SOME IDEAS FOR 4400 FINAL PROJECTS

1. Project parameters

You can work in groups of size 1 to 3. Your final project should be a paper of 6 to 10 double spaced pages in length. Ideally it should touch on some elements of exposition, history and also mathematics (theorems and proofs). It need not (and probably will not) contain any *new* mathematics, but it will not be a good project if the mathematics – including its presentation – is taken from any one source.

2. Some project ideas

2.1. **Schuh's Divisor Game.** Report on the history of this game, and write a computer program that plays it better than you (or I) do.

Comment: This was done by a student in the 2009 course, and I still have the program. It's fun!

2.2. **Nonunique factorization in the ring $\mathbb{R}[\cos\theta, \sin\theta]$ of trigonometric polynomials.** See [Tr88], [Cl09], [FID].

2.3. **Mordell's proof of Holzer's theorem on minimal solutions to Legendre's equation.** See [Mo69], [CM98], [Nu10].

2.4. **Find all integers of the form $x^2 + 5y^2$.** This is significantly harder than the cases we looked at in class!

2.5. **Study of isotropic binary quadratic forms: $ax^2 + bxy$.** A quadratic form $f(x_1, \ldots, x_n)$ is isotropic if there is a nonzero $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $f(x_1, \ldots, x_n) = 0$. A binary quadratic form $f(x, y) = Ax^2+Bxy+Cy^2$ is isotropic iff $\Delta := B^2 - 4AC$ is a perfect square. If so, after a change of variables, f can be brought into the form $Ax^2 + Bxy$. For instance, the form $f(x, y) = x^2 - y^2$ is isotropic, and after a change of variables it can be brought into the form $x^2 + 2xy = x(x + 2y)$. Notice that this makes it a little easier to show that the form represents precisely those integers that are not exactly divisible by 2.

For some reason, most of the modern theory of binary quadratic forms excludes the isotropic case. Paul Pollack and I have recently explored it, and it is nontrivial and interesting and also somewhat easier than the other cases. For instance, one can determine all integers represented by $2x^2 + 5xy$ using only elementary congruence arguments, and one can show that for the form $x^2 + 5xy$, congruence arguments are not sufficient: there are integers n such that $x^2 + 5xy$ represents n modulo N for all N but does not represent n over $\mathbb{Z}$.

2.6. **Discuss the history of quadratic reciprocity.** See [Cx], [W], [Lem]

2.7. **Zolotarev's proof of quadratic reciprocity using signs of permutations.** . This is described in the course text...but not very well. The paper on which the discussion in the text is based is [BC12]. But this makes things much more algebraically fancy than necessary. The source I found easiest to understand is [Ba13].

2.8. **Discuss the complexity of any/all of the following algorithms: mod p powering algorithm, the Euclidean algorithm, the Jacobi symbol algorithm.** See [Co].

2.9. **Investigate algorithms for reprsenting an integer as a sum of squares.** We have determined exactly which integers are sums of 2 squares. Later in the course we will prove which integers are sums of four squares (Lagrange's theorem) and state without proof which integers are sums of three squares (Legendre-Gauss Theorem). But these methods do not give efficient algorithms for actually finding such a representation. E.g. if $p \equiv 1 \pmod 4$ is a large prime, we know there are $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$...but how to find them? There is an obvious trivial and error approach: compute $p - 1^2$, $p - 2^2$, $\ldots$ until we get a perfect square. But this is very slow. Find out how to do better! See [Co], [PT18].

2.10. **Primes of the form $x^2 - Dy^2$: an elementary approach.** I worked out an aggressively elementary approach that works to find primes represented by these forms for certain further values of D: it is based on a lemma of Thue-Vinogradov, whose proof uses the pigeonhole principle. See [Cl-TV].

2.11. **The linear Diophantine problem of Frobenius.** This is the following problem, which we've seen before: let $a_1, \ldots, a_n$ be coprime positive integers, let N be a positive integer and let

$$r(a_1, \ldots, a_n; N) = \#\{(x_1, \ldots, x_n) \in \mathbb{N}^n \mid a_1x_1 + \ldots a_nx_n = N\}.$$

Study this function. In particular, determine when it is positive. This is a rich problem on which hundreds of people (including me) have written papers. It is a nice problem because (i) it is difficult or impossible to solve in general but (ii) not so hard to prove *something* about. See [Al], [AC05].

2.12. **Solution of systems of linear Diophantine equations.** We discussed methods leading to a complete solution of any single linear Diophantine equation

$$a_1x_1 + \ldots + a_nx_n = N.$$

It is also natural to study *systems* of Diophantine equations: i.e., simultaneous solutions to a set of polynomial equations:

$$P_1(x_1, \ldots, x_n) = \ldots = P_r(x_1, \ldots, x_n) = 0.$$

Discuss the (simplest) case in which each polynomial P_i is linear. (To solve the problem you will need to combine elementary number theory with some linear algebra, so you should only consider this project if you know and enjoy linear algebra.) Try to come up with "natural problems" that lead one to solve a system of linear Diophantine equations. One famous example is Part I of the Cattle Problem of Archimedes.

2.13. **Survey of numbers known to be irrational and/or transcendental.**

2.14. **FLT(4) and elliptic curves.** Fermat's proof of Fermat's Last Theorem for $n = 4$ is a bit mysterious, but it can be recast as an argument involving the elliptic curve $y^2 = x^4 - 1$. Explain this. [Kn], [W].

2.15. **Hasse norms versus Euclidean norms on quadratic rings.** We defined a Euclidean norm $N : R \to \mathbb{N}$ on a domain R and observed that the existence of such a norm implies that R is a PID. However the converse is not true.
a) (Motzkin) Show that $R_{-19} := \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID that does not admit a Euclidean norm.
b) There is another type of multiplicative norm, a **Hasse norm** $N : R \to \mathbb{N}$, which still implies that R is a PID and for which the converse is true. Show that our standard norm

$$N(x + y\sqrt{-19}) = x^2 + 19y^2$$

is a Hasse norm on R_{-19}.
c) The complete list of imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ for which the ring R_D of algebraic integers of K is a PID is

$$D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

It is known that the standard norm is Euclidean iff $|D| < 19$, whereas for $D = -19$ the standard norm is a Hasse norm. What about $D = -43, -67, -163$: are the standard norms Hasse norms?[1] [Ca88], [Cl18].

2.16. **The negative Pell equation $x^2 - Dy^2 = -1$.** Investigate conditions on its solvability and relate it to continued fractions.

2.17. **Erudite proofs of the infinitude of primes.**
a) Try to adapt Euclid's proof to some other rings R. It works especially nicely in the ring $k[t]$ of polynomials in one variable over a field.
b) Fill in the details of Larry Washington's proof, as discussed briefly in the course text.
c) Say something about Furstenberg's topological proof. See e.g. [Cl17]. Note that Furstenberg was 20 years old when his article was *published* in the *Monthly*, so it was probably written while he was a teenager.

[1] In the 2009 version of this project, there was a footnote saying that I didn't know the answer and also didn't know whether it was a true open problem. I do know the answer now! It appears in [Cl18].

2.18. **Report on Green-Tao and recent updates.** In 2004, Ben Green and Terry Tao proved an instantly classical result: there are arbitrarily long arithmetic progressions in the primes. A result like this deserves a first class PR team: it is easy enough to understand that every educated adult should be exposed to it. Lend a hand in this regard:
a) Write a three to five sentence summary of the Green-Tao Theorem that any literate adult can read, understand and have a non-negative response to.
b) Write a one to two page article, suitable for publication in a newspaper, with the following title: "Where are they now: arithmetic progressions 14 years after Green-Tao." (Once you write what would be reasonable article with that title, you can change the title!)
c) Write a five page paper describing Green-Tao and recent updates, at whatever level pleases you (but be explicit about your intended audience). Deifnitely state actual theorems and conjectures. Try to work in a few simple proofs, e.g. explaining why one result or conjecture implies another. Of course it is out of the question to give complete proofs of any of the real results in this area in this amount of space.

2.19. **The phenomenon of almost square root error.** Read the first two sections of [Ma08]. Don't expect to understand it all; concentrate on the parts you find interesting. Find another number theoretic problem where there is an "expected answer," and as Barry does in his article, do some computations and examine the error terms.

References

[AC05] G. Alon and P.L. Clark, *On the number of representations of an integer by a linear form.* Integers Vol. 8 (2005), Article 05.5.2, `https://cs.uwaterloo.ca/journals/JIS/VOL8/Clark/clark80.html`

[Al] J.L. Ramírez Alfonsín, *The Diophantine Frobenius problem.* Oxford Lecture Series in Mathematics and its Applications, 30. Oxford University Press, Oxford, 2005.

[Ba13] M. Baker, `https://mattbaker.blog/2013/07/03/quadratic-reciprocity-and-zolotarevs-lemma/`

[BC12] A. Brunyate and P.L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity.* Ramanujan J. 37 (2015), 25-50.

[Ca88] O.A. Cámpoli, *A principal ideal domain that is not a Euclidean domain.* Amer. Math. Monthly 95 (1988), 868-871.

[Cl09] P.L. Clark, *Elliptic Dedekind domains revisited.* Enseignement Math. 55 (2009), 213–225.

[Cl17] P.L. Clark, *The Euclidean criterion for irreducibles.* Amer. Math. Monthly 124 (2017), 198216.

[Cl18] P.L. Clark, *Rabinowitsch times six.* `http:alpha.math.uga.edu/~pete/Rabinowitsch.pdf`

[Cl-TV] P.L. Clark, *Thue-Vinogradov and primes of the form $x^2 + Dy^2$*, `http://alpha.math.uga.edu/~pete/thuelemmav7.pdf`.

[CM98] T. Cochrane and P. Mitchell, *Small solutions of the Legendre equation.* J. Number Theory 70 (1998), 62–66.

[Co] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[Cx] D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication.* New York: John Wiley & Sons, Inc.; 1989.

[FID] P.L. Clark, *Factorization in integral domains.* `http://alpha.math.uga.edu/~pete/factorization2010.pdf`

[Kn] A.W. Knapp, Knapp, *Elliptic curves.* Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[Lem] F. Lemmermeyer, *Proofs of the quadratic reciprocity law.* `https://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`

[Ma08] B. Mazur, *Finding meaning in error terms.* Bull. Amer. Math. Soc. (N.S.) 45 (2008), 185-228.

[Mo69] L.J. Mordell, *On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$.* J. Number Theory 1 (1969), 1–3.

[Nu10] L.M. Nunley, *Geometry of numbers approach to small solutions of the extended Legendre Equations*, 2010 UGA master's thesis. `http://alpha.math.edu/~pete/Laura_Nunley_Master_Thesis.pdf`

[PT18] P. Pollack and E. Treviño, *Finding the four squares in Lagrange's theorem.* `pollack.uga.edu/finding4squares.pdf`

[Tr88] H.F. Trotter, *An overlooked example of nonunique factorization.* Amer. Math. Monthly 95 (1988), no. 4, 339–342.

[W] A. Weil, *Number theory. An approach through history from Hammurapi to Legendre*. Reprint of the 1984 edition. Modern Birkhäuser Classics, Boston, MA, 2007.