MATH 340 Assignment 2, Fall 2010

Michael Monagan

This assignment is to be handed in by 11:20 am Friday October 1st in the MATH 340 drop off box (box #10). Late penalty: -20% for up to 24 hours late. Zero for more than 24 hours late.

Section 1.3 The Euclidean Algorithm

Program the extended Euclidean algorithm (Theorem 1.3.6 on page 16) in Maple. For each step $i \geq 2$, after you compute the values q_i, r_i, x_i, and y_i, print them on one line so that you get a table of values like the table in Example 1.3.7 on page 16.

Execute your program on the input $a = 710, b = 68$ (Example 1.3.7) to verify that it is correct. Now execute your program on the input $a = 1023$ and $b = 601$ and identify the inverse of 601 in $\mathbb{Z}_{1023}$. Hand in a printout of a Maple worksheet showing your program and the output for both inputs.

Reference: See the Loops section in the MapleNotes worksheet on the course webpage.

Section 1.4: Prime Numbers

Exercises 3, 4, 9.

For exercise 9 use the Maple command `isprime` command. For the prime p that you find, factor the integer $n = 2^p - 1$ using the `ifactor` command.

Section 1.5: Relations and Partitions

Exercises 1, 5, 9.

Section 1.6: Modular Arithmetic

Exercises 11, 12. Also prove Theorem 1.6.6 parts 3, 5, and 6.

Section 1.7: Equations in $\mathbb{Z}_n$

Exercises 3, 5, 6, 10, 11, 12.

For problem 5, apply the extended Euclidean algorithm by hand to calculate the inverse for practice.