Polynomials: Projects

These projects are intended to allow you to engage the course at the level of intensity that you wish, and to allow you the opportunity to work at a particular area in depth. A lot of the work on polynomials is very detailed and technical, and so would be of interest only to the specialist. However, there is also a great deal that would interest people who do not want to go to the frontiers of research.

You can approach these on the level of personal research (say, recording your work on a problem or giving a detailed study of illustrative examples) or as a way of going to the literature and bringing together results that are related. It is expected that everything you draw from the literature will be fully referenced. I would like to make a written version of each project available to all the participants in the course, and may make use of some of them, with appropriate acknowledgment in the book that may arise out of this course. You are also expected to give a talk in class on some part of your project.

Each of the following topics is a suggestion and you are free to take it in whatever direction you want. None of them are prescriptive and it would be unreasonable in most cases to tackle every question mentioned. Pick a subset of the questions raised so that your project can be coherent. One approach is to consider in detail an example or set of examples that either has some meat in it or can be used to exemplify the main theory. As a rough guide, the project should run between 10 and 20 pages, and the talk should be for 30 minutes. Pick a reasonably narrow focus, and avoid results and proofs that simply get bogged down in detail. Your proofs should be as transparent as possible; if you use other than standard results, make sure that these result are explained carefully with proofs either given or outlined. In the oral presentation, you should not be too ambitious. There are essentially two options: give a brief summary of some line of theory, illustrating it by a strategic use of examples, or pick a nice result whose proof can be completed nicely in the time and does not rely on outside material that you cannot make intelligible to the class. Note that some of the proposals might involve a great deal of experimental mathematics using a computer.

One source of possible projects are the explorations in my books *Polynomials* and *Pell's equation*. You may also consult the list of papers to see if there is something interesting.

Some of the topics may be ones that you have encountered in previous courses, and I am leaving it to your integrity not to "double-dip", *i.e.* simply import material that you have learned elsewhere or use a project that has already been granted credit in the other course. The purpose of the exercise is that you learn something new, or investigate in detail aspects of a situation that you previous might only have had a general knowledge of.

1. Quadratic forms. What is the class group? What is the class number? (Reference: D.A. Buell, *Binary quadratic forms*)

2. Pell's equation. When are the equations $x^2 - dy^2 = \pm 4$ solvable in odd integers (x, y)? When is the equation $x2 - dy^2 = -1$ solvable? (Reference: D.A. Buell, *Binary quadratic forms*)

3. Pell's equation. Describe the structure of the set of solutions of $x^2 - dy^2 = 1$. How are the solutions obtained? How large is the smallest positive solution of the equation? You may, if you wish, discuss computational issues. (Reference: E.J. Barbeau, *Pell's equation*)

4. Pell's equation of higher degree. Describe the structure of the solutions of $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$. How can a basic solution be obtained? What is the fourth degree analogue of Pell's equation? Describe the stucture of the solution set for various values of the parameter. What can be said about solutions of Pell's equation of higher degree? (Reference: E.J. Barbeau, *Pell's equation*) Related to this is the solution of diophantine equations that are norm forms. Let $p(x)$ be a monic irredicible polynomial over the integers of degree $n > 1$ whose distinct roots are $r_1, r_2, \cdots, r_n$ and let $P(x_0, x_1, \cdots, x_{n-1})$ be the product of $x_0 + x_1r_i + \cdots + x_{n-1}r_i^{n-1}$ over all i. P is a polynomial in n variables with integer coefficients. What can be said about the solutions of the diophantine equation $P(x_0, \cdots, x_{n-1}) = 1$?

5. The fundamental theorem of algebra. Describe different approaches and proofs to the fundamental theorem of algebra, that every polynomial equation of positive degree of **C** has at least one root.

6. Solution of equations and Galois theory. What are the possible Galois groups for an equation? Give examples to illustrate the possibilities. Examine the quintic equation. What are the Galois groups? Not every quintic equation can be solved by radicals (*i.e.* reduced to solving equations of the form $x^k = r$, where $k = 2, 3, 5$. Can we introduce another canonical type of equation that would help us solve every quintic? What about $x^5 + bx + c = 0$?

7. Polynomials in two variables. What polynomials in two variables can be inverted under composition? Suppose that $S(x, y)$ and $T(x, y)$ are real polynomials of the form $\sum a_{ij} x^i y^j$. The Jacobean conjecture says that the mapping $(x, y) - -- > (S, T)$ is a homeomorphism of the plane when its Jacobian everywhere fails to vanish. Consider especially the case that the maximum degree of S and T is 2. Chapter 3 of Terry Sheil-Small, *Complex polynomials* is a good place to start.

Are there nonlinear polynomials in several values whose composition inverses are also polynomials?

8. Orthogonal polynomials. Discuss orthogonal polynomials with respect to different weights on closed intervals, particularly the traditional ones.

9. Roots of polynomials. How are the roots of the derivative of a polynomial related to those of the polynomial itself? There are different directions in which this might be taken. One possibility is to examine polynomials over the integers, the roots of both it and its derivatives are all integers. There are several unsolved problems here, discussed in the Unsolved Problems column of the December, 1995 issue of the *American Mathematical Monthly* (page 292).

10. Factorization and irreducibility. How can one determine the irreducibility of a polynomial over the rationals? What are techniques for factoring polynomials over the integers or the rationals, and how efficient are they? Investigators in this area are Berlekamp, Musser, Wang, Zassenhouse and Lenstra, Lenstra & Lovasz.

11. Dynamial systems. Study the dynamics of the polynomials $z^2 + c$ in the complex plane for various values of the parameter c, and of $kx(1 - x)$ for various values of k on the closed unit interval $[0, 1]$. What is Sarkovskii's theorem? A good reference is the book *An introduction to chaotic dynamical systems* by Robert L. Devaney.

12. Nature of the the real and imaginary part curves of a polynomial equation. Let $p(z) = u(x, y) + iv(x, y) = u(r\cos\theta, r\sin\theta) + iv(r\cos\theta, r\sin\theta)$. One way to examine the solutions of $p(z) = 0$ in the complex plane is to look at how the curves $u(x, y) = 0$ and $v(x, y) = 0$ relate to each other. For large values of R, they intersect the circumference of the circle of radius R alternately, but within the disc, they can cross each other in a number of ways. What are the possibilities?

13. The Miramonoff Conjecture. Let n be a positive integer. Then

$$P_n(x) \equiv (x + 1)^n - x^n - 1 = x(x + 1)^a (x^2 + x + 1)^b Q_n(x) ,$$

where $a = b = 0$ when n is even, $a = 1$ when n is odd, and $b = 0, 1, 2$ according as $n \equiv 3, 5, 1 \pmod 6$. Miramanoff conjectured that $Q_n(x)$ is irreducible whenever n is prime? (See D. Miramanoff, *Sur léquation* $(x+1)^l - x^l - 1 = 0$. Nouv. Ann. Math. 3 (1903), 385-397. What is the current status of this conjecture? See also Charles Helou, *Cauchy-Mirmanoff Polynomials* `[check whether this has been published in 1991 by Math. Reviews of RSC]`.

14. Mahler's measure. Jensen's inequality in complex variables leads to the following equation for an irreducible polynomial $p(z) = a_0 + a_1 z + \cdots + a_n z^n$:

$$M(p) \equiv |a_0| \prod \{\max\ \{1, |w|\} : p(w) = 0\} = \exp\left(\int_0^1 \log |p(e^{2\pi i t})| dt \right) .$$

In 1934 Lehmer conjectured that, unless $p(x) = x$ or $p(x)$ is cyclotomic, there exists δ such that $M(p) \geq 1+\delta$ for every other polynomial p. David Boyd has done much work on this problem. What is the current state of the conjecture? See, for example, D.H. Lehmer, *Factorizations of certain cyclotomic functions* Ann. Math. 34 (1933), 461-469; C.J. Smyth, *On the product of conjugates outside the unit circle of an algebraic integer* Bull. Lond. Math. Soc. 3 (1971), 169-175; E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial* Acta Arith. 34 (1979), 391-401; R. Laboutin, *Sur la mesure de Mahler d'un nombre algébrique* C.R. Acad. Sci. Paris I, 296 (1983), 539-542.

15. An almost polynomial equation. Let n be a positive integers and a, b be integers. Investigate the number of real solutions of the equation

$$x^n + a\lfloor x \rfloor + b = 0 \ .$$

[$\lfloor x \rfloor$ is the "floor" function that maps each real number to the largest integer that does not exceed it.]

16. Irreducibility and factorization of binomials. Let K be an arbitrary field. When is the binomial $x^n - a$ reducible over K; does it necessarily have an irreducible factor with three or fewer nonzero coefficients?

17. Irreducibility and factorization of trinomials. Under what circumstances is a trinomial polynomial $ax^n + bx^m + c$ reducible? See, for example, A. Schinzel, *On reducible trinomials* Dissertationes Math. 329 (1993).

18. The algebraic structure of polnomials under composition. The composition of two polynomials is a polynomial. A polynomial is prime if it cannot be written as the composition of two polynomials whose degrees both exceed 1. This is a noncommutative operation. Do we have such a thing as a prime factor decomposition, and, if so, is it unique? See for example, J.F. Ritt, *Prime and composite polynomials* Trans. A.M.S. 23 (1922), 51-66; M. Fried and R.E. MacRae, *On the invariance of the chain of fields* Illinois J. Math. 13 (1969), 165-171; F. Dorey and G. Whaples, *Prime and composite polynomials* J. Algebra 28 (1974), 88-101; U. Zannier, *Ritt's second theorem for arbitrary characteristic* J. Reine Angew. Math. 445 (1993), 175-203.

19. Number of coefficients of a power of a polynomial. Let p be a given polynomial. Is it possible for p^2, or more generally p^k for positive integer k to have fewer coefficients than p? See, for example, P Erdös, *On the number of terms of the square of a polynomial* Nieuw. Arch. Wiskunde (2) 23 (1949), 63-65; A. Schinzel, *On the number of terms of a power of a polynomial* Acta Arith. 49 (1987), 55-70.

20. Algebras over quaternions. For algebras over fields, there are certain restrictions on such things as the number of roots and how it can factor. What happens if we allow the coefficients to range over a division ring - in particular, over the quaternions, which can be regarded as a real four-dimensional vector space with basis $\{1, i, j, k\}$, with multiplication determined by $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$?