MAT 312 / AMS 351 final exam

August 16, 2012

Name:
SBU ID:

Please do not "show work"; write your work on the backs of the pages. It is not graded. Instead, after solving a problem, write the solution in the form of a series of concise sentences or computations. These should appear in a logical order rather than the order in which you thought of them. For example, to present the fact that the number $x = 4$ satisfies the equation $x + 3 = 7$, the following is not acceptable:

$$\begin{aligned} x + 3 &= 7 \\ x + 3 - 3 &= 7 - 3 \\ x &= 4 \end{aligned}$$

Instead, you would write something like:
If $x = 4$, then $x + 3 = 4 + 3 = 7$. Then this x solves the equation $x + 3 = 7$.

No cheating.

1. Use the Euclidean algorithm to:

   (a) find the greatest common divisor of 1000 and 105

   (b) find two integers s and t such that $1000s + 105t = 5$, and

   (c) list two integers that are inverses for 21 modulo 200.

2. Find an integer x such that

$$(\mathrm{mod}\, 1000)105x \equiv 10$$

3. Compute all of the powers of $[2]_{30} \in \mathbb{Z}_{30}$. Find an integer congruent to 2^{902} (using the modulus 30).

4. Find two integers y such that

$$y \equiv 0 \bmod 200$$
$$y \equiv 5 \bmod 21$$

5. Recall that for a positive integer n, the Euler function $\phi(n)$ is by definition the number of elements $[x]_n$ of $\mathbb{Z}_n$ that have multiplicative inverses (that is, those that satisfy $\gcd(x, n) = 1$). It can be computed in terms of the prime factorization for n by

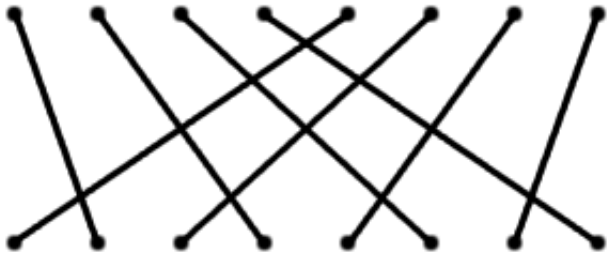
$$\phi({p_1}^{a_1}{p_2}^{a_2}...{p_k}^{a_k}) = (p^{a_1} - p^{a_1-1})(p^{a_2} - p^{a_2-1})...(p^{a_k} - p^{a_k-1})$$

   (a) Compute $\phi(21)$

   (b) List the elements of $\mathbb{Z}_{21}^*$ (the invertible classes).

   (c) Show that $[2]_{21}$ has order 6 in the group $\mathbb{Z}_{21}^*$

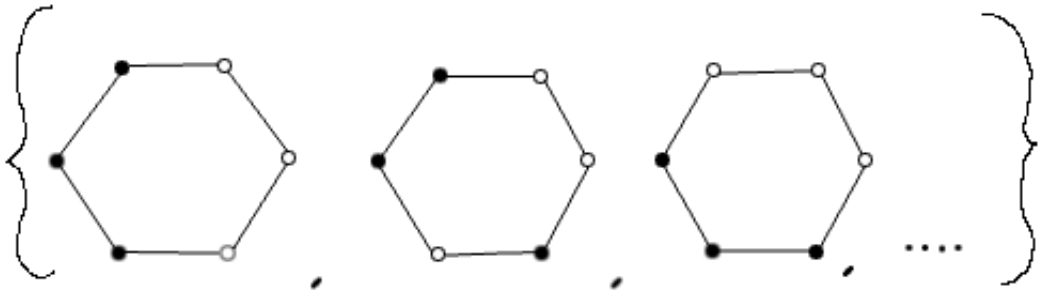
6. You shuffle an 8-card deck perfectly:



(a) Write this permutation $\sigma \in S_8$ in the cycle notation, as a product of disjoint cycles. How many times would you have to perform this exact shuffle to return to the original configuration?

(b) Suppose I switched cards 3 and 6 before you shuffle. What shuffle is accomplished after you do σ? Express your answer in cycle notation.

7. Let S be the set of ways of choosing 3 beads in a circle of 6 to be black, so S is:



Notice that S has $\binom{6}{3} = 20$ elements. The group $\mathbb{Z}_6$ acts on this set by rotating. How many distinct configurations of beads are there? That is, how many orbits are there for the action of $\mathbb{Z}_6$ on S? Draw a sample of each type of configuration (in addition to the two displayed above).

8. I encrypt an integer between 0 and 4 using your RSA public key with modulus 55 and exponent 27. You receive 18. What was my number? You may use the following facts:

$$18^1 = 18$$
$$18^2 = 324$$
$$18^3 = 5832$$
$$18^4 = 104976$$

9. Part of an infinite planar figure is shown. On the second diagram:

   - draw all lines of reflective symmetry with a dotted line
   - draw all lines of "only glide symmetry" (lines which are not also lines of reflective symmetry) with solid lines, with at least one darkened interval indicating the amount of the translation part
   - draw small circles at all points of rotational symmetry, labelled with an integer indicating the order of the rotation (for example, with 2 if 180°)
   - draw two vectors, somewhere near the bottom of the diagram, generating the translation symmetries