MATH 135 Fall 2020: Extra Practice 11

Warm-Up Exercises

WE01. Find a real cubic polynomial whose roots include 1 and i.

Solution. Apply the Factor Thorem to create $f(x) = (x-1)(x-i)(x-r)$. To ensure the polynomial is real, make $(x-r)$ the conjugate of $(x-i)$, i.e., $r = -i$. Then, $f(x) = (x-1)(x^2+1) = x^3 - x^2 + x - 1$. □

WE02. Divide $f(x) = x^3 + x^2 + x + 1$ by $g(x) = x^2 + 4x + 3$ to find the quotient $q(x)$ and remainder $r(x)$ that satisfy the requirements of the *Division Algorithm for Polynomials* (DAP)

Solution. Perform polynomial long division:

$$
\begin{array}{r|rrrr}
 & & & x & -3 \\
\hline
x^2+4x+3 & x^3 & +x^2 & +x & +1 \\
 & -x^3 & -4x^2 & -3x & \\
\hline
 & & -3x^2 & -2x & +1 \\
 & & 3x^2 & +12x & +9 \\
\hline
 & & & 10x & +10
\end{array}
$$

and conclude that $q(x) = 10x + 10$ and $r(x) = x - 3$. □

Recommended Problems

RP01. Let $z \in \mathbb{C}$. Prove that $(x-z)(x-\overline{z}) \in \mathbb{R}[x]$.

Proof. Let z be a complex number. Expand the product to obtain

$$
\begin{aligned}
(x-z)(x-\overline{z}) &= x^2 - zx - \overline{z}x + z\overline{z} \\
&= x^2 - (z+\overline{z})x + z\overline{z}
\end{aligned}
$$

which is a polynomial in x with coefficients 1, $-(z+\overline{z})$, and $z\overline{z}$. Clearly, $1 \in \mathbb{R}$. From PCJ3, we have $z + \overline{z} = 2\operatorname{Re} z$ so $-(z+\overline{z}) = -2\operatorname{Re} z \in \mathbb{R}$. Also, from PM3, $z\overline{z} = |z|^2 \in \mathbb{R}$. Therefore, the polynomial is a member of $\mathbb{R}[x]$. □

RP02. Prove that there exists a polynomial in $\mathbb{Q}[x]$ with the root $2 - \sqrt{7}$.

Proof. We propose $f(x) = x^2 - 4x - 3 \in \mathbb{Q}[x]$.

$$f(2-\sqrt{7}) = (2-\sqrt{7})^2 - 4(2-\sqrt{7}) - 3 = 11 - 4\sqrt{7} - 8 + 4\sqrt{7} - 3 = 0$$ □

RP03. For each of the following polynomials $f(x) \in \mathbb{F}[x]$, write $f(x)$ as a product of irreducible polynomials in $\mathbb{F}[x]$.

(a) $x^2 - 2x + 2 \in \mathbb{C}[x]$

Solution. We apply the quadratic formula to find that $x = \frac{2+\sqrt{-4}}{2} = 1 + i$. Then, we also have $x = 1 - i$ as a solution. Therefore, we may write in irreducible polynomials $f(x) = (x - 1 - i)(x - 1 + i)$. □

(b) $x^2 + (-3i + 2)x - 6i \in \mathbb{C}[x]$

Solution. By inspection, $x = -2$ is a root. Divide by $g(x) = x + 2$ to obtain $q(x) = x - 3i$. Therefore, we write in irreducible polynomials $f(x) = (x + 2)(x - 3i)$. □

(c) $2x^3 - 3x^2 + 2x + 2 \in \mathbb{R}[x]$

Solution. The RRT gives $x = 1, -1, 2, -2, \frac{1}{2}, -\frac{1}{2}$ as candidates for roots of f. We find that $f(-\frac{1}{2}) = 0$, so we divide by $g(x) = 2x + 1$ to find $q(x) = x^2 - 2x + 2$. Now, the discriminant of q is negative, so it has no real solutions and is irreducible in $\mathbb{R}[x]$. Therefore, we write $f(x) = (2x + 1)(x^2 - 2x + 2)$. □

(d) $3x^4 + 13x^3 + 16x^2 + 7x + 1 \in \mathbb{R}[x]$

Solution. By inspection, $x = -1$ is a root. Divide by $g(x) = x + 1$ to obtain $q(x) = 3x^3 + 10x^2 + 6x + 1$. To find roots of this cubic, the RRT gives candidates $x = 1, -1, \frac{1}{3}, -\frac{1}{3}$. In fact, $q(-\frac{1}{3}) = 0$. Dividing $q(x)$ by $(3x + 1)$, we obtain the factor $(x^2 + 3x + 1)$. The discriminant of this quadratic is negative, so it is irreducible in $\mathbb{R}[x]$. Therefore, $f(x) = (x + 1)(3x + 1)(x^2 + 3x + 1)$. □

(e) $x^4 + 27x \in \mathbb{C}[x]$

Solution. Factor: $f(x) = x(x^3 + 27)$. The roots are $x = 0$ and $x = \sqrt[3]{-27} = 3\sqrt[3]{-1}$. By the CNRT, the cube roots of -1 are -1, $\frac{1}{2} + \frac{\sqrt{3}}{2}i$, and $\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Therefore,

$$f(x) = x(x - 1)(x - \frac{3}{2} - \frac{3\sqrt{3}}{2}i)(x - \frac{3}{2} + \frac{3\sqrt{3}}{2}i)$$ □

RP04. Let $g(x) = x^3 + bx^2 + cx + d \in \mathbb{C}[x]$ be a monic cubic polynomial. Let z_1, z_2, and z_3 be three roots of $g(x)$ such that

$$g(x) = (x - z_1)(x - z_2)(x - z_3)$$

Prove that

$$\begin{aligned} z_1 + z_2 + z_3 &= -b \\ z_1z_2 + z_2z_3 + z_3z_1 &= c \\ z_1z_2z_3 &= -d \end{aligned}$$

Proof. Let g be a monic cubic polynomial over $\mathbb{C}$, where z_1, z_2, and z_3 are its roots. Then, by CPN, $g(x) = x^3 + bx^2 + cx + d = (x - z_1)(x - z_2)(x - z_3)$ for some coefficients $b, c, d \in \mathbb{C}$. We expand using standard arithmetic:

$$\begin{aligned} x^3 + bx^2 + cx + d &= (x - z_1)(x - z_2)(x - z_3) \\ &= (x^2 - xz_1 - xz_2 + z_1z_2)(x - z_3) \\ &= x^3 - x^2z_1 - x^2z_2 + z_1z_2x - x^2z_3 - z_1z_3x - z_2z_3x - z_1z_2z_3 \\ &= x^3 - (z_1 + z_2 + z_3)x^2 + (z_1z_2 + z_2z_3 + z_3z_1)x - z_1z_2z_3 \end{aligned}$$

Recall that two polynomials are defined to be equal if and only if their coefficients agree. Therefore, $b = -(z_1 + z_2 + z_3)$, $c = z_1z_2 + z_2z_3 + z_3z_1$, and $d = -z_1z_2z_3$ and the conclusion immediately follows. □

RP05. Using the Rational Roots Theorem, prove that $\sqrt{3} + \sqrt{7}$ is irrational.

Proof. Let $a = \sqrt{3} + \sqrt{7}$. Then, $a^2 = 10 + 2\sqrt{21}$ and $a^2 - 10 = 2\sqrt{21}$. Squaring again, $a^4 - 20a^2 + 100 = 84$, i.e., $a^4 + 20a^2 - 16 = 0$.

Now, we can let $f(x) = x^4 - 20x^2 + 16$ such that $f(a) = 0$. The RRT gives that rational roots of f are of the form p/q with coprime integers p and q where $p \mid 16$ and $q \mid 1$. The divisors of 1 are ± 1 and of 16 are $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$. Note that f is even, so we need only test $x = 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$.

Now, $f(1) = 5$, $f(\frac{1}{2}) = -\frac{175}{16}$, $f(\frac{1}{4}) = -\frac{3775}{256}$, $f(\frac{1}{8}) = -\frac{64255}{4096}$, and $f(\frac{1}{16}) = -\frac{1043455}{65536}$.

Therefore, f has no rational roots. However, a is a root of f, therefore, a is irrational. □

RP06.

(a) Prove that for every prime p, there exists a polynomial $f(x)$ over $\mathbb{Z}_p$, of degree p, such that every element of $\mathbb{Z}_p$ is a root of $f(x)$.

Proof. Let p be a prime number. Then, $\mathbb{Z}_p$ is a field. For each element $[n] \in \mathbb{Z}_p$, there is a linear factor $([1]x - [n]) \in \mathbb{Z}_p[x]$. The product of polynomials is well-defined and is a polynomial, so we may say that the polynomial $f(x) \in \mathbb{Z}_p[x]$

$$f(x) = \prod_{[i] \in \mathbb{Z}_p} ([1]x - [i])$$

has p roots corresponding to each of the p elements in $\mathbb{Z}_p$. The degree of a product is the sum of the degrees of the factors, but each factor is linear with degree 1 so the sum is simply p. □

(b) Prove that for every prime p, there exists a polynomial $f(x)$ over $\mathbb{Z}_p$, of degree p, which has no roots in $\mathbb{Z}_p$.

Proof. Let p be a prime number and let $g(x)$ be the polynomial from (a) above for p. Then, $g(x) \equiv 0 \pmod{p}$ for any $x \in \mathbb{Z}_p$. Therefore, $g(x) \not\equiv 1 \pmod{p}$ for any x and we may say the polynomial $f(x) = g(x) - 1$ has no solutions in $\mathbb{Z}_p$. □

RP07. Suppose $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{C}[x]$ with degree n. We say $f(x)$ is *palindromic* if the coefficients a_j satisfy

$$a_{n-j} = a_j \quad \text{for all} \quad 0 \le j \le n$$

Prove that

(a) If $f(x)$ is a palindromic polynomial and $c \in \mathbb{C}$ is a root of $f(x)$, then c must be non-zero, and $\frac{1}{c}$ is also a root of $f(x)$.

Proof. Let $f(x) \in \mathbb{C}[x]$ be a palindromic polynomial with coefficients a_n and root c so

$$0 = a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0$$

Since $f(x)$ has degree n, $a_n \neq 0$. As $f(x)$ is palindromic, $a_0 \neq 0$. Suppose that $c = 0$ and substitute above. We have that $a_0 = 0$, which is a contradiction. Therefore, $c \neq 0$. Now, multiplying through by c^{-n}, we have

$$0 = a_n + a_{n-1}c^{-1} + \cdots + a_1 c^{-n+1} + a_0 c^{-n}$$

but since $f(x)$ is palindromic we substitute a_{n-j} for a_j and write

$$0 = a_0 + a_1\left(\frac{1}{c}\right) + \cdots + a_{n-1}\left(\frac{1}{c}\right)^{n-1} + a_n\left(\frac{1}{c}\right)^n$$

But this is just saying $f(\frac{1}{c}) = 0$, that is, $\frac{1}{c}$ is a root of $f(x)$. □

(b) If $f(x)$ is a palindromic polynomial of odd degree, then $f(-1) = 0$.

Proof. Let $f(x)$ be a palindromic polynomial in $\mathbb{C}$ with odd degree n and coefficients a_n. Since n is odd, we have $n = 2k + 1$ for some integer k. Then,

$$f(-1) = a_{2k+1}(-1)^{2k+1} + a_{2k}(-1)^{2k} + \cdots + a_1(-1) + a_0$$

and we apply the fact that $a_{n-j} = a_j$ for all $0 \leq j \leq k$ to get

$$f(-1) = a_0(-1)^{2k+1} + a_1(-1)^{2k} + \cdots + a_k(-1)^{k+1} + a_k(-1)^k + \cdots + a_1(-1) + a_0$$

Notice that there are an even ($n + 1 = 2k + 2$) number of terms. We pair them by common coefficients. Let $0 \leq i \leq k$. Then, the coefficient a_i appears in the terms $a_i(-1)^{2k+1-i}$ and $a_i(-1)^i$. The difference in the powers is $2(k-i)+1$, an odd number. Therefore, one is even and the other is odd. Suppose WLOG that i is even. Then, $a_i(-1)^{2k+1-i} = -a_i$ and $a_i(-1)^i = a_i$.

It follows that each term cancels its palindromic term, and the resulting sum is 0. □

(c) If $\deg f = 1$ and $f(x)$ is a monic, palindromic polynomial, then $f(x) = x + 1$.

Proof. Let $f(x)$ be a first-degree polynomial in $\mathbb{C}$, that is, $f(x) = a_1 x + a_0$. Since $f(x)$ is monic, its leading coefficient a_1 is 1. However, since $f(x)$ is palindromic, $a_{\deg f - 1} == a_{1-1} = a_0 = 1$ as well. Therefore, $f(x) = x + 1$. □

Challenge

C01. We call a polynomial primitive if the greatest common divisor of all of its coefficients is 1. Show that the product of two primitive polynomials is again primitive.