FINAL TEST REVIEW II

1. Let p be a prime number. Show that $a^{p-1} \equiv 1 \mod p$ for any positive integer a with $\gcd(a,p)=1$.

2. Compute the last two digits of 2015^{2016}, 2016^{2015}.

3. Find a pair of integers $m, n > 2016$ such that $37^m + 23^n$ has the last digit 8.

4. Let p be a prime number. Prove that $[p]^{-1} \equiv p \mod p+1$. Find $[a]^{-1}$ in $\mathbf{Z}_{2018}$ for $a = 2017$.

5. Define the Euler function $\phi(n)$. How many non-zero divisors are there in $\mathbf{Z}_{33}$? in $\mathbf{Z}_{333}$? $\mathbf{Z}_{3333}$, $\mathbf{Z}_{33333}$?

6. Show that $(n-1)^3 + n^3 + (n+1)^3 \equiv 0 \pmod 9$ for all integers $n \geq 2$.

7. Show that $3^n + 2n - 1 \equiv 0 \pmod 4$ for all positive integers n.

8. Find a general solution of the system

$$\begin{cases} x \equiv 11 & \mod 13 \\ x \equiv 13 & \mod 17 \\ x \equiv 17 & \mod 19 \end{cases}$$

9. Find how many zero divisors are there in $\mathbf{Z}_{2016 \cdot 2017}$.

10. Solve the equations

(a) $19x \equiv 17 \mod 2017$

(b) $31x \equiv 40 \mod 2016$

11. Let a, n be positive integers and $\gcd(a,n)=1$. Show that $a^{\phi(n)} \equiv 1 \mod n$, where $\phi(n)$ is the Euler function.

12. Let $p = 61$, $q = 13$, $n = pq$, and you are an RSA-code manager. You have assigned a public key $e = 47$ to the user A. Find a secret key d.

13. Let $n = pq$, where p and q are prime numbers. Assume you know the value $\phi(n)$, where ϕ is the Euler function. Determine p and q from n and $\phi(n)$.

14. The encoding function $\alpha : \mathbf{Z}_2^4 \to \mathbf{Z}_2^7$ is given by the parity check matrix

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

(a) Find a generating matrix G of this code.

(b) Find the minimal distance $\delta(x,y)$ for $x, y \in \mathcal{C} = \alpha(\mathbf{Z}_2^4)$ if $x \neq y$.

(c) Decode the messages 1011111, 0101100.

15. The encoding function $\alpha : \mathbf{Z}_2^3 \to \mathbf{Z}_2^5$ is given by the generating matrix

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

(a) Find a parity-check matrix H of this code.

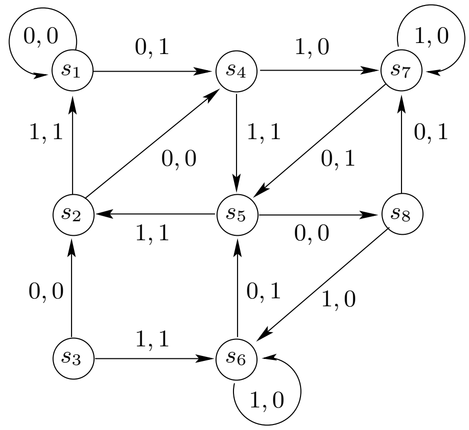
(b) Find the minimal distance $\delta(x,y)$ for $x, y \in \mathcal{C} = \alpha(\mathbf{Z}_2^3)$ if $x \neq y$.

(c) Decode the messages 10110, 00110.

16. Design a finite state machine $M = (S, O, \nu, \omega)$, where $S = O = \{0, 1\}$, which recognized a patern "1001" in a binary string.

17. Design a finite state machine $M = (S, O, \nu, \omega)$, where $S = O = \{0, 1\}$, which recognized a patern "1001" in a binary string only when the zero occurs at the position which is multiple of 2.

18. Consider the finite state machine $M = (S, O, \nu, \omega)$, where $S = O = \{0, 1\}$, given by the diagram:



(i) Write the output of the string 001100110011.

(ii) Write the transitional table for the machine.

(iii) Apply the minimization process to this machine.

19. Carefuly explain what is the Busy Beaver Problem. Prove that there is no Turing Machine which solves the Busy Beaver Problem.