INTRODUCTION TO HIGHER MATHEMATICS V2000

Homework, week 8, due November 3

1. Divisibility in the integers: Dumas-McCarthy, Exercises 7.1, 7.3, 7.2, 7.6, 7.7, 7.8, 7.14.

2. Let p be an odd prime number. Let $a \in \mathbb{Z}$ be an integer not divisible by a.

(i) Show that the residue class $[a]$ of a in $\mathbb{Z}_p$ satisfies either

$$(*)\ [a]^{\frac{p-1}{2}} = [1]$$

or

$$(**)\ [a]^{\frac{p-1}{2}} = [-1] = [p-1].$$

(ii) There are $p-1$ residue classes in $\mathbb{Z}_p$ not equal to $[0]$. How many of them satisfy equation (*)? How many satisfy equation (**)?

(Hint: If you don't know the answer, you can check $p = 3$, $p = 5$, $p = 7$, and formulate a guess for the general case based on what you observe. Then you can try to prove your guess.)

3. Daepp-Gorkin, Problems 28.3, 28.4.