MME 529 Summer 2015

Number Theory & Algebra

John Goulet PhD goulet@wpi.edu

Part One

Division, Factoring, Primes
Euclid's Algorithm
Pythagorean Triples
Mersenne Primes
Diophantine Equations
Fermat's Last Theorem

Part Two

Congruences; modulo arithmetic
$\mathbf{Z}_n$ vs $\mathbf{Z}_p$
Fields and Rings
Fermat's Little Theorem

Exam

Part Three

RSA Encryption

Part Four

Elliptic Curve Cryptography – 20th century approaches

Grade based on:

Homework	70%
Exam	20%
Historical Presentation	10%

Resources:

Text: *Elementary Number Theory* 7th ed David Burton

Maple Software, esp *numtheory* library. Access via Remote Desktop

The Proof (video) on Andrew Wiles and FLT