MAT C15: REMARKS ON FINAL EXAM

The final exam is cumulative, i.e. you should be comfortable with all material taught in the course. Unless otherwise specified, you may refer to any theorem proved in lecture, *without* re-proving it on the exam. However, questions on the exam may ask you to prove theorems from lecture.

The topics below are the ones we have covered since the midterm; most of the final will concentrate on these, although topics from before the midterm are also fair game.

(1) Modular arithmetic: addition, subtraction, and multiplication in $\mathbb{Z}_n$; multiplication, division, and exponentiation in $\mathbb{Z}_n^\times$. (Writing out multiplication tables for $\mathbb{Z}_n^\times$.) Definition of $a \equiv b \pmod{n}$. Euler's theorem, Fermat's Little Theorem. Definition and properties of the function $\varphi(n)$.

(2) The order of an element of $\mathbb{Z}_n^\times$: definition, properties (e.g. it divides $\varphi(n)$.) Definition of primitive root.

(3) For every prime p, $\mathbb{Z}_p^\times$ has a primitive root. **You will be asked to prove this on the exam.**

(4) The Diffie-Hellman Key Exchange algorithm; how it works, why it's secure, circumstances under which it's not secure.

(5) Equations over $\mathbb{Z}_n^\times$ (e.g. find all solutions to $x^2 = 1$ in $\mathbb{Z}_n^\times$). The number of solutions of a polynomial congruence. Wilson's Theorem.

(6) The Legendre symbol; you should be able to evaluate it using Euler's Criterion or Quadratic Reciprocity.

(7) Quadratic Reciprocity. **You will be asked to state and prove this on the exam.**