MATH 5645

TOPICS IN NUMBER THEORY. 2014

Assignment 1. Due Week 3.

Marks will be deducted for poor and illogical setting out or for solutions that are unnecessarily complicated or obscure.

1a. Prove Theorem 1.1 in the notes.

b. Show that if p is a prime of the form $6k-1$, then $x^3 \equiv a \bmod p$ has a unique solution for every integer a.

2. Suppose q and $p = 2q+1$ are both prime, with $q > 2$. Prove that $2q$ is the only element in $\mathbb{Z}_p$ which is a quadratic non-residue, but not a primitive root. Hence find all the primitive roots in $\mathbb{Z}_{23}$.

3a. Show that for any positive integer n, the number $4n+2$ is the sum of three squares, exactly two of which are odd.

b. Deduce that every odd positive integer can be expressed in the form $a^2 + b^2 + 2c^2$.