Problem 3

Let integer polynomials $P(x) = \Sigma_{i=0}^{n-1} p_i x^i,\ Q(x) = \Sigma_{i=0}^{n} q_i x^i$, We instigate in the relationship between a, b, d in the equation

$$P(x) \cdot (ax+b) + Q(x) \cdot (d) = 1.$$

(a) We claim that no combination of $2x+5$ and 3 can equal 1.

method 1. We prove by contradiction.
Assume there exist integer polynomials $P(x)$ and $Q(x)$ such that $P(x) \cdot (2x+5) + Q(x) \cdot 3 = 1$.
When $x = -\frac{5}{2}$, we know

$$P(-\frac{5}{2}) \cdot 0 + Q(-\frac{5}{2}) \cdot 3 = 1$$
$$Q(-\frac{5}{2}) = \frac{1}{3}$$

The LHS is a linear combination of $\frac{5}{2}$ with integer coefficients, so its denominator must be a power of 2; while the RHS has a denominator of 3, which is not a power of 2. Hence there is a contradiction.
Therefore, there is no such $P(x), Q(x)$ satisfying this equation. $\square$

method 2. Since $P(x) \cdot (2x+5) + Q(x) \cdot (3) = 1$ we expand $P(x)$ and $Q(x)$, we get the following system of equations:

$$\begin{cases} 2p_{n-1} + 3q_n = 0 \\ 2p_{n-2} + 5p_{n-1} + 3q_{n-1} = 0 \\ \cdots \\ 2p_0 + 5p_1 + 3q_1 = 0 \\ 5p_0 + 3q_0 = 1 \end{cases}$$

Thus, $2p_{n-1} + 3q_n = 0 \Rightarrow 3|p_{n-1}$.
Since $2p_{i-1} + 5p_i + 3q_i = 0,\ i = 1, 2, \ldots, n-1$, and $3|3q_i$, if $3|2p_i$, then $2p_{i-1}$ must also divide 3, which means $3|p_{i-1},\ i = 1, 2, \ldots, n-1$.
Since $3|p_{n-1}$, so will $3|p_{n-2}, 3|p_{n-3}, \ldots$ Therefore, $3|p_0$.
Substitute into $5p_0 + 3q_0 = 1, 5\mathrm{p}_0 + q_0 = \frac{1}{3}$.
$Since \mathrm{p}_0, q_0 \in \mathbb{Z}$, their linear combination must also be an integer, which is a contradiction.
Therefore, such $P(x), Q(x)$ do not exist. $\square$

(b) Let n =2, i.e.$P(x) = p_1x + p_0,\ Q(x) = q_2x^2 + q_1x + q_0$. Then

$$\begin{aligned} P(x)(2x+5) + Q(x)\cdot 4 &= 1 \\ (p_1x+p_0)(2x+5) + 4(q_2x^2 + q_1x + q_0 &= 1 \\ (2p_1 + 4q_2)x^2 + (5p_1 + 2p_0 + 4q_1)x + (5p_0 + 4q_0) &= 1 \end{aligned}$$

Hence, we know that
$$\begin{cases} 2p_1 + 4q_2 = 0 \\ 5p_1 + 2p_0 + 4q_1 = 0 \\ 5p_0 + 4q_0 = 1, \end{cases}$$
Let two free variable, say $p_1 = 2,\ p_0 = 1$, we solve to get $q_2 = -1,\ q_1 = -3,\ q_0 = -1$.
Therefore, $P(x) = 2x + 1,\ Q(x) = -x^2 - 3x - 1$ satisfy this equation.

(c)(i) Let n =2, i.e.$P(x) = p_1x + p_0,\ Q(x) = q_2x^2 + q_1x + q_0$.

$$\begin{aligned} P(x)(15x+9) + Q(x)\cdot 25 &= 1 \\ (p_1x+p_0)(15x+9) + 25(q_2x^2 + q_1x + q_0) &= 1 \\ (15p_1 + 25q_2)x^2 + (9p_1 + 15p_0 + 25q_1)x + (9p_0 + 25q_0) &= 1 \end{aligned}$$

Hence, we know that
$$\begin{cases} 15p_1 + 25q_2 = 0 \\ 9p_1 + 15p_0 + 25q_1 = 0 \\ 9p_0 + 25q_0 = 1, \end{cases} \Rightarrow \begin{cases} -15q_2 + 15p_0 + 25q_1 = 0 \\ 9p_0 + 25q_0 = 1, \end{cases} \Rightarrow \begin{cases} -3q_2 + 3p_0 + 5q_1 = 0 \\ 9p_0 + 25q_0 = 1, \end{cases}$$
Solve the Diophantine equation, $9p_0 + 25q_0$, we get $p_0 = 14,\ q_0 = -5$.
Substitute to get $p_1 = 10, q_2 = -6,\ q_1 = -12$.
Therefore, $P(x) = 10x + 14,\ Q(x) = -6x^2 - 12x - 5$ satisfy this equation.

(c)(ii) There do not exist $P(x), Q(x)$ for the combination of $15x + 9$ and 20. The argument is similar to what we did in (a):
Let $x = -\frac{3}{5}$, the equation becomes

$$\begin{aligned} P(-\frac{3}{5})(15(-\frac{3}{5}) + 9) + Q(-\frac{3}{5})(20) &= 1 \\ Q(-\frac{3}{5}) &= \frac{1}{20} \end{aligned}$$

The denominator of the LHS is a power of 5. However, the denominator of the RHS is $20 = 4 \times 5$. Therefore, such $P(x), Q(x)$ cannot exist.

(d) Following the same argument as (a) and (c)(ii), we have the following propositions:

Proposition 1. *If* $P(x) \cdot (ax+b) + Q(x) \cdot (d) = 1$, *then* $gcd(b,d) = 1$.

Proof. If $P(x) \cdot (ax+b) + Q(x) \cdot (d) = 1$, then

$$ax \cdot P(x) + b(x) + d \cdot Q(x) = 1,$$

$$bp_0 + dq_0 = 1.$$

According to Bézout's identity, $gcd(b,d) = 1$. □

Proposition 2. *If* $P(x) \cdot (ax+b) + Q(x) \cdot (d) = 1$, $d \mid [gcd(a,d)]^n$.

Proof. Let $x = -\frac{b}{a}$. The equation becomes

$$P(-\frac{b}{a}) \cdot (a(-\frac{b}{a}) + b) + Q(-\frac{b}{a}) \cdot (d) = 1$$

$$\Rightarrow Q(-\frac{b}{a}) = \frac{1}{d}$$

Multiply both sides by $-a^n$, we get

$$\Sigma_{i=0}^{n} a^{n-i} b^i q_i = -\frac{a^n}{d}$$

The LHS must be an integer, so in order for the RHS to be an integer as well, d must divide a^n.
In other words, $d|a^n$.
Let $gcd(a,d) = k,\ a = a^{'}k,\ d = d^{'}k$.
$gcd(a^{'}, d^{'}) = 1$.
Then $d^{'}k \mid (a^{'}k)^n \Rightarrow d^{'} \mid a^{'n}k^{n-1}. \Rightarrow d^{'} \mid k^{n-1} \Rightarrow d \mid k^n$.
In other words, $d \mid [gcd(a,d)]^n$. □

We can also check these by looking at a couple of examples:

Example 1. When $P(x)(3x+8) + Q(x) \cdot 27 = 1$, we find

$$P(x) = -9x^2 - 3x - 10,\ Q(x) = x^3 + 3x^2 + 2x + 3.$$

Check that $gcd(b,d) = gcd(8,27) = 1$, and $gcd(a,d) = gcd(3,27) = 3,\ 27 \mid 3^3$, which satisfy both propositions.

Example 2. When $P(x)(21x+1)+Q(x)\cdot 9=1$, we find

$$P(x)=-3x+1,\ Q(x)=7x^2+2x.$$

Check that $gcd(b,d)=gcd(1,9)=1$, and $gcd(a,d)=gcd(21,9)=3,\ 9\mid 3^2$, which satisfy both propositions.

Example 3. When $P(x)(-18x+17)+Q(x)\cdot 27=1$, we find

$$P(x)=1152x+8,\ Q(x)=-768x^2-720x-5.$$

Check that $gcd(b,d)=gcd(17,27)=1$, and $gcd(a,d)=gcd(-18,27)=9,\ 27\mid 9^2$, which satisfy both propositions.