【Example 26.1】
(1) 10 進表記された有理数 $\dfrac{11}{26}$ を 3 進小数表記すると，$0.\dot{a_1}a_2\dot{a_3}$ となる．a_1, a_2, a_3 を求めよ．
(2) 10 進表記された小数 α $(0<\alpha<1)$ は，p 進表記では $0.\dot{b_1}\dot{b_2}$，$p+2$ 進表記では $0.\dot{b_2}$ と表される．
また，b_2 は b_1 の倍数である．このとき，α を 10 進表記で求めよ．

Point (p 進小数)
10 進小数 α が正整数 $p(\geq 2)$ によって，

$$\alpha=\frac{a_1}{p}+\frac{a_2}{p^2}+\cdots+\frac{a_k}{p^k}+\cdots \quad (\text{各 } a_k\text{は, } 0\leq a_k\leq p-1 \text{ の整数})$$

の形に表されるとき，$0.a_1a_2\cdots a_k\cdots$ を α の p 進小数表記という．
また，10 進小数と同様に p 進循環小数を $0.\dot{a_1}a_2\cdots\dot{a_k}$ などのように表す．

【解説】
(1) 題意より，

$$\begin{aligned}\frac{11}{26}&=\frac{a_1}{3}+\frac{a_2}{3^2}+\frac{a_3}{3^3}+\frac{a_1}{3^4}+\frac{a_2}{3^5}+\frac{a_3}{3^6}+\cdots\cdots\\&=\left(\frac{a_1}{3}+\frac{a_2}{3^2}+\frac{a_3}{3^3}\right)\left(1+\frac{1}{3^3}+\frac{1}{3^6}+\cdots\cdots\right)\\&=\frac{3^2a_1+3a_2+a_3}{3^3}\times\frac{1}{1-1/3^3}=\frac{3^2a_1+3a_2+a_3}{26}\end{aligned}\quad\cdots\cdots(1.1)$$

従って，

$$a_1\times3^2+a_2\times3+a_3=11_{(10)}=102_{(3)}\iff a_1=1,\ a_2=0,\ a_3=2\quad\cdots\cdots(1.2)$$

(2) b_1, b_2 は p 進小数表記の各桁を表すので，

$$b_j=0,\ 1,\ 2,\ \cdots,\ p-1\quad(j=1,2)\quad\cdots\cdots(1.3)$$

このとき，(1) と同様に，

$$\alpha=\left(\frac{b_1}{p}+\frac{b_2}{p^2}\right)\left(1+\frac{1}{p^2}+\frac{1}{p^4}+\cdots\right)=\frac{pb_1+b_2}{p^2-1}\quad\cdots\cdots(1.4)$$

更に，

$$\alpha=\frac{b_2}{p+2}+\frac{b_2}{(p+2)^2}+\cdots=\frac{b_2}{p+2}\left(1+\frac{1}{p+2}+\frac{1}{(p+2)^2}+\cdots\right)=\frac{b_2}{p+1}\quad\cdots\cdots(1.5)$$

(1.4), (1.5) より，

$$\frac{pb_1+b_2}{p^2-1}=\frac{b_2}{p+1}\iff pb_1+b_2=(p-1)b_2\iff pb_1=(p-2)b_2\quad\cdots\cdots(1.6)$$

更に題意より，b_2 は b_1 の倍数であるから，

$$b_2=kb_1\ \wedge\ k=1,2,\cdots,p-1\ (\because\ (1.3))\quad\cdots\cdots(1.7)$$

$b_1\neq0$ に注意して，(1.6), (1.7) より，

$$p=(p-2)k\iff k=1+\frac{2}{p-2}\ (\because\ p=2\text{ は不合理})\quad\cdots\cdots(1.8)$$

(1.8) において，$k=1,2,\cdots,p-1$ であり，$p>2$ としてよいので，

$$p=4 \ \wedge \ k=2 \qquad \cdots\cdots(1.9)$$

このとき，

$$b_2=2b_1 \ \wedge \ b_j=0,1,2,3 \ (j=1,2) \iff b_1=1 \ \wedge \ b_2=2 \qquad \cdots\cdots(1.10)$$

従って，(1.5) より，

$$\alpha=\frac{b_2}{p+1}=\frac{2}{5} \qquad \cdots\cdots(1.11)$$

Comment

10 進循環小数の定義を既知とすれば，p 進循環小数も容易に類推できる．例題においては，p 進循環小数の定義から直ちに解法の方針が立てられる．ここでは，10 進循環小数表記から導かれる「約数 · 倍数」の性質を 1 つ紹介する．正整数 a に対して，有理数 $1/a$ を 10 進小数表記したとき，$0.\dot{b_1}b_2\cdots\dot{b_k}$ と循環小数で表されたとする．即ち，

$$\frac{1}{a}=0.\dot{b_1}b_2\cdots\dot{b_k}=\frac{b_1b_2\cdots b_k}{99\cdots9} \ (k\geq 2;\text{分母は } k \text{ 桁すべて } 9)$$

このとき，

$$9\times 11\cdots1=a\times b_1b_2\cdots b_k \ (\text{左辺第 2 因数は } k \text{ 桁すべて } 1)$$

ここで，$\gcd(9,a)=1$ であるならば，a は $11\cdots1$ (k 桁すべて 1) の倍数である．

Point (有限小数 · 循環小数)

● 有理数が (10 進) **有限小数**を表すための必要十分条件は，分母が 2, 5 以外の素因数を含まないこと．

● 既約真分数が**純循環小数**を表すための必要十分条件は，分母が 2, 5 いずれの素因数も含まないこと．

● 既約真分数が**混循環小数**を表すための必要十分条件は，分母が 2, 5 の少なくとも一方と，2, 5 以外の素因数を含むこと．

Point (循環小数 ⇒ 分数)

(1) 純循環小数

$$0.\dot{a_1}a_2\cdots\dot{a_n}=\frac{a_1a_2\cdots a_n}{99\cdots9}$$

分母は n 桁で，すべての桁が 9 である．

(2) 混循環小数

$$0.a_1\cdots a_m\dot{b_1}\cdots\dot{b_n}=\frac{a_1\cdots a_mb_1\cdots b_n-a_1\cdots a_m}{99\cdots900\cdots0}$$

分母は最初に 9 が連続して n 個，続いて 0 が連続して m 個．

【Review 26.1.1】
有理数 $\dfrac{b}{a}$ が循環節 c 桁の純循環小数のとき，

$$10^c \equiv 1 \pmod{a}$$

が成り立つことを示せ.

[証明略]

【Review 26.1.2】
ある正数 N を 5 進表記すると，整数部分が 2 桁の循環小数 $ab.\dot{c}$ となり，また，$N-1$ を 7 進表記すると，整数部分が 2 桁の循環小数 $cb.\dot{a}$ となる．このとき，a, b, c の値を求めよ.

[答] $a=3,\ c=2,\ b=0,1,2,3,4$

【Review 26.1.3】
$\dfrac{1}{23}=0.\dot{0}4347826086956521739\dot{1}\dot{3}$ であり，この小数の循環節を左 11 桁と右 11 桁に分けて，

$$04347826086+95652173913=99999999999$$

とすると 9 が 11 桁連続して並ぶ．この理由について説明せよ.

[証明略]

【Example 26.2】
p を素数として，2^p-1 が素数であるとする．
整数 $m=2^{p-1}(2^p-1)$ のすべての約数を $d_1, d_2, \cdots, d_n$ とする．ただし，$d_1=1, d_n=m$ である．
(1) m の約数の個数 n を求めよ．また，$\sum_{k=1}^{n} d_k$ を m の式で表せ．
(2) $p=5$ のとき，m と互いに素な m 以下の正整数の個数を求めよ．
(3) 一般の素数 p に対して，m と互いに素な m 以下の正整数の個数を p の式で表せ．

[Note] 2^p-1 (p : 素数) なる形の素数を**メルセンヌ素数**という．

【解説】
(1) m の素因数は $2,\ 2^p-1$ の 2 種類であり，m の約数をすべて列挙すると，

$$2^0,\ 2^1,\ 2^2,\ \cdots,\ 2^{p-1},\ \ 2^0(2^p-1),\ 2^1(2^p-1),\ 2^2(2^p-1),\ \cdots,\ 2^{p-1}(2^p-1) \qquad \cdots\cdots(2.1)$$

従って，約数の個数は

$$n=((p-1)+1)(1+1)=2p \qquad \cdots\cdots(2.2)$$

であり，それらの総和は，

$$\begin{aligned}\sum_{k=1}^{n} d_k &=(1+2+2^2+\cdots+2^{p-1})(1+(2^p-1)) \\ &=\frac{2^p-1}{2-1}\times 2^p=2\times 2^{p-1}(2^p-1)=2m\end{aligned} \qquad \cdots\cdots(2.3)$$

(2) $p=5$ のとき，$m=2^4(2^5-1)=496$ である．
496 と**互いに素でない**，即ち，素因数として 2 あるいは 31 を含む約数の個数を数える．
496 の約数で素因数として 2 を含むもの (即ち，2 の倍数) は，$\dfrac{496}{2}=248$ 個あり，
これら以外の約数で素因数として 31 を含むものは，

$$31\times 1,\ 31\times 3,\ 31\times 5,\ \cdots,\ 31\times 15 \quad (8\text{ 個}) \qquad \cdots\cdots(2.4)$$

であるから，$496-(248+8)=240$ 個である．
(3) (2) と同様の要領で数える．
m の約数で素因数として 2 を含むものは，$\dfrac{m}{2}=2^{p-2}(2^p-1)$ 個あり，
これら以外の約数で素因数として 2^p-1 を含むものは，

$$(2^p-1)\times 1,\ (2^p-1)\times 3,\ (2^p-1)\times 5,\ \cdots,\ (2^p-1)\times(2^{p-1}-1) \quad (2^{p-2}\text{個}) \qquad \cdots\cdots(2.5)$$

であるから，

$$2^{p-1}(2^p-1)-\{2^{p-2}(2^p-1)+2^{p-2}\}=2^{p-1}(2^{p-1}-1)\text{ 個} \qquad \cdots\cdots(2.6)$$

【Note】 – 完全数 –

[Review 24.3.6] でも紹介したが，整数 m のすべての約数の和 $\sum_{k=1}^{n} d_k$ が $2m$ に一致するような m を**完全数**といい，偶数の完全数は $2^{k-1}(2^k-1)$ (2^k-1 : 素数, k : 正整数) の形に限られる．(1) は m が完全数であるための十分条件を示させる設問である．また，奇数の完全数が存在するか否かは知られていない．

Comment

例題の (2), (3) は「整数論」で有名な Euler 関数についての設問である．Euler 関数とは，m と互いに素な m 以下の正整数の個数を与える関数 $\varphi(m)$ のことで，m の素因数分解を ${p_1}^{n_1}{p_2}^{n_2}\cdots{p_k}^{n_k}$ とするとき，

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\times\cdots\times\left(1-\frac{1}{p_k}\right) \qquad \cdots\cdots(2.7)$$

なる「定理」が成り立つ．これを既知とすれば，$m=2^{p-1}(2^p-1)$ のとき，

$$\varphi(m)=m\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2^p-1}\right)=2^{p-2}(2^p-1)-2^{p-2}=2^{p-1}(2^{p-1}-1) \qquad \cdots\cdots(2.6)$$

のように瞬時に $\varphi(m)$ が求められる．
例えば，$m=p^n$ (p : 素数, n : 正整数) のとき，m と**互いに素でない** m 以下の整数は，

$$p,\ 2p,\ 3p,\ \cdots,\ p^{n-1}\times p \quad (p^{n-1}\text{個}) \qquad \cdots\cdots(2.8)$$

に限られるので，$\varphi(m)=p^n-p^{n-1}=m(1-1/p)$ は容易に理解できる．
一般の $m(={p_1}^{n_1}\cdots{p_k}^{n_k})$ に対しては，次の「補助定理」を用いて即座に証明できるので確認して貰いたい．

Point (補助定理)

$\gcd(m_1,m_2)=1$ なる正整数 m_1, m_2 に対して，

$$\varphi(m_1\times m_2)=\varphi(m_1)\times\varphi(m_2)$$

即ち，Euler 関数 φ は**乗法的である**．

[Note] この定理を証明せよ．(Drichlet の原理を用いる)

【Review 26.2.1】

xy 平面上の領域 $1\leq x\leq 10\ \wedge\ 0\leq y\leq 10$ 内にある 100 個の格子点を考える．
原点 $(0,0)$ とこれらの格子点を結ぶ線分で，端点以外に格子点が存在しないものは何本あるか．

[答] 63 本

【Review 26.2.2】 – Euler の定理 –

m を正整数，$\varphi(m)$ を Euler 関数とするとき，

$$a^{\varphi(m)}\equiv 1 \pmod m$$

が成り立つことを示せ．ただし，$\gcd(m,a)=1$ とする．

[証明略]

【Example 26.3.1】 – Fermat の小定理 –

a を整数, p を素数とするとき,

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ. ただし, $a \not\equiv 0 \pmod{p}$ とする.

【解説】

$p-1$ 個の整数の集合 **A** を

$$\mathbf{A} = \{1, 2, \cdots, p-1\} \qquad \cdots\cdots(3.1.1)$$

と定義し, **A** の各要素に $a(\not\equiv 0 \pmod{p})$ を掛けて得られる集合 **B** を

$$\mathbf{B} = \{a, 2a, \cdots, (p-1)a\} \qquad \cdots\cdots(3.1.2)$$

とすると, **B** の要素は modulus p ですべて異なる. 即ち, $\mathbf{A} \equiv \mathbf{B} \pmod{p}$ が成り立つ.
何故なら, $1 \leq j < k \leq p-1$ なる任意の整数 j, k に対して,

$$ja \equiv ka \pmod{p} \qquad \cdots\cdots(3.1.3)$$

を仮定すると,

$$(k-j)a \equiv 0 \pmod{p} \iff k-j \equiv 0 \pmod{p} \qquad \cdots\cdots(3.1.4)$$

が導かれ, $1 \leq k-j \leq p-2$ に矛盾する.

$$\therefore \quad ja \not\equiv ka \pmod{p} \quad (j \neq k) \qquad \cdots\cdots(3.1.5)$$

従って, **B** の各要素は modulus p で異なり, **A** の各要素と modulus p で 1 対 1 に対応する. (**Dirichlet の原理**)
このとき, **A** のすべての要素の積と **B** のすべての要素の積に対して,

$$\begin{aligned} 1 \times 2 \times \cdots \times (p-1) &\equiv a \times 2a \times \cdots \times (p-1)a \pmod{p} \\ &\iff (p-1)!\,(a^{p-1}-1) \equiv 0 \pmod{p} \\ &\iff a^{p-1} - 1 \equiv 0 \pmod{p} \qquad \cdots\cdots(3.1.6) \end{aligned}$$

(3.1.6) により題意は示された.

【Note】 – 既約剰余系 –

すべての整数を modulus m によって m 個の**類** (class) に分類することができる. 即ち, 任意の整数を m で割った剰余は, $\{0, 1, \cdots, m-1\}$ の何れかであるから, 剰余が一致する整数をまとめて 1 つの集合 (類) を作れば, 全部で m 個の集合 (類) ができる. ここで, 剰余が $r\,(0 \leq r \leq m-1)$ である類を C_r で表すとき,

$$C_0, C_1, C_2, \cdots, C_{m-1} \qquad \cdots\cdots(3.1.7)$$

を modulus m による**剰余類** (residue class) という.
各 $C_r\,(0 \leq r \leq m-1)$ から要素を 1 個ずつとって作った m 個の整数の集合を**完全剰余系**といい, m と互いに素な整数 r による剰余類 C_r から要素を 1 個ずつとって作った整数の集合を**既約剰余系**という. $m = p\,(p:\text{素数})$ のとき, 集合 $\{1, 2, \cdots, p-1\}$ は既約剰余系の集合として一番代表的なものであり, 上の集合 **B** も既約剰余系の集合である. また, $\mathbf{A} \equiv \mathbf{B} \pmod{p}$ を結論する部分で「Dirichlet の原理」が用いられていることに注意してほしい.

【Example 26.3.2】　– Willson の定理 –

素数 p に対して，

$$(p-1)! \equiv -1 \pmod{p} \qquad \cdots\cdots(3.2.1)$$

が成り立つことを示せ．

【解説】

$p=2$ のときは明らかなので，$p \geq 3$ で考える．

素数 $p \geq 3$ に対して，方程式

$$a^x \equiv 1 \pmod{p} \ (1 \leq a \leq p-1) \qquad \cdots\cdots(3.2.2)$$

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，既約剰余系の集合に対して，

$$\{a^1, a^2, \cdots, a^{p-1}\} \equiv \{1, 2, \cdots, p-1\} \pmod{p} \qquad \cdots\cdots(3.2.3)$$

が成り立つ．

何故ならば，$0 \leq j < k \leq p-2$ に対して，

$$a^j \equiv a^k \pmod{p} \qquad \cdots\cdots(3.2.4)$$

が成り立つことを仮定すると，

$$a^j(a^{k-j}-1) \equiv 0 \pmod{p} \iff a^{k-j} \equiv 1 \pmod{p} \qquad \cdots\cdots(3.2.5)$$

ここで，$1 \leq k-j \leq p-2$ であるから，(3.2.5) は x_0 の最小性に反する．

このとき，(3.2.3) より，

$$(p-1)! \equiv a^{1+2+\cdots+(p-1)} \equiv a^{\frac{p(p-1)}{2}} \pmod{p} \qquad \cdots\cdots(3.2.6)$$

が成り立つが，Fermat の小定理より，

$$\begin{aligned} a^{p-1} \equiv 1 \pmod{p} &\iff (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod{p} \\ &\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \end{aligned} \qquad \cdots\cdots(3.2.7)$$

となるので，(3.2.6), (3.2.7) より，

$$(p-1)! \equiv \left(a^{\frac{p-1}{2}}\right)^p \equiv (-1)^p \equiv -1 \qquad \cdots\cdots(3.2.8)$$

従って，(3.2.1) は示された．

[Note]　**原始根**の存在については次頁に証明を与えておく．

【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,

$$a^m \equiv 1 \pmod{p} \qquad \cdots\cdots(3.3.1)$$

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以下に示す;

$$a^m \equiv 1 \pmod{p} \ \wedge\ 1 \leq a \leq p-1 \ \wedge\ 0 < m < p-1 \qquad \cdots\cdots(3.3.2)$$

のとき,

$$\{1,\, a,\, a^2,\, \cdots,\, a^{m-1}\} = \mathbf{A} \qquad \cdots\cdots(3.3.3)$$

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

その 1 つを b とし, b の指数を n とする. 即ち, $b^n \equiv 1 \pmod{p}$. このとき, n は m の約数とはならない.

何故なら, n が m の約数とすると, $b^m \equiv 1 \pmod{p}$ となるが, これは $b \notin \mathbf{A}$ の仮定に反する.

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

何故なら,

$$(ab)^{mn} \equiv (a^m)^n \times (b^n)^m \equiv 1 \pmod{p} \qquad \cdots\cdots(3.3.4)$$

が成り立ち, 逆に, $(ab)^x \equiv 1 \pmod{p}$ とすると,

$$(ab)^{mx} \equiv (a^m)^x \times b^{mx} \equiv b^{mx} \equiv 1 \pmod{p} \qquad \cdots\cdots(3.3.5)$$

となり, mx は n の倍数でなければならないが, $\gcd(m, n) = 1$ より, x が n の倍数となる.

同様にして,

$$(ab)^{nx} \equiv a^{nx} \times (b^n)^x \equiv a^{nx} \equiv 1 \pmod{p} \qquad \cdots\cdots(3.3.6)$$

となり, nx は m の倍数でなければならないが, $\gcd(m, n) = 1$ より, x が m の倍数となる.

(3.3.5), (3.3.6) により, x は mn の倍数である.

従って, $mn\,(> m)$ は ab の指数となり, m より大きな指数 mn を持つ既約剰余系 ab が構成できることになる.

● $\gcd(m, n) = d\,(> 1)$ のとき, $\mathrm{LCM}(m, n) = l$ とする.

このとき,

$$m = m_0 \times d \ \wedge\ n = n_0 \times d \ \wedge\ l = m_0 \times n_0 \times d \ \wedge\ \gcd(m_0, n_0) = 1 \qquad \cdots\cdots(3.3.7)$$

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 2 数 d_1, d_2 の積 $d_1 \times d_2\,(= d)$ で表せば,

$$m' = \frac{md_1}{d} = m_0 \times d_1 \ \wedge\ n' = \frac{nd_2}{d} = n_0 \times d_2 \ \wedge\ m' \times n' = l \qquad \cdots\cdots(3.3.8)$$

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 の約数ではないので, $l = m_0 \times n_0 \times d > m$ が成り立つ. 即ち, m より大きな指数 l を持つ既約剰余系 $a^{\frac{m}{m'}} b^{\frac{n}{n'}}$ が構成できることになる.

以上により, $m\,(< p-1)$ から真に増加な指数の列が構成でき, それらは何れも $p-1$ 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ことになる. 即ち, 原始根は必ず存在すると言える.

【Review 26.3.1】　70 IMO

n を任意の正整数とするとき,

$$n,\ n+1,\ n+2,\ n+3,\ n+4,\ n+5$$

を 2 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.

[証明略]

【Review 26.3.2】　– Willson の定理の逆 –

$n(>1)$ を整数とする.

$(n-1)! \equiv -1 \pmod{n}$ が成り立つとき，n は素数であることを示せ.

[証明略]