MATH 348
Exam 2
April 3rd, 2013

Name: ____________________________
UIN: _____________________________

• There are 5 questions, worth 20 points each. Please complete all in the space provided.

• For questions with multiple parts, each part is worth an equal portion of the total value of the question unless otherwise indicated.

• No paper of your own is allowed. There is a scratch sheet at the end, and you may use the backs of the pages for extra space. You may also ask me for more paper if needed.

• No calculators or other resources are allowed.

• Write your solutions as clearly and neatly as you are able. The better able I am to follow what you are trying to do, the more likely you are to receive partial credit.

• Work carefully, and try to complete the problems you find easier before going back to the harder ones. Good luck!

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>VALUE</th>
<th>SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
1. (20 points)

(a) (5 pts.) A relation $\sim$ on a set $S$ is an equivalence relation if...

It is

1. Reflexive: $x \sim x \ \forall x \in S$
2. Symmetric: $x \sim y \Rightarrow y \sim x \ \forall x, y \in S$
3. Transitive: $x \sim y, y \sim z \Rightarrow x \sim z \ \forall x, y, z \in S$.

(b) (10 pts.) Consider the following relation $\sim$ on $\mathbb{R}$: $x \sim y$ if and only if $x = 2^ny$ for some integer $n$. Prove that $\sim$ is an equivalence relation.

1. Reflexive: $x = 2^0 \cdot x$ so $x \sim x \ \forall x \in \mathbb{R}$
2. Symmetric: If $x = 2^ny$ then $y = 2^{-n}x$, so $x \sim y \Rightarrow y \sim x$ for $x, y \in \mathbb{R}$
3. Transitive: If $x = 2^ny$ and $y = 2^nz$ then $x = 2^{n+m}z$, so $x \sim y, y \sim z \Rightarrow x \sim z$ for $x, y, z \in \mathbb{R}$.

(c) (5 pts.) For the equivalence relation given in part (b), describe the equivalence classes $\overline{0}$ and $\overline{1}$.

$\overline{0} = \{0^3\}$

$\overline{1} = \{1, 2, 4, 8, 16, 32, \ldots\}$
2. (20 points) Use the Euclidean Algorithm to find a solution to the Diophantine equation $588x + 231y = 63$. (You need not characterize all solutions, just find one.)

See Homework 8 Solutions.
3. (20 points)

(a) (5 pts.) State the **Chinese Remainder Theorem**.

If \( n_1, \ldots, n_r \) are pairwise relatively prime, then any system of congruences

\[
\begin{align*}
    x &\equiv a_1 \pmod{n_1} \\
    & \quad \vdots \\
    x &\equiv a_r \pmod{n_r}
\end{align*}
\]

has a solution \( x \). The solution is unique modulo \( \prod_{i=1}^{r} n_i \).

(b) (15 pts.) By the Chinese Remainder Theorem, the following system of congruences has a solution, unique modulo 84:

\[
\begin{align*}
    x &\equiv 1 \pmod{3}, \\
    x &\equiv 2 \pmod{4}, \\
    x &\equiv 6 \pmod{7}.
\end{align*}
\]

Solve this system of congruences, finding the smallest positive value of \( x \) which satisfies them. (You should use some systematic approach, such as the one used in class, to solve the problem, showing your work in an organized manner. Do not simply guess and check until you find a solution, as this will not receive full credit.)

\[
\begin{align*}
x &= 3n + 1 \\
3n + 1 &= 2 \pmod{4} \\
3(3n + 1) &= 1 \pmod{4} \\
n &= 3 \pmod{4} \\
n &= 4k + 3 \\
x &= 3(4k + 3) + 1 \\
&= 12k + 10.
\end{align*}
\]

\[
\begin{align*}
\Rightarrow & \quad k \equiv 9 \equiv 2 \pmod{7} \\
\Rightarrow & \quad k = 7l + 2 \\
\Rightarrow & \quad x = 12(7l + 2) + 10 \\
& \quad = 84l + 34. \\
\Rightarrow & \quad x \equiv 34 \pmod{84}.
\end{align*}
\]
4. (20 points)

(a) (5 pts.) State Fermat's Little Theorem.

If \( p \) is prime and \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \).

(b) (10 pts.) Using Fermat's Little Theorem, prove the following statement: If \( p \) is prime, then for any \( a \in \mathbb{Z} \), \( a^p \equiv a \pmod{p} \).

If \( p \nmid a \), then by the theorem, \( a^{p-1} \equiv 1 \pmod{p} \), and multiplying on both sides by \( a \), we get \( a^p \equiv a \pmod{p} \). On the other hand, if \( p \mid a \), then \( a \equiv 0 \pmod{p} \), and \( 0^p \equiv 0 \pmod{p} \), hence \( a^p \equiv a \pmod{p} \) again.
(c) (5 pts.) Using part (b), explain how one might prove that a number is not prime without actually finding a factorization of it.

The contrapositive form is: If $a^p \not\equiv a \pmod{p}$ for some $a \in \mathbb{Z}$, then $p$ is not prime. So if one can find a single integer $a$ such that $a^p \not\equiv a \pmod{p}$, then this proves that $p$ is not prime.
5. (20 points)

(a) Prove directly (i.e. using only algebra/arithmetic) that for any \( m \in \mathbb{N} \),

\[
m^3 = 6 \binom{m}{3} + 6 \binom{m}{2} + mn.
\]

\[
6 \binom{m}{3} + 6 \binom{m}{2} + m = \\
6 \frac{m!}{(m-3)!3!} + 6 \frac{m!}{(m-2)!2!} + m = \\
6 \frac{m(m-1)(m-2)}{3!} + 6 \frac{m(m-1)}{2!} + m = \\
m(m-2)(m-1) + 3(m)(m-1) + m = \\
m(m-1) \left[ m-2 + 3 \right] + m = \\
m(m-1)(m+1) + m = \\
m(m^2 - 1) + m = \\
m^3 - m + m = m^3.
\]

(b) Give a second proof of the above identity by showing that the two sides of the equation count the set of ordered triples of elements of \( \{1, \ldots, m\} \) in 2 different ways.

Clearly, the left hand side counts such triples.

The right hand side groups the triples by how many repeats they contain:

- All coordinates repeated: \((x,x,x)\) with \(x \in [m]\); \(m\) choices
- 2 coordinates repeated: \((x,x,y)\) or \((x,y,x)\) or \((y,x,x)\)
  - Choose \(x\), \(\binom{m}{1}\) and two positions \(\binom{3}{2}\), then choose \(y\), \(\binom{m-1}{1}\):
    \[
    \binom{m}{1} \binom{3}{2} \binom{m-1}{1} = m \cdot 3 \cdot (m-1) \\
    = 3 \cdot 2 \cdot \binom{m}{2} = 6 \binom{m}{2}.
    \]
- No coordinates repeated: \((x,y,z)\). Choose 3 coordinates \(\binom{m}{3}\) and one of the \(3!\) orderings of them: \(6 \binom{m}{3}\).