Freshman Seminar 21n: Elliptic Curve **Projects**

William Stein

April 1, 2003

Your common track has come to an end, and now your paths diverge. For the rest of this semester each of you will dive into a specific project that involves elliptic curves. You will give presentations about your project each week during class. For example, I might give you specific homework problems about your project whose solutions you will present in class.

Your project should be comprehensible to everyone in the freshman seminar, and I hope it will be something you can be proud of and post on the web page for the course. Do library research, web research, look in (possibly old) books and papers, draw diagrams, do computations, etc. Your project can be typed and printed, it can be a web page, or it could even be carefully hand written. Just make it exciting!

1 Schedule

April 8	Initial 15m presentations on projects
April 15	Second presentation (very rough draft due)
April 22	Third presentation
April 29	Fourth presentation (fairly polished draft due)
May 6	Fifth presentation (get comments on your polished draft)
May 13	Give a polished 40 minute presentation

Note: I will be gone on April 8 (US Congress) and May 5–6 (Institute for Defense Analysis), but Grigor will lead class those two days. I will be easy to reach via email.

2 Possible Projects

If there is a project not listed here that you want to do, that is also possible.

1. What does it mean to say that an elliptic curve over $\mathbb{Q}$ is modular? What is known about modularity of elliptic curves?

2. Give a complete verification that there is an elliptic curve over $\mathbb{Q}$ of rank ≥ 24 and explain why the computations you do show this. Draw a graph of this curve of rank ≥ 24 and label the 24 independent points on this graph. Trace the history of finding curves of large ranks. Draw a graph of the rank as a function of time and (silly) use data fitting methods to predict when we will find a curve of rank 30.

3. What is the Schoof-Elkies-Atkin algorithm for finding $\#E(\mathbb{F}_p)$ in time polynomial in $\log(p)$? How does it work? What is its significance in cryptography?

4. Give a survey of Newton's classification of cubic curves. Also give a complete proof there every cubic plane curve with a rational point P has a Weierstrass equation (a partial proof of this is given in Section I.3 of [Silverman-Tate]).

5. Do a project about the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$. Look at and describe the original papers in which Birch and Swinnerton-Dyer first announced their conjecture and discussed the computer computations that led to it. Give a precise and complete statement of the conjecture. Verify that the conjecture is true for $y^2 = x^3 + 3x$ (this will probably require applying a deep theorem of Karl Rubin).