$d = \gcd(n, m)$, $n > m$ のとき $\gcd(3m, n - m) = \gcd(3d, n - m)$ であることの証明

白石 啓一* 清水 共†

On a proof of $\gcd(3m, n - m) = \gcd(3d, n - m)$ where $d = \gcd(n, m)$, $n > m$

Keiichi SHIRAISHI Tomo SHIMIZU

Abstract

The purpose of this study is to prove "$\gcd(3m, n - m) = \gcd(3d, n - m)$ where $d = \gcd(n, m)$, $n > m$." The source of this problem is structure of a single-wall carbon nanotube. The problem is proved using properties of greatest common divisor. A numerical approach is shown to help students understanding the problem.

Keywords: Single-Wall Carbon Nanotube, Chiral Vector, Translational Vector, Greatest Common Divisor

1 はじめに

現代社会は，高度な情報機器であふれている．携帯電話を筆頭に，パソコンから生活家電製品，産業界から身近な個人生活環境に至るまで，ありとあらゆる分野に電子機器が投入されている．近年の産業界を牽引するキーワードは「ナノテクノロジー」である．1974 年に谷口紀男教授が，国際生産技術会議において「ナノテクノロジー」の概念を提唱して以来，様々な分野で基盤技術として研究・開発が進められている．特にエレクトロニクスにおいては，「ナノエレクトロニクス」として盛んに研究・開発されている．中でも注目される代表的素材の一つとして，1991 年に飯島澄男博士が発見した「カーボンナノチューブ (CNT)」があり，原子間力顕微鏡のカンチレバー，電子銃，電界効果トランジスタ等として将来の技術研究が続けられている．

最先端のデバイスとして用いられる CNT の電子状態を解析するためには，CNT の構造 (蜂の巣構造のように六方格子として炭素原子が配置した層状物質であるグラフェンを円筒状に丸めた立体構造) を取り入れた量子効果を過不足なく考慮する必要がある [1)]．この電子状態の解析において，初等的な代数学ないし数論を真面目に学んだ者には簡単に証明可能である「$d = \gcd(n, m)$, $n > m$ のとき $\gcd(3m, n-m) = \gcd(3d, n-m)$」の関係が利用されるが，CNT 分野の専門書で，この関係の証明が説明されていることは少ない．そこで，CNT 分野を研究する学生の一助として，また初等数学と最先端エレクトロニクスを結びつける一例として，本稿に証明を示す．

2 記法

$\gcd(a, b)$ 正整数 a, b の最大公約数 (GCD). $\gcd(a, b) = \gcd(b, a)$ である．

$a \mid b$ 正整数 a は，正整数 b を割り切る．つまり，$b = qa$ を満たす正整数 q が存在する．

$a \nmid b$ 正整数 a は，正整数 b を割り切れない．つま

*香川高等専門学校 詫間キャンパス 通信ネットワーク工学科
†香川高等専門学校 詫間キャンパス 電子システム工学科

り，$b = qa + r$, $0 < r < a$ を満たす，正整数 q, r が存在する．

3　最大公約数の性質

正整数 a, b を考えよう．$d' \mid a$ かつ $d' \mid b$ を満たす d' は a, b の公約数である．$a = qd'$ と表すと，$d' \leq qd' = a$ であるので，a の約数は有限個しか存在しない．したがって，a, b の公約数も有限個しか存在しない．その公約数の中で最大のものを最大公約数という．

$d = \gcd(a, b)$, $a > b$ とする．$c = a - b$ を考えると，d は a, b の約数なので，c の約数である．よって，d は b, c の公約数である．$d_1 = \gcd(c, b)$ とすると，

$$d \leq d_1 \tag{1}$$

となる．逆に，d_1 は b, c の約数なので，a の約数となる．よって，d_1 は a, b の公約数である．$d = \gcd(a, b)$ なので，

$$d_1 \leq d \tag{2}$$

となる．式 (1)，(2) より，$d = d_1$ が得られる．つまり，

$$\gcd(a, b) = \gcd(c, b) = \gcd(a - b, b) \tag{3}$$

である．

式 (3) を繰り返し使うと，

$$a = qb + r, \quad 0 \leq r < b$$

となる q, r が存在し，

$$\begin{aligned} \gcd(a, b) &= \gcd(a - b, b) = \gcd(a - 2b, b) \\ &= \cdots \\ &= \gcd(a - qb, b) = \gcd(r, b) \end{aligned}$$

となる．$r = 0$ ならば，$a = qb$ なので，$\gcd(a, b) = b$ である．$r > 0$ ならば，b を a に，r を b に置き直し，式 (3) を繰り返せば，最大公約数が得られる．

このように最大公約数を求める方法を「ユークリッドの互除法」という [2]．

4　単層ナノチューブの概形と問題の定式化

円筒形の層が 1 層のナノチューブを特に単層ナノチューブと呼ぶ．その円筒部はグラフェンを円筒状に巻いた状態にあり，その両端はキャップと呼ばれるフラーレンの半球で閉じている (図 1)．単層ナノチューブの軸方向に平行な線分 OB と，O, B を含み，線分 OB に垂直な (ナノチューブの赤道面に平行な) 面で切り開くと，図 2 が得られる．このとき，基準点 O は六方格子であるグラフェンの格子点に位置して，点 B は点 O から軸方向に延ばした直線が最初に通る格子点として決まる [3]．

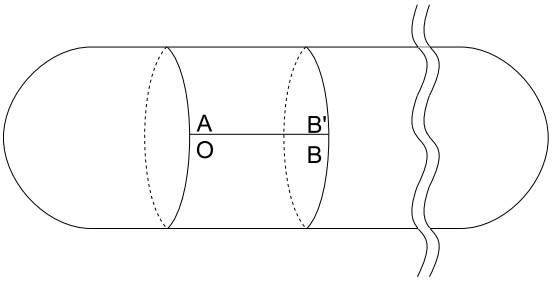

図 1　単層ナノチューブ概形 (Fig. 3.1[1] を参考に作成)

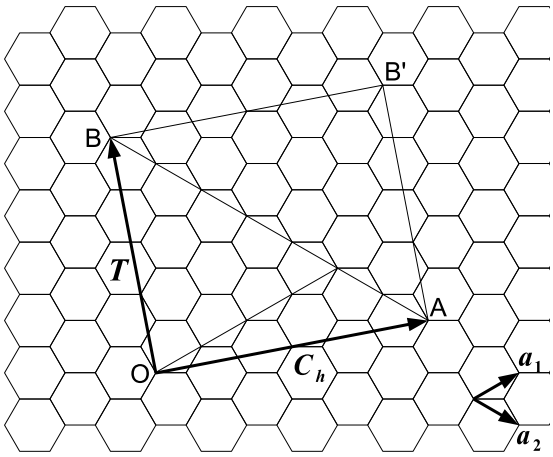

図 2　単層ナノチューブ展開図 (Fig. 3.2[1] を参考に作成, $\boldsymbol{C_h} = (4, 2)$, $\boldsymbol{T} = (4, -5)$)

チューブの構造は，$\vec{OA}$ で指定できる．$\vec{OA}$ を「カイラルベクトル $\boldsymbol{C_h}$」と呼ぶ．$\boldsymbol{C_h}$ を六方格子の基本格子ベクトル $\boldsymbol{a_1}, \boldsymbol{a_2}$ を用いて，

$$\boldsymbol{C_h} = n\boldsymbol{a_1} + m\boldsymbol{a_2} = (n, m)$$

(n, m は整数，$0 \leq |m| < n$) と表す．

$\vec{OB}$ を「並進ベクトル $\boldsymbol{T}$」と呼ぶ．T は，

$$\boldsymbol{T} = t_1\boldsymbol{a_1} + t_2\boldsymbol{a_2} = (t_1, t_2)$$

と表すことができる．ここで t_1, t_2 は互いに素 (最大公約数が 1) の整数である．t_1, t_2 は，$\boldsymbol{C_h} \cdot \boldsymbol{T} = 0$ より，

$$t_1 = \frac{2m + n}{d_R}, \quad t_2 = -\frac{2n + m}{d_R}$$

である．ここで，d_R は (2m+n) と (2n+m) の最大

公約数であり，ユークリッド則 (式 (3)) を用いれば，

$$\begin{aligned} d_R &= \gcd(2m+n, 2n+m) && (4)\\ &= \gcd(2m+n, n-m) && (5)\\ &= \gcd(3m, n-m) && (6)\\ &= \gcd(3d, n-m) && (7) \end{aligned}$$

である．したがって，

$$d_R = \begin{cases} d & (3d \nmid (n-m)) \\ 3d & (3d \mid (n-m)) \end{cases} \qquad (8)$$

である [1]．

式 (4)∼(6) の式変形は，

$$2n+m-(2m+n) = n-m$$

$$2m+n-(n-m) = 3m$$

より，明らかである．一方，式 (6)∼(7) の式変形，および，式 (8) は，式 (3) のみでは不明瞭である．

なお，m が負数の場合，最大公約数を求める対象が負数になることがある．その場合，絶対値を取った上で最大公約数を求めれば，十分である．

5 証明

正整数 n, m について，「$d = \gcd(n, m)$, $n > m$ のとき $\gcd(3m, n-m) = \gcd(3d, n-m)$」を証明する．

式 (3) より，

$$d = \gcd(n, m) = \gcd(n-m, m)$$

である．$n = ad$, $m = bd$, $\gcd(a, b) = 1$ を満たす，正整数 a, b が存在する．$\gcd(a, b)$ に対し，式 (3) を使うと，

$$\gcd(a, b) = \gcd(a-b, b) = 1 \qquad (9)$$

がいえる．

I. $3d \mid (n-m)$，つまり，$3 \mid (a-b)$ のとき
$n - m = (a-b)d = 3cd$ を満たす，正整数 c が存在する．
式 (9) より，$\gcd(3c, b) = 1$ なので，$\gcd(b, c) = \gcd(3, b) = 1$ である．したがって，

$$\begin{aligned} \gcd(3m, n-m) &= \gcd(3bd, 3cd) \\ &= 3d \end{aligned}$$

である．また，

$$\begin{aligned} \gcd(3d, n-m) &= \gcd(3d, 3cd) \\ &= 3d \end{aligned}$$

なので，$\gcd(3m, n-m) = \gcd(3d, n-m)$ である．

II. $3d \nmid (n-m)$，つまり，$3 \nmid (a-b)$ のとき
式 (9) より，

$$\begin{aligned} \gcd(3m, n-m) &= \gcd(3bd, (a-b)d) \\ &= d \end{aligned}$$

である．また，

$$\begin{aligned} \gcd(3d, n-m) &= \gcd(3d, (a-b)d) \\ &= d \end{aligned}$$

なので，$\gcd(3m, n-m) = \gcd(3d, n-m)$ である．

I, II より，正整数 n, m について，「$d = \gcd(n, m)$, $n > m$ のとき $\gcd(3m, n-m) = \gcd(3d, n-m)$」である．□

6 数値実験

正整数 n, m について，「$d = \gcd(n, m)$, $n > m$ のとき $\gcd(3m, n-m) = \gcd(3d, n-m)$」は，CNT 分野において瑣末な問題なので，CNT 分野を学ぶ者にとって，証明を完全に理解するより，この問題がある程度正しいと分かることが重要であろう．そこで，確認のための数値実験を行った．

次に示す手続きを踏めば，この問題が正しいことを示すことができる．

1. $n = 2, 3, \ldots$ について，2. を実行する．
2. $m = 1, 2, \ldots, n-1$ について，3.∼7. を実行する．
3. $d = \gcd(n, m)$
4. $d_1 = \gcd(3m, n-m)$
5. $d_2 = \gcd(3d, n-m)$
6. $3d \mid (n-m)$ の場合，
   (a) $3d = d_1 = d_2$ ならば，「OK」と出力する．
   (b) そうでなければ，「NG!」と出力し，終了する．
7. $3d \nmid (n-m)$ の場合，
   (a) $d = d_1 = d_2$ ならば，「OK」と出力する．
   (b) そうでなければ，「NG!」と出力し，終了する．

n, m に関し無限大まで計算し，すべての組み合わせで「OK」と表示されれば，この問題が正しいと示したことになるが，そのためには無限の時間が必要なので，実験できない (数学的証明は，強力である)．時間の許す限り計算すれば，この問題が，ある範囲の n, m について正しいと言える．

数式処理システム Risa/Asir を用いて実験した[1]．プログラムを図 3 に，実行用シェルスクリプトを図 4 に示す．なお，先にも述べたとおり，これは無限に続く処理なので，実験を適切な時間に収めるためにプログラムを停止する必要がある．CPU に Core i7(2.8GHz) を持つパーソナルコンピュータを用いて 29 分 41 秒実験したところ，「$n = 2, 3, \ldots, 21734, m = 1, 2, \ldots, n-1$」と「$n = 21735, m = 1, 2, \ldots, 10936$」に関し OK が表示され，この範囲で正しいことが示された．計算ログの一部を図 5 に示す．

7 おわりに

正整数 n, m について，「$d = \gcd(n, m)$, $n > m$ のとき $\gcd(3m, n-m) = \gcd(3d, n-m)$」を証明し，数値実験を行った．初等数学の問題なので，CNT 分野を研究する学生でも証明を理解できると考えられる．もし理解できなかったとしても，数値実験をとおし，題意の理解が進むと考えられる．

今後，本稿を CNT 分野を研究する学生向けの教材として利用し，理解度を確認していきたい．

謝辞

本校 情報工学科 奥山 真吾 准教授から証明に関するアドバイスをいただきました．ここに感謝の意を表します．

参考文献

1) R. Saito, G. Dresselhaus and M. S. Dresselhaus, Physical Properties of Carbon Nanotubes, Imperial College Press(1998)

2) 和田 秀男, 計算数学, 朝倉書店 (2000)

3) 齋藤 理一郎, 篠原 久典, カーボンナノチューブの基礎と応用, 培風館 (2004)

[1] n, m が CPU の整数レジスタに収まる範囲であれば，素の汎用プログラミング言語でも実装できる．ただし，GCD を求める関数を用意する必要がある．著者が Risa/Asir に慣れていたこと，Risa/Asir が多倍長整数を扱え，GCD を持っていることが，Risa/Asir を利用した理由である．多倍長整数により，時間さえかければ，非常に大きな整数について実験できる．

```
def
cnt()
{
  F = 0;
  for (N = 2; F == 0; N++)
    for (M = 1; M < N; M++) {
      D = igcd(N, M);
      D1 = igcd(3 * M, N - M);
      D2 = igcd(3 * D, N - M);
      if (irem((N - M) / D, 3) == 0) {
        if (3 * D == D1 && D1 == D2)
          MSG = "OK";
        else {
          MSG = "NG!";
          F = 1;
        }
      } else {
        if (D == D1 && D1 == D2)
          MSG = "OK";
        else {
          MSG = "NG!";
          F = 1;
        }
      }
      print(["n=", N, " m=", M,
             " d=gcd(n, m)=", D,
             " gcd(3m, n-m)=", D1,
             " gcd(3d, n-m)=", D2,
             MSG]);
    }
}

end$
```

図 3 確認プログラム (ファイル名:cnt.asir)

```
#!/bin/sh
LOG=‘date "+%Y%m%d%H%M%S"‘.log
asir 2>&1 > ${LOG} <<EOF
load("./cnt.asir");
cnt();
quit;
EOF
```

図 4 実行用シェルスクリプト

```
This is Risa/Asir + Interval Arithmetic, Version 20070806 (Plotting Group
 Distribution).
Copyright (C) 1994-2000, all rights reserved, FUJITSU LABORATORIES LIMITED.
Copyright 2000-2007, Risa/Asir committers, http://www.openxm.org/.
GC 6.8 Copyright 1988-2005, H-J. Boehm, A. J. Demers, Xerox, SGI, HP.
GP/PARI CALCULATOR Version 2.3.5 (released), Copyright (C) 2000-2005 The PARI Group.
[0] [2] [n=,2, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,3, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,3, m=,2, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,4, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,4, m=,2, d=gcd(n, m)=,2, gcd(3m, n-m)=,2, gcd(3d, n-m)=,2,OK]
[n=,4, m=,3, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,5, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,5, m=,2, d=gcd(n, m)=,1, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,5, m=,3, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,5, m=,4, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,6, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,6, m=,2, d=gcd(n, m)=,2, gcd(3m, n-m)=,2, gcd(3d, n-m)=,2,OK]
[n=,6, m=,3, d=gcd(n, m)=,3, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,6, m=,4, d=gcd(n, m)=,2, gcd(3m, n-m)=,2, gcd(3d, n-m)=,2,OK]
[n=,6, m=,5, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,7, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,7, m=,2, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,7, m=,3, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,7, m=,4, d=gcd(n, m)=,1, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,7, m=,5, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,7, m=,6, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,8, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,8, m=,2, d=gcd(n, m)=,2, gcd(3m, n-m)=,6, gcd(3d, n-m)=,6,OK]
[n=,8, m=,3, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,8, m=,4, d=gcd(n, m)=,4, gcd(3m, n-m)=,4, gcd(3d, n-m)=,4,OK]
[n=,8, m=,5, d=gcd(n, m)=,1, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,8, m=,6, d=gcd(n, m)=,2, gcd(3m, n-m)=,2, gcd(3d, n-m)=,2,OK]
[n=,8, m=,7, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,9, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,9, m=,2, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,9, m=,3, d=gcd(n, m)=,3, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,9, m=,4, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,9, m=,5, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,9, m=,6, d=gcd(n, m)=,3, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
[n=,9, m=,7, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,9, m=,8, d=gcd(n, m)=,1, gcd(3m, n-m)=,1, gcd(3d, n-m)=,1,OK]
[n=,10, m=,1, d=gcd(n, m)=,1, gcd(3m, n-m)=,3, gcd(3d, n-m)=,3,OK]
```

図 5 実行ログ (一部)