小山工業高等専門学校研究紀要
第 37 号（2005）65 － 70

ある種の整数係数多項式の可約性について1

ある多項式の可約性について(1)

河 島　博
Hiroshi KAWASHIMA

1．はじめに

整数係数の２次方程式の根を調べる問題で定数項だけ書き損じたのに，やはり有理数の根を持つことから，次の問題を得ることが出来た。

[問題] $y=f(x)\equiv 6x^2+11x+k$(但しkは正の整数)が可約になるのは，kがどんな値のときか。
[解答] $D=11^2-4\times 6\times k=121-24k$
であるから，
k=1,2,3,4,5を代入して見ると
k=１のとき，D=121-24=97で不可。
k=２のとき，D=121-48=73で不可。
k=３のとき，D=121-72=49=7^2で可。
実際　$y=6x^2+11x+3=(2x+3)(3x+1)$
k=４のとき，D=121-96=25=5^2で可。
実際　$y=6x^2+11x+4=(2x+1)(3x+4)$
k=５のとき，D=121-120=1=1^2で可。
実際　$y=6x^2+11x+5=(x+1)(6x+5)$
〈注：この結果は後で活用する。〉

(Ⅰ)次の定理がこの論文の出発点となる。

[定理１.Ⅰ.1]　$f(x)\equiv px^2+bx+k$（但しpは素数，bは整数，kは正の整数）は，
$|b|\leqq p$のとき，どんなkに対しても，この２次式f(x)は既約である。
[証明]まず(ⅰ)b=０のときを考えると，
$f(x)=px^2+k=0$ は$x=\pm\sqrt{-\frac{k}{p}}=\pm\sqrt{\frac{k}{p}}$ iとなるから，
定理は正しい。

(ⅱ)b＞０のときを考え，f(x)が可能だと矛盾が出ることを言う。

ガウスの定理〈注：文献[１]の定理18.2(P.66)〉により，もし有理数係数の多項式で因数分解可能であるならば，
$px^2+bx+k=(x+k_1)(px+k_2)$
とかける。(但しk_1，k_2は正の整数)
右辺$=px^2+(pk_1+k_1)x+k_1k_2$
であるから
$b=pk_1+k_2\geqq p\cdot 1+1=p+1$
となり矛盾である。
(ⅲ)b＜０のとき、f(x)が可約だと
$px^2+bx+k=(x+k_1)(px+k_2)$
とかけるから(但しk_1，k_2は負の整数)
$b=pk_1+k_2\leqq p(-1)+(-1)=-(p+1)$
となり矛盾である。[了]
〈注：この[定理１.１]から，判別式$D=b^2-4pk$は正の大部分は平方数にならない。
つまりk=１,２,３,…,n,…とkを動かしたとき，有限個を除いたD＜０で，D＞０のときはDは平方数にはならない。〉

[定理１.Ⅰ.２]　$f(x)\equiv px^2+bx+k$(但しpは素数，bは整数，kは正の整数)において，
|b|≧p+1であるならば，kを適当に選ぶと，
f(x)は可約になる。
[証明]（ⅰ）$b\geqq p+1$のとき
$f(-1)=p-b+k\equiv 0$とすると，
$k=b-P\geqq 1$よりよい。
(ⅱ)$b\leqq -(p+1)$のとき
$f(1)=p+b+k\equiv 0$とすると、
$k=(-b)-p\geqq(p+1)-p=1$よりよい。[了]

この[定理１.Ⅰ.１]，[定理１.Ⅰ.２]により，次の[定理１.３]が言える。

[定理１.Ⅰ.３]　$f(x)\equiv px^2+bx+k$（但しpは素数，bは整数，kは正の整数）において，次の事実が成り立つ。

(ⅰ) f(x)が既約⇔$|b|\leqq p$

(ⅱ) f(x)が可約⇔$|b|\geqq p+1$

〈注：(ⅱ)が成り立つ事は簡単に分る。(例えばb＞0のときを考えて)，それの否定命題が(ⅰ)だからよい。〉

(Ⅱ) 次に，$g(x)\equiv pqx^2+bx+k$（但しp，qは相異なる素数，b，kは正の整数）として，その可約の必要条件を求めて見ると，

(ⅰ) $g(x)=(px+k_1)(qx+k_2)$のときは，

$b=pk_2+qk_1$，　$k=k_1k_2$となる。

このときは，

$b\geqq p\cdot 1+q\cdot 1=p+q\Rightarrow b\geqq p+q$　　(イ)

(ⅱ) $g(x)=(x+k_1)(pqx+k_2)$のときは，

$b=pqk_1+k_2$，$k=k_1k_2$となる。

このときは，

$b\geqq pq\cdot 1+1=pq+1\Rightarrow b\geqq pq+1$　　(ロ)

所が$(pq+1)-(p+q)=(p-1)(q-1)\geqq 2$より，(ロ)の下限の方が(イ)の下限より大きいことが解る。

つまり，

$b<p+q\Leftrightarrow b\leqq p+q-1$ならば可約でないことが解った。

まとめて

[定理１.Ⅱ.１]　$g(x)\equiv pqx^2+bx+k$（但しp，qは相異なる素数，bは整数，kは正の整数）は，

$|b|\leqq p+q-1$であるならば，どんなkに対してもg(x)は概約である。

〈注：b＜0のときは$X\equiv -x$として，$G(X)=g(-x)=pqx^2+(-b)x+k$を考えればよい。〉

更に，$g(x)\equiv pqx^2+bx+k$（但しp，qは相異なる素数，b，kは正の整数）の可約の十分条件を考えて見る。

$b\geqq pq+1$だと

$g(-1)=pq-b+k\equiv 0$として

$k=b-pq\geqq 1$で可約である。

つまり，これはCase(ⅱ)の可約の必要十分条件である。

また，b=p+qのときは，可約でk=1と取れるが，これはCase(ⅰ)のときのみ可能である。

まとめて

[定理１.Ⅱ.２]　$g(x)\equiv pqx^2+bx+k$（但しp，qは相異なる素数，bは整数，kは正の整数）において

Case(ⅱ)の可約⇔$|b|\geqq pq+1$

Case(ⅱ)の既約⇔$|b|\leqq pq$

また，$b=\pm(p+q)$のときは，Case(ⅰ)のみが可約である。

〈注１：$pq-(p+q)=(p-1)(q-1)-1\geqq 2-1=1$〉

〈注２：b=p+qのときk=1の上記の注意から

$D=b^2-4pqk$はk≧２のとき非平方数である。〉

ここで，更に[定理１.Ⅱ.２]の$|b|\geqq pq+1$の場合のCase(ⅰ)の解の個数の評価を与える[定理１.Ⅱ.３]を与える前に，次の補助定理を証明することにする。

[補助定理]　$px+qy=r$（但しp，qは相異なる素数，rは正の整数）の正の整数解の組は

$mpq<r\leqq(m+1)pq$（但しmは１以上の整数）とすれば，m個以上かつ(m+1)個以下である。

[証]　与式の1つの解を(x_0,y_0)，一般の解を(x,y)とする。

$$\begin{cases} px+qy=r & \text{(イ)} \\ px_0+qy_0=r & \text{(ロ)} \end{cases}$$

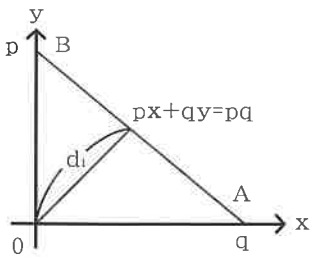
(イ)-(ロ)により

$p(x-x_0)+q(y-y_0)=0\Leftrightarrow$

$t\equiv \dfrac{x-x_0}{-q}=\dfrac{y-y_0}{p}$ として

$x=x_0-qt$，$y=y_0+pt$とかける。

(注：tは(x,y)と共に動く整数である。)



(イ)を標準形に直せば

$$\frac{p}{\sqrt{p^2+q^2}}x+\frac{q}{\sqrt{p^2+q^2}}y=\frac{r}{\sqrt{p^2+q^2}}\equiv d\text{として}\quad(ハ)$$

$$\frac{p}{\sqrt{p^2+q^2}}x+\frac{q}{\sqrt{p^2+q^2}}y=\frac{pq}{\sqrt{p^2+q^2}}\equiv d_1\text{として}\quad(ニ)$$

と比較して，(ハ)は(ニ)に対してm倍より大きく，(m+1)倍以下である。〈注：r=pqのときは，(イ)の第１象限切片線分が$\overline{AB}$に一致し，両端は(q,0)，(p,0)で，共に正の整数解の組ではない。〉
これにより確かに言えた。[了]
〈注１：2x+3y=11のときは正の整数解９組は，2×1+3×3=11，2×4+3×1=11より(1,3),(4,1)の2組で[問題]の結論と一致する。〉
〈注２：2x+3y=7のときは，2×2+3×1=7で(2,1)の1組しかない。〉
〈注３：整数係数の２次式$f(x)\equiv ax^2+bx+k$（但しa，kは正とする）は，$D=b^2-4ak$により可約な方程式の組は有限で，$k\leqq\frac{b^2}{4a}$で,その個数は評価される。〉
[定理１.Ⅱ.３] $g(x)\equiv pqx^2+bx+k$（但しp,qは相異なる素数，bは整数，kは正の整数変数）は$mpq<b\leqq(m+1)pq$（但しmは１以上の整数）のとき，(ｉ)型の可約方程式をm個乃至(m+1)個を，(ii)型の可約方程式を１個を持つ。
〈注：上記の2つの定理・補助定理より明らかである。〉

2.二項多項式

二項多項式　$f(x)\equiv x^n+k$（但しkは正の整数変数）の因数分解を考えよう。(但しnは２以上の整数)
$n=2$のとき$f(x)=x^2+k=0\Leftrightarrow x^2=-k\Leftrightarrow x=\pm\sqrt{-k}=\pm\sqrt{k}i$より，これは既約である。
$n=2m+1$(mは１以上の整数)のとき，$k=a^{2m+1}$とおけば(但しaは正の整数)
$f(x)=x^{2m+1}+a^{2m+1}=x^{2m+1}-(-a)^{2m+1}$
$=(x+a)\{x^{2m}-x^{2m+1}a+x^{2m+2}a^2+\cdots+(-a)^{2m}\}$で可約である。
$n=4$のとき
$x^4+a^4=(x^2+a^2)^2-2a^2x^2=\{(x^2+a^2)+\sqrt{2}ax\}\times\{(x^2+a^2)-\sqrt{2}ax\}$であるから，
ここで$a\equiv\sqrt{2}b$として
$x^4+4b^4=(x^2+2bx+2b^2)(x^2-2bx+2b^2)$
つまり，$k\equiv 4b^4$（但しbは正の整数）として
$f(x)\equiv x^4+4b^4$は可約である。
$n=6$のときは
$X^3+a^3=(X+a)(X^2-aX+a^2)$で，
$X=x^2$，$a=b^2$とおくと
$x^6+b^6=(x^2+b^2)(x^4-b^2x^2+b^4)$
で可約である。（但し，bは正の整数）
一般に$n=2^{\ell}\times(2m+1)$のときは$(\ell,m\geqq 1)$
$X^{2m+1}+A^{2m+1}=(X+A)\{X^{2m}-AX^{2m-1}+A^2X^{2m-2}-\cdots+(-1)^rA^rX^{2m-r}+\cdots+A^{2m}\}$
において，$X\equiv x^{2^{\ell-2}}$，$A\equiv a^{2^{\ell}}$を代入して
$x^n+a^n=(x^{2^{\ell}}+a^{2^{\ell}})\{(x^{2^{\ell}})^{2m}-a^{2^{\ell}}(x^{2^{\ell}})^{2m-1}+(a^{2^{\ell}})^2\times(x^{2^{\ell}})^{2m-2}-\cdots+(-1)^r(a^{2^{\ell}})^r(x^{2^{\ell}})^{2m-r}+\cdots+(a^{2^{\ell}})^{2m}\}$
で，やはり可約である。
また，$n=2^{\ell}$（ℓは３以上の整数)の時は
$X^4+4A^4=(X^2+2AX+A^2)(X^2-2AX+A^2)$
において，
Case(ｉ)　$n=2^{2m}=4^m$(mは１以上の整数)
では$X\equiv x^{4^{m-1}}$，$A\equiv a^{4^{m-1}}$として
$(x^{4^{m-1}})^4+4(a^{4^{m-1}})^4=\{(x^{4^{m-1}})^2+2(a^{4^{m-1}})x^{4^{m-1}}+(a^{4^{m-1}})^2\}\{(x^{4^{m-1}})^2-2a^{4^{m-1}}x^{4^{m-1}}+(a^{4^{m-1}})^2\}\Leftrightarrow$
$x^n+4a^n=x^{4^{m-1}\times 4}+4a^{4^{m-1}\times 4}=(x^{4^{m-1}\times 2}+2a^{4^{m-1}}\times x^{4^{m-1}}+a^{4^{m-1}\times 2})(x^{4^{m-1}\times 2}-2a^{4^{m-1}}x^{4^{m-1}}+a^{4^{m-1}\times 2})\Leftrightarrow$
$x^n+4a^n=x^{4^m}+4a^{4^m}=x^{2^{2m}}+4a^{2^{2m}}=(x^{2^{2m-1}}+2a^{2^{2m-2}}\times x^{2^{2m-2}}+a^{2^{2m-1}})(x^{2^{2m-1}}-2a^{2^{2m-2}}x^{2^{2m-2}}+a^{2^{2m-1}})$
で可約である。

Case(ⅱ)$n=2^{2m+1}$(mは1以上の整数)では,
$X\equiv x^{2^{2m-1}}$, $A\equiv a^{2^{2m-1}}$ 〈注：$X^4=x^{2^{2m-1}\times 4}=x^{2^{2m+1}}$〉
として，代入して
$x^n+4a^n=(x^{2^{2m-1}\times 2}+2a^{2^{2m-1}}x^{2^{2m-1}}+a^{2^{2m-1}\times 2})(x^{2^{2m}}-2a^{2^{2m-1}}x^{2^{2m-1}}+a^{2^{2m}})$
まとめて，次の[定理2.1]を得る。
[定理2.1] $f(x)\equiv x^n+k$ (但しkは正の整数変数)はn=2のときのみ既約で($n\neq 1$として)，$n\geqq 3$では可約になる。
またkとしての形は
(ⅰ) $n=2l\times(2m+1)$ $(l,m\geqq 1)$のときは$k=a^n$
(ⅱ) $n=2^l(l\geqq 2)$のときは$k=4a^n$と取れることが解った。

3.定数項が負の場合

(ⅰ)まず，$f(x)\equiv ax^2+bx-k$(a,b,kは整数で，aとkは正で，kを動かす)の可約性を調べてみよう。
$D=b^2-4\times a\times(-k)=b^2+4ak\equiv d^2$として
$\Leftrightarrow 4ak=d^2-b^2=(d-b)(d+b)$
ここで
$d-b=4al\Leftrightarrow l\equiv \frac{d-b}{4a}$ と更におくと
$d+b=4al+2b$により，
$k=l(4al+2b)=2l(2al+b)$
よって
$f(x)=(x-2l)\{ax+(2al+b)\}$
となる。〈注：$D=b^2+4a\times 2l(2al+b)=b^2+8alb+16a^2l^2=(b+4al)^2$
つまり$d=|b+4a|$となる。〉

また，$2l\equiv y$としてみると，
$f(x)=(x-y)\{ax+(ay+b)\}=(ax^2-axy)+(axy+bx)-(ay^2+by)=(ax^2+bx)-(ay^2+by)$
となる。
つまり，$k\equiv ay^2+by=y(ay+b)$とおけば$f(x)$は可約となる，（但し，$y>-b/a\Leftrightarrow y$を十分大きい整数と取る。）
この考えは，一般のn次の整数係数多項式についても言えるから，次の[定理3.1]を得る。

[定理3.1] $f(x)\equiv ax^n+a_1x^{n-1}+\cdots+a_{n-1}x-k$(但し$a,a_1,a_2,\cdots,a_{n-1}$，kは整数で，aとkは正とし，更にkは変数として扱う）は，
$k\equiv ay^n+a_1y^{n-1}+a_2y^{n-2}+\cdots+a_{n-1}y$として，yを十分大きい正の整数として動かせれば，常に可約になる。(但し$a_1^2+a_2^2+\cdots+a_{n-1}^2\neq 0$とする)
〈注1：$|\frac{k}{y^n}|\geqq a-|a_1|\times\frac{1}{y}-|a_2|\times\frac{1}{y^2}-\cdots\cdots-|a_{n-1}|\times\frac{1}{y^{n-1}}\geqq a-M(\frac{1}{y}+\frac{1}{y^2}+\cdots+\frac{1}{y^{n-1}})$
(但し$M\equiv \underset{1\leqq i\leqq n-1}{\mathrm{Max}}\ a_i$)
$>a-M(\frac{1}{y}+\frac{1}{y^2}+\cdots+\frac{1}{y^{n-1}}+\cdots)$(但し$y\geqq 2$)$=a-M\times\frac{1}{y}\times\frac{1}{1-\frac{1}{y}}=a-\frac{M}{y-1}$ となるから，
つまり$a\geqq\frac{M}{y-1}\Leftrightarrow y-1\geqq\frac{M}{a}\Leftrightarrow y\geqq\frac{M}{a}+1$
となる全ての整数yについて，$f(x)$は可約となることが解った。($\because\frac{k}{y^n}>0\Leftrightarrow k>0$より)〉

〈注２：定数項が負の整数変数の場合は，可約の多項式は無数に，しかもある所からは，整数的な連続で，可約多項式が得られる。
これは，２次多項式で定数項が正の場合は有限個の可約多項式しか得られなかった場合と根本的に異なる。〉
〈注３：定数項が０のときは，２次以上の多項式は可約であることは自明なので今までは敢えて触れなかった。〉
[証明] $k\equiv ay^n+a_1y^{n-1}+a_2y^{n-2}+\cdots+a_{n-1}y$とすれば
$f(x)=a(x^n-y^n)+a_1(x^{n-1}-y^{n-1})+a_2(x^{n-2}-y^{n-2})+\cdots+a_{n-1}(x-y)$
であるから，$f(x)$は$(x-y)$を因数に持ち，商は$(n-1)$次の整数係数の多項式になるからよい。
（但し，nは２以上の整数とする。）[了]

(ii)次に
$Z=g(x)\equiv ax^{2m+1}+a_1x^{2m-1}+\cdots+a_{2k-1}x^{2m-(2k-1)}+\cdots+a_{2m-1}x+k$（但し，m;$a,a_1,a_3,\cdots,a_{2k-1},\cdots,a_{2m-1}$,kは整数で,m,a,kは正とする）において
$k\equiv ay^{2m+1}+a_1y^{2m-1}+\cdots+a_{2k-1}y^{2m-(2k-1)}+\cdots+a_{2m-1}y$
とおけば，$g(x)=a(x^{2m+1}+y^{2m+1})+a_1(x^{2m-1}+y^{2m-1})+\cdots+a_{2k-1}(x^{2m-(2k-1)}+y^{2m-(2k-1)})+\cdots+a_{2m-1}(x+y)$
となるから，$g(x)$は$(x+y)$を因数に持つ。
よって，$g(x)$は可約である。

まとめて
[定理３.Ⅱ.１] $Z=g(x)\equiv ax^{2m+1}+\sum_{k=1}^{m}a_{2k-1}x^{2m(2k1)}+k$は$k\equiv ay^{2m+1}+\sum_{k=1}^{m}a_{2k-1}y^{2m-(2k-1)}$とすれば可約となる。

〈注１：正の整数変数yの動く範囲を調べてみると

$$\frac{k}{y^{2m+1}}\geqq a-|a_1|\times\frac{1}{y^2}-|a_3|\times\left(\frac{1}{y^2}\right)^2-\cdots-|a_{2k-1}|\times\left(\frac{1}{y^2}\right)^k-\cdots-|a_{2m+1}|\times\left(\frac{1}{y^2}\right)^m\geqq a-M\left(\frac{1}{y^2}\right)-M\left(\frac{1}{y^2}\right)^2-\cdots-M\left(\frac{1}{y^2}\right)^m$$

（但し$M\equiv\underset{1\leqq k\leqq m}{\mathrm{Max}}|a_{2k-1}|$）〉

$$a-M\left(\frac{1}{y^2}\right)-M\left(\frac{1}{y^2}\right)^2-M\left(\frac{1}{y^2}\right)^3-\cdots$$

$$=a-M\times\frac{\frac{1}{y^2}}{1-\frac{1}{y^2}}=a-M\frac{1}{y^2-1}$$

より(kが正の十分条件は)

$$a\geqq\frac{M}{y^2-1}\Leftrightarrow y^2-1\rangle\frac{M}{a}\Leftrightarrow y^2\rangle\frac{M}{a}+1$$

$$\Leftrightarrow y\geqq\sqrt{\frac{M}{a}+1}$$

なる範囲をyは動けばよい。〉

〈注2：このように，yが連続した正の整数上を動いても，元の多項式$g(x)$が常に可約となるから非常に使い易いのである。
これらの定理の応用は，次回の論文で述べることにする。〉

文献表
[1]竹之内　脩：数学的構造 (1992,朝倉書店)
[2]高木　貞治：代数学講義 (1956,共立出版)
[3]藤原　松三郎：代数学Ⅰ,Ⅱ (1956,内田老鶴圃)

「受理年月日　2004 年 9 月 30 日」