18.786 Writing Project - Spring 2008

Due on May 15

You must select one of the following two options (or a combination of the two):

A Write an expository paper at least 5 pages in length on a topic of your choice that relates to algebraic number theory. This could be something from lectures or the course book that we did not cover in-depth, or an application of ideas in algebraic number theory to other areas of mathematics (or other sciences).

B Gather and analyze computational data pertaining to important conjectures or algorithms from algebraic number theory. You also must include an adequate written summary (no strict length requirements) of what you have computed and why it is relevant.

Project Ideas

1. **Cyclotomic polynomials**
   Investigate the coefficients of cyclotomic polynomials in general; check examples computationally and research known results.

2. **Fermat's last theorem for regular primes**
   Study Kummer's proof in detail, and learn more about factorization and primes in cyclotomic fields.

3. **Regular primes**
   Investigate the distribution of regular primes; use Bernoulli numbers and class numbers to gather numerical data and learn about current conjectures.

4. **Coefficients of modular forms**
   The key result is that the coefficients of a modular form on a congruence subgroup lie in a field of algebraic integers. This field is connected to Galois representations, elliptic curves, Hecke operators, etc.; the arithmetic of the coefficients is also relevant to questions of divisibility, multiplicativity, etc. Any one of these is sufficient for a project. There is a huge amount of material available in books and journals, as well as many natural computational problems.

5. **Elliptic curves**
   The study of rational points and automorphisms of elliptic curves is connected to algebraic number theory, especially in the context of curves with "complex multiplication".

6. **Class numbers**
   Although class numbers are always finite, they are poorly understood in general. Very recent results describe the 2-part and 3-part in somewhat more detail. Options: gather computational data; study quadratic extensions in depth; read the proofs for lower/upper bounds; focus on the special case of class number one.

7. **Quadratic forms**
   Class numbers for quadratic fields were first studied through the theory of representations by quadratic forms. Here the class group is represented by equivalence classes of quadratic forms under certain composition laws. You can learn more about the classical theory of quadratic forms and representing integers, or you may also learn about the connections to class numbers for number fields. There are also cubic, quartic, and higher degree forms; the theory is less developed, but you can learn about higher composition laws, and connections to other number fields.

8. **p-adic fields**
   Learn about this special class of number theoretic local fields; possible topics include valuation theory, places, and the adelic viewpoint. Another alternative is to simply learn how to use SAGE or PARI/GP to perform p-adic computations.

9. **Primality testing**
   It was recently shown that there are polynomial-time procedures for testing the primality of a given integer. These depends on algebraic number theory in a fundamental way. You may either study the most cutting-edge version of these algorithms or explore the computational aspects of simpler versions.

10. **Integer factoring**
    The best known algorithms for integer factorization are the quadratic and number field sieves. As their name implies, they use algebraic number theory; you may study either the computational or theoretical aspects.

11. **Higher reciprocity**
    Learn about analogs of quadratic reciprocity to higher degrees using cyclotomic fields.

12. **L-functions and characters**
    A number-theoretic multiplicative character is a homomorphism into the cyclotomic units, and the corresponding L-functions are a powerful tool for studying the distribution of primes, the Chebatorev density Theorem, etc.

13. **Gauss sums**
    A special application of characters, that lead to a better understanding of cyclotomic fields. Estimating character sums in general leads to distribution results on quadratic (and higher) residues.

⋆ **Other**
   If you have other interests, please don't hesitate to discuss them with me – any area of mathematics with notions of counting, factorization, primes, etc. probably has some connection to algebraic number theory!