

MATH 713 ALGEBRAIC NUMBER THEORY: FINAL PROJECT

FARSHID HAJIR
OCTOBER 11, 2005 – 01 : 34

Unless you choose to do a final exam instead, you will have to do a final project. You will choose, or be assigned, a topic, together with some suggested reading to get you started. You will then read about the topic and write a 5-10 page article giving an overview of the topic. Part of the assignment is to look for and use further references if necessary.

We should settle on your topic by Oct. 18: please discuss it with me or send me an e-mail. I would like to make sure no two students are working on the same topic.

The first draft of your write-up will be due by Nov. 15. This first draft does not have to be as complete or as polished as the final project but it should show your intimate familiarity with the topic. I'll meet with each student to discuss the first draft and make suggestions for additions/modifications.

In writing your report, your goal is to communicate the key ideas, definitions, theorems of the topic you have chosen to your classmates. If it helps you, think of the audience as your future self: when you come back to your write-up a year from now, say, you'd like to find it easy, pleasant, and above all informative reading.

To increase the feedback you will receive, you will also give a first draft to one of your classmates who will give you his/her written comments. Later on, I'll describe the automorphism of the set of students that assigns first drafts to their readers; it won't have any elements of order 2.

You are not restricted to the topics that follow, but you should discuss your choice with me as soon as possible. In one-on-one meetings, I would be very happy to provide further details and make suggestions based on what you are interested in.

TOPICS FOR FINAL PROJECT

1. **Class number and unit group of real quadratic fields.** These can be described in terms of quadratic forms but now reduced

forms can be equivalent according as whether a continued fraction algorithm related to the Pell equation (giving the fundamental unit) relates them or not. [Reference: SO MANY! e.g. book by Dan Flath]

2. **Brauer-Siegel Theorem.** If K runs through a family of number fields of degree n_K and discriminant d_K such that $\log(|d_K|)/n_K \rightarrow \infty$, then $\lim h_K/\log(|d_K|) = 1/2$. The proof uses the analytic class number formula. [Ref: Lang’s book on algebraic number theory, Neukirch, Stark’s 1974 article in *Inventiones*, recent result of Tsfasman-Valdut extending B-S...].

3. **Class Field Towers.** If K_1 is the Hilbert class field of K and $K_{i+1} = (K_i)_1$, then $K \subseteq K_1 \subseteq K_2 \subseteq \dots$ is called the class field tower of K . The Galois group $\text{Gal}(K_\infty/K)$ is the (maximal pro-solvable quotient of) the “fundamental group” of K . It was thought for a long time that this tower is always finite. In the 60s Shafarevich and Golod showed this was not the case. [Ref: Roquette’s article in *Cassels-Frohlich*].

4. **Generalized Riemann Hypothesis.** Each number field has a zeta function called the Dedekind zeta function, just like \mathbb{Q} has the Riemann zeta function. Each Dedekind zeta function has a functional equation, Riemann hypothesis, etc. [Ref: Neukirch, many many others].

5. **Theta functions and sums of four squares.** The classical (Jacobi) theta function is $\theta(z) = \sum_{n=0}^{\infty} q^{n^2}$ where $q = \exp(2\pi iz)$. The coefficients of $\theta^4(z)$ count how many ways each integer can be written as a sum of four squares. One can use this fact to prove Lagrange’s theorem on sums of four squares. [I think this is in Serre’s course in arithmetic, but there are many other references including Jacobi’s collected works!]

6. **Goldfeld-Gross-Zagier’s lower bound for $h(-d)$.** Through some brilliant work using zeta functions and Heegner points, we now have an explicit lower bound for class numbers of imaginary quadratic fields, but it is far from the optimal one we “know” to be the truth. [Oesterle’s *Seminaire Bourbaki*].

7. **Adèles and Idèles.** These are topological groups which allow a formulation of class field theory which takes in infinite extensions all at once. [Ref: *Cassels-Frohlich*, Neukirch, Lang, ...]

8. **Functional Equation for Hecke L-functions.** Hecke L-functions are important generalizations of Dedekind zeta function of a number field and of Dirichlet L-functions. In 1950, Tate gave a new way of understanding them in his thesis which has been very influential.

[Goldstein's Analytic number theory, Tate's thesis in Cassels-Frohlich, GTM book by Ramakrishnan and Valenza, Neukirch].

9. **Local fields, local class field theory.** When you complete a number field at a prime ideal you get a finite extension of \mathbb{Q}_p , the field of p -adic numbers. This localization process is extremely useful. The abelian extensions of local fields are much better understood. [The "Bible" is Serre's *Corps Locaux*, translated in GTM series. chapter in Cassels-Frohlich, Gouvea, Neukirch, Lang, ...]

10. **The Hilbert symbol.** a "local" invariant with "global" properties [Cassels-Frohlich, Neukirch, ...]

11. **Newton polygons.** A very useful gadget for factoring polynomials. Fun and of theoretical importance too. [Gouvea's book on p -adic numbers].

12. **Euler's Idoneal numbers.** these are the negative discriminants for which there is only one class per genus. It is expected that the 65 known ones are it, but there could be one more (but only if the Generalized Riemann Hypothesis is false). [Cox, and various articles].

13. **The Shimura reciprocity law.** Given a function in the modular function field, this law tells us how the Galois group acts on it and on its values at Heegner points in the upper half-plane (these values generate abelian extensions of the corresponding imaginary quadratic field.) [Shimura's book on automorphic forms, Stark's paper in *Advances in Math* 1980]

14. **The Stark conjectures.** Throughout the 1970's Stark made a number of increasingly precise conjectures about special values of Artin L-functions. Many generalizations have ensued. Beside the case of abelian extensions of \mathbb{Q} or of imaginary quadratic fields, extremely little has been proved, but much convincing numerical evidence exists. [Stark's paper in *Adv. in Math*, Tate's book on Stark conjectures]

15. **Cyclotomic units and the Stickelberger ideal.** Kummer could already write down units in cyclotomic fields which gave "almost" the whole unit group. There is also an explicit ideal in the group ring $\mathbb{Z}[G]$, where G is the Galois group of the cyclotomic field K in question, which kills the class group of K . [Washington's book on cyclotomic fields].

16. **Kummer theory.** If K is a number field with w roots of unity in K , then abelian extensions of K of exponent w can be very well understood in terms of elements of K^*/K^{*w} . [Short article in Cassels-Frohlich].

17. **The (first or second) Kronecker limit formula.** This is purely a theorem of analysis with a tremendous application to determining class numbers of abelian extensions of imaginary quadratic

fields (and proves Stark's conjecture for same). [Siegel's book Advanced Analytic number theory, Stark's adv. in math article 1980].

18. **Heegner's 1952 paper.** In this paper, Heegner proved the class number 1 problem for imag quad fields but no one believed it for more than a decade. He also introduced the method of Heegner points, of great significance in the 80s and beyond. [Heegner's paper itself and articles by Birch, Deuring, Stark].

19. **Group cohomology.** A very powerful and useful technique in much of algebra; of particular importance in the modern treatment of class field theory. [Cassels-Frochlich, chapter on group cohomology].

20. **The Kronecker-Weber theorem.** It states that if K/\mathbb{Q} is a finite abelian extension, then $K \subseteq \mathbb{Q}(\exp(2\pi i/n))$ for some n . [Washington's book]

21. **The Stark-Odlyzko discriminant bounds.** Using the functional eqn of the Dedekind zeta function, Stark introduced a method perfected by his student Odlyzko for giving improved bounds of Minkowski type for discriminants of number fields. These are believed to be quite sharp and in favorable situations can be used to give bounds for class numbers. [Articles by Stark and Odlyzko].

22. **Iwasawa theory.** In the tower of extensions $\mathbb{Q}(\exp(2\pi i/p^k))$ where p is a fixed prime number, there is an explicit formula for the p -part of the class number! This fruitful discovery of Iwasawa played a very important role in much of algebraic number theory in the last forty years. [Iwasawa's original article and Washington's book].

23. **The use of CM elliptic curves in elliptic curve cryptography.** There is a kind of cryptosystem based on elliptic curves. For such a system, one choose a very large prime p and one looks for an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ with a prescribed number of points. One of the most efficient ways for doing this is to find an elliptic curve with complex multiplication over \mathbb{C} whose reduction modulo p is the desired curve. [Frey et al, handbook of elliptic curve cryptography].