1. Let $\text{plq}$ mean $p \land \lnot q$. Show that the formula $\lnot p$ is not tautologically equivalent to a proposition whose only connective is $\lnot$. (10 pts.)

**Proof:** We first show that no proposition with $\lnot$ as the only connective can assume the truth value always 1. Assume not. Let $\alpha$ be such a proposition of smallest length. Write $\alpha = \beta \gamma$. Then $\beta$ must always assume the truth value 1, contradicting the fact that $\alpha$ was the smallest such proposition.

We can now show that no proposition with $\lnot$ as the only connective can be tautologically equivalent to $\lnot p$.

A proposition $\alpha = \alpha(p, ...)$ with $\lnot$ as the only connective is of the form

$$\beta(p, ...) \eta(p, ...)$$

for some shorter propositions $\beta$ and $\eta$. Here "..." denotes the fact that we may have other atomic propositions in the expressions. Choose $\alpha$ to be tautologically equivalent to $\lnot p$ and of minimal length with this property. Since $\alpha$ is tautologically equivalent to $\lnot p$ we must have,

a) $\beta(0, ...) = 1$ and $\gamma(0, ...) = 0$ (so that $\alpha(0, ...) = \lnot 0 = 1$) and

b) Either $\beta(1, ...) = 0$ or $\gamma(1, ...) = 1$ (so that $\alpha(1, ...) = \lnot 1 = 0$).

Let us consider the two subcases of case b separately.

If $\beta(1, ...) = 0$, then, because of condition a, $\beta$ is itself equivalent to $\lnot p$, contradicting the fact that $\alpha$ is of minimal length with this property. Thus $\beta(1, ...) = 1$. Thus $\beta$ always assumes the truth value 1, contradicting our first fact.

2. How many words can you write using all the letters of ABRAKADABRA? (A must be used 5 times, B twice etc.) (10 pts.)

**Answer:** Let us first replace the five A’s by A, A, A, A, A in the order of their appearance and the two B’s and R’s by B and B and R and R in that order. Now we have 11 different letters. We can order them in 11! different ways. Identifying the A’s, B’s and R’s reduces this number to $11!/(5!2!2!) = 11 \times 10 \times 9 \times 8 \times 7 \times 6/4 = 11 \times 10 \times 9 \times 2 \times 7 \times 6 = 110 \times 18 \times 42 = 1980 \times 42 = 83160$.

3. Consider the polynomial $(X_1 + X_2 + ... + X_n)^k$ in $n$ variables $X_1, ..., X_n$. When multiplied out, this polynomial is equal to a polynomial of the form

$$\sum_{i_1 + i_2 + ... + i_n = k} a(i_1, ..., i_n) X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$$

for some $a(i_1, ..., i_n) \in \mathbb{N}$. Here, $k$ runs over all natural numbers and $i_1, i_2, ..., i_n$ run over all natural numbers whose sum is $k$. Find $a(i_1, ..., i_n)$. Applying the above formula to various values of $X_1, X_2, ..., X_n$ deduce some combinatorial formulas. (20 pts.)

**Answer:** Write the product $(X_1 + X_2 + ... + X_n)^k$ in the form

$$(X_1 + X_2 + ... + X_n) (X_1 + X_2 + ... + X_n) ... (X_1 + X_2 + ... + X_n).$$

Here, there are $k$ factors. To execute the multiplication, from each factor we choose one of the $X_i$’s and multiply these choice to get some monomial of the form $X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$. Given $i_1, ..., i_n$ whose sum is $k$, we have to find out in how many ways we can choose the $X_i$’s from each factor so as to obtain $X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$. We have $k$ factors to choose $i_1$ many $X_i$’s. Thus $X_1^{i_1}$ can be chosen in $\binom{k}{i_1}$ many ways. Now for $X_2$, there are only $k - i_1$ factors left to choose from.
From these \( k - i_1 \) factors we have to choose \( i_2 \) many \( X_2 \)'s. Hence the number of choice for \( X_2^{i_2} \) is \( \binom{k - i_1}{i_2} \). In a similar way, we find that the number of choices for \( X_3 \) is \( \binom{k - i_1 - i_2}{i_3} \). Hence the monomial \( X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} \) can be chosen in
\[
\binom{k}{i_1} \binom{k - i_1}{i_2} \binom{k - i_1 - i_2}{i_3} \ldots \binom{k - i_1 - i_2 - \ldots - i_{n-1}}{i_n}
\]
many ways. This can also be written as,
\[
\frac{k!}{i_1! (k - i_1)! i_2! (k - i_1 - i_2)! i_3! (k - i_1 - i_2 - i_3)! \ldots i_n! (k - i_1 - i_2 - i_3 - \ldots - i_{n-1})!}
\]
\[
= \frac{k!}{i_1! i_2! \ldots i_n!}.
\]
Thus
\[
a(i_1, \ldots, i_n) = \frac{(i_1 + \ldots + i_n)!}{i_1! i_2! \ldots i_n!}.
\]

**Application.** Thus,
\[
(X_1 + \ldots + X_n)^k = \sum_{i_1 + i_2 + \ldots + i_n = k} a(i_1, \ldots, i_n) X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}
\]
\[
= \sum_{i_1 + i_2 + \ldots + i_n = k} \frac{(i_1 + \ldots + i_n)!}{i_1! i_2! \ldots i_n!} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}
\]
Let us take \( X_i = 1 \) for all \( n \) to get,
\[
\sum_{i_1 + i_2 + \ldots + i_n = k} \frac{(i_1 + \ldots + i_n)!}{i_1! i_2! \ldots i_n!} = n^k,
\]
a nice formula to my taste.

4. **Show that in any ring a prime element is irreducible.** (10 pts.)

**Proof:** Let \( R \) be any (commutative) ring (with 1). Recall that an element \( p \in R \setminus R^* \) which is not a zero divisor is called **prime** if whenever \( p \) divides \( xy \) then \( p \) divides either \( x \) or \( y \). An element \( p \in R \setminus R^* \) which is not a zero divisor is called **irreducible** if whenever \( p = xy \) then either \( x \) or \( y \) is in \( R^* \). Assume \( p \) is prime in \( R \). Assume \( p = xy \). Then \( p \) divides \( xy \). Since \( p \) is prime, this implies that \( p \) divides either \( x \) or \( y \). The situation being symmetrical with respect to \( x \) and \( y \), we may assume that \( p \) divides \( x \). Let \( z \in R \) be such that \( x = pz \). Now \( p = xy = pzy \) and \( p(1-zy) = 0 \). Since \( p \) is not a zero divisor, this implies that \( 1 - zy = 0 \), i.e. \( zy = 1 \) and so \( z = 1 \) and so \( y \in R^* \).

5. **Let \( f_i \) be the number of words in letters \( a, b \) and \( c \)'s of length \( n \) without the subword \( abc \).**

5a. **Find a recursive formula for \( f_n \).**

5b. **Compute \( f_6 \) and \( f_7 \).**

(20 pts.)

**Answer:** Clearly \( f_1 = 1 \) (the empty word), \( f_2 = 9, f_3 = 27 - 1 = 26 \) (all but \( abc \)), \( f_4 = 3^4 - 6 \) (all but \( abca, abeb, abcc, aabc, babc, cabc \)). Now let \( n \geq 3 \). Given a word \( w \) without \( abc \) of length \( n - 1 \), we can freely add \( a \) or \( b \) to the end of \( w \) to obtain the words \( wa \) and \( wb \) without
abc. We can also add c to get the words wa, wb and wc without abc in case the word w of length \( n - 1 \) does not end with ab. If \( g_n \) denotes the number of words without abc that end with ab then, the above discussion shows that

\[ f_n = 3(f_{n-1} - g_{n-1}) + 2g_{n-1}. \]

So let us compute \( g_n \). Clearly to any word w without abc of length \( n - 2 \), we can add ab to the end to get wab, a word without abc and that ends with ab. Thus,

\[ g_n = f_{n-2}. \]

Therefore

\[ f_n = 3(f_{n-1} - g_{n-1}) + 2g_{n-1} = 3(f_{n-1} - f_{n-3}) + 2f_{n-3} = 3f_{n-1} - f_{n-3}. \]

By using this formula we can compute \( f_n \) recursively:

\[
\begin{align*}
  f_1 &= 1, \\
  f_2 &= 9, \\
  f_3 &= 3f_2 - f_0 = 27 - 1 = 26 \\
  f_4 &= 3f_3 - f_1 = 3 \times 26 - 1 = 75 \\
  f_5 &= 3f_4 - f_2 = 3 \times 75 - 9 = 216 \\
  f_6 &= 3f_5 - f_3 = 3 \times 216 - 26 = 622 \\
  f_7 &= 3f_6 - f_4 = 3 \times 622 - 75 = 1791.
\end{align*}
\]

6. **How many irreducible polynomials are there in \( \mathbb{Z}[X] \) of the form \( X^2 + aX + b \) where \( a, b \in \{-2, -1, 0, 1, 2\} \)? (15 pts.)**

**Answer:** A reducible polynomial of the form \( X^2 + aX + b \) must be a product of two monic polynomials of degree 1, thus they must have at least one root in \( \mathbb{Z} \). Since the roots are given by

\[ a \pm \sqrt{a^2 - 4b} \]

the coefficients \( a \) and \( b \) must satisfy the following two conditions:

a) the discriminant \( a^2 - 4b \) must be a perfect square in \( \mathbb{Z} \), and

b) Since an eventual root must be in \( \mathbb{Z} \) and not in \( \mathbb{Q} \), \( -a + \sqrt{a^2 - 4b} \) must be divisible by 2, i.e. \( a^2 - 4b \) and \( a \) must be of the same parity, but this is always the case.

We compute \( a^2 - 4b \) case by case to see which pairs \((a, b)\) satisfy the condition a (condition b is automatically satisfied):

\[
\begin{array}{c|c|c|c|c|c|c|c}
  a^2 - 4b & a = -2 & a = -1 & a = 0 & a = 1 & a = 2 \\
  b = -2 & 12 & 9 & 8 & 9 & 12 \\
  b = -1 & 8 & 5 & 4 & 5 & 8 \\
  b = 0 & 4 & 1 & 0 & 1 & 4 \\
  b = 1 & 0 & -3 & -4 & -3 & 0 \\
  b = 2 & -4 & -7 & -8 & -7 & -4
\end{array}
\]

We printed bold face the output \( a^2 - 4b \) in case it is not a square. There are 15 of them.

So there are 15 irreducible polynomials that satisfy the given conditions.

7. **Find all irreducible polynomials of degree 3 of \((\mathbb{Z}/2\mathbb{Z})[X]\).** (15 pts.)

**Answer:** Clearly a reducible polynomial of degree 3 must have a factor of degree 1, i.e. must be divisible either by \( X \) or by \( X - 1 \), hence it must have a root (either 0 or 1). Let us list all polynomials of degree 3 and find out the ones that do not have a root, these are the irreducible ones:
<table>
<thead>
<tr>
<th>Polynomial $f(X)$</th>
<th>$f(0)$</th>
<th>$f(1)$</th>
<th>Result</th>
<th>Decomposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X^3$</td>
<td>0</td>
<td>1</td>
<td>reducible</td>
<td>$XXX$</td>
</tr>
<tr>
<td>$X^3 + 1$</td>
<td>1</td>
<td>0</td>
<td>reducible</td>
<td>$(X + 1)(X^2 + X + 1)$</td>
</tr>
<tr>
<td>$X^3 + X$</td>
<td>0</td>
<td>0</td>
<td>reducible</td>
<td>$X(X + 1)^2$</td>
</tr>
<tr>
<td>$X^3 + X + 1$</td>
<td>1</td>
<td>1</td>
<td>irreducible</td>
<td></td>
</tr>
<tr>
<td>$X^3 + X^2$</td>
<td>0</td>
<td>0</td>
<td>reducible</td>
<td>$X^2(X + 1)$</td>
</tr>
<tr>
<td>$X^3 + X^2 + 1$</td>
<td>1</td>
<td>1</td>
<td>irreducible</td>
<td></td>
</tr>
<tr>
<td>$X^3 + X^2 + X$</td>
<td>0</td>
<td>1</td>
<td>reducible</td>
<td>$X(X^2 + X + 1)$</td>
</tr>
<tr>
<td>$X^3 + X^2 + X + 1$</td>
<td>1</td>
<td>0</td>
<td>reducible</td>
<td>$(X+1)^3$</td>
</tr>
</tbody>
</table>