Math 223, Spring 2009
Midterm 2 Preparation

Your second midterm is on Thursday, April 23. It is a closed-note, closed-book, open-brain, no-calculator 70-minute examination held during the regular class time. It will cover the material covered since the first exam, up to and including Chapter 21 (so the exam will include primitive roots, but not quadratic reciprocity).

The exam will contain 6–7 questions, some with parts. You may be asked to recall some definitions or reproduce statements of theorems or proofs listed on this sheet. You might also see some problems that have already appeared in class, on homework assignments, or quizzes. Another portion of the exam will consist of problems you had not see before, i.e. you will have to solve new problems using techniques you already know. This portion will not comprise the bulk of the exam, and most (but not all) of the exam will have the format and difficulty level of an average homework problem.

A review session will take place on Wednesday, April 22, in class (this will be an extra Wednesday class). Please come prepared with questions. I will not prepare any materials for the review session beyond this document and will only answer your question during the hour.

What you need to commit to memory

(1) You must know the definitions of the following.

- (a) Euler's Phi Function
- (b) Mersenne prime
- (c) Perfect number
- (d) Sigma function
- (e) Primitive root modulo p (both definitions)
- (f) Order of a number modulo p

(2) You must know the statements of the following.

- (a) Fermat's Little Theorem
- (b) Euler's Formula
- (c) Chinese Remainder Theorem
- (d) Theorem on Primes in Arithmetic Progression
- (e) Prime Number Theorem
- (f) Euclid's Perfect Number Formula
- (g) Euler's Perfect Number Theorem
- (h) Euler's ϕ function Summation Formula
- (i) Order Divisibility Property
- (j) Primitive Root Theorem

(3) Proofs you must learn.

- (a) Proof of Chinese Remainder Theorem
- (b) Proof that there are infinitely many primes
- (c) Proof that there are infinitely many primes congruent to 3 mod 4
- (d) Proof of Euclid's Perfect Number Formula
- (e) Proof of the lemma stating that $x^k \equiv d \pmod{m}$ has a unique solution under some conditions
- (f) Proof of Order Divisibility Property

Topics you must study

(1) Euler's Formula
(2) Euler's Phi Function
(3) Mersenne primes and perfect numbers
(4) Powers modulo m and successive squaring
(5) Primitive roots and order

Computational problems you must be able to do

(1) Finding $\phi(m)$ using prime factorization of m and properties of ϕ
(2) Solving systems of congruences using Chinese Remainder Theorem
(3) Computing $\sigma(n)$
(4) Computing large powers modulo m using successive squaring
(5) Showing a number is not composite using successive squaring
(6) Solving $x^k \equiv d \pmod{m}$
(7) Finding order of a number modulo p
(8) Given a primitive root, finding all others from it

How to study for the exam

The exam will be friendly to those who have studied carefully and followed all the instructions on this sheet. Most of the test questions will look familiar. As mentioned above, you will be asked to repeat some definitions, state some theorems, and reproduce some proofs you have seen before. The exam will contain some exercises you have not seen before, but they will not comprise the bulk of the exam, and there will be no questions that only divine intervention will help you solve. You will do poorly if you fail to follow the advice on this preparation sheet.

(1) Read this worksheet thoroughly.
(2) Read and understand your class notes.
(3) Know how to do all the homework and quiz problems. The solutions are on our class conference.
(4) Go to office hours to ask questions.
(5) After you have done all of the above, start on the review questions below.

Review Problems (solutions will be provided later)

(1) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, three coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time evenly among the survivors. What was the least number of coins that could have been stolen?

(2) For $m, n \in \mathbb{N}$, if $gcd(m, n) = 1$, prove that $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

(3) For $m, n \in \mathbb{N}$, prove that $\phi(3n) = 3\phi(n)$ if $3|n$ and $\phi(3n) = 2\phi(n)$ if $3 \nmid n$.

(4) Use Euler's Formula to confirm that, for any $n \in \mathbb{N}$, $10^{32n+9} - 7$ is divisible by 51.

(5) Prove that the sequence 5, 12, 19, 26, ... contains no terms of the form 2^a or $2^a - 1$.

(6) Compute $\sigma(30)$ and $\sigma(2200)$.

(7) Let k be an integer greater than 1 and let $2^k - 3$ be prime. If $n = 2^{k-1}(2^k - 3)$, show that $\sigma(n) = 2n + 2$.

(8) If n is an integer greater than 2 and is the product of distinct Mersenne primes, prove that $\sigma(n) = 2^k$ for some $k \in \mathbb{Z}$.

(9) Use successive squaring to compute $7^{15} \pmod{17}$.

(10) (17.1) Solve the congruence $x^{329} \equiv 452 \pmod{1147}$. (Hint: 1147 is not prime.)

(11) How many primitive roots modulo 17 are there? Find one and then use it to find all others.

(12) Let p be a prime, $a \in \mathbb{Z}$, $a \geq 2$, and $gcd(a, p) = 1$. Suppose that $r, s \in \mathbb{N}$ with $a^r \equiv a^s \pmod{p}$. Prove or disprove: $r \equiv s \pmod{p-1}$. If the statement is false, determine t such that $r \equiv s \pmod{t}$ and prove your conjecture.

(13) Let g be a primitive root modulo an odd prime p. Prove that $-g$ is also a primitive root modulo p if $p \equiv 1 \pmod{4}$, but the order of $-g$ is $(p-1)/2$ if $p \equiv 3 \pmod{4}$.

(14) Find all solutions x modulo 29 of the equation $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{29}$. (Hint: Multiply both sides by a particular linear polynomial to simplify the left side. It may also be helpful to know that 2 is a primitive root mod 29.)