Math 100A, Fall 2012, Midterm, 11/9/12

Instructions. Answer all questions.

1. (a) (5 points) Show that the remainder of $4^{121}$ when divided by 17 is 4.
(b) (10 points) Solve the following system of congruences:

$$x \equiv 3 \mod 5, x \equiv 4 \mod 7.$$ 

Solutions. (a) $4^{121} = (4^2)^{60} \cdot 4$, and $4^2 = 16 \equiv -1 \mod 17$. Thus $4^{121} \equiv (-1)^{60}4 = 4 \mod 17$.

(b) Note gcd(5, 7) = 1, so that there exists $m, n$ such that $5m + 7n = 1$. For example, we can take $m = 3, n = -2$ by inspection. Then to solve this system of equations, take $x = 4(5m) + 3(7n) = 60 - 42 = 18$. 

2. Let \( n \) be a positive integer, and let \( G \) be the set of all \( 2 \times 2 \) matrices

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]

where \( a, b, c, d \) are integers, \( ad - bc = 1 \), and \( c \equiv 0 \mod n \). The set \( G \) along with the operation of ordinary matrix multiplication is a group (you don’t need to show this).

(a) (5 points) Show that if a matrix \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) is in \( G \), then \( \gcd(a, n) = 1 \), so that \( [a]_n \in \mathbb{Z}_n^\times \).

(b) (7 points) Define \( \phi : G \to \mathbb{Z}_n^\times \) to be the map given by

\[
\phi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = [a]_n.
\]

Show that \( \phi \) is a group homomorphism.

(c) (8 points) Show that \( \phi \) is surjective.

**Solution.** (a) Since \( c \equiv 0 \mod n \), we must have \( c = qn \) for some \( q \). Thus since \( ad - bc = 1 \), we have \( ad - n(qb) = 1 \), which implies \( \gcd(a, n) = 1 \).

(b) We check

\[
\phi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \phi \left( \begin{pmatrix} aa' + bc' & ac' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \right) = [aa' + bc']_n.
\]

Since \( c' \equiv 0 \mod n \), this is

\[
[aa']_n = [a]_n[a']_n = \phi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \phi \left( \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right).
\]

(c) Suppose \( [a]_n \in \mathbb{Z}_n^\times \). Then \( \gcd(a, n) = 1 \), so there are integers \( d, b \) such that \( ad - bn = 1 \). So the matrix \( A := \begin{pmatrix} a & b \\ n & d \end{pmatrix} \) is in \( G \), and clearly \( \phi(A) = [a]_n \), proving surjectivity.
3. (10 points) Identify all subgroups of $\mathbb{Z}_{24}$.

*Solution.* The subgroups are $\mathbb{Z}_{24}$, $2\mathbb{Z}_{24}$, $3\mathbb{Z}_{24}$, $4\mathbb{Z}_{24}$, $6\mathbb{Z}_{24}$, $8\mathbb{Z}_{24}$, $12\mathbb{Z}_{24}$, and $\{0\}$. 
4. (10 points) Let $\sigma \in S_9$ be the permutation

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
3 & 5 & 8 & 2 & 4 & 1 & 9 & 6 & 7
\end{pmatrix}
\]

Express $\sigma$ as a disjoint product of cycles, and give the order of $\sigma$.

Solution. $\sigma = (1386)(254)(79)$. 