Homework 4

Sean Eva

March 2022

4. There are no solutions to this polynomial congruence.

2. (a) The solution to this systems is $x = 4$ and $y = 6$

   (b) This systems has no solution.

7. *Proof.* Since we are given that A is involutory, then we know that $A^2 = I$. Given that the $\det(I) \equiv 1 \mod m$ by definition. Given that the product of determinants is the determinant of the product we can conclude that $\det(A) * \det(A) = \det(A)^2 = 1$ which implies that $\det(A) = \pm 1$. □

3. For Pollard Rho we want to generate suitable large numbers to encompass the domain of a known non-trivial factor. Once repetition occurs in a generating polynomial, it is supposed to terminate. If a linear function is used, the probability that there is a good amount of exhaustion around the non-trivial factor is smaller which indicates that using a linear function would be a poor choice.

1. Let us represent the license plate number as k. Therefore, we are going to denote $h(k) = k \mod 101$. If we number the spaces from 0 to 100, this makes up the 101 spaces. Obviously since there are over 101 passes being handed out there are going to be collisions where there are multiple people trying to park in the same spot. In order to fix this we are going to reassign them $h(k)+g(k)$ where $g(k) = k+1 \mod 99$. If there is another collision, we are going to use $h(k) + 2g(k)$ and so on until we are able to put them into a spot. Since $(g(k), 101) = 1$ we will use all spaces eventually.

8. (a) $7 \cdot 0 + 3 \cdot 0 + 9 \cdot 1 + 7 \cdot 8 + 3 \cdot 5 + 9 \cdot 4 + 7 \cdot 0 + 3 \cdot 3 = 125 \equiv 5 \mod 10$

   (b) Let us say that we replace x_i with y_i. The new check digit, we will denote with y_9. Then we know that $x_9 - y_9 \equiv ax_i - ay_i \mod 10$ where a is either 7, 3, or 9. So if the replacement creates no change in the check digit, we have that $x_i \equiv y_i \mod 10$ because $7, 3$, and 9 have inverses mod 10. Therefore, this calculation accounts for all single errors.

   (c) If two digits x_i, x_j are transposed, the difference in the check digits will be $a_i x_i + a_j x_j - a_i x_j - a_j x_i \equiv (a_i - a_k)(x_i - x_j) \mod 10$ where a_i, a_j are 3, 9, or 7. The transposition will go undetected if and only if $(a_i - a_j)(x_i - x_j) \equiv 0 \mod 10$. Because $a_i - a_j$ is even, if either $x_i \equiv x_j \mod 5$ or $a_i = a_j$, then the transposition will go undetected.

17. Since the check digit is chosen based on the value of the other digits in the code, if one of them is changed and the sum does not result in $0 \mod 10$ then we automatically know that there is an problem.

18. There is a chance the UPC system will not detect a transposition error. If the two transposed numbers have the same coefficient (1 or 3 for evens and odds) then the error will not be detected.

26. (a) There are 4 sets of congruences that we need to satisfied. In order to satisfy all of them, we need to fix the last 4 digits of the number. So we only have the first 6 digits so we have 10^6 valid numbers.

(b) Any two errors in the code words can be detected. If these are the errors $x_i \to x_i + a$ and $x_j \to x_j + b$ in the i and j positions respectively. Therefore,

$$\begin{aligned}
\sum_{i=1}^{10} x_i &\equiv a + b \mod 11 \\
\sum_{i=1}^{10} i x_i &\equiv ia + jb \mod 11 \\
\sum_{i=1}^{10} i^2 x_i &\equiv i^2 a + j^2 b \mod 11 \\
\sum_{i=1}^{10} i^3 x_i &\equiv i^3 a + j^3 b \mod 11.
\end{aligned}$$

Therefore, there are 4 congruences and 4 unknowns which can be solved to find the individual values.

(c) The given number is 0204906710. Therefore,

$$\begin{aligned}
a + b &\equiv 7 \mod 11 \\
ia + jb &\equiv 7 \mod 11 \\
i^2 a + j^2 b &\equiv 9 \mod 11 \\
i^3 a + j^3 b &\equiv 2 \mod 11.
\end{aligned}$$

Solving the values we get $a = 9, b = 9, i = 5, j = 8$. Therefore, the correct code is 0204706510.