My NAME is:

Problem	1	2	3	4	5	Total
Score						

MAT 312
Applied Algebra
Midterm 2

November 2, 2010

No books or notes may be consulted during this test. You may use a programmable graphing calculator, but no "computer algebra" systems.
Explain your answers carefully.
Total score = 100.

1. (a) (15 points) Solve the congruence equation

$$40x \equiv 3 \mod 177$$

(b) (15 points) Find all solutions to the congruence equation

$$30x \equiv 9 \mod 177$$

2. Reminder: The Chinese Remainder algorithm for the solution of a system of congruences:

$$x \equiv a_1 \mod m_1, \quad x \equiv a_2 \mod m_2, \quad ..., \quad x \equiv a_n \mod m_n$$

where $m_1, m_2, \ldots, m_n$ are all relatively prime, is

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n,$$

where $M_i = m_1 \cdots \hat{m}_i \cdots m_n$ (i.e. m_i has been left out of the product), and y_i is the multiplicative inverse of M_i modulo m_i.

(a) (15 points) Solve:

$$x \equiv 1 \mod 6$$

$$x \equiv 2 \mod 7$$

$$x \equiv 3 \mod 5.$$

(b) (5 points) Adapt the algorithm to solve

$$2x \equiv 2 \mod 12$$

$$x \equiv 2 \mod 7$$

$$x \equiv 3 \mod 5$$

3. (a) (10 points) Explain why if a is not divisible by 2 or by 5, then $a^4 \equiv 1 \mod 10$.

   (b) (10 points) What are the last three digits of 377^{400}? Explain your work carefully!

4. Given the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 8 & 4 & 6 & 1 & 3 & 9 & 7 \end{pmatrix},$$

   (a) (10 points) calculate π^3 and π^{-1} (Use "matrix" or cycle notation, as you prefer).

   (b) (10 points) Write π as a product of disjoint cycles.

5. (10 points) Here is the mathematical center of the RSA algorithm: You know that $N = pq$ is the product of 2 large primes. A number x, which is smaller than p and smaller than q, has been encoded as $y = x^a \mod N$. You know $\varphi(N)$, and that $(a, \varphi(N)) = 1$. Explain carefully how you get $x \mod N$ back from y. Explain why the competition, even knowing N and a, cannot decode y.

END OF EXAMINATION