Math 261 — Fall 2001–2002
Midterm Quiz, November 20, 2001

Remarks: This exam booklet is also your answer sheet; **please answer question 0 on this page, and answer questions 1–7 inside the booklet.** (The questions are repeated on pages 1–7.) You may continue your solutions on the backs of pages and on the extra blank sheets at the end.

Each of questions 1–7 counts for 10 points. Make sure to communicate your ideas by explaining all of your steps clearly. Calculators are allowed, but none of the problems requires much computation.

Good luck!

Question 0. a) Your name: b) Your AUB ID#:

Question 1. Find the prime factorizations of 8536 and 7007, and use these to calculate $\varphi(7007)$ and the GCD $(8536, 7007)$.

Question 2. Calculate $\left(\frac{3}{11}\right)$ in two ways, first by Euler's criterion, and second by Gauss' Lemma (not by quadratic reciprocity).

Question 3. Find one solution to the equation $x^2 \equiv 5 \pmod{11^2}$. (You do not need to find the most general solution.)

Question 4. Show that every number a has a unique cube root x modulo 101.

(For example, the number 14 has the cube root 6, since $6^3 = 216 \equiv 14 \pmod{101}$. I am asking you to show both existence and uniqueness of the cube root for any a, not just for 14.)

Question 5. Using the Chinese Remainder Theorem, find one solution x to the equation $x^2 \equiv 1 \pmod{91}$ with $x \not\equiv \pm 1 \pmod{91}$. (Again, you do not need to find the most general x of this form. It may help you to notice that $91 = 7 \cdot 13$.)

Question 6. Let p be a prime dividing $10^{32} + 1$. Show that $p \equiv 1 \pmod{64}$. Hint: what is the order of 10 modulo p?

Question 7. In this question, p is a prime with $p \neq 2, 3$. Even if you cannot prove every part of this problem, you may assume the result of a previous part in all subsequent parts.

a) Show that $p \equiv \pm 1 \pmod{6}$.

b) Show that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.

c) Conclude that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{6}$.

d) Show that there exist infinitely many primes of the form $6k + 1$.