互除法の原理とオイラー関数の乗法性

この説明は高校生・中学生でも読めるように留意してあります。ただし一部で高校数学で習う内容が含まれるため、中学生には少し難しく思えるかもしれません。具体的に高校で習う内容とは「命題」分野“必要条件・十分条件・背理法・対偶”と「数列」の表記です。数列については数を表すのにそのような書き方をするぐらいの理解で問題はありません。例えば web サイト「ky の書架」の別ファイル「ウィルソンの定理の初等的証明」の 1 ページ目を参照して下さい。

それから「命題」についてですが、厳密な議論のためには確かに重要です。しかし細かいところは気にしないで、何となくこんな感じ、で済ませておくというのも一つの勉強法です。特に「定理 1 の証明に移る前に・・」で説明してある手順が感覚的にとらえられれば、近い将来、厳密な証明をきちんと理解できるはずです。

ここでは数論初学者が初期段階に学習するオイラー関数 $\varphi(n)$ について、$\varphi(n)$ が乗法的関数であること、およびその帰結として得られる基本性質の解説をする。

(定義)

正の整数 n に対して、1 から n までの n 個の整数のうちで n と互いに素であるものの個数を対応させた関数をオイラー(のファイ)関数といい $\varphi(n)$ で表す。

注）a と b の最大公約数が 1 であることを「a, b は互いに素」という。

例) $\varphi(1)=1$, $\varphi(2)=1$ である。また 1 から 10 のうちで 10 と互いに素であるものは 1, 3, 7, 9 の 4 数なので $\varphi(10)=4$ である。なお素因数分解形との一般的な関係は最後の方で述べるが、素数 p について $\varphi(p)=p-1$ であることは容易に分かる事実である。

オイラー関数 $\varphi(n)$ については興味深いいくつかの事実があるが、本講の大きな目的の一つは次の定理 1 を証明することである。

(定理 1)

オイラー関数 $\varphi(n)$ は乗法的関数である。すなわち任意の互いに素な正整数 a, b について

$$\varphi(ab)=\varphi(a)\varphi(b)$$

が成り立つ。

これについては既にいろいろな証明法が提示されているが、今回はその中でも、乗法性が成り立つ仕組みをより直感的に示してくれると思われる「ユークリッドの互除法の原理」を用いた証明を試みることとする。それでは順番に必要となるいくつかの概念を確認してみよう。

ユークリッドの互除法の原理

（補助定理 1）
$a = rb + c$（r は整数かつ a, b, c は正の整数）であるとき、a, b の最大公約数と b, c の最大公約数は一致する。

(証明)[*1]
g は a, b の公約数とする。$a = xg$, $b = yg$ と表せるが、このとき $a = rb + c$ は
$$xg = ryg + c,\ c = (x - ry)g$$
すなわち g は c の約数であって、b, c の公約数でもある。
次に g' は b, c の公約数とする。$b = zg'$, $c = wg'$ と表せて、
$$a = rzg' + wg',\ a = (rz + w)g'$$
すなわち g' は a, b の公約数でもある。
以上より a, b の公約数の集合と b, c の公約数の集合は一致する。また 2 つの集合はともに有限個の要素からなり、最大元が存在する。よって a, b の最大公約数と b, c の最大公約数は一致する。
補）ユークリッドの互除法とはまさにこの補助定理 1 の示す事実を用いた計算に他ならない。
例えば 2 数 1037, 323 について
$$1037 = 323 \times 3 + 68\ ,\ 323 = 68 \times 4 + 51\ ,\ 68 = 51 \times 1 + 17$$
であることから、x, y の最大公約数を $\gcd(x, y)$ と表すことにして
$$\gcd(1037, 323) = \gcd(323, 68) = \gcd(68, 51) = \gcd(51, 17) = 17$$
となる。

さらに必要となる 2 つの定理

「互除法の原理」に加えて定理 1 の証明では次の 2 つの補助定理が活躍する。

（補助定理 2）
整数 a, b はともに 2 以上で定数とする。この a, b について、正の整数 n を
$$n = ap + r\ ,\ n = bq + s\ (p, q, r, s \text{ は整数かつ } 1 \leqq r \leqq a\ ,\ 1 \leqq s \leqq b)$$
と表したときの r と s の組 (r, s) を考え、それを A_n とする。このとき互いに素である(2 以上の任意定数)a, b に対して A_1, A_2, A_3, $\cdots$, A_{ab} の ab 個はすべて異なる組であり、特に (r, s) $(1 \leqq r \leqq a, 1 \leqq s \leqq b)$ の一つ一つがちょうど一度ずつ現れる。

注）n が a で割り切れないとき r は n を a で割った余りに他ならない。また割り切れるときの余りは 0 であるが、ここではこの余りをそのまま使わず、後の証明のため $r = a$ と定めている。s についても同様である。なお n に対しての余りは一意的(ただ一つ定まる)なので (r, s) も一意的である。

[*1] この部分は拙著『大学入試「整数問題」の類型とその解法』からの抜粋です。

例）例として $a=3\,,\,b=4$ を最初に与える。次の表より $A_1 \sim A_{12}$ がすべて異なる組であることが分かる。

n	1	2	3	4	5	6	7	8	9	10	11	12
r	1	2	3	1	2	3	1	2	3	1	2	3
s	1	2	3	4	1	2	3	4	1	2	3	4

実際 $A_1=(1\,,\,1)\,,\,A_2=(2\,,\,2)\,,\,A_3=(3\,,\,3)\,,\,A_4=(1\,,\,4)\,,\,A_5=(2\,,\,1)\,,\,A_6=(3\,,\,2)\,,$
$A_7=(1\,,\,3)\,,\,A_8=(2\,,\,4)\,,\,A_9=(3\,,\,1)\,,\,A_{10}=(1\,,\,2)\,,\,A_{11}=(2\,,\,3)\,,\,A_{12}=(3\,,\,4)$
であり、同じ組は現れない。なお、3 で割った余りは $0\,,\,1\,,\,2$（→ 順に $r=3\,,\,1\,,\,2$）の 3 通りで、4 で割った余りは $0\,,\,1\,,\,2\,,\,3$（→ 順に $s=4\,,\,1\,,\,2\,,\,3$）の 4 通りなので、ありうる $(r\,,\,s)$ は $3\times4=12$ 組である。いわゆる鳩の巣原理であるが、この 12 組が $A_1 \sim A_{12}$ として一度ずつ現れている。この性質はオイラー関数の乗法性の証明で重要になる。

さて、例) では $a=3\,,\,b=4$ としたが、どのような(条件に合う) $a\,,\,b$ から出発しても同様のことが起こるというのが補助定理 2 の主張である。

(補助定理 2 の証明)

$1\leqq x\leqq y\leqq ab$ $\cdots$① である $x\,,\,y$ について、A_x と A_y は同じ組とする。このときある整数 $p\,,\,p'\,,\,q\,,\,q'\,,\,r\,,\,s$ $(1\leqq r\leqq a\,,\ 1\leqq s\leqq b)$ について

$$x=ap+r=bp'+s\ ,\ y=aq+r=bq'+s$$

であって $y-x=a(q-p)$ かつ $y-x=b(q'-p')$ である。よって $y-x$ は a の倍数かつ b の倍数であって、$a\,,\,b$ が互いに素であることから $y-x$ は ab の倍数である。ところが①より $0\leqq y-x\leqq ab-1$ なので $y-x=0\,,\,y=x$ である。

以上より $1\leqq x<y\leqq ab$ であるすべての $x\,,\,y$ について $A_x\,,\,A_y$ が異なる組であることが示されたが、これから $A_1,\,A_2\,,\,\cdots\,,\,A_{ab}$ はすべて異なる ab 組である。一方で $(r\,,\,s)$ としてありうるのは定義から ab 個であるので、この一つ一つがちょうど 1 度ずつ $A_1\,,\,A_2\,,\,\cdots\,,\,A_{ab}$ において現れることが分かる。

注 1）前半で示したのは「$A_x=A_y$ ならば $x=y$」が成り立つことである。そしてこの対偶が「$x\neq y$ ならば $A_x\neq A_y$」であり、いわゆる対偶証明法を用いている。

注 2)「$a\,,\,b$ は互いに素で n は a の倍数かつ b の倍数ならば n が ab の倍数である」ことは素因数分解形を考えれば直感的である。ただし多くの書物では以下のように説明されている。すなわち $a\,,\,b$ が互いに素であるとき、ある整数 $x\,,\,y$ が存在して $ax+by=1$[*2]である。これから $anx+bny=n\cdots(*)$ であるが、n が a の倍数かつ b の倍数であるとき、やはりある整数 $a'\,,\,b'$ について $n=aa'=bb'$ であって $(*)$ は $abb'x+baa'y=n\,,\,ab(b'x+a'y)=n$ となり n が ab の倍数であることが分かる。

(補助定理 3)

互いに素な整数 $a\,,\,b$ と整数 n について

「$a\,,\,n$ は互いに素かつ $b\,,\,n$ は互いに素 $\Longleftrightarrow$ ab と n は互いに素」

[*2] これについても脚注*1 で触れた書に説明があります。

素因数分解形を考えればやはり直感的な定理なので、問題なしと思う人は証明を跳ばしてくれて構わないだろう。

注)「$p \Longleftrightarrow q$」は「p ならば q」と「q ならば p」がどちらも成り立つことを表す記号である。さらにこのとき 2 つの条件 p, q は同値という。

(証明) 以下では文字はすべて整数である。

$\Longleftarrow$) 対偶を示す。a, n が互いに素でないとすると、ある 2 以上の整数 g が存在して $a = a'g$, $n = n'g$ と表される。このとき $ab = a'gb$ であって g は ab, n の公約数である。すなわち ab と n は互いに素ではない。b, n が互いに素でないときも同様で、対偶が真であることが分かる。

$\Longrightarrow$) 背理法による。

a, n は互いに素かつ b, n は互いに素で、ab と n は互いに素ではないとする。a, n が互いに素であることから $nx + ay = 1$ を満たす整数 x, y が存在し[*2] $bnx + bay = b \cdots$① である。ところで ab と n は互いに素でないので 2 以上のある整数 g について $ab = cg$, $n = dg$ である。これを①に代入して $bdgx + cgy = b$, $(bdx + cy)g = b$ より g は b の約数であるが、このとき b, n が 2 以上の公約数 g をもつことになり、b, n が互いに素である条件に反して不合理である。

定理 1 の証明に移る前に‥‥

以下の説明は蛇足という気もするが、具体例を挙げて概念の確認をしておく。$a = 9$, $b = 10$, $ab = 90$ について考えよう。この場合 $\varphi(ab)$ は $1 \sim 90$ の 90 個の数のうちで 90 と互いに素であるものがいくつあるかを表す。これは n $(1 \leqq n \leqq 90)$ のそれぞれと 90 との最大公約数を求めることで解決する。ここで補助定理 3 よりその最大公約数が 1 であることは n と a, b との最大公約数がいずれも 1 であることに他ならない。そして補助定理 1 より、この 2 つの最大公約数が 1 かそうでないかは、補助定理 2 で定義された $A_n = (r\,,\, s)$ においての r, s が鍵を握っている。(ユークリッドの互除法とはまさにこの最大公約数を求める方法であった。)

$n = 67$ について $a(= 9)$, $b(= 10)$ で割った余りはそれぞれ 4, 7 で $A_{67} = (4\,,\, 7)$

↓

$r = 4$ と $a = 9$ は互いに素で $s = 7$ と $b = 10$ も互いに素

↓

したがって $n = 67$ と $ab = 90$ は互いに素

それに対して $n = 50$ については以下のようになる。

$n = 50$ について $a(= 9)$, $b(= 10)$ で割った余りはそれぞれ 5, 0 で $A_{50} = (5\,,\, 10)$

↓

$r = 5$ と $a = 9$ は互いに素であるが $s = 10$ と $b = 10$ は互いに素でない

↓

したがって $n = 50$ と $ab = 90$ は互いに素でない

この流れで各 n を考えてゆくのだが a と互いに素である r の個数が $\varphi(a)$ であり、b と互いに素である s の個数が $\varphi(b)$ なので、補助定理 2 を用いれば定理 1 が成り立つことは問題ないであろう。(さらに蛇足であるが、右の表を参考にされたし。)

$r \diagdown s$	①	2	③	4	5	6	⑦	8	⑨	10
①	①	82	⑬	64	55	46	㊲	28	⑲	10
②	⑪	2	㊸	74	65	56	㊼	38	㉙	20
3	21	12	3	84	75	66	57	48	39	30
④	㉛	22	⑬	4	85	76	㊼	58	㊾	40
⑤	㊶	32	㉓	14	5	86	㊼	68	㊾	50
6	51	42	33	24	15	6	87	78	69	60
⑦	㊶	52	㊸	34	25	16	⑦	88	㊾	70
⑧	㊶	62	㊸	44	35	26	⑰	8	㊾	80
9	81	72	63	54	45	36	27	18	9	90

定理 1 の証明

それでは一つの目標を達成しよう。まず $\varphi(1)=1$ であった。したがって $a=1$ または $b=1$ のときは $\varphi(ab)=\varphi(a)\varphi(b)$ である。

$a\geqq 2\,,\ b\geqq 2$ のとき。A_n は補助定理 2 の定義に従うとして、補助定理 3 および補助定理 1 より以下の同値関係が成り立つ。

$$\begin{aligned} &n\,,\ ab \text{ は互いに素} \iff n\,,\ a \text{ は互いに素かつ } n\,,\ b \text{ は互いに素} \\ &\qquad\qquad \iff A_n=(r\,,\ s) \text{ について } r\,,\ a \text{ は互いに素かつ } s\,,\ b \text{ は互いに素} \end{aligned}$$

これと補助定理 2 から $(r\,,\ s)$ $(1\leqq r\leqq a\,,\ 1\leqq s\leqq b)$ の ab 個の中で $r\,,\ a$ が互いに素かつ $s\,,\ b$ が互いに素であるものの個数が $\varphi(ab)$ であるが、$r=1\,,\ 2\,,\ 3\,,\ \cdots\,,\ a$ のうち a と互いに素であるものは $\varphi(a)$ 個で、$s=1\,,\ 2\,,\ 3\,,\ \cdots\,,\ b$ のうち b と互いに素であるものは $\varphi(b)$ 個であることから $\varphi(ab)=\varphi(a)\varphi(b)$ が導かれる。　□◪

素因数分解形と $\varphi(n)$

定理 1 の帰結として定理 2(2)が得られる。これを示すことも本講の目的の一つである。

(定理 2)

オイラー関数 $\varphi(n)$ について以下が成り立つ。

(1) 2 以上の整数 n の素因数分解が $n=p^m$ であるとき $\varphi(n)=p^m-p^{m-1}=n\Big(1-\dfrac{1}{p}\Big)$

(2) 2 以上の整数 n の素因数分解が $n=p_1^{m_1}p_2^{m_2}p_3^{m_3}\cdots p_l^{m_l}$ であるとき

$$\begin{aligned}\varphi(n)&=(p_1^{m_1}-p_1^{m_1-1})(p_2^{m_2}-p_2^{m_2-1})(p_3^{m_3}-p_3^{m_3-1})\cdots(p_l^{m_l}-p_l^{m_l-1})\\&=n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\Big(1-\frac{1}{p_3}\Big)\cdots\Big(1-\frac{1}{p_l}\Big)\end{aligned}$$

(証明)

(1) $1\,,\ 2\,,\ 3\,,\ \cdots\,,\ p^{m-1},\ p^m$ のうち p^m と互いに素でないものは p の倍数で $p\times 1\,,\ p\times 2\,,\ \cdots\,,\ p\times p^{m-1}$ の p^{m-1} 個である。

$$\therefore\ \varphi(p^m)=p^m-p^{m-1}=p^m\Big(1-\frac{1}{p}\Big)=n\Big(1-\frac{1}{p}\Big)$$

(2) $p_1\,,\ p_2\,,\ p_3\,,\ \cdots\,,\ p_l$ がすべて異なる素数であるとき $i=1\,,\ 2\,,\ \cdots\,,\ l-1$ のそれぞれに対して $p_i^{m_i}$ と $p_{i+1}^{m_{i+1}}p_{i+2}^{m_{i+2}}\cdots p_l^{m_l}$ は互いに素である。したがって定理 1 を繰り返し用いて

$$\begin{aligned}\varphi(p_1^{m_1}p_2^{m_2}\cdots p_l^{m_l})&=\varphi(p_1^{m_1})\varphi(p_2^{m_2}p_3^{m_3}\cdots p_l^{m_l})=\varphi(p_1^{m_1})\varphi(p_2^{m_2})\varphi(p_3^{m_3}p_4^{m_4}\cdots p_l^{m_l})\\&=\cdots\cdots=\varphi(p_1^{m_1})\varphi(p_2^{m_2})\varphi(p_3^{m_3})\cdots\varphi(p_{l-1}^{m_{l-1}}p_l^{m_l})\\&=\varphi(p_1^{m_1})\varphi(p_2^{m_2})\varphi(p_3^{m_3})\cdots\varphi(p_{l-1}^{m_{l-1}})\varphi(p_l^{m_l})\end{aligned}$$

である。さらに(1)で示したことから

$$\begin{aligned}&\varphi(p_1^{m_1}p_2^{m_2}\cdots p_l^{m_l})\\&\quad=(p_1^{m_1}-p_1^{m_1-1})(p_2^{m_2}-p_2^{m_2-1})(p_3^{m_3}-p_3^{m_3-1})\cdots(p_l^{m_l}-p_l^{m_l-1})\\&\quad=p_1^{m_1}p_2^{m_2}\cdots p_l^{m_l}\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\Big(1-\frac{1}{p_3}\Big)\cdots\Big(1-\frac{1}{p_l}\Big)\\&\quad=n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\Big(1-\frac{1}{p_3}\Big)\cdots\Big(1-\frac{1}{p_l}\Big)\end{aligned}$$

（補足）

ここでは $\varphi(n)$ が乗法的関数であることを示しそれから定理 2 を導いたが、逆順での説明も可能である。例えば定理 2(2)が成り立つことは l 個の集合の和集合 $\mathrm{P}_1 \cup \mathrm{P}_2 \cup \cdots \cup \mathrm{P}_l$ の要素の個数を表す式との対応で示すことができて、得られる関係式のもつ意味は直感的になる。

2009.12/27

「ky の書架」（http://kynoshoka.com/）

web サイト「ky の書架」にはこれ以外にも「ウィルソンの定理の初等的証明」・「大学入試の整数問題」などのファイルがあります。興味のある方は url を直接入力するか、サイト名で google 検索してアクセスして下さい。（yahoo 検索ではヒットしないかもしれません。）