1. 18CE6 Show that \( f(x) = x^5 + x^4 + 2x^3 + 2x + 2 \) is irreducible in \( \mathbb{F}_3[x] \) as follows: (i) Show that \( f(x) \) has no roots in \( \mathbb{F}_3 \). (ii) Suppose \( f(x) = (ax^2 + bx + c)(dx^3 + ex^2 + fx + g) \), then you can assume \( a = d = 1 \); multiply the right side together collect coefficients of \( x^4, x^3, x^2, x, 1 \) together and equate them to the coefficients of \( f(x) \) to get five equations in the five unknowns \( b, c, e, f, g \). Show the the five equations have no simultaneous solution in \( \mathbb{F}_3 \).

(i) To check whether \( f(x) \) has any linear factors we check to see if it has any roots (this is enough by the root theorem). But clearly:

\[
\begin{align*}
f(0) &= (0)^5 + (0)^4 + 2(0)^3 + 2(0) + 2 = 2 \\ f(1) &= (1)^5 + (1)^4 + 2(1)^3 + 2(1) + 2 = 8 = 2 \\ f(2) &= (2)^5 + (2)^4 + 2(2)^3 + 2(2) + 2 = 70 = 1 
\end{align*}
\]

so we conclude that \( f \) has no linear factors.

(ii) If \( f(x) \) has any factors, it must have a quadratic factor, so that \( f(x) = (ax^2 + bx + c)(dx^3 + ex^2 + fx + g) \). Now \( ad = 1 \), thus \( a = d^{-1} \). So if \( a \neq 1 \neq d \) we can rewrite \( f \) as

\[
f(x) = (ax^2 + bx + c)(dx^3 + ex^2 + fx + g) = ad(ax^2 + bx + c)(dx^3 + ex^2 + fx + g) = (aax^2 + abx + ac)(dax^3 + ebx + dc) = (x^2 + abx + ac)(x^3 + eax^2 + afx + ag)
\]

and thus it is clear that we may take \( a = 1 = d \).

Expanding our expression for \( f \) we find that:

\[
x^5 + x^4 + 2x^3 + 2x + 2 = f(x) = x^5 + (b + e)x^4 + (c + be + f)x^3 + (ce + bf + g)x^2 + (cf + bg)x + cg \text{ or thus that}
\]

\[
\begin{align*}
b + e &= 1 \\
c + be + f &= 2 \\
cea + b + f + g &= 0 \\
cf + bg &= 2 \\
cg &= 2 
\end{align*}
\]

These equations aren’t linear, of course, so we have to be a little more thoughtful to solve them. We know, for instance, that \( c = 1 \) or \( c = 2 \) (remember we are in \( \mathbb{F}_3 \)). It is also the case that \( b = 0, b = 1, \) or \( b = 2 \).

Note that \( g = 2/c \) and \( e = 1 - b \) so that \( f = 2 - c - be, f = (-g - ce)/b \), and \( f = (2 - bg) \).

A little table will be helpful.

<table>
<thead>
<tr>
<th>c</th>
<th>g</th>
<th>b</th>
<th>e</th>
<th>f = 2 - c - be</th>
<th>f = (-g - ce)/b</th>
<th>f = (2 - bg)/c</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>*</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>*</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>
2. 21AE5 If \( p(x) \) has degree \( 2d \) and \( n_1, \ldots, n_d \) are distinct integers such that \( p(n_i) = p_i \) is prime for each \( i, 1 \leq i \leq d \), how many polynomials \( a_s(x) \) arise as possible divisors of \( p(x) \) using Lagrange interpolation? Do they all pair off as associates?

First of all, there is a typo in this problem. It should say: \( n_1, \ldots, n_d \) are distinct integers such that \( p(n_i) = p_i \) is prime for each \( i, 0 \leq i \leq d \) . . .

That settled, suppose that \( s = \{s_0, \ldots, s_d\} \) is a vector such that \( s_i \mid p_i \) for all \( 0 \leq i \leq d \). Because the \( p_i \) are prime, it follows that \( s_i = 1, s_i = -1, s_i = p_i, \) or \( s_i = -p_i \). Thus for each \( s_i \) there are four possibilities, and thus it is clear that there are \( 4^{d+1} \) such vectors.

We need to show that if \( s \) and \( s' \) are two such vectors with the additional property that \( s \neq s' \), then \( a_s(x) \neq a_{s'}(x) \). This will guarantee that there are \( 4^{d+1} \) possible polynomials \( a_s(x) \).

By reordering the \( n_i \) we may assume that \( s_0 \neq s'_0 \). If \( a_{s_1}(x) = a_{s_2}(x) \) we know that \( s_0 h_0(n_0) + \cdots + s_n h_d(n_0) = s'_0 h'_0(n_0) + \cdots + s'_{n_d} h'_{d}(n_0) \). But \( h_0(n_0) = 0 = h'_i(n_0) \) for \( i \geq 1 \), and \( h_0(n_0) = 1 = h'_0(n_0) \), so \( s_0 h_0(n_0) = s'_0 h'_0(n_0) \), that is, \( s_0 = s'_0 \), a contradiction. We conclude that \( a_s(x) \neq a_{s'}(x) \) as required.

Finally, not that if \( s = \{s_0, \ldots, s_d\} \) is a vector such that \( s_i \mid p_i \) for all \( 0 \leq i \leq d \), then the same is also true of \( -s = \{-s_0, \ldots, -s_d\} \). But because \( a_s(x) \) is the unique polynomial of degree \( \leq d \) such that \( a_s(n_i) = p_i \) for \( 0 \leq i \leq d \), the fact that \( -a_s(s_i) = -s_i = a_{-s} \) implies that \( -a_s(x) = a_{-s}(x) \). That says that \( -a_s(x) \) and \( a_{-s}(x) \) are associates so that the \( a_s(x) \) do pair off as associates.

3. Problem 2. How many ways are there of coloring the following, where two colorings are considered identical if they differ by a rotation: (a) a 2x2 square with 3 colors, (b) a 3x3 square with 3 colors, (c) a 2x2 square with \( n \) colors.

We could use Burnside lemma to do each of these problems, but probably it is easier to use theorem 11.1.

Here the group \( G \) acting on our solids is \( G = \{\epsilon, \rho, \rho^2, \rho^3\} \), where \( \rho \) is rotation a quarter turn counter clockwise. Thus if \( X = \{1, \ldots, n\} \) is the number of squares, the element \( \pi^{(k)} \in G^{(k)} \) acts on \( \{c_1, \ldots, c_n\} \in C_k(X) \) by the rule \( \pi^{(k)}(\{c_1, \ldots, c_n\}) = \{c_{\pi^{-1}(1)}, \ldots, c_{\pi^{-1}(n)}\} \). Under this scheme, and numbering the squares of the matrix from 1 to \( n \), the color of the \( i \)th square in the resulting matrix (after acting by \( \pi^{(k)} \)), is the color that was in the \( \pi^{-1}(i) \)th square in the original matrix. This change in subscripts put color \( c_i \) in the \( j \)th square if and only if the color \( c_i \) is in the square that moves onto the \( j \)th square after acting on our matrix with \( \pi \).

Thus the orbits of \( G^{(k)} \) are in one-to-one correspondence with the \( nxn \) matrices colored with \( k \) colors where we regard two matrices equal if one can be obtained from the other by a rotation.

But \( P_G(x) \) is easy to calculate. For (a) the elements of group \( G \) are in cycle notation \( \epsilon = (1)(2)(3)(4), \rho = (1234), \rho^2 = (13)(24), \) and \( \rho^3 = (1432) \). Thus \( P_G(x) = 1/4(x^4 + x^2 + 2x) \) and \( P_G(3) = 1/4(3^4 + 3^2 + 2 \cdot 3) = 24 \).
For (b), the elements of group $G$ are in cycle notation $\epsilon = (1)(2)(3)(4)(5)(6)(7)(8)(9)$, $\rho = (1793)(2486)(5)$, $\rho^2 = (19)(37)(28)(46)(5)$, and $\rho^3 = (1397)(2684)(5)$.

Here I am thinking of the squares labeled as follows:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

Thus in this instance $P_G(x) = 1/4(x^9 + x^5 + 2x^3)$, so $P_G(3) = 1/4(3^9 + 3^5 + 2 \cdot 3^3) = 4995$.

Finally, in (c) we note that the same polynomial from part (a) tells us that there are $P_G(n) = 1/4(n^4 + n^2 + 2n)$ possible colorings. $P_G(n) = 1/4(n^4 + n^2 + 2 \cdot n)$. 