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

Directions

Do all work in the blue exam booklet. There are 100 possible points.

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?

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

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. *Note: We discussed a general rule for finding the multiplicative inverse of a 2×2 matrix on a problem set earlier in the semester. If you don't remember it, you can "buy" it from me during the exam in return for a reduction of 5 points on your score for this problem.*

III.

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

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

B) (5) Find *all of* the generators of the cyclic subgroup $H = \langle [15] \rangle \subset \mathbf{Z}_{24}$.

C) (5) How many different subgroups does $\mathbf{Z}_{24}$ contain, including $\mathbf{Z}_{24}$ itself and $\{[0]\}$?

D) (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.

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 $a \in H$.

Extra Credit (10) A group G is generated by elements x, y satisfying $x^n = e$, $y^2 = e$, 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.

The General Pattern for 2×2 Matrix Inverses

If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then A has a inverse matrix (for multiplication) if and only if $\det(A) = ad - bc \neq 0$, and then

$$A^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$