Instructions. Answer each of the questions on your own paper, and be sure to show your work so that partial credit can be adequately assessed. Credit will not be given for answers (even correct ones) without supporting work. Put your name on each page of your paper.

1. [10 Points] What is the minimum number of students in a class to guarantee that at least 5 of them were born in the same month (regardless of the year of their birth)?

► Solution. From the Pigeonhole principle, if there are at least $4 \cdot 12 + 1 = 49$ students, then some month will have to contain at least $4 + 1 = 5$ birthdays of students. ◄

2. [15 Points]

(a) Find the greatest common divisor $d = (7605, 5733)$ of 7605 and 5733, using the Euclidean Algorithm.
(b) Write $d = (7605, 5733)$ in the form $d = s \cdot 7605 + t \cdot 5733$.
(c) Find the least common multiple $[7605, 5733]$. (The formula $[a, b](a, b) = ab$ may be useful.)

► Solution. (a) Apply the Euclidean Algorithm:

\[
\begin{align*}
7605 &= 5733 + 1872 \\
5733 &= 3 \cdot 1872 + 117 \\
1872 &= 16 \cdot 117
\end{align*}
\]

Hence, $d = (7605, 5733) = 117$.
(b) From Part (a):

\[
\begin{align*}
117 &= 5733 - 3 \cdot 1872 \\
&= 5733 - 3(7605 - 5733) \\
&= 4 \cdot 5733 - 3 \cdot 7605
\end{align*}
\]

Thus $117 = s \cdot 117 + t \cdot 5733$ where $s = -3$ and $t = 4$.
(c) $[7605, 5733] = \frac{7605 \cdot 5733}{117} = 372,645$. ◄

3. [15 Points]

(a) What is the relationship between $a$ and $n$ which guarantees that $a$ has a multiplicative inverse in $\mathbb{Z}_n$? (Just state the condition. It is not necessary to verify it.)
(b) Find the multiplicative inverse of 13 in $\mathbb{Z}_{225}$.

► Solution. (a) $a$ and $n$ should be relatively prime.
(b) Apply the Euclidean algorithm:

\[
\begin{align*}
225 &= 17 \cdot 13 + 4 \\
13 &= 3 \cdot 4 + 1
\end{align*}
\]

Hence $1 = 13 - 3 \cdot 4 = 13 - 3(225 - 17 \cdot 13) = 52 \cdot 13 - 3 \cdot 225$. Therefore, the multiplicative inverse of 13 in $\mathbb{Z}_{225}$ is 52. ◄
4. [15 Points] In the group $S_{10}$, let $\alpha = (1 \ 3 \ 5 \ 7 \ 9)$, $\beta = (1 \ 2 \ 6)$, and $\gamma = (1 \ 2 \ 5 \ 3)$.

(a) If $\sigma = \alpha\beta\gamma$, write $\sigma$ as a product of disjoint cycles, and use this to find its order and its inverse.

(b) Is $\sigma$ even or odd?

(c) Solve the group equation $x\beta = \gamma$ for $x$. Express $x$ as a product of disjoint cycles.

▶ Solution. (a) 

\[
\sigma = \alpha\beta\gamma = (1 \ 3 \ 5 \ 7 \ 9)(1 \ 2 \ 6)(1 \ 2 \ 5 \ 3) = (1 \ 6 \ 3 \ 2 \ 7 \ 9).
\]

Hence the order of $\sigma$ is 6 and $\sigma^{-1} = (1 \ 9 \ 7 \ 2 \ 3 \ 6)$.

(b) $\sigma$ is odd since it is a cycle of even length 6.

(c) $x = \gamma\beta^{-1} = (1 \ 2 \ 5 \ 3)(1 \ 6 \ 2) = (1 \ 6 \ 5 \ 3)$.

▶

5. [15 Points] Let $G$ be a group and let $a$ and $b$ be elements of $G$. Show by induction that $(aba^{-1})^n = ab^n a^{-1}$ for all natural numbers $n \in \mathbb{N}$.

▶ Solution. Let $S = \{n \in \mathbb{N} : (aba^{-1})^n = ab^n a^{-1}\}$. Since $(aba^{-1})^1 = aba^{-1} = ab^1a^{-1}$, it follows that $1 \in S$. Now assume that $k \in S$ and consider $n = k + 1$. Then 

\[
(aba^{-1})^{k+1} = (aba^{-1})^k(aba^{-1}) = (ab^ka^{-1})(aba^{-1}) = ab^ka^{-1}ba^{-1} = ab^{k+1}a^{-1}.
\]

Hence $k + 1 \in S$, and by the induction principle, $S = \mathbb{N}$. That is, the required formula holds for all $n \in \mathbb{N}$.

▶

6. [15 Points]

(a) State Lagrange’s Theorem.

(b) Suppose that a group $G$ has subgroups of order 9 and 12. If $|G| < 150$, what are the possibilities for $|G|$?

▶ Solution. (a) If $G$ is a finite group and $H$ is a subgroup, then $|G| = [G : H]|H|$ where $[G : H]$ is the number of left cosets of $H$ in $G$. In particular, $|H| \| |G|$.

(b) By Lagrange’s Theorem, $9 \| |G|$ and $12 \| |G|$. Hence $[9, 12] \| |G|$. Since $[9, 12] = 36$, the possibilities for $|G|$ with $|G| < 150$ are 36, 72, 108, and 144.

▶
7. [15 Points] The elements of $\mathbb{Z}_{16}$ which have a multiplicative inverse form a group $G$ with the following multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>9</th>
<th>11</th>
<th>13</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>15</td>
<td>5</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>15</td>
<td>9</td>
<td>3</td>
<td>13</td>
<td>7</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>15</td>
<td>13</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>13</td>
<td>3</td>
<td>9</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>5</td>
<td>15</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>13</td>
<td>11</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

(a) Let $H = \{1, 7\}$. Explain why $H$ is a subgroup of $G$.

(b) List all of the left cosets of $H$.

(c) Write the multiplication table for the quotient group $G/H$.

(d) Is $G/H$ a cyclic group? Explain.

**Solution.** (a) $1 \cdot 1 = 1$, $1 \cdot 7 = 7$, $7 \cdot 1 = 7$, and $7 \cdot 7 = 7$. Hence $H$ is closed under all possible multiplications and thus is a subgroup.

(b) $H = 1H = \{1, 7\}$, $3H = \{3, 5\}$, $9H = \{9, 15\}$, $11H = \{11, 13\}$.

(c) $\cdot$

<table>
<thead>
<tr>
<th></th>
<th>$H$</th>
<th>$3H$</th>
<th>$9H$</th>
<th>$11H$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$H$</td>
<td>$3H$</td>
<td>$9H$</td>
<td>$11H$</td>
</tr>
<tr>
<td>$3H$</td>
<td>$3H$</td>
<td>$9H$</td>
<td>$11H$</td>
<td>$H$</td>
</tr>
<tr>
<td>$9H$</td>
<td>$9H$</td>
<td>$11H$</td>
<td>$H$</td>
<td>$3H$</td>
</tr>
<tr>
<td>$11H$</td>
<td>$11H$</td>
<td>$H$</td>
<td>$3H$</td>
<td>$9H$</td>
</tr>
</tbody>
</table>

(d) $G/H$ is cyclic with generator $3H$ since $G/H = \{H, 3H, 9H = (3H)^2, 11H = (3H)^3\}$.

8. [20 Points] Let $C$ be the binary linear code with generator matrix

$$
\begin{bmatrix}
1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 
\end{bmatrix}
$$

and let $\tilde{C}$ be the ternary linear code with the same generator matrix $G$.

(a) List all of the codewords of $C$.

(b) How many codewords does $\tilde{C}$ have? (Do not list them.)

(c) Write parity check matrices $H$ for $C$ and $\tilde{H}$ for $\tilde{C}$.

(d) Is the word $\tilde{x} = 2120102$ a code word for $\tilde{C}$? Explain.
(e) What are the parameters \((n, k, d)\) for the code \(C\)? Be sure to give reasons for your answers.

(f) How many errors can \(C\) detect and how many errors can \(C\) correct?

▶ Solution. (a) 0000000, 0010111, 0101011, 0111100, 1001101, 1011010, 1100110, 1110001

(b) \(|\bar{C}| = 3^3 = 27\)

c) \[ H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \]

\[ \tilde{H} = \begin{bmatrix} 2 & 2 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 1 \end{bmatrix} \]

(d) Since \(\tilde{H}\hat{x} = \hat{0}, \hat{x}\) is a codeword.

(e) The length of words is \(n = 7\); \(k = 3\) = the rank of \(G\); \(d = 4\) since the minimum weight of any codeword listed in Part (a) is 4.

(f) \(C\) can detect 3 errors and correct 1 error.

9. [15 Points] Let \(C\) be the \((4, 2, 3)\) ternary linear code with parity check matrix

\[ H = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix}. \]

That is, \(C\) is the Hamming code \(\text{Ham}(2, 3)\).

(a) List all of the words \(\hat{x} \in (\mathbb{Z}_3)^4\) such that \(d(\hat{x}, \hat{c}) \leq 1\), where \(\hat{c} = 1201\).

(b) Decode each of the following words using syndrome decoding.

i. 2021

ii. 1221

iii. 1011

▶ Solution. (a) It is only necessary to change at most 1 of the digits of \(\hat{c}\). Thus the requested words are: 1201, 0201, 2201, 1001, 1101, 1211, 1221, 1200, 1202; a total of 9 words.

(b) i. \(H \begin{bmatrix} 1 \\ 2 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}\). Thus 2021 is a codeword.

ii. \(H \begin{bmatrix} 2 \\ 0 \\ 2 \\ 1 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 2H\hat{c}_3\). Thus we must subtract 2 from the third digit in order to decode the word. Hence the decoded word is 1201.
iii. \[ H \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 2H \hat{e}_4. \] Thus we must subtract 2 from the last digit in order to decode the word. Hence the decoded word is 1012.

10. [15 Points] A wheel is divided evenly into five different compartments. Each compartment can be painted purple or gold. The back of the wheel is black. How many different such color wheels are there?

► **Solution.** This problem is an application of Burnside's theorem. Let \( X \) be the set of all possible purple and gold colorings of the compartments of the wheel without regard to any symmetries. Then \( |X| = 2^5 \). Let \( G \) be the cyclic group of rotations of the wheel by multiples of 72°. The group \( G \) acts on the set \( X \), and the distinct colorings of the wheel are the orbits of this group action. Because the back of the wheel is black, the only symmetries of the wheel are rotations; reflections are not allowed since they involve turning over the wheel. If the compartments of the wheel are labeled from 1 to 5 in a clockwise direction, then \( G \) is generated by the 5-cycle \( \sigma = (1 \ 2 \ 3 \ 4 \ 5) \). Hence the non-identity elements of \( G \) are:

\[
\begin{align*}
\sigma &= (1 \ 2 \ 3 \ 4 \ 5) \\
\sigma^2 &= (1 \ 3 \ 5 \ 2 \ 4) \\
\sigma^3 &= (1 \ 4 \ 2 \ 5 \ 3) \\
\sigma^4 &= (1 \ 5 \ 4 \ 3 \ 2)
\end{align*}
\]

The following table then lists all the sizes of fixed point sets for \( G \) acting on \( X \).

\[
\begin{array}{c|c}
\mathcal{g} & |X_\mathcal{g}| \\
\hline
\varepsilon & 2^5 \\
\sigma & 2 \\
\sigma^2 & 2 \\
\sigma^3 & 2 \\
\sigma^4 & 2 \\
\end{array}
\]

The number of distinct colorings of the wheel is then the number \( N \) of orbits under of action of \( G \) on \( X \). By Burnside's theorem, this is

\[
N = \frac{1}{|G|} \sum_{\mathcal{g} \in G} |X_\mathcal{g}| = \frac{1}{5} (2^5 + 2 + 2 + 2 + 2) = \frac{40}{5} = 8.
\]