math 22

Solutions to Sample Midterm Questions

1. Explain why, with 2 weighings on a pan balance, you cannot find a counterfeit among 10 coins, assuming that the counterfeit is slightly heavier than all the rest. Only the coins themselves are available for weighing

   SOLUTION: The best you can do is divide the coins into 3 groups — one for each pan, and one to be set aside. When you divide 10 coins into three piles, at least one pile has 4 or more coins. The first weighing may only confirm that the counterfeit is among those 4 coins. On the next weighing, when these 4 are divided into 3 groups, there will be a group with at least 2 coins, and the weighing may only determine that the counterfeit coin is one of those 2 coins.

2. Dr. Ecco concluded that the aliens from whom the message was received also had an "alphabet" consisting of 37 distinct characters. Another moment's thought convinced him that the code was a linear code with encoding function $C(x) \equiv 5x \pmod{37}$. Your mission, should you decide to accept it, is to help Dr. Ecco find the decoding function $D(x)$, that is, find an integer a such that

$$D(x) \equiv ax \pmod{37}.$$

   SOLUTION: Since $15 \cdot 5 \equiv 75 \equiv 1 \pmod{37}$, then 15 is the inverse of 5 mod 37, and therefore the decoding function is

$$D(x) \equiv 15x \pmod{37},$$

   that is, $a = 15$.

3. The telephone numbers in town run from 000000 to 999999. The automated switchboard may transpose two digits which have exactly **three** other digits between them, but makes no other kinds of errors. How should a seventh digit be added to each telephone number so that no wrong numbers will be reached because of a switching error?

   SOLUTION: One of many possible solutions is to choose the seventh digit g of $abcdefg$ so that

$$a + b + g \equiv 0 \pmod{10}.$$

   The numbers that could be switched are a and e, or b and f, or c and g. Suppose a and e are switched. Then the switch will not be detected only if the congruence is satisfied in both cases, which would mean that $a + b + g \equiv e + b + g \pmod{10}$. This implies that $a \equiv e \pmod{10}$, and since a and e are between 0 and 9, this implies that $a = e$. But then there is no error. The same reasoning applies for the other possible switches.

4. The following message is received using the 15-digit Hamming Code. Correct the number if it is not correct.

a	a	a	a		a	a	a				a			
b	b	b		b	b			b	b			b		
c	c		c	c		c		c		c			c	
d		d	d	d			d		d	d				d
1	1	1	1	0	0	0	0	0	0	0	1	1	1	1

SOLUTION: Only the parity check bit in the column labeled by a is incorrect, and therefore an error occurred in the column labeled by the subset $\{a\}$. The corrected codeword is

1 1 1 1 0 0 0 0 0 0 0 | 0 1 1 1

5. There are three curtains — labeled A, B, and C. Behind one of them is a brand new BMW, behind each of the others is a goat. Eleven people know what is behind each curtain. You may ask each person one question, which has to have a yes or no answer. Unfortunately, three of them may lie. Devise a set of questions to ask them, and explain clearly why you will be able to tell from the answers where the BMW is.

SOLUTION: Since up to three of the people may lie, we need code words such that the Hamming distance between any two of them is at least 7. For example, the code words could be

		A				B				C		
a	=	1	1	1	1	0	0	0	0	0	0	0
b	=	0	0	0	0	1	1	1	1	0	0	0
c	=	0	0	0	0	0	0	0	0	1	1	1

Thus, the first 4 questions you ask are: "Is the BMW behind curtain A?"

The next 4 questions you ask are: "Is the BMW behind curtain B?"

You then ask the remaining 3 questions: "Is the BMW behind curtain C?"

6. Consider the following list of binary numbers (it goes on forever):

1
1 0 1
1 0 0 1
1 0 0 0 1
1 0 0 0 0 1
1 0 0 0 0 0 1
1 0 0 0 0 0 0 1
1 0 0 0 0 0 0 0 1
1 0 0 0 0 0 0 0 0 1
1 0 0 0 0 0 0 0 0 0 1
1 0 0 0 0 0 0 0 0 0 0 1
. . . .

Which of these integers is divisible by 5? Justify your answer.

SOLUTION: Note that except for the first row, the binary numbers in the list represent the integers

$$2^n + 1$$

for $n = 2, 3, \ldots$, we will show that $5 \,\big|\, 2^n + 1$ if and only if $n \equiv 2 \pmod 4$.

• If $n \equiv 0 \pmod 4$, then $n = 4k$ for some positive integer k, so that

$$2^n + 1 = 2^{4k} + 1 = \left(2^4\right)^k + 1 = 16^k + 1,$$

and since $16 \equiv 1 \pmod 5$, then $2^n + 1 \equiv 2 \pmod 5$.

• If $n \equiv 1 \pmod 4$, then $n = 4k + 1$ for some positive integer k, so that

$$2^n + 1 = 2^{4k+1} + 1 = 2 \cdot \left(2^4\right)^k + 1 = 2 \cdot 16^k + 1,$$

and since $16 \equiv 1 \pmod 5$, then $2^n + 1 \equiv 3 \pmod 5$.

• If $n \equiv 2 \pmod 4$, then $n = 4k + 2$ for some positive integer k, so that

$$2^n + 1 = 2^{4k+2} + 1 = 4 \cdot \left(2^4\right)^k + 1 = 4 \cdot 16^k + 1,$$

and since $16 \equiv 1 \pmod 5$, then $2^n + 1 \equiv 0 \pmod 5$.

• If $n \equiv 3 \pmod 4$, then $n = 4k + 3$ for some positive integer k, so that

$$2^n + 1 = 2^{4k+3} + 1 = 8 \cdot \left(2^4\right)^k + 1 = 8 \cdot 16^k + 1,$$

and since $16 \equiv 1 \pmod 5$, then $2^n + 1 \equiv 4 \pmod 5$.

Since every positive integer n is congruent to exactly one of 0, 1, 2, 3 modulo 4, then the only case when $2^n + 1$ is divisible by 5 is when $n \equiv 2 \pmod 4$.