NAME (please print legibly): ______________________________________________________________
Your University ID Number: ______________________________________________________________

- Show all work and justify all answers. You MUST provide complete, clear responses for each problem, except when otherwise indicated. A correct answer without sufficient work may not receive full credit!
- Use of unauthorized electronic devices, books, or notes is strictly forbidden.
- Box all final numerical answers.
- You may appeal to any theorems, propositions, etc. covered at any point in the course, but please make clear what results you are using.
- In problems with multiple parts, you may use the results of previous parts in later parts, even if you did not solve the earlier parts correctly.
- You are responsible for checking that this exam has all 8 pages.

Pledge of Honesty
I affirm that I will not give or receive any unauthorized help on this exam, and that all work will be my own.

Signature: ______________________________________________________________

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>VALUE</th>
<th>SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>
1. (12 points) Let $a = 488$ and $b = 212$.

(a) Find the greatest common divisor $\gcd(a, b)$.

(b) Show that $a$ is a zero divisor modulo $b$ by finding an explicit nonzero element $\overline{s}$ such that $\overline{a} \cdot \overline{s} = \overline{0}$ modulo $b$.

(c) Find integers $x$ and $y$ such that $ax + by = \gcd(a, b)$. 
2. (15 points) Calculate the following things (no work or justification is required):

(a) Find the greatest common divisor of $2^3 \cdot 3^5 \cdot 5^4$ and $2^4 \cdot 3^3 \cdot 7$.

(b) Given that $669 \cdot 477 - 226 \cdot 1412 = 1$, find the multiplicative inverse of $477$ modulo $1412$.

(c) Find $\varphi(9000)$.

(d) Given that $2$ is a primitive root modulo $2027$ and $2027$ is prime, find the order of $8$ modulo $2027$.

(e) Given the prime factorizations $10^{10} - 1 = 3^2 \cdot 11 \cdot 41 \cdot 271 \cdot 9091$ and $10^{11} - 1 = 3^2 \cdot 21649 \cdot 513239$, find a prime $p$ such that the decimal expansion of $1/p$ has period $11$. 
3. (16 points) Solve the following problems (justify all answers and show all work):

(a) Solve the simultaneous congruences $x \equiv 11 \pmod{12}$ and $x \equiv 4 \pmod{11}$.

(b) Show that $2^{72} \equiv 4 \pmod{71}$.

(c) Show that $7^{108} \equiv 1 \pmod{81}$.

(d) Show that 2 is a primitive root modulo 11.
4. (8 points) The numbers $a_i$ are defined by the recursive relation $a_1 = 1$ and $a_n = 3a_{n-1} + 4$ for each $n \geq 2$. Prove that $a_n = 3^n - 2$ for every positive integer $n$.

5. (8 points) Show that $a^6 - a^2$ is divisible by 12 for every positive integer $a$. [Hint: Work mod 3 and mod 4 separately.]
6. (21 points) Decide whether each of the given statements is true or false, and explain (briefly) why in 1-2 sentences.

(a) The Caesar shift is the most secure cryptosystem ever designed.

(b) Rabin encryption is a completely secure cryptosystem because breaking it is equivalent to factorization.

(c) If $a^{200} \equiv 1 \pmod{m}$, then $a$ has order 200 modulo $m$. 
(d) If Alice sends Bob a message encrypted with Bob’s 5000-digit RSA modulus, nobody but Bob can possibly decode the message in a reasonable amount of time.

(e) There exists a way for Peggy to prove to Victor that she knows a secret without divulging any useful information about it.

(f) The only way to prove a 5000-digit integer is composite is to give an explicit factorization.

(g) The fastest way to find the factorization of $N$ is to test every possible number from 1 to $\sqrt{N}$ to see if it divides $N$. 
Blank page for scratch work.