

## SOME SUGGESTED TOPICS FOR FINAL PAPER

1. *The number field sieve (NFS)*: This is a method for factoring integers which utilizes extensive computations in number fields. It is currently the fastest known general method for factoring large integers.
2. *Jacobi sums and primality testing*: The APR test was the first deterministic primality testing algorithm which ran in subexponential time. It uses the arithmetic of cyclotomic fields.
3. *The Riemann hypothesis for algebraic curves*: This is a theorem of Weil related to counting the number of solutions  $(X, Y)$  with  $X, Y \in \mathbf{F}_{p^n}$  to a polynomial equation  $F(X, Y) = 0$  as  $n$  tends to infinity.
4. *The cubic reciprocity law*: After establishing quadratic reciprocity, Gauss discovered the law of cubic reciprocity, which is based on arithmetic in the ring  $\mathbf{Z}[\omega]$ , where  $\omega$  is a cube root of unity.
5. *Dirichlet's class number formulae*: There are some amazing analytic formulas due to Dirichlet for the class number of a quadratic field.
6. *Regular and irregular primes*: Kummer proved some amazing results connecting class numbers of cyclotomic fields, Bernoulli numbers, and special values of the Riemann zeta function.
7. *Binary quadratic forms and Gauss' composition law*: There is a useful and fascinating relationship between the ideal class group of a quadratic field and composition of binary quadratic forms.
8. *Extensions of Kummer's decomposition theorem*: How to factorize  $p\mathcal{O}_K$  when  $p$  divides the index of  $\mathbf{Z}[\theta]$  in  $\mathcal{O}_K$ ?
9. *Riemann-Roch for number fields*: The Riemann-Roch formula from the theory of Riemann surfaces (or algebraic curves) has an interesting analogue for number fields.

10. *The Cohen-Lenstra heuristics*: There are some interesting predictions about how frequently various class numbers and class groups should occur among all number fields.
11. *The class group factoring method*: There is a method for factoring integers due to Schnorr and Lenstra which uses ideal class groups and is notable for the small amount of memory it uses.
12. *Coding theory and geometry of numbers*: There are important applications of Minkowski's geometry of numbers to coding theory, especially to sphere-packing problems.
13. *The Hasse (local/global) principle*: An important goal of modern number theory is to quantify the failure of the "local/global principle".