Graphing calculators may be used, but no books or notes may be consulted during this test.
Explain your answers carefully.
Total score = 140.

1. (a) (10 points) Find a positive integer $x$ satisfying $51x \equiv 3 \mod 100$.

(b) (10 points) In an RSA encoding scheme, $x$ is encoded as $x^{35} \mod 323$. These numbers are public. The factorization $323 = 17 \times 19$ is kept secret. If you receive message $x^{35}$, how do you retrieve $x \mod 323$? Explain in detail.

2. (a) (10 points) A prime is an integer greater than 1 that is only divisible by itself and by 1. Prove that there are infinitely many primes.

(b) (10 points) If $a = 2 \cdot 3^2 \cdot 5^3 \cdot 17 \cdot 23$ and $b = 3^3 \cdot 5^2 \cdot 19 \cdot 23$, calculate the greatest common divisor of $a, b$ and their least common multiple.

(c) (10 points) Calculate the greatest common divisor of 19189 and 15221.

3. (a) (10 points) Write the permutation

$$\pi = \left( \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 5 & 7 & 9 & 8 & 2 & 6 & 3 \end{array} \right)$$

as a product of disjoint cycles, and calculate its order.

(b) (10 points) Explain why the permutations

$$\pi_1 = \left( \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{array} \right)$$

and

$$\pi_2 = \left( \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 9 \end{array} \right)$$

1
are conjugate.

(c) (5 points) Find the permutation $\sigma$ such that $\pi_2 = \sigma \pi_1 \sigma^{-1}$.

4. In $S(5)$, the group of permutations of $\{1, 2, 3, 4, 5\}$, let $H$ be the set of permutations preserving $\{1, 2, 3\}$, i.e. if $\pi \in H$ then $\pi(1), \pi(2)$ and $\pi(3)$ all belong to $\{1, 2, 3\}$.

(a) (10 points) Prove that $H$ is a subgroup.

(b) (10 points) How many elements are in $H$?

(c) (5 points) Is $H$ a normal subgroup of $S(5)$? Explain carefully.

5. (a) (10 points)

(a) Show that the group code $f_G : \mathbb{B}^4 \to \mathbb{B}^7$ generated by the matrix

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

is suitable for single-error correction or double-error detection.

(b) (10 points) How does adding a fourth check bit

$$\begin{pmatrix}
1 \\
1 \\
1 \\
0
\end{pmatrix}$$

change the error correction/detection capability of this code? (It is now of the form $g : \mathbb{B}^4 \to \mathbb{B}^8$).

6. (a) (10 points) Show that $\mathbb{Z}_{13}^*$ and $\mathbb{Z}_{21}^*$ have the same cardinality.

(b) (10 points) Show that $\mathbb{Z}_{13}^*$ and $\mathbb{Z}_{21}^*$ are not isomorphic.

END OF EXAMINATION