NAME: (print!) ______________________________

E-Mail address: ______________________________

MATH 356, Dr. Z., Exam II, Tue., Nov. 26, 2013, 10:20-11:40am, SEC-218

No Calculators! No Cheatsheets!

Write the final answer to each problem in the space provided. Incorrect answers (even due to minor errors) can receive at most one half partial credit, so please check and double-check your answers.

Do not write below this line (office use only)

1. (out of 8)
2. (out of 8)
3. (out of 8)
4. (out of 8)
5. (out of 8)
6. (out of 8)
7. (out of 8)
8. (out of 8)
9. (out of 9)
10. (out of 9)
11. (out of 9)
12. (out of 9)

________

tot.: (out of 100)
1. Using the formula (no credit for other methods!) to find the unique $x$ between 0 and 34 such that

a. $x \equiv 2 \pmod{5}, \ x \equiv 1 \pmod{7}.$

**Reminder:** The unique solution of the system $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ in $0 \leq x < m_1m_2$, when $m_1$ and $m_2$ are relatively prime

$$x \equiv a_1m_2[m_2^{-1}]_{m_1} + a_2m_1[m_1^{-1}]_{m_2} \pmod{m_1m_2}.$$  

(Note: you may find the modular inverse by trial-and-error rather than by the ‘official’ way, using the Extended Euclidean Algorithm.)

**Ans.:** $x =$  

2. (8 pts.) Using a suitable divisibility test, determine which of the following integers is divisible by 7
a. 115223601160511
b. 223421008707115

Ans.: a. 115223601 is/is not divisible by 7
b. 223421008707115 is/is not divisible by 7.
3. (8 pts.) Illustrate the proof of Wilson’s theorem for $p = 7$. 
4. (8 pts.) Use the Miller-Rabin primality test to investigate whether 10 is prime or composite by picking one random a between 2 and 8.
5. (8 pts.) Compute $\phi(9)$.  

a. Using the definition;  
b. Using the formula (in terms of the factorization into prime powers). Explain!

**Ans.:** $\phi(9) =$
6. (8 pts.) Suppose Alice used RSA to send you the encrypted message $c$, using the public key $e$ that you gave her. Check that this is an OK message (coprime to $n = pq$). Also check that the key is a valid key. If they are both OK, find her original message $m$.

$p = 7$, $q = 5$, $e = 11$, $c = 18$

Ans.: $m =$
7. (8 pts.) Prove that for every integer $n$

$$ n = \sum_{d|n} \phi(d) , $$

where $\phi(n)$ is Euler’s totient formula.
8. (8 pts.) Prove that if $p$ and $q$ are distinct odd primes, then $pq$ can \textbf{not} be a perfect number.

\textbf{Ans.:}
9. (9 pts.) Compute
\[ \sum_{n=1}^{8} \mu(n), \]
where \( \mu(n) \) is the Möbius function.

\[ \text{Ans.: } \sum_{n=1}^{8} \mu(n) = \]
10. (9 pts.) By ‘brute force’, find the set of quadratic residues, and the set of quadratic non-residues, for the prime \( p = 11 \).

\[
\begin{align*}
\text{Ans.}: \ & QR(11) = \\
& QNR(11) =
\end{align*}
\]
11. (9 pts. altogether) For the integer partition

\[ \lambda = (4, 4, 4, 3, 3, 2, 1, 1, 1) \]

(i) Draw the Ferrers graph (4 pts.)
(ii) Find the conjugate partition \( \lambda' \) (5 pts.)

\textbf{Ans.:} \( \lambda' = \)
12. (9 pts.)

i. Apply Glashier’s bijection (in the odd To distinct direction) to the odd partition \((5, 5, 5, 3, 3, 3, 1, 1, 1)\) to get a distinct partition, call it \(\lambda\)

ii. Apply Glashier’s bijection (in the distinct To odd direction) to the partition \(\lambda\) and show that you get \((5, 5, 5, 3, 3, 3, 1, 1, 1)\) back, as you should!

\textbf{Ans.}: \(\lambda = \)