Math 223, Spring 2009
Second Midterm Exam, April 23, 2009 — Solutions

Name: _____ Student ID: _____

Directions: Check that your test has 10 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 70 minutes. Good luck!

1. (6 points) _____
2. (6 points) _____
3. (5 points) _____
4. (7 points) _____
5. (7 points) _____
6. (8 points) _____
7. (10 points) _____
8. (7 points) _____

Total (out of 56): _____

Total after the curve (out of 100): _____

Exam letter grade: _____

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

   (a) Mersenne prime

   Solution: See lecture notes or textbook.

   (b) Perfect number

   Solution: See lecture notes or textbook.

   (c) Primitive root modulo prime p (either definition)

   Solution: See lecture notes or textbook.

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

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

   Solution: See lecture notes or textbook.

   (b) Euclid's Perfect Number Formula

   Solution: See lecture notes or textbook.

   (c) Primitive Root Theorem

   Solution: See lecture notes or textbook.

3. (5 pts) Prove that there are infinitely many primes.

Solution: See lecture notes or textbook.

4. (7 pts) Prove Order Divisibility Property.

   Solution: See lecture notes or textbook.

5. (7 pts) 9 monkeys store their bananas in 7 piles of equal size with the eighth pile of 3 left over. When they divide the bananas into 9 equal groups, 5 remain. What is a possible number of bananas they could have? Answers found by inspection will receive no credit.

Solution: This problem is asking for a solution to the system of congruences

$$x \equiv 3 \pmod 7$$
$$x \equiv 5 \pmod 9).$$

Since 7 and 9 are relatively prime, Chinese Remainder Theorem says that this system has a solution. From the first equation we have that

$$x = 7y + 3$$

for some $y \in \mathbb{Z}$. Plugging this into the second equation gives

$$7y + 3 \equiv 5 \pmod 9)$$

or

$$7y \equiv 2 \pmod 9).$$

By Linear Congruence Theorem, this equation has a single solution which is found by solving

$$7y + 9v = 2.$$

However, since $gcd(7, 9) = 1$, we first have to solve

$$7y + 9v = 1,$$

for which one can use Linear Equation Theorem, or observe that a solution is $(y, v) = (-5, 4)$. Then

$$y = 2 \cdot (-5) = -10$$

solves the congruence $7y \equiv 2 \pmod 9)$. Taking the least residue modulo 9 gives $y = 8$. Then

$$x = 7y + 3 = 7 \cdot 8 + 3 = 59$$

is a solution to the original system.

6. (4 pts each)

(a) How many primitive roots modulo 11 are there? Justify your answer. Answers found by inspection will receive no credit.

Solution: By Primitive Root Theorem, there are $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$ quadratic residues modulo 11.

(b) Given that 2 is a primitive root modulo 11, find all the other primitive roots modulo 11 (you do not need to reduce your answer mod 11). Answers found by inspection will receive no credit.

Note: This was essentially problem 7 on homework 8.

Solution: Recall that, given a primitive root g, g^k is also a primitive root mod p if $gcd(k, p-1) = 1$. Since 2 is a primitive root modulo 11 and since 3, 7, and 9 are relatively prime to 10, $2^3, 2^7$, and 2^9 are also primitive roots. From part (a), we know that there are 4 primitive roots, so we have found them all.

7. (10 pts) Let m be a positive integer such that $\phi(m) = 480$. Find a positive integer a such that

$$a \equiv 23^{482} \ (m).$$

Solution: We want to apply Euler's Formula, but to do this, we have to be sure that $gcd(23, m) = 1$. Since 23 is prime, showing $gcd(23, m) = 1$ is the same as showing that 23 does not divide m. Suppose it does. Then $m = 23^{\alpha}k$ for some $\alpha, k \in \mathbb{Z}$ with $gcd(23, k) = 1$, and

$$\phi(m) = \phi(23^{\alpha}k) = \phi(23^{\alpha})\phi(k) = (23^{\alpha} - 23^{\alpha-1})\phi(k) = 23^{\alpha-1} \cdot 22 \cdot \phi(k) = 480.$$

It then follows that 22 must divide 480, which is not true. Thus $gcd(23, m) = 1$.

So by Euler's Formula,

$$23^{\phi(m)} = 23^{480} \equiv 1 \pmod{m},$$

and so

$$23^{482} = 23^{480}23^2 \equiv 23^2 \pmod{m}.$$

The answer is therefore $a = 23^2 = 529$.

8. (7 pts) If p and q are odd primes, prove that pq cannot be a perfect number.

Note: This was essentially problem 8 on homework 7.

Solution: Suppose pq is a perfect number. This means that

$$2pq = \sigma(pq) = (p+1)(q+1) = pq + p + q + 1.$$

Rewritting this gives

$$p + q + 1 = pq.$$

Since p and q are odd, let $p = 2k+1$ and $q = 2l+1$ for some $k, l \in \mathbb{N}$. Then the above equation becomes

$$2k + 2l + 3 = (2k+1)(2l+1) = 4kl + 2k + 2l + 1$$

or

$$2kl = 1.$$

However, this is impossible since k and l are integers and we have a contradiction.