Mathematics 243–Algebraic Structures
Selected Solutions – Problem Set 8
November 13, 2006

2.8/22. Since it is given that $m = 51$, we need to factor: $51 = 3 \cdot 17$, so we take $p = 3$ and $q = 17$. This means that the decoding exponent d will satisfy

$$de \equiv 1 \bmod (p-1)(q-1), \text{ so } 5d \equiv 1 \bmod 32$$

This says $[d]$ should be the multiplicative inverse of $[5]$ in $\mathbf{Z}_{32}$. We see $d = 13$, since $5 \cdot 13 = 65 \equiv 1 \bmod 32$. (This can also be derived by carrying out the Euclidean algorithm to find $\gcd(5, 32) = 1$, of course.)

To decode the given message, we must apply the decoding function

$$g(x) = x^{13} \bmod 51$$

to each two-digit block in the ciphertext. This can be done without too much trouble by the technique of *repeated squaring*. For instance, the third block is $x = 32$:

$$\begin{aligned} x &\equiv 32 \bmod 51 \\ x^2 &\equiv 32^2 = 1024 \equiv 4 \bmod 51 \\ x^4 &\equiv 4^2 = 16 \bmod 51 \\ x^8 &\equiv 16^2 = 256 \equiv 1 \bmod 51 \\ \text{so } x^{13} &= x^8 \cdot x^4 \cdot x \equiv 1 \cdot 16 \cdot 32 = 512 \equiv 2 \bmod 51 \end{aligned}$$

This means that

$$g(32) = 32^{13} \equiv 2 \bmod 51$$

and the third block decodes to the letter 'C'. Carrying out the same process on each 2-digit block gives the decoded message 'EUCLIDEAN ALGORITHM'.

3.1/5. Let $S = \{x \in \mathbf{R} : 0 < x \leq 1\}$ with the operation of multiplication. This set is closed under products since $0 < x \leq 1$ and $0 < y \leq 1$ implies $0 < xy \leq 1$. Multiplication in $\mathbf{R}$ is associative in general, so that property also holds for products of elements of S. The multiplicative identity 1 in $\mathbf{R}$ is in S, so S has a multiplicative identity. But note that if $x \in S$ then the multiplicative inverse $1/x$ need not be in S. For instance, if $x = 1/3$, then $x^{-1} = 3 \notin S$. We conclude that S is not a group under multiplication.

3.1/24. We have the following operation table for multiplication modulo 10 on the set $S = \{[0], [2], [4], [6], [8]\} \subset \mathbf{Z}_{10}$:

	[0]	[2]	[4]	[6]	[8]
[0]	[0]	[0]	[0]	[0]	[0]
[2]	[0]	[4]	[8]	[2]	[6]
[4]	[0]	[8]	[6]	[4]	[2]
[6]	[0]	[2]	[4]	[6]	[8]
[8]	[0]	[6]	[2]	[8]	[4]

The set is closed under multiplication modulo 10 as can be seen from the table. Multiplication is associative in $\mathbf{Z}_{10}$, so the same is true for multiplication mod 10 on the elements in this subset. *There is* an identity element for multiplication, but it's not what you expect. Look at the row and column for the element [6]. This shows that [6] is an identity for this operation on this subset. The only property that fails is that [0] has no multiplicative inverse – there is no $[x] \in S$ such that $[0][x] = [6]$. Note that the subset $\{[2], [4], [6], [8]\}$ *does* form a group under multiplication mod 10.

3.1/33. Let

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{R} \right\}$$

We claim that G is a group under matrix multiplication.

First, G is closed under matrix products because

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \tag{1}$$

Since this matrix has the correct form (1's on main diagonal, 0's below, real numbers above), this is an element of G. Matrix multiplication is associative whenever the product of three matrices is defined, so that property holds for the matrices in G. The identity matrix

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is in G (take $a = b = c = 0$), and is an identity element for matrix multiplication. Finally, from (1) we see that if $d = -a$, $f = -c$, and $e = -af - b = ac - b$, then

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$$

The product in the other order also gives I, so

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

This is a matrix in G, so every element of G has an inverse in G.