# Virtual Class, Week 13

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

---

This is our Virtual Class week, and we are **bringing together the "old" and the "new"**: cryptosystems that we are very familiar with (from before the first midterm!), shifted to the setting of elliptic curves! Besides our capstone project, this week is the **last week we will have homework assigned** in MATH 601.

0. I have really missed seeing you during class and office hours, and very much appreciate your hard work and flexibility during this transition. This big and unexpected shift has been a challenge for everyone (myself included!), and I have been so impressed with your performance (e.g., I just saw your work when grading the EEA/RSA Programming Investigation Module). Be proud of the mathematics you have mastered, especially in such a new setting. Keep it up!

   **Announcements.**

   - New 4/29: We've updated the provided "skeleton" for `rand_elliptic` function (notice the very slight change in output!). You can use either version, depending on what you prefer.
   - The grader has finished grading all our homework assignments thus far. Please check it over on Gradescope, and submit *regrade requests* if you have grading questions.
   - Email me if you would like to know your current course grade. Remember that if you would like to improve your grade, there is still room to do so in our final assignments!
   - A couple notes about the final Programming Investigation Module: (1) Currently the addition function only checks whether a *finite* point entered in on the given curve. Make sure to address the case when a point is the identity throughout your work! (2) The last partnering problem has been slightly updated, so please download it before you apply your code to solve these problems.

1. **Read the full lecture notes** for Week 13 in the **Daily Update**. Refer to Hoffstein, et al. 5.3 (up until 5.3.1 begins) and 5.4 as a supplement.

2. Access Blackboard, and **watch the instructional video** *Elliptic curve cryptography.*

3. Complete the following **homework problems** and submit your solutions to Gradescope by next Tuesday (5/5). *For this problem set, if you use code from your Programming Investigation Module, explicitly point out where you use it. However, you do not need to attach your code since you will turn it in later.*

   1. (12 points) Alice and Bob agree to use elliptic curve Diffie-Hellman key exchange with the prime $p = 2671$, elliptic curve $E(2671)$ given by

      $$y^2 \equiv x^3 + 171x + 853 \bmod 2671$$

      and point $P = (1980, 431)$ on $E(2671)$.

(a) (3 points) Alice sends Bob the point $Q = (2110, 543)$. Bob decides to use the private key $m = 1943$. What point should Bob send to Alice?

(b) (3 points) What is their shared secret value?

(c) (6 points) Alice and Bob want to agree on a new shared secret key using the same prime, curve, and point above. This time Alice sends Bob only the $x$-coordinate of her point $Q$, $x_Q = 2$. Bob decides to use the secret multiplier $m = 875$. What single number modulo $p$ should Bob send to Alice, and what is their new shared secret key?

2. (8 points) A shortcoming of using an elliptic curve $E(p)$ modulo a prime $p$ for cryptography is the fact that it takes two coordinates to specify a point in $E(p)$. However, as discussed briefly at the end of Section 5.4.2 of Hoffstein, et al., the second coordinate conveys very little additional information, once the first coordinate is known.

(a) (4 points) Suppose that Bob wants to send Alice the point $R \in E(p)$. Explain why it suffices for Bob to send Alice the $x$-coordinate of $R = (x_R, y_R)$ together with the value

$$\alpha_R = \begin{cases} 0 & \text{if } 0 \leq y_R < \frac{p}{2} \\ 1 & \text{if } \frac{p}{2} \leq y_R < p \end{cases}$$

Here, you can assume that Alice is able to efficiently compute square roots modulo a prime $p$ (and we happen to know very well how to do so if $p \equiv 3 \bmod 4$!)

(b) (4 points) Alice and Bob decide to use the prime $p = 1123$ and the elliptic curve $E(1123)$ given by

$$y^2 \equiv x^3 + 54x + 87 \bmod 1123.$$

Bob sends Alice the $x$-coordinate $x_R = 278$ and the value $\alpha_R = 0$. What point is Bob trying to convey to Alice? What about if instead Bob had sent $\alpha_R = 1$?

4. **Office Hours and Programming Office Hours.**

- See the course website/Blackboard for info on **Zoom Office Hours** with our Programming Investigation Module course assistants, or with me.
- You can also **email me or our Programming course assistants** (email addresses on Blackboard) with questions.
- Of course, you can still access **Virtual Office Hours** on Blackboard if you prefer.

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

- Section 5.5 in Hoffstein, et al., titled *The evolution of public key cryptography* is an extremely interesting account of the relationship of elliptic curves to cryptography, including relevant factors that we don't consider in this class, including general "trust" in cryptosystems based on how much they have been used, and even on *patents*!
- Interested in attacks on the elliptic curve discrete logarithm problem, and on its difficulty? See the *The Double-and-Add Algorithm* in Section 5.3.1 in Hoffstein, et al., as well as Section 5.3.2.

- See Cipolla's algorithm if you're interested in a method for computing the square roots of an integer modulo a prime