Mathematics 243 – Algebraic Structures
Solutions for Review Problems for Final Exam
December 8, 2006

I. A) φ *is* one-to-one. If x and x' are two even numbers, then $\varphi(x) = \varphi(x')$ implies $5x = 5x'$, which implies $x = x'$ (since $5(x - x') = 0$ implies $x - x' = 0$). Similarly if x and x' are both odd, then $\varphi(x) = \varphi(x')$ implies $x - 2 = x' - 2$. Adding 2 to both sides, $x = x'$. Finally if x is even and x' is odd, then $\varphi(x)$ is even and $\varphi(x')$ is odd, so $\varphi(x) \neq \varphi(x')$.

φ is not onto, since for instance $\varphi(x) \neq 2$ for all $x \in \mathbf{Z}$.

B)

$$\varphi^{-1}(\{3,4,5,6,7\}) = \{x \in \mathbf{Z} : \varphi(x) \in \{3,4,5,6,7\}\} = \{5,7,9\}$$

(There are no integers mapping to the even numbers $4, 6$ here.)

C)

$$\varphi(\{1,2,3\} \cap \{x \in A : x^2 < 5\}) = \varphi(\{1,2\}) = \{-1, 10\}$$

II. A) See class notes or the text.

B) Applying the Euclidean Algorithm we have

$$\begin{aligned} 753 &= 4 \cdot 154 + 137 \\ 154 &= 1 \cdot 137 + 17 \\ 137 &= 8 \cdot 17 + 1 \end{aligned}$$

So $\gcd(753, 154) = 1$. Then

$$\begin{array}{ccc} & 1 & 0 \\ & 0 & 1 \\ 4 & 1 & -4 \\ 1 & -1 & 5 \\ 8 & 9 & -44 \end{array}$$

So $1 = 9 \cdot 753 + (-44) \cdot 137$.

C) From the hypothesis that $\gcd(a, c) = 1$ we have $1 = ra + sc$ for some integers r, s. Multiplying both sides of this equation by b we obtain $b = rab + sbc$. Since we know also $a|(bc)$, $bc = qa$ for some integer q. Hence $b = rab + sbc = a(rb + sq)$, which shows $a|b$.

III. A)

$$A^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad A^3 := \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$$

B) Note that $f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2$. etc. The base case for the induction is $n = 1$, and

$$A^1 = A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}$$

as claimed. Now assume that the statement is true for $n = k$:

$$A^k = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix}.$$

Then

$$A^{k+1} = A^k \cdot A = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

By the definition of matrix multiplication this is

$$A^{k+1} = \begin{pmatrix} f_{k+1} + f_k & f_{k+1} \\ f_k + f_{k-1} & f_k \end{pmatrix}$$

Using the recurrence for the Fibonacci numbers, this gives

$$A^{k+1} = \begin{pmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix}$$

which is what we wanted to show.

IV. A) We want to assume that A is represented by $[0]$, B by $[1]$, etc. through Z by $[25]$, all mod 26. The encryption function for an affine cipher has the form $f([x]) = [a][x] + [b]$ so from $f([4]) = [25]$ and $f([19]) = [1]$,

$$[a][4] + [b] = [25] \quad \text{and} [a][19] + [b] = [1].$$

Hence subtracting, $[15][a] = [-24] = [2]$. $[15]$ has a multplicative inverse in $\mathbf{Z}_{26}$ since $\gcd(26, 15) = 1$, and $[15]^{-1} = [7]$, since $7 \cdot 15 = 105 \equiv 1 \bmod 26$. Therefore $[a] = [7][2] = [14]$ and $[b] = [25] - [56] = [25] - [4] = [21]$ in $\mathbf{Z}_{26}$. Therefore

$$f([x]) = [14][x] + [21].$$

This is actually a sort of trick question because it turns out that this mapping *does not have an inverse function*(!) It would not be suitable for use as an affine cipher. The reason is that $[14]$ *does not* have an inverse in $\mathbf{Z}_{26}$, so this mapping is not one-to-one. Note that $f([x]) = f([x + 13])$ since $[14x] = [14x + 26]$.

B) The integer $m = 323 = 17 \cdot 19$. So we want $ed = 29d \equiv 1 \bmod (17 - 1)(19 - 1) = 288$. This implies $d = 149$ (by calculations like the ones in II A above).

V. A) G is closed under matrix sums since

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ 0 & d + d' \end{pmatrix}$$

which is also in G. Matrix addition in G is associative because addition in $\mathbf{R}$ is associative:

$$\begin{aligned}
&\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}\right) + \begin{pmatrix} a'' & b'' \\ 0 & d'' \end{pmatrix} \\
&= \begin{pmatrix} (a+a')+a'' & (b+b')+b'' \\ 0 & (d+d')+d'' \end{pmatrix} \\
&= \begin{pmatrix} a+(a'+a'') & b+(b'+b'') \\ 0 & d+(d'+d'') \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} + \left(\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ 0 & d'' \end{pmatrix}\right)
\end{aligned}$$

The matrix $Z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is in G (take $a = b = d = 0$) and is an identity element for matrix addition. Finally, for each $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$, $-A = \begin{pmatrix} -a & -b \\ 0 & -d \end{pmatrix} \in G$ too and satisfies $A + (-A) = Z$ (as above). Therefore G is a group under matrix sums.

B) No. The set H is not closed under matrix *sums*. For instance

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix}$$

which is not in H (because of the 2's on the main diagonal).

VI. A) The elements that have multiplicative inverses in $\mathbf{Z}_{30}$ are the $[x]$ with $\gcd(x, 30) = 1$:

$$[1], [7], [11], [13], [17], [19], [23], [29]$$

B) The elements that generate the additive subgroup $\langle [24] \rangle$ are the classes $[x]$ such that $\gcd(30, x) = \gcd(30, 24) = 6$. This gives

$$[6], [12], [18], [24].$$

VII. A) $\ker(\varphi) = \{x \in G : \varphi(x) = e_H\}$.

B) First, if $k \in K = \ker(\varphi)$, then by properties we know for group homomorphisms,

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e_H(\varphi(g))^{-1} = e_H$$

Therefore $gkg^{-1} \in K$, so $gKg^{-1} \subseteq K$. To get the other inclusion, note that if $k \in K$, then $k = g\left(g^{-1}kg\right)g^{-1}$. By an argument exactly like the other direction, we see that $g^{-1}kg \in K$ if $k \in K$. Therefore $k \in gKg^{-1}$ and $K \subseteq gKg^{-1}$. Hence $K = gKg^{-1}$.

C) The relation R is reflexive since for all $x \in G$, $xx^{-1} = e_G \in \ker(\varphi)$. The relation R is symmetric since if xRy, then $xy^{-1} \in \ker(\varphi)$. But $\ker(\varphi)$ is a subgroup of G, so it closed under inverses. $(xy^{-1})^{-1} = yx^{-1}$ (reverse order rule for inverses). Hence yRx follows. Finally, the relation R is transitive since if xRy and yRz then $xy^{-1}, yz^{-1} \in \ker(\varphi)$. $\ker(\varphi)$ is a subgroup of G so it is closed under products:

$$(xy^{-1})(yz^{-1}) = x(y^{-}y)z^{-1} = xz^{-1}$$

Hence xRz and R is transitive.