Problem Set 4

Problem 1
Make a list of all 2-bit patterns (straight-line, not circular). Group them into distinct circular sets. How many sets S are there (not counting 00 and 11)? Does S satisfy $S = (2^n - 2)/n$, where $n = 2$?

Problem 2
Let $n = 6$, which is not prime ($6 = 2 \times 3$). Make a list of all 6-bit patterns (straight-line, not circular). Group them into distinct circular sets. How many sets S are there (not counting 000000 and 111111)? The tendency is to not notice that some set is actually rotations of another set you've already counted, so I'll tell you that you should end up with $S = 12$. Note that it is not true that $S = (2^n - 2)/n$, because $n = 6$ is not prime.

How many sets are 6 long? Call this number of sets S_6. How long are the shorter sets? Do you see any similarity of the shorter sets to your answer for Problem 1 and to the case for $n = 3$ in the lecture? Call the number of sets in those cases S_2 and S_3. Can you find an expression for S_6 in terms of S_2 and S_3 and $n = 6$?

In general, if you have a non-prime number $n = p \times q$, where p and q are prime, give an expression for the number S of distinct circular sets in terms of p and q.

Problem 3
We found in Lecture 1 that $(a^{p-1} - 1)/p$ is an integer if p is prime. For example, for $a = 10$ and $p = 3$, $(10^{3-1} - 1)/3 = 99/3 = 33$ (an integer). But for $a = 10$ and $p = 5$, $(10^{5-1} - 1)/5 = 9999/5 = 1999.8$ (not an integer). The reason is that 5 is a factor of 10, which is not allowed in Fermat's Little Theorem.

We can say that the Circular Code Theorem is that $(a^p - a)/p$ is an integer. Since this result didn't depend on p not being a factor of a, show that $(a^p - a)/p$ is an integer for $a = 10$ and $p = 5$. Try some other values of a and prime p where p is a factor of a.

Problem 4
In the lecture we derived Fermat's Little Theorem from the Circular Code Theorem. Can you derive the Circular Code Theorem from Fermat's Little Theorem? If so, then the two theorems are equivalent —just different forms of the same thing.

Problem 5
The Circular Code Theorem says that if you divide $(a^p - a)$ by p, the remainder is 0. What is the remainder if you divide a^p by p ? Try it for $a = 2$ and $p = 7$. Try it for $a = 3$ and $p = 5$. Can you state the general result as a modulo equation (see Lecture 1)?

Problem 6
Make a list of all 2-trit trinary numbers. There should be nine of them. (A "trit" is like a bit, but in the trinary number system that has only 0, 1, and 2.) Organize these into sets that are alike under rotation. Show that $S = (3^2 - 3)/2 = 3$.