**Example 3.** Still working in our 26-letter alphabet, suppose that we know the most frequently occurring letter of ciphertext is "K", and the second most frequently occurring letter is "D". It is reasonable to assume that these are the encryptions of "E" and "T", respectively, which are the two most frequently occurring letters in the English language. Thus, replacing the letters by their numerical equivalents and substituting for $P$ and $C$ in the deciphering formula, we obtain:

$$10a' + b' \equiv 4 \ mod\ 26,$$
$$3a' + b' \equiv 19 \ mod\ 26.$$

We have two congruences with two unknowns, $a'$ and $b'$. The quickest way to solve is to subtract the two congruences to eliminate $b'$. We obtain $7a' \equiv 11 \ mod\ 26$, and $a' \equiv 7^{-1}11 \equiv 9 \ mod\ 26$. Finally, we obtain $b'$ by substituting this value for $a'$ in one of the congruences: $b' \equiv 4 - 10a' \equiv 18 \ mod\ 26$. So messages can be deciphered by means of the formula $P \equiv 9C + 18 \ mod\ 26$.

Recall from linear algebra that $n$ equations suffice to find $n$ unknowns only if the equations are independent (i.e., if the determinant is nonzero). For example, in the case of 2 equations in 2 unknowns this means that the straight line graphs of the equations intersect in a single point (are not parallel). In our situation, when we try to cryptanalyze an affine system from the knowledge of the two most frequently occurring letters of ciphertext, we might find that we cannot solve the two congruences uniquely for $a'$ and $b'$.

**Example 4.** Suppose that we have a string of ciphertext which we know was enciphered using an affine transformation of single letters in a 28-letter alphabet consisting of A—Z, a blank, and ?, where A—Z have numerical equivalents 0—25, blank=26, ?=27. A frequency analysis reveals that the two most common letters of ciphertext are "B" and "?", in that order. Since the most common letters in an English language text written in this 28-letter alphabet are " " (blank) and "E", in that order, we suppose that "B" is the encryption of " " and "?" is the encryption of "E". This leads to the two congruences: $a' + b' \equiv 26 \ mod\ 28$, $27a' + b' \equiv 4 \ mod\ 28$. Subtracting the two congruences, we obtain: $2a' \equiv 22 \ mod\ 28$, which is equivalent to the congruence $a' \equiv 11 \ mod\ 14$. This means that $a' \equiv 11$ or $25 \ mod\ 28$, and then $b' \equiv 15$ or $1 \ mod\ 28$, respectively. The fact of the matter is that both of the possible affine deciphering transformations $11C + 15$ and $25C + 1$ give " " and "E" as the plaintext letters corresponding to "B" and "?", respectively. At this point we could try both possibilities, and see which gives an intelligible message. Or we could continue our frequency analysis. Suppose we find that "I" is the third most frequently occurring letter of ciphertext. Using the fact that "T" is the third most common letter in the English language (of our 28 letters), we obtain a third congruence: $8a' + b' \equiv 19 \ mod\ 28$. This extra bit of information is enough to determine which of the affine maps is the right one. We find that it is $11C + 15$.