CPSC 499 / MATH 499 Approval

Prerequisite Permission of the instructor (*i.e.,* me).

Check-list If you have two or more of

- MATH 320;
- one of MATH 420, MATH 421, or an equivalent MATH 499;
- CPSC 281, or a B or better in CPSC 200, or an A^{+++} in CPSC 101;
- an A^{-} or better in MATH 223, and (or?) A^{-} or better in MATH 220;
- an intense burning desire to know how to factor polynomials in sub-exponential time;

you are probably qualified to take this course. If you are interested, talk to me. If you don't quite have two, but are still intensely interested, talk to me anyway.

Topics This course covers a very small piece of the general area of symbolic (*i.e,* exact) mathematical computation. I shall discuss how to implement and perform arithmetic on arbitrary size integers, polynomials, rationals, and possibly more exotic objects such as matrices. We will look at both practical and theoretical efficiency of algorithms.

From the mathematical point of view, most of the objects that we shall discuss are *rings*, and I shall attempt to explain what rings and ring homomorphisms are, and why they are important for efficient computation (à la Chinese remainder theorems, integer Fast Fourier transforms, and Hensel lifting). I shall attempt to keep the mathematical exposition self-contained, but a willing to accept and reason with abstract algebraic ideas is essential.