Sample Test 1

The real test will have less questions and you will have about 75 minutes to answer them. The usage of books or notes, or communicating with other students will not be allowed. You will have to give the simplest possible answer and show all your work. The questions below are sample questions related to stating and proving theorems. Besides trying to answer these questions, make sure you also review all homework exercises. The test may also have questions similar to those exercises. During the test, the usage of books or notes, or communicating with other students will not be allowed.

1. State the well-ordering axiom.
2. Prove by induction that $1 + 3 + \cdots + (2n - 1) = n^2$ holds for all $n \geq 1$.
3. The sequence $a_0, a_1, a_2, \ldots$ is given by the initial conditions $a_0 = 2$ and $a_1 = 5$, and by the recurrence $a_{n+2} = 3a_{n+1} - 2a_n$. Prove by induction that $a_n = 3 \cdot 2^n - 1$ holds for all $n \geq 0$.
4. Define the quotient and the remainder arising when the positive integer a is divided by the positive integer b. (Write down the defining equation, and state the properties of the quotient and the remainder.)
5. Prove that for every positive integer a and every positive integer b there is a quotient q and a remainder r satisfying $a = qb + r$ and $0 \leq r < b$.
6. Prove the uniqueness of the quotient and the remainder.
7. Prove that the relation "divides" is a partial order on the set of positive integers, that is, it is reflexive, antisymmetric and transitive. (Antisymmetry means that "a divides b and b divides a" imply $a = b$.)
8. Is the relation "a divides b and b divides a" an equivalence relation on integers? How about the same relation on positive integers? Justify your answer!
9. Define the greatest common divisor of two integers a and b and prove that every other common divisor divides the greatest common divisor.
10. Use Euclid's algorithm to find the greatest common divisor d of 68 and 89, and to express d as an integer linear combination $u \cdot 68 + v \cdot 89$ of 68 and 89. *You will not get any credit if you find your answers by any other means!*
11. Describe Euclid's algorithm and explain how it may be used to find the greatest common divisor.
12. Prove that the greatest common divisor of two integers a and b may be written as an integer linear combination of a and b.
13. Define primes and show that they satisfy the property stated in Euclid's lemma.

14. Let p be an integer with the following property: if p divides ab then it also divides at least one of a and b. Prove that p is a prime.

15. Explain how Euclid's lemma may be used to prove the uniqueness of prime factorization.

16. Prove that every integer may be written as a product of primes.

17. Let $n > 1$ be a positive integer. Define congruence modulo n and prove it is an equivalence relation.

18. Prove that congruence is compatible with addition and multiplication.

19. Prove that $\mathbb{Z}_n$ has exactly n elements.

20. For which values of $n > 1$ is it true that $a \cdot b \equiv 0 \pmod{n}$ implies $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$? Justify your answer!

21. Prove that addition and multiplication of congruence classes is associative and commutative in $\mathbb{Z}_n$.

22. Assume p is a prime and a is not a multiple of p. Prove that the congruence $ax \equiv 1 \pmod{p}$ has a solution.

Good luck. Gábor Hetyei