Math 223, Spring 2009
Final Exam — Solutions

Name: _____ Student ID: _____

Directions: Check that your test has 16 pages, including this one and the blank one on the bottom (which you can use as scratch paper or to continue writing out a solution if you run out room elsewhere). Please answer all questions and **show all your work**. **Write neatly: solutions deemed illegible will not be graded, so no credit will be given.** This exam is closed book, closed notes, and no calculators are allowed. You have 2.5 hours. Good luck!

1. (10 points) _____
2. (10 points) _____
3. (5 points) _____
4. (7 points) _____
5. (10 points) _____
6. (5 points) _____
7. (7 points) _____
8. (10 points) _____
9. (10 points) _____
10. (5 points) _____
11. (10 points) _____
12. (5 points) _____
13. (5 points) _____

Total (out of 99): _____

Total after the curve (out of 100): _____

Extra credit (out of 5.3): _____

Final course grade: _____ Final exam letter grade: _____

Before you start the exam, please indicate the following so that I can give you the appropriate amount of extra credit:

1. Did you give a talk in the student seminar this semester?

   Answer "yes" or "no" here: _____

2. How many student seminars have you attended this semester?

   Write the number here: _____

3. Did you attend the colloquium on matrices given by Alex Diesl from Bowling Green University?

   Answer "yes" or "no" here: _____

4. Did you attend the colloquium on combinatorics and tilings given by Bridget Tenner from DePaul University?

   Answer "yes" or "no" here: _____

5. Did you attend the colloquium on origami given by Mike Hill from University of Virginia?

   Answer "yes" or "no" here: _____

6. Did you attend the colloquium on Poincaré Conjecture given by Pascal Lambrechts from Louvain-la-Neuve University?

   Answer "yes" or "no" here: _____

7. Did you attend the colloquium on combinatorics and integration given by Mark Kayll from University of Montana?

   Answer "yes" or "no" here: _____

8. Did you attend the colloquium on complexity given by Joe Mileti from Dartmouth University?

   Answer "yes" or "no" here: _____

1. (2 pts each) Give precise definitions of the following. Please write in full sentences.

   (a) Order of a number modulo p

   Solution: See your class notes or textbook.

   (b) Sigma function.

   Solution: See your class notes or textbook.

   (c) Symmetric cipher

   Solution: See your class notes or textbook.

   (d) Monoalphabetic cipher

   Solution: See your class notes or textbook.

   (e) One-way function

   Solution: See your class notes or textbook.

2. (2 pts each) State the following theorems.

(a) Linear Equation Theorem

Solution: See your class notes or textbook.

(b) Fundamental Theorem of Arithmetic

Solution: See your class notes or textbook.

(c) Dirichlet's Theorem on Primes in Arithmetic Progression

Solution: See your class notes or textbook.

(d) Primitive Root Theorem

Solution: See your class notes or textbook.

(e) Euler Criterion

Solution: See your class notes or textbook.

3. (1 pt each) Identify each of the following statements as True, False, or Unknown. No explanation is necessary and no partial credit will be given.

(a) A contrapositive of an implication is logically equivalent to that implication.

Solution: True. (See your class notes.)

(b) The equation $x^5 + y^5 = z^5$ has infinitely many solutions with $x, y, z \in \mathbb{Z}$.

Solution: False. (Fermat's Last Theorem says this is impossible. We saw a movie about this.)

(c) A degree k polynomial has at most k solutions modulo prime p.

Solution: True. (Lagrange's Theorem.)

(d) A quadratic congruence always has a solution.

Solution: False. (Any example we've had of Legendre symbol being -1 means that a certain quadratic congruence does not have a solution.)

(e) RSA encryption is unbreakable.

Solution: False. (It is just practically irreversible.)

4. (7 pts) Let a, b, c be any integers. Show $gcd(a + cb, b) = gcd(a, b)$.

Solution: Let $G = gcd(a, b)$ and $g = gcd(a + cb, b)$. Note that $g|cb$ for any $c \in \mathbb{Z}$ since $g|b$. Also $g|(a + cb)$ and thus $g|(a + cb) - cb = a$. So g divides both a and b and hence $g \leq G$.

On the other hand, since $G|a$ and $G|b$, we also have $G|bc$ and thus $G|(a + bc)$. So $G \leq g$.

From the two inequalities it follows that $G = g$.

5. (5 pts each) Use Fermat's Little Theorem or Euler's Formula to do the following.

(a) Find a solution to the congruence $x^{38} \equiv 3\ (13)$.

Solution: By Fermat's Little Theorem, we have $x^{12} \equiv 1 \pmod{13}$. Thus

$$x^{38} = (x^{12})^3 x^2 \equiv x^2 \pmod{13},$$

so it suffices to solve $x^2 \equiv 3 \pmod{13}$. By inspection, we find that this equation has a solution $x = 4$ (or $x = 9$).

(b) Find the last digit of 3^{1000}.

Solution: This question is asking to reduce 3^{1000} modulo 10. Since $\phi(10) = 4$, by Euler's Formula we have

$$3^{1000} = (3^4)^{250} \equiv 1^{250} \pmod{10} \equiv 1 \pmod{10},$$

and so the last digit of 3^{1000} is 1.

6. (5 pts) Prove that there are infinitely many primes.

Solution: See class notes, textbook, or Midterm 2.

7. (7 pts) Let p be a prime and suppose b is the inverse of a modulo p. Prove that $e_p(a) = e_p(b)$.

Solution: This was a homework problem.

8. (5 pts each)

(a) Let p be an odd prime. Prove that there are $\frac{p-1}{2} - \phi(p-1)$ quadratic nonresidues of p that are not primitive roots of p.

Solution: This was a problem on final review.

(b) Prove that, if p is a Fermat prime, then every quadratic nonresidue of p is also a primitive root of p. (Recall that a Fermat prime has the form $2^{2^n} + 1$ for some $n \in \mathbb{N}$.)

Solution: This was a problem on final review.

9. (5 pts each)

(a) Let p be an odd prime and let $a, b \in \mathbb{Z}$ be inverses modulo p. Prove that if a is a quadratic residue modulo p, then so is b.

Solution: This was a homework problem.

(b) Determine whether 13 is a quadratic residue modulo 17.

Solution: Since $13 \equiv 1 \pmod 4$ (same for 17), we have by Quadratic Reciprocity

$$\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1.$$

Thus 13 is a quadratic residue modulo 17.

10. (5 pts) Encrypt HELLO using the Vigenère cipher with codeword HI. Use $A = 0, B = 1, \ldots, Z = 25$.

Solution: Ciphertext is $OMSTV$.

11. (10 pts) Describe how RSA encryption and decryption works. Make sure to clearly identify the public and private keys and write equations which produce ciphertext C and recover plaintext P. (If you want, you can use Alice and Bob as two parties exchanging RSA-encrypted messages.)

Solution: See your class notes.

12. (5 pts) Suppose A and B agree to use the prime 5 and its primitive root 2 for Diffie-Hellman key exchange. Suppose A then privately chooses 3 while B chooses 2. What is the key they will share?

Solution: The key is $4 \equiv (2^3)^2 \equiv (2^2)^3 \pmod 5$.

13. (5 pts) Write a short explanation of why one-time pad is an unbreakable cipher.

Solution: This was a homework problem.