Virtual Class, Week 11

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

Welcome to Week 11 of Virtual MATH 601! Congrats on completing two of the three Programming Investigation Modules last week. Look out for an announcement about the final Module after we've covered Lenstra's factoring algorithm!

1. **Read the full lecture notes** for Week 11 in the **Daily Update**. Read Trappe-Washington 16.1 and 16.2, and refer to Section 12.3 in Savin for more examples of elliptic curves modulo a prime p.

   You can use Hoffstein, et al., Chapter 5, as an additional reference on elliptic curve group (also available on Blackboard); you will find that it has different notation, but it is not too difficult to navigate.

2. Access Blackboard, and **watch the instructional videos** entitled:

   (a) Conventions on elliptic curve groups

   (b) Elliptic curves mod p

3. Complete the following **homework problems** and submit your solutions to Gradescope by **next Tuesday** (4/21). As usual, show all your steps in each problem, and follow my previous instructions if you are programming in SAGE or Python to complete any parts of the assignment (and let me know if you need a reminder of these instructions).

   1. (10 points) Determine all primes p for which the elliptic curve $E(p)$ given by
   $$y^2 \equiv x^3 + 2x + 3 \bmod p$$
   is singular. Then for each such p, factor the right-hand side of this equation, $f(x) = x^3 + 2x + 3$ (where the coefficients are considered modulo p) to show that $f(x)$ has a double root.

      Hint: Since $f(x)$ is cubic and has a double root, it has exactly two roots. It is easy to see that $x = -1$ is a root of $f(x)$. What does the derivative of $f(x)$ tell us about where it has a double root?

   2. (10 points) Compute, by hand, $(1,5) + (9,3)$ on the elliptic curve $E(19)$ given by
   $$y^2 \equiv x^3 + 2x + 3 \bmod 19.$$

   3. (10 points) Compute, by hand, the orders of the points $(0,0)$ and $(6,2)$ on the elliptic curve $E(7)$ given by
   $$y^2 \equiv x^3 + 2x \bmod 7$$

      Hint: Apply Lagrange's theorem to save time!

4. (10 points) Determine the number of elements in the elliptic curve group $E(19)$ of

$$y^2 \equiv x^3 + 8 \bmod 19$$

using an analogous method to that in the Virtual Lecture Notes for $E(5)$ given by $y^2 \equiv x^3 + 1 \bmod 5$. Then compare your answer to Hasse's bound.

4. Access **Virtual Office Hours** on Blackboard with any questions.

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

- Check out the "graphs" of some elliptic curves modulo p in the Section *Elliptic curves over finite fields* on the Wikipedia page titled *Elliptic curve.*
- Make sure to check out the history behind the word "elliptic" in *elliptic curves* in your Trappe-Washington reading (*Historical point* on p. 349). We know that their graphs are not ellipses!
- See mathematician Igor Tolkov's 2009 paper proving Hasse's bound on the order of elliptic curves modulo p, along with recent related developments.