Mathematics 243, section 3 – Algebraic Structures
Solutions for Exam 3 Review Questions
November 29, 2012

I. An RSA public-key cryptographic system has $m = 143$ and the encryption exponent $e = 17$.

A) What is the corresponding decryption exponent d?
Solution: Since $m = 143 = 11 \cdot 13$, the primes are $p = 11$ and $q = 13$, and $(p-1)(q-1) = 120$. Since $e = 17$ satisfies $\gcd(17, 120) = 1$, $[17]$ has a multiplicative inverse $[d] = [17]^{-1}$ in $\mathbf{Z}_{120}$ and that gives the decryption exponent. We can compute the multiplicative inverse using the Euclidean Algorithm technique, but in fact this works out very simply here:

$$120 = 7 \cdot 17 + 1$$

So $[17]^{-1} = [-7] = [113]$. Thus $d = 113$. (Note: We could also use $d = -7$, but that is not usually done with RSA decryption, since it requires computations of inverses at every step.)

B) If you use a 26-letter alphabet, represented by the numbers $0, 1, \ldots, 25$, and 3-digit blocks to represent the encrypted symbols, what would be the encrypted form of the plaintext: HC?
Solution: We have $H \leftrightarrow 7$ and $C \leftrightarrow 2$ (since we're starting from 0). The H encrypts to $7^{17} \equiv 50 \bmod 143$ and the C encrypts to $2^{17} \equiv 84 \bmod 143$. If we use three-digit blocks to represent each letter, we get $050, 084$ as the encrypted form. Practical Note: The best way to compute powers like this is via *repeated squaring*, since that keeps the sizes of the integers encountered small. We have, for instance

$$\begin{aligned} 7^2 &\equiv 49 \bmod 143 \\ 7^4 &\equiv 49^2 \equiv 113 \bmod 143 \\ 7^8 &\equiv 113^3 \equiv 42 \bmod 143 \\ 7^{16} &\equiv 42^2 \equiv 48 \bmod 143 \\ \text{So, } 7^{17} &= 7^{16} \cdot 7 \equiv 48 \cdot 7 = 336 \equiv 50 \bmod 143. \end{aligned}$$

II. Let $\mathbf{Q}$ be the set of rational numbers: $\mathbf{Q} = \{m/n : m, n \in \mathbf{Z}, n \neq 0\}$. Define a binary operation $*$ on $\mathbf{Q} - \{-1\}$ by $x * y = x + y + x \cdot y$ (where $\cdot$ is ordinary multiplication). Is $G = \mathbf{Q} - \{-1\}$ a group under $*$? Why or why not?

Solution: The answer is: *Yes.* Note that

$$x * y = (1 + x) \cdot (1 + y) - 1$$

(where the $\cdot$ is ordinary multiplication). If x, y are rational numbers, then $x * y$ is definitely a rational number since $\mathbf{Q}$ is closed under sums and products. The displayed formula above also says that if $x \neq -1$ and $y \neq -1$, then $x * y \neq -1$. (Equivalently, if $x * y = -1$, then

$(1+x)(1+y) = 0$, so $x = -1$ or $y = -1$, which is the contrapositive form of the first statement.) Hence G is closed under $*$. Next, we have

$$(x * y) * z = (x + y + x \cdot y) * z = x + y + z + x \cdot y + x \cdot z + y \cdot z + x \cdot y \cdot z = x * (y * z)$$

so the operation $*$ is associative. The element $0 \in G$ acts as an identity for $*$ since $x * 0 = x = 0 * x$ for all $x \in G$. Finally, if $x \in G$, then $x * y = x + y + x \cdot y = 0$ if and only if $y = \frac{-x}{1+x}$. This makes sense in $\mathbf{Q}$ as long as $x \neq -1$, and $y \neq -1$ since $\frac{-x}{1+x} = -1$ has no rational solutions. Therefore every element in G has an inverse in G.

III.

A) Find all generators of the group $G = \mathbf{Z}_{21}$, in which the operation is addition mod 21.
Solution: The generators are the $[a]$ such that $\gcd(a, 21) = 1$, which are:

$$[1], [2], [4], [5], [8], [10], [11], [13], [16], [17], [18], [20]$$

B) What are the possible orders of elements of the group G from part A?
Solution: By the "big theorem" on cyclic groups, the order of the element $[a]$ is $o([a]) = 21/\gcd(a, 21)$. There are exactly four possible orders: $o([a]) = 1$ if $a = 0$, $o([a]) = 3$ if $a = 7, 14$, $o([a]) = 7$ if $a = 3, 6, 9, 12, 15, 18$ and $o([a]) = 21$ for the a in part A of this question. We also have

$$\langle [3] \rangle = \langle [6] \rangle = \cdots = \langle [18] \rangle$$

and

$$\langle [7] \rangle = \langle [14] \rangle.$$

IV. Let $G = \langle a \rangle$ be a cyclic group.

A) Show that every subgroup $H \subset G$ is cyclic.

B) Show that if G is finite, with $|G| = n$, then $\langle a^k \rangle = \langle a^d \rangle$ where $d = \gcd(n, k)$.
See the class notes for these.

V. Let $G = \mathbf{Z}_{12}$ and $H = \mathbf{Z}_9$, which are both groups under addition. We write $[x]_{12}$ for the congruence class of x mod 12, and similarly $[x]_9$ for the class mod 9. Define $\phi : G \to H$ by $\phi([x]_{12}) = [3x]_9$.

A) Show that $[x]_{12} = [y]_{12}$ implies $[3x]_9 = [3y]_9$ (so that this mapping actually makes sense).
Solution: If $[x]_{12} = [y]_{12}$, then $12|(x - y)$, or $x - y = 12k$ for some integer k. But then $3x - 3y = 3(x - y) = 36k = (4k) \cdot 9$, so $9|(3x - 3y)$. This shows $[3x]_9 = [3y]_9$.

B) Show that ϕ is a *group homomorphism*.
Solution: We have by the definitions of the additions in $\mathbf{Z}_{12}$ and $\mathbf{Z}_9$, plus the definition of ϕ:

$$\begin{aligned}
\phi([x]_{12} + [y]_{12}) &= \phi([x + y]_{12}) \\
&= [3(x + y)]_9 \\
&= [3x + 3y]_9 \\
&= [3x]_9 + [3y]_9 \\
&= \phi([x]_{12}) + \phi([y]_{12})
\end{aligned}$$

Since this is true for all x, y, the mapping ϕ is a homomorphism of groups.

C) Find all the elements of $\ker(\phi)$.
Solution: $\ker(\phi) = \{[x]_{12} \in \mathbf{Z}_{12} \mid [3x]_9 = [0]_9\}$. This is the set $\{[0], [3], [6], [9]\}$ (the subgroup $\langle [3] \rangle$ in $\mathbf{Z}_{12}$).

VI. Let G be a group and let $a \in G$ be a fixed element. Define

$$C(a) = \{x \in G : ax = xa\}$$

A) Is $b = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ in $C(a)$ for $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $G = GL(2, \mathbf{R})$ (a group under matrix multiplication)? Why or why not?
Solution: We check:

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ 3 & 4 \end{pmatrix}$$

But

$$ba = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 3 & 7 \end{pmatrix}$$

Since these are different, the answer is *no*.

B) Show that $C(a)$ is a subgroup of G.
Solution: We use the "shortcut method" from Theorem 3.10 in the text. $C(a)$ is not empty since the identity e in G satisfies $ae = ea = a$. So $e \in C(a)$. Next, if $x, y \in C(a)$, then we have $ax = xa$ and $ay = ya$. The second equation also implies $ay^{-1} = y^{-1}a$ (multiply on both sides of the equation by y^{-1} on left and right). Then

$$\begin{aligned} a(xy^{-1}) &= (ax)y^{-1} \text{ by associativity} \\ &= (xa)y^{-1} \text{ since } x \in C(a) \\ &= x(ay^{-1}) \text{ by associativity} \\ &= x(y^{-1}a) \text{ by the above observation} \\ &= (xy^{-1})a \text{ by associativity} \end{aligned}$$

This shows that $xy^{-1} \in C(a)$, so $C(a)$ is a subgroup of G.