ECSE 325 Lab 3: Register Transfer Level Design of a Pipelined Modular Exponentiator Digital Circuit

Cédric Barré (260792994)
Andy Li (260832377)
Yuankang Wei (260787802)

g40_modulo33401_pipelined

The g40_modulo33401_pipelined digital circuit was designed to calculate the modulo 33401 of any 32-bit input by passing it through a pipeline and returning the result as a 16-bit output. To do so, it uses properties of the modulo function to avoid having to operate on extremely large numbers. In the end, the circuit implements the modulo as the following equations:

$$A \, mod \, 33401 = A - (floor(A/33401) * 33401)$$
$$floor(A/33401) = (A * 32147) > 30$$

Here, *A* is the 32-bit input and the 16-bit output corresponds to the *A mod 33401* signal. Moreover, we have an extra 17-bit output that corresponds to the *floor(A/33401)* signal. The *floor(A/33401)* signal is calculated by approximating the division through a multiplication with a constant and a 30-bit shift to the right. This is an approximation of the division which automatically rounds down the result of the division calculation.

To accomodate pipelining, the *g40_modulo33401_pipelined* circuit has been split into a number of stages with the help of registers that update every clock cycle. The block diagram for this new circuit is available below. The *g40_mod_exp_revised* circuit which acts as a wrapper for the *g40_modulo33401_pipelined* has also been adapted to pipelining by handling the latency of the *g40_modulo33401_pipelined* circuit and returning the result of the calculation at the right time.

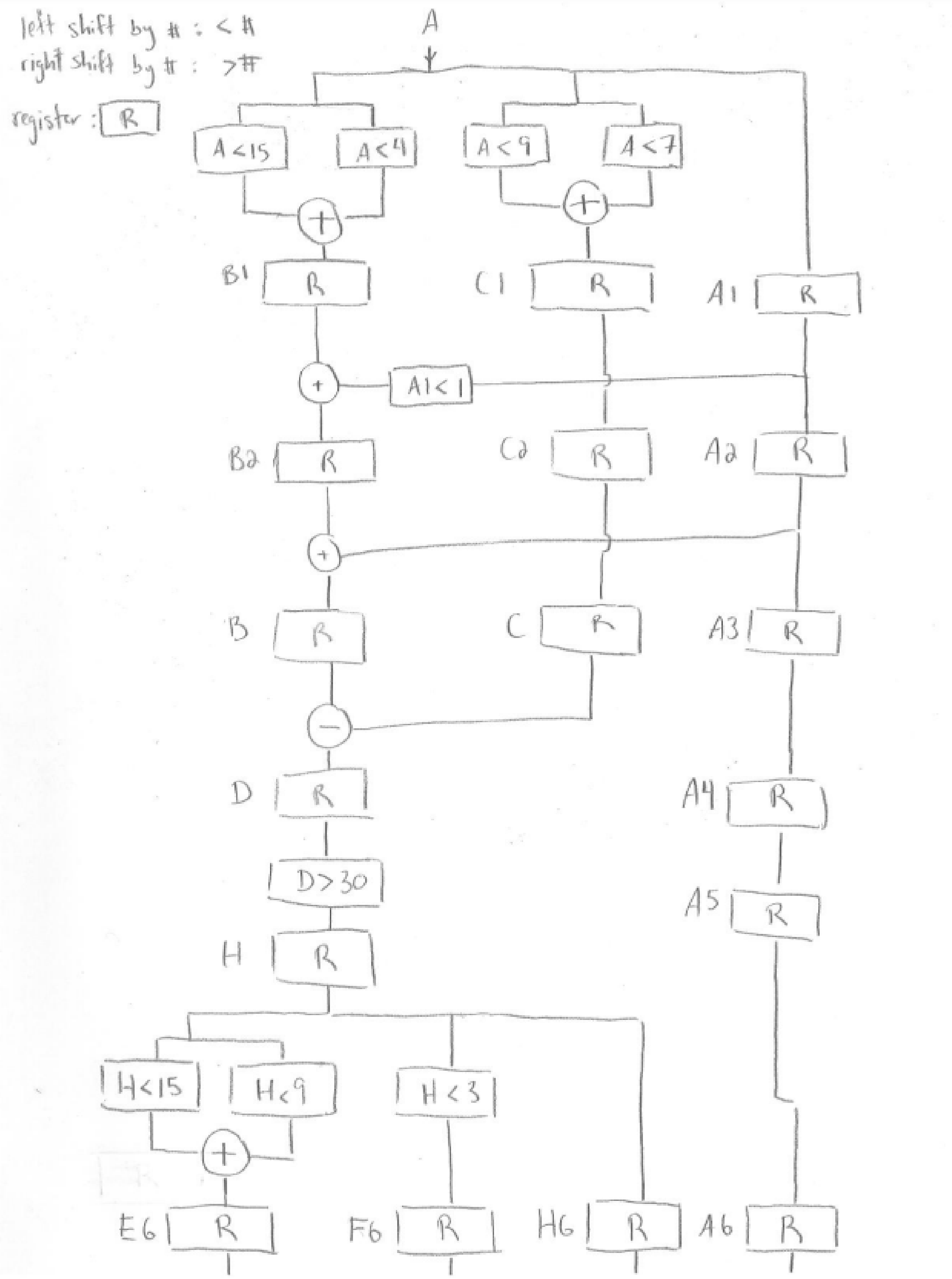
Table 1: *g40_modulo33401_pipelined* Inputs

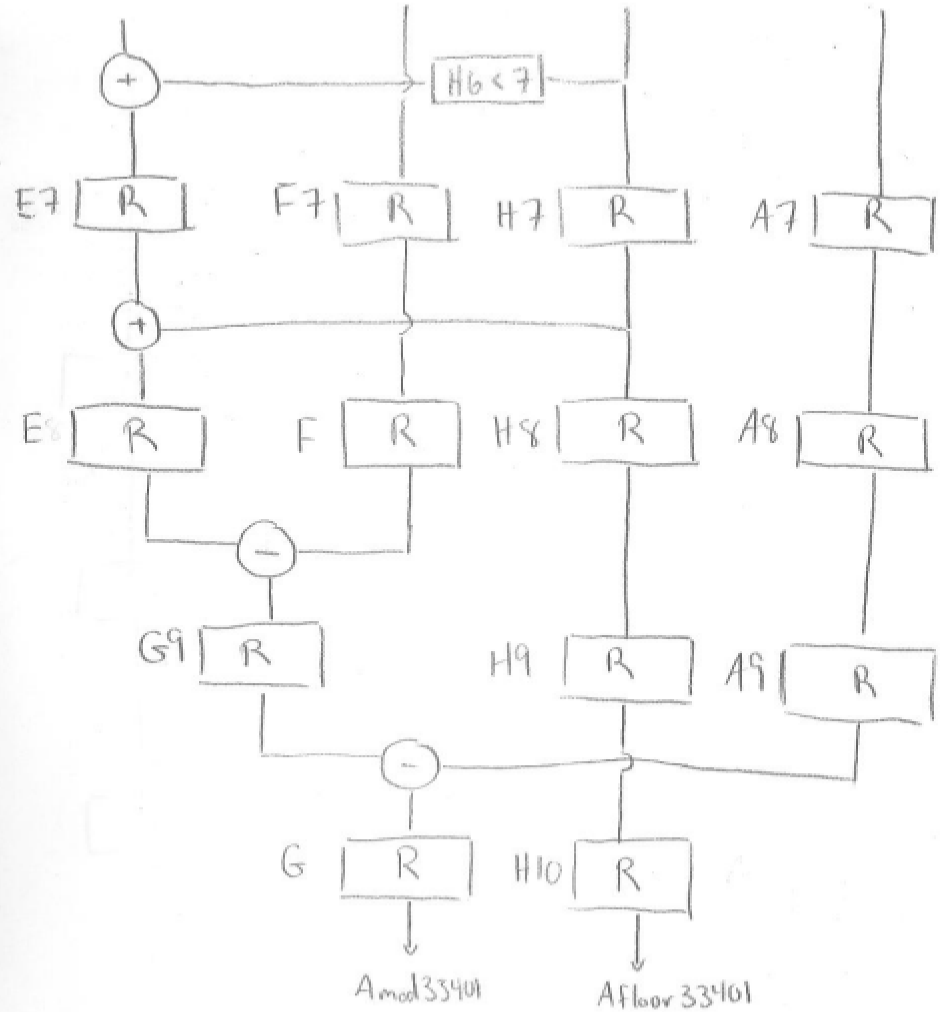
Name	Size	Description
A	32 bits	Operand onto which we apply the modulo 33401 operation.
clk	1 bit	Clock signal which drives the circuit. The circuit is driven by the rising edge of the clock.

Table 2: *g40_modulo33401_pipelined* Outputs

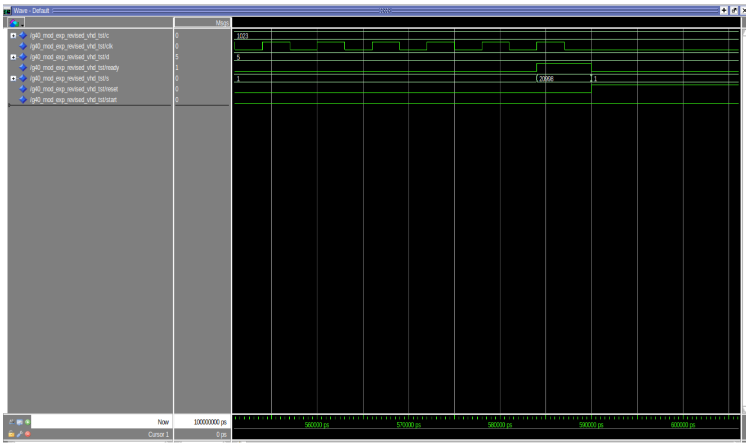
Name	Size	Description
Amod33401	16 bits	Signal representing the output of the calculation.
Afloor33401	17 bits	Signal representing the quotient of the input divided by 33401.

g40_modulo33401_pipelined Block Diagram



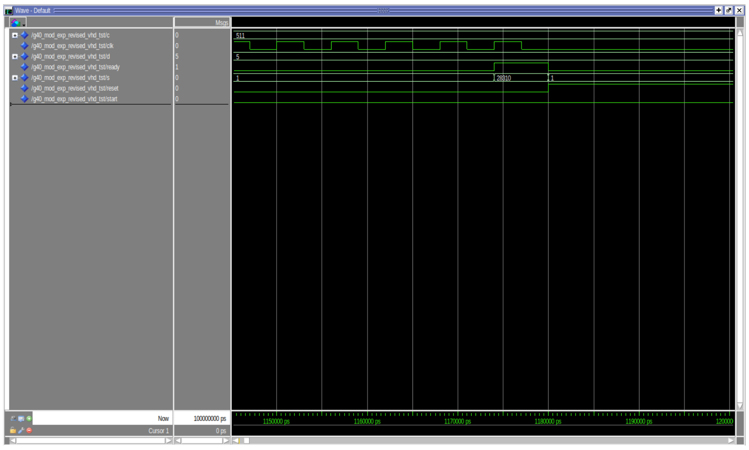

+
H6<7
E7
R
F7
R
H7
R
A7
R
+
E8
R
F
R
H8
R
A8
R
−
G9
R
H9
R
A9
R
−
G
R
H10
R
Amod33401
Afloor33401

Functional Simulation



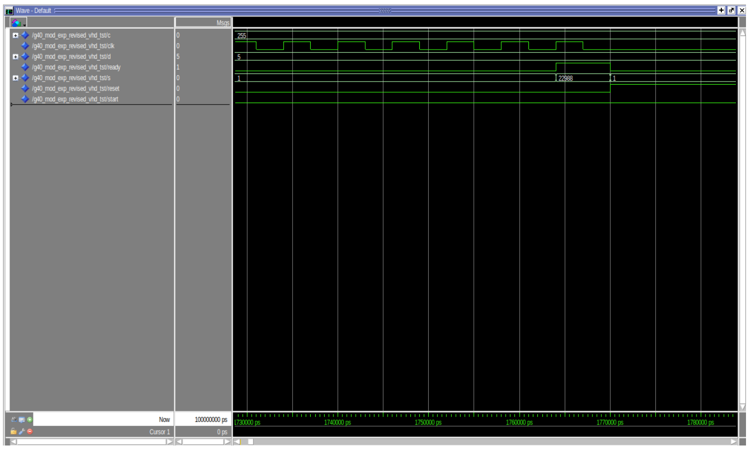
```
/g40_mod_exp_revised_vhd_tst/c       0
/g40_mod_exp_revised_vhd_tst/clk     0
/g40_mod_exp_revised_vhd_tst/d       5
/g40_mod_exp_revised_vhd_tst/ready   1
/g40_mod_exp_revised_vhd_tst/s       0
/g40_mod_exp_revised_vhd_tst/reset   0
/g40_mod_exp_revised_vhd_tst/start   0
Now        100000000 ps
Cursor 1   0 ps
```

c = 1023, d = 5 and Amod33401 = 20998



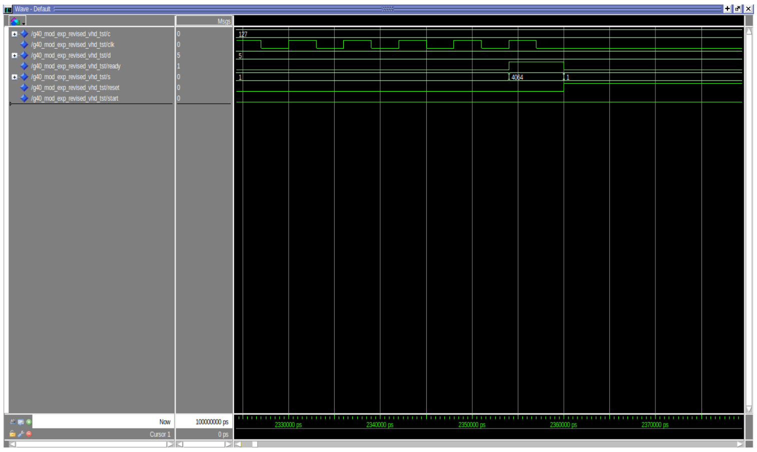
```
/g40_mod_exp_revised_vhd_tst/c       0
/g40_mod_exp_revised_vhd_tst/clk     0
/g40_mod_exp_revised_vhd_tst/d       5
/g40_mod_exp_revised_vhd_tst/ready   1
/g40_mod_exp_revised_vhd_tst/s       0
/g40_mod_exp_revised_vhd_tst/reset   0
/g40_mod_exp_revised_vhd_tst/start   0
Now        100000000 ps
Cursor 1   0 ps
```

c = 511, d = 5 and Amod33401 = 28310



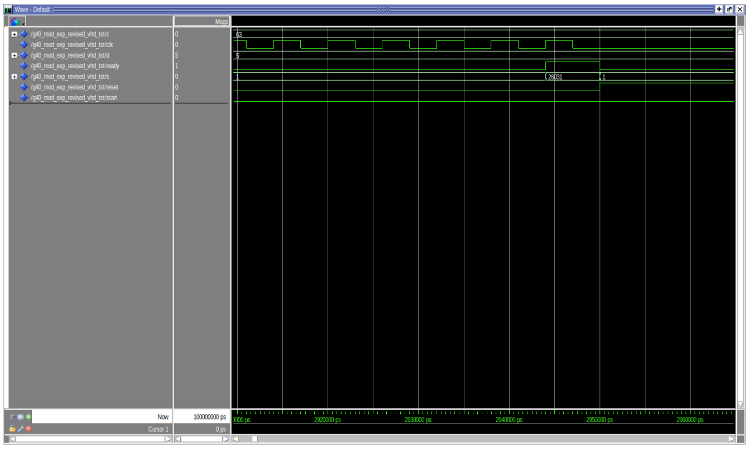
```
/g40_mod_exp_revised_vhd_tst/c       0
/g40_mod_exp_revised_vhd_tst/clk     0
/g40_mod_exp_revised_vhd_tst/d       5
/g40_mod_exp_revised_vhd_tst/ready   1
/g40_mod_exp_revised_vhd_tst/s       0
/g40_mod_exp_revised_vhd_tst/reset   0
/g40_mod_exp_revised_vhd_tst/start   0
Now        100000000 ps
Cursor 1   0 ps
```

c = 255, d = 5 and Amod33401 = 22988



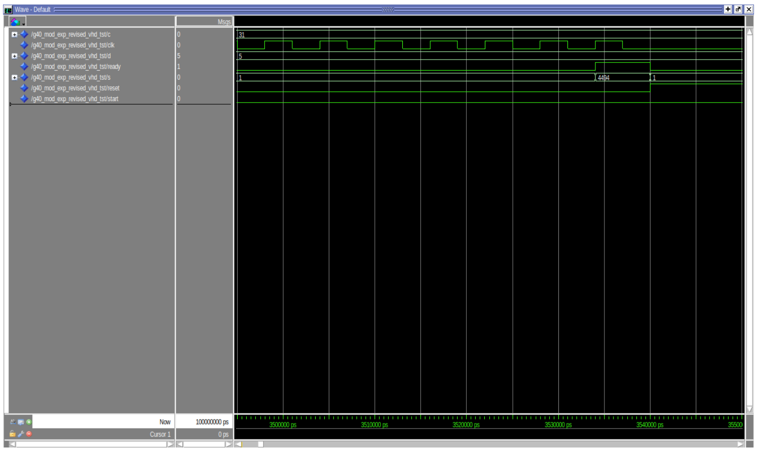
```
/g40_mod_exp_revised_vhd_tst/c       0
/g40_mod_exp_revised_vhd_tst/clk     0
/g40_mod_exp_revised_vhd_tst/d       5
/g40_mod_exp_revised_vhd_tst/ready   1
/g40_mod_exp_revised_vhd_tst/s       0
/g40_mod_exp_revised_vhd_tst/reset   0
/g40_mod_exp_revised_vhd_tst/start   0
Now        100000000 ps
Cursor 1   0 ps
```

c = 127, d = 5 and Amod33401 = 4064



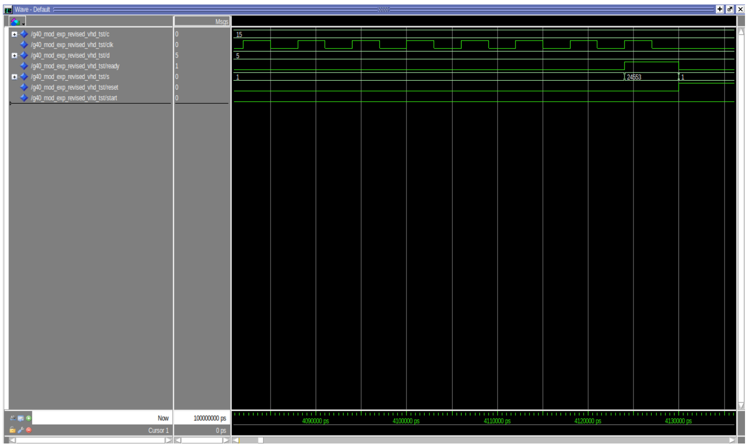
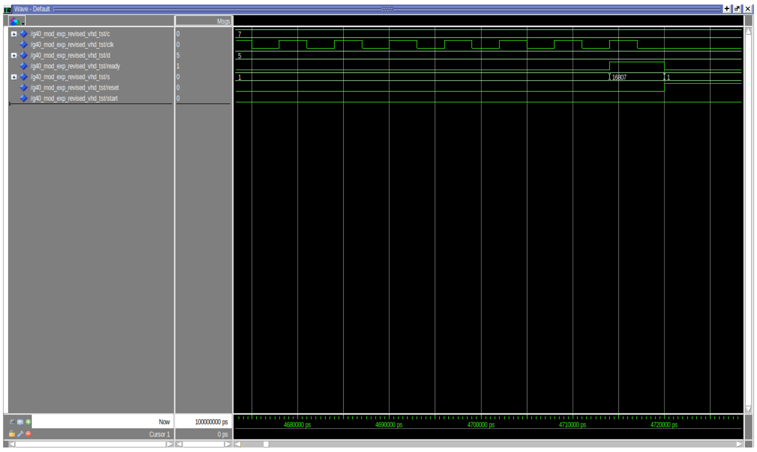
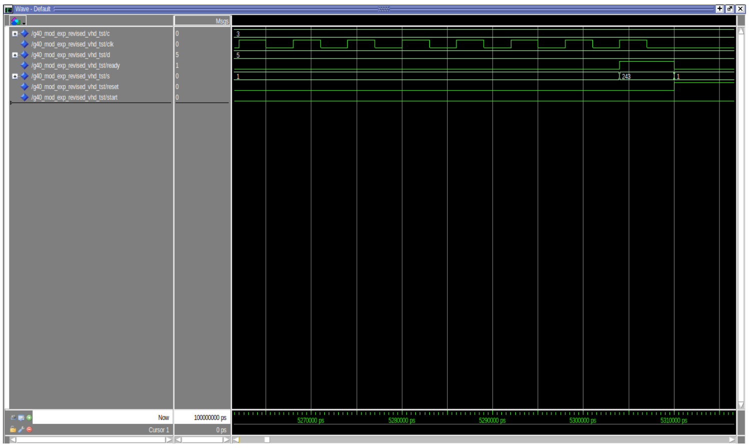
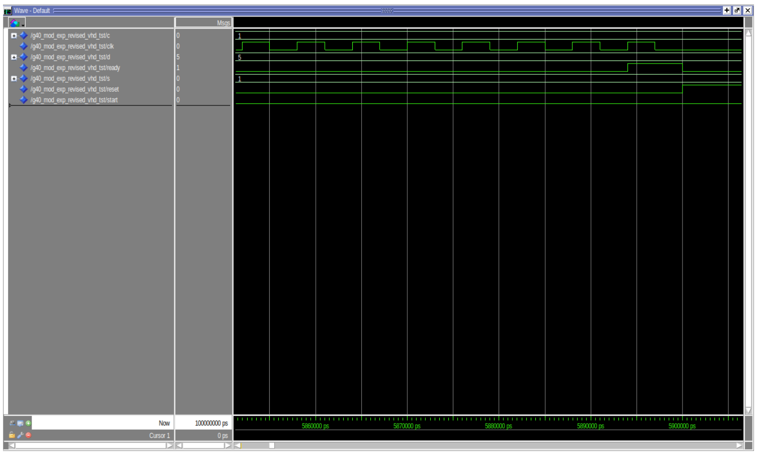
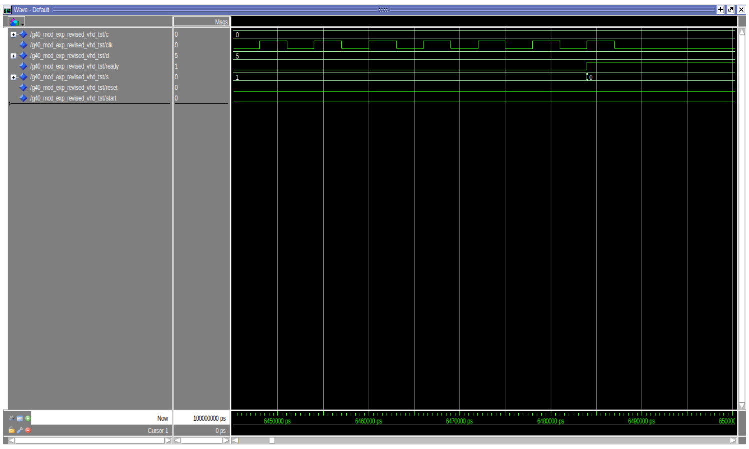
```
/g40_mod_exp_revised_vhd_tst/c       0
/g40_mod_exp_revised_vhd_tst/clk     0
/g40_mod_exp_revised_vhd_tst/d       5
/g40_mod_exp_revised_vhd_tst/ready   1
/g40_mod_exp_revised_vhd_tst/s       0
/g40_mod_exp_revised_vhd_tst/reset   0
/g40_mod_exp_revised_vhd_tst/start   0
Now        100000000 ps
Cursor 1   0 ps
```

c = 63, d = 5 and Amod33401 = 26031



```
/g40_mod_exp_revised_vhd_tst/c       0
/g40_mod_exp_revised_vhd_tst/clk     0
/g40_mod_exp_revised_vhd_tst/d       5
/g40_mod_exp_revised_vhd_tst/ready   1
/g40_mod_exp_revised_vhd_tst/s       0
/g40_mod_exp_revised_vhd_tst/reset   0
/g40_mod_exp_revised_vhd_tst/start   0
Now        100000000 ps
Cursor 1   0 ps
```

c = 31, d = 5 and Amod33401 = 4494

 Wave - Default Msgs /g40_mod_exp_revised_vhd_tst/c 0 /g40_mod_exp_revised_vhd_tst/clk 0 /g40_mod_exp_revised_vhd_tst/d 5 /g40_mod_exp_revised_vhd_tst/ready 1 /g40_mod_exp_revised_vhd_tst/s 0 /g40_mod_exp_revised_vhd_tst/reset 0 /g40_mod_exp_revised_vhd_tst/start 0 15 5 1 24553 1 Now 100000000 ps Cursor 1 0 ps 4090000 ps 4100000 ps 4110000 ps 4120000 ps 4130000 ps c = 15, d = 5 and Amod33401 = 24553	 Wave - Default Msgs /g40_mod_exp_revised_vhd_tst/c 0 /g40_mod_exp_revised_vhd_tst/clk 0 /g40_mod_exp_revised_vhd_tst/d 5 /g40_mod_exp_revised_vhd_tst/ready 1 /g40_mod_exp_revised_vhd_tst/s 0 /g40_mod_exp_revised_vhd_tst/reset 0 /g40_mod_exp_revised_vhd_tst/start 0 7 5 1 16807 1 Now 100000000 ps Cursor 1 0 ps 4680000 ps 4690000 ps 4700000 ps 4710000 ps 4720000 ps c = 7, d = 5 and Amod33401 = 16807
 Wave - Default Msgs /g40_mod_exp_revised_vhd_tst/c 0 /g40_mod_exp_revised_vhd_tst/clk 0 /g40_mod_exp_revised_vhd_tst/d 5 /g40_mod_exp_revised_vhd_tst/ready 1 /g40_mod_exp_revised_vhd_tst/s 0 /g40_mod_exp_revised_vhd_tst/reset 0 /g40_mod_exp_revised_vhd_tst/start 0 3 5 1 243 1 Now 100000000 ps Cursor 1 0 ps 5270000 ps 5280000 ps 5290000 ps 5300000 ps 5310000 ps c = 3, d = 5 and Amod33401 = 243	 Wave - Default Msgs /g40_mod_exp_revised_vhd_tst/c 0 /g40_mod_exp_revised_vhd_tst/clk 0 /g40_mod_exp_revised_vhd_tst/d 5 /g40_mod_exp_revised_vhd_tst/ready 1 /g40_mod_exp_revised_vhd_tst/s 0 /g40_mod_exp_revised_vhd_tst/reset 0 /g40_mod_exp_revised_vhd_tst/start 0 1 5 1 Now 100000000 ps Cursor 1 0 ps 5860000 ps 5870000 ps 5880000 ps 5890000 ps 5900000 ps c = 1, d = 5 and Amod33401 = 1
 Wave - Default Msgs /g40_mod_exp_revised_vhd_tst/c 0 /g40_mod_exp_revised_vhd_tst/clk 0 /g40_mod_exp_revised_vhd_tst/d 5 /g40_mod_exp_revised_vhd_tst/ready 1 /g40_mod_exp_revised_vhd_tst/s 0 /g40_mod_exp_revised_vhd_tst/reset 0 /g40_mod_exp_revised_vhd_tst/start 0 0 5 1 0 Now 100000000 ps Cursor 1 0 ps 6450000 ps 6460000 ps 6470000 ps 6480000 ps 6490000 ps c = 0, d = 5 and Amod33401 = 0	

Timing Analysis

Requested Fmax = 250 MHz

- Fast 1100mV 0C Model Hold Slack Value = 0.109 ns
- Slow 1100mV 85C Model Setup Slack Value = 0.848 ns

- Slow 1100mV 85C Model Fmax = 317.26 MHz

Our circuit now works with a clock of 4 ns!

Before the pipelining, these were the best results for the timing analysis:

Requested Fmax = 66.7 MHz

- Fast 1100mV 0C Model Hold Slack Value = 0.187 ns
- Slow 1100mV 85C Model Setup Slack Value = 0.510 ns
- Slow 1100mV 85C Model Fmax = 69.01 MHz

We went from a 69.01 MHz maximum frequency to a 317.26 MHz maximum frequency.