MATHEMATICS PROBLEM 138

Describe and give an equation for the locus of all those points (x, y, z) given by the parametric equations

$$x = 3u + v + 4,$$
$$y = u + 5v + 9,$$
$$z = 2u + 6v + 5,$$

as the parameters u and v assume all real values.

Each midshipman submitting a correct solution with a correct explanation to Problem 138 by 1700 Friday 2 April 2004 will be recognized as a solver on the next problem. Submit solutions to Prof. Wardlaw at mathprob@usna.edu (please no attachments!) or via his mailbox in Chauvenet 301.

Midshipmen Jordan Kehrer and Stephen McMath each submitted a correct solution to all parts of Mathematics Problem 137. In addition, Midshipmen John Appelbaum, Matthew Butlin, and Spencer Weber submitted solutions to part c. All submitted solutions to part c were done on the computer. A solution is on the back of this page and posted on the right wall at the Bancroft entrance to Chauvenet Hall.

Remark: The first paragraph of Mathematics Problem 137 is quoted from Lockhart & Wardlaw, Chain addition cycles, *Linear Algebra and Its Applications*, 362 (2003) 1-10.

MATHEMATICS PROBLEM 137

Chain addition is a technique employed in cryptography for extending a short sequence of digits, called the *seed* to a longer sequence of pseudorandom digits. Quoting David Kahn (in *Kahn on Codes,* MacMillan, New York, 1983, p. 154), "the first two digits of the [seed] are added together modulo 10 [which means they are added and the carry is neglected] and the result placed at the end of the [sequence], then the second and third digits are added and the sum placed at the end, and so forth, using also the newly generated digits when the [seed] is exhausted, until the desired length is obtained". Thus, the seed 3964 yields the sequence 3964250675632195... .

a. Show that this sequence eventually repeats itself.
b. Show that the sequence begins repeating itself with "3964".
c. EXTRA CREDIT: How many digits are there before the first repetition of "3964"?

Solution. a. Since there are only 10000 four digit numbers, at least one repetition of a four digit block must occur by digit 10004 of the sequence. The sequence following the repeated block is clearly identical to the sequence following the first occurrence of the block, so the segment of the sequence beginning with the first block up to but not including the second block repeats itself forever.

b. Each four digit block abcd after the first has a uniquely determined digit, namely $p = d - a \pmod{10}$, preceding it.. Going backwards from the first repeated block must bring us back to its first occurrence. That block has to be 3964, since otherwise we could back up one digit to a block that was repeated before "the first repeated block".

c. Let A be the 4 x 4 matrix with 3 1s down the super-diagonal and a 1 in the lower left corner. Then $A^4 = A + I$. Note that if we write the 4 digit block abcd as the column vector $\mathbf{v} = \mathrm{col}(a, b, c, d)$ and do our arithmetic modulo 10, then $A\mathbf{v} = \mathrm{col}(b, c, d, a+b)$ gives us the next 4 digit block. Thus, taking $\mathbf{v}_0 = \mathrm{col}(3, 9, 6, 4)$ as the zeroeth block, we see that the kth block is $\mathbf{v}_k = A^k\mathbf{v}_0$. The first block is repeated exactly when $A^k = I$ is the identity matrix mod 10. But this happens if and only if $A^k = I \pmod 2$ and $A^k = I \pmod 5$. Since $(a + b)^2 = a^2 + b^2 \pmod 2$, $A^4 = A + I$ gives us $A^{16} = A^4 + I = A + I + I = A \pmod 2$. Multiplying by the inverse of A gives $A^{15} = I \pmod 2$. Similarly, the identity $(a + b)^5 = a^5 + b^5 \pmod 5$ and $A^4 = A + I$ gives $A^{20} = A^5 + I = (A + I)A + I = A^2 + A + I \pmod 5$, so $A^{20} = A^2 + A + I \pmod 5$. Multiplying this by A^2 and simplifying gives $A^{22} = A^3 + A^2 + A + I \pmod 5$. Similarly, $A^{25} = 2A^3 + 2A^2 + 2A + I \pmod 5$, so $A^{100} = (A^5 + I)^5 = A^{25} + I = 2A^3 + 2A^2 + 2A + 2I = 2A^{22} \pmod 5$ and $A^{78} = 2I \pmod 5$. Taking the 4th power gives $A^{312} = I \pmod 5$. Now $312 = 2x2x2x3x13$. Checking that $A^n \neq I \pmod 5$ for $n = 312/2$, $312/3$ and $312/13$ guarantees that $312 = \mathrm{ord}_5(A)$ is the smallest power of A which is the identity modulo 5. Similarly $\mathrm{ord}_2(A) = 15$, and so $\mathrm{ord}_{10}(A) = 1560$ is the least common multiple of these two. Now we know that the first block 3964 is repeated after 1560 digits, but could it be repeated earlier? Let $V = [\mathbf{v}_0\ \mathbf{v}_1\ \mathbf{v}_2\ \mathbf{v}_3]$ be the 4x4 matrix formed by the first 4 blocks. Row reduction shows V is invertible modulo 10. Hence $A^k\mathbf{v}_0 = \mathbf{v}_0$ implies that $A^kV = V$. Multiplying by the inverse of V shows that $A^k = I$. It follows that the first repetition occurs when $k = \mathrm{ord}_{10}(A) = 1560$. This completes the solution!