MATH 406 – HOMEWORK VIII

(due Friday 17 April 2009)

1. Assume that $ord_n a = k$ and that $d|k$. Show that there is some b with $ord_n b = d$.

2. Suppose that $\bar{r}$ is an inverse of r modulo n. Show that $ord_n r = ord_n \bar{r}$.

3. Show that 20 has no primitive roots.

4. Find all primitive roots of 18. Explain carefully, and express your answers as least positive residues. Show all necessary calculations – you do not need a calculator.

5. How many incongruent roots does $x^3 + 12$ have modulo 13? Explain carefully.

NOTE: Explain your work clearly. Your solutions must include enough detail to justify your conclusions.