Math 13 – Chapters 16 & 17 – Take-home Problems Solutions

1. If the third digit of the American Express Travelers Check number 390124323 is mistyped as a 9, the check digit won't detect the error since both 3+9+1+2+4+3+2+3=27 and 3+9+9+1+2+4+3+2+3=36 are divisible by 9.

2. Consider the National rental car number 3960040.
   a. The check digit is the 0 at the end – though it's no really needed since 396004 is a multiple of 7.
   b. If the last digit is mistyped as a 7, the error isn't caught since 3940047 is evenly divisible by 7.
   c. An error of the type abc←cba will be detetected if $(100a+c) - (100c+a) = 99(a-c)$ is a multiple of 7 i.e. only if $a-c$ is a multiple of 7, i.e. a and c could be one of the pairs 0&7, 1&8 or 2&9.

3. Consider the UPC code 0-48000-03254-5.
   a. The check digit here is the 5 at the right end. Since 4+3*8+3+3*2+5+3*4+5 = 59 is not divisible by 10, the check digit may or may not be right – in any case there is some error somewhere.
   b. Draw the bar code in which this UPC would be encoded (I used MS Excel).

      Although the correct number would appear like this

   c. If only second digit is read in error then there is a unique value of x for which x+3*8+3+3*2+5+3*4+5 = 55+x is divisible by 10; namely, $x = 5$.

4. The check sum of the bank identification number 250150205 is 7*2+3*5+7*1+3*5+7*2+9*5=110, which is good since it's divisible by 10. If the third and fourth digits of are exchanged, then we have 251050205 and the check sum is 7*2+3*5+9*1+3*5+7*2+9*5=112 so the error is detected.

5. The check sum for the codabar number 4128 0012 4389 0110 is 2(4+2+1+4+8+1)+1+(1+8+2+3+9+1)=65. Thus the last digit should be a 5, not a 0 and this is not a viable Codabar number.

6. Suppose the ISBN number were modified to the alpha-numeric code "ISBN-13" with the characters 0,1,2,3,4,5,6,7,8,9,A,B,C, where A=10, B=11 and C=12. A valid code word would be of the form $a_1 a_2 \cdots a_{12}$ where $\sum_{i=1}^{12}(13-i)a_i$ is divisible by 13.
   a. The check value of the correct number is divisible by 11. If the check value of the erroneous number is not divisible by 11, then the error is detected. Suppose the j^{th} digit is wrong so that the difference between the correct sum (divisible by 13) and the error sum is
   $$\sum_{i=1}^{12}(13-i)a_i - \left((13-j)d_j + \sum_{i \neq j}(13-i)a_i\right) = (13-j)a_j - (13-j)d_j = (13-j)\left(a_j - d_j\right)$$
   Now since $1 \le j \le 12$, $1 \le 13 - j \le 12$. This means that $13-j$ is not divisible by 13. Similarly $0 < \left|a_j - d_j\right| < 13$ and so $a_j - d_j$ is not divisible by 13. Thus the product of these, which is also the difference between the correct check sum and the mistaken check sum, $(13-j)\left(a_j - d_j\right)$, is not

divisible by thirteen and so the mistaken checksum cannot be divisible by 13. Therefore a single digit error can always be corrected.

b. A transposition error can also always be corrected. Such an error is characterized by all digit being the same except $a_i \neq a_{i+1}$ which are swapped. The absolute difference between the check sums is then $0 < \left|(13-j)d_j + (13-j-1)d_{j+1} - \left((13-j)d_{j+1} + (13-j-1)d_j\right)\right| = \left|-d_{j+1} + d_j\right| < 13$
This is because the difference of two different characters in the set {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12} . Thus again, since the correct check sum is divisible by 13 and the difference between that and the error check sum is not divisible by 13, the error correct sum is not divisible by 13.

7. Consider the Zip+4 code 92260-9399.
   a. Since 9+2+2+6+9+3+9+9=49, the postnet code check digit is 1, making the sum divisible by 10.
   b. On an envelope, the bar code would look like this: 9 2 2 6 0 9 3 9 9 1
   c. If a single digit is in error, a computer still determine the correct number using the fact that the check sum must be divisible by 10.

8. To determine whether or not the number 0-413882-5 is a viable UPC Version E number, you'll need to do some research outside the text, since that topic isn't covered in the text. The web site http://www.barcodeisland.com/upce.phtml contains all the relevant information to show that the UPC Version A form of this number would be 0-41200-00388-0 but the final digit would need to be changed from a 5 to a 0.

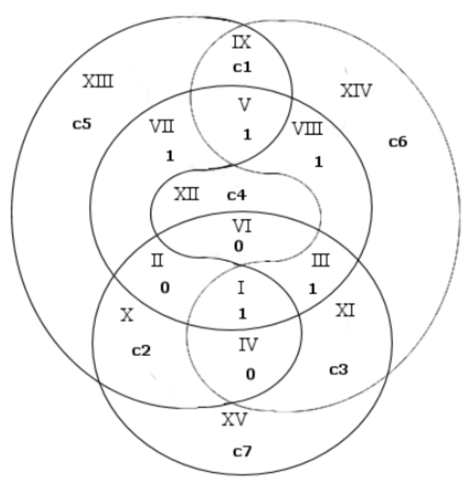
9. Since the codabar check sum 2*(5+1+2+4+5+4+1+8)+3+(2+1+8+6+3+2+3+6) = 94 is not divisible by ten, 5211 2846 5342 1386 is not a valid credit card number.

10. What is the Soundex Coding System version of your last name? (answers may vary) For "Hagopian" it's H215.

11. 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 $c_2 = a_2 + a_3$. The resulting code is {00000, 00101, 01011, 10010, 01110, 10111, 11001, 11100} whose weight is 2. Thus the code can detect 1 error and correct none.

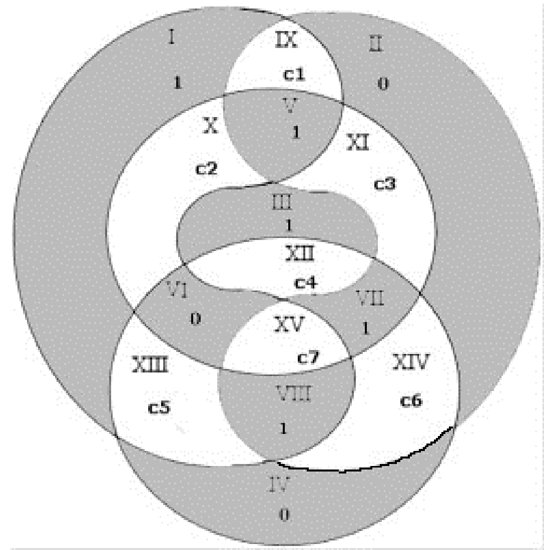
12. By analogy with the diagrams on page 602 of the text, discuss how the Venn diagram can be used to determine a parity check code for a 8-digit binary message. Note that regions A and B are sort of peanut-shaped while regions C and D are circular.

    a. There are 15 different regions in the diagram, as numbered in the diagram at right.



b. If we say a_1 is in region labeled I, a_2 in II, and so on up to a_8 in VIII. For instance with the message 10101011 we determine digits for the other regions so that each set A, B, C and D has total parity = 0 by requiring that
A: $a_1 + a_2 + a_4 + a_5 + a_7 + c_1 + c_3 + c_6 = c_1 + c_3 + c_6 + 3$
B: $a_1 + a_3 + a_4 + a_5 + a_8 + c_1 + c_2 + c_5 = c_1 + c_2 + c_5 + 4$,
C: $c_4 + c_5$ and
D: $c_2 + c_3 + c_7 + 2$ are even. Certainly c4 = 1. But the analogy with the method of page 602 breaks down since the choices for the other check digits are not unique here. For instance, both c1c2c3c4c5c6c7 = 0011111 and 1101111will do.

c. To make this a well-defined binary linear code, number the 8 regions where an odd number (1 or 3) of A, B, C or D overlap I, II, III, IV, V, VI, VII, VIII – as shown at right and consider these the digits $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$, respectively. The remaining regions are then labeled $c_1, c_2, c_3, c_4, c_5, c_6, c_7$. We need another 7 equations in these 7 variables to specify their values in the binary linear code. and are chosen so that the sums of the regions A&B:



$a_1+a_2+a_5+a_6+a_7+a_8+c_1+c_2+c_3+c_5+c_6+c_7$,
A&C:
$a_1+a_3+a_5+a_6+a_7+a_8+c_1+c_2+c_3+c_4+c_5+c_7$
A&D:
$a_1+a_3+a_4+a_5+a_7+a_8+c_1+c_2+c_4+c_5+c_6+c_7$
B&C:
$a_2+a_3+a_5+a_6+a_7+a_8+c_1+c_2+c_3+c_4+c_6+c_7$
B&D
$a_2+a_4+a_5+a_6+a_7+a_8+c_1+c_3+c_4+c_5+c_6+c_7$
C&D
$a_3+a_4+a_5+a_6+a_7+a_8+c_2+c_3+c_4+c_5+c_6+c_7$
and A&B&C&D:
$a_1+a_2+a_3+a_4+a_5+a_6+a_7+a_8+c_1+c_2+c_3+c_4+c_5+c_6+c_7$
are even.

d. What would the weight of this binary linear code be?
SOLN: Let's look at the code words with the fewest number of 1's.
00000001 would require

$$\begin{aligned}
c_1+c_2+c_3+c_5+c_6+c_7 &= 1\text{mod}2\\
c_1+c_2+c_3+c_4+c_5+c_7 &= 1\text{mod}2\\
c_1+c_2+c_4+c_5+c_6+c_7 &= 1\text{mod}2\\
c_1+c_2+c_3+c_4+c_6+c_7 &= 1\text{mod}2\\
c_1+c_3+c_4+c_5+c_6+c_7 &= 1\text{mod}2\\
c_2+c_3+c_4+c_5+c_6+c_7 &= 1\text{mod}2\\
c_1+c_2+c_3+c_4+c_5+c_6+c_7 &= 1\text{mod}2
\end{aligned}$$

Wow…!

e. How many errors can this code correct?
SOLN: Oooooo, I wish I knew!

f. How many errors can it detect?
SOLN: See party above.

13. If we append a fourth check digit to each seven-digit code created by the Venn Diagram method, $c_4 = a_1 + a_2 + a_3 + a_4$. This additional check digit, leads to the code {00000000, 00010111, 00101111, 01001011, 10001101, 11000110, 10100010, 10011010, 01100100, 01011100, 00111000,11101001, 110100001,10110101, 011100011, 111111110}. The weight of the code is $t = 3$ so there is no improvement from the extra check digit: two errors are detected and 1 error is corrected.

14. To create a binary linear code with eight possible code words that can detect and correct any single-digit error you need at least 5 binary digits and every non-zero code word needs to have at least 3 ones: {00000,11100,11010,10110,11110,00111,01011,11011}, for instance.

15. The code C = {00000, 11111} could be of use when needing to broadcast a "yes or no" message in a noisy line. The weight of the code is 5, so it could correct two errors.

16. Using the Caesar cipher to decrypt the message DOO LV ZHOO we get "ALL IS WELL"

17. Using modular arithmetic, 17^7 mod 41 = $\left(17^2\right)^3 17 \bmod 41 = 2^3 17 \bmod 41 = 13$

18. For the RSA scheme with p = 5, q = 11, m = LCM(4,10) = 20. r = 3 means 23 is encoded as 23^3mod55 = (55*221+12)mod55 = 12.

19. For the RSA scheme with p = 17, q = 23, m = LCM(16,22) = 176 so r = 3 will do. To encode 13, compute 13^3mod391 = (5*391+242)mod391 = 242

20. Using the Vigenere cipher with the keyword RELATIONS we decipher
```
KSMEHZBBL KSMEMPOGA JXSEJCSFL ZSY
RELATIONS RELATIONS RELATIONS REL
TOBEORNOT TOBETHATI STHEQUEST ION
```