Math 17: Term paper topics

You should soon start thinking seriously about term papers for the course. You will each write a research term paper, and present the contents of that paper to the class late in the term; the term paper is due on the last day of classes. The paper should be approximately 10-15 pages in length, and cover a topic closely related to the course. A sample list of potential topics is included below as well as a list of books on reserve in Baker which would be useful to peruse.

When you find something of potential interest, stop by to see if the topic, scope, prerequisites etc are reasonable.

I will want a one-page outline of the term paper by February 8. That will leave you three weeks to write the paper and prepare your oral presentation! Student presentations are the last four days of class; see the syllabus. Note that by February 1, we will have talked about public-key cryptography and RSA encryption, so you will have a better idea of some of the broader cryptographic concepts of the course.

Below are some starter ideas for term papers. There will soon be some books on 24 reserve at Baker which are worth browsing. Obviously take some of these key words and feed them into Google, sorry . . . your favorite search engine.

Remember, the term paper and presentation constitutes half of your grade, so don't take it lightly.

Sample topics

1. Two points determine a line; 5 points determine a conic; 9 points determine a cubic
2. Applications of conic sections, especially hyperbolas
3. Some simple cases of the proof of Fermat's last theorem.
4. Congruent Numbers and Elliptic Curves; Tunnell's theorem
5. Computing congruent numbers
6. Primality testing: pseudoprimes, Carmichael numbers, strong pseudoprimes, Miller Rabin test, deterministic versus probabilistic primality tests
7. Factoring efforts: Fermat, Pollard Rho, quadratic sieve
8. Cryptographic attacks (general types, specific instances)
9. Tweaks needed to make RSA secure
10. AES and Rijndael
11. Other public-key cryptosystems: El Gamal, Diffie-Hellman
12. Historical aspects of cryptography
13. SSL (secure web transactions)
14. Commercial implementation of public key systems

(continued on reverse)

Harder projects

1. Elliptic curves over the complex numbers
2. Birch and Swinnerton-Dyer conjecture
3. Elliptic functions and elliptic integrals

The following books will be on 24 hour reserve at Baker:

1. Rational points on elliptic Curves (Silverman)
2. Elementary Number Theory and its applications (Rosen)
3. Introduction to Cryptography (Buchmann)
4. A course in number theory and cryptography (Koblitz)
5. Introduction to elliptic curves and modular forms (Koblitz)
6. Applied Cryptography (Schneier)
7. Beyond fear : thinking sensibly about security in an uncertain world (Schneier)

Certainly there are lots of other elementary number theory books or books on cryptography or primality testing in the library.