Math 261 — Fall 2001–2002
Final Exam, February 1, 2002

Remarks: This exam booklet is also your answer sheet; **please answer question 0 on this page, and answer questions 1–10 inside the booklet.** (The questions are repeated on pages 1–10.) You may continue your solutions on the backs of pages and on the extra blank sheets at the end.

This is a long exam; do as much of it as you can, and budget your time wisely. Each of questions 1–10 counts for 10 points. Make sure to communicate your ideas by explaining all of your steps clearly. Calculators **are** allowed.

Good luck!

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

Question 1. a) Find the prime factorization of $N = 93933$.
b) How many (positive) divisors does N have?
c) Show that N is not a sum of two squares.

Question 2. a) Use the Euclidean algorithm to find the multiplicative inverse of 7 modulo 33.
b) Find all solutions $(x, y) \in \mathbf{Z}/33\mathbf{Z} \times \mathbf{Z}/33\mathbf{Z}$ satisfying

$$\begin{cases} 7x + 5y \equiv 0 \pmod{33} \\ 11x + 7y \equiv 3 \pmod{33} \end{cases}.$$

Hint: use the first equation to eliminate x from the second equation.

Question 3. Factorize the Gaussian integer $420 + 240i$ into a product of powers of Gaussian primes (times a unit, if necessary).

Question 4. How many solutions (modulo 2201) are there to the equation $x^{14} \equiv 1 \pmod{2201}$?
Hint: $2201 = 31 \times 71$, where 31 and 71 are prime. Use the Chinese remainder theorem.

Question 5. a) Show that the quadratic form $x^2 + xy + 3y^2$ represents only positive integers.
b) Show that the quadratic form $x^2 - 61y^2$ does not represent 23, by working modulo 61.

Question 6. In this problem, $x, y \geq 1$. Feel free to find one or both of the solutions to each part by inspection.
a) Find two different solutions to the equation $x^2 - 5y^2 = -1$.
b) Find two different solutions to the equation $x^2 - 5y^2 = -4$.

Question 7. a) By trial and error, write each of 23 and 29 as a sum of four squares $a^2+b^2+c^2+d^2$, where $a, b, c, d \in \{0, 1, 2, 3, \ldots\}$.
b) Use your answer to part a) to write $667 = 23 \times 29$ as a sum of four squares.

Question 8. a) Calculate the number α defined by the eventually periodic continued fraction

$$\alpha = 2 + \frac{1}{6+}\,\frac{1}{1+}\,\frac{1}{6+}\,\frac{1}{1+}\,\frac{1}{6+}\,\frac{1}{1+}\cdots.$$

b) Write down the first few convergents A_n/B_n for α, until you reach a convergent for which you can prove that

$$\left|\frac{A_n}{B_n} - \alpha\right| \leq \frac{1}{1000}.$$

Question 9. a) Let p be any prime with $p \geq 5$. Show that the equation

$$(x^2 - 2)(x^2 - 3)(x^2 - 6) \equiv 0 \pmod{p}$$

has at least one solution.

b) Show that if furthermore $p \equiv 1 \pmod{24}$, then the above equation has six solutions modulo p.

Question 10. This exercise will lead you through another proof of the fact that if $p \equiv 1 \pmod{4}$, then p is a sum of two squares.

a) Let p be any prime number, and fix any $x \not\equiv 0 \pmod{p}$. Using the pigeonhole principle, show that there exist two different pairs of integers (m, n) and (m', n') satisfying

$$0 \leq m, n, m', n' < \sqrt{p}, \qquad \text{and } mx + n \equiv m'x + n' \pmod{p}.$$

Cultural note: Writing $a = m - m'$ and $b = n' - n$, the result of part a) implies that there exist integers a, b with $0 < |a|, |b| < \sqrt{p}$ and $ax \equiv b \pmod{p}$. This is called **Thue's lemma** and you can use it in part b) below.

b) In the case where $p \equiv 1 \pmod{4}$, we further choose x such that $x^2 \equiv -1 \pmod{p}$. Conclude that the a and b of Thue's lemma satisfy

$$a^2 + b^2 = p.$$

Hint: show first that $a^2 + b^2 \equiv 0 \pmod{p}$. Then look at the size of $a^2 + b^2$.