Affine functions and their inverses

Overview. A function of the form $x \mapsto ax + b$ is called *affine*. In modular arithmetic, some affine functions have inverses and some do not.

Background. In ordinary algebra, we find the inverse of the function $y = ax + b$ by solving for x and then interchanging x and y. (If you don't remember this, don't worry.)

We'll use a slightly different approach here. The mapping $x \mapsto ax + b$ says "first multiply by a, then add b." So the inverse of this mapping should say "first subtract b, then divide by a." For example, the inverse of the mapping

$$x \mapsto 5x + 7 \text{ ("first multiply by 5, then add 7")}$$

is

$$x \mapsto \frac{x - 7}{5} \text{ ("first subtract 7, then divide by 5").}$$

We can verify that this is the correct inverse by plugging in a few numbers. For example, the original mapping takes the number 3 to $5 \times 3 + 7$, which is 22. If we feed the number 22 into the inverse mapping, we get $(22 - 7)/5$, which is, indeed, 3. So it appears that our inverse correctly "undoes" the original mapping.

In modular arithmetic, the process is the same, except that instead of dividing, we multiply by a multiplicative inverse. So for instance, the inverse of the map $x \mapsto 5x + 7 \bmod 26$ ("first multiply by 5, then add 7, and take the result modulo 26") would read

"first subtract 7, then multiply by the multiplicative
inverse of 5 modulo 26 and take the result modulo 26."

To write this as a formula, we need to know that the multiplicative inverse of 5 modulo 26 is 21 (from a table in an earlier activity). The inverse mapping is $x \mapsto 21(x - 7)$.

Again, we can verify that this is right by plugging in numbers. If we apply the original mapping to 10, we get $5 \times 10 + 7$, which is 57, which is 5 when we reduce it modulo 26. If we feed 5 into the inverse mapping, we get $21(5 - 7)$, or -42. When we reduce -42 modulo 26, we get 10, as expected.

Things to do.

1. Using ordinary arithmetic, find the inverses to the following functions. Check your results by plugging in a couple of numbers to see if your inverse correctly "undoes" the original mapping.

   (a) $x \mapsto 3x + 8$

   (b) $x \mapsto 5x - 1$

   (c) $x \mapsto -x + 2$

2. Find the inverses modulo 26 to the following mappings. Again, check your answers by plugging in a few numbers to see that your inverses correctly undo the original functions.

   (a) $x \mapsto 7x + 5 \bmod 26$

   (b) $x \mapsto 25x - 3 \bmod 26$

3. Each of these mod-26 mappings gives a correspondence of the alphabet (plaintext) with the alphabet (ciphertext). For example, here's the alphabet correspondence that comes from the mapping $x \mapsto 5x + 2$. The plaintext is on the bottom.

   ```
   K F A V Q L G B W R M H C X S N I D Y T O J E Z U P
   a b c d e f g h i j k l m n o p q r s t u v w x y z
   ```

   Make a similar alphabet table for the mapping $x \mapsto 3x + 4$. Can you think of a fast way to do this?

4. Make an alphabet table for the mapping $x \mapsto 6x + 5$. Do you see any problems with using this table for a cipher?