も、実はこの解から作ることができる。

具体的には、もし、ある a, b で、 $am + bn = d$ であれば、実は、 $(a + kn)m + (b - kn)n = d$ も、もちろん成立するし、実は、この形しか存在しない。

よって、一つの組が発見できれば、この a, b の組を探すという問題は、全部解けたようなものである。

5 整数係数不定方程式とユークリッドの互除法

ここでは、 $an + bm = k$ の形をした不定方程式⁷の整数解について考える。

ただし、 m, n, k に関しては、具体的に、整数値が与えられており、この方程式を満す、 a, b 組を探すという問題である。

⁷方程式には、解が有限個ではなく、無数(無限個)にある場合がある。そのような場合、その方程式は不定方程式と呼ばれる。もちろん、不定だからといって、任意の数でよいという意味ではない(方程式を満さない、数の組もある..)。また、方程式自身の解が無限にあっても、解の取り得る範囲を限定することにより、解の集合が有限になることも在り得る。

5.1 $an + bm = 1$ の整数解

$a13 + b20 = 1$ を満す整数解を求めるとい問題を考える。これは前章で示した問題 (d を m, n で表す為、その係数 a, b を探す) と良く似ている。

しかし、前章では、 $an + bm = d$ という形というだけでなく、 d が、 m, n の最大公約数という限定がついている場合であり、もちろん、 $an + bm = k$ の k が、最大公約数になっているという保証はない。

したがって、この問題に、前回の手法を適用してよいか? という疑問が生じる。

ところが、次の事実がある。

定理 3 m, n の最大公約数を d とすると、勝手な $a, b \in \mathbb{Z}$ に対して、 $am + bn$ は、 d の倍数になる。

すなわち、 $a13 + b20 = 1$ を満す a, b が存在すると仮定すると、実は、この左辺は、13 と 20 の最大公約数の倍数になる。ところが、これが左辺の 1 に等しいということになるわけだから、13 と 20 の最大公約数は、1 の約数でなければならない (1 は最大公約数の倍数なので..)。しかし、1 の約数は 1 自身しかないので、結局、13 と 20 の公約数は、1 である⁸ことが解る。

したがって、このような問題を解く場合にもユークリッドの互除法が利用できることになる。

5.2 $an + bm = k (k \neq 1)$ の整数解

前節では、 $k = 1$ の場合の解法について述べた。 $k = 1$ の場合は、自動的に m, n の最大公約数が 1 になるため、前章の手段が適用できたが、今度は、その保証がない。

勿論、たまたま、 m, n の最大公約数 d と k が一致すれば、前章の方法で解くことができるわけであるが、もし、 k が d と一致しない場合は、問題である。

ところが、繰り返すようであるが、 k は d の倍数である。すなわち、 $k = ud$ となる整数 u が存在するわけである。

すると、今、 m, n が与えられていると、前章の議論から、ユークリッドの互除法を用いて、 $a'm + b'n = d$ となる整数 a', b', d が得られる。そこで、この式の両辺を u 倍すれば、 $ua'm + ub'n = ud = k$ となるので、結局、この結果得られた ua' が a 、 ub' が b となり、 a, b をやはり、ユークリッドの互除法で求めることができる。

⁸つまり、互いに素である。このように、もし、二つの整数 m, n に対して、ある整数 a, b が存在し、 $am + bn = 1$ となれば、自動的に、 m, n の最大公約数が 1 となり、 m と n は互いに素となる。もちろん、 a, b も互いに素になるということは言うまでもない。

6 おまけ

定理 4 $((m, n) = d \Leftrightarrow (2^m - 1, 2^n - 1) = 2^d - 1)$ [証明] $m = n$ の時に成立するし、また、 $n = 0$ の時にも成立するので、ので、一般性を失わずに $m > n > 0$ の場合を示せばよい。

m に関する帰納法によって証明する。

$m = 2$ の時 $m > n$ となる n は 1 しかないが、これは、 $(m, n) = (2, 1) = 1$ であり、また、その一方 $(2^2 - 1, 2^1 - 1) = (3, 1) = 1 = 2^1 - 1$ なので成立。

$m = k + 1$ の時 $1 < m \leq k$ に関して、命題が成立するとして、 $m = k + 1$ の場合を示す。

今、 $m > n$ であるので、

$$2^m - 1 = 2^m - 2^{m-n} + 2^{m-n} - 1 = 2^{m-n}(2^n - 1) + (2^{m-n} - 1)$$

となる。したがって、

$$(2^m - 1, 2^n - 1) = (2^{m-n} - 1, 2^n - 1)$$

である。また、

$$(m, n) = (m - n, n)$$

ある。

一方、 $m - n$ も n も仮定より、 k 以下なので、帰納法の仮定より、

$$(2^{m-n} - 1, 2^n - 1) = 2^{(m-n, n)} - 1$$

以上により、

$$\begin{aligned} \text{左辺} &= (2^m - 1, 2^n - 1) \\ &= (2^{m-n} - 1, 2^n - 1) \\ &= 2^{(m-n, n)} - 1 \\ &= 2^{(m, n)} - 1 \end{aligned}$$

よって、

$$\text{左辺} = \text{右辺}$$

よって、与えられた等式は成立する。

よって、 $m = 2$ 時に成立し、 $m = k$ 以下で成立すると仮定して $m = k + 1$ の時にも成立することがわかったので、 m に関する帰納法により、与えられた命題は成立する。