Math 117 **S04 SOLNS7.**

Solutions to non-text problems from Assignment #7

M-1: The Amazon public modulus has about 1024 bits so the number of decimal digits is about $\log_{10}(2^{1024}) = 1024 \log_{10}(2) = 1024 \cdot .30103 \approx 308.25$, which should be about 309 decimal digits. And that's how many the modulus has. (Notice that the decimal integer with base-10 log equal to 2 is 100, which is the first integer with 3 decimal digits, etc., so 10^{39} would be the first integer with 40 decimal digits and $10^{39} - 1$ would be the last integer with 39 decimal digits.)

M-2: I found the following decodings. (Where it's someone's name I'll write some dots.) `TEST`, `RATS`, `CH..`, `OK`, `COOK`, `MATH`, `CAT`, `FOOD`, `DELL`, `MATG` (math?), `UCLA`, `TIME`, `GOD`, `LOVE`, `MYSH` (myth?), `RAMS`, `A...`, `GOOD`, `FLIP`, `ROW`, `TEA`, `HI THIS IS D...` (using separate encodings with several letters each).

There were two styles: (1) encoding three or four letters into one large integer and encrypting it (which is what I intended) or (2) encoding individual letters into separate small integers and then encrypting into separate large integers. While (2) does illustrate the encryption method, it's not secure, because anyone could try encrypting all 26 letters in advance and then would be able to decrypt any message of single letters.

For a few people, I didn't get anything meaningful in decrypting.

M-3: $\phi(n) = \phi(p_1 p_2) = \phi(p_1)\phi(p_2) = (p_1 - 1)(p_2 - 1) = 2^2 q_1 q_2$, where $p_i = 2q_i + 1$, since q_1, q_2 are prime.

(It's considered bad if $\phi(n)$ factors into lots of smallish primes, so this is one way of making sure it doesn't. The problem should have made that comment about $\phi(n)$ rather than n.)

M-4: $r = \texttt{00010001}$ means $r = \alpha^4 + 1$ and $s = \texttt{00010010}$ means $s = \alpha^4 + \alpha$. Since the field is of characteristic 2, any element plus itself is 0. So $r + s = \alpha + 1 = \texttt{00000011}$ and $rs = \alpha^8 + \alpha^5 + \alpha^4 + \alpha =$
$(\alpha^4 + \alpha^3 + \alpha + 1) + \alpha^5 + \alpha^4 + \alpha = \alpha^5 + \alpha^3 + 1 = \texttt{00101001}$.

M-5: Step 1(a): Following the suggestion: $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$, so $\alpha^7 = \alpha^3 + \alpha^2 + 1 + \alpha^{-1}$ and $\alpha^{-1} = \alpha^7 + \alpha^3 + \alpha^2 + 1 = \texttt{10001101}$.

Step 1(b): in the column vector on p. L 3, a_i is the coefficient of α^i, so the matrix multiplication is

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix}1\\0\\1\\1\\0\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\\1\\0\\0\\0\end{bmatrix} = \mathsf{00010100}.$$

Step 2(c): $\mathsf{00010100} + \mathsf{11000110} = \mathsf{11010010}$, which becomes the output of the round.

M-6: In $\mathbb{F}_{2^8}$, there are $2^8 - 1 = 255$ nonzero elements. Then $a^{255} = 1$ for any nonzero element a, and the order of a must divide 255, which is $3 \cdot 5 \cdot 17$. The possible orders are therefore $1, 3, 5, 15, 17, 51, 85, 255$.

(This is all the problem asked for. However, we know that there is actually a generator g, which means an element of order 255. If d is any of the divisors of 255 then $g^{255/d}$ will have order d, so all the possible orders *do* occur.)

M-7: (a) $n = pq$ gives $\phi(n) = \phi(pq) = \phi(p)\phi(q)$ (since p, q are coprime) $= (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$, so $p + q = n - \phi(n) + 1$. Therefore we know both pq $(= n)$ and $p + q$.

(b) $(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1 r_2 = x^2 - Sx + P$. This should sound familiar; it says that when you have a quadratic polynomial with leading coefficient 1 (a "monic" quadratic), the sum of the roots is minus the coefficient of x and the constant coefficent is the product of the roots. By the quadratic formula, the roots are

$$\frac{S \pm \sqrt{S^2 - 4P}}{2}.$$

Since we are told $r_1 < r_2$ we can say $r_1 = \frac{1}{2}(S - \sqrt{S^2 - 4P})$ and $r_2 = \frac{1}{2}(S + \sqrt{S^2 - 4P})$. For example, if two numbers have sum 5 and product 6, the square root is $\sqrt{5^2 - 4 \cdot 6} = 1$ and the numbers are $(5-1)/2 = 2$ and $(5+1)/2 = 3$.

(c) Using (b) with $p + q = n - \phi(n) + 1 = 2451 - 2352 + 1 = 100$ and $pq = n = 2451$, the square root is $\sqrt{10000 - 9804} = \sqrt{196} = 14$ and p and q are $\frac{1}{2}(100 \pm 14) = 43, 57$. However, as one of you pointed out, 57 is not prime and in fact $n = 2451 = 3 \cdot 19 \cdot 43$, which leads to $\phi(n)$ not having the value given, so the problem is incorrect.

A corrected problem is $n = 3551, \phi(n) = 3432$, for which $p + q = 3551 - 3432 + 1 = 120$ and the square root is $\sqrt{14400 - 14204} = \sqrt{196} = 14$ and p and q are $\frac{1}{2}(120 \pm 14) = 53, 67$.

M-8: (a) The 1-dimensional subspaces of $(\mathbb{F}_2)^3$ are $\{\mathbf{0}, \mathbf{v}\}$, where $\mathbf{0}$ means $(0,0,0)$ and $\mathbf{v}$ is any of $(0,0,1)$, $(0,1,0)$, $(0,1,1)$, $(1,0,0)$, $(1,0,1)$, $(1,1,0)$, and $(1,1,1)$ (seven in all).

(b) The 2-dimensional subspaces of $(\mathbb{F}_2)^3$ are

$$\begin{gathered}
\{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\} \\
\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\} \\
\{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\} \\
\{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\} \\
\{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\} \\
\{(0,0,0),(0,1,1),(1,0,0),(1,1,1)\} \\
\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}
\end{gathered}$$

(c) For convenience, number the plants as 1, … ,7, think of each triple as binary, and have the 1-dimensional subspace $\{0,3\}$ correspond to plant 3, etc. Then the 2-dimensional subspaces listed in (b) give blocks

1	2	3
1	4	5
1	6	7
2	4	6
2	5	7
3	4	7
3	5	6

As you can see, these blocks have the required properties: Any two blocks intersect in one plant and any two plants are in exactly one block.