Virtual Class, Week 12

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

I hope to find you well as we begin Week 12 of Virtual MATH 601! We are now starting to bring many of our course goals together–using theoretical mathematics to make, and break, codes–in a powerful way: using the algebra of elliptic curves!

This week, we introduce the focus of our final Programming Investigation module–which you may remember is our **capstone project**. It is more involved than the previous modules, and is correspondingly worth a larger portion of your final course grade (please see our updated syllabus posted on the course site for details). The topic of this capstone project is **Lenstra's elliptic curve factoring method**, and the project has **two parts**:

1. **Programming portion**, in which we implement Lenstra's method, and
2. **Partnering problems**, in which we can test and apply our implementation of this factoring algorithm.

Both parts are posted on the course website, and are due on the last day of Final's Week, **Friday, May 15**.

Your goal for Week 12 of MATH 601 should be to to become oriented with Lenstra's factoring algorithm, and to finish the first stage of implementing it in Sage.

1. **Read the full lecture notes** for Week 12 in the **Daily Update**.

   For more examples of applying Lenstra's method, see Savin 13.1, Trappe-Washington 16.3, and Hoffstein, et al. 5.6.

2. Access Blackboard, and **watch the instructional video** entitled **Lenstra's elliptic curve factoring algorithm**.
3. From the course website, download the two parts of our capstone project: the **final Programming Investigation Module**, and the **partnering problems** that should be solved using the completed module.
4. Start the programming portion of the module. This week, your goal is to complete (at least) **Exercise 1 of the programming portion**. Though the capstone project (including the partnering problems) are due at noon on the last day of Finals Week (Friday, May 15), finishing Exercise 1 will be advantageous, since a solution to Exercise 2 may be useful in homework problems assigned in the remainder of the semester.

5. To be clear, there is no homework that should be turned in next Tuesday, but make sure to follow (4) above carefully!

6. Note that **Office Hours for our Programming Investigation Modules** with our course assistants who designed the modules, Doug and Zach, will be held twice a week. Check the course website for details on how to join them; hours will be updated weekly and posted on the course website. If you find that the hours during one week don't work for you, email me your full availability, and I will communicate it to them so that they can do their best to accommodate you the following week.

7. Along with Virtual Office Hours hosted on Blackboard, I will also have on-demand **Virtual "In-Person" Office Hours on Zoom** during during regular class periods (11 am - 12:15 pm on Tuesdays and Thursdays, in case you forgot!). Just email me at least an hour ahead of time, and I will send you the info on how to connect. Of course, you can still **email me with any questions you may have!**

8. Interested in delving deeper into this week's topics?

   - Most of the factoring algorithms we've developed in MATH 601 can be thought of as being based on a group's structure. Read about this general notion, and think carefully about which groups our various factorization algorithms correspond to.
   - You may have noticed the term *B-smooth* in discussions/articles about the efficiency of different factoring methods. After becoming oriented with the concept of smooth numbers, think about what these smoothness properties say about the effectiveness of our different factoring algorithms.