Mathematics 243, section 3 – Algebraic Structures
Solutions for Exam 3 – December 5, 2012

I. In an RSA public key cryptosystem, the public key information is $m = 323$ and $e = 13$. Messages consisting of capital roman letters and blanks are encoded as 3-digit blocks $000, 001, \cdots, 026$ (with blank = 000, A = 001, B = 002, ... , Z = 026) and encrypted as 3-digit blocks.

A) (15) How would the plaintext symbol N be encrypted?

Solution: The RSA encryption function is $f(x) = x^{13} \bmod 323$. The letter N is encoded as the integer 14 so we need to compute $14^{13} \bmod 323$. Applying the repeated squaring process:

$$14^2 \equiv 196 \bmod 323$$
$$14^4 \equiv 302 \bmod 323$$
$$14^8 \equiv 118 \bmod 323$$

So $14^{13} \equiv 14^8 \cdot 14^4 \cdot 14 \equiv 192 \bmod 323$. The plain text symbol N is encrypted as the 3-digit block 192.

B) (15) What is the (secret) decryption exponent d?

Solution: We have $323 = 19 \cdot 17$, so $(p-1)(q-1) = 18 \cdot 16 = 288$. So we want d so that $[13][d] = [1]$ in $\mathbf{Z}_{288}$. We apply the Euclidean algorithm:

$$288 = 22 \cdot 13 + 2$$
$$13 = 6 \cdot 2 + 1$$

Then the Extended Euclidean Algorithm table gives

	1	0
	0	1
22	1	−22
6	−6	133

This shows $(-6)(288) + (133)(13) = 1$, so $d = 133$.

II. (20) Let

$$H = \left\{ A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbf{R} \text{ and } a \neq 0 \right\}$$

Is H a group under the operation of matrix multiplication? If so, give a proof. If not, say which of the group properties fail.

Solution: H is a group under matrix multiplication.

1. First, H is closed under matrix products, since if $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $A' = \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}$ are in H (so $a, a' \neq 0$), then the product

$$AA' = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix} \in H$$

   (because $aa' \neq 0$).
2. Matrix multiplication is associative whenever the products are defined (proved in class).
3. The identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ and acts as the identity element for H.
4. The inverse matrix of $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ is $A^{-1} = \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} \in H$.

So all of the properties of groups are satisfied.

III.

A) (15) Let G be a cyclic group with generator a. Show that every subgroup of G is also cyclic.

Solution: Let H be the subgroup. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic and there is nothing more to show. If $H \neq \{e\}$, then H must contain positive powers of the generator a, so $\{n \mid a^n \in H\} \cap \mathbf{Z}^+ \neq \emptyset$. By the Well-Ordering Principle, this set has a smallest element, say k. We claim that $H = \langle a^k \rangle$, so H is cyclic. First $a^k \in H$, so $\langle a^k \rangle \subseteq H$, since H is closed under products and inverses. Next, if $a^n \in H$, then we can use the Division Algorithm in $\mathbf{Z}$ to write $n = qk + r$ for some r with $0 \leq r < k$. But notice that $a^r = a^n (a^k)^{-q} \in H$. So it follows that $r = 0$ since k was the smallest positive integer such that $a^k \in H$. This shows $H \subseteq \langle a^k \rangle$. We have both inclusions so $H = \langle a^k \rangle$.

The next parts of this question refer to $\mathbf{Z}_{24}$, which is a cyclic group under addition mod 24.

B) (10) How many different subgroups does $\mathbf{Z}_{24}$ contain, including $\mathbf{Z}_{24}$ itself and $\{[0]\}$?

Solution: There is one subgroup of size d for each divisor d of 24, that is: $d = 1, 2, 3, 4, 6, 8, 12, 24$. Hence there are 8 of them. Part A) implies all of these subgroups are cyclic too. One choice of generator for each of the 8 subgroups:

$$[0], [12], [8], [6], [4], [3], [2], [1],$$

respectively.

C) (15) Show that if $\gcd(a, 24) = 1$, then $\phi : \mathbf{Z}_{24} \to \mathbf{Z}_{24}$ defined by $\phi([x]) = [ax]$ is a 1-1 and onto group homomorphism.

Solution: $\gcd(a, 24) = 1$ implies that $[a]$ has a multiplicative inverse in $\mathbf{Z}_{24}$. Hence if $\phi([x]) = [ax] = [a][x] = [a][y] = [a][y] = \phi([y])$, then we can multiply both sides by $[a]^{-1}$ to get $[x] = [y]$. That shows ϕ is 1-1. Similarly, if $[y] \in \mathbf{Z}_{24}$ is any class, the equation $\phi([x]) = [a][x] = [y]$ has the solution $[x] = [a]^{-1}[y]$. Hence ϕ is onto. Finally we compute:

$$\phi([x] + [y]) = \phi([x + y]) = [a(x + y)] = [ax + ay] = [ax] + [ay] = \phi([x]) + \phi([y]).$$

Hence ϕ is a group homomorphism.

IV. (10) Let G be a group, let H be a subgroup of G, and let $a \in G$ be a fixed element. Let $aH = \{ah \mid h \in H\}$. Show that aH is a subgroup of G if and only if $a \in H$.

Solution: If aH is a subgroup of G, then we must have $ah = e$ for some $h \in H$, but then $a = h^{-1} \in H$ too since H is a subgroup of G and closed under taking inverses. Conversely, if $a \in H$, then $aH \subseteq H$ since H is closed under products. Moreover, if $k \in H$ is arbitrary, then $k = ah \in aH$ for $h = a^{-1}k$. Therefore $H \subseteq aH$. This shows that if $a \in H$, then $aH = H$ so aH is a subgroup of G.

Extra Credit (10) A group G is generated by elements x, y satisfying the relations $x^n = e$, $y^2 = e$, and $yx = x^{n-1}y$. Show that all of the elements $x^\ell y$ for $\ell = 0, 1, \ldots, n-1$ have order 2.

Solution: We must show that $(x^\ell y)(x^\ell y) = e$. We can argue by induction that this is true for all $\ell \geq 0$ as follows. First, if $\ell = 0$, it is given that $y^2 = e$, so the statement is true in that case. Then suppose we know that $(x^k y)(x^k y) = e$ and consider

$$\begin{aligned}
(x^{k+1}y)(x^{k+1}y) &= x^{k+1}(yx)(x^k y) \text{ by associativity} \\
&= x^{k+1}(x^{n-1}y)(x^k y) \text{ by the given relations} \\
&= (x^{k+1}x^{n-1}y)(x^k y) \text{ by associativity} \\
&= (x^k x^n y)(x^k y) \text{ by rules for exponents} \\
&= (x^k y)(x^k y) \text{ by the given relations} \\
&= e \quad \text{by the induction hypothesis}
\end{aligned}$$

It follows that $x^\ell y$ has order 2 for all $\ell \geq 0$. Since $x^n = e$, we start repeating the same elements when $\ell = n$, though.