SWARTHMORE COLLEGE
Department of Mathematics and Statistics
Honors Examination

Honors Exam
May, 1998

Number Theory and Modern Algebra II

INSTRUCTIONS: Try to do all six problems on this exam.

Part I

1.) (a) Denote the greatest common divisor of two integers x and y by (x, y).
(i) Show that if $(a, b) = 1$ and c divides $a + b$, then $(a, c) = (b, c) = 1$.
(ii) If $(a, b) = 1$, prove that $(a + b, a - b) = 1$ or 2.
(iii) Show that if $(b, c) = 1$ and m divides b, then $(m, c) = 1$.

(b) Prove that $2^{37} - 1$ is a multiple of 223.

2.) (a) Show that the equation $x^2 - 4y^2 = 10$ has no integer solutions.
(b) Find all solutions to the equation $x^2 + x + 7 \equiv 0 \pmod{81}$.
(c) Show that $n^3 + 11n + 1$ is not divisible by the first four primes for any integer n.
(d) Prove that no integer of the form $8k + 7$ is a sum of three squares.

3.) (a) For which primes p is the congruence $x^4 \equiv -1 \pmod{p}$ solvable?

(b) Using quadratic reciprocity, describe the odd prime divisors of

(i) $n^2 + 1$;

(ii) $n^2 + 2$;

(iii) $n^2 + 3$

4.) (a) If g is a primitive root mod p and d divides $p-1$, show that $g^{(p-1)/d}$ has order d. Also, show that a is a d-th power iff $a \equiv g^{kd} \pmod{p}$ for some integer k.

(b) Show that if a has order 3 modulo p, then $1+a$ has order 6.

(c) Let p and q be distinct primes such that $p-1$ divides $q-1$. If n and pq are relatively prime, show that $n^{q-1} \equiv 1 \pmod{pq}$.

(d) How many solutions are there to the equation $x^2 \equiv 1 \pmod{n}$ if

(i) n is prime?

(ii) n is the product of two distinct primes?

(iii) n is the product of three distinct primes?

Part II

1.) Let $\zeta = e^{2\pi i/7}$ and let $\mathbf{Q}$ denotes the rational numbers. If $E = \mathbf{Q}(\zeta)$ is the field extension of $\mathbf{Q}$ generated by ζ,

(a) Show that E is a Galois extension of $\mathbf{Q}$ whose Galois group is cyclic of order 6.

(b) Show that E has a unique subfield K which is of degree 2 over $\mathbf{Q}$.

(c) Let $\tau = \zeta + \zeta^2 + \zeta^4$. Show that $K = \mathbf{Q}(\tau)$.

(d) It is known that every quadratic extension of $\mathbf{Q}$ has the form $\mathbf{Q}(\sqrt{d})$, where d is a square free integer. Determine a d so that $K = \mathbf{Q}(\sqrt{d})$.

2.) (a) Let R be a ring . Show that if R is a principal ideal domain, then every non - zero prime ideal of R is maximal.

(b) Let

$$S = Z[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in Z\}$$

where Z denotes the integers.

(i) Prove that if I is a non -zero ideal of S , then the quotient ring S/I has only finitely many elements.

(ii) Hence, (or otherwise) show that every non - zero prime ideal of S is maximal.

(iii) Let

$$J = \{2\alpha + (1 + \sqrt{-5})\beta : \alpha, \beta \in S\}$$

so that J is the ideal of S generated by 2 and $1 + \sqrt{-5}$. Show that J is not principal.