

## MATHEMATICS PROBLEM 160

This problem continues the ideas of Mathematics Problem 158. To check whether a positive integer is divisible by 13, add four times the last digit to the number left after removing the last digit of the original number. The original number is divisible by 13 if and only if the resulting number is divisible by 13. That is,  $n = 10t + u$  is divisible by 13 if and only if  $t + 4u$  is. For example, 3094 is divisible by 13 because  $309 + 4 \times 4 = 325$  is, and 325 is divisible by 13 since  $32 + 4 \times 5 = 52$  is. 1776 is not divisible by 13 since  $177 + 4 \times 6 = 201$  is not divisible by 13 since  $20 + 4 \times 1 = 24$  is not.

Explain (with a proof) why this method works. Then produce similar rules for divisibility by 17 and by 19, and explain why they work.

Each person submitting a correct solution with a correct explanation to Mathematics Problem 160 by noon Friday 1 December 2006 will be recognized as a solver on the next problem (which should come out in early January 2007). Submit solutions to Prof. Wardlaw at [wpw@usna.edu](mailto:wpw@usna.edu).

Correct solutions to Mathematics Problem 159 were submitted by Professors Russell Jackson, Amy Ksir, Caroline Melles and Mark Meyerson. My solution to Mathematics Problem 159 is on the back of this page and on the Mathematics Department bulletin board on the third floor of Chauvenet Hall across from the Mathematics Department Office.

## MATHEMATICS PROBLEM 159

Let  $A$  be the  $3 \times 3$  matrix over the integers modulo 3 with first row  $A_1 = [0 \ 1 \ 0]$ , second row  $A_2 = [0 \ 0 \ 1]$ , and third row  $A_3 = [2 \ 1 \ 0]$ .

a. Show that  $A$  has multiplicative order 26. That is,  $A^{26} = I$  is the identity matrix, but  $A^k$  is not  $I$  for any positive integer  $k < 26$ . (All calculations are done modulo 3.)

b. Show that the sum of any two powers of  $A$  is either a power of  $A$  or the zero matrix. (Again, all calculations are done modulo 3.)

**Solutions:** a. The most straightforward solution is to take thirty minutes to multiply  $A$  by itself 25 times to get  $A^k$  for  $k = 1, 2, \dots, 26$  with  $A^{26}$  being the only power equal to the  $3 \times 3$  identity matrix  $I$ .

b. Then show that  $I + A^k$  is another power  $A^s$  or is the zero matrix for each of the matrices  $A^k$  found for part a. (Actually,  $I + A^{13} = 0$ . Remember, all arithmetic is done modulo 3.) This shows that  $A^j + A^{(j+k)} = A^j(I + A^k) = (A^j)(A^s) = A^{(j+s)}$  or is the zero matrix for any two powers  $j$  and  $j+k$  of  $A$ .

A less computational but more sophisticated method is as follows:

a. The characteristic polynomial of  $A$  is  $p(x) = \det(xI - A) = x^3 + 2x + 1$ , so  $A$  is a zero of this polynomial over the three element field  $GF(3)$ . Thus  $A^3 + 2A + I = 0$ . (This can also be seen by direct calculation.) Solving for  $A^3$  gives (Remember we are working modulo 3, so  $2 = -1$ ):

$$\begin{aligned} A^3 &= A - I; \\ A^4 &= A^2 - A, \\ A^{12} &= (A^2 - A)^3 = A^6 - A^3 \\ &= A^3(A^3 - I) = (A - I)(A - I - I) \\ &= (A - I)(A + I) = A^2 - I, \\ A^{13} &= A^3 - A = (A - I) - A = -I, \\ &\text{so } A^{26} = (-I)^2 = I. \end{aligned}$$

If  $A^k = I$  for  $k < 26$ ,  $k$  would have to divide 26; i.e.,  $k = 1, 2$ , or  $13$ . But  $A^1 = A$  is not  $I$ ,  $A^{13} = -I$  is not  $I$ , and  $A^2 = I$  implies  $A^3 = A$  contradicting  $A^3 = A - I$ . Hence  $A$  has multiplicative order 26.

b. Since  $p(x) = x^3 + 2x + 1$  has no zero in  $GF(3) = \{0, 1, 2\}$ , it is irreducible over  $GF(3)$ . Therefore  $p(A) = 0$  implies that  $A$  is a generator of the 27 element field  $GF(27)$ . Since the 26 powers of  $A$  are distinct, it follows that  $GF(27) = \{0, A, A^2, A^3, \dots, A^{26}\}$ . Hence the sum of any two elements of  $GF(27)$  is again in  $GF(27)$ , so the sum of any two powers of  $A$  is either a power of  $A$  or 0.