CAS705 Test 4 Fall 2008

Name ________________________ Student No. ________________________

No aids allowed. Answer all questions on test paper. Use backs of sheets for scratch work.

Total Marks 10.

1. Let $a, b, x, y \in \mathbb{Z}$ and such that $ax + by = 1$. Show that $\gcd(a, b) = 1$.
2. Suppose that $g^a \equiv 1 \pmod{m}$ and $g^b \equiv 1 \pmod{m}$. Prove that $g^{\gcd(a,b)} \equiv 1 \pmod{m}$.
3. Suppose that p is a prime; show that $\mathbb{Z}_p^*$ equals $\{1, 2, \ldots, p-1\}$ and is a group.
4. State and prove Lagrange's theorem; deduce Euler's theorem from it.