1. (10 points) Let \( f(x) = x^4 + rx^3 + 5x^2 + 1 \in \mathbb{Z}[x] \). For which integers \( r \) is \( f(x) \) irreducible? Prove your answer.

**Solution:** If \( a \) is a zero of \( f(x) \), then \( x - a \) is a factor of \( f(x) \), \( f(a) = 0 \) and \( a \) must be \( \pm 1 \) since the constant term in \( f(x) \) is one. Since \( f(1) = 7+r \) and \( f(-1) = 7 - r \), \( f(x) \) has zero if \( r = \pm 7 \).

Now suppose that \( f(x) \) has two quadratic factors

\[
f(x) = (x^2 + ax + b)(x^2 + cx + d)
\]

\[
= x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd.
\]

Since \( bd = 1 \), \( b = d = \pm 1 \), and the coefficient of \( x \) is \( \pm(a + c) = 0 \). This means that \( r = 0 \) and the coefficient of \( x^2 \) is \( -a^2 \pm 2 = 5 \), or \( a^2 = -5 \pm 2 < 0 \), but there is no integer \( a \) that satisfies this condition.

Therefore, \( f(x) \) is irreducible unless \( r = \pm 7 \).

A common mistake was to say that \( f(x) \) is reducible if \( r = 0 \), but this is not the case, as explained above.

2. (10 points) Prove that in a finite \( G \)-set \( X \), if \( g \) and \( g' \) are conjugate elements in \( G \), then their fixed point sets \( X_g \) and \( X_{g'} \) have the same cardinality.

**Solution:** Since \( g' \) is conjugate to \( g \), \( g' = hgh^{-1} \) for some \( h \in G \). Now suppose \( x \in X_g \). Then

\[
g'(h(x)) = hgh^{-1}h(x) = hg(x) = h(x),
\]

so \( h(x) \in X_{g'} \). Similarly, if \( x' \in X_{g'} \), then \( h^{-1}(x') \in X_g \). Hence the action of \( h \) gives a one-to-one correspondance between \( X_g \) and \( X_{g'} \), so \( |X_g| = |X_{g'}| \).

3. (15 points) You are painting blocks that are shaped like triangular prisms. Each block has two triangular faces and three rectangular ones. You have \( n \) colors to choose from for each of the 5 faces. Use Burnside’s formula to determine the number of distinguishable blocks that can be made in this way. How big does \( n \) have to be in order to get 100 distinguishable blocks? (Hint: The relevant group here is \( S_3 \). A prism has 9 edges, three surrounding each triangular face and three others that are parallel and have rectangular faces on either side of them. Each rotation of the prism permutes the three parallel edges.)
SOLUTION: Since the group is \( S_3 \), Burnside’s formula says that the number of orbits is
\[
r = \frac{\sum_{g \in S_3} |X_g|}{6},
\]
where \( X \) is the set of all possible colorings. Since a prism has 5 faces, \( |X| = n^5 \). There are three conjugacy classes of elements in \( S_3 \). In order to describe the rotation of the prism corresponding to each of them, assume that the prism is placed so that its triangular faces are horizontal (at the top and bottom) and its rectangular faces are vertical. The following table shows the relevant information.

| \( g \in S_3 \) | Size of conjugacy class | Rotation of prism | \( |X_g| \) | Burnside term |
|-----------------|------------------------|-------------------|-----------|-------------|
| \( e \)         | 1                      | none              | \( n^5 \)  | \( n^5 \)    |
| \( (12) \)      | 3                      | 180° rotation about rectangular face center | \( n^3 \)  | \( 3n^4 \)   |
| \( (123) \)     | 2                      | 120° rotation about vertical axis | \( n^3 \)  | \( 2n^5 \)   |

The 180° rotation interchanges the two triangular faces, and two of the rectangular ones, making three possible colors. The 120° rotation leaves each triangular face invariant while cyclically permuting the three rectangular ones, also making three possible colors. It follows that
\[
r = \frac{n^5 + 5n^3}{6}
\]
This is 63 for \( n = 3 \) and 224 for \( n = 4 \).

4. (10 points) Find the largest integer \( m \) which divides \( n^{21} - n \) for all integers \( n \).

SOLUTION: We will use Fermat’s little theorem, which says that if a prime \( p \) does not divide \( n \), then \( n^{p-1} \equiv 1 \) modulo \( p \). Since
\[
n^{21} - n = n(n^{20} - 1),
\]
if \( p - 1 \) divides 20, then \( n^{21} - n \) is divisible by \( p \). The primes \( p \) for which this is true are 2, 3, 5 and 11. This means that \( n^{21} - n \) is always divisible by their product, 330. For any other prime \( q \) there is an \( n \) such that neither \( n \) nor \( n^{20} - 1 \) are divisible by \( q \). For any prime \( p \), the number \( p^{21} - p = p(p^{20} - 1) \) is divisible by \( p \), but not by \( p^2 \). This means \( m \) is not divisible by the square of any prime (it is square free), so our \( m \) is 330.

5. (15 points) Prove that every finite integral domain \( D \) is a field.

SOLUTION: Suppose \( |D| = n \) and
\[
D = \{0, 1, a_1, a_2, \ldots, a_{n-2}\},
\]
so the set of nonzero elements in \( D \) is
\[
D^* = \{1, a_1, a_2, \ldots, a_{n-2}\}
\]
For $x \in D^*$, consider the set

$$xD^* = \{x, xa_1, xa_2, \ldots xa_{n-2}\}.$$  

Since $D$ is a domain, this set does not contain 0. Its elements are all distinct since $xa_i = xa_j$ for $i \neq j$ would mean $x(a_i - a_j) = 0$, which would make $x$ a zero divisor. Hence $xD^*$ has all $n - 1$ nonzero elements of $D$, including 1. This means that $x$ has an inverse, so $D$ is a field.

6. (10 points) Describe the center subgroup of every simple
(a) abelian group
(b) nonabelian group
and prove your answer.

Solution: If $G$ is abelian, then $Z(G) = G$, even if $G$ is not simple. The center of any group is a normal subgroup, so if $G$ is a simple nonabelian group, $Z(G)$ is a normal subgroup smaller than $G$, so it is the trivial subgroup.

7. (10 points) Show that in the ring $\mathbb{Z}/p$, $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{Z}/p$.

Solution: The binomial theorem tells us that in any commutative ring,

$$ (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i. $$

We also know that the binomial coefficient is given by

$$ \binom{p}{i} = \frac{p!}{i!(p-i)!}. $$

For $0 < i < p$ and $p$ prime, the numerator is divisible by $p$ but the denominator is not, so the integer $\binom{p}{i}$ is divisible by $p$. This means that the second sum above is divisible by $p$, so that in $\mathbb{Z}/p$,

$$ (a+b)^p = a^p + b^p. $$

8. (15 points) Recall that the third Sylow theorem says that if $|G| = ps$ where $p$ is prime and does not divide $s$, then the number $k_p$ of subgroups of order $p$ divides $s$ and is congruent to 1 modulo $p$. Use it to prove that every group $G$ of order 1001 is cyclic.

Solution: We will show that $G$ is cyclic by showing that is has an element of order 1001. We will do this by showing that there are fewer than 1001 elements of smaller order. Since $1001 = 7 \cdot 11 \cdot 13$, so there are three primes in the picture. The possible smaller orders are 1, 7, 11, 13, 77, 91 and 143.

For each of the relevant primes, the number $s$ in the third Sylow theorem is the product of the other two primes, so $k_p$ must equal 1, one of the two primes or their product. In each case the only one of these four that is congruent to 1 modulo $p$ is 1, so $G$ has unique (and therefore normal)
subgroups of order 7, 11 and 13. Hence the number of elements of prime order is

\[(7 - 1) + (11 - 1) + (13 - 1) = 28.\]

Suppose \(g\) has order 77. (We are not assuming here that there is a subgroup of order 77, which would have to be cyclic by Theorem 37.7. We are examing what would happen if there were an element of order 77.) Then it generates a cyclic subgroup of order 77 which contains the unique subgroups of order 7 and 11. In it the product of generators of the two subgroups generates the subgroup of order 77. The same could be said for any subgroup of order 77, so there is only one such subgroup. Thus the number of elements of order 77 is smaller than 77. The same can be said of elements of orders 91 and 143. It follows that the number of elements of smaller order is less than 1001, so there has to an element of order 1001 and \(G\) is cyclic.

Alternate proof. For each of the three primes \(p\) dividing 1001, there is a unique subgroup \(C_p\) of order \(p\), so it is normal. The order of quotient group is the product of the other two primes, and in each case Theorem 37.7 applies and says that it is abelian. This means that \(C_p\) contains the commutator subgroup \(C(G)\). Hence \(C(G)\) is in the intersection of the three subgroups of prime order, so it is trivial. This means that \(G\) is abelian and hence cyclic.

Cautionary note. Theorem 37.7 does not say that \(G\) has subgroups of order 77, 91 or 143 or that a subgroup of such order has to be normal. We only know these things after the fact, i.e., after we have shown that \(G\) is cyclic.

Only one person got full credit for this problem.

9. (15 points) Let \(G\) be \(C_{30}\) (the cyclic group of order 20) and let \(a\) be a generator (so \(G = \langle a \rangle\)) and let \(e \in G\) be the identity element.

(a) list all elements of \(G\) or order 30.
(b) list all elements of \(G\) or order 10.
(c) list all elements of \(G\) or order 6.
(d) list all elements of \(G\) or order 5.
(e) list all elements of \(G\) or order 4.
(f) list all other elements of \(G\).

Solution: We will use additive notation. The answers are

(a) \(a, 7a, 11a, 13a, 17a, 19a, 23a, \) and \(29a\).
(b) \(3a, 9a, 21a, \) and \(27a\).
(c) \(5a\) and \(25a\).
(d) \(6a, 12a, 18a, \) and \(24a\).
(e) There are no elements of order 4 since 4 does not divide 30.
(f) There are 12 other elements: \(e, 2a, 4a, 8a, 10a, 14a, 15a, 16a, 20a, 22a, 26a, \) and \(28a\). They have orders 1, 2, 3 and 15.
10. (10 points) Let $G$ be a finite group with a subgroup $H$ such that $|G| = 2|H|$.

(a) Prove that if $a \in G$ is not in $H$, then $a^2 \in H$. (Hint: it suffices to show that $a^2 H \neq aH$.)

(b) Prove that if $a$ is not in $H$, then the order $a$ is even. (Hint: Show that $a^n$ is not in $H$ for any odd integer $n$.)

**Solution:**

(a) $G$ has two left $H$-cosets, namely $H$ itself and its compliment $G - H$.

If $aH = a^2 H$, then $H = aH$, but if $a$ is not in $H$, then $aH = G - H$.

Hence $aH \neq a^2 H$, so $a^2 H = H$, which means that $a^2 \in H$.

(b) For an odd integer $n = 2m + 1$, $a^n = a \cdot a^{2m} \in aH$, so $a^n$ is not in $H$.

This means the order of $a$ cannot be odd.

11. (10 points) Let $G$ be a group of order $n$. Show that $x^n = e$ (the identity element) for every $x \in G$.

**Solution:** Each element $g \in G$ generates a cyclic subgroup, and by Lagrange’s theorem its order (which is that of $g$) divides $n$. It follows that $g^n = e$.

12. (15 points) Determine the number of subgroups of order 3 in

(a) $C_{27} \times C_{27}$
(b) $C_9 \times C_9 \times C_9$
(c) $C_3 \times C_3 \times C_3$

**Solution:** Any element of order 3 in $C_{27} \times C_{27}$ or $C_9 \times C_9 \times C_9$ is contained in the subgroups isomorphic to $C_3 \times C_3$ or $C_3 \times C_3 \times C_3$. In these groups (which are called *elementary abelian groups*), every element other than the identity has order 3, and every subgroup of order 3 contains two such elements. Thus $C_3 \times C_3$ and $C_3 \times C_3 \times C_3$ contain respectively 4 and 13 subgroups of order 3.

13. (10 points) Let $G$ be a group of order $pq$ where $p$ and $q$ are distinct prime numbers. (Such a group need not be abelian.) Prove that every proper subgroup of $G$ is cyclic.

**Solution:** The order of a subgroup $H \subset G$ must divide $pq$ by Lagrange’s theorem. This means that if $H$ is a proper subgroup, then its order is $p$, $q$ or 1, so it is cyclic.

14. (10 points) Find all primes $p$ such that $x + 2$ is a factor of $f(x) = x^6 + x^3 + 1$ in $\mathbb{Z}/p[x]$.

**Solution:** $x + 2$ is a factor of $f(x)$ in $\mathbb{Z}/p[x]$ iff $f(-2) \equiv 0$ modulo $p$. We have $f(-2) = -2^6 - 2^3 + 1 = 57 = 3 \cdot 19$ so the primes are 3 and 19.
15. (10 points) Prove that if \( n \) is an odd integer, then \( n^2 \equiv 1 \) modulo 8 and \( n^4 \equiv 1 \) modulo 16.

**Solution:** Let \( n = 2m + 1 \). Then

\[
n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 4m(m + 1) + 1
\]

The number \( m(m + 1) \) is the product of two successive integers, one of which has to be even, so it is even. This means \( 4m(m + 1) \) is divisible by 8, so \( n^2 \equiv 1 \) modulo 8. Thus we can write \( n^2 = 8s + 1 \), so

\[
n^4 = (8s + 1)^2 = 64s^2 + 16s + 1 = 16(4s^2 + s) + 1
\]

so \( n^4 \equiv 1 \) modulo 16.