Mathematics 243, section 1 – Algebraic Structures
Solutions for Practice Exam 3
November 27, 2006

I. A) By the definition of RSA systems, we need to know the prime factorization of m, which is $m = 11 \cdot 13$ here. Then d is the multiplicative inverse of $e = 17 \bmod (11-1)(13-1) = 120$. We have

$$120 = 7 \times 17 + 1.$$

This equation says $7 \times 17 \equiv -1 \bmod 120$, so $d = 113 \equiv -7 \bmod 120$.

B) We have $H = 7$ and $C = 2$ (starting from $A = 0$). Hence by repeated squaring,

$$7^2 \equiv 49 \bmod 143, \quad 7^4 \equiv 113 \bmod 143, \quad 7^8 \equiv 42 \bmod 143, \quad 7^{16} \equiv 48 \bmod 143$$

and

$$2^2 \equiv 4 \bmod 143, \quad 2^4 \equiv 16 \bmod 143, \quad 2^8 \equiv 113 \bmod 143, \quad 2^{16} \equiv 42 \bmod 143.$$

Hence

$$f(7) = 7^{17} \equiv 7 \cdot 7^{16} \equiv 7 \cdot 48 \equiv 50 \bmod 143$$
$$f(2) = 2^{17} \equiv 2 \cdot 2^{16} \equiv 2 \cdot 42 \equiv 84 \bmod 143$$

The encrypted form is 050, 084 (with three-digit blocks).

II. The answer is *yes*. The operation $*$ defined here on the set of rational numbers other than -1 does satisfy all the properties needed for a group operation:

i. $\mathbf{Q}$ is closed under $*$ since if $x = m/n$ and $y = p/q$ are any two rational numbers,

$$x * y = m/n + p/q + m/n \cdot p/q = (mq + np + mp)/(nq)$$

is a quotient of integers – an element of $\mathbf{Q}$.

ii. The operation $*$ is associative: We have

$$(x * y) * z = (x + y + xy) * z = x + y + xy + z + xz + yz + xyz$$

and

$$x * (y * z) = x * (y + z + yz) = x + y + z + yz + xy + xz + xyz$$

are equal for all $x, y, z \in \mathbf{Q}$ (by commutativity of addition).

iii. The element $0 \in \mathbf{Q}$ is an identity element for $*$:

$$x * 0 = x + 0 + x \cdot 0 = x = 0 + x + 0 \cdot x = 0 * x$$

for all x.

iv. If we try to find an inverse element for $x \in \mathbf{Q}$, that is, a y such that

$$0 = x * y = x + y + xy$$

we see $y = \frac{-x}{1+x}$. This is only defined if $x \neq -1$. Since we removed $x = -1$, then the remaining elements of $\mathbf{Q}$ *do form a group under this operation*(!)

III. A) We'll use the result that if $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator for G if and only if $\gcd(k, n) = 1$. (This follows, for instance from IV B below!). The additive group $\mathbf{Z}_{21}$ is cyclic with generator $[1]$ for instance. Hence

$$[1], [2], [4], [5], [8], [10], [11], [13], [16], [17], [19], [20]$$

are all generators (for instance $[5] = k \cdot [1]$ and $\gcd(21, 5) = 1$).

B) The elements from part A all have order 21. The elements $[3], [6], [9], [12], [15], [18]$ all generate $\langle [3] \rangle$ and have order 7. The elements $[7], [14]$ generate $\langle [7] \rangle$ and have order 3. $[0]$ has order 1.

IV. A) Let $G = \langle a \rangle$, so H consists of some set of powers a^k. If $H = \{a^0 = e\}$, then $H = \langle e \rangle$ is cyclic. Hence from now on we can assume that H contains some a^k for $k > 0$. Let m be the *smallest strictly positive integer* such that $a^m \in H$. We will show that $H = \langle a^m \rangle$, which will show that H is cylic. First $\langle a^m \rangle \subseteq H$ since H is a subgroup of G, hence closed under products and inverses. Conversely, suppose $a^n \in H$. In the integers, divide m into n, yielding

$$n = qm + r$$

for some unique integers q, r with $0 \leq r \leq m-1$. We have $a^n = a^{qm+r} = (a^m)^q \cdot a^r$. Hence

$$a^r = ((a^m)^q)^{-1} \cdot a^n. \tag{1}$$

We are assuming $a^m \in H$ and $a^n \in H$. Since H is a subgroup, it is closed under products and inverses, hence the equation (1) above shows that $a^r \in H$ too. But we assumed that m was the smallest strictly positive integer such that $a^m \in H$. Hence $r = 0$, so $n = qm$ and $a^n = a^{mq} = (a^m)^q \in \langle a^m \rangle$. It follows that $H \subseteq \langle a^m \rangle$. Since we have both inclusions now, $H = \langle a^m \rangle$.

B) Since G is finite cyclic of order n with generator a, we have $a^n = e$. Let $d = \gcd(k, n)$. Then we know $d = pk + qn$ for some integers p, q. It follows that

$$a^d = a^{pk+qn} = (a^k)^p \cdot (a^n)^q = (a^k)^p \cdot e^q = (a^k)^p$$

This shows that $a^d \subseteq \langle a^k \rangle$. Since $\langle a^k \rangle$ is a subgroup of G, it follows that $\langle a^d \rangle \subseteq \langle a^k \rangle$ because the other elements of $\langle a^d \rangle$ are the powers of a^d. To see the other inclusion, note that $d \mid k$. Hence $k = dm$ for some integer ℓ. Hence $a^k = a^{d\ell} = (a^d)^\ell \in \langle a^d \rangle$. Since $\langle a^d \rangle$ is a subgroup of G, it follows that $\langle a^k \rangle \subseteq \langle a^d \rangle$.

V. A)

$$\begin{aligned}[x]_{12} = [y]_{12} &\Leftrightarrow 12 \mid (x-y)\\ &\Rightarrow 3 \mid (x-y)\\ &\Rightarrow 9 \mid 3(x-y)\\ &\Rightarrow 9 \mid (3x-3y)\\ &\Rightarrow [3x]_9 = [3y]_9\end{aligned}$$

B) We have by the definition of addition in $\mathbf{Z}_{12}$ and $\mathbf{Z}_9$:

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

Hence ϕ is a group homomorphism.

C) The kernel of ϕ is the set of all elements of the domain mapping to the identity in the codomain:

$$\ker(\phi) = \{[x]_{12} \mid \phi([x]_{12}) = [0]_9\} = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$$

VI. A) $GL_2(\mathbf{R})$ is the group of invertible 2×2 matrices under *matrix multiplication.* We have

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

but

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

So $ab \neq ba$ and $b \notin C(a)$.

B) To show $C(a)$ is a subgroup of G, we must show that $C(a)$ is nonempty, and closed under products and inverses. First, $ae = ea = a$, so $e \in C(a)$ no matter what a is. Hence $C(a) \neq \emptyset$. If $x, y \in C(a)$, then by associativity of the operation in G, the product xy satisfies:

$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$$

Hence $xy \in C(a)$. Finally, let $x \in C(a)$. The equation $ax = xa$ implies that $x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1}$. But cancelling, this shows $x^{-1}a = ax^{-1}$. Hence $x^{-1} \in C(a)$ too.