Mathematics 243, section 1 – Algebraic Structures
Solutions for Exam 3 – December 1, 2006

I. In an RSA public key cryptosystem, the public key information is $m = 323$ and $e = 11$. Messages consisting of capital roman letters and blanks are encoded as 3-digit blocks $000, 001, \cdots, 026$ (with $A = 000$, $B = 001$, ... , $Z = 025$, and blank $= 026$) and encrypted as 3-digit blocks.

A) (15) How would the letters US be encrypted?

Solution: The encryption function is $f(x) = x^{11} \bmod 323$. We have $U = 020$ so U is encrypted as $20^{11} \bmod 323$. To compute this, we can use repeated squaring:

$20^2 = 400 \equiv 77 \bmod 323, 20^4 \equiv 77^2 = 5929 \equiv 115 \bmod 323, 20^8 \equiv 115^2 \equiv 305 \bmod 323.$

Then

$$20^{11} = 20^8 \cdot 20^2 \cdot 20 \equiv 305 \cdot 77 \cdot 20 \equiv 58 \bmod 323.$$

Similarly, $S = 018$, and $18^2 \equiv 1 \bmod 323$, so S is encrypted as

$$18^{11} \equiv 18 \bmod 323$$

So US is encrypted as $058, 018$.

B) (10) What is the (secret) decryption function g?

Solution: By the specifications for RSA systems, since $323 = 17 \cdot 19$, g is the function $g(x) = x^d \bmod 323$, where $11d \equiv 1 \bmod (17-1)(19-1) = 288$. We can carry out the Euclidean algorithm to find d:

$$288 = 26 \cdot 11 + 2$$
$$11 = 5 \cdot 2 + 1$$

(so $\gcd(11, 288) = 1$ and 11 has a multiplicative inverse mod 288). Then

	1	0
	0	1
26	1	−26
5	−5	131

So $(-5)(288) + (131)(11) = 1$, and the multiplicative inverse of 11 mod 288 is 131. Hence $d = 131$.

II. (20) Let

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

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. This is true because, first, if

$$A = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \quad \text{and} \quad A' = \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}$$

then

$$AA' = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba' + cb' & cc' \end{pmatrix}$$

This is also an element of H, so H is closed under products. Next, matrix multiplication is associative. The identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in H (take $a = c = 1$ and $b = 0$), so H has an identity element for matrix multiplication. Finally,

$$A = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \Rightarrow A^{-1} = \begin{pmatrix} 1/a & 0 \\ -b/(ac) & 1/c \end{pmatrix}$$

Since this is also in H every element in H has a multiplicative inverse in H. Therefore H is a group.

III. Let G be a group, let $a \in G$ be a fixed element, and consider the mapping $\ell_a : G \to G$ defined by $\ell_a(x) = ax$ for all $x \in G$.

A) (10) Show that ℓ_a is one-to-one and onto.

Solution: ℓ_a is one-to-one since if $x, y \in G$, then

$$\ell_a(x) = \ell_a(y) \Rightarrow ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow ex = ey \Rightarrow x = y.$$

ℓ_a is onto because if $y \in G$ is any element, then $\ell_a(x) = y$ when $x = a^{-1}y$:

$$\ell_a(a^{-1}y) = aa^{-1}y = y.$$

B) (5) What is the inverse mapping of ℓ_a?

Solution: The last part of the above shows that the inverse mapping of ℓ_a is $\ell_{a^{-1}} : G \to G$ defined by $\ell_{a^{-1}}(x) = a^{-1}x$.

IV.

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

Solution: Let H be a subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. So now assume that H contains some element other than e. Since every element of G has the form a^k for some integer k, by the Well-Ordering Property, let k be the smallest positive integer such that $a^k \in H$. We will show $H = \langle a^k \rangle$. The inclusion $H \supseteq \langle a^k \rangle$ is automatic since H is a subgroup of G and $a^k \in H$. For the other inclusion, let a^n be any element in H. Apply the division algorithm in $\mathbf{Z}$ to write $n = qk + r$ for some quotient $q \in \mathbf{Z}$ and remainder $r \in \mathbf{Z}$ with $0 \le r < k$. Then

$$a^n = a^{qk+r} = (a^k)^q a^r,$$

which implies

$$a^r = a^n (a^k)^{-q}$$

Since $a^n, a^k \in H$, the right-hand side is in H. Therefore a^r is also in H. But this is only possible if $r = 0$, since $r < k$ and k was the smallest positive integer such that $a^k \in H$. Hence $a^n = (a^k)^q \in \langle a^k \rangle$. Since every element in H is in $\langle a^k \rangle$, we have $H \subset \langle a^k \rangle$ also.

B) (10) $G = \mathbf{Z}_{30}$ is a group under the operation of addition mod 30. Find *all of* the generators of the cyclic subgroup $H = \langle [18] \rangle$.

Solution: Recall our theorem that in a cyclic group of order n with generator a, the subgroup $\langle a^k \rangle$ is the same as $\langle a^d \rangle$ where $d = \gcd(k, n)$. Here we can take $a = [1]$ and the operation is addition, so this says $\langle [x] \rangle = \langle [18] \rangle$ when $\gcd(x, 30) = \gcd(18, 30) = 6$. This gives $x = 6, 12, 18, 24$.

V. Let G, H be two groups.

A) (5) What is the definition of a group homomorphism from G to H?

Solution: A mapping $\varphi : G \to H$ is a group homomorphism if

$$\varphi(x *_G y) = \varphi(x) *_H \varphi(y)$$

for all $x, y \in G$.

B) (10) Let $G = \mathbf{Z}_{24}$ with operation addition mod 24. What is the kernel of the group homomorphism $\phi : G \to G$ defined by $\phi([x]) = [9x]$?

Solution: When φ is a general group homomorphism $\varphi : G \to H$,

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

Here $H = G$, and the additive identity element is $[0] \in \mathbf{Z}_{24}$. So $[9x] = [0]$ exactly when $9x \equiv 0 \bmod 24$. Since 9 is divisible by 3, this means x must be divisible by 8: $x = 0, 8, 16$.