18.781 Final Exam: Monday, May 22, 1995

This is an “open-book” exam. You may use Davenport’s *Higher Arithmetic*, class notes and handouts, homework assignments, and a hand calculator if you wish.

Do all four problems. Explain your reasoning and show your calculations; I don’t expect you to just quote a table of class-numbers, for example.

1. Is $x^2 + 23x + 40$ divisible by 67 for some $x \in \mathbb{Z}$?

2. Assume that p is a prime larger than 3 such that $\frac{p-1}{2}$ is also prime. Show that that 5 is a primitive root mod p if and only if the last decimal digit of p is 3 or 7.

3. Let $d = 205$ and $\alpha = \frac{11+\sqrt{d}}{2}$.

(a) Show that α is a reduced quadratic integer of discriminant d.

(b) What is the continued fraction for α?

(c) What is the rational number $\frac{a}{b}$ with $a, b \in \mathbb{Z}, 0 < b \leq 150$, which best approximates α?

(d) List the reduced quadratic irrationals of discriminant d.

(e) What is the class-number $h(d)$? What is the strict class number $h_s(d)$? Explain briefly why.

(f) How many *equivalence* classes of primitive quadratic forms of discriminant d are there? Give representatives.

(g) Write down the fundamental unit for $A(d)$.

(h) Write down the smallest solution to $t^2 - du^2 = 4$ other than $(\pm 2, 0)$, and write down the smallest solution to $t^2 - du^2 = -4$ or explain why there are no solutions.

(i) The primitive quadratic form f corresponding to α is $f(x, y) = x^2 - 11xy - 11y^2$. Write down an automorphism of f (i.e., $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ such that $f \circ \gamma = f$) other than $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(j) What is the group-structure of the strict class group $\mathrm{Cl}_s(d)$?

4. Let $A = A(-39)$, the maximal order in the field $\mathbb{Q}(\sqrt{-39})$.

(a) Determine the set of reduced quadratic irrationals of discriminant -39. What is $h(-39)$? Is A a principal ideal domain? Write down a list of representatives of the ideal classes of A.

(b) What do you know about the splitting of rational primes p in A? Explain why the answer to the question “Is p split, ramified, or inert in A?” depends only upon the value of p modulo some number D. What is this this number? For example, what happens to 2? To 41?

(c) What is the group structure of the class group $\mathrm{Cl}(-39)$? Give the multiplication table in terms of the representatives you wrote down in **(a)**.