Question: 3

Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$ for each of the following pairs of polynomials.

a. $a(x) = 5x^3 + 6x^2 - 3x + 4$ and $b(x) = x - 2$ in $\mathbb{Z}_7[x]$

b. $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ and $b(x) = x^2 + x - 2$ in $\mathbb{Z}_7[x]$

c. $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ in $\mathbb{Z}_5[x]$

d. $a(x) = x^5 + x^3 - x^2 - x$ and $b(x) = x^3 + x$ in $\mathbb{Z}_2[x]$

Solution:

a. $5x^3 + 6x^2 - 3x + 4 = (5x^2 + 4x + 6)(x - 2) + (2x + 5) \pmod 7$.

b. $6x^4-2x^3+x^2-3x+1 = (6x^2-8x+21)(x^2+x-2)+(-40x+43) = (6x^2-x)(x^2+x-2)+(2x+1) \pmod 7$.

c. $4x^5 - x^3 + x^2 + 4 = (4x^2 - 1)(x^3 - 2) + (2) \pmod 5$.

d. $x^5 + x^3 - x^2 - x = (x^2)(x^3 + x) - (x^2 + x) \pmod 2$

Question: 4

Find the greatest common divisor of each of the following pairs $p(x)$ and $q(x)$ of polynomials. If $d(x) = \gcd(p(x), q(x))$, find two polynomials $a(x)$ and $b(x)$ such that $d(x) = a(x)p(x) + b(x)q(x)$.

a. $p(x) = x^3 - 6x^2 + 14x - 15$ and $q(x) = x^3 - 8x^2 + 21x - 18$, where $p(x), q(x) \in \mathbb{Q}^x$.

b. $p(x) = x^3 + x^2 - x + 1$ and $q(x) = x^3 + x - 1$, where $p(x), q(x) \in \mathbb{Z}_2[x]$.

c. $p(x) = x^3 + x^2 - 4x + 4$ and $q(x) = x^3 + 3x - 2$, where $p(x), q(x) \in \mathbb{Z}_5[x]$.

d. $p(x) = x^3 - 2x + 4$ and $q(x) = 4x^3 + x + 3$, where $p(x), q(x) \in \mathbb{Q}^x$.

Solution:

a. Finding $d(x)$:

$$
\begin{aligned}
x^3 - 8x^2 + 21x - 18 &= (1)(x^3 - 6x^2 + 14x - 15) + (2x^2 - 7x + 3) \\
x^3 - 6x^2 + 14x - 15 &= (1)\left(\frac{1}{2}x - \frac{9}{4}\right) + \left(\frac{15}{4}x - \frac{45}{4}\right) \\
\frac{1}{2}x - \frac{9}{4} &= \left(\frac{15}{4}x - \frac{45}{4}\right)\left(\frac{8}{15}x - \frac{4}{15}\right) \\
\gcd(p(x), q(x)) &= x - 3
\end{aligned}
$$

Second part:

$$\begin{aligned}
\left(\frac{15}{4}x - \frac{45}{4}\right) &= (x^3 - 8x^2 + 21x - 18) - (2x^2 - 7x + 3)\left(\frac{1}{2}x - \frac{9}{4}\right) \\
&= (x^3 - 8x^2 + 21x - 18) - ((x^3 - 6x^2 + 14x - 15) - (x^3 - 8x^2 + 21x - 18))\left(\frac{1}{2}x - \frac{9}{4}\right) \\
&= (x^3 - 8x^2 + 21x - 18)\left(\frac{1}{2}x - \frac{5}{4}\right) + (x^3 - 6x^2 + 14x - 15)\left(-\frac{1}{2}x + \frac{9}{4}\right) \\
(x - 3) &= (x^3 - 8x^2 + 21x - 18)\left(\frac{2}{15}x - \frac{1}{3}\right) + (x^3 - 6x^2 + 14x - 15)\left(-\frac{2}{15}x + \frac{3}{5}\right)
\end{aligned}$$

b. Finding $d(x)$:

$$\begin{aligned}
x^3 + x^2 - x + 1 &= (1)(x^3 + x - 1) + (x^2) \pmod 2 \\
x^3 + x - 1 &= (x)(x^2) + (x - 1) \pmod 2 \\
x^2 &= (x)(x - 1) + (1) \pmod 2 \\
x - 1 &= (x)(1) + (1) \pmod 2 \\
1 &= (1)(1) \pmod 2 \\
\gcd(p(x), q(x)) &= 1
\end{aligned}$$

Second part:

$$\begin{aligned}
1 &= (x - 1) - (x)(1) \pmod 2 \\
&= (x - 1) - ((x^2) - (x)(x - 1)) \pmod 2 \\
&= (x - 1)(x + 1) - (x^2) \pmod 2 \\
&= ((x^3 + x - 1) - (x^2)(x))(x + 1) - (x^2) \pmod 2 \\
&= (x^3 + x - 1)(x + 1) - (x^2)(x^2 + x - 1) \pmod 2 \\
&= (x^3 + x - 1)(x + 1) - ((x^3 + x - 1) - (x^2 + x - 1))(x^2 + x + 1) \pmod 2 \\
&= (x^3 + x - 1)(x^2) - (x^3 + x^2 - x + 1)(x^2 + x + 1) \pmod 2
\end{aligned}$$

c.

$$\begin{aligned}
x^3 + x^2 - 4x + 4 &= (1)(x^3 + 3x - 2) + (x^2 + 3x + 1) \pmod 5 \\
x^3 + 3x - 2 &= (x)(x^2 + 3x + 1) + (x + 1) \pmod 5 \\
x^2 + 3x + 1 &= (x + 2)(x + 1) + (4) \pmod 5 \\
4 &= (x^2 + 3x + 1) - (x + 2)(x + 1) \pmod 5 \\
&= (x^2 + 3x + 1) - (x + 2)((x^3 + 3x - 2) - (x)(x^2 + 3x + 1)) \pmod 5 \\
&= (x^2 + 4x)(x^2 + 3x + 1) - (x + 2)(x^3 + 3x - 2) \\
&= (x^2 + 4x)((x^3 + x^2 - 4x + 4) - (x^3 + 3x - 2)) - (x + 2)(x^3 + 3x - 2) \pmod 5 \\
&= (x^2 + 4x)(x^3 + x^2 - 4x + 4) - (x^2 + 2)(x^3 + 3x - 2)
\end{aligned}$$

Negating this equation gives us

$$1 = (4x^2 + x)(x^3 + x^2 - 4x + 4) + (x^2 + 2)(x^3 + 3x - 2)$$

meaning that the gcd is 1.

d.

$$\begin{aligned}
4x^3 + x + 3 &= (4)(x^3 - 2x + 4) + (9x - 13) \\
x^3 - 2x + 4 &= \left(\frac{1}{9}x^2 + \frac{13}{81}x + \frac{7}{729}\right)(9x - 13) + \left(\frac{3007}{729}\right) \\
\frac{3007}{729} &= (x^3 - 2x + 4) - \left(\frac{1}{9}x^2 + \frac{13}{81}x + \frac{7}{729}\right)(9x - 13) \\
&= (x^3 - 2x + 4) - \left(\frac{1}{9}x^2 + \frac{13}{81}x + \frac{7}{729}\right)((4x^3 + x + 3) - (4)(x^3 - 2x + 4)) \\
&= \left(\frac{4}{9}x^2 + \frac{52}{81}x + \frac{757}{729}\right)(x^3 - 2x + 4) - \left(\frac{1}{9}x^2 + \frac{13}{81}x + \frac{7}{729}\right)(4x^3 + x + 3)
\end{aligned}$$

Some algebraic manipulation shows the following:

$$1 = \frac{729}{3007}\left[\left(\frac{4}{9}x^2 + \frac{52}{81}x + \frac{757}{729}\right)(x^3 - 2x + 4) + \left(-\frac{1}{9}x^2 - \frac{13}{81}x - \frac{7}{729}\right)(4x^3 + x + 3)\right]$$

revealing that the gcd is 1.

Question: 5

Find all of the zeros for each of the following polynomials.

a. $5x^3 + 4x^2 - x + 9$ in $\mathbb{Z}_{12}[x]$

b. $3x^3 - 4x^2 - x + 4$ in $\mathbb{Z}_5[x]$

c. $5x^4 + 2x^2 - 3$ in $\mathbb{Z}_7[x]$

d. $x^3 + x + 1$ in $\mathbb{Z}_2[x]$

Solution: You just have to plug all the numbers from 0 to $n - 1$ in $\mathbb{Z}_n$ to see if there are any zeros $\pmod{n}$.

a. There are no zeroes.

b. $x \cong 2 \pmod{5}$.

c. $x \cong 3, 4 \pmod{7}$.

d. There are no zeroes.

Question: 6

Find all of the units in $\mathbb{Z}^x$.

Solution: If $pq = 1$, then $\deg(pq) = 0 \Rightarrow \deg(p) + \deg(q) = 0 \Rightarrow \deg(p) = \deg(q) = 0$. Therefore, p and q can only be ± 1.

Question: 7

Find a unit $p(x)$ in $\mathbb{Z}_4[x]$ such that $\deg p(x) > 1$.

Solution: If we look at $p(x) = (2x+1)^2 = 4x^2 + 4x + 1 = 1 \pmod 4$, we have found at degree 2 unit.

Question: 10

Give two different factorizations of $x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.

Solution: Testing all values of x from 0 to 9, we see that the zeroes $x \cong 1, 3, 6, 8$. Pairing these numbers to add up to -1, we see that they can't. Therefore, we have to make two of these values negative. So, we can say that $x \cong 1, 3, -4, -2$ and pair as follows:

$$\begin{aligned} x^2 + x + 8 &= (x-1)(x+2) \\ &= (x-3)(x+4). \end{aligned}$$

Question: 25

Let F be a field and $f(x) = a_0 + a_1 x + \cdots + a^n x^n$ be in $F[x]$. Define $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ to be the ***derivative*** of $f(x)$.

a. Prove that
$$(f+g)'(x) = f'(x) + g'(x)$$
Conclude that we can define a homomorphism of abelian groups $D : F[x] \longrightarrow F[x]$ by $D(f(x)) = f'(x)$.

b. Calculate the kernel of D if $\operatorname{char} F = 0$.

c. Calculate the kernel of D if $\operatorname{char} F = p$.

d. Prove that
$$(fg)'(x) = f'(x)g(x) + f(x)g'(x).$$

e. Suppose that we can factor a polynomial $f(x) \in F[x]$ into linear factors, say
$$f(x) = a(x-a_1)(x-a_2)\cdots(x-a_n).$$
Prove that $f(x)$ has no repeated factors if and only if $f(x)$ and $f'(x)$ are relatively prime.

Solution:

a.

$$\begin{aligned}(f+g)'(x) &= [f(x)+g(x)]' \\ &= \lim_{h\to 0}\frac{f(x+h)+g(x+h)-f(x)-g(x)}{h} \\ &= \lim_{h\to 0}\frac{f(x+h)-f(x)}{h} + \lim_{h\to 0}\frac{g(x+h)-g(x)}{h} \\ &= f'(x)+g'(x) \quad 😄\end{aligned}$$

This is a homomorphism because we essentially have that $D(f(x)+g(x)) = D(f(x)) + D(g(x))$.

b. $\ker(D) = \{f(x) \in F[x] : f'(x) = 0\}$
$\ker(D) = \{f(x) \in F[x] : f(x) = a, a \in F\}$
$\ker(D) = F$

c. If $\operatorname{char} F = p$, then $f'(x) = 0$ under a few conditions:

(a) Is constant
(b) If not constant, coefficients are multiples of p
(c) If coefficients aren't multiples of p, then exponents are multiples of p
(d) Both

So, the kernel can be described as polynomials that fall under the above criteria.

d. Let us have $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$. Then,

$$(fg)(x) = \sum_{k=0}^{2n}\left\{\sum_{i=max(k-n,0)}^{min(n,k)} a_i b_{k-i}\right\} x^k$$

$$(fg)'(x) = \sum_{k=0}^{2n}\left\{\sum_{i=max(k-n,0)}^{min(n,k)} a_i b_{k-i}\right\} kx^{k-1}$$

We also have the following:

$$f'(x)g(x) = \sum_{k=0}^{2n}\left\{\sum_{i=max(k-n,0)}^{min(k,n)} ia_i b_{k-i}\right\} x^{k-1}$$

$$f(x)g'(x) = \sum_{k=0}^{2n}\left\{\sum_{i=max(k-n,0)}^{min(k,n)} (k-i)a_i b_{k-i}\right\} x^{k-1}$$

So, we have that

$$f'(x)g(x) + f(x)g'(x) = \sum_{k=0}^{2n}\left\{\sum_{i=max(k-n,0)}^{min(k,n)} a_i b_{k-i}\right\} kx^{k-1} = (fg)'(x) \quad 😄$$

e. If $f(x)$ has no repeated factors, then we have that all α_i are distinct in

$$f(x) = \alpha_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Now, let us define $g_i(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_{i+1}) \cdots (x - \alpha_n)$. Then we have that $f(x) = (x - \alpha_i)g_i(x)$.

By the product rule, we have that

$$f'(x) = (x - \alpha_i)g_i'(x) + g_i(x)$$

$$f'(\alpha_i) = g_i(\alpha_i) = \alpha_0(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_n)$$

Since all the zeroes are distinct, this does not evaluate to 0. So, $(x - \alpha_i)$ is not a factor of $f'(x)$. $f(x)$ only has linear factors in the form $(x - \alpha_k)$ for $1 \leqslant k \leqslant n$. Therefore, $f(x)$ and $f'(x)$ are relatively prime.

Now suppose that $f(x)$ has a repeated factor that is $(x-\alpha_i)$ such that $f(x) = (x-\alpha_i)^k g_i(x)$ for some $k \geqslant 2$ and $g_i(x) = \dfrac{f(x)}{(x - \alpha_i)^k}$. Then we have that $f'(x) = k(x - \alpha_i)^{k-1} g_i(x) + (x - \alpha_i)^k g_i'(x)$. So, $f'(x - \alpha_i) = 0$ and as such, is a factor of both $f(x)$ and $f'(x)$, meaning that they are not relatively prime.

Since both directions have been proven, the statement is true. 😄