

## SOME IDEAS FOR FINAL PROJECTS

PETE L. CLARK

### 1. PROJECT IDEAS

1.1. **Write a computer program that plays Schuh's divisor game better than you (or I) do.**

1.2. **Nonunique factorization in the ring  $\mathbb{R}[\cos \theta, \sin \theta]$  of real trigonometric polynomials.**

Reference: H.F. Trotter, *An Overlooked Example of Nonunique Factorization*, American Mathematical Monthly 95 (1988), 339–342.

<http://www.math.uga.edu/~pete/trotter.pdf>

1.3. **Mordell's proof of Holzer's Theorem on Minimal Solutions to Legendre's Equation.**

Reference: L.J. Mordell, *On the Magnitude of the Integer Solutions of the Equation  $ax^2 + by^2 + cz^2 = 0$* , Journal of Number Theory 1 (1969), 1–3.

<http://www.math.uga.edu/~pete/Mordell11968.pdf>

1.4. **Find all integers of the form  $x^2 + Dy^2$  for  $D = \pm 2, 3$ .**

1.5. **Find all integers of the form  $x^2 + 5y^2$ .**

Remark: This is significantly harder than the cases we looked at in class.

Reference: D.A. Cox, *Primes of the form  $x^2 + ny^2$* .

1.6. **Discuss the history of quadratic reciprocity.**

References: D.A. Cox, *Primes of the form  $x^2 + ny^2$* .

André Weil, *Number Theory: An Approach Through History From Hammurapi to Legendre*.

1.7. **Discuss the complexity of the following algorithms: powering algorithm, Euclidean algorithm, Jacobi symbol algorithm.**

Reference: Henri Cohen, *A Course in Computational Algebraic Number Theory*.

1.8. **Investigate algorithms for expressing an integer as a sum of squares.**

We have determined exactly which integers are sums of two squares. Later on 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 any of these representations. E.g, if  $p \equiv 1 \pmod{4}$  is a large prime number, we know that there exist  $x, y \in \mathbb{Z}$  such that  $p = x^2 + y^2$ ? There is an obvious trial and error approach to finding  $x$  and  $y$ : compute  $p - 1^2, p - 2^2, \dots$  until we get a perfect

square. But this is very slow. Find out how to do better!

Reference: Henri Cohen, *A Course in Computational Algebraic Number Theory*.

**1.9. Non/integrality of partial sums of  $\sum_{n=1}^{\infty} a_n$  with  $a_n \in \mathbb{Q}$ .**

We proved that for all  $N \geq 2$ ,  $\sum_{n=1}^N \frac{1}{n} \notin \mathbb{Z}$ . There must be similar non-integrality results for other series with rational coefficients, e.g. for partial sums of the  $p$ -series  $\sum_{n=1}^{\infty} \frac{1}{n^p}$  for  $p \in \mathbb{Z}^+$ . What interesting results can you find, either by a literature search (and this is one case where I don't myself know what the literature has to say about this, so it is interesting to me) or by figuring things out yourself? Feel free to change the statement of the problem a little bit if it leads somewhere: e.g. start the sums somewhere other than at  $n = 1$ , skip some terms, etc.

**1.10. The linear Diophantine problem of Frobenius.**

This is a fancy name for the following problem which we have seen before: let  $a_1, \dots, a_n$  be positive integers which are coprime as a set. What can be said about the set of positive integers  $N$  of the form  $a_1x_1 + \dots + a_nx_n = N$  for  $x_1, \dots, x_n \in \mathbb{N}$ ? (Or in  $\mathbb{Z}^+$ ?) What can be said about the function  $r(a_1, \dots, a_n; N)$  which counts the number of representations of  $N$  by the above linear form? This is a rich problem on which hundreds of people (including me) have written papers, in large part because it is difficult or impossible to solve in general but not so hard to prove *something* about. See Homework Problem 2.9 and Theorem 15 of [Introduction; The Fundamental Theorem and Some Applications] for things to prove that would make a nice project.

**1.11. Solution of systems of linear Diophantine equations.**

We discussed methods leading to a complete solution of any single linear Diophantine equation

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

It is also natural to study systems of Diophantine equations, i.e., simultaneous integer solutions to a finite set  $P_1(x_1, \dots, x_n), \dots, P_m(x_1, \dots, x_n)$  of polynomial equations. Discuss the simplest case in which each polynomial  $P_i$  is linear. (To solve the problem you will need to combine the elementary number theory we have already seen with some linear algebra, so only consider doing this project if you know and enjoy linear algebra.) Try to come up with some examples of "natural problems" which lead one to solve a system of linear Diophantine equations. One famous example here is Part I of the Cattle Problem of Archimedes.

**1.12. Survey of numbers known to be irrational and/or transcendental, especially  $e$  and  $\pi$ .**

**1.13. Educational project: the rational roots theorem.**

The rational roots theorem is an important and useful result of high school algebra. Nevertheless, after a decade of teaching at the university level I have found that very few college students remember it, and still fewer ever think to try to use it. I am pretty sure that this result does appear in most Algebra II textbooks and on most syllabi for high school algebra (but please check me on this), so there is a pedagogical problem here: students are being exposed to this result, but they are

not learning it.

Your project is to address this pedagogical problem. There are several aspects:

- Research the place of the rational roots theorem in state and national curricula.
- Try to figure out why students are not remembering this theorem.
- Write a treatment of the rational roots theorem that is accessible and appealing to a high school student. Definitely give some proof/explanation of the result, but in a way which you think will be appropriate for a high school student. Recall that the proof of this theorem uses unique factorization in  $\mathbb{Z}$ , but in a way that could be underplayed or even swept under the rug, if you think that is best. Try to include some snappy applications of the rational roots theorem, for instance to show things like the irrationality of  $\sqrt{n}$  for  $n$  an integer which is not a perfect square.

#### 1.14. FLT(4) and elliptic curves.

Fermat's proof of Fermat's Last Theorem for  $n = 4$  is mysterious, but it can be recast as an argument involving the elliptic curve  $y^2 = x^4 - 1$ . Explain this.

References:

Anthony Knapp, *Elliptic Curves*.

André Weil, *Number Theory: An Approach Through History From Hammurapi to Legendre*.

**1.15. Computer implementation of integral points on conics.** Write a computer program which accepts as input nonzero integers  $a, b, c$  and returns either:

- The smallest nontrivial integral solution  $(x, y, z)$  to  $ax^2 + by^2 + cz^2 = 0$ , or
- A positive integer  $N$  such that  $ax^2 + by^2 + cz^2 \equiv 0 \pmod{N}$  has no primitive solutions.

#### 1.16. Euclidean quadratic rings.

Let  $D$  be a squarefree integer  $\neq 0, 1$ , let  $K = \mathbb{Q}(\sqrt{D})$ , and let  $\mathbb{Z}_K$  be the ring of integers of  $K$ :  $\mathbb{Z}_K = \mathbb{Z}[\sqrt{D}]$  if  $D \equiv 2, 3 \pmod{4}$ ,  $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$  if  $D \equiv 1 \pmod{4}$ .

a) For which values of  $D$  is the ring  $\mathbb{Z}_D$  Euclidean with respect to the standard norm  $N(x + y\sqrt{D}) = |x^2 - Dy^2|$ ?

A complete answer to this is **known**, but the full proof is well beyond the scope of a project. A reasonable goal would be to state the full answer, with proper attributions and history, and then to prove some of it, going a bit beyond what we did in class and in the notes.

b) For which values of  $D$  does the ring  $\mathbb{Z}_K$  admit a generalized Euclidean norm in the sense of [Quadratic Rings, p. 5]?

The complete answer to this is **unknown**, although there are many interesting results to report on. For instance, the ring  $\mathbb{Z}[\sqrt{14}]$  was shown to admit a generalized Euclidean norm in the year 2004!

Further remarks: In that there are many different things to report on, this would be a good project for more than one person to work on.

#### 1.17. Hasse norms versus Euclidean norms on quadratic rings.

We defined a generalized Euclidean norm  $N : R \rightarrow \mathbb{N}$  on an integral domain  $R$

and observed that the existence of such a norm implies that  $R$  is a PID. The converse is not true, however:

a) Show that  $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ , the ring of integers of  $\mathbb{Q}(\sqrt{-19})$ , is a PID but nevertheless does not carry a generalized Euclidean norm.

b) There is another type of multiplicative norm, a **Hasse norm**,  $N : R \rightarrow \mathbb{N}$ , which still implies PID and for which the converse is true: any PID carries some multiplicative Hasse norm. Show that in fact the standard norm  $N(x + y\sqrt{-19}) = x^2 + 19y^2$  is a Hasse norm on  $\mathbb{Z}[\sqrt{1 + \sqrt{-19}}]$ .

c) The complete list of rings of integers of imaginary quadratic fields which are PIDs is  $K = \mathbb{Q}(\sqrt{D})$  for  $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$ . It is known that the standard norm is a Euclidean norm iff  $|D| < 19$ , whereas for  $|D| \geq 19$  it is not Euclidean. Above you were asked to show that when  $D = -19$  the standard norm is Hasse. What about  $D = -19, -43, -67, -163$  – are the standard norms Hasse norms?<sup>1</sup>

References: O. Campoli, *A principal ideal domain that is not a Euclidean domain*, American Mathematical Monthly 95 (1988), 868–871,

<http://www.uwlax.edu/faculty/LeDocq/MTH%20412/PID%20not%20ED.pdf>

P.L. Clark, *Factorization in integral domains*,

<http://math.uga.edu/~pete/factorization.pdf>

1.18. **Class groups of number fields.**

1.19. **Computational project: primitive roots and applications.**

1.20. **Primitive roots in  $\mathbb{Z}[\sqrt{-1}]$  and other abstract number rings.**

1.21. **Pedagogical project: introducing university level number theory to high school students.**

If you are a future high school math teacher, I hope you often ask yourself whether and how the university level mathematics you learn can be passed on to your high school students. More than many other areas of advanced mathematics, it is tempting to try to communicate some number theory to high school students, since many of the statements of the results are quite understandable to them. However, it is certainly challenging to present “real” number theory to high school students in a way which will be enjoyable and meaningful for them: on the one hand you have to explain things in very concrete ways, and without relying on any background in abstract algebra. On the other hand, if you don’t convey at least some real understanding, what’s the point? As a personal example, in a fifth grade “math enrichment” class I was taught about the Euclidean algorithm. To me it seemed to be an excuse to have us occupy ourselves doing tedious division and subtraction operations. I am not sure whether we were even told that the output of the EA is the GCD of the two numbers! If so, we were certainly not told why the EA is preferable to finding the GCD by factoring the two numbers, which seemed at the time to be an easier and more sensible thing to do.

---

<sup>1</sup>I don’t know the answer to this question. Whether it is truly an open problem or not I can’t say, but I posted this question on a math research newsgroup a few weeks ago and have not gotten an answer yet.

**1.22. Quadratic reciprocity: other proofs.**

There are amazingly many different proofs of quadratic reciprocity. The one I am presenting in class is the one that I think is the shortest and most enlightening for students with a background in undergraduate algebra but without a background in graduate level algebraic number theory. Write a project discussing some of the various different proofs which have been given over the years – try to talk about ones which use very different ideas – and give one or two of them in detail. Some notable ones include: a) Gauss’s six proofs.

b) Eisenstein’s proof.

c) Zolotareff’s proof.

d) The Duke-Hopkins<sup>2</sup> reciprocity law.

To get a sense of what is out there, see

<http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html>

**1.23. Gauss sums.**

**1.24. The negative Pell equation:**  $x^2 - Dy^2 = -1$ .

**1.25. Representation numbers for sums of squares.**

a) Discuss, with proof, the exact formula for  $r_2(n) = \#\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}$ .

b) Discuss, with proof, the exact formula for

$$r_4(n) = \#\{(x, y, z, w) \in \mathbb{Z}^4 \mid x^2 + y^2 + z^2 + w^2 = n\}.$$

c) Say something about similar formulas  $r_k(n)$  for the number of representations of  $n$  as a sum of  $k$  squares for other values of  $k$ .

**1.26. Cyclotomic polynomials.**

a) Show that for all  $n \in \mathbb{Z}^+$ , the cyclotomic polynomial  $\Phi_n(t)$  (whose roots are the distinct primitive  $n$ th roots of unity) is irreducible over  $\mathbb{Q}$ .

b) Use cyclotomic polynomials to show that for any  $n \geq 2$ , there are infinitely many primes  $p \equiv 1 \pmod{n}$ .

**1.27. Counting irreducible polynomials.**

a) Prove Theorem 7.2 in <http://math.uga.edu/~pete/4400arithmetic2.pdf>.

b) Look for other counting results in algebra which can be proved in a similar way.

**1.28. Erudite proofs of the infinitude of primes.**

a) Try to adapt Euclid’s proof to some other rings  $R$ . It works especially nicely in  $k[t]$ , i.e., the polynomial ring in one variable over a field.

b) Fill in the details of Larry Washington’s proof, as described briefly in §1.7 of [The Primes: Infinitude, Density and Substance].

c) Say something about Furstenberg’s topological proof. It doesn’t make much sense to say “fill in the details”, because Furstenberg’s article already contains enough details for someone with a working knowledge of point-set topology to fill in. But there must be an interesting history surrounding the proof: for instance, it was published in Monthly when Furstenberg was 20 years old, so must have been first discovered at least a year or so before that. Note that, so far as I know, Furstenberg remains alive and well, so that contacting him to ask about the history is within

---

<sup>2</sup>Kimberly Spears was an undergraduate at UC Santa Barbara when she and Bill Duke (a distinguished number theorist at UCLA) discovered a result which significantly generalizes quadratic reciprocity. By the time of publication, her surname changed to “Hopkins.” Kim Hopkins is currently a graduate student at the University of Texas.

the realm of possibility.

d) Prove the following fact, and explain why it gives a proof of the infinitude of primes: Let  $R$  be an infinite (commutative) ring with only finitely many units. Show that  $R$  has infinitely many maximal ideals.

e) Find a ring  $R$  for which the result of part c) is the easiest way to see that it has infinitely many prime ideals.

### 1.29. Journalism: report on Green-Tao and recent updates.

In 2004, Ben Green and Terry Tao proved an instantly classic 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 of Primes Five Years After Green-Tao.” (Once you write what would be a reasonable article with that title, you can change the title if you wish.)

c) Write a five-page paper describing Green-Tao and recent updates, at whatever level pleases you the most (but be explicit about your intended audience).<sup>3</sup> Definitely state actual theorems and conjectures. Try to work in a few simple proofs, e.g. explaining why one result or conjecture follows from another. Of course it is out of the question to give complete proofs of any results in this area in this amount of space.

### 1.30. On the Phenomenon of Almost Square Root Error.

a) Read the first 2 sections of B. Mazur’s<sup>4</sup> article *Finding Meaning in Error Terms*: <http://www.ams.org/bull/2008-45-02/S0273-0979-08-01207-X/S0273-0979-08-01207-X.pdf>. Don’t expect to understand it all; concentrate on parts that you find interesting.

b) Find another number theoretic problem where there is an “expected answer”, and, as Barry does in his article, do computations and examine the error terms.

---

<sup>3</sup>Assuming a constant amount of background knowledge, it is generally *easier* to write an article at a higher level than a lower level, since at a lower level you will either need to translate the results into a less technical language, or help the reader through the needed technicalities.

<sup>4</sup>Full disclosure: Barry Mazur was my thesis advisor.