Matt Drummond
Final Project
ECE 645

Montgomery Multiplication

Timing Analysis: Arch1

I. Clock Cycle Count:

Assume that cycles taken to load values of M and Y into RAMs are ignored.
Assume 1024 bit parameters, 16 bit words, with 65 PEs, as discussed in Huang paper.
This means we will need 16 cycles for a PE to complete.
Total count:
NumPEs + CCsPerPE = 56 + 16 = 7**2 CCs per multiplication**

II. Time Between Operations:

This time consists of the number of CCs for a single operation plus the number of CCs for loading next set. Currently, the prep time would be 64 CCs for loading the new operands into the RAMs, yielding: **77 + 64 = 141 CCs between operations**

Note: If Y and M RAMs were made to be dual port RAMs this time between operations could be reduced. After the first CC of the multiplication operation the next set of operands could begin loading into the RAMs from address 0 on. This would eliminate the 64 CC addition.

III. Throughput:

Throughput will be equal to the time between operations, in CCs, times T_{clk}.
= **NUM_CCs * T_{clk}**

IV. Confimations:

The Clock Cycle Count and Time Between Operations (in CCs) were both verified using simulation. Simulation otuput from the Monty_Arch1_tb testbench was sufficient to ensure the values were correct.