Recently Asked Questions
in Math 502

1. Q. Will all the code files be available on the T drive?

   A. Yes.

2. Q. I would like to understand whether the block size specified in "sqvec" must be set larger than the highest value in a string of ASCII codes which has been shifted prior to encryption. In other words, if a vector of ASCII codes has been shifted n digits before encryption, should the block size be greater than (127+n)?

   A. Note that the first argument of "sqvec" is supposed to be a vector of digits in base b, where b is the second argument. So `sqvec(v,2,3)` converts a vector of digits in base 2 to a vector of digits in base $2^3 = 8$. If by "block size" you mean the third argument, the answer to your question is *no*. If, on the other hand, it refers to the second argument, then the answer is *yes*.

   Note, however, that "sqvec" is not, strictly speaking, useful for general base conversions since it "pads" its first argument with trailing 0's so that the number of components is a multiple of the block size specified in the third argument.

   Do the following illustrations cover your question? If not, please try to restate your question in a more specific way.

```
> v:=convert(40487,base,2);
              v := [1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1]

> sqvec(v,2,3);
                                  [7, 1, 0, 7, 4, 4]

> w:=convert(40487,base,3);
                         w := [2, 1, 1, 2, 1, 1, 1, 0, 0, 2]

> sqvec(w,2,3);
Error: term 2 (seq. 1) not a digit in base 2

> x:=convert(``test string'', bytes);
           x := [116, 101, 115, 116, 32, 115, 116, 114, 105, 110, 103]

> xs:=vshift(x,-30);
                xs := [86, 71, 85, 86, 2, 85, 86, 84, 75, 80, 73]

> xsq:=sqvec(xs,97,2);
                   xsq := [8413, 8331, 279, 8426, 7355, 7081]

> convert(vshift(exvec(xsq,97,2),30),bytes);
                                    ``test string''
```