Multiplication in modular arithmetic

Overview. You'll create some modular multiplication tables and explore the modular analogue to division.

Things to do.

1. Fill in this mod-6 multiplication table. You can probably do all the addition in your head.

$\times$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

2. Pick an integer m somewhere between 10 and 25 and use Excel to make a mod-m multiplication table. Refer to the activity on modular addition for instructions.

3. Make a list of the rows in your table that contain all the numbers 0 through $m-1$, and a list of the rows in which some numbers are missing. What do you notice about the rows where some numbers are missing?

4. Make a list of the rows in your table in which the number 1 appears. How does this compare with your lists from step 3?

5. A *multiplicative inverse modulo* m for a number x is an integer y such that $xy \bmod m = 1$. Make a table of multiplicative inverses modulo m for the numbers 0 through $m-1$.

6. Note that only some numbers have multiplicative inverses modulo m. Can you find a simple rule that predicts whether or not a number x will have a multiplicative inverse modulo m?

7. Make a mod-26 multiplication table. Which numbers have multiplicative inverses? Are they the ones you predicted?

8. On a clean sheet of paper, make a table of the multiplicative inverses (modulo 26) of all the numbers between 0 and 25 that have multiplicative inverses. Keep this table handy in your notebook.

9. One of the rows in your table should show that the multiplicative inverse of 3 (modulo 26) is 9. It's called a *multiplicative inverse* because if you take any number x and multiply it by 3 (modulo 26) and then multiply the result by 9 (modulo 26), the answer is the original number x. So multiplication by 9 "undoes" multiplication by 3.

   Make up a few simple calculations to verify for yourself that the multiplicative inverses in your table have this property.