AFFINE SUBSTITUTIONS

- For fixed integers a and b, with $\gcd(a, 26) = 1$, we can define a substitution by $\theta_{a,b} : x \mapsto ax + b \pmod{26}$. In this formula, we assume that the English alphabet is enumerated by $0, 1, 2, \ldots, 25$. (Eg, a=0 and z=25.)
- These are slightly harder than Caesar ciphers, but still quite easy to solve.

Example. Suppose we have discovered (say, by frequency analysis) that the letters c=2 and f=5 in the plaintext have been encrypted to H=7 and Q=16 in the ciphertext, respectively. This would be enough to determine the affine substitution. Namely, we need to solve this system of congruence equations to find a and b:

$$2a + b \equiv 7 \pmod{26},$$
$$5a + b \equiv 16 \pmod{26}.$$

The solutions is $a = 3$, $b = 1$. The affine substitutions $\theta_{3,1}$ can be depicted as:

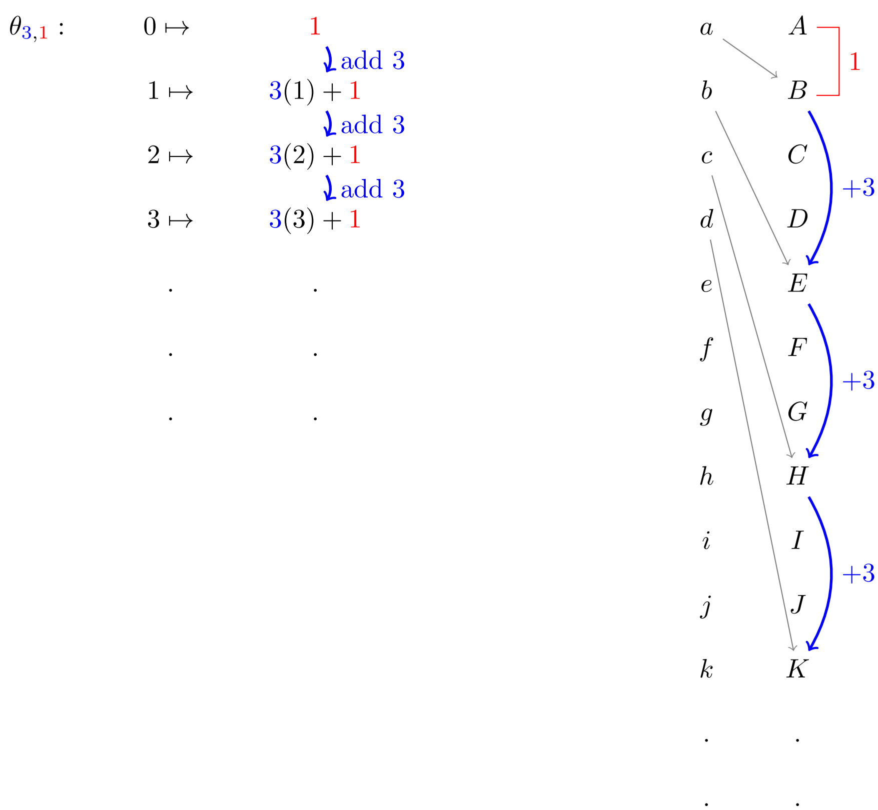

Figure 1. Visualizing the affine map $\theta_{3,1} : x \mapsto 3x + 1 \pmod{26}$