# Math 168: Project Ideas

William Stein

November 16, 2005

1. How to compute $a_p(E)$ for an elliptic curve $E$ and small $p$ (see Henri Cohen's first GTM book).

2. How (e.g., PARI) computes Bernoulli numbers so much faster than anything else

3. Write discussion about factorization of RSA challenge numbers (e.g., a new $20000 one was factored a few days ago!)

4. Write about geometry on the upper half plane (the Poincare metric, the Poincare disk, etc.)

5. Prove that reduction $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ is surjective (following, e.g., the proof in Shimura's book *Introduction to Arithmetic Theory of Automorphic Forms*).

6. A project on the dimension of $S_2(Gamma_0(N))$. This requires more background than you need for the course; in particular, you must know the Riemann-Roch theorem for curves/Riemann surfaces. You would also want to look at the paper by Csirik et al. about $d$'s that are not dim $S_2(Gamma_0(N))$ for any $N$.

7. Proof of Manin's theorem that the 2 and 3 term relations between Manin symbols are everything. References: Manin's original 1972 paper; a very very complicated paper by Shokoruv; Tseno's student project (for me) on Shokoruv; Gabor Weise's recent Ph.D. thesis (I have a copy); notes for Math 252 at Harvard. This is sufficiently broad that it could be a joint project with two people. (Gabor's Ph.D. claims to have an easier way to do this...)

8. Write a project about "the" baby-step giant-step algorithm. How is it used to — solve discrete log problems? — find the structure of a group? etc.?