MAT 312 - AMS 351

FINAL EXAM

SUMMER II, 14 August 2014

Question 1.

a. Find all four solutions to the equation $x^2 - 1 \equiv 0 \mod 35$. (5 pts)

b. Solve the equation $[243]_n \cdot [x]_n \equiv [1]_n$ for $n = 1130$. (7 pts)

c. Find the last three digits of the integer $2003^{2002^{2001}}$. (8 pts)

Proof. a. Clearly, $1^2 = (-1)^2 \equiv 1 \mod 35$. Since, $1 \equiv 36 \mod 35$, we see that 6 and $-6$ are also solutions to $x^2 \equiv 1 \mod 35$. Therefore, the solutions are $[1]_{35}, [6]_{35}, [-6]_{35}, [-1]_{35}$, or equivalently, $[1]_{35}, [6]_{35}, [29]_{35}, [34]_{35}$.

b. We need to calculate the multiplicative inverse of 243 modulo 1130. By the Euclidean algorithm,

\[
\begin{align*}
1130 &= 4 \cdot 243 + 158 \\
243 &= 1 \cdot 158 + 85 \\
158 &= 1 \cdot 85 + 73 \\
85 &= 1 \cdot 73 + 12 \\
73 &= 6 \cdot 12 + 1 \\
12 &= 1 \cdot 12.
\end{align*}
\]

(This also confirms that $(1130, 243) = 1$ and the multiplicative inverse of 243 modulo 1130 does exist. Now we find a form $a \cdot 243 + b \cdot 1130 = 1$ for some $a, b \in \mathbb{Z}$. By the
algorithm above,

\[
1 = 73 - 6 \cdot 12 \\
= 73 + 6(73 - 85) \\
= 7 \cdot 73 - 6 \cdot 85 \\
= 7(158 - 85) - 6 \cdot 85 \\
= 7 \cdot 158 - 13 \cdot 85 \\
= 7 \cdot 158 - 13(243 - 158) \\
= 20 \cdot 158 - 13 \cdot 243 \\
= 20(1130 - 4 \cdot 243) - 13 \cdot 243 \\
= 20 \cdot 1130 - 93 \cdot 243.
\]

So, the inverse is \([−93]_{1130}\), or equivalently, \([1037]_{1130}\). Multiplying the both sides of \([243]_n \cdot [x]_n \equiv [1]_n\) by \([1037]_{1130}\) gives \([x]_{1130} = [1037]_{1130}\).

c. We are asked to calculate 

\[2003^{2002^{2001}} \mod 1000.\]

We have \(ϕ(1000) = φ(2^35^3) = 4 \cdot 100 = 400\). So, by Euler’s Theorem, for any \(a \in \mathbb{Z}\) with \((a, 1000) = 1\), we have \(a^{400} \equiv 1 \mod 1000\). Using that we calculate

\[
2003^{2002^{2001}} \equiv 3^{2002^{2001}} \\
\equiv ((3^{400})^{53})^{2001} \\
\equiv (1^{53})^{2001} \\
\equiv 9^{2001} \\
\equiv (9^{400})^59 \equiv 9 \mod 1000.
\]

\(\square\)
Question 2. Consider the permutations

\[ \pi = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
9 & 5 & 10 & 11 & 7 & 1 & 12 & 4 & 3 & 2 & 8 & 6
\end{pmatrix} \]

\[ \sigma = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
1 & 4 & 10 & 8 & 2 & 7 & 9 & 12 & 11 & 3 & 5 & 6
\end{pmatrix} \]

a) Write \( \pi \) and \( \sigma \) as a product of disjoint cycles. (6 pts)

b) Calculate the order, sign of the permutations \( \pi \), \( \sigma \) and \( \pi \sigma \) (show the formula that you use in each case). (14 pts)

Proof. a) \( \pi = (1 \ 9 \ 3 \ 10 \ 2 \ 5 \ 7 \ 12 \ 6 \)(4 \ 11 \ 8) \), \( \sigma = (2 \ 4 \ 8 \ 12 \ 6 \ 7 \ 9 \ 11 \ 5)(3 \ 10) \).

b) \( \pi \sigma = (1 \ 9 \ 8 \ 6 \ 12)(2 \ 11 \ 7 \ 3) \).

\begin{align*}
\text{ord}(\pi) &= \text{lcm}(9, 3) = 9, \\
\text{ord}(\sigma) &= \text{lcm}(9, 2) = 18, \\
\text{ord}(\pi \sigma) &= \text{lcm}(5, 4) = 20, \\
\text{sgn}(\pi) &= (-1)^{9-1}(-1)^{3-1} = 1, \\
\text{sgn}(\sigma) &= (-1)^{9-1}(-1) = -1, \\
\text{sgn}(\pi \sigma) &= (-1)^{5-1}(-1)^{4-1} = -1.
\end{align*}

□
Question 3.

a. Find the smallest subgroup of \( S(5) \) which contains both of the permutations 
\( \pi = (1 4 5) \) and \( \sigma = (1 4) \). (10 pts)

b. What is the order of the subgroup? (4 pts)

c. Determine the number of distinct cosets of the (same) subgroup in \( S(5) \) without listing them. (6 pts)

\textit{Proof.} a. Let us denote the smallest subgroup containing \( \pi \) and \( \sigma \) by \( H \). Since \( H \) is a subgroup, it must contain the identity permutation \( \text{id} \) and the inverse of each member, and it must be closed under the composition. So \( \pi^{-1}, \sigma^{-1}, \text{id} \in H \). Also, all positive powers of \( \pi \) and \( \sigma \) must belong to \( H \). Since, the length of \( \pi \) is 3, we have \( \pi^3 = \text{id} \). Similarly, \( \sigma^2 = \text{id} \). We have

\[
\begin{align*}
\pi^2 &= \pi^{-1} = (1 5 4), \\
\sigma^{-1} &= \sigma = (1 4), \\
\pi \sigma &= (1 5), \\
\sigma \pi &= (4 5).
\end{align*}
\]

Moreover,

\( (\pi \sigma) \pi = \sigma, \pi \sigma \pi^2 = \sigma \pi, \pi^2 \sigma \pi = \pi \sigma, \pi^2 \sigma = \sigma \pi, \sigma \pi^2 = \pi \sigma, \sigma \pi \sigma = \pi^{-1}, \pi \sigma \pi = \sigma \).

So, \( H = \{ \text{id}, (1 4 5), (1 4), (1 5 4), (1 5), (4 5) \} \) and it is closed under composition.

b. The order of a group is equal to the number of its elements. Therefore, the order of \( H \) is 6.

c. The order of \( S(5) \) is equal to \( 5! = 120 \). By Lagrange’s Theorem,

\[
\text{the number of cosets of } H = \frac{\text{ord}(S(5))}{\text{ord}(H)} = \frac{120}{6} = 20.
\]

\( \square \)
**Question 4.** Let \( f : G \to H \) be a group homomorphism. Define the set
\[ K = \{ g \in G \mid f(g) = e_H \} \]
where \( e_H \) is the identity element in \( H \).

a) Prove that \( K \) is subgroup of \( G \). \hfill (10 pts)

b) Prove that \( f \) is injective if and only if \( K = \{e_G\} \). \hfill (10 pts)

**Proof.**

a) Let \( g_1, g_2 \in K \). Then, by the definition of \( K \), \( g_1 \) and \( g_2 \) are mapped to the identity of \( H \) by \( f \).

\[
f(g_1g_2) = f(g_1)f(g_2) = e_H e_H = e_H
\]

So, \( g_1g_2 \in K \). Also, \( f(g_1) = e_H \) implies that \( (f(g_1))^{-1} = e_H \) (here, \( (f(g_1))^{-1} \) is the inverse of \( f(g_1) \) with respect to the group operation over \( H \)). By the properties of group homomorphisms, \( (f(g_1))^{-1} = f(g_1^{-1}) \). Therefore, \( g_1^{-1} \in K \). Hence, \( K \) is a subgroup of \( G \).

Note. We can also show that \( g^{-1} \in K \) for any \( g \in K \) as follows. Since \( g \in K \), we have
\[
e_H = f(e_G) = f(g \cdot g^{-1}) = f(g)f(g^{-1}) = e_H f(g^{-1}) = f(g^{-1}).
\]

Therefore, \( g^{-1} \in K \).

b) Assume that \( K = \{e_G\} \). Let \( g_1, g_2 \in G \) such that \( f(g_1) = f(g_2) \). Then,
\[
f(g_1)(f(g_2))^{-1} = e_H.
\]

Since \( f \) is group homomorphism
\[
f(g_1)(f(g_2))^{-1} = f(g_1)f(g_2^{-1}) = f(g_1g_2^{-1}) = e_H
\]

which implies that \( g_1g_2^{-1} \in K \). Since \( K = \{e_G\} \), we must have \( g_1g_2^{-1} = e_G \), equivalently, \( g_1 = g_2 \). Hence, \( f : G \to H \) is injective.

Now, assume that \( f \) is injective. Let \( k \in K \). Then \( f(k) = e_H \). We also have \( f(e_G) = e_H \) since \( f \) is a group homomorphism. However, by the assumption, \( f \) is injective, and \( f(k) = f(e_G) \) implies that \( k = e_G \). Therefore \( K = \{e_G\} \). \( \square \)
**Question 5.** Calculate the two column decoding table (which is formed by syndromes and coset leaders) for the code generated by the matrix

\[
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}.
\]

A message is encoded using the letter equivalents

\[
000 = \text{M}, \ 010 = \text{B}, \ 001 = \text{T}, \ 100 = \text{A},
\]

\[
110 = \text{S}, \ 101 = \text{H}, \ 011 = \text{E}, \ 111 = \text{C}
\]

and received as

\[
0010000, \ 1101011, \ 0011001, \ 1010110.
\]

Correct and decode the received message. \( (20 \text{ pts}) \)

**Proof.** The parity check matrix is given by

\[
M = \begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

The rows from the 2nd to the 8th are formed by the rows of \( M \) in the two column decoding table. We fill the rows by adding the missing syndromes (which spans the whole \( \mathbb{F}^4 \)). We get
Next, we calculate the coset leaders. Notice that each syndrome can be written as the sum of two or more syndromes. For example, $1010 = 1000 + 0010$. (Note that this is not a unique presentation.) Then we can choose the coset leader corresponding to $1010$ to be the sum of coset leaders corresponding to $1000$ and $0010$. Repeating that for the rest of the syndromes we can fill the table as follows.

```
0000  000000
1011  100000
0111  010000
1001  001000
1000  000100
0100  000010
0010  0000010
0001  0000001
1010
1100
0101
0110
0011
1101
1110
1111
```

```
In order to correct the received message, we calculate the syndromes
\[
\begin{align*}
0010000 \cdot M &= 1001, \\
1101011 \cdot M &= 0111, \\
0011001 \cdot M &= 0000, \\
1010110 \cdot M &= 0100.
\end{align*}
\]

We add the corresponding coset leaders to the words to get
\[
\begin{align*}
0010000 + 0010000 &= 0000000, \\
1101011 + 0100000 &= 1001011, \\
0011001 + 0000000 &= 0011001, \\
1010110 + 0000100 &= 1010010.
\end{align*}
\]

Therefore the original message is 000, 100, 001, 101, which reads “MATH”. □
Question 6.

a. Let $f : \mathbb{B}^4 \rightarrow \mathbb{B}^5$ be a function defined by $f(w) = wM$ where $M$ is the matrix

$$
M = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0
\end{pmatrix}
$$

Show whether $f$ is a code function or not. \hspace{1cm} (5 pts)

b. Let $W = \{000000, 101110, 001010, 110111, 100100, 011001, 111101, 010011\}$ be the set of codewords for some linear code function. Find a generator matrix for the code. Determine the minimum distance, and the number of errors that can be detected and corrected by the code. \hspace{1cm} (8 pts)

c. Let $d(x, y)$ be the distance between two words $x, y \in \mathbb{B}^n$. Prove that for any $x, y, z \in \mathbb{B}^n$,

- $d(x, y) \geq 0$, with equality if and only if $x = y$,
- $d(x, y) = d(y, x)$,
- $d(x, y) \leq d(x, z) + d(z, y)$. \hspace{1cm} (7 pts)

Proof. \hspace{0.5cm} a. It is not a code word since it is not injective. For example, both 0001 and 1100 are mapped to 01110.

b. We can take

$$
M = \begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}.
$$

The minimal distance is 2. So, the code function can detect 1 error but correct none.

c. Note that $d(x, y) = \text{wt}(x + y)$ and it counts the number of digits that differ between $x$ and $y$.

- $d(x, y) \geq 0$, with equality if and only if $x = y$. This is clear since, by definition, the weight cannot be negative, and all the 1s in $x$ can be cancelled only by adding $x$ to $x$.
- $d(x, y) = d(y, x)$. This follows from $\text{wt}(x + y) = \text{wt}(y + x)$.
- $d(x, y) \leq d(x, z) + d(z, y)$. First notice that $\text{wt}(x + y) \leq \text{wt}(x) \text{wt}(y)$ (by adding $x$ to $y$ we cannot produce a word with more 1s). Secondly, $\text{wt}(x) \text{wt}(y) = \text{wt}(x + z) \text{wt}(y + z)$ for any word $z$ (if $x$ and $y$ agree on the $i$th digit then adding another word $z$ to $x$ and $y$ does not change the sum of the new values on the $i$th digit). This completes the proof.