Name: **Student ID:**

Sample Final Exam Questions (mandatory part)

The actual final exam will have a mandatory and an optional section. The optional questions will be similar to the ones on the previous (sample) tests, and need to be answered only if you do not want me to re-use your average test score. The questions below are supposed to help you prepare for the mandatory part of the final. You will have 120-150 minutes to answer them, without using your notes or communicating with other students. You will have to give the simplest possible answer and show all your work.

1. Prove that there exists a primitive root for a prime p. (5000-level students: prove that the nonzero elements in a finite field form a cyclic group with respect to multiplication.)

2. Using the fact that there is a primitive root for an odd prime p, prove that there is a primitive root for p^2.

3. Assume r is a primitive root for p^2 where p is an odd prime. Prove, by induction on k, that r is also a primitive root for all p^k.

4. The positive integer n has a primitive root. What can you say about the prime factors of n? Prove the necessity of your conditions.

5. Using the fact that 3 is a primitive root for 17, and the table of indices provided on page 167 of our textbook, solve the congruence $5x^4 \equiv 3 \pmod{17}$.

6. Solve the quadratic congruence $3x^2 - x + 1 \equiv 0 \pmod{47}$, or give a reason why no solution exists.

7. State and prove Euler's criterion for a number being a quadratic residue of a prime p. Use the criterion to give a formula for the Legendre symbol $(-1/p)$.

8. Prove that the Legendre symbol satisfies $(ab/p) = (a/p)(b/p)$.

9. Prove that there are infinitely any primes of the form $4k + 1$.

10. State and prove Gauss' lemma.

11. Using Gauss' lemma prove that

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

12. Using Gauss lemma prove that

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}$$

For any odd prime p and odd integer a that is relative prime to p.

13. Using the previous statement state and prove that quadratic reciprocity law.

14. Using quadratic reciprocity, find a formula for the Legendre symbol $(3/p)$.

15. Evaluate the Legendre symbol $(1321/2357)$.

16. Name the reason why it is sufficient to know how to solve quadratic congruences for prime power moduli. As an illustration, solve the congruence $x^2 \equiv 39 \pmod{50}$.

Good luck. Gábor Hetyei