【W.2.1】

t の関数

$$u(t)=1+2at+b(t^2-1)\quad(-1\le t\le 1) \qquad \cdots\cdots(1.1)$$

に対して，$u(t)\ge 0\,(-1\le t\le 1)$ を満たす点 $(a,\,b)$ の存在範囲を図示せよ．

【解答】

• $b=0$ のとき，$u(t)=1+2at$ であるから求める条件は，

$$u(-1)=1-2a\ge 0\ \wedge\ u(1)=1+2a\ge 0 \qquad \cdots\cdots(1.2)$$

従って，

$$-\frac{1}{2}\le a\le\frac{1}{2}\ \wedge\ b=0 \qquad \cdots\cdots(1.3)$$

• $b\neq 0$ のとき，$u(t)=0$ を ab 平面上の直線の方程式と考える．即ち，

$$2at+(t^2-1)b+1=0\iff bt^2+2at+1-b=0 \qquad \cdots\cdots(1.4)$$

このとき，直線 $u(t)=0$ が $-1\le t\le 1$ なる変化に伴い通過する領域の**包絡線**は，
t の 2 次方程式 (1.4) が重根を持つ条件によって導かれるので，その判別式を D として，

$$\mathrm{D}/4=a^2-b(1-b)=0\iff a^2+\left(b-\frac{1}{2}\right)^2=\frac{1}{4} \qquad \cdots\cdots(1.5)$$

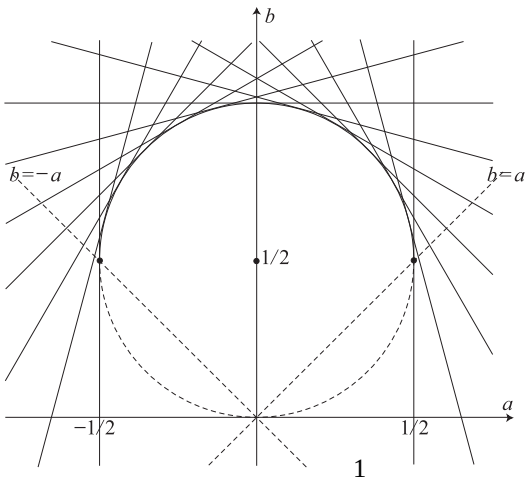
(1.4), (1.5) を連立して，(1.4) の重根を求めると，

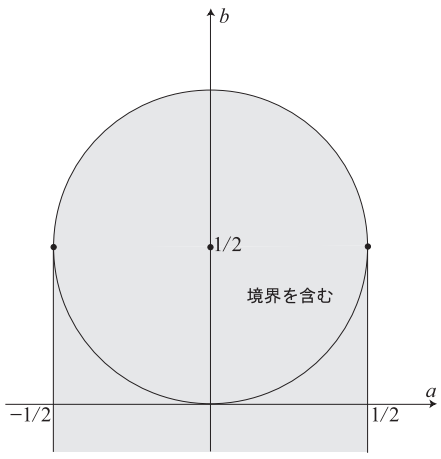
$$(bt+a)^2=0\iff bt+a=0\iff t=-\frac{a}{b}\quad(\because\ b\neq 0) \qquad \cdots\cdots(1.6)$$

このとき，円 (1.5) と直線 (1.6) の接点に関して，

$$-1\le t\le 1\ \wedge\ bt+a=0\ \wedge\ a^2+\left(b-\frac{1}{2}\right)^2=\frac{1}{4}\iff b\ge a\ \wedge\ b\ge -a\ \wedge\ a^2+\left(b-\frac{1}{2}\right)^2=\frac{1}{4} \qquad \cdots\cdots(1.7)$$

(1.7) により，(1.5), (1.6) の接点は**左図**の半円周上に存在し，これが直線 $u(t)=0$ の通過領域の包絡線である．
更に，点 $(a,\,b)$ の存在範囲は $u(t)\ge 0$, 即ち，直線 $u(t)=0$ を境界とする 2 個の領域の原点を含む側の領域であるから，すべての直線 $u(t)=0$ に対して，その共通領域を考慮して**右図**の領域を得る．また，これは (1.3) の線分をも含むので求める領域である．





【W.2.2】

三角形 ABC と同一平面内の点 P に対して，$\max(\angle A, \angle B, \angle C) < 120^\circ$ のとき，

$$\mathrm{AP}+\mathrm{BP}+\mathrm{CP} \qquad \cdots\cdots(2.1)$$

の値を最小にするのは，

$$\angle\mathrm{APB}=\angle\mathrm{BPC}=\angle\mathrm{CPA}=120^\circ \qquad \cdots\cdots(2.2)$$

【解答】　– 等長変換 –

P を三角形 ABC の内部にあるとして議論して一般性を失わない．

B を中心として，A を 60° 回転した点を A'，P を 60° 回転した点を P'とすると，(**左図**)

三角不等式により，

$$\mathrm{AP}+\mathrm{BP}+\mathrm{CP}=\mathrm{A}'\mathrm{P}'+\mathrm{P}'\mathrm{P}+\mathrm{PC}\geq\mathrm{A}'\mathrm{C} \quad \left(\because\ \mathrm{BP}=\mathrm{BP}'=\mathrm{PP}'\right) \qquad \cdots\cdots(2.3)$$

一方，**右図**において，線分 $\mathrm{A}'\mathrm{C}$ 上に 2 点 P, P'を

$$\angle\mathrm{PBP}'=60^\circ\ \wedge\ \mathrm{BP}=\mathrm{BP}' \qquad \cdots\cdots(2.4)$$

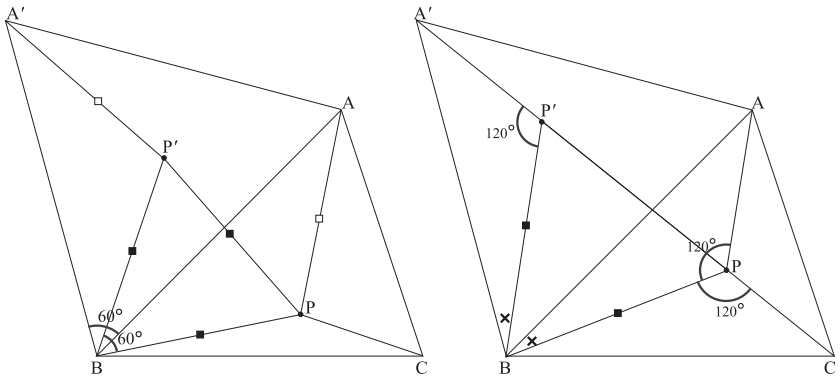
を満たすようにとれば，三角形 BPP'は正三角形であるから，

$$\angle\mathrm{BPC}=\angle\mathrm{A}'\mathrm{P}'\mathrm{B}=\angle\mathrm{APB}=120^\circ \quad \left(\because\ \triangle\mathrm{APB}\equiv\triangle\mathrm{A}'\mathrm{P}'\mathrm{B}\right) \qquad \cdots\cdots(2.5)$$

(2.3), (2.5) により，(2.1) を最小にする点 P に対して，

$$\angle\mathrm{APB}=\angle\mathrm{BPC}=\angle\mathrm{CPA}=120^\circ \qquad \cdots\cdots(2.2)$$

が成り立つ．



【別解】 – Ptolemy の定理 –

BC を 1 辺とする正三角形 BCD を三角形 ABC の反対側にとる．
また，三角形 ABC の内部にある点を P とするとき，四角形 PBDC に対して，

$$\mathrm{BP}\cdot\mathrm{CD}+\mathrm{CP}\cdot\mathrm{BD}geq\mathrm{PD}\cdot\mathrm{BC} \iff \mathrm{BP}+\mathrm{CP}\geq\mathrm{PD} \quad (\because \mathrm{CD}=\mathrm{BD}=\mathrm{BC})$$

$$\iff \mathrm{AP}+\mathrm{BP}+\mathrm{CP}geq\mathrm{AP}+\mathrm{PD}\geq\mathrm{AD} \quad (\because \text{Ptolemy の定理}) \quad \cdots\cdots(2.6)$$

(2.6) における等号条件は，四角形 PBDC が円に内接し，P が線分 AD 上にあるとき，
即ち，P が線分 AD と外接円との交点 P′ の位置にあるときに限る．このとき，

$$\angle\mathrm{BPC}=\angle\mathrm{BP'C}=180^\circ-\angle\mathrm{BDC}=180^\circ-60^\circ=120^\circ \quad \cdots\cdots(2.7)$$

∠CPA, ∠APB に対して同様の議論を適用し，(2.2) が導かれる．

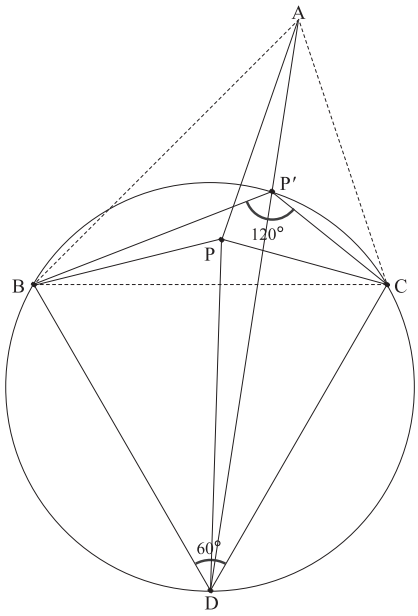
[Note] 任意の四辺形 ABCD に対して，

$$\mathrm{AB}\cdot\mathrm{CD}+\mathrm{BC}\cdot\mathrm{DA}\geq\mathrm{AC}\cdot\mathrm{DB}$$

が成り立ち，特に，円に内接するとき，

$$\mathrm{AB}\cdot\mathrm{CD}+\mathrm{BC}\cdot\mathrm{DA}=\mathrm{AC}\cdot\mathrm{DB}$$

が成り立つ．(Ptolemy **の定理**)



【別解】 – 楕円の反射定理 –

(2.1) において，BP＋CP の値を固定するとき，楕円における**反射定理**により，
BP＋CP＝(**一定**) を満たす点 P は 2 点 B, C を焦点とするある楕円の周上に存在する．
この楕円周上の点 P と A との距離が最小になるのは，P における接線 $\mathfrak{g}$ と線分 AP とが直交するときである．
このとき，楕円上の点における接線の性質 $\angle \mathrm{BP}\mathfrak{g} = \angle \mathrm{CP}\mathfrak{g}$ により，

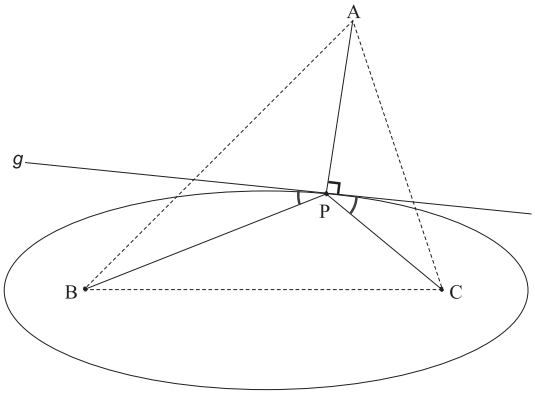
$$\angle \mathrm{BPA} = \angle \mathrm{BP}\mathfrak{g} + 90^\circ = \angle \mathrm{CP}\mathfrak{g} + 90^\circ = \angle \mathrm{CPA} \iff \angle \mathrm{BPA} = \angle \mathrm{CPA} \qquad \cdots\cdots(2.8)$$

同様に，CP＋AP の値を固定して議論すれば，

$$\angle \mathrm{CPB} = \angle \mathrm{APB} \qquad \cdots\cdots(2.9)$$

が導けるので，(2.8), (2.9) により，

$$\angle \mathrm{APB} = \angle \mathrm{BPC} = \angle \mathrm{CPA} = 120^\circ \qquad \cdots\cdots(2.2)$$



【Lemma】

三角形 ABC と同一平面上の点 P に対して，$\angle \mathrm{BAC} \geq 120^\circ$ のとき，

$$\mathrm{AP} + \mathrm{BP} + \mathrm{CP}$$

を最小にする P は，P＝A である．

【Lemma】

三角形 ABC と同一平面上の点 P に対して，$\angle \mathrm{BAC} \geq 120^\circ$ のとき，

$$\mathrm{AP}+\mathrm{BP}+\mathrm{CP}$$

を最小にする P は，$\mathrm{P}=\mathrm{A}$ である．

【Proof】

A を中心に AC を回転して，B, A, C′を共線とする．(このときの回転角を $2\omega \leq 60^\circ$ とする)
更に，A を中心に AP を角 2ω 回転して，AP′とするとき，

$$\mathrm{PP'}=2\mathrm{AP}\sin\omega \qquad \cdots\cdots(2.10)$$

が成り立つので，

$$\mathrm{AP}+\mathrm{BP}+\mathrm{CP}=\mathrm{AP}(1-2\sin\omega)+\mathrm{PP'}+\mathrm{BP}+\mathrm{C'P'} \quad \left(\because\ \mathrm{CP}=\mathrm{C'P'}\right) \qquad \cdots\cdots(2.11)$$

ここで，**三角不等式**により，

$$\mathrm{PP'}+\mathrm{BP}+\mathrm{P'C'} \geq \mathrm{BP'}+\mathrm{P'C'} \geq \mathrm{BC'} \qquad \cdots\cdots(2.12)$$

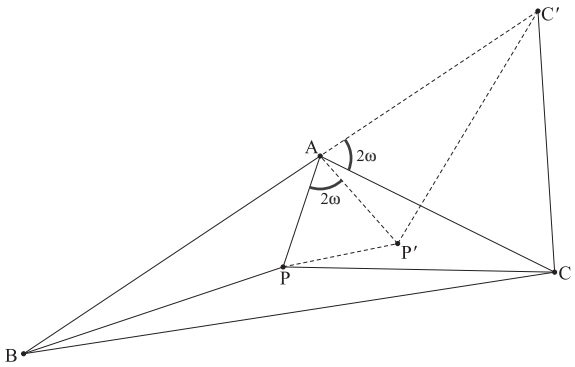
(2.12) における等号条件は，4 点 B, P, P′, C′が共線のときに限り同時に成立．
更に，$0^\circ < \omega \leq 30^\circ$ より，

$$\mathrm{AP}(1-2\sin\omega) \geq 0 \qquad \cdots\cdots(2.13)$$

(2.13) の等号条件は，$\omega = 30^\circ \vee \mathrm{AP}=0$ のときに限り成立．
(2.11), (2.12), (2.13) により，

$$\mathrm{AP}+\mathrm{BP}+\mathrm{CP} \geq \mathrm{BC'}=\mathrm{AB}+\mathrm{AC} \qquad \cdots\cdots(2.14)$$

(2.14) の等号条件は，$\mathrm{B},\ \mathrm{A}=\mathrm{P}=\mathrm{P'},\ \mathrm{C'}$ が共線のときに限り成立するので題意は示された．



【W.2.3】

複素数 $z=\cos 20^\circ+\mathbf{i}\sin 20^\circ$ に対して，$\alpha=z+\overline{z}$ と定める．

(1) α はある整数係数の 3 次方程式の解であることを示せ．

(2) この 3 次方程式は 3 個の実数解を持ち，そのいずれも有理数でないことを示せ．

(3) 有理係数の 2 次方程式で α を解とするものは存在しないことを示せ．

【解答】

(1) $\alpha=2\cos 20^\circ$ であるから，

$$\cos 3\theta=4\cos^3\theta-3\cos\theta$$

に $\theta=20^\circ$ を代入して，

$$\cos 60^\circ=4\cos^2 20^\circ-3\cos 20^\circ \iff \frac{1}{2}=4\times\left(\frac{\alpha}{2}\right)^3-3\times\frac{\alpha}{2} \iff \alpha^3-3\alpha-1=0 \qquad \cdots\cdots(3.1)$$

即ち，α は 3 次方程式 $x^3-3x-1=0$ の解である．

(2) $u(x)=x^3-3x-1$ と置く．

$u'(x)=3(x^2-1)$ より，$u(x)$ は $x=-1$ で極大値，$x=1$ で極小値をとり，

$$u(-1)=1>0 \ \wedge \ u(1)=-3<0 \qquad \cdots\cdots(3.2)$$

より，$u(x)$ のグラフは x 軸を異なる 3 個所で切り，方程式 $u(x)=0$ は異なる 3 個の実数解を持つ．

その実数解を小さい順に x_1, x_2, x_3 と表せば，グラフより，

$$-2<x_1<-1<x_2<0<1<x_3<2 \qquad \cdots\cdots(3.3)$$

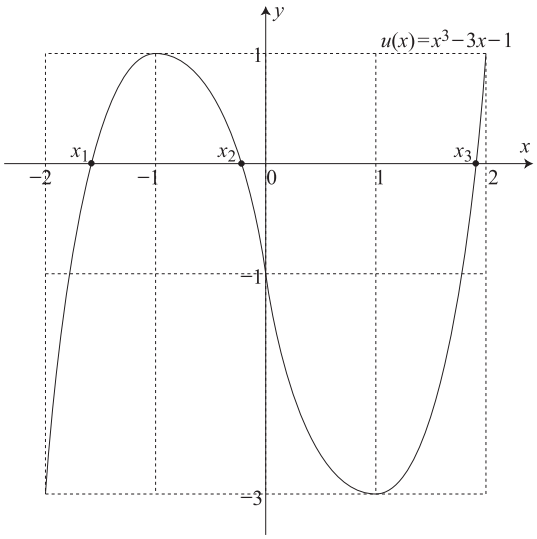
次に，$u(x)=0$ が有理数 $\dfrac{n}{m}$ を解に持つと仮定する．ただし，m : 正整数 $\wedge$ n : 整数 $\wedge$ $\gcd(m,\,n)=1$ とする．

このとき，

$$\left(\frac{n}{m}\right)^3-3\times\frac{n}{m}-1=0 \iff n^3-3m^2n-m^3=0 \iff n^3=m^2(3n+m) \qquad \cdots\cdots(3.4)$$

ここで，$\gcd(m,\,n)=1$ により，(3.4) の成立は $m=1$ の場合に限られる．

このとき，$u(x)=0$ の解は整数 n となり，(3.3) に矛盾する．即ち，$u(x)=0$ は有理数を解に持たない．



(3) 有理係数の 2 次方程式

$$x^2+px+q=0 \quad (p,\ q:\text{有理数}) \qquad \cdots\cdots(3.5)$$

が α を解に持つと仮定すると,

$$\alpha^2+p\alpha+q=0 \qquad \cdots\cdots(3.6)$$

(3.6) の両辺に $\alpha\neq 0$ を乗じて,

$$\alpha^3+p\alpha^2+q\alpha=0 \qquad \cdots\cdots(3.7)$$

(3.7) を (3.1) によって書き換えれば,

$$(3\alpha+1)+p\alpha^2+q\alpha=0 \iff p\alpha^2+(q+3)\alpha+1=0 \qquad \cdots\cdots(3.8)$$

(3.6), (3.8) の係数を比較して,

$$1:p:q=p:(q+3):1 \iff p^2=q+3 \ \wedge\ p=q(q+3) \qquad \cdots\cdots(3.9)$$

(3.9) より q を消去して,

$$p^3-3p-1=0 \qquad \cdots\cdots(3.10)$$

有理数 p に対する (3.10) の成立は (2) の結果に矛盾する.
即ち, α を解とする有理係数の 2 次方程式は存在しない.

[Note] 有理係数 $p,\ q$ の 2 次方程式

$$x^2+px+q=0 \quad (p,\ q:\text{有理数}) \qquad \cdots\cdots(3.5)$$

が α を解に持つと仮定する.
このとき, (1) により α は,

$$C_1(x^3-3x-1)+C_2(x^2+px+q)=0 \quad \left(\forall C_1,\ \forall C_2\right) \qquad \cdots\cdots(3.11)$$

の解であるから, $C_1=-1,\ C_2=\alpha$ として,

$$-(\alpha^3-3\alpha-1)+\alpha(\alpha^2+p\alpha+q)=0 \iff p\alpha^2+(q+3)\alpha+1=0 \qquad \cdots\cdots(3.12)$$

が成り立ち, α は方程式

$$px^2+(q+3)x+1=0 \qquad \cdots\cdots(3.13)$$

の解でもある.
更に, (3.5), (3.13) により α は,

$$C_1(x^2+px+q)+C_2(px^2+(q+3)x+1)=0 \quad \left(\forall C_1,\ \forall C_2\right) \qquad \cdots\cdots(3.14)$$

の解であるから, $C_1=p,\ C_2=-1$ として,

$$p(\alpha^2+p\alpha+q)-(p\alpha^2+(q+3)\alpha+1)=0 \iff (p^2-q-3)\alpha+pq-1=0 \qquad \cdots\cdots(3.15)$$

ここで, $p^2-q-3=pq-1=0$ とすると,

$$p^3-3p-1=0 \qquad \cdots\cdots(3.16)$$

が導かれ, (2) により p が有理数であることに反する.
従って, (3.15) は α の方程式として成立し,

$$\alpha=\frac{1-pq}{p^2-q-3} \quad (p,\ q:\text{有理数}) \qquad \cdots\cdots(3.17)$$

が導かれ, これは α が有理数でないことに反する.
従って, 背理法により, α を解に持つ有理係数の 2 次方程式は存在しない.

【Note】　– 解の公式 –

3 次方程式 $x^3+ax^2+bx+c=0$ の解の公式

$$x_1=\sqrt[3]{-\frac{27c+2a^3-9ab}{54}+\sqrt{\left(\frac{27c+2a^3-9ab}{54}\right)^2+\left(\frac{3b-a^2}{9}\right)^3}}+\sqrt[3]{-\frac{27c+2a^3-9ab}{54}-\sqrt{\left(\frac{27c+2a^3-9ab}{54}\right)^2+\left(\frac{3b-a^2}{9}\right)^3}}-\frac{1}{3}a$$

$$x_2=\frac{-1+\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{-\frac{27c+2a^3-9ab}{54}+\sqrt{\left(\frac{27c+2a^3-9ab}{54}\right)^2+\left(\frac{3b-a^2}{9}\right)^3}}+\frac{-1-\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{-\frac{27c+2a^3-9ab}{54}-\sqrt{\left(\frac{27c+2a^3-9ab}{54}\right)^2+\left(\frac{3b-a^2}{9}\right)^3}}-\frac{1}{3}a$$

$$x_3=\frac{-1-\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{-\frac{27c+2a^3-9ab}{54}+\sqrt{\left(\frac{27c+2a^3-9ab}{54}\right)^2+\left(\frac{3b-a^2}{9}\right)^3}}+\frac{-1+\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{-\frac{27c+2a^3-9ab}{54}-\sqrt{\left(\frac{27c+2a^3-9ab}{54}\right)^2+\left(\frac{3b-a^2}{9}\right)^3}}-\frac{1}{3}a$$

に依れば, 方程式 $x^3-3x-1=0$ の場合, $a=0,\ b=-3,\ c=-1$ であるから,

$$x_1=\sqrt[3]{\frac{1+\sqrt{3}\mathbf{i}}{2}}+\sqrt[3]{\frac{1-\sqrt{3}\mathbf{i}}{2}}=\left(\cos\frac{\pi}{3}+\mathbf{i}\sin\frac{\pi}{3}\right)^{\frac{1}{3}}+\left(\cos\left(-\frac{\pi}{3}\right)+\mathbf{i}\sin\left(-\frac{\pi}{3}\right)\right)^{\frac{1}{3}}$$
$$=\cos\frac{\pi}{9}+\mathbf{i}\sin\frac{\pi}{9}+\cos\left(-\frac{\pi}{9}\right)+\mathbf{i}\sin\left(-\frac{\pi}{9}\right)=2\cos\frac{\pi}{9}$$

$$x_2=\frac{-1+\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{\frac{1+\sqrt{3}\mathbf{i}}{2}}+\frac{-1-\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{\frac{1-\sqrt{3}\mathbf{i}}{2}}$$
$$=\left(\cos\frac{2\pi}{3}+\mathbf{i}\sin\frac{2\pi}{3}\right)\left(\cos\frac{\pi}{3}+\mathbf{i}\sin\frac{\pi}{3}\right)^{\frac{1}{3}}+\left(\cos\left(-\frac{2\pi}{3}\right)+\mathbf{i}\sin\left(-\frac{2\pi}{3}\right)\right)\left(\cos\left(-\frac{\pi}{3}\right)+\mathbf{i}\sin\left(-\frac{\pi}{3}\right)\right)^{\frac{1}{3}}$$
$$=\cos\frac{7\pi}{9}+\mathbf{i}\sin\frac{7\pi}{9}+\cos\left(-\frac{7\pi}{9}\right)+\mathbf{i}\sin\left(-\frac{7\pi}{9}\right)=2\cos\frac{7\pi}{9}$$

$$x_3=\frac{-1-\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{\frac{1+\sqrt{3}\mathbf{i}}{2}}+\frac{-1+\sqrt{3}\mathbf{i}}{2}\times\sqrt[3]{\frac{1-\sqrt{3}\mathbf{i}}{2}}$$
$$=\left(\cos\frac{4\pi}{3}+\mathbf{i}\sin\frac{4\pi}{3}\right)\left(\cos\frac{\pi}{3}+\mathbf{i}\sin\frac{\pi}{3}\right)^{\frac{1}{3}}+\left(\cos\left(-\frac{4\pi}{3}\right)+\mathbf{i}\sin\left(-\frac{4\pi}{3}\right)\right)\left(\cos\left(-\frac{\pi}{3}\right)+\mathbf{i}\sin\left(-\frac{\pi}{3}\right)\right)^{\frac{1}{3}}$$
$$=\cos\frac{13\pi}{9}+\mathbf{i}\sin\frac{13\pi}{9}+\cos\left(-\frac{13\pi}{9}\right)+\mathbf{i}\sin\left(-\frac{13\pi}{9}\right)=2\cos\frac{13\pi}{9}$$

[**解答**] の index に従って表せば,

$$x_3=2\cos\frac{\pi}{9},\ x_2=2\cos\frac{13\pi}{9},\ x_1=2\cos\frac{7\pi}{9}$$

【W.2.4】

nを任意の正整数とするとき，

$$n,\ n+1,\ n+2,\ n+3,\ n+4,\ n+5 \qquad \cdots\cdots(4.1)$$

を 2 通りの組に分け，それぞれの積を等しくすることはできないことを示せ．

【解答】

(4.1) を素数 7 の既約剰余系と考える．即ち，

$$\{n,\ n+1,\ n+2,\ n+3,\ n+4,\ n+5\} \equiv \{1,\ 2,\ 3,\ 4,\ 5,\ 6\} \pmod 7 \qquad \cdots\cdots(4.2)$$

ここで，(4.1) の中に 7 の倍数が存在するとすれば，
(4.1) を 2 個のグループに分けた一方の積を P_1，他方の積を P_2 として，

$$\mathrm{P}_1 \equiv 0 \pmod 7 \ \wedge\ \mathrm{P}_2 \not\equiv 0 \pmod 7 \qquad \cdots\cdots(4.3)$$

が成り立ち，

$$\mathrm{P}_1 \not\equiv \mathrm{P}_2 \pmod 7 \implies \mathrm{P}_1 \neq \mathrm{P}_2 \qquad \cdots\cdots(4.4)$$

即ち，(4.1) の中に 7 の倍数は存在せず，(4.2) の前提で議論してよい．
このとき，

$$\mathrm{P}_1 \times \mathrm{P}_2 \equiv 6! = 6 \times (5 \times 3) \times (4 \times 2) \equiv (-1) \times 1 \times 1 \equiv -1 \pmod 7 \qquad \cdots\cdots(4.5)$$

(4.5) において，$\mathrm{P}_1 = \mathrm{P}_2 = x$ と仮定すれば，

$$x^2 \equiv -1 \pmod 7 \implies x^2 + 1 \equiv 0 \pmod 7 \qquad \cdots\cdots(4.6)$$

ここで，(4.6) は如何なる整数 x に対しても成り立たない．実際，

$$x \equiv \pm 1,\ \pm 2,\ \pm 3 \pmod 7 \implies x^2 + 1 \equiv 2,\ 5,\ 3 \pmod 7 \qquad \cdots\cdots(4.7)$$

以上により題意は示された．

[Note] (4.5) は Willson **の定理**である．次頁に定理の証明を与える．

【Willson の定理】

素数 p に対して，

$$(p-1)! \equiv -1 \pmod{p}$$

が成り立つ．

【証明】

$p=2$ に対しては自明なので，$p \geq 3$ で考える．

素数 $p \geq 3$ に対して，方程式

$$a^x \equiv 1 \pmod{p} \quad (1 \leq a \leq p-1) \qquad \cdots\cdots(4.8)$$

の最小正整数解 x_0 が $x_0 = p-1$ となる正整数 a を素数 p の**原始根**という．

このとき，**既約剰余系**に関して，

$$\{a, a^2, \cdots, a^{p-1}\} \equiv \{1, 2, \cdots, p-1\} \pmod{p} \qquad \cdots\cdots(4.9)$$

が成り立つ．

何故ならば，$1 \leq j < k \leq p-1$ に対して，

$$a^j \equiv a^k \pmod{p} \qquad \cdots\cdots(4.10)$$

が成り立つと仮定すると，

$$a^j\left(a^{k-j}-1\right) \equiv 0 \pmod{p} \iff a^{k-j} \equiv 1 \pmod{p} \qquad \cdots\cdots(4.11)$$

ここで，$1 \leq k-j \leq p-2$ であるから，(4.11) は x_0 の最小性に反する．

このとき，(4.9) により，

$$(p-1)! \equiv a^{1+2+\cdots+(p-1)} \equiv a^{\frac{p(p-1)}{2}} \pmod{p} \qquad \cdots\cdots(4.12)$$

が成り立つが，Fermat **の小定理**により，

$$a^{p-1} \equiv 1 \pmod{p} \iff \left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0 \pmod{p} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \qquad \cdots\cdots(4.13)$$

(4.12), (4.13) により，

$$(p-1)! \equiv \left(a^{\frac{p-1}{2}}\right)^p \equiv (-1)^p \equiv -1 \qquad \cdots\cdots(4.14)$$

【Lemma】 – 原始根の存在 –

素数 p の既約剰余系 $a\ (1 \leq a \leq p-1)$ に対して，

$$a^m \equiv 1 \pmod{p} \qquad \cdots\cdots(4.15)$$

を満たす最小の正整数 m を a の**指数** (index) という．

このとき，Fermat **の小定理**により，m は $p-1$ の約数であり，

$m < p-1$ のとき，a を元にして m より大きな指数を持つ既約剰余系が構成できることを示す．

$$a^m \equiv 1 \pmod{p} \ \wedge\ 1 \leq a \leq p-1 \ \wedge\ 0 < m < p-1 \qquad \cdots\cdots(4.16)$$

のとき，

$$\{1,\ a,\ a^2,\ \cdots,\ a^{m-1}\} = \mathsf{A} \qquad \cdots\cdots(4.17)$$

とすれば，$\{1,\ 2,\ \cdots,\ p-1\}$ 内の既約剰余系で A に属さないものが存在する．$\left(\because\ m < p-1\right)$

その 1 つを b とし，b の指数を n とする．即ち，

$$b^n \equiv 1 \pmod{p} \ \wedge\ b \notin \mathsf{A} \qquad \cdots\cdots(4.18)$$

このとき，n は m の約数とはならない．

即ち，n が m の約数とすると，$b^m \equiv 1 \pmod{p}$ となり，$b \notin \mathsf{A}$ に反する．

• $\gcd(m,\ n) = 1$ のとき，既約剰余系 ab の指数は mn である．即ち，

$$(ab)^{mn} \equiv (a^m)^n \times (b^n)^m \equiv 1 \pmod{p} \qquad \cdots\cdots(4.19)$$

逆に，$(ab)^x \equiv 1 \pmod{p}$ とすると，

$$(ab)^{mx} \equiv (a^m)^x \times b^{mx} \equiv b^{mx} \equiv 1 \pmod{p} \qquad \cdots\cdots(4.20)$$

となり，mx は n の倍数であり，$\gcd(m,\ n) = 1$ より，x は n の倍数．

同様にして，

$$(ab)^{nx} \equiv a^{nx} \times (b^n)^x \equiv a^{nx} \equiv 1 \pmod{p} \qquad \cdots\cdots(4.21)$$

となり，nx は m の倍数であり，$\gcd(m,\ n) = 1$ より，x は m の倍数．即ち，x は mn の倍数．

従って，mn は ab の指数となり，m より大なる指数 mn を持つ既約剰余系 ab が構成できる．

• $\gcd(m,\ n) = d > 1$ のとき，$\mathrm{LCM}(m,\ n) = L$ として，

$$m = m_0 \times d \ \wedge\ n = n_0 \times d \ \wedge\ L = m_0 \times n_0 \times d \ \wedge\ \gcd(m_0,\ n_0) = 1 \qquad \cdots\cdots(4.22)$$

を満たす m の約数 m_0，n の約数 n_0 を考える．

また，d を互いに素な d_1, d_2 の積 $d_1 \times d_2 = d$ で表せば，

$$m' = \frac{md_1}{d} = m_0 \times d_1 \ \wedge\ n' = \frac{nd_2}{d} = n_0 \times d_2 \ \wedge\ m' \times n' = L \qquad \cdots\cdots(4.23)$$

を満たす整数 m', n' が得られる．

このとき，$a^{\frac{m}{m'}}$, $b^{\frac{n}{n'}}$ は指数がそれぞれ m', n' となり，$a^{\frac{m}{m'}} \times b^{\frac{n}{n'}}$ の指数は $m' \times n' = L$ となるが，

n は m の約数でないので，$L = m_0 \times n_0 \times d > m$ が成り立つ．

即ち，m より大なる指数 L を持つ既約剰余系 $a^{\frac{m}{m'}} b^{\frac{n}{n'}}$ が構成できる．

以上により，$m < p-1$ から真に増加な指数の列が構成でき，それらはいずれも $p-1$ を超えないので，

有限回の操作の後に指数が $p-1$ の既約剰余系が構成できる．即ち，**原始根は必ず存在する**．