MAT331 Exercises, Spring 08

set number 8

27. (*expires 5/21*) Reimplement the `AffineMatEncode` and `AffineMatDecode` programs from the notes (section 4.8) to use the routines from the `LinearAlgebra` package instead of `linalg`.

28. (*expires 5/21*) Twenty-one pirates are dividing their horde of gold dubloons. Since they are a democratic outfit, they first try to divide the coins evenly, but they find there are 19 coins left over. The "discussion" about how to divide the remaining coins results in only 16 pirates still needing to divide the horde (the remaining five went to a place where you can't bring money or anything else with you). The redivision among 16 pirates leaves 1 coin left over, and three of the pirates make a grab for it. These three find themselves to be missing their hands after this attempt, and the remaining thirteen pirates decide to divide the share among themselves, leaving the handless ones with nothing. Fortunately, the horde divides evenly among the thirteen. What is the minimum number of coins in the horde?

29. (*expires 5/21*) Use RSA with the modulus $n = 119$ and the exponent $e = 7$, with the 95-character alphabet consisting of the printable ASCII characters to encrypt the word "Yes". Recall that the alphabet is given by

```
Alphabet:=cat(op(select(IsPrintable, [seq( convert([i],bytes), i=1..255)])))
```

so that Y=58, e=70, s=84. Give your encryption as a list of three numbers.

30. (*expires 5/21*) With the same setup as the previous problem (that is $n = 119$, $e = 7$), the message after encrypting with RSA is the list of numbers

$$[42, 59, 4, 59, 27, 59].$$

Decrypt the message. (This is doable because 119 is easily factored).