Problem 1.

(a) Consider the following matrix, whose entries are elements of the field $\mathbb{Z}_{11}$.

$$A = \begin{bmatrix} 7 & 4 \\ 4 & 3 \end{bmatrix}.$$  

The characteristic polynomial of this matrix is:

$$|A - \lambda I| = \begin{vmatrix} 7 - \lambda & 4 \\ 4 & 3 - \lambda \end{vmatrix} = (7 - \lambda)(3 - \lambda) - 16 = \lambda^2 + \lambda + 5.$$  

This polynomial factors over $\mathbb{Z}_{11}$:

$$\lambda^2 + \lambda + 5 = (\lambda - 2)(\lambda - 8).$$  

Therefore, the eigenvalues are 2 and 8.

(b) Using the usual procedure for finding eigenvectors, we find that $\begin{bmatrix} 8 \\ 1 \end{bmatrix}$ is an eigenvector for 2, and $\begin{bmatrix} 4 \\ 1 \end{bmatrix}$ is an eigenvector for 8.

Problem 2.

(a)  

**Proposition.** If $p$ is prime and $0 < k < p$, then $\binom{p}{k}$ is a multiple of $p$.  

**Proof.** Let $p$ be a prime number and let $0 < k < p$. Recall that

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k(k-1)(k-2)\cdots(1)}.$$

Clearly the numerator is a multiple of $p$. Moreover, since $k < p$, all of the terms in the denominator are smaller than $p$, so none of them have $p$ as a factor. It follows that the quotient is a multiple of $p$.  

Proposition. If $p$ is prime, then

$$(x + y)^p \equiv x^p + y^p \pmod{p}$$

for all $x, y \in \mathbb{Z}$.

Proof. Let $p$ be a prime number, and let $x, y \in \mathbb{Z}$. By the Binomial Theorem

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \cdots + \binom{p}{p-1} x y^{p-1} + y^p.$$

From part (a), we know that each of the binomial coefficients appearing in the middle is a multiple of $p$. That is, each of these coefficients is congruent to 0 modulo $p$. Then

$$(x + y)^p \equiv x^p + 0x^{p-1}y + 0x^{p-2}y^2 + \cdots + 0xy^{p-1} + y^p \pmod{p}$$

$$\equiv x^p + y^p \pmod{p}.$$

\[\square\]

(c)

Proposition. If $p$ is prime, then

$$(x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \pmod{p}$$

for all $n \in \mathbb{N}$ and all $x_1, \ldots, x_n \in \mathbb{Z}$.

Proof. Let $p$ be a prime. We proceed by induction on $n$. The base case is $n = 1$, for which the proposition is trivially true.

Now suppose that the proposition holds for sums of length $n$, and let $x_1, \ldots, x_n, x_{n+1} \in \mathbb{Z}$. From part (b), we know that

$$(x_1 + \cdots + x_n + x_{n+1})^p = ((x_1 + \cdots + x_n) + x_{n+1})^p$$

$$\equiv (x_1 + \cdots + x_n)^p + x_{n+1}^p \pmod{p}.$$

From our induction hypothesis, we know that

$$(x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \pmod{p}$$

and thus

$$(x_1 + \cdots + x_n + x_{n+1})^p \equiv x_1^p + \cdots + x_n^p + x_{n+1}^p \pmod{p}.$$

Therefore, by induction, the proposition holds for all $n \in \mathbb{N}$. \[\square\]
Theorem (Fermat’s Little Theorem). If $p$ is prime, then

$$n^p \equiv n \pmod{p}$$

for any $n \in \mathbb{N}$.

Proof. Let $n \in \mathbb{N}$. By part (c), we know that

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod{p}$$

for any $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. Substituting $x_1 = x_2 = \cdots = x_n = 1$ gives

$$(1 + 1 + \cdots + 1)^p \equiv 1^p + 1^p + \cdots + 1^p \pmod{p}$$

which simplifies to

$$n^p \equiv n \pmod{p}.$$ 

\[ \square \]

Problem 3.

(a) There are four automorphisms:

1. The identity function, which we will denote by the letter $e$.
2. The function $f$ that switches $1 \rightleftharpoons 2$, $3 \rightleftharpoons 6$, and $4 \rightleftharpoons 5$.

\[
\begin{array}{|c|ccccccc|}
\hline
x & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
f(x) & 2 & 1 & 6 & 5 & 4 & 3 \\
\hline
\end{array}
\]

3. The function $g$ that switches $1 \rightleftharpoons 4$ and $2 \rightleftharpoons 5$, and fixes $3$ and $6$.

\[
\begin{array}{|c|ccccccc|}
\hline
x & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
g(x) & 4 & 5 & 3 & 1 & 2 & 6 \\
\hline
\end{array}
\]

4. The function $h$ that switches $1 \rightleftharpoons 5$, $2 \rightleftharpoons 4$, and $3 \rightleftharpoons 6$.

\[
\begin{array}{|c|ccccccc|}
\hline
x & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
h(x) & 5 & 4 & 6 & 2 & 1 & 3 \\
\hline
\end{array}
\]

(b) The following table shows the compositions of the automorphisms from part (a).

\[
\begin{array}{|c|cccccc|}
\hline
\circ & e & f & g & h \\
\hline
e & e & f & g & h \\
f & f & e & h & g \\
g & g & h & e & f \\
h & h & g & f & e \\
\hline
\end{array}
\]