Solutions to non-text problems in Assignment #8

N-1: (a) We get the subspace $\{0, \alpha, \alpha^2, \alpha^4\}$.

(b) The complete collection of 2-dimensional subspaces is

$$\begin{array}{ccccc}
\{ & 0 & 1 & \alpha & \alpha^3 & \} \\
\{ & 0 & \alpha & \alpha^2 & \alpha^4 & \} \\
\{ & 0 & \alpha^2 & \alpha^3 & \alpha^5 & \} \\
\{ & 0 & \alpha^3 & \alpha^4 & \alpha^6 & \} \\
\{ & 0 & \alpha^4 & \alpha^5 & 1 & \} \\
\{ & 0 & \alpha^5 & \alpha^6 & \alpha & \} \\
\{ & 0 & \alpha^6 & 1 & \alpha^2 & \}
\end{array}$$

(c) We get blocks

013
124
235
346
450
561
602

Now you can see that to remember the design, all you have to remember is the first block $0, 1, 3$; the others are obtained by successively adding 1 (mod 7).

(d) Yes, adding 1 gives a symmetry, since as you can see, blocks go to to blocks.

N-2: As a warmup, try this handshake problem: If ten people shake hands with each other, once for each pair, how many handshakes are there? It's not 10 times 9, since that would "overcount" by counting each handshake both ways around. So allow for that by dividing by 2: $\frac{10 \cdot 9}{2} = 45$.

In this problem, we have $p^3 - 1$ nonzero vectors. However, each 1-dimensional subspace consists of the p scalar multiples of a vector, which means $p - 1$ nonzero vectors. So in counting nonzero vectors we are overcounting 1-dimensional subspaces $p - 1$ times; the answer is therefore $\frac{p^3 - 1}{p - 1}$, which equals $p^2 + p + 1$.

There is a point here that should not be overlooked: It is important that two different 1-dimensional subspaces overlap only at **0**, so that each 1-dimensional subspace does correspond to one bunch of $p-1$ nonzero vectors. But this is the case because a one-dimensional subspace is the span of any one of the nonzero vectors it contains.

N-3: (a) One way to say it: Let $\ell = \frac{kn}{m}$ and write the prime factorization $\ell m = kn = p_1^{e_1} \dots p_r^{e_r}$. Since each prime in m is not a prime factor of n, it must be a prime factor of k. Therefore m divides k.

(b) Because if $k = p_1^{e_1} \dots p_r^{e_r}$ then these prime powers include the prime factors of m and also the prime factors of n and these two sets of prime factors do not overlap.

(c) As suggested, suppose $(ab)^k = 1$, which gives $a^k = b^{-k}$, and take the n-th power of both sides to get $a^{nk} = (b^{-k})^n = b^{-nk} = (b^n)^{-k} = 1^{-k} = 1$. Since every m-th power of a is 1, we have $m|nk$. By part (a) that gives $m|k$. Similarly, taking the m-th power instead of the n-th power gives $b^{mk} = \dots = 1$, so $n|mk$ and then $n|k$. Since m and n both divide k, $mn|k$. This says that the powers of ab that equal 1 are the multiples of mn, so ab has order mn.

N-4: (a) Since any two rows agree in 8 places and disagree in 8 places, it takes eight bit changes to turn one row into another row. Therefore an error of up to seven bits can be detected.

(b) We would decode a string of 16 bits by using the row that matches it best. Since any two rows are 8 bit-changes apart, we can correct up to three bit errors. (With 4 bit errors there is the possibility of being halfway between two rows so we couldn't tell which row is right.)

(c) This is 17 bits, but even so we can see that it is closest to row #6 (counting from #0) since it takes only deleting the first received bit and changing one other received bit to make the received bits into row #6. So the decoding is `0110` (which is 6 in binary).

N-5: See the solution to **M-7**.