Math 312, Section 101
Final Exam
December 5, 2008
Duration: 150 minutes

Please identify yourself **in ink** with name, student number and signature.

Name: _____ Student Number: _____ Signature: _____

Do not open this test until instructed to do so! This exam should have 10 pages, including this cover sheet. No textbooks, notes, calculators, or other aids are allowed. Turn off any cell phones, pagers, etc. that could make noise during the exam. You must remain in this room until you have finished the exam.

All your solutions must be written clearly and understandably. Always give an explanation for you final answer (unless explicitly stated otherwise). If you are unable to do a subproblem of a specific problem, you may still use the result later on for another subproblem. Use the backs of the pages if necessary. You might find some of the problems quite easy; try to solve these first. Good luck!

The following are the rules governing formal examinations:

1. Each candidate must be prepared to produce, upon request, a UBCcard for identification.
2. Candidates are not permitted to ask questions of the invigilators, except in cases of supposed errors or ambiguities in examination questions.
3. No candidate shall be permitted to enter the examination room after the expiration of one-half hour from the scheduled starting time, or to leave during the first half hour of the examination.
4. Candidates suspected of any of the following, or similar, dishonest practices shall be immediately dismissed from the examination and shall be liable to disciplinary action:
   - having at the place of writing any books, papers or memoranda, calculators, computers, sound or image players/recorders/transmitters (including telephones), or other memory aid devices, other than those authorized by the examiners;
   - speaking or communicating with other candidates; and
   - purposely exposing written papers to the view of other candidates or imaging devices. The plea of accident or forgetfulness shall not be received.
5. Candidates must not destroy or mutilate any examination material; must hand in all examination papers; and must not take any examination material from the examination room without permission of the invigilator.
6. Candidates must follow any additional examination rules or directions communicated by the instructor or invigilator.

Problem	Out of	Score
1	16	
2	22	
3	18	

Problem	Out of	Score
4	14	
5	14	
6	16	
Total	100	

1.**[16 pts]** For each of the following statements, indicate if it holds for every $a, b, c \in \mathbb{Z}_{>0}$ (if so, a simple 'true' without a proof suffices, if not, a 'false' together with a counterexample is expected).

(i) If $a|b+c$, then $a|b$ and $a|c$.
(ii) If a is even, then a is not a prime.
(iii) If a is odd, then $\phi(2a) = \phi(a)$.
(iv) If $4a \equiv 6 \pmod{10}$, then $a \equiv 4 \pmod{10}$.
(v) If $\gcd(a, b) = 1$, then $a^{b-1} \equiv 1 \pmod{b}$.
(vi) If $\gcd(a, b, c) = 1$, then $\phi(abc) = \phi(a)\phi(b)\phi(c)$.

2.

(a) **[16 pts]** For each of the following congruences, find the least nonnegative integer x that satisfies it.

(i)
$$\frac{60!}{31!} \equiv x \pmod{31}.$$

(ii)
$$\frac{59!}{30!} \equiv x \pmod{31}.$$

(iii)
$$x^2 \equiv 9 \pmod{5}.$$

(iv)
$$-9x \equiv 3^{162} \pmod{17}.$$

(b) **[6 pts]** Find the last three digits of the decimal expansion of 2009^{1202}.

3.

(a) **[6 pts]** Determine, using no moduli other than 111 in your final answer, all integers x that satisfy the following linear congruence.

$$21x \equiv 6 \pmod{111}.$$

(b) **[6 pts]** Find the least nonnegative integer x that satisfies the following system of linear congruences.

$$\begin{aligned} x &\equiv 998 \pmod{999} \\ x &\equiv 999 \pmod{1000} \\ x &\equiv 1000 \pmod{1001}. \end{aligned}$$

(c) **[6 pts]** Determine all integers x that satisfy the following system of linear congruences.

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 1 \pmod{10}. \end{aligned}$$

4.

(a) **[4 pts]** Let $b \in \mathbb{Z}_{>0}$. Explain what a pseudoprime to the base b is.

(b) **[6 pts]** Prove that $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number. (Hint: $1728 = 6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96$.)

(c) **[4 pts]** Show, without using the explicit prime factorization of 1729, but using the following congruences instead, that 1729 is composite.

$$\begin{aligned} 2^{18} &\equiv 1065 \pmod{1729} \\ 2^{36} &\equiv 1 \pmod{1729}. \end{aligned}$$

5. Alice wants Bob to send her a secret integer P between 0 and 1250 using RSA encryption with key $(e, n) = (1189, 1271)$ (so the exponent is 1189 and the modulus is 1271, it is way to small to be really secure, but basic RSA encryption and decryption methods still work of course).

(a) **[4 pts]** Bob knows that (the plaintext) $P = 101$, he computes the ciphertext $C = 35$ and communicates this number to Alice. Explain how Bob computed C.

(b) **[6 pts]** To obtain P from C, Alice first computes and inverse $d \in \mathbb{Z}$ of e modulo $\phi(n)$, since she created the key, she knows that $1271 = 31 \cdot 41$ (in fact, the prime factorization of n can easily be found since it is so small). Compute such a d.

(c) **[4 pts]** Explain what Alice has to do next to obtain P back.

6. The purpose of this problem is to prove the following theorem.

Theorem 1. *For all* $a, m \in \mathbb{Z}_{>0}$ *we have* $a^m \equiv a^{m-\phi(m)} \pmod{m}$.

Let $a, m \in \mathbb{Z}_{>0}$. For $m = 1$, the theorem holds trivially, so we assume from now on that $m > 1$ and write its prime-power factorization as $m = p_1^{e_1} \dots p_k^{e_k}$ for different primes $p_1, \dots, p_k$, exponents $e_1, \dots, e_k \in \mathbb{Z}_{>0}$ and some $k \in \mathbb{Z}_{>0}$. Let $i \in \{1, \dots, k\}$ and focus on the prime power $p_i^{e_i}$ in the prime-power factorization of m.

(a) **[4 pts]** Prove that if $p_i \nmid a$, then $p_i^{e_i} | a^{\phi(m)} - 1$. (Hint: Use Euler's theorem and prove/use that $\phi(p_i^{e_i}) | \phi(m)$.)

(b) **[4 pts]** Proof that if $p_i | a$, then $p_i^{e_i} | a^{m-\phi(m)}$. You might want to do this as follows.
- Prove that $p_i^{e_i - 1} | m - \phi(m)$.
- Prove that $m - \phi(m) \geq p_i^{e_i - 1}$.
- Prove that $p_i^{e_i} | p_i^{m-\phi(m)}$ (here you may use without proof that $p_i^{e_i - 1} \geq e_i$).

(c) **[4 pts]** Prove that $p_i^{e_i} | a^m - a^{m-\phi(m)}$. (Hint: combine the results of (a) and (b).)

(d) **[4 pts]** Complete the proof of Theorem 1 above.

3 extra pages to write solutions on