5.3　解説

(1) $g(x)$ を $f(x)$ で割った商を $P(x)$ とすると，

$$g(x)=f(x)\cdot P(x)+r(x)$$

と表せるから，この両辺を 7 乗すると，

$$\begin{aligned} g(x)^7 &= \sum_{r=0}^{6}\left\{{}_7\mathrm{C}_r\cdot(f(x)\cdot P(x))^{7-r}\cdot r(x)^r\right\}+r(x)^7 \\ &= f(x)\cdot\sum_{r=0}^{6}\left({}_7\mathrm{C}_r\cdot f(x)^{6-r}\cdot P(x)^{7-r}\cdot r(x)^r\right)+r(x)^7 \end{aligned}$$

したがって，$g(x)^7$ を $f(x)$ で割った余りは，$r(x)^7$ を $f(x)$ で割った余りに等しい。 ■

(2) 条件より，$f(x)$ を法として，$h(x)^7\equiv h_1(x)$，$h_1(x)^7\equiv h_2(x)$ がそれぞれ成り立つから，

$$h(x)^{49}=(h(x)^7)^7\equiv h_1(x)^7\equiv h_2(x)\pmod{f(x)}$$

これより，$h(x)^{49}\equiv h(x)\pmod{f(x)}$ となるような $a,\ b$ の組を求める。ここで，$p(x)$ を次のようにおく。

$$p(x)=h(x)^{49}-h(x)\quad \therefore\ p'(x)=49h(x)^{48}\cdot h'(x)-h'(x)$$

そして，

$$h(x)^{49}\equiv h(x)\pmod{f(x)} \iff p(x)\equiv 0\pmod{f(x)} \iff p(1)=p'(1)=p(2)=0$$

であるから，$p(1)=p'(1)=p(2)=0$ を満たす $a,\ b$ の組を求める。$p(1)=p'(1)=p(2)=0$ に関して，以下の ①，②，③ 式を得る。

$$\begin{cases} p(1)=(1+a+b)^{49}-(1+a+b)=(1+a+b)\{(1+a+b)^{48}-1\}=0 & \cdots ① \\ p'(1)=49(1+a+b)^{48}(2+a)-(2+a)=(2+a)\{49(1+a+b)^{48}-1\}=0 & \cdots ② \\ p(2)=(4+2a+b)^{49}-(4+2a+b)=(4+2a+b)\{(4+2a+b)^{48}-1\}=0 & \cdots ③ \end{cases}$$

① 式について，$1+a+b=x$ とおくと，

$$\begin{aligned} ① &\iff x^{49}-x=0 \\ &\iff x(x^{24}+1)(x^{12}+1)(x^6+1)(x^3+1)(x^3-1)=0 \\ &\iff x=0 \lor x=1 \lor x=-1 \quad (\because\ x\in\mathbb{R}) \end{aligned}$$

$x=1+a+b$ が 0，1，-1 のいずれの場合においても，② に代入すると $a=-2$ となるから，

$$①\land② \iff (a,\ b)=(-2,\ 1)\lor(a,\ b)=(-2,\ 2)\lor(a,\ b)=(-2,\ 0)$$

$$\therefore\ ①\land②\land③ \iff (a,\ b)=(-2,\ 1)\lor(a,\ b)=(-2,\ 0)$$

よって，求めるべき $a,\ b$ の組は，$\boldsymbol{(a,\ b)=(-2,\ 1),\ (-2,\ 0)}$ ……(答)