THE PI MU EPSILON 100TH ANNIVERSARY PROBLEMS: PART I

STEVEN J. MILLER (SENIOR EDITOR), JAMES M. ANDREWS (EDITOR),
AND AVERY T. CARR (EDITOR)

Contents

As 2013 marks the 100$^{\text{th}}$ anniversary of Pi Mu Epsilon, we thought it would be fun to celebrate with 100 problems related to important mathematics milestones of the past century. The problems and notes below are meant to provide a brief tour through some of the most exciting and influential moments in recent mathematics. No list can be complete, and of course there are far too many items to celebrate. This list must painfully miss many people's favorites. As the goal is to introduce students to some of the history of mathematics, accessibility counted far more than importance in breaking ties, and thus the list below is populated with many problems that are more recreational. Many others are well known and extensively studied in the literature; however, as our goal is to introduce people to what can be done in and with mathematics, we've decided to include many of these as exercises since attacking them is a great way to learn. We have tried to include some background text before each problem framing it, and references for further reading. This has led to a very long document, so for space issues we split it into four parts (based on the congruence of the year modulo 4). That said: Enjoy!

- 1913: Erdős: How many contacts do you have in your cell phone? How many friends do you have on Facebook? Over the course of his life, Paul Erdős (March 26, 1913 to September 20, 1996) published over 1,500 mathematical papers with over **500 different people**. These are truly staggering numbers. He worked in many fields, especially in combinatorics, number theory and probabilistic methods. The famous Kevin Bacon name (or six degrees of Bacon) has been adopted to describe an actors or actress' collaborative distance from him, known as a Bacon number. This game of collaborative distance was originally inspired by Erdős' extreme collaboration; see the problem from 1969 for more details. His main interest was in solving assorted problems and open conjectures as opposed to developing theory. Many conjectures formulated by him are still open, and have small cash prizes associated with them to attract and reward. One of his famous conjectures deals with primes in arithmetic progression (which are sequences of integers that successively differ by adding a fixed amount). For instance, 5, 8, 11, 14, 17 is an arithmetic progression of length five, containing the primes 5, 11 and 17. Erdős conjectured that any set of natural numbers that is "not too sparse" contains "lots" of arithmetic progressions. More specifically,

Date: October 17, 2013.

if S is an infinite set of natural numbers, the sum of whose reciprocals diverges, then S contains arithmetic progressions of any given length. Currently \$5000 is offered for the prof of this. Progress includes the Green-Tao Theorem (see the 2004 entry), stating that the primes (the sum of whose reciprocals diverge) contain arithmetic progressions of any given length. Even though this is one particular case of the more general conjecture, it is a profound one: this special case shows that a set of naturals as erratic as the primes can have some sort of regularity here and there.

He used to remark that one didn't have to believe in G-d to be a mathematician, but one had to believe in THE BOOK, where the supreme being collected the most elegant, 'a-ha' proofs of results. See the book of Aigner and Ziegler for a beautiful approximation of what that book might be (the first chapter gives six proofs of the infinitude of primes, including a proof (see the 1955 entry) that uses a non-standard topology on the integers).

On the other hand, one of Erdős' most famous proofs was his work with Selberg on an elementary proof of the Prime Number Theorem: if $\pi(n)$ is the number of primes less than or equal to n, then $\pi(n)/(x/\log x)$ goes to 1 as n goes to infinity. That is, $\pi(n)$ is asymptotically equal to $x/\log x$. This was not a proof from the book. This was not a particularly elegant proof that showed a deep connection in mathematics. His proof wasn't even the first. The Prime Number Theorem was proven earlier using complex analysis, and it was believed for awhile that complex analysis or other similarly "deep" methods were needed to prove it. This was unsatisfying to many in the mathematics community, as why should one have to use complex numbers to count integers! (If you know complex analysis it isn't surprising that it can allow you to deduce powerful theorems, and many searched for a more elementary approach. A famous, humorous dictum is that the shortest path between two statements involving real numbers is through the complex plane; that is certainly the case here.) Even though the complex variable proof provides more information, it is nice to see just what machinery is really needed for the proof.

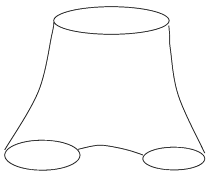
Problem (proposed by Craig Corsi and Steven J. Miller, Williams College): One open conjecture is the Erdős-Gyarfas Conjecture in graph theory, which states that every graph of minimum degree three contains a cycle whose length is a power of two. Erdős offered \$100 for a proof and \$50 for a counterexample. Here are some related questions for you to consider. (1) True or false: There exists some n such that every finite graph of minimum degree n contains an odd cycle. (2) True or false: For every n there exists some finite graph G of minimum degree n such that every cycle contained in G is odd. (3) True or false: For every n there exists some finite graph G of minimum degree n whose automorphism group is trivial. (If a counterexample exists, how small can you make it?)

References:

- M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1998.
- Paul Hoffman, *The Man Who Loved Only Numbers: The Story of Paul Erdos and the Search for Mathematical Truth*, Hyperion, 1996.

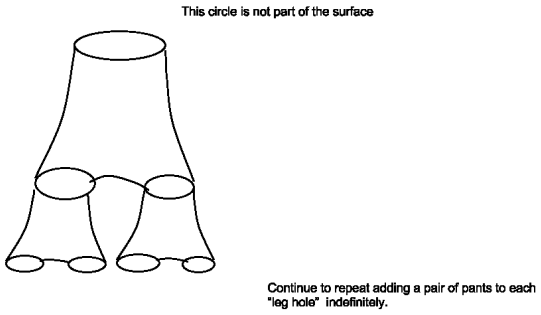
– http://www.ams.org/notices/199801/vertesi.pdf
– http://www.math.ucsd.edu/~erdosproblems/All.htmlformoreproblems

- 1917: Morse's thesis: Marston Morse was inspired by the work of the mathematicians Jacques Hadamard, Henri Poincaré, and his advisor George Birkhoff. In choosing a topic for his thesis, he wished to combine the fields of analysis and geometry, a theme throughout his life's work. The shortest distance between two points is a straight line, and straight lines have constant slope. Suppose, however, one is considering two points on a surface. The analog for the straight line is a curve called a geodesic. For example, the geodesics on a sphere are the great circles. The analog for constant slope is that the tangent vectors to the curve are parallel. Morse focused on surfaces with negative curvature, such as the "pair of pants" below.



In a first paper, Morse gave a combinatorial representation of the geodesics on surfaces of negative curvature that lie wholly in a finite portion of space. Building on this work, in his thesis, he established that on such surfaces, there exist geodesics that are recurrent without being periodic.

Problem (proposed by Joanne Snow, Colleen Hoover, and Steven Broad, Saint Mary's College): The following problem (from Michael Spivak's text named below, p. 29) concerning a specific surface of negative curvature lies at the intersection of analysis and topology, a recurring theme in much of Morse's work. Let $C \subset \mathbb{R} \subset \mathbb{R}^2$ be the Cantor set. Show that $\mathbb{R}^2 \backslash C$ is homeomorphic to the surface pictured below.



References:
– M. Morse, *A One-to-One Representation of Geodesics on a Surface of Negative Curvature*, American Journal of Mathematics **63** (1921), no. 1, 33–51.

– M. Morse, *Recurrent Geodesics on a Surface of Negative Curvature*, Transactions of the AMS **22** (1921), no. 1, 84–100.
– M. Spivak, *A Comprehensive Introduction to Differential Geometry*, Volume One, Publish or Perish, Inc, Houston, Texas, 1970.

- 1921: Mordell's Theorem: Let $E : y^2 = x^3 + ax + b$ where a and b are integers; if the discriminant $-16(4a^3 + 27b^2)$ is non-zero this is called an elliptic curve, and there are many fascinating questions we can ask, as well as important applications (elliptic curves are the building block of some powerful modern encryption systems). In 1921-1922 Mordell proved that the group of rational points on an elliptic curve, $E(\mathbb{Q}) := \{(x, y) : x, y \in \mathbb{Q} \text{ and } y^2 = x^3 + ax + b\}$, is finitely generated. This means that this group is isomorphic to $\mathbb{Z}^r \oplus \mathbb{T}$ for some positive integer r and some finite group $\mathbb{T}$. Massive generalizations of this theorem were conjectured and proved. One of the reasons elliptic curves are so important in cryptography is that they have a more complicated group structure than other popular choices, such as the cyclic groups $(\mathbb{Z}/pq\mathbb{Z})^\times$ with p, q distinct primes which is used in RSA (see the problem from 1977).

  Problem (proposed by Steven J. Miller, Williams College): The miracle behind elliptic curves is that if we take two points with rational coordinates there is a way to generate a third on it, also with rational coordinates, and obtain a commutative group law. To see this, draw a straight line connecting $P_1 = (x_1, y_1)$ with $P_2 = (x_2, y_2)$ (for simplicity assume the two points are distinct). The line hits the curve in a third point (which may be 'the point at infinity', requiring some care); the reflection of that point about the x-axis is considered the sum of the two points. Consider quartics of the form $y^2 = x^3 + ax^2 + bx + c$; for what choices of coefficients will there be an analogous definition of adding two rational points and obtaining a rational point? Or *any* definition for adding two rational points?

  References:
  – L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc Cam. Phil. Soc. **21** (1922).
  – J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, New York, 1986.

- 1925: The Schrödinger equation. One of the most important intersections between mathematics and physics is differential equations. Probably the most famous differential equation of all is Newton's second law: $\overrightarrow{F} = m\overrightarrow{a}$ (here F is the force, m is the mass, and a is the acceleration, which is the second derivative of position). There are many equivalent formulations, such as the Euler-Lagrange equations and Hamilton's equations. The analogue for quantum systems is the Schrödinger equation, formulated in 1925: $i\hbar\frac{\partial}{\partial t}\Psi = \widehat{H}\Psi$, where $i = \sqrt{-1}$, $\hbar = h/2\pi$ (with h Planck's constant), $\widehat{H}$ is the Hamiltonian operator of the system and Ψ is the wave function we are trying

to find.

Problem (proposed by Steven J. Miller, Williams College): Solving differential equations in general is enormously difficult, and is the subject of extensive research in many disciplines. Inspired by the success of Hilbert's list of problems at the start of the twentieth century, in 2000 the Clay Mathematics Institute published 7 Millennium Prize Problems, each carrying a million dollar prize. To date only one has been solved (though the prize money was declined; see the problem from 2003). Two of the six open problems involve solving differential equations: the Navier-Stokes problem and Yang-Mills theory. Read the descriptions from the Clay Mathematics institute of these (and the other problems) to get a sense of the big open questions.

References:

- Clay Mathematics Institute, *Navier-Stokes*, `http://www.claymath.org/millennium/Navier-Stokes_Equations/`.
- Clay Mathematics Institute, *Yang-Mills*, `http://www.claymath.org/millennium/Yang-Mills_Theory/`.
- E. Schrödinger, *An Undulatory Theory of the Mechanics of Atoms and Molecules*, Phys. Rev. **28** (1926), no. 6, 1049–1070.

- 1929: Gödel's Incompleteness Theorems: Suppose that this very sentence is false. Of course, if it is false, it is true, and likewise, if it is true it is false. This apparent self-contradiction does not allow for a single truth value, true or false, to be attributed to the statement. This is known as the Liar's Paradox and relates to Austrian logician Kurt Gödel's proof of the Incompleteness Theorems in 1931, extending his earlier results on the Completeness Theorem in 1929. Around the turn of the 20th century, the mathematician David Hilbert initiated a program that proposed to show that all theory in mathematics can be derived by a set of consistent axioms. The program was pursued in earnest by two theorists, Bertrand Russell and Alfred North Whitehead, who in their three volume work *Principia Mathematica* set out to show that the foundations of mathematics are consistent and complete. This was an ambitious task. For instance, using methods in formal logic, it took over 300 pages in their prolific work to establish the consistency that $1 + 1 = 2$. However, Gödel's proof of the Incompleteness Theorems brought light to the true complexity and impossibility of such tasks. The First Incompleteness Theorem states that any adequate axiomatizable theory is incomplete. In a similar manner, the Second Incompleteness Theorem states that the consistency of a system is not provable in a system that is formed by any consistent axiomatizable theory. Together, the First and Second Theorems show that Hilbert's program is not attainable. In other words, all truths about an axiomatizable theory cannot necessarily be derived by its axioms. Ultimately, Gödel's contribution influenced other theories and revolutionized the way we, as mathematicians, view the foundations of mathematics.

Problem (proposed by Avery T. Carr, Emporia State University and Steven J. Miller, Williams College): Consider the standard model of set theory, ZFC (Zermelo-Fraenkel plus Choice), and let $\aleph_0$ be the cardinality of the natural numbers. Then $\aleph_1$ equals....

References: K. Gödel, *Über die Vollständigkeit des Logikkalküls*, Doctoral dissertation, University Of Vienna, 1929.

- 1933: Skewes' number. For many years, Skewes' number may have held the record as the largest finite number to meaningfully appear in a research paper. Let $\pi(x)$ denotes the number of primes at most x, and define $\mathrm{Li}(x)$ to equal $\int_2^x dt/\log t$. The Prime Number Theorem says that $\pi(x)$ is asymptotic to $\mathrm{Li}(x)$; however, for small values of x it was noticed that the approximation $\mathrm{Li}(x)$ always overcounted the number of primes. It was natural to conjecture that this held for all x, but Littlewood showed in 1914 that this is not the case. In fact, the flip infinitely often as to which is larger. He tasked one of his students, Skewes, to compute how high one must go to find $\pi(x) > \mathrm{Li}(x)$. Assuming the Riemann Hypothesis is true, in 1933 Skewes proved that one can find an x with $x < \exp(\exp(\exp(79)))$; in 1955 he showed that if the Riemann Hypothesis is false then one can take an x at most $\exp(\exp(\exp(\exp(7.705))))$. While much progress has been made, the best bounds are on the order of e^{728}, far too large to be checked by a computer. See Rubinstein and Sarnak's paper on Chebyshev's Bias for generalizations to primes in arithmetic progression.

  Problem (proposed by Steven J. Miller, Williams College): Let $e_{\uparrow n}(x)$ mean $\exp(\exp(\cdots\exp(\exp(x))))$ (so we have the n exponentials). Thus Skewes' 1955 result is a bound of $e_{\uparrow 4}(7.705)$. If we were to write this as 10^y, what would y equal? More generally, if $e_{\uparrow n}(x) = 10^{f(x;n)}$, how fast does f grow with n? With x? This is also known as iterated towers; for more enormously growing quantities look at Graham's number.

  References:
  - M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Experimental Mathematics **3** (1994), no. 3, 173–197.
  - S. Skewes, *On the difference* $\pi(x) - \mathrm{Li}(x)$, Journal of the London Mathematical Society **8** (1933), 277–283.
  - S. Skewes, *On the difference* $\pi(x) - \mathrm{Li}(x)$ *(II)*, Proceedings of the London Mathematical Society **5** (1955), 48–70.
  - Wikipedia, *Graham's number*: `http://en.wikipedia.org/wiki/Graham%27s_number`.

- 1937: Vinogradov's Theorem. There are many interesting properties of the primes. Though we normally think of them in a multiplicative way (as every integer can be written uniquely as a product of prime powers), there are many interesting additive

questions we can investigate. A particularly interesting conjecture, due to Goldbach, is that every 'sufficiently large' even number can be written as the sum of two primes; we believe that 'sufficiently large' means at least 4! This is sometimes called the binary Goldbach problem, and is significantly easier than the ternary Goldbach problem, which states that every 'sufficiently large' odd number is the sum of three primes; it was believed that 7 suffices. A major advance towards the proof of the ternary case was made by Vinogradov in 1937, who proved that there is some finite C such that every odd number exceeding C is the sum of three primes. Sadly, the value of C produced is much too large for computers to check; until a short time ago the best C was over 10^{1000}! Recently, though, there have been major breakthroughs in obtaining better bounds on the error terms. The problem was solved in full by Harald Helfgott in May 2013, who showed $C = 7$ suffices by obtaining better estimates on the error term which brought C down to a range checkable by computers. These approaches use the Circle Method, which converts the problem to estimating integrals of exponential sums of primes. For example, the number of ways an integer N can be written as the sum of three primes is just

$$\int_0^1 \left(\sum_{p \le N,\ p \text{ prime}} e^{2\pi i p x} \right)^3 e^{-2\pi i N x} dx$$

with $e^{i\theta} = \cos\theta + i\sin\theta$ and $i = \sqrt{-1}$. To see this, if we expand the sum and incorporate the other exponential factor, we have terms such as $e^{2\pi i(p_1+p_2+p_3-N)x}$; the integral of this from 0 to 1 is 1 if $p_1 + p_2 + p_3 - N = 0$ (as then we are integrating the constant function 1) and 0 otherwise (as then we are integrating sines and cosines over full periods). Thus we have reduced the Goldbach problems to determining if an integral, which is clearly integer valued, is non-zero! Unfortunately, this is a very difficult integral to analyze, as we need to know how the primes are distributed if we are to understand the exponential sum. All approaches to date involve highly technical arguments to understand these sums.

Problem (Proposed by Steven J. Miller, Williams College): Perhaps if we are willing to allow more primes we can prove a related result more elementarily. Let's consider writing integers as sums and differences of primes. Can you prove, in an elementary manner, whether or not there is a finite integer I such that every odd number is the sum and difference of at most I primes? For example, if $I = 4$ we could consider quantities of the form $p_1 + p_2 + p_3 + p_4$, $p_1 + p_2 + p_3 - p_4$, $p_1 + p_2 - p_3 - p_4$ and $p_1 - p_2 - p_3 - p_4$. There is a beautiful set of conjectures, called the Hardy-Littlewood Conjectures, which state that for every even number $2k$ there is a non-zero constant C_{2k} (which can be explicitly written down in terms of functions of the factors of $2k$) such that, for all x sufficiently large, the number of pairs of primes of the form $(p, p + 2k)$ with $p \le x$ is approximately $C_{2k}x/\log^2 x$. Unwinding the above, it says that for any even number $2k$ there are *a lot* of pairs of primes up to x where the two primes differ by $2k$. Amazingly, it is an open problem whether or not for each even number $2k$ there is *at least one pair of primes differing by* $2k$. This shows just how poor the state of our knowledge is. We believe (and have strong numerical evidence supporting) that the number of prime pairs differing by $2k$ tends to infinity; however,

for a general $2k$ we cannot even prove the existence of one such pair! The situation has improved recently, though. In a phenomenal work, in April 2013 Yitang Zhang proved that there is some $2k \le 70,000,000$ such that infinitely many pairs of primes differ by that $2k$; subsequent work has lowered seventy million to under 10,000. Prove that if for any even $2k$ you knew there was at least one pair of primes differing by $2k$ then you could take $I = 2013$ in the original problem. Can you get a better value of I than 2013?

References:

- Dan Goldston, *Zhang's Theorem on Bounded Gaps Between Primes*, http://www.aimath.org/news/primegaps70m/
- Harald Helfgott, *Major arcs for Goldbach's theorem*, http://arxiv.org/abs/1305.2897.
- Harald Helfgott, *The ternary Goldbach conjecture*, posted on July 2, 2013, http://valuevar.wordpress.com/2013/07/02/the-ternary-goldbach-conjecture/.
- PoylMath, *Bounded gaps between primes*, http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes.
- Terry Tao, *Online reading seminar for Zhangs "bounded gaps between primes"*, http://terrytao.wordpress.com/2013/06/04/online-reading-seminar-for-zhangs-bounded-gaps-between-primes/.
- I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers* (Russian), Trav. Inst. Math. Stekloff **10**, 1937.
- Yitang Zhang, *Bounded gaps between primes*, Annals of Mathematics http://annals.math.princeton.edu/wp-content/uploads/YitangZhang.pdf.

- 1941: On August 1, 1941, Isaac Asimov visited John Campbell, editor of Astounding Science Fiction. The meeting led to the Foundation series, one of the most influential science-fiction series of all time (the original Foundation Trilogy won the Hugo for best series ever, beating out Tolkien's Lord of the Rings). The story is modeled on Gibbons' "The Decline and Fall of the Roman Empire", and tells the story of how the Galactic Empire will fall and 30,000 years of anarchy will reign before a new empire arises. Hari Seldon develops the mathematical theory of psycho-history. Inspired by statistical mechanics, while it is impossible to predict the behavior of individuals with accuracy, in this story it is possible to mathematically predict the general behavior of galactic populations with high precision. While it is too late to stop the fall, he and his colleagues analyze the equations and take steps to minimize its impact, so that a new empire will rise after just a thousand years.

  Asimov's work is but one of many examples of science-fiction writers whose work has inspired scientists and engineers. NASA seriously considered adopting the Star Trek logo; while that never happened, the first shuttle was named Enterprise.

  Problem (proposed by Steven J. Miller, Williams College): One of the most famous quotes in Asimov's original trilogy is "A circle has no end"; in case you're not familiar with the story I won't spoil it for you by divulging its meaning in the work. While mathematically a circle has no end (as we can just keep going around

and around), it does have a perimeter and it does have an area. Consider, then, the following generalization. Consider the ellipse $(x/a)^2 + (y/b)^2 = 1$. (1) Find the area enclosed by the ellipse. (2) Find the perimeter of the ellipse. *Note: the first problem is often done in multivariable calculus problems. The second problem has been studied by many, and how difficult it is to solve may surprise you, and beautifully illustrates that for many problems the boundary is harder to deal with than the interior.*

References:

– I. Asimov, *The Foundation Trilogy*, `http://www.angelfire.com/un/corosus/books/Asimov_the_foundation.pdf`.

- 1945: As the prime numbers are the building blocks of the integers (since every integer can be written uniquely as a product of prime powers), it's not surprising that much of number theory is concerned with counting these objects and determining their properties. A very useful approach is through the Riemann zeta function, $\zeta(s)$. For $\mathrm{Re}(s) > 1$ it is defined by the infinite series $\sum_{n=1}^{\infty} 1/n^s$; however, by unique factorization it also equals $\prod_{p \text{ prime}} (1 - p^{-1})^{-1}$. This product formula gives a hint as to why it is so useful, as it allows us to pass from information about the integers (which are well understood) to information about the primes. It turns out this function can be continued and defined for all s, and the location of its zeros are intimately connected to questions concerning the distribution of the primes. The famous Riemann hypothesis says that all the complex zeroes of $\zeta(s)$ lies on the line $\mathrm{Re}(s) = \frac{1}{2}$; this is one of the biggest open problems in mathematics (see the 2nd and 5th references).

  It is frequently easier to prove results for function fields instead of number fields, and the Riemann hypothesis is no exception. Let F be a field (not necessarily a finite field). A function field in one variable over F is a field K, containing F and at least one element x, transcendental over F, such that $K/F(x)$ is a finite algebraic extension. Such a field is said to have transcendence degree one over F. A function field in one variable over a finite constant field is called a global function field.

  Our next goal is to define the zeta function of a global function field $K/\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field with q elements. A prime in K is, by definition, a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. The group of divisors of K, $\mathcal{D}_K$, is by definition the free abelian group generated by the primes. For $A \in \mathcal{D}_K$ we define the norm of A, NA, to be $q^{\deg(A)}$. The zeta function of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{A \geq 0} \frac{1}{NA^s} = \prod_{P \text{ primes in } K} \left(1 - \frac{1}{NP^s}\right)^{-1}, \qquad \mathrm{Re}(s) > 1.$$

  The most amazing thing is that the analogous statement of the Riemann Hypothesis over global function fields is a theorem, first proved by Weil in the 1940s.

  The Riemann Hypothesis for Function Fields: Let K be a global function field whose constant field F has q elements. All the roots of $\zeta_K(s)$ lie on the line $\mathrm{Re}(s) = 1/2$.

The theorem above was first conjectured for hyper–elliptic function fields by Artin in his thesis. The simplest case, i.e., for elliptic curves, was proven by Hasse. The first proof of the general result was published by Weil in 1948. Weil presented two, rather difficult, proofs of this theorem. The first used the geometry of algebraic surfaces and the theory of correspondences. The second used the theory of abelian varieties (see references 6 and 7). The whole project required revisions in the foundations of algebraic geometry since he needed these theories to be valid over arbitrary fields not just algebraically closed fields in characteristic zero. In the early seventies, a more elementary proof appeared due, in a special case to Stepanov, and in the general case to Bombieri (building on Stepanov's ideas).

Problem (proposed by Julio Andrade, IHÉS:) Let K be a global junction field in one variable with a finite

constant field $\mathbb{F}_q$ with q elements. Suppose that the genus of K is g. Prove that there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) \;=\; \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

where the genus g is a natural number which is an invariant of the function field K. (Hint: You will need to use the Riemann–Roch theorem. For more details about the genus of a function field and the Riemann–Roch theorem see references 4.)

References:

- E. Artin, *Quadratische Körper in Geibiet der Höheren Kongruzzen I and II*, Math. Z. **19** (1924), 153–296.
- E. Bombieri, *Riemann Hypothesis* in The Millenium Prize Problems, edited by: J. Carlson, A. Jaffe and A. Wiles (AMS, 2006; CLAY 2000).
- E. Bombieri, *Counting Points on Curves over Finite Fields*, Séminaire: Bourbaki, No. 430, 1972/3.
- C. Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, Cambridge (1993).
- P. Sarnak, *Problems of the Millennium: The Riemann Hypothesis* (2004), Clay Mathematics Institute.
- A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, 1948.
- A. Weil, *Variétés Abéliennes et Courbes Algébriques*, Hermann, Paris, 1948.

- 1949: 100th Anniversary of Kummer proving Fermat's Last Theorem for regular primes. Fermat's Last Theorem says that, for a fixed integer $n \geq 3$, there cannot be $x, y, z \in \mathbb{Z}$ such that $xyz \neq 0$ and $x^n + y^n = z^n$. As a solution for some n produces solutions for all multiples of n, the proof reduces to the cases where n is 4 or an odd prime. 1949 marks the centennial of Kummer's proof of Fermat's Last Theorem for regular primes. In brief, if $p \geq 3$ is prime and ζ_p is a primitive pth root of unity, then the *class number* of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ is a positive integer that measures the extent to which unique prime factorization fails in $\mathbb{Z}[\zeta_p]$. We say p is *regular* if and

only if it does not divide the class number of $\mathbb{Q}(\zeta_p)$. Essentially, Kummer's idea was to use Lamé's factorization $z^p - y^p = \prod_{j=1}^{p}(z - \zeta_p^j y)$ and study the ideals generated by the $z - \zeta_p^j y$ in $\mathbb{Z}[\zeta_p]$. In developing the theory of the p-adic numbers, Kummer also found an elementary characterization of regular primes in terms of the *Bernoulli numbers* B_n. Recall that $B_0 = 1$, and that for all positive $n \in \mathbb{Z}$, $0 = \sum_{k=0}^{n} \binom{n+1}{k} B_k$. Using combinatorics, one can prove that $B_n = 0$ for all odd $n \geq 3$. The first few Bernoulli numbers of even index $n \geq 2$ are: $B_2 = +1/6$, $B_4 = -1/30$, $B_6 = +1/42$, $B_8 = -1/30$, $B_{10} = +5/66$, $B_{12} = -691/2730$, ...

Kummer proved that an odd prime p is regular if and only if p does not divide the numerator of B_n, in lowest terms, for all even $n \leq p - 3$. Little is known about the Bernoulli numerators; by contrast, a theorem by Clausen-von Staudt says that

$$B_{2n} \; + \sum_{\substack{p \text{ prime} \\ (p-1)|2n}} \frac{1}{p} \; \in \; \mathbb{Z},$$

so the denominator of B_{2n} in lowest terms divides $\prod_{(p-1)|2n} p$. Unfortunately, we do not even know whether infinitely many regular primes exist, though we believe in the limit $e^{-1/2}$ percent of all primes are regular and we know there are infinitely many irregular primes.

Problem (proposed by Minh-Tam Trinh, Princeton University): The following is called Kummer's Congruence: If p is prime and n_1, n_2 are positive even integers such that $n_1 \equiv n_2 \not\equiv 0 \bmod p-1$, then $B_{n_1}/n_1 \equiv B_{n_2}/n_2 \bmod p$, where a/b modulo p is the solution x to the congruence $bx \equiv a \bmod p$, when the latter exists. Use Kummer's Criterion and the Clausen-von Staudt's Theorem to show that if n is a product of irregular primes and $2n < B_{2n}$, then there is an irregular prime $p \nmid n$. (Note: with more work, one can build on this and prove there are infinitely many irregular primes.)

- 1953: The Metropolis Algorithm. While it is wonderful to solve problems exactly, with explicit parameter dependence, for many real world problems this is not even remotely feasible. This year honors the Metropolis Algorithm. It and various generalizations have led to the explosive growth of *Markov chain Monte Carlo (MCMC) algorithms*, which have revolutionized subjects from statistical physics to Bayesian inference to theoretical computer science to financial mathematics by giving us the ability to simulate in real time.

  A *Markov chain* is a random sequence of states, each of whose probabilities depend iteratively on the previous state. Metropolis et al. realized in 1953 that Markov chains could be run on then-new electronic computers to converge to, and hence sample from, a probability distribution of interest. Consider the special case where the set of possible states is equal to the integers, $\mathbb{Z}$. Let $\{\pi_i\}_{i\in\mathbb{Z}}$ be any positive probability distribution on S, i.e., a collection of real numbers $\pi_i > 0$ with $\sum_{i\in\mathbb{Z}} \pi_i = 1$. Let $\{p_{i,j}\}_{i,j\in\mathbb{Z}}$ be Markov chain transition probabilities, so $p_{i,j}$ equals the probability, given that the state at time n equals i, that the state at time $n+1$ equals j. The question

is, can we find simple transition probabilities $p_{i,j}$, such that the chain "converges to π", i.e., for each $i \in \mathbb{Z}$, the probability that the state at time n is equal to i converges, as $n \to \infty$, to π_i.

The answer is yes! For $i \in \mathbb{Z}$, let $p_{i,i+1} = \frac{1}{2}\min[1, \pi_{i+1}/\pi_i]$, $p_{i,i-1} = \frac{1}{2}\min[1, \pi_{i-1}/\pi_i]$, and $p_{i,i} = 1 - p_{i,i+1} - p_{i,i-1}$, with $p_{i,j} = 0$ otherwise. Then this Markov chain is easily run on a computer (for an animated version see for example `www.probability.ca/met`), and has good convergence properties as the following problem shows.

Problem (proposed by Jeffrey Rosenthal, University of Toronto): Show that the above Markov chain:
(a) is *irreducible*, i.e., for any $i, j \in \mathbb{Z}$ there are $m \in \mathbb{N}$ and $k_1, \ldots, k_m \in \mathbb{Z}$ such that $p_{i,k_1} > 0$ and $p_{k_m,j} > 0$ and $p_{k_n,k_{n+1}} > 0$ for $1 \le n \le m-1$.
(b) is *aperiodic*, in particular there is at least one $i \in \mathbb{Z}$ with $p_{i,i} > 0$.
(c) is *reversible*, i.e., $\pi_i p_{i,j} = \pi_j p_{j,i}$ for all $i, j \in \mathbb{Z}$.
(d) leaves π *stationary*, i.e., $\sum_{i \in \mathbb{Z}} \pi_i p_{i,j} = \pi_j$ for all $j \in \mathbb{Z}$. [Hint: Use part (c).]
(e) *converges to* π as described above. [Hint: This follows from parts (a), (b), and (d) by the standard Markov chain convergence theorem, see e.g. Section 1.8 of Norris (1998).]

References:

- N. Metropolis, A. Rosenbluth, M. Rosenbluth, A. Teller and E. Teller, *Equations of state calculations by fast computing machines*, J. Chem. Phys. **21** (1953), 1087–1091.
- J. R. Norris, *Markov Chains*, Cambridge University Press, 1998. Available at: http://www.statslab.cam.ac.uk/∼james/Markov/

- 1957: The Ross Program. The Ross Mathematics Program is an intensive residential summer program for high school students who are talented and well trained in math. In 1957 Arnold Ross founded his program at the University of Notre Dame and moved it to the Ohio State University in 1964. Dr. Ross stepped down in 2000, but the Ross Program continues to run, involving about 40 first-year students every summer. The central goal of this Program is to inspire students to learn how to think like mathematicians, and to write convincing, logical proofs of their mathematical observations. Dr. Ross chose number theory as the vehicle for this learning process. Starting from axioms for $\mathbb{Z}$ (the ring of integers), Ross participants analyze topics like modular arithmetic, Euclid's algorithm, quadratic reciprocity, and existence of primitive roots. They also consider analogues of those ideas in other contexts, like Gaussian integers, and the ring of polynomials over $\mathbb{Z}/p\mathbb{Z}$. Further information about the Ross Program is posted at `http://www.math.osu.edu/ross`. The problems below are taken from some of the Ross problem sets.

  Problems (sent by Dan Shapiro, The Ohio State University): We write $\gcd(a, b)$ for the "greatest common divisor" of integers a and b. The sequence $2^n - 1$

enjoys a curious property: $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$. Let's give that property a name: A sequence $\{A_n\}_{n\geq 1}$ of positive integers has the *GCD-property* if: $\gcd(A_m, A_n) = A_{\gcd(m,n)}$ for every pair of indices m, n.

Problem 0. Show that the following sequences have the GCD-property.
(1) For $r \in \mathbb{Z}^+$, the constant sequence $C_n = r$, and linear sequence $L_n = rn$.
(2) For $k, c \in \mathbb{Z}^+$, let

$$E(k,c)_n = \begin{cases} c & \text{if } n \text{ is a multiple of } k, \\ 1 & \text{otherwise.} \end{cases}$$

(3) If $a > b$, let $R_n = a^n - b^n$.
(4) Fibonacci numbers F_n.

For a sequence $\{b_n\}_{n\geq 1}$ of positive integers, define $B_n = \prod_{d|n} b_d$. For instance, $B_2 = b_1 b_2$, $B_4 = b_1 b_2 b_4$, and $B_6 = b_1 b_2 b_3 b_6$. If $\gcd(b_m, b_n) = 1$ whenever $m \neq n$, check that $\{B_n\}$ has the GCD-property.

Problem 1.
(1) Which $\{b_n\}$ produce sequences $\{B_n\}$ with the GCD-property?
(2) Does every $\{B_n\}$ with the GCD-property arise from some (unique) integer sequence $\{b_n\}$?

This is related to the factorization $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Those factors $\Phi_d(x)$ are polynomials with integer coefficients (the "cyclotomic polynomials"). Consequently, if $B_n = 2^n - 1$ then $b_d = \Phi_d(2)$ is a sequence of integers.

If $L_n = n$ what is the corresponding sequence ℓ_n ?

The Fibonacci sequence F_n: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ... arises from f_n: 1, 1, 2, 3, 5, 4, 13, 7, 17, 11, 89, 6, 233, ... Why is every term f_n an integer?

References: M. Dziemiańczuk and Wiesław Bajguz, *On GCD-morphic sequences*, `http://arxiv.org/abs/0802.1303`.

- 1961: When starting out in math classes, we get used to homework assignments where not only are we are asked to find exact answers, but we can. For example, if we're given a quadratic $ax^2 + bx + c$ we can solve explicitly for the two roots as functions of the coefficients a, b, c by using the quadratic formula. We find the roots are $(-b \pm \sqrt{b^2 - 4ac})/2a$. A very nice feature is that if we vary the coefficients a bit, the roots continuously change.

You can't be blamed if you are thus led to believe that all math is like this, namely that if we have enough accuracy in our inputs we can approximate the output arbitrarily well. Beginning just before the start of the twentieth century, with the work of Poincaré on the orbits of planets, this belief began to be tested. A milestone in our understanding of how wild behavior can be is the work of Lorenz. One of his seminal papers in the subject is Deterministic Nonperiodic Flow, published in 1963 (but based on work started in 1961), which introduces a property of dynamical systems now known as sensitive dependence on initial conditions. This refers to a system where minute changes in the initial conditions affect drastically the behavior of the system over time. To put it simply, very small changes in the starting configuration very quickly lead to wildly different behavior. He was considering a very simple deterministic system in an attempt to understand weather. He wanted to re-run some calculations from a certain point, and when he inputed the output from a previous run was shocked to see the system behave very differently very quickly. What happened was the printer only displayed three digits of the output, while the computer code worked with six. Many people are familiar with such behavior under the phrase 'Butterfly Effect', which insinuates that the flap of a butterfly's wings may cause (or prevent) the onset of a tornado hundreds of miles away. The application of this theory to meteorology shows that long-term weather or climate forecasting may be impossible if can be affected by seemingly trivial changes to wind speed and other factors, as we will never know all the parameter values with perfect accuracy.

Problem (proposed by Craig Corsi and Steven J. Miller, Williams College): Imagine playing billiards, where the billiards table is the unit square in $\mathbb{R}^2$, and the ball is a point. You place the ball on the lower-left edge of the table (that is, the point $(0,1)$) and strike the ball at some angle θ with the x-axis with $\theta \in (0, \pi/2)$. Assume that there is no friction, so that after striking the ball, the ball will keep bouncing off the walls of the table forever. For instance, if $\theta = \pi/1$, then the ball will bounce back and forth forever between the lower left and upper right corners of the table.

Let t be time in seconds, and let $\hat{x}_\theta(t)$ be the function representing the position of the billiards ball in the plane at time t if it was struck at angle θ with the x-axis. (a) For any $N \in \mathbb{N}$, show that if $\theta \neq \phi$, then there exists a $t > N$ such that $|\hat{x}_\theta(t) - \hat{x}_\phi(t)| > 1/2$. (b) For any $\theta \in (0, \pi/2)$, show that either (i) the number of points on the edge of the billiards table hit by the ball is finite, or (ii) **any** line segment contained in the boundary of the unit square, however small, is hit infinitely often by the ball. (c) Classify all angles for which (i) is satisfied.

References:

- `http://eaps4.mit.edu/research/Lorenz/Deterministic_63.pdf`
- `http://eaps4.mit.edu/research/Lorenz/How_Much_Better_Can_Weather_Prediction_1969.pdf`

- 1965: Fast Fourier Transform: 1965: It is hard to understate just how important it is to do something fast and with minimal effort. The following example does a great

job. Imagine you are a young Babylonian math scholar. Your education would be very different from a child of today, due to the Babylonian love of 60. Yes, instead of working base 10 they worked base 60 (and before you laugh too much at them, think of how many days there are (approximately) in a year, how many degrees we have in a circle, how many hours in a day, ...). To learn one's multiplication table requires memorizing $60 \cdot 60 = 3600$ values (instead of the $10 \cdot 10 = 100$ that we must do). Of course, one can be a bit more clever and notice that $x \cdot y = y \cdot x$, which almost cuts our work in half (1830 versus 55). As stone tablets are expensive and heavy to carry, one clearly doesn't want to memorize this many multiplications. The Babylonians, fortunately, had a very clever idea. They noticed that $x \cdot y = ((x+y)^2 - x^2 - y^2)/2$; thus if they could just memorize squaring (or bring tables of 120 or so squares), they could compute any multiplication by squaring, subtraction and division by two (the last two operations are significantly easier). This simple idea is incredibly powerful, and is the basis of the look-up table (if you can pre-compute useful expressions and then combine them intelligently later, there is the potential for enormous computational savings).

There are many milestones in our efforts to find better and faster ways to solve problems. In 1965, a paper written by mathematicians James William Cooley and John Tukey described a more efficient way of calculating Discrete Fourier Transforms, which decompose a signal into its component frequencies. The Fast Fourier Transform (FFT) was based on a technique developed by Gauss, in 1805, to calculate the coefficients in a trigonometric expansion related to a the trajectories of two asteroids. Cooley and Tukey's new approach to Gauss' techniques, the Fast Fourier Transform Algorithm, had a major impact on the science and engineering community, particularly in the field of digital signal processing. The Fast Fourier Transform allowed a variety of problems, in mathematics and science, to be solved more efficiently and quickly. There are currently a wide range of Fast Fourier Transform variations, most based on Cooley and Tukey's algorithm, that can be used to solve problems in many areas of both pure and applied mathematics.

Problem (Proposed by Steven J. Miller, Williams College, and Bree Yeates, Emporia State University): Frequently we find a problem that appears to require a certain approach to be solved, but in fact can be done in significantly less time if we adopt a better vantage. One of my favorites is the Strassen algorithm from 1969. Assume when multiplying matrices that multiplication is expensive and addition is cheap (this is a reasonable assumption, as for large numbers it is significantly faster to add than multiply). If A and B are $n \times n$ matrices then there are n^2 entries in their product. Each entry requires n multiplications and $n-1$ additions. Thus to find AB it seems like we need n^3 multiplications. It turns out that, at the cost of changing which multiplications and additions we do, we can do this in less. (1) Show that we can group terms and compute the 4 entries of the product of two 2×2 matrices with just 7 multiplications (and 18 additions). (2) You might think saving one multiplication isn't a big deal. While that is correct for small matrices, the saving scales, and we can do the product of two $n \times n$ matrices with on the order of $n^{\log_2 7}$ multiplications (the savings from 8 to 7 multiplications becomes the

exponent $\log_2 8$, which is 3, being replaced by $\log_2 7$, which is about 2.807). While there has been constant improvement since, with the exponent now down to about 2.3727, the original implementation already leads to enormous computational savings.

References:

- C. Burrus, *Fast Fourier Transforms*, Retrieved from the Connexions, (November 18, 2012). `http://cnx.org/content/col10550/1.22/`
- V. Strassen, *Gaussian Elimination is not Optimal*, Numer. Math. **13** (1969), 354–356.
- J. M. Pollard, *The Fast Fourier Transform in a Finite Field*, Mathematics of Computation **25** (1971), 365–374.

- 1969: Erdős Numbers: Mathematicians like to have fun with their profession. The most prolific mathematical researcher of the 20th century was Paul Erdős (1913–1996). He wrote about 1500 articles and had about 500 different coauthors. People started to think of Paul as the center of the research collaboration world. In 1969 Casper Goffman, an analyst with about 100 papers himself, wrote a whimsical article in which he described a notion that was making the rounds, a way to measure one's distance from Erdős in terms of mathematical collaborations. Paul Erdős has Erdős number 0. A person who has published a joint paper with Erdős has Erdős number 1. A person who has published a paper with a person with Erdős number 1 (but does not qualify for a smaller number) has Erdős number 2, and so on. Everyone wanted to have a small Erdős number. As of today, nearly 10,000 people have Erdős number 2, and nearly every practicing mathematician has Erdős number 6 or less.

  From a mathematical point of view, we can view Erdős numbers simply as distances in the "collaboration graph." The vertices of this graph are researchers, and an edge is present between every pair of researchers who have published together. (Actually there are two such graphs, depending on whether an edge appears only for two-authored papers, or whether all the authors of a multi-authored paper are considered to be adjacent to each other.) A tool on MathSciNet allows people to calculate these distances. See the Erdős Number Project website for a wealth of information about Erdős numbers, the collaboration graph, and related topics. The collaboration graph is just one example of a large social network; other examples include Facebook and graphs recording telephone calls. Research into the structure and dynamics of such networks has reached a feverish pace in the past several years. Much of that work deals with how graphs can evolve randomly, a topic pioneered by Erdős himself decades ago.

  Near the end of his life, Paul Erdős expressed the opinion that this fuss over Erdős number numbers was all a bit silly. But even he had gotten into the game, having written a short paper in 1972 in which he proved that the (more restrictive, two-author version of the) collaboration graph could not be drawn in the plane without

its edges crossing.

Problem (Proposed by Jerrold Grossman, Oakland University): Here is a problem about a social network. Suppose that in a group of at least three people, it happens that every pair of them have precisely one common friend. Prove that there is always a person who is everybody's friend, and describe the structure of this "friendship graph." Paul Erdős solved this problem in a paper with Alfréd Rény and Vera Sós in 1966.

References:

- P. Erdős, *On the fundamental problem of mathematics*, Amer. Math. Monthly **79** (1972), 149–150. `http://www.math.ucla.edu/~mwilliams/erdos.pdf`.
- P. Erdős and A. Rényi, *On the evolution of random graphs*, Magyar Tud. Akad. Mat. Kutató Int. Közl. **5** (1960), 17–61. `http://www.renyi.hu/~p_erdos/1961-15.pdf`.
- C. Goffman, *And what is your Erdős number?*, American Mathematical Monthly **76** (1969), no. 7, 791.
- J. W. Grossman, *The Erdős Number Project*, `www.oakland.edu/enp`.
- M. Newman, A.-L. Barabási, and D. J. Watts, eds., *The Structure and Dynamics of Networks*, Princeton University Press (2006).

- 1973: 100th Anniversary that e is transcendental. If there exists a polynomial $p(x)$ of finite degree and integer coefficients such that $p(\alpha) = 0$ then we say α is an algebraic number; if there is no such polynomial then α is transcendental. Thus all rational numbers are algebraic, as are numbers such as $\sqrt{2}$, $i = \sqrt{-1}$, and more interestingly $\sqrt{5 + \sqrt{3} + \sqrt{1 + \sqrt{2}}}$. Using a diagonalization argument, Cantor proved that almost all real numbers are transcendental, although his method could not give a specific example.

  It's hard to prove specific numbers are transcendental, but Charles Hermite established the transcendence of e in 1873, and Ferdinand von Lindemann proved the transcendence of π in 1882.

  Problem (Proposed by Steven J. Miller): Find a 1-to-1, increasing function $f : [0, 1] \to \mathbb{R}$ such that $f(x)$ is transcendental for all x.

  References: There are many proofs of the transcendence of e online; see for example `http://www.math.brown.edu/~res/M154/e.pdf`.

- 1977: RSA: U.S. Patent 4,405,829 was given to Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman for RSA (Clifford Cocks developed something similar a few years earlier while working for Britain's Government Communications Headquarters, where his work was understandably classified). RSA was a major breakthrough in cryptography. Using prime numbers, it allows two people who have never met to securely

sign and exchange messages. Both aspects are important, as it is essential that one be able to verify the identity of the sender as well as protect the information to be sent. One of the key steps of RSA is to compute high exponents of a message (which can be assumed to be a number) modulo a large number quickly. Without algorithms such as RSA, modern e-commerce would be impossible; the entire point is that we can buy something from Amazon.com or pay our bills online without going in person to the vendors and proving who we are.

One of the key inputs in RSA is Fermat's little Theorem (FℓT), which says that if a is relatively prime to p and p is prime then $a^{p-1} \equiv 1 \bmod p$. Note that FℓT can be turned into a primality test: if $a^{n-1} \not\equiv 1 \bmod n$ then n is composite; unfortunately the converse is not true and there are integers n such that $a^{n-1} \equiv 1 \bmod n$ for all a relatively prime to n. Such numbers are called Carmichael numbers (see the 2010 entry), and cause minor headaches in the field. RSA is based on the assumption that while it is easy to multiply two numbers, it is hard to factor a product unless you have extra information (such as, for example, one of the factors!). If a method for fast factorization were to be found, then RSA would cease being a secure method. Shor found such an algorithm for fast factorization, but it requires a quantum computer. So far, the largest number such computers can successfully factor is 21, though the potential exists for them to do so much more. Other cryptographic systems, such as lattice based methods, are believed to be more secure against quantum computer attacks.

Problem (Proposed by Steven J. Miller, Williams College): Rivest, Shamir and Adleman formed RSA Laboratories to market and further develop applications of RSA. The company put forth factoring challenges in 1991 to encourage research into cryptographic methods, and to get a sense of how large a number must be so that, with existing technology, it is impractical to factor. These challenge numbers are all the product of two primes, and thus once one factor is found the number is completely factored. Cash prizes were offered, ranging from \$1,000 t0 \$200,000. The challenge was officially closed in 2007, though many people continue to try to factor them. The smallest RSA challenge number is RSA-100, with 100 decimal digits. It is

$$1522605027922533360535618378132637429718068114961 3$$

$$8068865790849458012296325895289765400035069200613 9.$$

While it was successfully factored in 1991 (less than a month after the challenge began), don't let that stop you: find the factors yourself! The full list is available online (see either RSA laboratories or Wikipedia); for the unfactored numbers, no factorization is known (when generated, the computers were not connected to the network, and after finding the products they were destroyed!).

References:

- R. Rivest, A. Shamir and L. Adleman, RSA patent (1977). `http://www.google.com/patents/US4405829`.
- RSA Laboratories, *The RSA Challenge Numbers*, `http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-challenge-numbers.htm`.

– Wikipedia, *RSA Factoring Challenge*, `http://en.wikipedia.org/wiki/RSA_Factoring_Challenge`.
– Wikipedia, *Shor's Algorithm*, `http://en.wikipedia.org/wiki/Shor's_algorithm`.

- 1981: The Mason-Stothers Theorem: A child learns of the nonnegative numbers at an early age. Polynomials, on the other hand, demand a little more sophistication and are reserved in a U.S. child's education for middle school. Those fortunate enough to take an undergraduate abstract algebra class realize that the chasm between the integers and polynomials is not so vast. One learns there are similarities: both integers and polynomials form rings; and that there are analogies: the integers have prime factors as their basic building blocks, whereas polynomials (over $\mathbb{C}$) have linear factors. Given this, it is not that surprising that we have the following definitions.
  – The Radical of an Integer: For $n \in \mathbb{Z}^+$ suppose $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ where the p_i's are distinct primes and the e_i's are positive integers. We the define the **radical** of n to be $r(n) = p_1 \cdots p_k$ with $r(1) := 1$. In other words, $r(n)$ *is the greatest square-free factor of* n or, more simply, *the product of distinct prime factors of* n. As an example, $r(100) = r(2^2 \cdot 5^2) = 2 \cdot 5 = 10$.
  – The Radical of a Polynomial: Let $p(t)$ be a polynomial whose coefficients belong to an algebraically closed field of characteristic 0. We put $\mathbf{n_0(p(t))} =$ the number of distinct zeros of $p(t)$. (In a ring R, if there exists a $n \in \mathbb{Z}^+$ such that $na = 0$ for all $a \in R$, then the least such positive integer is called the *characteristic of the ring*. *Algebraically closed* just means we are in the right place for all the roots of the polynomial to exist; think of polynomials with coefficients in $\mathbb{C}$ - they can be written as a product of linear factors if we allow roots from $\mathbb{C}$).

  With these definitions we state the Mason-Stothers Theorem: Let $a(t), b(t)$, and $c(t)$ be polynomials whose coefficients belong to an algebraically closed field of characteristic 0. Suppose $a(t), b(t)$, and $c(t)$ are relatively prime and that $a(t) + b(t) = c(t)$. Then $\max \deg\{a(t), b(t), c(t)\} \leq n_0(a(t) \cdot b(t) \cdot c(t)) - 1$.

  This beautiful theorem is easily understood, and it's proof requires just a little knowledge of abstract algebra. What is intriguing is that the analogous statement for the integers is still unproven (though we note that Shinichi Mochizuki of Kyoto University has offered a proof in the form of a series of papers on his website; a review is in progress). This is an important open problem in Number Theory, and is known as the *abc Conjecture*. It was originally posed in 1985 by David Masser (considering an integer analog of Mason's Theorem) and in 1988 by Joseph Oesterlé (considering a conjecture of Szpiro regarding elliptic curves). Explicitly, the abc Conjecture (Masser's Version) says that for a nontrivial triple of integers (a, b, c) such that $a + b = c$ and $\gcd(a, b, c) = 1$, then for every $\epsilon > 0$ there exists a universal constant $\mu(\epsilon)$ such that $\max\{|a|, |b|, |c|\} \leq \mu(\epsilon)[r(abc)]^{1+\epsilon}$. Hence, the remarkable fact that we have a problem for polynomials that is much easier to establish than the analogous statement for integers. This is not the only one. We offer the following problem.

Problem (proposed by Jeffery Paul Wheeler, University of Pittsburgh) Use the Mason-Strother's Theorem to establish a polynomial Fermat's Last Theorem: Let $x(t), y(t)$, and $z(t)$ be relatively prime polynomials whose coefficients belong to an algebraically closed field of characteristic 0 such that at least one of them has degree > 0. Then $x(t)^n + y(t)^n = z(t)^n$ has no solution for $n \geq 3$.

References:

- R. C. Mason, *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Note Series 96, Cambridge, England, Cambridge University Press, 1984.
- D. W. Masser, *Open problems.* In Chen, W. W. L. Proceedings of the Symposium on Analytic Number Theory. London: Imperial College, 1985.
- S. Mochizuki, http://www.kurims.kyoto-u.ac.jp/∼motizuki/top-english.html.
- J. Oesterlé, *Nouvelles approches du ≪théoréme≫ de Fermat*, Séminaire Bourbaki exp. 694 (1988), 165–186.
- W. W. Stothers, *Polynomial identities and hauptmoduln*, Quarterly J. Math. Oxford **32** (1981), no. 2, 349–370.

- 1985: The Jones Polynomial: Knot theory is a branch of topology that primarily deals with embeddings of circles in 3-dimensional space. The major motivating problem of knot theory is this: How can we tell if two knots are really the same? In other words, given two knots is it possible to manipulate one so that it becomes the other? Mathematicians try to solve this problem by finding *invariants* of knots, mappings from knots to some other type of object defined in such a way that equivalent knots have the same image. Thus knots which have different images under a particular invariant must be different knots.

  Finding and studying knot invariants is a thriving area of research that can be traced back to Vaughan Jones' discovery of the Jones Polynomial. The Jones Polynomial is a Laurent polynomial in a variable t assigned to a knot in $\mathbb{R}^3$. It exposed links between knot theory and physics that revitalized interest in the subject. In addition, Jones' discovery has led to the discovery of new polynomial invariants (such as the HOMFLY polynomial) and new methods for calculating polynomial invariants (such as the Kauffman bracket).

  Jones' original method for calculating his polynomial is complicated, but easier methods are available. A good example can be found in chapter 6 of Colin Adams' *The Knot Book* (for a method using braids, see `http://arxiv.org/abs/math/0505064`).

  Problem (proposed by Chad Wiley, Emporia State University): The Jones polynomial of the unknot is the constant polynomial 1. Are there any nontrivial knots which also have this property? Surprisingly, despite all the research that has been done on the Jones polynomial, we still don't know the answer to this question. A more accessible problem would be to show, perhaps using Rolfsen's tables, that a nontrivial knot with Jones polynomial 1 must have at least 11 crossings. (In fact, it can be shown that such a knot would need to have at least 18 crossings; see the

paper by Dasbach and Hougardy for details.)

References:

- C. Adams, *The Knot Book*, American Mathematical Society, 2004.
- O. T. Dasbach and S. Hougardy, *Does the Jones Polynomial detect unknottedness?*, Experimental Mathematics **6** (1997), 51–56. `http://www.or.uni-bonn.de/~hougardy/paper/does_the.pdf`.
- V. F. R. Jones, *A polynomial invariant for knots via von Neumann algebra*, Bull. Amer. Math. Soc. (N.S.) **12** (1985), 103–111.

- 1989: PROMYS: Twenty-five years ago, David Fried and Glenn Stevens (graduates of Ross' Secondary Science Training Program; see the problem from 1957) co-founded PROMYS. Since then over 1000 students have gone through the program. Currently about 80 high school students each year come to Boston University for six weeks of challenging discovery, mentored by top graduate students and faculty drawn from all over the world. Programs like this play a key role in both exciting young students into mathematics, as well as teaching older students how to mentor and design classes and research programs. In addition to standard classes and challenging problems, students have the opportunity to participate in research, and there are numerous advanced lectures on topics ranging from "The Schoenflies Conjecture and Morse Theory" to "Statistical Inference and Modeling the Unseen: How Bayesian statistics powers Google's voice search."

  Problem (proposed by Steven J. Miller, Williams College): I've had the fortune of speaking at PROMYS several times. In 2009 I gave a talk on heuristics and ballpark estimates. It's very important to be able to approximate answers. One item I discussed was a standard heuristic to estimate how many of the Fermat numbers are prime (the n^{th} Fermat number, F_n, is $2^{2^n}+1$). The Prime Number Theorem says the number of primes at most x is approximately $x/\log x$ (so for large n the probability it is prime is about $1/\log n$). Use this and some (hopefully!) reasonable assumptions to show that we expect about 2 or 3 of the Fermat numbers to be prime. It's an open question whether or not there are infinitely many of these (we believe there are exactly five, corresponding to $n \in \{0,1,2,3,4\}$). Fermat primes occur in many different places in mathematics. A regular n-gon is constructable by straight edge and compass if and only if $n = 2^m p_1 \cdots p_k$, where m is a non-negative integer and the p_i's are Fermat primes (thus a regular 17-gon is constructable, but a 7-gon is not). Another occurrence is that there is a proof of the infinitude of the primes by considering the sequence of Fermat primes – find that proof! (This is one of the six proofs from Chapter 1 of THE BOOK, see the problem from 1913).

  References:

  - M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1998.

- 1993: Lagrange's well-known "Four Squares Theorem" shows that every positive integer can be expressed as a sum of four squares of integers. That is, for any positive integer k, there is a representation of k in the form $k = x_1^2+x_2^2+x_3^2+x_4^2 = x^T I x$, where $x \in \mathbb{Z}^4$ and I is the 4×4 identity matrix. More generally, we say that a quadratic form Q—a degree-two homogeneous polynomial in n independent variables—represents an integer k if there is a solution $x \in \mathbb{Z}^n$ to the equation $k = Q(x)$. In 1993, John Conway and William Schneeberger found a striking criterion, the "Fifteen Theorem," that characterizes the integral quadratic forms that represent all positive integers: *Suppose that $Q(x) = x^T Ax$ is a quadratic form with positive definite, integral matrix A. Then Q represents all positive integers if and only if it represents the positive integers up to* 15. Thus, verification of representations up to 15 suffices to confirm verifications for all positive integers—even large ones like 15365639. (While 15365639 is interesting for its own reasons, that's another story.) Manjul Bhargava gave an elegant proof of the Fifteen Theorem in 2000. Since then, a number of beautiful generalizations and analogs have been found: Bhargava obtained a criterion for the representation of primes. Then, in joint work with Jonathan Hanke, he proved the "290 Theorem," an analog of the Fifteen Theorem for quadratic forms that have integer coefficients but do not have integral matrices (e.g., $x_1^2+x_1x_2+x_2^2+x_3^2+x_3x_4+x_4^2$). Meanwhile, Wieb Bosma and Ben Kane obtained a version of the Fifteen Theorem for representation of integers by sums of triangular numbers. And Byeong Moon Kim, Myung-Hwan Kim, and Byeong-Kweon Oh found criteria for representation of quadratic forms by other quadratic forms(!).

Problem (proposed by Scott Duke Kominers, Harvard University): (1) Prove that every positive integer can be represented in the form $T_p+T_q+T_r$, where T_p, T_q, and T_r are triangular numbers. (2) Prove that every positive integer can be represented in the form $p\bar{p}+3q\bar{q}$, where $p = p_1+p_2\sqrt{-2}$ $(p_1, p_2 \in \mathbb{Z})$ and $q = q_1+q_2\sqrt{-2}$ $(q_1, q_2 \in \mathbb{Z})$ are integers in the quadratic field $\mathbb{Q}(\sqrt{-2})$. (3) Can you characterize the complete set of integers that the quadratic form $p^2 + q^2 + 10r^2$ *does not* represent?

References:

- M. Bhargava, *On the Conway-Schneeberger fifteen theorem*, Quadratic forms and their applications: Proceedings of the Conference on Quadratic Forms and Their Applications, July 5–9, 1999, University College Dublin, Contemporary Mathematics, vol. 272, American Mathematical Society, 2000, pp. 27–37.
- J. H. Conway, *Universal quadratic forms and the fifteen theorem*, Quadratic forms and their applications: Proceedings of the Conference on Quadratic Forms and Their Applications, July 5–9, 1999, University College Dublin, Contemporary Mathematics, vol. 272, American Mathematical Society, 2000, pp. 23–26.
- M.-H. Kim, *Recent developments on universal forms*, Algebraic and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics, vol. 344, American Mathematical Society, 2004, pp. 215–228.

– S. D. Kominers, *On universal binary hermitian forms*, INTEGERS **9** (2009), no. 1, 9–15.
– J. Liouville, *Nouveaux théorèmes concernant les nombres triangulaires*, Journal de Mathématiques Pures et Appliquées **8** (1863), 73–84.
– I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, 2008.
– K. Ono and K. Soundararajan, *Ramanujan's ternary quadratic form*, Inventiones Mathematicae **130** (1997), no. 3, 415–454.

• 1997: Merton and Scholes Nobel Prize: In addition to applications in the physical sciences, mathematics plays a key role in many other fields, including economics and finance. While there isn't a Nobel prize in economics or in mathematics, the Royal Swedish Academy of Sciences awards the Bank of Sweden Prize in Economic Sciences in Memory of Alfred Nobel, which is for all practical purposes a Nobel prize in economics. From their award announcement in 1997: *Robert C. Merton and Myron S. Scholes have, in collaboration with the late Fischer Black, developed a pioneering formula for the valuation of stock options. Their methodology has paved the way for economic valuations in many areas. It has also generated new types of financial instruments and facilitated more efficient risk management in society.* When one considers the trillions of dollars traded annually in the world economy, the impact and importance of such mathematics is clear. (See the problem from 1962 for another Nobel prize in economics from very interesting mathematics.)

Problem (proposed by Steven J. Miller, Williams College): One of the inputs in the Black-Scholes-Merton formula is the cumulative distribution function of the standard normal. If X is a normal variable with mean μ and variance σ^2, it's density is $f_{\mu,\sigma}(x) = (2\pi)^{-1/2}\exp(-(x-\mu)^2/2\sigma^2)$, and its cumulative distribution function $F_{\mu,\sigma}(x) = \int_{-\infty}^{x} f_{\mu,\sigma}(t)dt$. Unfortunately there is no closed-form expression for the cumulative distribution function, but one can derive a rapidly converging series expansion; find it! *Note: this function is well-studied in the literature, and is a simple rescaling of the error function.*

References:
– The Royal Swedish Academy of Sciences, Press Release, 14 October 1997. `http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1997/press.html`.
– Wikipedia, *Black-Scholes*, `http://en.wikipedia.org/wiki/Black%E2%80%93Scholes`.

• 2001: Project Euler was created by Colin Hughes in 2001. It's an outstanding website, and has provided countless hours of enjoyment to mathematicians, computer scientists, and other computationally minded people. From the website: *Project Euler is a series of challenging mathematical/computer programming problems that will require more than just mathematical insights to solve. Although mathematics will help*

you arrive at elegant and efficient methods, the use of a computer and programming skills will be required to solve most problems. The motivation for starting Project Euler, and its continuation, is to provide a platform for the inquiring mind to delve into unfamiliar areas and learn new concepts in a fun and recreational context.

Problem (proposed by Steven J. Miller, Williams College): There are over 400 problems of varying level of difficulty on its website: `http://projecteuler.net/`. To solve these problems quickly (typically in a minute or less) requires a deep understanding of both mathematics (which often has formulas to cut down on the computations) and computer science (to efficiently code the problem). Form a group at your school and see how many of these problems you can solve.

- 2005: Today computers are indispensable tools for many researchers, and they are constantly being tasked with more and more different assignments. Unfortunately, many of the popular programs are closed-source, which means the actual nuts and bolts of the algorithms and the implementations are hidden from the user. This makes it difficult for a researcher to check and verify that the program will do what it claims. William Stein developed Sage in response to these issues. Starting in 2005 word of Sage began to spread. From its homepage: *Sage is a free open-source mathematics software system licensed under the GPL. It combines the power of many existing open-source packages into a common Python-based interface. Mission: Creating a viable free open source alternative to Magma, Maple, Mathematica and Matlab.*

  Problem (proposed by Steven J. Miller, Williams College): Go to Sage's homepage and see what it can do.

  References:
  - `http://www.sagemath.org/`.
  - `http://sagemath.blogspot.com/2009/12/mathematical-software-and-me-very.html`

- 2009: 100th Anniversary of Brouwer's Fixed Point Theorem. Whether one admires the elegance of a far-reaching theorem in mathematics or its applications, Luitzen E.J. Brouwer proved one in 1912 (a specific case in 1909) that captures both tastes. Let $f : B^n \to B^n$ be a continuous function on the unit ball $B^n := \{x \in \mathbb{R}^n : \|x\| \leq 1\}$ in a Euclidean space $\mathbb{R}^n$. Brouwer showed that f always has at least one fixed point. In other words, there exists an $x \in B^n$ such that $f(x) = x$.

  Theorems of this nature can spend decades in the the realm of abstraction, devoid of visible applications to other fields. However, Brouwer's Fixed-Point Theorem is found in areas beyond its classical use in Analysis and Topology. John Forbes Nash Jr. sealed its place in the field of Game Theory with his groundbreaking 1950 thesis, "Non-Cooperative Games". Using Brouwer's Fixed-Point Theorem, Nash proved the existence of equalibria in the theory of non-cooperative games. Nash Equilibria, as

they later became to be known, are equalibrium points in an n person non-cooperative game in which each of the n players with pure or mixed strategies make the best decision possible taking into account the best decision that can be made by the other $n-1$ players. In 1994, Nash received the Nobel Prize in Economics for his epic contribution. This application, among others, highlights the importance of such theorems in the past, present, and the future to come.

Problem (Proposed by James M. Andrews, University of Memphis, and Avery T. Carr, Emporia State University): Let n be a natural number and $\mathbf{C}(\mathbf{B^n})$ be the set of continuous functions f such that $f : B^n \to B^n$. By Brouwer's Fixed-Point Theorem there exists a set $\mathbf{D} := \{x \in \mathbf{B}^n : \exists f \in \mathbf{C}(\mathbf{B^n}),\ f(x) = x\}$. Show that $\mathbf{D} = \mathbf{B}^n$. What if we only assume that $\mathbf{C}(\mathbf{B^n})$ is the set of all continuous functions that are 1-1 and onto? What if we consider them to be onto only? Furthermore, what if we consider them to be 1-1 only?

References:

– J. Nash's Thesis, *Non-Cooperative Games*, PhD Thesis, Princeton University 1950.
http://www.princeton.edu/mudd/news/faq/topics/Non-Cooperative_Games_Nash.pdf.
– Wikipedia, *Brouwer's fixed-point theorem*,
http://en.wikipedia.org/wiki/Brouwer_fixed_point_theorem.

E-mail address: sjm1@williams.edu

Associate Professor of Mathematics, Department of Mathematics and Statistics, Williams College, Williamstown, MA 01267

E-mail address: jmandrew@memphis.edu

Alumni, Department of Mathematics, University of Memphis, Memphis, TN 38152

E-mail address: acarr3@g.emporia.edu

Graduate Student, Mathematics Department, Emporia State University, Emporia, KS 66801