Explorations with Polynomials

MME 529 Project Ideas

William J. Martin, WPI

Abstract: *After having considered polynomials in one or more variables over the real numbers, rational number, integers, integers mod n, we now select team projects that explore how the basic tools can be used.*

1 Project Guidelines

Teams should consist of exactly two students whenever possible. Projects will focus on mathematics: side issues such as history or technology should appear in the oral presentations only when necessary. Most topics will require the team to provide precise mathematical definitions and multiple theorems. At least one proof should be provided in the oral presentation whenever possible. Frequent reference will be made to the text by Gallian and for each concept, several examples will be worked out in detail in the report and, subject to time constraints, examples should be included in the oral presentation. Avoid examples that are already given in the text or on the web; develop your own examples.

Oral presentations should be limited to 20 minutes and should be chock-full of mathematics. To the greatest extent possible, this mathematics should be at the level seen in our text and not at the grade school level.

IMPORTANT: Any project which contains unattributed graphics or plagiarizes examples or text from another source – on paper or on the web – will earn a grade of zero.

2 Suggested Projects

- The ideal of the icosahedron: Explore all polynomials over $\mathbb{R}$ in three variables which vanish at the twelve vertices of the icosahedron. For the Golden Ratio $\varphi = (1+\sqrt{5})/2$, we can take our vertices to be

  $$(\pm 1, \pm\varphi, 0), \quad (0, \pm 1, \pm\varphi), \quad (\pm\varphi, 0, \pm 1).$$

  What can you say about the polynomials $F(x, y, z)$ in $\mathbb{R}[x, y, z]$ satisfying $F(p) = 0$ for every point p in the above set? Explore ideals of other finite sets in Euclidean space, such as the n-dimensional cube, whose vertices are all vectors with entries ± 1.

- Vandermonde determinants: Study Lagrange interpolation and Vandermonde determinants. What does the family of parabolas look like when two parameters (say two of a, b, c or two points on the curve) are fixed? Use this to introduce Shamir's secret sharing scheme:

  Imagine a bank vault 50 years ago. It may be that the bank does not trust any one employee to enter the vault, requiring at least two employees to insert their metal keys simultaneously before the door opens. Nowadays, there are many applications that call for us to limit access to a file or (generically) "secret" to acceptable subsets of an

initial collection of users. The simplest solution to this problem remains among the most elegant. In this project, the team will explore Shamir's secret sharing scheme, how it operates, and the various real-world contexts in which it is used.

- RAID architecture for computer storage: Some beautiful algebra is used to back up storage devices in large computer storage systems. But present-day storage demands are forcing us to think of new, more efficient methods for backing up hard drives. For example, in 2013 it was estimated that Facebook had over 100 PB of storage capacity and was processing 750 TB of data every day. This project will use a WPI masters essay as a text and will introduce the team — and the class — to the number theory behind Redundant Arrays of Independent (or Inexpensive) Disks (RAID). See `http://users.wpi.edu/~martin/THESESPROJECTS/` for Ron Lesniak's master's project.

- The math behind the compact disk: The text by Vanstone and van Oorschot is freely available from the Springer website when navigating from a WPI address (`http://www.springer.com/us/book/9780792390176`). The last chapter of the book gives the exact details of how compact discs are encoded. While CDs have fallen out of fashion, essentially the same encoding is used for DVDs and MP3 files. The reason the music is so clear is mainly due to creative use of abstract algebra, specifically rings of polynomials. (This talk can use my PowerPoint presentation `http://users.wpi.edu/~martin/TALKS/CompactDisc.ppt` as a starting point, but any non-original content must be attributed.)

- Weak RSA Keys: We studied the RSA public key encryption scheme in class. While we generally believe that this scheme is secure, there are many ways to misuse it. There are weak moduli $n = pq$ and, even if a good modulus is chosen, there can be weak keys. This project explores some of these pitfalls and the cryptographic attacks that exploit them.

- Counting roots: Over the rational numbers or the real numbers, a polynomial of degree $n \geq 1$ in one variable has at most n roots. (Over the complex numbers, such a polynomial has *exactly* n roots.) What happens over other rings? Try finding roots of quadratics over $\mathbb{Z}_{12}$, etc. What can you say about $\mathbb{Z}_n$? What are the algorithms for finding roots of polynomials? How does a calculator estimate square roots of real numbers?

- Two Gems from Combinatorics: The farmer's helper is tasked with weighing n bags of grain. For some reason, the helper instead weighs the bags in pairs, and returns $\binom{n}{2}$ weights instead. Is it possible for the farmer to deduce from this data the original weights of the n bags? [I can't currently find this paper on the internet. (It's in the bibliography below.) It may be simplest for the team to hear the proof from me verbally.]

  Ross Honsberger wrote a very nice, very short paper on the following question. For a multi-set $A = \{a_1, \ldots, a_n\}$ of n integers, define $A_2 = \{a_i + a_j \mid i < j\}$ to be the multiset of $\binom{n}{2}$ pairwise sums. For sets A and B, is it true that $A_2 = B_2$ forces $A = B$?

The second part of this project explores whether our familiar pair of dice is the only possible pair that give its sets of probability outcomes. Again, the idea of a generating polynomial plays a role, but unique factorization is also used here.

- The Chinese Remainder Theorem: This classic theorem from almost 2000 years ago is quite beautiful. It has many applications, is naturally generalized to polynomial rings, and leads to some enjoyable number theory puzzles. The team should talk with me before going too far into this project.

References

I finish with a few books one might glance at to get new ideas for enrichment projects in cryptography and number theory.

James K. Strayer, *Elementary Number Theory*, PWS Publishing Co., Boston, 1994.

Douglas R. Stinson, *Cryptography: Theory and Practice* (3rd ed.), CRC Press, Boca Raton, 2005.

Neal Koblitz, Cryptography As a Teaching Tool, *Cryptologia*, **21**, no. 4 (1997), 317–326.

Ross A. Honsberger, A gem from combinatorics, *Bulletin of the ICA*, **1** (1991) 56–58.