

Show all work for credit. Write responses using complete sentences, as appropriate.

Note: HW will no longer be routinely collected. Instead, we'll have spot quizzes in class.

1. Suppose you create a binary code by appending to each message word  $a_1 a_2 a_3 a_4$  three parity check digits  $c_1 = a_1 + a_2 + a_4$ ,  $c_2 = a_2 + a_3 + a_4$ , and  $c_3 = a_2 + a_3 + a_4$ . Will the resulting code detect and/or correct all single-digit errors?
2. Suppose you create a binary code by appending to each message word  $a_1 a_2 a_3$  two parity check digits  $c_1 = a_1 + a_2$  and  $c_2 = a_2 + a_3$ . Will the resulting code detect and/or correct all single-digit errors?
3. Suppose you create a binary code by appending to each message word  $a_1 a_2 a_3$  three parity check digits  $c_1 = a_1 + a_2$ ,  $c_2 = a_2 + a_3$ , and  $c_3 = a_1 + a_3$ . Will the resulting code detect and/or correct all single-digit errors?
4. Append a fourth check digit to each seven-digit code created by the Venn Diagram method,  $c_4 = a_1 + a_2 + a_3 + a_4$ . With this additional check digit, can double errors be detected and/or corrected?
5. For the message word  $a_1 a_2 a_3 a_4$ , append four check digits:  $c_1 = a_1$ ,  $c_2 = a_2$ ,  $c_3 = a_3$ , and  $c_4 = a_4$ . Will the resulting code detect and/or correct all single-digit errors? Can double errors be detected and/or corrected?
6. Construct a code for five-digit binary message words that has four parity check digits. Can it detect and/or correct single-digit errors?
7. Construct a code for five-digit binary message words that has three parity check digits. Can it detect and/or correct single-digit errors?
8. Create a binary linear code with eight possible code words that can detect and correct any single-digit error.
9. Create a binary linear code with four possible code words that can detect and correct any single-digit or double-digit error.
10. Give an example of a circumstance where the code  $C = \{00000, 11111\}$  could be of use.
11. Use the Caesar cipher to encrypt the message ABANDON HOPE.

12. Use the Caesar cipher to decrypt the message DOO LV ZHOO.
13. How does the weight of a code compare to the number of errors that can be detected?
14. How does the weight of a code compare to the number of errors that can be corrected?
15. Using modular arithmetic, determine  $(42 \cdot 17) \bmod 23$ .
16. Using modular arithmetic, determine  $(16 \cdot 31) \bmod 41$ .
17. Using modular arithmetic, determine  $12^7 \bmod 53$ .
18. Using modular arithmetic, determine  $17^7 \bmod 41$ .
19. Determine the value of  $s$  so that  $9s = 1 \bmod 17$ .
20. Determine the value of  $s$  so that  $11s = 1 \bmod 13$ .
21. For the RSA scheme with  $p = 5$ ,  $q = 11$ , choose a value for  $r$ . Then encode the message sent for the string "23."
22. For the RSA scheme selected above, decode the message "7," if possible.
23. For the RSA scheme with  $p = 17$ ,  $q = 23$ , choose a value for  $r$ . Then encode the message sent for the string "13."