Final Project: Class numbers and binary quadratic forms

Written by Jonathan Hanke

February 14, 2005

Abstract

In class, one of our main goals has been to study primes, and to prove unique prime factorization for $\mathbb{Z}$. However not all number systems we enounter will be as simple, and it may happen that unique prime factorization fails. The *class number* $h \in \mathbb{N}$ is a number which tells us how far we are from having unique prime factorization (with $h = 1$ meaning that unique factorization holds), and so it is important to be able to compute h, and decide when $h = 1$. This question was first addressed by Gauss, who computed these class numbers by studying quadratic forms $ax^2 + 2bxy + cy^2$ for some $a, b, c \in \mathbb{Z}$. Your project should describe this connection, and use it to compute the class number of the integers in any quadratic number field $\mathbb{Q}(\sqrt{D})$, and perhaps for other number systems in $\mathbb{Q}(\sqrt{D})$. **[3-4]**

The following is a rough outline which may be useful in thinking about/organizing your project. Good general references are [1], [2, Chapters 7–9, 12, 13], [6, Chapters 7 and 8], [5, Chapter VI], and [3, pp354–366]. It is also briefly mentioned in [7, §13.1]. There is also an interesting discussion in [4, pp 23–73] from a more historical point of view. If you have any questions about your project and/or readings, feel free to let me know, and we can setup a time to talk about it. Have Fun! =)

1. **Equivalence of binary quadratic forms**
2. **Reduction theory of positive definite forms**
3. **Reduction theory of negative definite forms**
4. **Ideals in the integers $\mathcal{O}_k$**
5. **Unique prime ideal factorization**
6. **Connection with ideals in quadratic number fields**

References

[1] Duncan A. Buell. *Binary quadratic forms.* Springer-Verlag, New York, 1989. Classical theory and modern computations.

[2] Harvey Cohn. *Advanced number theory.* Dover Publications Inc., New York, 1980. Reprint of *A second course in number theory*, 1962, Dover Books on Advanced Mathematics.

[3] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[4] David A. Cox. *Primes of the form $x^2 + ny^2$.* A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[5] H. Davenport. *The higher arithmetic.* Cambridge University Press, Cambridge, seventh edition, 1999. An introduction to the theory of numbers, Chapter VIII by J. H. Davenport.

[6] Harold M. Edwards. *Fermat's last theorem*, volume 50 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996. A genetic introduction to algebraic number theory, Corrected reprint of the 1977 original.

[7] Jeffrey Stopple. *A primer of analytic number theory.* Cambridge University Press, Cambridge, 2003. From Pythagoras to Riemann.