

Pries: 405 Number Theory: Spring 2020: Project topics

Deadlines:

Mon 3/23: 3 project choices due

Fri 3/27: computer lab due

Fri 4/3: Midterm 2 postponed. Rough draft of project due.

Continue with reading and warm-up problems.

Possible topics for a project:

1. Sections of Stillwell that we are not covering:

- (a) Taxi-cab numbers and $x^3 + y^3 = z^3 + w^3$, Section 7.5.
- (b) Fermat's Last Theorem in exponent 3, Sections 7.6-7.7.
- (c) Solving $p = x^2 + dy^2$ and quadratic reciprocity, Chapter 9, 12.8.
- (d) Non-commutative rings, Matrix rings.
- (e) Algebraic integers, Section 10.3

2. Class groups:

- (a) The growth of the size of the class group of $\mathbb{Q}(\sqrt{-d})$ as d grows.
- (b) Minkowski theory about the number of lattice points in spheres.
- (c) The class group of a quadratic field is finite.
- (d) Cohen-Lenstra heuristics - conjecture about how often a prime p divides the size of the class group.

3. Quadratic Forms

- (a) Applications of quadratic forms to signal processing, from Stanford. <https://cosmolearning.org/lectures/symmetric-matrices-quadratic-forms-and-matrix-norm/>
- (b) Vector form of multivariable quadratic approximation (Khan academy)
- (c) Quadratic reciprocity and solving quadratic forms
- (d) Sums of squares, cubes, and higher powers.

4. Elliptic Curves

- (a) The Nagell-Lutz theorem
- (b) Heights of rational points
- (c) Mordell's theorem
- (d) Hasse-Weil bound
- (e) Sato-Tate conjecture
- (f) Elliptic curve signature scheme
- (g) Elliptic curve cryptography

- (h) Cryptography based on isogeny graphs of supersingular elliptic curves
5. Groups and vector spaces by Benedict Gross,
from Harvard <https://cosmolearning.org/courses/abstract-algebra/>
Chapters that are closely related to our class.
33-34 Gauss' lemma and Eisenstein's criteria (irreducibility of polynomials)
36 Dedekind domains and ideal class groups
Chapters that are reasonably related to our class.
13-14 Orthogonal groups and geometry
15-16 Groups of motions
17-22 Group actions
6. Abstract algebra: groups, rings and fields, with Math Doctor Bob
<https://cosmolearning.org/courses/abstract-algebra-groups-rings-fields/>
Chapters that are closely related to our class.
50,55 Finite fields
62-63 Gauss' lemma and Eisenstein's criteria (irreducibility of polynomials)
64, 66, 67, 69, Number fields and extensions
73-75, 79, Roots of polynomials and splitting fields
77 Cyclotomic polynomials
78 Mobius inversion formula
79-83 Galois correspondence
Chapters that are reasonably related to our class.
19-22 Automorphisms of groups
23-24 Groups of order 8 and semi-direct products
27-28 Cayley's theorem
32-35 Cauchy's theorem
37-43 Sylow theorems
7. Documentaries (these might not be enough without other sources)
Fermat's Last Theorem <https://cosmolearning.org/documentaries/fermats-last-theorem-1996/>
Hamilton to Boole: quaternions to astrophysics cosmolearning.org/documentaries/topics-in-the-history-of-mathematics-the-liberation-of-algebra-1460/
Turing - breaking the code <https://cosmolearning.org/documentaries/breaking-the-code-1175/>
The music of the primes <https://cosmolearning.org/documentaries/the-music-of-the-primes-481/>

8. Algebraic Geometry

Toric geometry <https://cosmolearning.org/courses/basic-algebraic-geometry-with-dr-bob/>

(harder) <https://cosmolearning.org/courses/basic-algebraic-geometry-varieties-morphisms-local-rings-function-fields-nonsingularity/>

(harder) representation theory <https://cosmolearning.org/courses/representation-theory-finite-groups/>