In this lab you will use *Mathematica* to help you with exercises 3.3.1, 3.3.2, and 3.3.3. You may work in groups of 2-3. As a group, you will write a report with your findings.

Report:

Your report should have a title and an introductory paragraph stating the purpose of the report and your principal findings. Then your report should include several paragraphs explaining what you did (procedure) and what you discovered (results). Finally, your report should include a paragraph with your conjectures and conclusions. The report should be illustrated with tables that display your observations. I would recommend creating one *Mathematica* notebook for scratch work and one *Mathematica* notebook (or Word document) for your report.

The report is due at the beginning of lab next Thursday, February 9. Bring a hard copy of your report to lab. Also, save the final draft of your report in the Lab5 folder (in the Math212 folder on the M-drive) and include your names in the filename, e.g. if I was turning in a report, I might name it lab04_report_decelles.nb.

Explorations:

In this lab we are looking for a property that all prime numbers share, and which is not too hard to check. (Obviously, all prime numbers share the property of primality, but the point is that this is hard/time consuming to check directly.) Finding such a property gives us an "industrial grade" test for primality.

Namely, if we know that all prime numbers have property P, and we have a whole number n that we would like to test for primality, we may check to see whether or not n has property P. If n does *not* have property P, then we know that n is *not* a prime. If, on the other hand, n *does* have property P, the test is inconclusive.

1. In 3.3.1, you are asked to make a conjecture regarding the divisibility of $2^n - 1$ by $(n+1)$. (Using the `Table` command in *Mathematica* can expedite the process while at the same time generating data that *Mathematica* can convert to a nice-looking table, using the `Grid` command. See the interactive notebook "Tables for Computation and Display" on the course website.)
2. In 3.3.2, you are asked to consider the divisibility of $1993^n - 1$ by $(n+1)$. You might want to try some smaller numbers before 1993, e.g. try 3, 6, 30, 42, 143.
3. In 3.3.3, you are asked to determine 3^{20002} modulo 11. It might help to observe that $3^{20002} = (3^2) \cdot (3^{10})^{2000}$. Then use your conjecture from 3.3.2 to determine 3^{10} modulo 11 ...

Some *Mathematica* Commands:

In Section 3.1 of the book, Shahriari gives examples of a few Maple commands relevant to working with prime numbers. Below are some of the corresponding commands in *Mathematica*. (Not all of them are necessarily relevant for this lab, but I thought it was worth including them for completeness.)

To find the 200$^{\text{th}}$ prime, type

```
Prime[200]
```

Then press `Shift` and `Enter` at the same time to evaluate.

To find the first prime larger than 200:

```
NextPrime[200]
```

The command that gives an integer factorization is `FactorInteger`. It returns a list of the prime factors along with their powers. For example, `FactorInteger[24]` returns `{{2, 3}, {3,1}}` since $24 = 2^3 \cdot 3^1$.

Shahriari does not mention a command for finding remainders, but in *Mathematica* you can use the command `Mod`. For example,

```
Mod[123, 7]
```

gives the remainder of 123 after dividing by 7.

The `Table` and `Grid` commands are useful for executing a command for several values of n simultaneously and for displaying the results nicely, respectively. See the interactive notebook "Tables for Computation and Display" on the course website for more details.