Name: **Student ID:**

Sample "Test III"

The actual test will have at most 9 questions and perhaps one bonus question. You will have 120-180 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.
2. Using the fact that 3 is a primitive root for 17, and the table of indices provided on page 177 of our textbook, solve the congruence $5x^4 \equiv 3 \pmod{17}$.
3. Solve the quadratic congruence $3x^2 - x + 1 \equiv 0 \pmod{47}$, or give a reason why no solution exists.
4. 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 $(-1/p)$.
5. Prove that the Legendre symbol satisfies $(ab/p) = (a/p)(b/p)$.
6. Prove that there are infinitely any primes of the form $4k + 1$.
7. State and prove Gauss' lemma.
8. Using Gauss' lemma prove that
$$(2/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ (mod 8),} \\ -1 & \text{if } p \equiv \pm 3 \text{ (mod 8.)} \end{cases}$$
9. 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.
10. Using the previous statement state and prove that quadratic reciprocity law.
11. Using quadratic reciprocity, find a formula for the Legendre symbol $(3/p)$.
12. Evaluate the Legendre symbol $(1321/2357)$.
13. Solve the quadratic congruence $x^2 \equiv 2 \pmod{17^3}$.
14. Prove that for an odd prime p and an odd integer a that is relative prime to p, the congruence $x^2 \equiv a \pmod{p^n}$ has a solution if and only of a is a quadratic residue of p. You may use your solution to the previous question as an illustration to your proof.
15. Explain how the previous statement and its proof needs to be modified if $p = 2$.

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 $x^2 \equiv 39 \pmod{50}$.
17. If $a^k - 1$ is prime, what can you say about a and k? Prove your claim. What is the name of the primes of this form?
18. Prove that for every prime p such that $2^p - 1$ is a prime, the number $2^{p-1}(2^p - 1)$ is perfect.
19. Which primes may be written as a sum of two squares? Prove your claim.
20. Give a formula for all Pythagorean triples (a, b, c) satisfying $\gcd(a, b, c) = 1$. Sketch the proof of the fact that your formula covers all solutions.
21. Prove that for a primitive Pythagorean triple (a, b, c), one of a and b must be even, while the other one is odd.
22. Assume that the product of a and b is the n-th power of an integer and that $\gcd(a, b) = 1$. Prove that either of a and b is the n-th power of some integer.
23. Find all primitive Pythagorean triples (a, b, c) satisfying $a + b \leq 11$.

Good luck. Gábor Hetyei