Lethbridge Number Theory and Combinatorics Seminar

Monday — February 12, 2018
Room: B543 Time: 12:00 to 12:50 p.m.

Ha Tran

University of Calgary

Reduced Ideals from the Reduction Algorithm

Abstract: Reduced ideals of a number field F have inverses of small norms and they form a finite and regularly distributed set in the infrastructure of F. Therefore, they can be used to compute the regulator and the class number of a number field [5, 3, 2, 1, 4]. One usually applies the reduction algorithm (see Algorithm 10.3 in [4]) to find them. Ideals obtained from this algorithm are called 1-reduced. There exist reduced ideals that are not 1-reduced. We will show that these ideals have inverses of larger norms among reduced ones. Especially, we represent a sufficient and necessary condition for reduced ideals of real quadratic fields to be obtained from the reduction algorithm.

[1] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990.

[2] Johannes Buchmann and H. C. Williams. On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. *Math. Comp.*, 50(182):569–579, 1988.

[3] H. W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Number theory days, 1980 (Exeter, 1980)*, volume 56 of *London Math. Soc. Lecture Note Ser.*, pages 123–150. Cambridge Univ. Press, Cambridge, 1982.

[4] René Schoof. Computing Arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[5] Daniel Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)*, pages 217–224. Univ. Colorado, Boulder, Colo., 1972.

EVERYONE IS WELCOME!

Visit the seminar web page at
http://www.cs.uleth.ca/∼nathanng/ntcoseminar/

Pacific Institute *for the* Mathematical Sciences