15. (*expires 3/15*) The string below was encrypted using an affine cipher on the 27 letter alphabet " abcdefghijklmnopqrstuvwxyz" (there is a space in the 0^{th} position.) Decrypt it.

```
fmw segjaweoouanerj a ceyqrype aswaheoaqbrqabeafrua eeaojerf afmjeayperjpu
```

Hint: this phrase follows the the typical pattern in English where there are (almost) as many spaces as words (and so spaces are very common), and the letter "e" is also very common. You can use the technique described in chapter 4 of the notes, section 7.3.

If you wish, the encrypted text can be loaded from the file `afftext.txt` in the problems section of the class web page

16. (*expires 3/15*) We saw that in order for an affine cipher given by $x \mapsto ax + b \mod p$ to be invertible, we must be able to solve the equation $ax = 1 \mod p$ for all nonzero values of x. This is equivalent to the condition $\gcd(a, p) = 1$, that is, that a and p must have no common divisors.

Something similar is true in the case when we do affine enciphering with a matrix (i.e. $v \mapsto Av + b \mod p$, where A is an $n \times n$ matrix and b and v are n-vectors). What is the exact condition needed on A and p for mapping to be invertible, that is, for $A^{-1} \mod p$ to exist? You don't have to give a proof of your answer (although you can), but use `Maple` to demonstrate several examples where the inverse exists and when it will fail to exist. (Obviously if the matrix A has a zero determinant, the inverse will not exist. But there are matrices which are invertible over the reals which do not have inverses $\mod p$.)

17. (*expires 3/15*) Modify the `AffineMatCrypt` routine we wrote in class on March 6 so that you can use a text string as a key instead of a matrix and a vector. (Alternatively, you can modify `AffineMatEncode` from section 8.2 of the notes, which is essentially the same thing.)

For example, if the phrase is k characters long, the key should be an $n \times n$ matrix and an n-vector, where $n^2 + n \approx k$, and n is determined from the length of the key phrase. The elements of the key matrix and vector should be the numerical equivalents of the characters in the key phrase. Do something sensible with any extra letters (that is, if $k \neq n^2 + n$). Be sure to check that the resulting matrix is nonsingular.

Demonstrate that your modifications work by encoding and decoding the text

```
Once upon a midnight dreary, while I pondered, weak and weary,
Over many a quaint and curious volume of forgotten lore,
While I nodded, nearly napping, suddenly there came a tapping,
As of some one gently rapping, rapping at my chamber door.
"Tis some visitor," I muttered, "tapping at my chamber door.
Only this, and nothing more."
```

with both a short key phrase (for example, `Lenore`, which would use a 2×2 matrix and a 2-vector) and with a longer keyphrase (for example, `Quoth the raven, "Nevermore"`, which requires either a 5×5 matrix and a 5-vector, or a 4×4 depending on how you treat extra letters.)

The text to encrypt can be found in the problems section of the class web page, in the file `raven.txt`.