Topics in Number Theory: Elliptic Curves

April 19, 2020

`http://math.colorado.edu/~kstange/teaching.html`
Homework assigned.

1 For Friday, January 31st.

Note: Please focus on the problems most appropriate to you (the ones you will learn something from). Aim to do at least 3/4 of the problems.

1. (a) Show $y^2 = x^3 + 1$ is smooth at $(2, 3)$ in both the ways we discussed in class.
   (b) Give a general way to figure out which linear combination of x and y in M_P vanishes modulo M_P^2.
2. JHS I.1.2(a),3,4,7,8,9,12
3. In class, I said that a rational map ϕ is defined over K if it can be given as $[f_0, \ldots, f_n]$ for $f_i \in K(V)$. Show that this is equivalent to the definition in JHS, bottom of page 11. (To be precise, in class I called two rational maps $[f_0, \ldots, f_n]$ and $[g_0, \ldots, g_n]$ equivalent if there is some $g \in \overline{K}(V)$ so that $f_i = gg_i$ for all i. So my definition allows us this freedom of multiplying by g to obtain $f_i \in K(V)$ whereas the definition in JHS only allows multiplying by $\lambda \in \overline{K}^*$.) [NOTE: IT TURNS OUT THIS IS FALSE. FIND A COUNTEREXAMPLE.]
4. Further about $y^2 = x^3 + 1$ at $(2, 3)$:
   (a) Compute the order of $2x - y - 1$ on $y^2 = x^3 + 1$ (the curve above) at $(2, 3)$ via a power series expansion. Suggestion: change variables to move $(2, 3)$ to $(0, 0)$.
   (b) In the local ring at the point, $x - 2$ and $y - 3$ are both uniformizers, hence generators of the maximal ideal. Write one as a multiple of the other and observe that the scaling factor is a unit.

2 For Friday, February 14th.

Try to have around 5 exercises prepared and ready to go for a presentation. Look through, work through and consider the others as appropriate, so you are ready to be a good audience to any of these. Please also feel welcomed to work other problems from the exercises if those are more appropriate for your background. You can present any exercise from JHS if you prefer (as long as you learned something from doing it).

1. JHS I.1.8 (repeating from last time because if someone wants to present it, that would still be useful I think)

2. Consider the morphism from $y^p = x$ to $\mathbb{P}^1$, over the field $\mathbb{F}_p$, given by $(x, y) \mapsto [x, 1]$. In class we worked out the degrees (usual, separable, inseparable) of this using the function fields. Now, work out the degrees by computing ramification indices and using II.2.6.

3. JHS II.2.1 if you want to shore up your algebra.

4. JHS II.2.2, 3, 7

5. JHS III.3.5, 9

3 For Friday, February 28th.

Try to have enough prepared so you can present an item if called upon. I think some of the exercises are sometimes long, so should count as a few items; you can do part of a problem as your item. As before, please look through, work through and consider the others as appropriate, so you are ready to be a good audience to any of these. Please also feel welcomed to work other problems from the exercises if those are more appropriate for your background. You can present any exercise from JHS if you prefer (as long as you learned something from doing it).

1. JHS II.2.10, 11, 14

2. JHS III.3.12, 21

3. Classify the 2-torsion in $E(\overline{K})$ without using the theorem we proved in class, i.e. directly. In other words, what possible groups may appear? Note: in the case that $\overline{K}$ has characteristic 2, things are different. Hint: In characteristic 2, we can still put the curve in the forms $y^2 + xy = x^3 + a_2x^2 + a_6$, $a_6 \neq 0$ or $y^2 + a_3y = x^3 + a_4x + a_6$, $a_3 \neq 0$ (JHS, Appendix A).

4. Late addition, will also appear next week: The definition in class I gave of a quadratic form is that $q(ax) = a^2q(x)$ and $\langle a, b\rangle := q(a+b) - q(a) - q(b)$ is bilinear. Verify that, for $q(x, y)$, this is equivalent to $q(x, y)$ being a homogeneous polynomial of degree 2 in the variables x and y (this holds for arbitrarily many variables too). Give the correspondence explicitly, i.e. what are the coefficients of the polynomial associated to a form q?

5. Late addition, will also appear next week: Let $\phi : E_1 \to E_2$ be an isogeny of degree m. Show that the kernel of $\widehat{\phi}$ is

$$\{Q : \phi^{-1}(Q) \subseteq E_1[m]\}.$$

Show that, if ϕ is separable, then this is of size m.

4 For Friday, March 13th.

Try to have enough prepared so you can present an item if called upon. I think some of the exercises are sometimes long, so should count as a few items; you can do part of a problem as your item. As before, please look through, work through and consider the others as appropriate, so you are ready to be a good audience to any of these. Please also feel welcomed to work other problems from the exercises if those are more appropriate for your background. You can present any exercise from JHS if you prefer (as long as you learned something from doing it).

1. Let $\phi : E_1 \to E_2$ be an isogeny of degree m. Show that the kernel of $\widehat{\phi}$ is

$$\{Q : \phi^{-1}(Q) \subseteq E_1[m]\}.$$

   Show that, if ϕ is separable, then this is of size m.

2. Ruofan gave a very nice solution to JHS III.3.12 that depended upon the Weierstrass equation. This week, you could give another solution to this that is more abstract using Corollary III.4.11 as well as properties of the degree including Lemma V.1.2.

3. JHS III.3.14.

4. JHS V.5.1 (start with Example V.2.1).

5. JHS III.3.20 (about orders in imaginary quadratic fields)

6. JHS III.3.24 (about Tate module)

7. JHS V.5.4 (using Tate module)

8. More may be posted as class continues.

5 For Friday, April 3rd.

Try to have enough prepared so you can present an item if called upon. I think some of the exercises are sometimes long, so should count as a few items; you can do part of a problem as your item. As before, please look through, work through and consider the others as appropriate, so you are ready to be a good audience to any of these. Please also feel welcomed to work other problems from the exercises if those are more appropriate for your background. You can present any exercise from JHS if you prefer (as long as you learned something from doing it). You can also do exercises from previous weeks that we never got to.

1. JHS VI.6.3 (a) and (b)

2. JHS VI.6.6

3. JHS VI.6.7
4. JHS VI.6.8
5. JHS VI.6.9
6. JHS VI.6.10

6 For Friday, April 24th (note date).

As I don't want to have the final day be a homework day, we'll have only one more homework day, the second-to-last week.

Try to have enough prepared so you can present an item if called upon. I think some of the exercises are sometimes long, so should count as a few items; you can do part of a problem as your item. As before, please look through, work through and consider the others as appropriate, so you are ready to be a good audience to any of these. Please also feel welcomed to work other problems from the exercises if those are more appropriate for your background. You can present any exercise from JHS if you prefer (as long as you learned something from doing it). You can also do exercises from previous weeks that we never got to.

1. JHS IV.4.1
2. JHS VII 7.3 (note the reference should be VII.3.5)
3. JHS VII 7.4
4. JHS VIII 8.1 if you are a number theorist and have those tools
5. JHS VIII 8.2
6. JHS VIII 8.10
7. I really picked a thin path through the proof of Mordell-Weil; dig into any detail missing or more general statement of results from within Joe's treatment and present it if you find it interesting.